Carlo Casolo

Appunti di

Teoria dei numeri

per l'insegnamento di "Complementi di Algebra"
per la laurea magistrale in Matematica

Anno Accademico 2018-2019

Indice

1

Aritmetica di base

Rispetto a quanto già studiato nel corso di Algebra I, in questo primo capitolo si vedrà relativamente poco di nuovo: esso è un prologo ed un ripasso, rapido ma con qualche precisazione, di concetti e strumenti elementari noti. Dando per superati (rispetto al percorso formativo) gli esercizi standard del tipo di quelli, già svolti, delle dispense di Algebra I, accompagneremo questo ripasso con alcuni problemi tratti da diverse competizioni matematiche.

Per tutte queste dispense indicheremo con $\mathbb{Z}$ l'insieme dei numeri interi, con $\mathbb{N}$ quello dei numeri naturali (cioè interi non negativi), e con $\mathbb{N}^*$ l'insieme dei numeri naturali diversi da 0 (interi positivi); $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sono, rispettivamente, gli insiemi dei numeri razionali, dei numeri reali, e dei numeri complessi.

1.1. Divisione

Cominciamo col rivedere una delle proprietà veramente fondamentali dell'insieme $\mathbb{Z}$: la *divisione euclidea*.

Teorema 1.1 (Divisone euclidea)**.** *Siano a, b numeri interi, con $b \neq 0$. Allora esistono, e sono unici, numeri interi q, r tali che*

$$a = bq + r$$

e $0 \leq r \leq |b| - 1$.

Dimostrazione. Sia S l'insieme di tutti i numeri naturali della forma $a - bt$, con $t \in \mathbb{Z}$. S non è vuoto; infatti, se $a \geq 0$ allora $a = a - b0 \in S$; se $a < 0$, allora, poiché $b^2 \geq 1$, $a - b(ba) = a(1 - b^2) \in S$. Dunque, per il principio del buon ordinamento, S ha un elemento minimo r, ed esiste un $q \in \mathbb{Z}$ tale che $a = bq + r$.
Se fosse $r \geq |b|$, allora

$$0 \leq r - |b| = a - bq - |b| = a - b(q \pm 1) \in S$$

contro la minimalità di r. Dunque $0 \leq r < |b|$.
La dimostrazione dell'unicità di q ed r è immediata. □

Siano $a, b \in \mathbb{Z}$: scriviamo $a|b$ e diciamo che a *divide* b se esiste $c \in \mathbb{Z}$ tale che $ac = b$. Osserviamo che $a|0$ per ogni $a \in \mathbb{Z}$.

Se m, n sono numeri interi, un elemento $d \in \mathbb{Z}$ si dice un *Massimo Comun Divisore* di m e n se $d|m$, $d|n$, e per ogni intero c, se $c|m$ e $c|n$ allora $c|d$. Ogni coppia di interi non entrambi nulli ammette due massimi comun divisori, che differiscono per il segno; denoteremo con (m, n) (oppure, nel caso possano nascere fraintendimenti, con $mcd(m, n)$) il massimo comun divisore *non negativo* di m e n. Si noti che $(a, 0) = |a|$ per ogni $a \in \mathbb{Z}$. I numeri interi m, n si dicono *coprimi* se $(m, n) = 1$.

Proposizione 1.2 (Identità di Bezout[1])**.** *Siano a, b numeri interi non entrambi nulli. Allora il massimo comun divisore (a, b) è il minimo intero positivo d che si può scrivere nella forma $d = ua + wb$, con $u, w \in \mathbb{Z}$.*

Dimostrazione. Siano a, b numeri interi non entrambi nulli; allora l'insieme

$$\{z = xa + yb \mid x, y \in \mathbb{Z},\ z \geq 1\}$$

è non vuoto e pertanto ha un minimo $d = ua + wb$. Dividiamo a per d, $a = qd + r$, con $0 \leq r \leq d - 1$. Ora

$$0 \leq r = a - qd = (1 - qu)a + (-qw)b,$$

e quindi, per la scelta di d, deve essere $r = 0$. Dunque d divide a. Analogamente si prova che d divide b. Infine, se c è un divisore comune di a e b, chiaramente c divide anche d. Pertanto $d = (a, b)$. □

Esercizio 1.1. Dati due numeri interi positivi coprimi a e b, provare che esistono $x, y \in \mathbb{N}^*$ tali che $xa - yb = 1$.

Molti fra i problemi proposti come esercizio in queste note, soprattutto nei primi capitoli, sono tratti da diverse competizioni matematiche per studenti delle scuole superiori. Il primo che - giustamente - affrontiamo, è stato proposto nella prima edizione delle Olimpiadi Matematiche Internazionali, che si disputò in Romania nel 1959. Oggi, questo problema risulta quasi banale.

Problema 1 (IMO[2], Bucarest 1959)**.** *Provare che per ogni intero positivo n la frazione*

$$\frac{21n + 4}{14n + 3}$$

è in forma ridotta.

Soluzione. Si tratta di provare che, per ogni intero positivo n,

$$mcd(21n + 4, 14n + 3) = 1.$$

Ma si trova subito che

$$3(14n + 3) + (-2)(21n + 4) = 1,$$

[1] Étienne Bézout (1730–1783), matematico francese.

[2] *International Mathematical Olympiad*: si tratta della più antica e importante competizione matematica internazionale per studenti delle scuole superiori.

quindi, per la Proposizione 1.2, $21n+4$ e $14n+3$ sono coprimi. ∎

La formula di Bezout si estende ad un numero finito arbitrario di numeri interi non tutti nulli. La dimostrazione è lasciata per esercizio.

Proposizione 1.3. *Siano $a_1, a_2, \ldots, a_s$ numeri interi non tutti nulli e $d = mcd(a_1, a_2, \ldots, a_s)$; allora d è il minimo intero positivo tale che esistono $x_1, x_2, \ldots, x_s \in \mathbb{Z}$ con*

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s = d.$$

Un *minimo comune multiplo* di due o più numeri interi $a_1, a_2, \ldots, a_s$ è un intero $m \in \mathbb{N}$ che è multiplo di ogni a_i e divide ogni altro multiplo comune di essi; se uno degli a_i è 0, l'unico multiplo comune è 0, altrimenti esiste un unico minimo comune multiplo positivo, che denotiamo con $mcm(a_1, \ldots, a_n)$. Se a, b sono interi positivi non è difficile verificare che

$$ab = mcd(a, b) \cdot mcm(a, b). \tag{1.1}$$

ESEMPIO 1. *Provare che per ogni $2 \leq n \in \mathbb{N}$, $u_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ non è un numero intero.*

Sia 2^k la massima potenza di 2 minore o uguale a n (quindi $2^k \leq n < 2^{k+1}$), e sia m il minimo comune multiplo tra gli tutti gli interi $1, 2, \ldots, n$ escluso 2^k. Allora la massima potenza di 2 che divide m è 2^{k-1}. Ora abbiamo

$$mu_n = m + \frac{m}{2} + \cdots + \frac{m}{n}$$

dove ogni addendo del termine di destra è un intero con l'eccezione di $\frac{m}{2^k}$. Poiché, per quanto osservato, $\frac{m}{2^k}$ non è un intero, si deduce che mu_n non è un numero intero, e quindi che u_n non è un intero. ∎

Esercizio 1.2. Sia n un intero positivo. Si provi che

$$v = 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n+1}$$

non è un numero intero.

Esercizio 1.3. Si dimostri l'identità (1.1).

L' Algoritmo di Euclide È tuttora il metodo meccanico più efficiente per determinare il massimo comun divisore di due numeri interi a, b non nulli. Non è restrittivo illustrarlo nel caso in cui a e b sono entrambi numeri positivi. Si pone $a_0 = a$, $a_1 = b$, ed il primo passo è dividere a_0 per a_1:

$$a_0 = q_1a_1 + a_2 \quad \text{con} \quad 0 \leq a_2 < a_1;$$

quindi, se $a_2 \neq 0$, si divide a_1 per a_2, ottenendo un resto a_3 con $0 \leq a_3 < a_2$. Si prosegue con tale catena di divisioni successive; ovvero, arrivati ad a_i si definisce a_{i+1} come il resto

della divisione di a_{i-1} per a_i:

$$\begin{aligned}
a_0 &= q_1 a_1 + a_2 \\
a_1 &= q_2 a_2 + a_3 \\
a_2 &= q_3 a_3 + a_4 \\
&\cdots\cdots \\
a_{i-1} &= q_i a_i + a_{i+1} \\
&\cdots\cdots
\end{aligned}$$

In questo modo, si ottiene una sequenza di resti positivi

$$b = a_1 > a_2 > a_3 > \cdots > a_{i-1} > a_i > a_{i+1} > \cdots > a_{n+1} = 0$$

Questa sequenza, costituita da numeri naturali, termina in zero dopo un numero finito di passi (che ho indicato con n). Sia quindi a_n l'ultimo resto non nullo; allora a_n *è il massimo comun divisore positivo di* a e b.

L'algoritmo di Euclide si basa sul seguente fatto ovvio, ma molto utile nella soluzione dei problemi che vedremo tra un po'.

Lemma 1.4 (Euclide)**.** *Siano a e b interi non nulli. Allora, per ogni $q \in \mathbb{Z}$, $(a, b) = (b, a + qb)$.*

L'algoritmo di Euclide consente inoltre, percorso a ritroso, di determinare anche due numeri interi ru, w tali che $(a, b) = ua + wb$.

Esempio 2. *Trovare $u, w \in \mathbb{Z}$ tali che* $6468u + 2275w = (6468, 2275)$.

Applicando l'algoritmo di Euclide,

$$\begin{aligned}
6468 &= 2 \cdot 2275 + 1918 \\
2275 &= 1 \cdot 1918 + 357 \\
1918 &= 5 \cdot 357 + 133 \\
357 &= 2 \cdot 133 + 91 \\
133 &= 1 \cdot 91 + 42 \\
91 &= 2 \cdot 42 + 7 \\
42 &= 6 \cdot 7 + 0
\end{aligned}$$

Quindi $(6468, 2275) = 7$. Ora

$$\begin{aligned}
7 \quad &= 91 - 2 \cdot 42 = 91 - 2(133 - 91) = 3 \cdot 91 - 2 \cdot 133 = \\
&= 3(357 - 2 \cdot 133) - 2 \cdot 133 = -8 \cdot 133 + 3 \cdot 357 = \\
&= 43 \cdot 357 - 8 \cdot 1918 = \\
&= -51 \cdot 1918 + 43 \cdot 2275 = \\
&= -51 \cdot 6468 + 145 \cdot 2275,
\end{aligned}$$

e pertanto $u = -51$, $w = 145$. ■

Dall'identità di Bezout e dal fatto ovvio che, se a, b sono numeri interi non entrambi nulli e $d = (a, b)$, allora $d | ax + by$ per ogni coppia di numeri interi x, y, segue la seguente Proposizione, che determina il caso fondamentale di *equazione diofantea* (vedi sezione 1.4).

Proposizione 1.5. *Siano a, b numeri interi non entrambi nulli e $n \in \mathbb{Z}$; allora l'equazione*

$$ax + by = n$$

ammette soluzioni in $\mathbb{Z}$ se e solo se $(a, b)|n$. In generale, se $a_1, a_2, \ldots, a_k$ sono interi non tutti nulli, l'equazione $a_1x_1 + a_2x_2 + \cdots + a_kx_k = n$ ammette soluzioni intere se e solo se $mcd(a_1, a_2, \ldots, a_k)$ divide n.

Esercizio 1.4. Siano $n \in \mathbb{N}^*$, a, b interi non nulli tali che $(a, b) \mid n$, e sia (x_0, y_0) una soluzione intera dell'equazione $ax + by = n$. Si provi che l'insieme delle soluzioni intere dell'equazione è

$$\left\{ \left(x_0 + t\frac{b}{(a,b)}, y_0 - t\frac{a}{(a,b)} \right) \;\middle|\; t \in \mathbb{Z} \right\}.$$

Problemi

Iniziamo a proporre alcuni problemi tratti da competizioni matematiche per studenti; vediamo prima tre esempi risolti.

Problema 2 (IMO, Taiwan 1998)**.** *Determinare tutte le coppie (a, b) di interi positivi tali che $ab^2 + b + 7$ divide $a^2b + a + b$.*

Soluzione. Se $ab^2 + b + 7$ divide $a^2b + a + b$ allora divide

$$b(a^2b + a + b) - a(ab^2 + b + 7) = b^2 - 7a. \qquad (*)$$

Se $b^2 = 7a$ si ha $a = 7x^2$, $b = 7x$ (con $x \in \mathbb{N}^*$) che sono delle soluzioni.
Se $b^2 - 7a > 0$, allora $0 < ab^2 + b + 7 \leq b^2 - 7a \leq b^2$ che è una contraddizione.
Sia $b^2 - 7a < 0$, allora $ab^2 < ab^2 + b + 7 \leq 7a - b^2 < 7a$, da cui $b^2 < 7$ e quindi $b = 1, 2$.
Se $b = 2$, sostituendo in $(*)$ si deduce che $4a + 9$ divide $7a - 4$, il che si vede subito non sussiste per $a \in \mathbb{N}^*$. Rimane il caso $b = 1$. Allora da $(*)$ si deduce che $a + 8$ divide $7a - 1$; quindi $a+8$ divide $7(a+8)-(7a-1) = 57 = 19 \cdot 3$. Poiché $a \geq 1$ si hanno le due possibilità $a + 8 = 19$ e $a + 8 = 57$, che danno, rispettivamente, $a = 11$ e $a = 19$.
In conclusione, le coppie (a, b) cercate sono $(11, 1), (49, 1)$ e $(7x^2, 7x)$ con $x \in \mathbb{N}^*$. ∎

Problema 3 (Putnam[3], 2000)**.** *Si provi, che per ogni coppia di interi $n \geq m \geq 1$, l'espressione*

$$\frac{mcd(m, n)}{n} \binom{n}{m}$$

è un numero intero.

Soluzione. Sia $d = \mathrm{m}cd(m, n)$. Per la Proposizione 1.2 esistono due numeri interi a, b tali che $d = an + bm$. Dunque

$$\frac{d}{n}\binom{n}{m} = \frac{an + bm}{n}\binom{n}{m} = a \cdot \binom{n}{m} + b \cdot \frac{m}{n}\binom{n}{m} = a \cdot \binom{n}{m} + b \cdot \binom{n-1}{m-1},$$

[3]La *William Lowell Putnam mathematical competition* è un gara matematica per studenti dei primi anni dell'Università che si disputa annualmente tra Canada e Stati Uniti dal 1938 (con l'interruzione negli anni della seconda guerra mondiale).

che è un numero intero. ∎

Quello che segue un problema più impegnativo (anche se, come si vedrà, i metodi della soluzione sono del tutto elementari).

Problema 4 (Giappone 1996)**.** *Siano n, m interi positivi coprimi. Si determini*

$$(5^m + 7^m, 5^n + 7^n).$$

SOLUZIONE. Possiamo porre $1 \leq m < n$. Il gioco si sviluppa intorno alla identità elementare

$$5^n + 7^n = (5^m + 7^m)(5^{n-m} + 7^{n-m}) - (7^m 5^{n-m} + 5^m 7^{n-m});$$

dalla quale segue, per la procedura euclidea (Lemma 1.4),

$$(5^m + 7^m, 5^n + 7^n) = (5^m + 7^m, 7^m 5^{n-m} + 5^m 7^{n-m}) \qquad (\dagger)$$

(si osservi che questo non richiede la coprimità di m e n).
Sia $n \geq 2m$; allora $n - m \geq m$ e $7^m 5^{n-m} + 5^m 7^{n-m} = 5^m 7^m (5^{n-2m} + 7^{n-2m})$; poiché né 5 né 7 dividono $5^m + 7^m$, dalla (†) segue

$$(5^m + 7^m, 5^n + 7^n) = (5^m + 7^m, 5^{n-2m} + 7^{n-2m}). \qquad (*)$$

Se invece $n < 2m$, allora $n - m < m$ e, ragionando in modo analogo a sopra, si ottiene

$$(5^m + 7^m, 5^n + 7^n) = (5^m + 7^m, 5^{2m-n} + 7^{2m-n}). \qquad (**)$$

Queste due identità suggeriscono chiaramente la possibilità di ragionare per induzione, ed osservando che un elemento che si mantiene nella relazione tra i due diversi esponenti nelle riduzioni $(*)$ e $(**)$ è la parità della loro somma ($n + m$ inizialmente), si capisce sarà opportuno distinguere i due casi $n + m$ pari e $n + m$ dispari.
Un punto essenziale è poter propriamente operare un passo induttivo; cioè che passando dalla coppia m, n alla coppia $m, 2n - m$ oppure $m, 2m - n$, secondo i casi, la somma dei termini effettivamente diminuisca. Nel primo caso si ha sempre $m + (n - 2m) = n - m < m + m$ e non dà problemi, nel secondo caso $m + (2m - n)$ è uguale a $m + n$ se $m = n$. Dobbiamo quindi escludere che in qualche passo della riduzione induttiva capiti che i due esponenti in ballo siano uguali (se non al termine, quando sono 1). Da qui la richiesta che n, m siano coprimi; questo infatti assicura che anche le coppie $m, n - 2m$ e $m, 2m - n$ sono coprime, e così via. Supponiamo quindi che m, n siano coprimi
Sia $n + m$ pari (dunque, in quanto coprimi, n e m sono entrambi dispari); poiché il caso più piccolo si ha per $n = 1 = m$ e in questo caso il MCD è $5 + 7 = 12$, formuliamo un primo enunciato:

(i) *se $n + m$ è pari, allora* $(5^m + 7^m, 5^n + 7^n) = 12$.

La dimostrazione è per induzione su $n + m$; il caso iniziale essendo stato osservato prima. Siano quindi n, m dispari con $n + m \geq 4$. Se $n > 2m$, applicando $(*)$ e l'ipotesi induttiva (dato che $n - 2m$ è dispari e $m + (n - 2m) < n + m$),

$$(5^m + 7^m, 5^n + 7^n) = (5^m + 7^m, 5^{n-2m} + 7^{n-2m}) = 12.$$

Se $n < 2m$, similmente si applica $(**)$ e l'ipotesi induttiva, ottenendo

$$(5^m + 7^m, 5^n + 7^n) = (5^m + 7^m, 5^{2m-n} + 7^{2m-n}) = 12.$$

Veniamo al caso $n + m$ dispari, il cui minimo si ha per $m = 1, n = 2$, per il quale si ha $(5 + 7, 5^2 + 7^2) = (12, 74) = 2$. In questo caso proviamo allora

(ii) *se $n + m$ è dispari, allora $(5^m + 7^m, 5^n + 7^n) = 2$.*

La dimostrazione è però del tutto analoga a quella del caso precedente e non la ripetiamo. ■

* * *

• Ed ora qualche problema da affrontare in proprio: le soluzioni si trovano nella sezione 4.4.

Problema 5 (Gara Matematica[4], 2017)**.** *Determinare un numero naturale di 100 cifre, tutte diverse da zero, che sia divisibile per la somma delle sue cifre.*

Problema 6 (Germania 1996)**.** *Una pietra si muove sui punti a coordinate intere del piano secondo le regole seguenti:*

(i) Da ogni punto (a, b) la pietra può spostarsi in $(2a, b)$ oppure $(a, 2b)$.

(ii) Da ogni punto (a, b) la pietra può muovere in $(a - b, b)$ se $a > b$, oppure in $(a, b - a)$ se $a < b$.

Si dica quali punti (x, y) può raggiungere la pietra partendo dal punto $(1, 1)$.

Problema 7 (IMO, Mosca 1992)**.** *Si determinino tutte le terne di numeri interi a, b, c con $1 < a < b < c$ tali che $(a - 1)(b - 1)(c - 1)$ divide $abc - 1$.*

Problema 8 (San Pietroburgo 2008)**.** *Siano a, b e c interi positivi distinti; si provi che*

$$mcd(ab + 1, ac + 1, bc + 1) < \frac{a + b + c}{3}.$$

1.2. Numeri primi

Un numero intero p è *primo* se $p \neq 0, 1, -1$ e l'insieme dei divisori di p è $\{1, -1, p, -p\}$.

La proprietà fondamentale dei numeri primi è espressa nella seguente Proposizione.

Proposizione 1.6. *Siano $a, b, c \in \mathbb{Z}$. Se $a|bc$ e $(a, b) = 1$ allora $a|c$. In particolare, se p è un numero primo e $p|bc$ allora $p|b$ o $p|c$.*

[4] La *Gara Matematica*, riservata agli studenti dell'ultimo biennio della scuola secondaria, si svolge annualmente presso il Dipartimento di Matematica di Firenze dal 1983.

Dimostrazione. Siano $a, b, c \in \mathbb{Z}$ con $a|bc$ e $(a, b) = 1$. La seconda condizione implica che a e b non sono entrambi nulli, quindi per la formula di Bezout, esistono $u, w \in Z$ tali che $1 = ua + wb$. Moltiplicando per c, si ha $c = uac + wbc$ e siccome a divide sia uac che wbc si conclude che a divide c.
Ora, sia p un primo e $p|bc$. Se p non divide b allora (essendo p primo) $(p, b) = 1$ e dunque p divide c per quanto appena provato. □

A partire dalla proposizione 1.6 e dal fatto (che si prova facilmente per induzione) che ogni numero intero diverso da $0, 1, -1$ è diviso da almeno un numero primo si dimostra il Teorema fondamentale dell'aritmetica (tutto questo è stato fatto nel corso di Algebra I).

Teorema 1.7. *Sia $a \in \mathbb{Z}$, $a \neq 0, 1, -1$. Allora esistono primi $p_1, p_2, \ldots, p_s$ tali che*

$$a = p_1 p_2 \cdots p_s.$$

Tale fattorizzazione è unica nel senso che se $a = q_1 q_2 \cdots q_t$, con $q_1, q_2, \ldots, q_t$ numeri primi, allora $s = t$ ed esiste una permutazione σ di $\{1, 2, \ldots, s\}$ tale che, per ogni $i = 1, 2, \ldots, s$, $q_i = \pm p_{\sigma(i)}$.

Denotiamo con $\mathbb{P}$ l'insieme di tutti i numeri primi positivi. Dal Teorema precedente segue che ogni intero $a \neq 0$ si scrive come il prodotto

$$a = \pm \prod_{p \in \mathbb{P}} p^{\nu_p(a)}$$

dove gli esponenti $\nu_p(a)$ sono numeri naturali univocamente determinati, e quasi tutti nulli (cioè $\nu_p(a) \neq 0$ solo per un numero finito di primi p).

Una celebre applicazione del Teorema 1.7 è il Teorema di Euclide.

Teorema 1.8. *Esistono infiniti numeri primi.*

Dimostrazione. Supponiamo, per assurdo, che l'insieme dei numeri primi sia finito. Siano $p_1, p_2, \ldots, p_k$ tutti i numeri primi positivi distinti e sia $n = p_1 p_2 \cdots p_k$. Poichè $n \geq 1$, il numero ammette un divisore primo, che deve essere pertanto uno dei p_i (con $i \in \{1, 2, \ldots, k\}$). Ma allora si avrebbe che tale primo divide sia n che $n+1$, il che è chiaramente impossibile. □

Radici di numeri interi. Un'altra semplice ma fondamentale applicazione della Proposizione 1.6 riguarda le radici di numeri interi. Se x è un numero reale positivo e m un numero naturale positivo, denotiamo con $\sqrt[m]{x}$ l'unica radice m-esima reale e positiva di x.

Teorema 1.9. *Siano a, m numeri interi positivi, allora $\sqrt[m]{a} \in \mathbb{Q}$ se e solo se $\sqrt[m]{a} \in \mathbb{N}$ (cioè a è la potenza m-esima di un numero intero positivo).*

Dimostrazione. Sia $\sqrt[m]{a}$ un numero razionale, cioè $\sqrt[m]{a} = \frac{r}{s}$ con r, s interi positivi e coprimi. Allora, elevando alla m-esima potenza,

$$s^m a = r^m.$$

In particolare, $a|r^m$. D'altra parte, poiché $(s^m, r^m) = 1$, la Proposizione 1.6 assicura che r^m divide a. Dunque $a = r^m$ e $\sqrt[m]{a} = r \in \mathbb{N}$. □

ESEMPIO 3. *Siano $a, b \in \mathbb{N}^*$ tali che $\sqrt{a} + \sqrt{b} \in \mathbb{Q}$; provare che a e b sono quadrati in $\mathbb{N}$.*
Sia $\sqrt{a} + \sqrt{b} = x$, con $x \in \mathbb{Q}$; allora

$$2\sqrt{ab} = (\sqrt{a} + \sqrt{b})^2 - (\sqrt{a}^2 + \sqrt{b}^2) = x^2 - a - b$$

è un numero razionale. Dunque, per il Teorema 1.9, $ab = t^2$ per qualche $t \in \mathbb{N}$. Allora

$$x = \sqrt{a} + \sqrt{b} = \sqrt{a} + \frac{t}{\sqrt{a}},$$

da cui

$$\sqrt{a} = \frac{a+t}{x} \in \mathbb{Q}.$$

Dunque, a è un quadrato in $\mathbb{N}$ per il Teorema 1.9; di conseguenza anche $\sqrt{b} \in \mathbb{Q}$ e b è un quadrato in $\mathbb{N}$. ■

Primi di Mersenne e di Fermat. I numeri primi sono uno degli argomenti di studio più importanti di tutta la Teoria dei Numeri, che annovera al suo attivo alcuni forse tra i più difficili e profondi risultati della matematica, ed una serie di congetture il cui enunciato riesce talvolta ad attirare anche i non matematici; ed anche noi, che nel seguito di questo modesto corso continueremo a dimostrare (o anche solo citare) risultati, magari non di vertiginosa altezza ma comunque interessanti, sui numeri primi. Per il momento, facciamo la conoscenza di due classi di numeri primi, quelli di Mersenne e quelli di Fermat, storicamente importanti, nei cui membri, attestati o presunti, non è raro imbattersi anche in altre parti della matematica.

Prima, richiamiamo due formule alla quali capita spesso di ricorrere nella soluzione di problemi numerici elementari; oltre ad essere certamente ben note, la loro dimostrazione, che consiste nello svolgimento del prodotto nei membri di destra, è immediata.

Proposizione 1.10. *Siano $a, b, n \in \mathbb{Z}$ con $n \geq 2$.*

1) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$.

2) Se n è dispari, $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \ldots - ab^{n-2} + b^{n-1})$.

(Si osservi che la 2) è di fatto un caso particolare della 1).) Un facile ma utile corollario è la seguente Proposizione.

Proposizione 1.11. *Siano $, n, m \in \mathbb{N}^*$ e $1, -1 \neq a \in \mathbb{Z}$; allora*

$$(a^n - 1, a^m - 1) = a^{(n,m)} - 1.$$

Dimostrazione. Siano $d = (a^n - 1, a^m - 1)$ e $c = mcd(n, m)$. Allora, $a^c - 1$ divide d per la Proposizione 1.10 (con $b = 1$).
Viceversa, siano $u, -v \in \mathbb{Z}$, tali che $c = un + (-v)m = un - vm$. Scambiando eventualmente n e m, risultano u, v sono positivi. Ancora dalla Proposizione 1.10 segue che d divide $a^{nu} - 1$ e $a^{mv} - 1$. Quindi d divide la differenza di questi, $a^{nu} - a^{mv} = a^{mv}(a^{nu-mv} - 1) = a^{mv}(a^c - 1)$. Poichè chiaramente d e a sono coprimi, si conclude che d divide $a^c - 1$. □

Un'altra formula di impiego frequente è quella dello sviluppo della potenza di un binomio (formula di Newton), che diamo per familiare e non ripetiamo, così come diamo per assodata la conoscenza dei coefficienti binomiali e delle loro proprietà fondamentali[5].

Ponendo $b = 1$ nella Proposizione 1.10 si dimostra agevolmente il seguente fatto.

Proposizione 1.12. *Siano $a, n \in \mathbb{N}^*$, $n > 1$.*

(1) Se $a^n - 1$ è un primo, allora $a = 2$ e n è un primo.

(2) Sia p un primo; se $p^n + 1$ è un primo, allora $p = 2$ e $n = 2^m$ per qualche $m \in \mathbb{N}^*$.

Dimostrazione. (1) Poichè $a^n - 1 = (a-1)(a^{n-1} + \cdots + a + 1)$, se $a^n - 1$ è primo allora $a = 2$ e, per la stessa considerazione, n è primo.

(2) Se $p^n + 1$ è primo allora deve essere dispari e quindi $p = 2$. Supponiamo che n abbia un divisore primo dispari q, e scriviamo $n = mq$. Allora

$$2^n + 1 = (2^m + 1)(2^{m(q-1)} - (2^{m(q-1)} + \cdots - 2^m + 1)$$

non è primo. Dunque, se $2^n + 1$ è primo, n deve essere una potenza di 2. □

• Per p primo, i numeri del tipo $M_p = 2^p - 1$ sono detti *numeri di Mersenne*. Non tutti i numeri di Mersenne sono primi (il più piccolo numero di Mersenne a non essere primo è $M_{11} = 23 \cdot 89$). Di fatto, non è nemmeno noto se esistano infiniti primi di Mersenne. Al momento della stesura di queste note[6], risultano noti 49 primi di Mersenne, il maggiore dei quali è M_p con $p = 74207281$, scoperto nel Gennaio 2016, la cui espansione decimale comprende 22.338.618 cifre (si tratta, per ora, anche del più grande numero primo conosciuto, ma di questi si sa dai tempi di Euclide che ce ne sono infiniti). E la ricerca continua: chi fosse interessato può consultare il sito internet www.mersenne.org/primes/

• I numeri primi del tipo (2) sono detti *primi di Fermat*. In generale, per $m \in \mathbb{N}$, l'intero $F_m = 2^{2^m} + 1$ è detto m-esimo numero di Fermat. I primi cinque numeri di Fermat

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

sono numeri primi. Sulla base di questa osservazione, P. Fermat affermò che ogni intero di questo tipo è primo. Fu L. Eulero a scoprire come il termine successivo $F_5 = 2^{32} + 1$ non sia primo: infatti $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$, dunque

$$2^{32} = 2^4 \cdot 2^{28} = (641 - 5^4) \cdot 2^{28} = 641 \cdot 2^{28} - (5 \cdot 2^7)^4 = 641 \cdot 2^{28} - (641 - 1)^4$$

e quindi esiste un intero positivo t tale che $2^{32} = 641t - 1$, cioè 641 divide $2^{32} + 1 = F_5$ (si verifica che $F_5 = 641 \cdot 6700417$, dove 641 e 6700417 sono numeri primi). Di fatto, oltre ai cinque detti, nessun altro primo di Fermat è stato a tutt'oggi trovato; e neppure è noto se ne esistano un numero infinito o finito, né se esistano infiniti numeri non-primi nella serie F_n.

[5] Un'altra identità, di uso meno frequente ma che è utile tenere nella cassetta degli attrezzi, è *l'identità di Sophie Germain*:

$$4a^4 + b^4 = (2a^2 + b^2 + 2ab)(2a^2 + b^2 - 2ab).$$

[6] agosto 2017

Esercizio 1.5. Per $n \in \mathbb{N}$, sia $F_n = 2^{2^n} + 1$. Si provi che se $n \neq m$ allora $(F_n, F_m) = 1$ [sugg.: dimostrare, per induzione su $m - n$, che se $n < m$ allora F_n divide $F_m - 2$].

Problemi

Problema 9 (Iberoamericana[7], 2006)**.** *Determinare tutte le coppie (a, b) di numeri interi positivi tali che $2a - 1$ e $2b + 1$ sono coprimi e $a + b$ divide $4ab + 1$.*

SOLUZIONE. Sia (a, b) una delle coppie cercate. Allora

$$a + b \mid 4a(a + b) - (4ab + 1) = 4a^2 - 1 = (2a + 1)(2a - 1), \qquad (*)$$

e similmente

$$a + b \mid 4b(a + b) - (4ab + 1) = 4b^2 - 1 = (2b + 1)(2b - 1). \qquad (**)$$

Sia $d = mcd(a+b, 2b+1)$. Poiché d e $2a-1$ sono coprimi per ipotesi, da $(*)$ e la Proposizione 1.6 segue che d divide $2a+1$, quindi d divide $(2b+1)+(2a+1)-2(a+b) = 2$, e pertanto, poiché $2b + 1$ è dispari, $d = 1$. Dunque, $a + b$ e $2b + 1$ sono coprimi e da $(**)$ (e la Proposizione 1.6) si deduce che $a+b$ divide $2b-1$. In particolare, $a+b \leq 2b-1$ e pertanto $a + 1 \leq b$. Similmente si dimostra che $a + b$ divide $2a + 1$, quindi $a + b \leq 2a + 1$ e dunque $b \leq a + 1$.
In conclusione $b = a + 1$. La verifica che tutte le coppie del tipo $(a, a + 1)$ con $a \geq 1$ soddisfano la condizione assegnata è immediata. ∎

Problema 10 (San Pietroburgo 1987)**.** *Rappresentare il numero $n = 989 \cdot 1001 \cdot 1007 + 320$ come un prodotto di primi.*

SOLUZIONE. Poniamo $a = 1001$; allora $n = (a - 12) \cdot a \cdot (a + 6) + 320$, da cui

$$n = a^3 - 6a^2 - 72a + 320.$$

Trattiamo il termine di destra come un polinomio a coefficienti interi nell'indeterminata a; esaminando i divisori del termine noto, si scopre che 4 ne è una radice, e che quindi il polinomio è diviso da $a - 4$. Svolgendo la divisione si trova

$$\begin{aligned} n &= (a-4)(a^2 - 2a - 80) = (a-4)((a-1)^2 - 81) = (a-4)((a-1)^2 - 9^2) = \\ &= (a-10)(a-4)(a+8) = 991 \cdot 997 \cdot 1009, \end{aligned}$$

che è la fattorizzazione di n in prodotto di primi. ∎

* * *

• Altri problemi da risolvere.

Problema 11 (Gara Matematica, 2009)**.** *Determinare tutte le coppie di numeri interi positivi (x, y) e tutte le coppie di primi distinti (p, q), con $p, q \geq 1$, tali che:*

$$\begin{cases} x^2 - y^2 = p^6 \\ x^3 - y^3 = p^4 q^2 \end{cases}$$

[7] *Olimpiada Iberoamericana de Matematicas*, si disputa dal 1985.

Problema 12 (Czech-Polish-Slovak[8], 2002). *Siano $n, p \in \mathbb{N}^*$ con $n \geq 2$ e p un primo. Si provi che se $n|p-1$ e $p|n^3-1$ allora $4p-3$ è un quadrato perfetto.*

Problema 13 (USA 1973). *Si provi che le radici cubiche di tre numeri primi distinti non sono mai termini (non necessariamente consecutivi) di una progressione aritmetica di numeri reali.*

Problema 14 (Italia[9] 2011). *Determinare tutte le soluzioni (p, n) dell'equazione*

$$n^3 = p^2 - p - 1,$$

dove p è un numero primo e n è un numero intero.

Problema 15 (San Pietroburgo 2001). *Provare che esistono infiniti interi positivi n tali che il più grande divisore primo di n^4+1 è maggiore di $2n$.*

1.3. Congruenze

In questa sezione richiamiamo quegli aspetti di base che dovrebbero essere già noti dal corso di Algebra I, riguardanti il fondamentale metodo delle congruenze; argomento che poi riprenderemo e svilupperemo nel Capitolo 4.

Sia $1 \leq m \in \mathbb{N}$; due numeri interi a e b si dicono *congrui modulo* m, e si scrive

$$a \equiv b \pmod{m},$$

se m divide $a-b$. Come immediata conseguenza della divisione euclidea si ha che due interi a, b sono congrui modulo m se e solo se hanno lo stesso resto nella divisione di ciascuno per m (e sono a loro volta congrui modulo m a tale resto).

Per ogni $1 \leq m \in \mathbb{N}$, la congruenza modulo m è una relazione d'equivalenza su $\mathbb{Z}$; per ogni $a \in \mathbb{Z}$ la classe di equivalenza di a (detta *classe di congruenza* di a modulo m) è l'insieme

$$a + m\mathbb{Z} = \{a + mz \mid z \in \mathbb{Z}\}.$$

L'insieme di tutte la classi di congruenza modulo m (ovvero l'insieme quoziente) si denota con $\mathbb{Z}/m\mathbb{Z}$. Per quanto detto, ogni intero a è congruo modulo m al resto della divisione di a per m; da questo segue che il quoziente $\mathbb{Z}/m\mathbb{Z}$ contiene esattamente m elementi, e che gli interi $0, 1, 2, \ldots, m-1$ costituiscono un insieme di rappresentanti delle classi di congruenza modulo m; ovvero

$$\mathbb{Z}/m\mathbb{Z} = \{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}\}.$$

La proprietà fondamentale delle congruenze consiste nel rispetto delle due operazioni di somma e prodotto; ovvero, fissato m, per ogni $a, b, c, d \in \mathbb{Z}$ con $a \equiv c \pmod{m}, b \equiv d \pmod{m}$, si ha

$$\begin{aligned} a + b &\equiv c + d \pmod{m} \\ ab &\equiv cd \pmod{m}. \end{aligned}$$

[8] Il *Czech–Polish–Slovak Match* si disputa dal 1995 (tra Cechia e Slovacchia prima, dal 2001 si è aggiunta la Polonia).

[9] Le *Olimpiadi di Matematica* italiane si svolgono annualmente dal 1983; la gara finale (da cui sono tratti i problemi) si tiene a Cesenatico.

La seconda si applica, in particolare, alle potenze: fissato $m \geq 2$, per ogni $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$,

$$a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}.$$

Esempio 4. *Determinare l'ultima cifra decimale di* 7^{139}.
L'ultima cifra decimale di $n = 7^{139}$ è il resto della divisione di n per 10, ovvero quell'intero $0 \leq k \leq 9$, tale che $7^{139} \equiv k \pmod{10}$. Ora $7^2 = 49 \equiv -1 \pmod{10}$ e dunque, poichè $139 = 2 \cdot 68 + 3$,

$$7^{139} = (7^2)^{68} \cdot 7^3 \equiv (-1)^{68} 7^3 \equiv 7^3 \equiv 3 \pmod{10}.$$

Quindi $k = 3$. ■

Un punto importante riguarda quegli interi che sono coprimi con il modulo $m \geq 2$. Infatti, per ogni $a \in \mathbb{Z}$, dalla formula di Bezout segue che $(a, m) = 1$ se e solo se esistono interi u, w tali che $au = 1 + wm$, e questo equivale a dire che esiste $u \in \mathbb{Z}$ tale che

$$au \equiv 1 \pmod{m}. \tag{1.2}$$

Osserviamo, ed è importante, che gli interi u che soddisfano la congruenza (1.2) sono univocamente determinati a meno di congruenza; infatti, se $u' \in \mathbb{Z}$ è tale che $au' \equiv 1 \pmod{m}$, allora

$$a(u - u') = au - au' \equiv b - b = 0 \pmod{m},$$

dunque $m | a(u - u')$ e quindi, dato che $(a, m) = 1$, $m | u - u'$, ovvero $u \equiv u' \pmod{m}$. In particolare, se $(a, m) = 1$ allora esiste uno ed un unico $1 \leq b \leq m - 1$ tale che $ab \equiv 1 \pmod{m}$.
In generale, con $m \geq$ ed $a, b \in \mathbb{Z}$, si avrà (Proposizione 1.5) che esiste $u \in \mathbb{Z}$ tale che $au \equiv b \pmod{m}$ se e soltanto se il massimo comun divisore tra m ed a divide b. Fissiamo queste osservazione in termini di equazioni.

Proposizione 1.13. *Sia* $2 \leq m \in \mathbb{N}$, *e siano* $a, b \in \mathbb{Z}$. *La congruenza*

$$ax \equiv b \pmod{n} \tag{1.3}$$

ammette soluzioni intere se e solo se $(a, n) | b$. *Se* $(a, n) = 1$ *le soluzioni costituiscono un'unica classe di congruenza modulo* m

In particolare, se $m = p$ è un numero primo, e p non divide a, allora per ogni $b \in \mathbb{Z}$ la congruenza (1.3) ammette soluzioni intere. Collegato a questo è un primo (e utilissimo) risultato non banale: il *piccolo Teorema di Fermat.*

Teorema 1.14 (Fermat)**.** *Siano* p *un numero primo e* $a \in \mathbb{Z}$. *Se* p *non divide* a *allora*

$$a^{p-1} \equiv 1 \pmod{p}.$$

In generale, per ogni $x \in \mathbb{Z}$, $x^p \equiv x \pmod{p}$.

Questo Teorema è stato provato nel corso di Algebra I; nel capitolo 4 lo dimostreremo di nuovo come caso particolare del teorema di Eulero.

ESEMPIO 5. *Provare che se p è un numero primo e q un divisore primo di $2^p - 1$ allora $p|q-1$.*

Sia q un divisore primo di $2^p - 1$; chiaramente $q \neq 2$ quindi, per il Teorema di Fermat, q divide $2^{q-1} - 1$. Quindi q divide sia $2^p - 1$ che $2^{q-1} - 1$; ma, per la Proposizione 1.11, $(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1$, e dunque $(p, q-1) = p$, che è quello che si voleva. ■

Con la stessa dimostrazione si dimostra, in generale, che se $a \geq 2$ e p, q sono numeri primi tali che q divide $a^p - 1$ allora $q|a-1$ o $p|q-1$.

ESEMPIO 6. *Per $n \in \mathbb{N}$, provare che ogni divisore primo del numero di Fermat $F_n = 2^{2^n}+1$ è del tipo $2^{n+1}k + 1$.*

Sia $n \in \mathbb{N}$ e sia p un divisore primo di F_n. Allora $2^{2^n} \equiv -1 \pmod{p}$, da cui, elevando al quadrato, $2^{2^{n+1}} \equiv 1 \pmod{p}$. Poiché $2^{p-1} \equiv 1 \pmod{p}$, se deduce che $2^{n+1}|p-1$, e quindi che $p = 2^{n+1}k + 1$ per qualche $k \in \mathbb{N}$. ■

ESEMPIO 7. *Si provi che il numero $n = 2^{2^{13}} + 2^{2^{11}} + 2^{2^7} + 1$ non è primo.*

Per il teorema di Fermat applicato al primo 5, $2^{13} = (2^4)^3 \cdot 2 \equiv 2 \pmod{5}$, quindi anche $2^{13} \equiv 2 \pmod{10}$. Similmente, $2^{11} = 2^8 \cdot 2^3 \equiv 2^3 \pmod{5}$, e dunque $2^{11} \equiv 8 \pmod{10}$, e ancora $2^7 = 2^4 \cdot 2^3 \equiv 2^3 \pmod{10}$. Ora, applicando il Teorema di Fermat per il primo 11,

$$2^{2^{13}} + 2^{2^{11}} + 2^{2^7} + 1 \equiv 2^2 + 2^8 + 2^8 + 1 = 4 + 512 + 1 = 517 \equiv 0 \pmod{11},$$

dunque 11 divide n. ■

Teorema di Wlison. Si tratta di un interessante risultato, che conviene conoscere.

Teorema 1.15 (Wilson[10])**.** *Sia p un numero primo. Allora*

$$(p-1)! \equiv -1 \pmod{p}.$$

Nel corso di Algebra I abbiamo dimostrato questo Teorema mediante il principio di identità dei polinomi; qui di seguito vediamo una diversa dimostrazione elementare.

Dimostrazione. Sia p un numero primo. Se $p = 2$ il risultato è banale; sia quindi $p \geq 3$ e poniamo $A = \{1, 2, \ldots, p-1\}$. Per quanto osservato prima dell'enunciato della Proposizione 1.13, per ogni $a \in A$ esiste un unico $\bar{a} \in A$ tale che $a \cdot \bar{a} \equiv 1 \pmod{p}$. Notiamo che, per ogni $a \in A$, $\bar{\bar{a}} = a$ e che, inoltre, $\bar{a} = a$ se e solo se $a \in \{1, p-1\}$: infatti, se $a \cdot a \equiv 1 \pmod{p}$, allora $p \mid a^2 - 1 = (a-1)(a+1)$ e dunque o $p \mid a-1$ (e allora $a = 1$), oppure $p \mid a+1$ (e allora $a = p-1$).
Dunque, l'insieme $A \setminus \{1, p-1\}$ si ripartisce in coppie disgiunte del tipo $\{a, \bar{a}\}$ (con $\bar{a} \neq a$), e quindi $b = \prod_{i=2}^{p-2} i \equiv 1 \pmod{p}$. In conclusione,

$$(p=1)! = 1 \cdot 2 \cdot \ldots \cdot (p-2)(p-1) = b(p-1) \equiv p - 1 \equiv -1 \pmod{p},$$

che è quel che si voleva. □

[10] John Wilson (1741–1793), matematico inglese. Di fatto, il teorema che porta il suo nome era già stato enunciato e applicato dal matematico arabo Ibn al-Haytham intorno all'anno 1000; vedi [**?**].

Teorema Cinese dei Resti. Concludiamo questo ripasso sulle congruenze con quell'altro classico pilastro dell'aritmetica che è il Teorema Cinese dei Resti.

Teorema 1.16 (Cinese dei resti)**.** *Siano $m_1, m_2, \ldots, m_s$ interi positivi a due a due coprimi e, per ogni $i = 1, 2, \ldots, s$, siano dati $a_i, b_i \in \mathbb{Z}$. Allora, il sistema di congruenze*

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \ldots \\ a_s x \equiv b_s \pmod{m_s} \end{cases}$$

ammette soluzioni in $\mathbb{Z}$ se e solo se ciascuna congruenza $a_i x \equiv b_i \pmod{m_i}$ ammette soluzioni; ovvero se e solo se $(a_i, m_i) \mid b_i$ per ogni $i = 1, \ldots, s$.

Anche in questo caso non riproduciamo la dimostrazione astratta vista nei corsi di Algebra, ed invece richiamiamo la procedura che, nelle notazioni dell'enunciato del Teorema 1.16, consente di ricavare una soluzione del sistema a partire dalle soluzioni x_i di ciascuna congruenza. Per ogni m_i, poniamo $m_i' = n/m_i$. Osserviamo che le ipotesi sugli m_i assicurano che, per ogni $i = 1, \ldots, s$, si ha $(m_i, m_i') = 1$ e $m_i' \equiv 0 \pmod{m_j}$ se $i \neq j$. Mediante l'algoritmo di Euclide, per ogni indice i, si trovano interi u_i, c_i tali che $u_i m_m + c_i m_i' = 1$ (ovvero, $c_i m_i' \equiv 1 \pmod{m_i}$). Se $x_1, x_2, \ldots, x_s$ sono soluzioni delle singole congruenze, si pone

$$y = x_1 m_1' c_1 + x_2 m_2' c_2 + \cdots + x_s m_s' c_s.$$

Per la definizione degli m_i' e la scelta dei c_i, si ha che, per ogni $i = 1, \ldots, s$,

$$y \equiv x_i m_i' c_i \equiv x_i \pmod{m_i}.$$

Dunque y è una soluzione del sistema di congruenze.

Il caso particolare in cui $a_i = 1$ per ogni indice i merita di essere enunciato a parte.

Corollario 1.17. *Se $m_1, m_2, \ldots, m_s$ sono interi positivi a due a due coprimi, allora per ogni $b_1, b_2, \ldots, b_s \in \mathbb{Z}$ il sistema di congruenze*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \ldots \\ x \equiv b_s \pmod{m_s} \end{cases}$$

ammette soluzioni in $\mathbb{Z}$ e le soluzioni costituiscono una classe di congruenza modulo $m_1 m_2 \cdots m_s$.

Esempio 8. *Sia $n \geq 1$ e siano $p_1, p_2, \ldots, p_n$ primi distinti assegnati. Si provi che esistono n interi positivi consecutivi $a_1, a_2 = a_1 + 1, \ldots, a_n = a + (n-1)$ tali che $p_i | a_i$ per ogni $i = 1, \ldots, n$.*

Per il Teorema Cinese dei Resti, il sistema di congruenze

$$\begin{cases} x \equiv 0 \pmod{p_1} \\ x \equiv -1 \pmod{p_2} \\ \dots \\ x \equiv -(n-1) \pmod{p_n} \end{cases}$$

ammette soluzioni intere positive. Basta prendere a_1 una di tali soluzioni. (Si osservi che la formula di Bezout è il caso $n = 2$.)

Infine, un'ulteriore generalizzazione (in realtà apparente, ma dal punto di vista pratico significativa), la cui dimostrazione è lasciata per esercizio.

Teorema 1.18. *Siano $m_1, m_2, \dots, m_s$ interi positivi a due a due coprimi, e $n = m_1 m_2 \cdots m_s$. Sia f un polinomio non nullo a coefficienti in $\mathbb{Z}$. Allora la congruenza*

$$f(x) \equiv 0 \pmod{n}$$

è risolubile in $\mathbb{Z}$, se e soltanto se $f(x) \equiv 0 \pmod{m_i}$ è risolubile in $\mathbb{Z}$ per ogni $i = 1, 2, \dots, s$.

Problemi

Il problema di cui svolgiamo subito la soluzione è a mio parere un piccolo gioiello[11].

Problema 16 (Baltic Way[12], 2014)**.** *Dire se il numero $712! + 1$ è un numero primo.*

Soluzione. Cominciamo con l'osservare che un divisore primo di $712! + 1$ non può essere minore o uguale di 712 (l'argomento di Euclide!). Scorrendo la lista dei numeri primi, troviamo che il più piccolo primo maggiore di 712 è 719. Per il teorema di Wilson,

$$712! \cdot 713 \cdot \ldots \cdot 717 \cdot 718 = 718! \equiv -1 \pmod{719}.$$

Quindi

$$-1 \equiv (-1)(-2)(-3)(-4)(-5)(-6)(712!) \equiv 720 \cdot (712!) \equiv 712! \pmod{719},$$

e dunque 719 divide $712! + 1$ che pertanto non è un numero primo. ∎

Anche il prossimo problema svolto è piuttosto interessante.

Problema 17 (Taiwan 2002)**.** *Un punto a coordinate intere $P = (a, b) \in \mathbb{Z}^2$, nel piano euclideo, si dice* visibile *se $mcd(a, b) = 1$ (cioè se il segmento che in $\mathbb{R}^2$ congiunge l'origine al punto P non incontra altri punti a coordinate intere). Si provi che per ogni $n \geq 1$ esiste un quadrato chiuso $\mathcal{Q}$ di lato n e vertici in $\mathbb{Z}^2$ tale che nessuno dei punti a coordinate intere appartenenti a $\mathcal{Q}$ è visibile.*

[11] Gli organizzatori della gara commenteranno a proposito della meta-logica che sottende un approccio efficace alla soluzione di questo problema: dato che è praticamente impossibile provare che un certo numero enorme è primo, la risposta 'deve' essere che non lo è...

[12] I giochi di matematica denominati *Baltic Way* si svolgono dal 1990 ed hanno la caratteristica di essere una competizione autenticamente tra squadre.

SOLUZIONE. Si tratta di una generalizzazione (in specie di matrice) dell'esempio 8. Sia

$$\{p_{i,j} \mid 0 \leq i, j \leq n-1\}$$

un insieme costituito da n^2 numeri primi tra loro distinti. Per il Teorema Cinese dei Resti, esistono interi positivi a e b tali che

$$a + i \equiv 0 \pmod{p_{i,0}p_{i,1}\cdots p_{i,n-1}}$$

per ogni $i = 0, 1, \ldots, n-1$, e

$$b + j \equiv 0 \pmod{p_{0,j}p_{1,j}\cdots p_{n-1,j}}$$

per ogni $j = 0, 1, \ldots, n-1$. Allora, si ha che per ogni coppia di interi i, j, compresi tra 0 e $n-1$, il massimo comun divisore $mcd(a+i, b+j)$ è un multiplo del primo $p_{i,j}$, quindi il punto $(a+i, b+j)$ non è visibile. Un quadrato che soddisfa le richiesta del problema è dunque $\mathcal{Q} = [a, a+99] \times [b, b+99]$. ∎

* * *

• Ecco ora qualche problema per voi da risolvere.

Problema 18 (EM Cup[13], 2015)**.** *Sia $A = \{a, b, c\}$ un insieme di tre numeri interi distinti. Si provi che esiste un sottoinsieme $B \subset A$, $B = \{x, y\}$ tale che*

$$10 \mid x^m y^n - x^n y^m$$

per ogni coppia m, n di interi positivi dispari.

Problema 19 (Nordic[14] MC, 1991)**.** *Determinare le ultime due cifre decimali del numero*

$$2^5 + 2^{5^2} + 2^{5^3} + \ldots + 2^{5^{1991}}.$$

Problema 20 (IMO, Merida (Messico) 2005)**.** *Determinare gli interi positivi che sono coprimi con tutti i termini della successione*

$$a_n = 2^n + 3^n + 6^n - 1, \ n \geq 1.$$

Problema 21 (Italia 2010)**.** *Dimostrare che esistono infiniti numeri primi che dividono almeno un intero della forma $2^{n^3+1} - 3^{n^2+1} + 5^{n+1}$ con n intero positivo.*

Problema 22 (Cechia-Slovacchia 1997)**.** *Si dimostri che esiste un successione strettamente crescente $a_1, a_2, \ldots$ di interi positivi tale che per ogni $k \geq 0$ la successione $\{a_n + k \mid n \geq 1\}$ contiene solo un numero finito, eventualmente nullo, di numeri primi.*

Problema 23 (Korea 1999)**.** *Trovare tutti gli interi positivi n tali che $2^n - 1$ è un multiplo di 3 e $\frac{2^n-1}{3}$ divide $4m^2 + 1$ per qualche $m \in \mathbb{Z}$.*

[13] *European Mathematical Cup*, si disputa in Croazia dal 2012, e comprende una sezione per studenti più giovani.

[14] Il *Nordic Mathematical Contest* rivolto a studenti dei 5 paesi nordeuropei (Danimarca, Finlandia, Islanda, Norvegia e Svezia), si disputa dal 1997.

1.4. Equazioni diofantee

Con *equazione diofantea* (dal matematico alessandrino Diofanto) si intende genericamente un'equazione algebrica, con coefficienti e parametri interi, della quale si cercano le soluzioni che sono numeri interi. Un primo caso, fondamentale, di equazione diofantea, quello lineare, è già stato descritto, determinandone in modo completo risolubilità e (mediante l'algoritmo di Euclide) soluzioni, nella Proposizione 1.5.

Terne pitagoriche. Un altro caso semplice di equazione diofantea, che è possibile risolvere completamente, è quello che consente di determinare tutte le *terne pitagoriche*.

Proposizione 1.19. *Ogni soluzione intera dell'equazione*

$$x^2 + y^2 = z^2$$

si scrive nella forma $x = k(m^2 - n^2), y = 2kmn$ *e* $z = k(m^2 + n^2)$*, dove* $mcd(m, n) = 1$.

Dimostrazione. Si verifica facilmente che per ogni $k, n, m \in \mathbb{N}^*$, con n e m coprimi, la terna $(x, y, z) = (k(m^2 - n^2), 2kmn, k(m^2 + n^2))$ è una soluzione dell'equazione data. Viceversa, siano $x, y, z \in \mathbb{N}^*$ tali che $x^2 + y^2 = z^2$, e sia $k = (x, y)$. Osserviamo che allora $k = (x, z) = (y, z)$. Siano $a, b, c \in \mathbb{N}^*$, con

$$x = ka, \quad y = kb, \quad z = kc\ .$$

Allora $(a, b) = (a, c) = (b, c) = 1$ e $a^2 + b^2 = c^2$. Dunque

$$c^2 = a^2 + b^2 = (a + b)^2 - 2ab.$$

Ora, a e b non sono entrambi pari. Se fossero entrambi dispari, allora $a + b$ e c sarebbero pari, e quindi $4|c^2$ e $4|(a + b)^2$, da cui segue la contraddizione $4|2ab$. Possiamo quindi assumere che a sia dispari e b sia pari (e quindi c è dispari). Sia $d = (c + a, c - a)$; allora $2|d$, ed inoltre $d|(c + a) + (c - a) = 2c$ (analogamente $d|2a$), e dunque, poiché a e c sono coprimi, $d = 2$. Siano ora $u, v \in \mathbb{N}^*$ tali che

$$c + a = 2u \qquad c - a = 2v.$$

Per quanto appena osservato $(u, v) = 1$. Inoltre

$$b^2 = c^2 - a^2 = (c + a)(c - a) = 4uv,$$

e dunque u e v sono quadrati: poniamo $u = m^2$ e $v = n^2$. Allora,

- $b^2 = 4m^2n^2$, e quindi $b = 2mn$, e $y = 2kmn$.
- $2c = 2(u + v) = 2(m^2 + n^2)$, e quindi $c = m^2 + n^2$, e $z = k(m^2 + n^2)$.
- $2a = 2(u - v) = 2(m^2 - n^2)$, e quindi $a = m^2 - n^2$, e $x = k(m^2 - n^2)$. □

Esercizio 1.6. Provare che l'equazione diofantea $x^4 + y^4 = z^2$ non ha soluzioni non banali (cioè tali che $xyz \neq 0$).

Equazioni diofantee e congruenze. Allo studio della risolubilità di particolari equazioni diofantee è riconducibile una considerevole parte della teoria dei numeri, così come sono molteplici gli strumenti sviluppati nel corso dei secoli per affrontare simili questioni. Le congruenze rappresentano uno di questi strumenti imprescindibile nello studio delle equazioni diofantee. Infatti, se una certa equazione diofantea ha soluzioni in $\mathbb{Z}$, allora la congruenza ricavata dall'equazione modulo un qualsiasi $n \geq 2$ ha soluzioni. Quindi, le congruenze sono usate per ottenere informazioni sul tipo di eventuali soluzioni (il caso più semplice che ciascuno applica in modo naturale, anche prima di aver fatto la conoscenza delle congruenze, è il controllo di parità), e nei casi più favorevoli, a provare che non ci sono soluzioni.
Vediamo subito un esempio, un po artificioso, lo ammetto, di questo principio.

Esempio 9. *Provare che il sistema di equazioni*

$$x^{12} + 5x^8y^4 - 8x^4y^4 + y^4 = 2018$$
$$y^{14} - xy + x^3 = 8101^{412}$$

non ha soluzioni intere.

Supponiamo che (x, y) sia una soluzione intera; allora, dato che $2018 \equiv 3 \pmod{13}$, (x, y) è anche soluzione della congruenza

$$x^{12} + 5x^8y^4 - 8x^4y^4 + y^4 \equiv 3 \pmod{13}. \qquad (*)$$

(1) Supponiamo $13 \nmid x$. Allora, poiché 13 è un numero primo, per il Teorema di Fermat,

$$1 + 5x^8y^4 + 5x^4y^4 + y^4 \equiv 3 \pmod{13},$$

e quindi

$$5x^4y^4(x^4 + 1) \equiv 2 - y^4 \pmod{13}. \qquad (**)$$

Osservato a questo punto che se $13 \nmid x$ allora $13 \nmid y$, facendo direttamente i calcoli, si trova che le quarte potenze modulo 13 sono congrue a $0, 1, 3$ o 9; in particolare, poiché né x né y sono multipli di 13 si avrà $x^4 + 1 \equiv 2, 4, 10$, e $2 - y^4 \equiv 1, -1, 6$. Elevando alla terza potenza, e applicando ancora Fermat,

$$5^3(x^4 + 1)^3 \equiv 8(x^4 + 1)^3 \equiv (2 - y^4)^3 \pmod{13},$$

dove. per quanto detto sopra, si ha,

$$8(x^4 + 1)^3 \equiv -1, 5 \pmod{13} \text{ e } (2 - y^4)^3 \equiv 1, -1, 8 \pmod{13}$$

quindi

$$8(x^4 + 1)^3 \equiv (2 - y^4)^3 \equiv -1 \pmod{13}.$$

Questo comporta, esaminando la tabelle delle potenze modulo 13 già ampiamente utilizzata, $(x^4 + 1)^3 \equiv 8 \pmod{13}$, e di seguito $x^4 + 1 \equiv 2 \pmod{13}$, da cui $x^4 \equiv 1 \pmod{13}$; per y si ha $2 - y^4 \equiv -1 \pmod{13}$ e di conseguenza $y^4 \equiv 3 \pmod{13}$. Sostituendo in $(**)$ si ricava la contraddizione

$$5 \cdot 1 \cdot 3 \cdot 2 \equiv -1 \pmod{13}.$$

(2) La sola possibilità rimasta è $x \equiv 0 \pmod{13}$. Dalla prima equazione (tradotta in congruenza), si ha allora $y^4 \equiv 3 \pmod{13}$ e quindi $y \equiv 2, 3, 10, 11 \pmod{13}$. La congruenza modulo 13 che deriva dalla seconda equazione, si scrive, tenendo conto che $x \equiv 0 \pmod{13}$, $13 \nmid y$, $8101 \equiv 2 \pmod{13}$, $412 = 12 \cdot 34 + 4$, e applicando Fermat,

$$y^2 \equiv 2^4 \equiv 3 \pmod{13}$$

che non è possibile perché i valori ammissibili per y forniti dalla prima equazione danno al quadrato 4 e 9 (modulo 13).
Poiché il sistema di congruenze modulo 13 derivato dal sistema intero iniziale non ha soluzioni, nemmeno quello ne ha. ■

Naturalmente, il fatto che una data equazione diofantea abbia soluzioni modulo un certo, o più, n non ne implica la risolubilità in $\mathbb{Z}$; anzi esistono equazioni, come ad esempio $x^2 = y^3 + 6$, che non sono risolvibili in $\mathbb{Z}$ mentre lo sono modulo qualsiasi $n \geq 2$.
Torneremo più avanti su questi ed altri aspetti generali. Ripensando al nostro esempio, si capisce che individuare un modulo 'giusto' (e non c'è nessun modo meccanico per farlo) consente di trasferire i calcoli ad una struttura forse meno immediata da gestire dei familiari numeri interi, ma con molte maggiori risorse strumentali. Certo, al livello di soluzione manuale di problemi assegnati, è importante che il modulo sia relativamente piccolo, in modo da consentire un controllo agevole, o comunque non troppo dispendioso, di tutte le eventualità che si presentano. E di particolare importanza, come un poco si è cercato di mostrare nell'esempio, è la gestione delle potenze. È chiaro che non sempre sarà possibile, come abbiamo fatto modulo 13, avere una tabella su cui controllare il valore di tutte le potenze, e strumenti generali che diano delle informazioni prescindendo dal valore specifico del modulo sono di particolare importanza.
Come detto, riprenderemo questo studio nel Capitolo 4. Per il momento dimostriamo uno dei più semplici di questi strumenti generali, che risale a Eulero.

Lemma 1.20. *Sia p un numero primo dispari; allora la congruenza*

$$x^2 \equiv -1 \pmod{p}$$

ha soluzioni se e solo se $p \equiv 1 \pmod{4}$.

Dimostrazione. Sia p un primo dispari tale che esiste $a \in \mathbb{Z}$ con $a^2 \equiv -1 \pmod{p}$. Allora $a^4 \equiv 1 \pmod{p}$; d'altra parte $a^{p-1} \equiv 1 \pmod{p}$ per il Teorema di Fermat, e dunque, posto $d = mcd(4, p-1) = k(p-1) - 4t$ (per $k, t \in \mathbb{N}^*$),

$$a^d \equiv a^d a^{4t} \equiv a^{k(p-1)} \equiv 1 \pmod{p}.$$

Ora, siccome $p - 1$ è pari, $d = 2$ o 4. Ma $a^2 \equiv -1 \not\equiv 1 \pmod{p}$; dunque $d = 4$, ovvero $4 \mid p - 1$ (cioè $p \equiv 1 \pmod{4}$).
Viceversa sia $p \equiv 1 \pmod{4}$, e $k = (p-1)/2$ (che è un numero pari). Sia $a = 1 \cdot 2 \cdots k$. Per ogni $1 \leq j \leq k$ si ha allora $k + j \equiv -(p - j) \pmod{p}$, quindi

$$(k+1)(k+2)\cdots(p-1) \equiv (-1)(-2)\cdots(-k) \equiv (-1)^k a \equiv a \pmod{p}.$$

Dunque, per il Teorema di Wilson,

$$a^2 \equiv 1 \cdot 2 \cdots k \cdot (k+1) \cdot (k+2) \cdots (p-1) \equiv -1 \pmod{p},$$

e a è soluzione di $x^2 \equiv -1 \pmod{p}$. □

Abbiamo in pratica dimostrato che se p è un primo e $4 \mid p-1$ allora $(\frac{p-1}{2}!)^2 \equiv -1 \pmod{p}$.
Nel Capitolo 4 rivedremo questo Lemma (come del resto i Teoremi di Fermat e di Wilson) da un punto di vista più algebrico, che, sebbene più astratto, consentirà di intendere con chiarezza una ragione, per così dire coerente, dietro certi risultati che, provati in modo diretto se pur elementare, come abbiamo fatto per il momento, sembrano avere ancora un carattere fortuito, se non leggermente miracoloso. Per intanto, vediamo il Lemma 1.20 in azione.

Problemi

Problema 24 (Balkan[15] MO, 1998)**.** *Provare che la seguente equazione diofantea non ha soluzioni:*

$$x^2 + 4 = y^5.$$

Soluzione. Consideriamo la congruenza

$$x^2 + 4 \equiv y^5 \pmod{11}.$$

Se $y \equiv 0 \pmod{11}$, allora $x^2 \equiv -4 \pmod{11}$ e quindi

$$(6x)^2 \equiv 36 \cdot (-4) \equiv -1 \pmod{11}$$

che contraddice, dato che $11 \not\equiv 1 \pmod{4}$, il Lemma 1.20.
Supponiamo quindi 11 non divida y. Per il teorema di Fermat $(y^5)^2 = y^{10} \equiv 1 \pmod{11}$, e dunque $y^5 \equiv 1, -1 \pmod{11}$.
Se $y^5 \equiv 1 \pmod{11}$, allora $x^2 \equiv -3 \pmod{11}$ e, ragionando come prima,

$$(2x)^2 \equiv 4 \cdot (-3) \equiv -1 \pmod{11}$$

contro il Lemma 1.20. Se $y^5 \equiv -1 \pmod{11}$, si fa allo stesso modo: da $x^2 \equiv -5 \pmod{11}$ segue la contraddizione

$$(3x)^2 \equiv 9 \cdot (-5) \equiv -1 \pmod{11}.$$

Dunque l'equazione diofantea nel testo non ha soluzioni in $\mathbb{Z}$. ■

Problema 25 (Iran 1994)**.** *Provare che per ogni primo $p \geq 5$, il numero $7^p - 6^p - 1$ è un multiplo di 43.*

[15] La *Balkan Mathematical Olympiad* si disputa annualmente, a rotazione in diverse località dei Balcani (in senso esteso, visto che è stata ospitata anche da Cipro) dal 1984; una squadra italiana è normalmente invitata.

Problema 26 (Austria 2001). *Dire per quali interi $n \geq 1$ l'equazione*

$$(19y + x)^{18} + (x + y)^{18} + (19x + y)^{18} = n^2$$

ammette soluzioni intere.

Problema 27. [a] (IMO, Mosca 1964) *Determinare tutti gli interi positivi n tali che 7 divide $2^n - 1$. Provare quindi che per ogni intero positivo n, 7 non divide $2^n + 1$.*

[b] (Vietnam 1983) *Dire quali sono le coppie di interi positivi a, b, con $b \geq 2$ tali che $2^a + 1$ è un multiplo di $2^b - 1$.*

Problema 28 (Putnam, 2001). *Si provi che esiste un'unica coppia (a, n) di interi positivi tale che $a^{n+1} - (a + 1)^n = 2001$.*

Problema 29 (Vietnam 2004). *Denotiamo con $S(n)$ la somma delle cifre della rappresentazione decimale del numero naturale n. Si determini il minimo valore di $S(m)$ al variare di m nell'insieme dei multipli positivi di 503.*

1.5. Il problema di Frobenius

Come abbiamo osservato, la formula di Bezout implica che se a, b sono interi coprimi allora ogni intero (in particolare ogni intero positivo) n si scrive come

$$n = ua + vb$$

dove u, v sono numeri interi. Ovviamente, in una tale rappresentazione di n non è detto che u, v siano (o anche possano) essere non-negativi. Il problema di Frobenius (anche detto 'Problema delle monete') riguarda proprio rappresentazioni come somme a coefficienti non-negativi.
Tale questione ha un risvolto pratico abbastanza tangibile. Ad esempio: *quali cifre è possibile pagare avendo a disposizione tre tagli di monete* (diciamo, del valore di 6, 10 e 15 unità)? e simili cose...

Se avete provato a fare qualche tentativo con queste monete (dai tagli un po' improbabili) avrete forse trovato che ogni cifra $n > 29$ si può pagare, mentre 29 non è possibile. Cioè, per ogni $n > 29$ esistono interi non negativi x, y, z tali che $n = 6x + 10y + 15z$, mentre 29 non ammette una tale rappresentazione.
Questo fatto (l'esistenza cioè di una 'soglia' sopra la quale ogni intero si rappresenta con coefficienti non negativi) non è fortuito, come vedremo tra poco (Teorema 1.21). Prima, concordiamo la seguente semplificazione espositiva: fissati interi positivi $a_1, a_2, \ldots, a_k$, diciamo semplicemente che un intero $n \geq 0$ è *rappresentabile* se è rappresentabile come combinazione a coefficienti interi non negativi dei numeri $a_1, a_2, \ldots, a_k$.
Osserviamo il fatto, ovvio, che se S, R sono numeri rappresentabili, allora è rappresentabile anche ogni intero del tipo $nR + mS$, con n, m interi non negativi.

Teorema 1.21. *Siano $a_1, a_2, \ldots, a_k$ interi positivi con $MCD(a_1, a_2, \ldots, a_k) = 1$. Allora esiste un massimo intero positivo $g(a_1, \ldots, a_k)$ che non è rappresentabile.*

(Ad esempio, come notato sopra, $g(6, 10, 15) = 29$.)

Dimostrazione. Sia $a_1 \leq a_2 \leq \ldots \leq a_k$, e sia $n \in \mathbb{N}$. Poiché $MCD(a_1, a_2, \ldots, a_k) = 1$, esistono interi $z_1, z_2, \ldots, z_k$ tali che

$$1 = z_1 a_1 + z_2 a_2 + \ldots + z_k a_k.$$

Sia P la somma dei termini $z_i a_i$ che sono positivi (quindi z_i positivo), e $-Q$ la somma dei termini negativi (cioè tali che $z_i < 0$). Quindi $1 = P - Q$; e, chiaramente, P e Q sono rappresentabili.
Sia n intero con $n \geq a_1 Q$, e lo si divida per a_1: $n = h a_1 + r$ con $h \geq Q$ e $0 \leq r < a_1$. Allora

$$n = (h - Q)a_1 + Q a_1 + r(P - Q) = (h - Q)a_1 + rP + (a_1 - r)Q;$$

poiché $h - Q, r, a_1 - r$ sono interi non negativi e a_1, P, Q rappresentabile, n è rappresentabile. Dunque

$$g(a_1, \ldots, a_k) \leq a_1 Q - 1.$$

□

La dimostrazione mostra che $g(a_1, \ldots, a_k) \leq a_1 Q$, ma si tratta di stime più che abbondanti: ad esempio, nel caso $(6, 10, 15)$ dell'esempio di prima, il valore minimo per Q si ricava dalla scrittura $1 = 1 \cdot 6 + 1 \cdot 10 - 1 \cdot 15$ ed $Q = 15$, per cui $a_1 Q = 6 \cdot 15 = 90$, che è ben più grande del valore preciso 29 trovato prima.
Il *Problema di Frobenius* consiste proprio nel determinare i valori esatti $g(a_1, \ldots, a_k)$. Formulato alla fine del diciannovesimo secolo è ancora in larga parte aperto (si veda, ad esempio, il testo [1]). Mentre per il caso $k = 2$ è piuttosto semplice trovare il valore $g(a_1, a_2)$ (la prima dimostrazione è di solito attribuita a Sylvester e apparve nel 1882), solo molto recentemente (2017) sono state trovate, da A. Tripathi, formule esplicite per i valori $g(a_1, a_2, a_3)$ (formule che sono troppo elaborate per essere riportate qui), anche se programmi efficienti per calcolarli erano noti da qualche decina d'anni. Per $k \geq 4$ molto poco Ŕ noto in generale, ad esclusione di casi piuttosto particolari. Esistono diverse limiti sia superiori che inferiori che funzionano più o meno bene a seconda dei casi; cito solo un risultato ormai classico di I. Schur, secondo il quale, se $1 < a_1 \leq a_2 \leq \cdots \leq a_k$ sono interi coprimi, allora $g(a_1, \ldots, a_k) \leq (a_1 - 1)(a_k - 1) - 1$.

Teorema 1.22 (Sylvester)**.** *Siano p, q interi non negativi e coprimi. Allora*

$$g(p, q) = pq - p - q.$$

Dimostrazione. Sia n un intero. Poiché p, q sono coprimi, esistono $x, y \in \mathbb{Z}$ tali che

$$n = xp + yq. \tag{1.4}$$

Se (x_1, y_1) è un'altra coppia di numeri interi tali che $x_1 p + y_1 q = n$, allora

$$(x - x_1)p = (y_1 - y)q$$

e, dunque, poiché p, q sono coprimi, $q \mid x - x_1$ (Proposizione 1.6) ovvero $x_1 \equiv x \pmod{q}$. Viceversa, si vede subito che per ogni $z \in \mathbb{Z}$ la coppia $x_1 = x + qz$, $y_1 = y - pz$ è una

soluzione di (1.4). Questo ci dice che tra le soluzioni (x, y) di (1.4) ce n'è una e una sola tale che $0 \leq x < q$.
Sia (x, y) tale soluzione; ne segue che n è rappresentabile (ovvero (1.4) ammette soluzioni non-negative) se $y \geq 0$, e non è rappresentabile se $y < 0$. Il più grande caso non-rappresentabile si ottiene per $x = q - 1$ e $y = -1$, ovvero

$$(q-1)p - q = qp - p - q.$$

Dunque, $g(p, q) = pq - p - q$. □

I problemi che proponiamo trattano due casi semplici per 3 interi; un problema collegato al teorema 1.22 si trova nel prossimo capitolo (problema 66).

Problema 30 (classico: Chicken McNuggets)**.** *Un certo prodotto alimentare viene venduto in confezioni che contengono* $6, 9$ *o* 20 *pezzi. Dire qual è il massimo numeri di pezzi che non è possibile acquistare.*

Problema 31. *Sia* n *un intero positivo pari; si provi che*

$$g(n, n+1, n+2) = \frac{n^2}{2} - 1.$$

1.6. Soluzioni dei problemi

Problema 5. Andare per tentativi o esperimenti non è in questo caso molto fruttifero. Intanto osserviamo che se n è un intero positivo di cento cifre tutte diverse da zero e denotiamo con $s(n)$ la somma delle sue cifre, allora $100 \leq s(n) \leq 900$; inoltre ogni intero s compreso tra 100 e 900 coincide con la somma delle cifre di un numero di cento cifre. L'idea giusta è individuare opportunamente un tale s e costruire n in modo che $s = s(n)|n$. Ora, se $n = a \cdot 10^3 + s$ con a un numero di 97 cifre e $100 \leq s \leq 900$, s divide n se divide $10^3 = 2^3 5^3$. Se si considera quindi $s = 5^3 = 125$, basta trovare a in modo che

$$s(a) = s(n) - s(125) = s(n) - 8 = 125 - 8 = 117.$$

E questo si fa in tanti modi, ad esempio si può prendere $a = 887(+94$ cifre uguali a $1)$.

* * *

Problema 6. Siano a, b interi positivi e $d = mcd(a, b)$; allora $mcd(a - b, b) = mcd(a, b - a) = d$, mentre $mcd(2a, b) = 2^\epsilon d$ e $mcd(2a, b) = 2^\mu d$, dove $\epsilon, \mu \in \{0, 1\}$.
Quindi, nel gioco descritto dal Problema, ogni mossa lecita della pietra sposta questa da un punto (a, b) a coordinate intere in un punto il cui massimo comun divisore delle coordinate è uguale oppure il doppio di $mcd(a, b)$. Da ciò segue immediatamente che se il punto (x, y) si può raggiungere da $(1, 1)$ allora $mcd(x, y) = 2^t$ per qualche $t \geq 0$.
Viceversa, proviamo che ogni punto (x, y), con $x, y \in \mathbb{N}^*$ e tale che $mcd(x, y) = 2^t$ per qualche $t \in \mathbb{N}$, è raggiungibile da $(1, 1)$ in un numero finito di mosse. Per induzione su $x + y$. Se $x + y = 2$, $(x, y) = (1, 1)$ e non c'è altro da aggiungere. Sia $x + y > 2$. Se $x = 2a$

è pari allora $mcd(a,y)$ è una potenza di due, (a,y) è raggiungibile da $(1,1)$ per ipotesi induttiva e quindi (x,y) è raggiungibile dato che ci si arriva da (a,y) con una mossa di tipo (i); lo stesso argomento si applica se y è pari. Rimane il caso in cui sia x che y sono dispari, quindi $mcd(x,y)=1$ e in particolare $x\neq y$; sia $x>y$, allora

$$mcd\Big(\frac{x+y}{2},y\Big)=1 \quad \text{e} \quad \frac{x+y}{2}+y<x+y,$$

dunque $(\frac{x+y}{2},y)$ è raggiungibile da $(1,1)$ per ipotesi induttiva, e quindi (x,y) è raggiungibile:

$$(1,1)\to\Big(\frac{x+y}{2},y\Big)\xrightarrow{\text{(i)}}(x+y,y)\xrightarrow{\text{(ii)}}(x,y).$$

La stessa cosa, nella seconda componente, si fa se $y>x$.

In conclusione: (x,y) è raggiungibile da $(1,1)$ se e soltanto se $mcd(x,y)$ è una potenza di 2.

* * *

PROBLEMA 7. Siano a,b,c come nelle ipotesi e supponiamo esista un $x\in\mathbb{N}^*$ tale che

$$x\cdot(a-1)(b-1)(c-1)=abc-1. \tag{$*$}$$

Chiaramente $x\geq 2$. Osserviamo poi che se uno tra i numeri a,b,c è dispari, allora il membro di sinistra in $(*)$ è pari, dunque abc deve essere dispari e quindi a,b,c sono tutti dispari. Pertanto, a,b,c sono tutti pari oppure tutti dispari.
Inoltre, tenendo conto che la funzione $n\to\frac{n}{n-1}$ è decrescente, da $(*)$ segue

$$x<\frac{a}{a-1}\cdot\frac{b}{b-1}\cdot\frac{c}{c-1}\leq\frac{a}{a-1}\cdot\frac{a+2}{a+1}\cdot\frac{a+4}{a+3}\leq\frac{2}{1}\cdot\frac{4}{3}\cdot\frac{6}{5}=\frac{16}{5}, \tag{$**$}$$

quindi $x\in\{2,3\}$.

Siano a,b,c pari. Allora il termine di destra in $(*)$ è dispari e dunque anche x è dispari; quindi, $x=3$. Se $a\geq 4$, allora, dalla $(**)$,

$$x<\frac{4}{3}\cdot\frac{6}{5}\cdot\frac{8}{7}=\frac{64}{35}<2$$

che è assurdo. Dunque $a=2$, $x=3$; sostituendo nella $(*)$ si ottiene $3(b-1)(c-1)=2bc-1$, da cui

$$bc+4=3b+3c\leq 3(c-2)+3c=6c-6,$$

e, poiché $b>2$ è pari, $b=4$. Sostituendo nella $(*)$, si ha $9(c-1)=8c-1$, da cui $c=8$.
Siano a,b,c dispari. Dalla $(**)$ si ricava

$$x<\frac{3}{2}\cdot\frac{5}{4}\cdot\frac{7}{6}=\frac{35}{16}<3$$

e quindi $x=2$. Ragionando poi come nel caso pari, se $a\geq 5$, sempre dalla $(**)$ si ha

$$x<\frac{5}{4}\cdot\frac{7}{6}\cdot\frac{9}{8}=\frac{105}{64}<2$$

che è assurdo. Dunque $a = 3$, $x = 2$; sostituendo nella $(*)$ si ottiene $4(b-1)(c-1) = 3bc-1$, da cui

$$bc + 5 = 4b + 4c \leq 4(c-2) + 4c = 8c - 8.$$

Dunque $b = 5, 7$. Sostituendo in $(*)$ si trova che il solo caso possibile e $b = 5$, che dà $c = 15$.

In conclusione, le soluzioni sono $(a, b, c) = (2, 4, 8), (3, 5, 15)$.

COMMENTO. La soluzione di questo problema, come anche quella del Problema 2, mostra come, nell'affrontare questioni sui numeri interi, convenga sempre avere in mente la relazione d'ordine naturale che c'è in questo insieme, perché potrebbe rivelarsi utile, se non decisiva. Certo, nel passare da una relazione $a|b$ ad $a \leq b$ si perde in genere dell'informazione, ma si guadagna in libertà di movimento e forza bruta. Sta nel tipo particolare di problema se il bilancio risulti o no favorevole.

* * *

PROBLEMA 8. Siano a, b, c interi positivi con $a < b < c$ e sia $d = mcd(ab+1, ac+1, bc+1)$. Allora,

$$d \mid (ab+1)c - a(bc+1) = c - a,$$

e similmente si prova $d|b - a$. Quindi esistono due numeri interi m, n con $1 \leq m < n$ (perché $a < b < c$, si osservi anche $m + n \geq 3$) tali che

$$\begin{aligned} b &= a + md \\ c &= a + nd. \end{aligned}$$

Dunque

$$\frac{a+b+c}{3} = \frac{a + (a+md) + (a+nd)}{3} = \frac{3a + (m+n)d}{3} \geq \frac{3a+3d}{3} = a + d > d,$$

come si voleva.

* * *

PROBLEMA 11. Poiché $y > 0$, si ha $x + y > x - y > 0$. Da $p^6 = x^2 - y^2 = (x-y)(x+y)$ si vede quindi che $x - y = p^m$ e $x + y = p^{6-m}$ per qualche $0 \leq m \leq 2$. Ora

$$4xy = (x+y)^2 - (x-y)^2 = p^{12-2m} - p^{2m}. \qquad (*)$$

D'altra parte

$$3xy(x-y) = 3x^2y - 3xy^2 = (x^3 - y^3) - (x-y)^3 = p^4q^2 - p^{3m},$$

quindi

$$3xy = p^{4-m}q^2 - p^{2m}. \qquad (**)$$

Se $m = 0, 1$, dal confronto di $(*)$ con $(**)$ segue

$$3p^{2m}(p^{12-4m} - 1) = 12xy = 4p^{2m}(p^{4-3m}q^2 - 1),$$

quindi $3p^{12-4m} - 4p^{4-3m}q^2 = -1$, che è assurdo dato che $12-4m$ e $4-3m$ sono maggiori o uguali a 1, e dunque p divide il termine di sinistra.
Resta quindi $m = 2$. Dal confronto di $(*)$ con $(**)$ si ricava allora

$$3(p^8 - p^4) = 4(p^2q^2 - p^4),$$

da cui

$$4p^2q^2 = 3p^8 + p^4 = p^4(3p^4 + 1).$$

Poiché p e q sono primi distinti, deve necessariamente aversi $p = 2$ e $q^2 = 3p^4 + 1 = 49$. Facendo ora facili conti si trova, in conclusione, che esiste una sola soluzione data dalle coppie $(x, y) = (10, 6)$ e $(p, q) = (2, 7)$.

* * *

PROBLEMA 12. Per ipotesi esiste $k \geq 1$ tale che $p = kn+1$. Ora $n^3-1 = (n-1)(n^2+n+1)$, e siccome p è primo ed è maggiore di n,

$$p = kn + 1 \big| n^2 + n + 1.$$

Ciò implica in particolare $k \leq n + 1$. D'altra parte, p divide

$$-np + k(n^2 + n + 1) = k(n^2 + n + 1) - n(nk + 1) = kn - n + k,$$

dunque $p = kn+1 \leq kn-n+k$, da cui $k \geq n+1$. Quindi $k = n+1$ e $p = kn+1 = n^2+n+1$, e pertanto

$$4p - 3 = 4n^2 + 4n + 1 = (2n + 1)^2.$$

* * *

PROBLEMA 13. Siano $p < q < r$ numeri primi positivi; poniamo $\alpha = \sqrt[3]{p}$, $\beta = \sqrt[3]{q}$, $\gamma = \sqrt[3]{r}$, e supponiamo per assurdo che α, β, γ siano termini di un stessa progressione aritmetica. Allora esiste un numero reale $\delta > 0$ e due numeri interi $1 \leq m \leq n$ tali che

$$\begin{aligned} \beta - \alpha &= m\delta \\ \gamma - \alpha &= n\delta. \end{aligned}$$

Quindi, $m(\gamma - \alpha) = n(\beta - \alpha)$, da cui

$$m\gamma - n\beta = (m - n)\alpha,$$

e, elevando alla terza potenza,

$$m^3r - 3m^2n\gamma^2\beta + 3mn^2\gamma\beta^2 - n^3q = (n - m)^3p.$$

Quindi, $3mn^2\gamma\beta^2 - 3m^2n\gamma^2\beta = (n - m)^3p - m^3r + n^3q \in \mathbb{Z}$ e di conseguenza

$$\gamma\beta(n\beta - m\gamma) = n\gamma\beta^2 - m\gamma^2\beta = \frac{(n - m)^3p - m^3r + n^3q}{3mn} \in \mathbb{Q}.$$

Dunque,

$$\gamma\beta(n\beta - m\gamma) = \gamma\beta(n(\alpha + m\delta) - m(\alpha + n\delta)) = \gamma\beta\alpha(n - m)$$

è un numero razionale, e quindi, poiché $n - m \neq 0$,

$$\gamma\beta\alpha = \sqrt[3]{rqp}$$

è un numero razionale. Ma allora, per la Proposizione 1.9, $\gamma\beta\alpha \in \mathbb{N}$, cioè rqp è un cubo in $\mathbb{N}$ e questo è assurdo perché p, q, r sono tre primi distinti.

* * *

PROBLEMA 14. Sia (p, n) una coppia che soddisfa l'identità data. Chiaramente, n è dispari e $1 \leq n \leq p + 1$. Riscrivendo l'equazione

$$(n + 1)(n^2 - n + 1) = n^3 + 1 = p^2 - p = p(p - 1). \qquad (*)$$

Poiché p è primo, $p|n + 1$ oppure $p|n^2 - n + 1$. Nel primo caso, per quanto osservato all'inizio, $p = n + 1$ che è un numero pari: dunque $p = 2$, $n + 1$, e di fatto la coppia $(2, 1)$ è una soluzione.

Supponiamo ora $p|n^2 - n + 1$; dunque, per un numero $t \in \mathbb{N}^*$,

$$n^2 - n + 1 = pt. \qquad (**)$$

Inoltre, per $(*)$, $(n + 1)pt = p(p - 1)$. Si ricava $p = nt + t + 1$, che sostituito in $(**)$ dà

$$n^2 - (t^2 + 1)n - (t^2 + t - 1).$$

Affinché $n \in \mathbb{N}^*$ esista è necessario che il discriminante dell'equazione di secondo grado sia un quadrato razionale, dunque, per il Teorema 1.9, un quadrato intero; cioè per qualche $c \in \mathbb{N}^*$,

$$\Delta = (t^2 + 1)^2 + 4(t^2 + t - 1) = t^4 + 6t^2 + 4t - 3 = (t^2 + 3)^2 + 4(t - 3) = c^2$$

Se $t = 3$, si ha di fatto $c = t^2 + 3$ e l'equazione di secondo grado diventa $n^2 - 10n - 11$ che ammette la soluzione $n = 11$; da $(**)$ si ricava quindi $p = 37$ che è un primo, dunque $(37, 11)$ è una soluzione.

Se $t = 1$ o 2, Δ è, rispettivamente, 8 e 45, e non è un quadrato. Se $t > 3$, poiché

$$(t^2 + 4)^2 - (t^2 + 3)^2 = 2t^2 + 7 > 4(t - 3),$$

si conclude ancora che Δ non è il quadrato di un numero intero.

In conclusione, le coppie (p, n) soluzioni del problema sono $(2, 1)$ e $(37, 11)$.

* * *

PROBLEMA 15. Sia p un divisore primo di $m^4 + 1$, per qualche $m \in \mathbb{N}^*$. Sia r il resto della divisione di m per p: $m = qp + r$ (con $q, r \in \mathbb{N}$, $r < p$); osserviamo che $r > 0$. Ora, come si vede facilmente sviluppando la potenza del binomio, p divide $(m - pq)^4 + 1 = r^4 + 1$ e, per la stessa ragione, divide anche $(p - r)^4 + 1$. Scegliendo $n = \min\{r, p - r\}$ si ha che $p|n^4 - 1$ e, poiché p è dispari, $n < p/2$, ovvero $p > 2n$.

Per vedere che il numero di interi positivi n di questo tipo è infinito, basterà provare che infinito è il numero di primi che dividono qualche numero del tipo $m^4 + 1$. Per provarlo,

si fa come Euclide: se infatti, per assurdo, ci fosse solo un numero finito $p_1, p_2, \ldots, p_k$ di tali primi, si avrebbe che almeno uno di essi divide $(p_1 p_2 \cdots p_k)^4 + 1$, che è una palese contraddizione.

* * *

PROBLEMA 18. Facciamo un'osservazione preliminare sulle potenze modulo 5: se a è un numero intero e $5 \nmid a$ allora $a^2 \equiv 1, -1 \pmod 5$ (questo si vede direttamente elevando al quadrato i numeri $1, 2, 3$ e 4).
Venendo al problema, per quanto appena osservato, dato un insieme A di tre numeri interi distinti, o almeno uno degli elementi, chiamiamolo x, è un multiplo di 5, oppure ne esistono due, diciamo x e y, tali che $x^2 \equiv y^2 \pmod 5$.
Nel primo caso, scegliendo y un qualsiasi altro elemento di A, si ha che 5 divide $x^n y^m$ per ogni $n, m \in \mathbb{N}^*$, e dunque 10 divide $x^m y^n - x^n y^m$ dato che quest'ultimo è un numero pari.
Nel secondo caso, siano m, n interi positivi dispari. Se $m = n$ si ha $x^m y^n - x^n y^m = 0$. Altrimenti, possiamo porre $m < n$, per cui $n - m = 2k$ per qualche $k \in \mathbb{N}^*$; ma allora, per la scelta di $\{x, y\} \subset A$,

$$x^m y^n - x^n y^m = x^m y^m (y^k - x^k) = x^m y^m ((y^2)^k - (x^2)^k) \equiv 0 \pmod 5.$$

Dunque 10 divide $x^m y^n - x^n y^m$ per ogni $m, n \in \mathbb{N}^*$ dispari.

* * *

PROBLEMA 19. Una soluzione elementare si ottiene provando preliminarmente che

$$2^{5^n} \equiv 2^5 \equiv 32 \pmod{100}, \qquad (*)$$

per ogni $n \geq 1$. Questo è banale per $n = 1$; per $n = 2$ si ha, sviluppando la differenza di potenze, che

$$2^{5^2} - 2^5 = 2^5 (2^{20} - 1) = 2^5 (2^5 - 1)(2^5 + 1)(2^2 + 1)(2^8 - 2^6 + 2^4 - 2^2 + 1)$$

è divisibile per $2^2 \cdot 5^2 = 100$. Procedendo per induzione, supponiamo l'asserzione vera per $n \geq 2$; allora

$$2^{5^{n+1}} - 2^{5^n} = (2^{5^n})^5 - (2^{5^{n-1}})^5$$

è un multiplo di $2^{5^n} - 2^{5^{n-1}}$, che a sua volta è multiplo di 100 per ipotesi induttiva. La congruenza $(*)$ è dunque provata. Pertanto, modulo 100 si ha

$$2^5 + 2^{5^2} + \ldots + 2^{5^{1991}} \equiv 2^5 \cdot 1991 \equiv 32 \cdot 91 \equiv 12 \pmod{100},$$

dunque il numero formato dalle ultime due cifre della rappresentazione decimale del numero dato, ovvero il resto della sua divisione per 100, è 12.

* * *

PROBLEMA 20. La risposta è che 1 è l'unico intero positivo coprimo con tutti i termini della successione data. Per provarlo, è sufficiente mostrare che ogni primo p divide almeno un termine della successione.

Ora, 2 divide $a_1 = 10$ e 3 divide $a_2 = 48$. Se $p \geq 5$, per il Teorema di Fermat,

$$6a_{p-2} = 6(2^{p-2}+3^{p-2}+6^{p-2}+1) = 3\cdot 2^{p-1}+2\cdot 3^{p-1}+6^{p-1}-6 \equiv 2+3+1-6 = 0 \pmod{p},$$

dunque p divide a_{p-2}.

* * *

Problema 21. Supponiamo, per assurdo, che l'insieme S dei divisori primi dei numeri

$$x_n = 2^{n^3+1} - 3^{n^2+1} + 5^{n+1},$$

al variare di n in $\mathbb{N}^*$, si finito; diciamo $S = \{p_1, p_2, \ldots, p_k\}$. Sia $m = (p_1 - 1)(p_2 - 1)\cdots(p_k - 1)$. Allora, per il Teorema di Fermat,

$$x_m \equiv 2 - 3 + 5 \equiv 4 \pmod{p}$$

per ogni primo $p \in S \setminus \{2, 3, 5\}$. Ma anche si ha $x_m \equiv -1 \pmod 5$ e $x_m \equiv 1 \pmod 3$. Poiché, per assunzione, ogni divisore primo di x_m appartiene a S, si conclude che x_m è necessariamente una potenza di 2. Questo è assurdo: infatti, dato che certamente $m \geq 2$, si ha $2^{n^3} > 3^{n^2+1} - 5^{n+1} > 0$, quindi

$$2^{n^3+1} > x_m > 2^{n^3+1} - 2^{n^3} = 2^{n^3}$$

e dunque x_m non può essere una potenza di 2.

* * *

Problema 22. Un'altra variazione sul Teorema Cinese dei Resti. Fissiamo una sequenza infinita $p_0, p_1, p_2, \ldots$ di numeri primi distinti. Scegliamo a_1 in modo che $a_1 \equiv 0 \pmod{p_0}$; quindi, applicando il TCR, prendiamo a_2 tale che

$$\begin{cases} a_2 \equiv 0 \pmod{p_0} \\ a_2 + 1 \equiv 0 \pmod{p_1} \end{cases}$$

e, come sicuramente si può fare, dato che a_2 si sceglie in una classe di congruenza modulo p_0p_1, $a_2 > a_1$. Procediamo quindi induttivamente; per $n \geq 2$, assumendo di avere determinato $a_1, a_2, \ldots, a_n$, scegliamo a_{n+1} in modo che $a_{n+1} > a_n$ e

$$\begin{cases} a_{n+1} \equiv 0 \pmod{p_0} \\ a_{n+1} + 1 \equiv 0 \pmod{p_1} \\ \ldots \\ a_{n+1} + n \equiv 0 \pmod{p_n} \end{cases}$$

In questo modo otteniamo una successione infinita $a_1 < a_2 < a_3 < \ldots$ di numeri interi positivi tale che, per ogni $i \geq 1$ ed ogni $0 \leq k < i$,

$$a_i + k \equiv 0 \pmod{p_k}.$$

Per costruzione, fissato $k \geq 0$, tutti i numeri del tipo $a_i + k$ con $i \geq k + 1$ sono multipli distinti del primo p_k, e dunque la successione $\{a_n + k \mid n \geq 1\}$ contene al più k numeri primi.

* * *

PROBLEMA 23. Sia $n \geq 1$ tale che $3 \mid 2^n - 1$ e $\frac{2^n-1}{3}$ divide $4m^2 + 1$ per qualche $m \in \mathbb{Z}$. Mostriamo che n è una potenza di 2.

Poiché $2^n \equiv 1 \pmod 3$, si ha subito che $n = 2k$ per qualche $k \geq 1$. Supponiamo per assurdo che esista un primo dispari s che divide n; allora, $2^s - 1$ divide $2^n - 1$ e, poiché $2^s \equiv 2 \pmod 3$, di ha che $2^s - 1$ divide $\frac{2^n-1}{3}$, quindi $2^s - 1$ divide $4m^2 + 1$. Ora, da $2^s - 1 \equiv 3 \pmod 4$ segue che $2^s - 1$ ammette almeno un divisore primo q con $q \equiv 3 \pmod 4$; quindi $q = 2\ell + 1$ per qualche ℓ dispari. Allora, tenendo conto che $4m^2 \equiv -1 \pmod q$, e applicando il teorema di Fermat modulo q,

$$1 \equiv (2m)^{q-1} \equiv (2m)^{2k} \equiv (4m^2)^{\ell} \equiv (-1)^{\ell} \equiv -1 \pmod q,$$

che è un assurdo. Pertanto, $n = 2k$ e k non ha divisori dispari; dunque n è una potenza di 2.

Viceversa, mostriamo che se $n = 2^t$ per qualche $s \geq 1$ allora le condizioni del Problema sono soddisfatte. Se $t = 1$ la cosa è banale; sia quindi $t \geq 2$. Intanto, poiché n è pari, 3 divide $2^n - 1$, inoltre

$$2^{2^t} - 1 = (2^{2^{t-1}} + 1)(2^{2^{t-1}} - 1) = \ldots = (2^{2^{t-1}} + 1)(2^{2^{t-2}} + 1) \cdots (2^2 + 1)(2 + 1).$$

Pertanto,

$$\frac{2^n - 1}{3} = F_{t-1} \cdot F_{t-2} \cdots F_2 \cdot F_1,$$

Dove $F_i = 2^{2^i} + 1$ è l'i-esimo numero di Fermat. Ora, i numeri $F_{t-1}, F_{t-1}, \ldots, F_1$ sono a due a due coprimi (questo è l'esercizio 1.5); possiamo dunque applicare il Teorema Cinese dei Resti per dedurre l'esistenza di un numero intero positivo u tale che $u \equiv 0 \pmod 2$ e

$$u \equiv 2^{2^{i-1}} \pmod{F_i}$$

per ogni $i1 \leq i \leq t - 1$. Allora $c = 2m$, e $c^2 \equiv 2^{2^i} \equiv -1 \pmod{F_i}$ per ogni $1 \leq i \leq t - 1$, e quindi

$$4m^2 = c^2 \equiv -1 \pmod{(2^n - 1)/3},$$

che è quel che si voleva. In conclusione, la proprietà richiesta del problema è soddisfatta da tutti e soli gli interi n che sono potenza di 2.

* * *

PROBLEMA 25. Osserviamo che $7^2 \equiv 6 \pmod{43}$ e $6 \cdot 7 \equiv -1 \pmod{43}$. Quindi, senza fare altri conti,

$$7^3 \equiv -1 \pmod{43} \quad \text{e} \quad 6^3 \equiv 1 \pmod{43}$$

Sia $p = 3k + i$ con $i = 1, 2$ (siccome p è primo $i = 0$ darebbe $p = 3$ che è escluso per ipotesi). Se $i = 1$, k è pari, dunque

$$7^p - 6^p - 1 = 7^{3k} \cdot 7 - 6^{3k} \cdot 6 - 1 \equiv (-1)^k 7 - 6 - 1 \equiv 7 - 6 - 1 \equiv 0 \pmod{43};$$

mentre se $i = 2$, k è dispari e

$$7^p - 6^p - 1 = 7^{3k} \cdot 7^2 - 6^{3k} \cdot 6^2 - 1 \equiv (-1)^k 7^2 - 6^2 - 1 \equiv -49 - 36 - 1 \equiv 0 \pmod{43}.$$

In ogni caso 43 divide $7^p - 6^p - 1$.

* * *

PROBLEMA 26. Sia $n \geq 1$ e supponiamo esistano interi x, y tali che

$$(19y + x)^{18} + (x + y)^{18} + (19x + y)^{18} = n^2. \qquad (*)$$

Se, ad esempio, $x = 0$, allora l'identità diventa

$$(19^{18} + 2)y^{18} = n^2,$$

e quindi $19^{18} + 2 = k^2$ per qualche $k \geq 1$, che chiaramente non è possibile (risulterebbe $2 = (k - 19^9)(k + 19^n)$ che non si dà); alllo stesso modo si ragiona per y.
Dunque $x \neq 0 \neq y$. Sia $d = mcd(x, y)$ e scriviamo $x = da$, $y = db$; allora nel termine di sinistra di $(*)$ si può raccogliere il fattore d^{18}, ottenendo

$$d^{18}[(19y + x)^{18} + (x + y)^{18} + (19x + y)^{18}] = n^2.$$

Quindi $n^2 = d^{18}m^2$ con $m \geq 1$, e (a, b) è soluzione di

$$(19y + x)^{18} + (x + y)^{18} + (19x + y)^{18} = m^2.$$

Dunque, se l'equazione $(*)$ ha una soluzione, allora c'è un opportuno valore del parametro n per cui l'equazione ha una soluzione i cui elementi sono non nulli e coprimi.
Sia data una tale soluzione (x, y), e passiamo alla congruenza associata modulo il primo 19, che è

$$x^{18} + (x + y)^{18} + y^{18} \equiv n^2 \pmod{19}.$$

Ora, il termine di destra è un quadrato modulo 19, quindi, da un esame diretto, appartiene a $\{0, 1, 4, 5, 6, 7, 9, 11, 17\}$, mentre, per il Teorema di Fermat, quello di sinistra è congruo a $0 \leq k \leq 3$, dove k è il numero di elementi dell'insieme $\{x, y, x + y\}$ che non sono multipli di 19. Dunque, $k = 0, 1$. Ma k non può essere 1 perchè se due tra i termini x, y e $x + y$ sono divisi da 19 allora lo è anche il terzo. Quindi $k = 0$; cioè sia x che y sono multipli di 19, il che contraddice il fatto che siano coprimi.
In conclusione, l'equazione $(*)$ non ha soluzioni con $n \geq 1$ (abbiamo di fatto provato che se $n = 0$ allora l'unica soluzione è quella nulla).

* * *

PROBLEMA 27. [a] La risposta alla prima domanda è che, per $n \geq 1$, $7 \mid 2^n - 1$ se e solo se $3 \mid n$. Infatti, se $n = 3m$, con $m \geq 1$, allora

$$2^n - 1 = 2^{3m} - 1 = (2^3 - 1)(2^{3(m-1)} + \ldots + 2^3 + 1)$$

è un multiplo di 7. Viceversa, poiché $7 \mid 2^3 - 1$, se $7 \mid 2^n - 1$, allora 7 divide

$$mcd(2^n - 1, 2^3 - 1) = 2^{mcd(n,3)} - 1,$$

quindi $mcd(n, 3) = 3$, cioè $n \mid 3$.

Per il seconda richiesta, supponiamo, per assurdo, che esista $n \geq 1$ tale che 7 divide $2^n + 1$; allora 7 divide $(2^n + 1)(2^n - 1) = 2^{2n} - 1$, dunque $3 \mid 2n$ per il punto precedente. Ma questo implica $3 \mid n$ e di conseguenza che 7 divide anche $2^n - 1$, quindi 7 divide $(7^n + 1) - (7^n - 1) = 2$, che è assurdo.

[b] È un'applicazione della Proposizione 1.11. Siano a, b interi positivi con $b \geq 2$, e assumiamo che $2^b - 1$ divida $2^a + 1$. Alllora $2^b - 1 \mid (2^a + 1)(2^a - 1) = 2^{2a} - 1$ e quindi, per la Proposizione 1.11, $b \mid 2a$. D'altra parte, poiché $mcd(2^a + 1, 2^a - 1) = 1$, si deve avere $mcd(2^b - 1, 2^a - 1) = 1$ e dunque, sempre per la Proposizione 1.11, $(a, b) = 1$. Pertanto $b = 2$ e a è dispari. In questi casi, di fatto, $2^2 - 1 = 3$ divide $2^a + 1$.

* * *

Problema 28. Supponiamo che la coppia (a, n) di interi positivi soddisfi l'identità data. Considerando l'espressione modulo a, si ha

$$2001 = a^{n+1} - (a + 1)^n \equiv -1 \pmod{a},$$

quindi a divide $2001 + 1 = 2002 = 2 \cdot 7 \cdot 11 \cdot 13$.
D'altra parte, poiché 3 divide 2001, $a^{n+1} \equiv (a+1)^n \pmod 3$ e, poiché a non è multiplo di 3, questo forza $a \equiv 1 \pmod 3$ e n pari; scriviamo $n = 2t$.
Posto $b = a + 1$, si ha $(b-1)^{2t+1} - b^{2t} = 2001$, e quindi, come prima, $2001 \equiv -1 \pmod b$. Dunque, sia a che $a + 1$ sono divisori di 2002. Mediante una breve verifica diretta si troca che vi sono solo due coppie di numeri consecutivi che sono divisori 2002, che sono $(1, 2)$ e $(13, 14)$. La coppia $(1, 2)$, cioè $a = 1$, si vede subito no va bene (2000 non è una potenza di 2). Rimane la seconda possibilità, ovvero $a = 13$, che invece funzione per $n = 2$:

$$13^3 - 14^2 = 2001,$$

e, per ovvie ragioni di ordine, per nessun altro esponente $n \geq 3$. Quindi la sola coppia che verifica l'identità proposta è $(a, n) = (13, 2)$.

* * *

Problema 29. La risposta è 3. Poiché nessuna potenza di 10 è un multiplo di 503, cominciamo col provare che non esistono multipli k di 503 con $S(k) = 2$.
Osserviamo subito che 503 è un numero primo e che $503 \equiv 3 \pmod 4$. Dunque, per il Lemma 1.20, la congruenza $x^2 \equiv -1 \pmod{503}$ non ha soluzioni. Sia, per assurdo, k multiplo di 503 con $S(k) = 2$; allora $k = 10^m + 10^t$ per qualche $1 \leq t < m$. Da ciò segue che 503 divide $10^t(10^{m-t} + 1)$, il che significa $10^{m-t} \equiv -1 \pmod{503}$ che, come abbiamo detto, non è possibile.

Per provare che esiste un multiplo k di 503 tale che $S(k) = 3$, utilizziamo un argomento che è un caso particolare di una proprietà delle classi di resto modulo un numero primo, che proveremo nel capitolo 4. Per $a \in \mathbb{Z}$ scriviamo $\overline{a}$ il resto della divisione di a per 503, quindi poniamo $X = \{\overline{10^n} \mid n \geq 0\}$. Sappiamo, per Fermat, che $10^{502} \equiv 1 \pmod{503}$, quindi $(10^{251})^2 \equiv 1 \pmod{503}$, e dunque (per quanto prima osservato) $10^{251} \equiv 1 \pmod{503}$. Poichè 251 è un numero primo, si ha $10^t \not\equiv 1 \pmod{503}$ per ogni $1 \leq t < 251$, il che comporta in particolare che, per $1 \leq i, j \leq 251$, $10^i \equiv 10^j \pmod{503}$ se e solo se $i = j$. Pertanto $|X| = 251$.

Chiaramente, $0 \notin X$ e, per quanto osservato, $502 = 503 - 1 \notin X$; quindi $X \subseteq \{1, \ldots, 501\}$. Posto $Y = 502 - X = \{502 - x \mid x \in X\}$, si ha ancora $Y \subseteq \{1, \ldots, 501\}$. Ora, $|Y| = |X| = 251$ e quindi

$$|X \cap Y| = |X| + |Y| - |X \cup Y| \geq 502 - |\{1, \ldots, 501\}| > 0.$$

Quindi $X \cap Y \neq \emptyset$ e dunque esistono interi positivi n, m tale che $\overline{10^n} = 502 - \overline{10^m}$, ovvero

$$10^n + 10^m \equiv 502 \equiv -1 \pmod{503}.$$

Il numero $k = 10^n + 10^m + 1$ è un multiplo di 503 e $S(k) = 3$.

COMMENTO. Il testo originale di questo problema ha il numero 2003 al posto di 503. Ho fatto la sostituzione per eliminare diversi calcoli; lo spirito della soluzione rimane.

* * *

PROBLEMA 30. Si tratta di determinare $g(6, 9, 20)$. Cominciamo osservando che, poiché

$$g(3, 10) = 30 - 3 - 10 = 17,$$

ogni numero *pari* strettamente maggiore di 34 è rappresentabile come combinazione a coefficienti non negativi di 6 e 20. Sia $n > 43$ un numero dispari, allora $n - 9 > 34$ è un numero pari, quindi $n = (n - 9) + 9$ è rappresentabile in $6, 9, 20$. D'altra parte, poichè 43 è dispari, se fosse rappresentabile come $43 = 6x + 9y + 20z$, il coefficiente y deve essere un numero dispari; ma né $43 - 9 = 34$, nè $43 - 27 = 16$ sono rappresentabili in $6, 20$. Quindi, 43 non è rappresentabile in $6, 9, 20$. Dunque

$$g(6, 9, 20) = 43$$

che è la risposta al problema.

* * *

PROBLEMA 31. Sia n un intero positivo pari, e sia $k \geq \frac{n^2}{2}$. Allora, $k = qn + r$ con $q \geq \frac{n}{2}$ e $0 \leq r < n$. Poniamo $(b, c) = (0, \frac{r}{2})$ se r è pari, $(b, c) = (1, \frac{r-1}{2})$ se r è dispari; in ogni caso $b + 2c = r$ e $b + c \leq \frac{n}{2} \leq q$; poniamo infine $a = q - (b + c)$. Allora

$$an + b(n + 1) + c(n + 2) = (a + b + c)n + (b + 2c) = qn + r = n,$$

dunque n è rappresentabile. Proviamo ora che $k = \frac{n^2}{2} - 1$ non è rappresentabile. Infatti, supponiamo per assurdo

$$\frac{n^2}{2} - 1 = an + b(n + 1) + c(n + 2) = (a + b + c)n + (b + 2c)$$

cone $a, b, c \in \mathbb{N}$; allora $b + 2c \equiv -1 \pmod{n}$, e dunque $b + 2c \geq n - 1$. Ma allora

$$n - 1 \leq b + 2c \leq 2(a + b + c) \leq 2(n/2 - 1) = n - 2,$$

che è assurdo. Abbiamo quindi provato $g(n, n + 1, n + 2) = \frac{n^2}{2} - 1$.

1.7. Speciale problemi con le cifre

Problemi riguardanti le cifre della rappresentazione decimale, o talvolta in altra base, dei numeri interi positivi sono piuttosto frequenti nei testi di competizioni matematiche per le scuole superiori. A parte le domande concernenti le ultime cifre (a destra) che, come abbiamo già visto in qualche esempio, sono di fatto problemi di congruenza modulo 10, 100, etc., si tratta in generale di questioni abbastanza semplici, alla cui soluzione si arriva impostando per bene un problema aritmetico; a volte però possono rivelarsi piuttosto complesse, richiedere una certa dose di immaginazione oltre che di abitudine a descrivere accuratamente procedure che intuitivamente possono sembrare quasi ovvie (e non sempre lo sono). Altre volte ancora (come ad esempio il Problema 29 della sezione precedente) prevedono il ricorso a tecnica e perizia non del tutto banali.

Somme e prodotti delle cifre.

Per ogni intero positivo n, denotiamo con $S(n)$ la somma delle cifre nella rappresentazione decimale di n e con $P(n)$ il loro prodotto. Per esempio, $S(4167) = 4 + 1 + 6 + 7 = 17$ e $P(4167) = 4 \cdot 1 \cdot 6 \cdot 7 = 168$.
Formalmente, scrivendo

$$n = a_{c-1}10^{c-1} + \ldots + a_1 10 + a_0, \tag{1.5}$$

con $a_i \in \{0, 1, \ldots, 9\}$ e $a_{c-1} \neq 0$ (c è il *numero di cifre* di n), si pone $S(n) = a_{c-1} + \ldots + a_1 + a_0$ e $P(n) = a_{c-1} \cdot \ldots \cdot a_1 \cdot a_0$.
Il criterio di divisibilità per 9 (la prova del nove) non è altro che una derivazione del fatto, semplice, che per ogni $n \geq 0$

$$S(n) \equiv n \pmod 9.$$

Altre proprietà immediate della funzione S, come ad esempio la *subadditività*:

$$S(n + m) \leq S(n) + S(m), \text{ per ogni } n, m \in \mathbb{N}^*$$

non sono difficili da intuire e dimostrare quando se ne presenti la necessità. Una cosa che risulta subito evidente è che, in genere, $S(n)$ è molto più piccola di n; infatti, se c è il numero di cifre decimali di $n \geq 1$,

$$S(n) \leq 9c \leq 9 \cdot ([\log_{10} n] + 1).$$

Anche delle stime grossolane, come ad esempio, nelle notazioni di (1.5),

$$n \geq (9a_{c-1} + S(n)) \cdot 10^{c-2} \tag{1.6}$$

possono tornare utili (si dimostri (1.6) per esercizio).

Problema 32 (Italia 2002)**.** *Determinare tutti gli interi positivi che sono uguali a* 34 *volte la somma delle loro cifre.*

SOLUZIONE. Sia $n \in \mathbb{N}^*$ tale che $n = 34S(n)$, e sia c il numero di cifre decimali di n. Da (1.6) segue immediatamente $C \leq 3$. Dunque

$$n = a_2 10^2 + a_1 10 + a_0 = 34(a_2 + a_1 + a_0)$$

da cui segue $66a_2 - 33a_0 = 24a_1$. Dunque, in particolare $11 \mid a_1$ e quindi $a_1 = 0$. Rimane $2a_2 = a_0$, e infine $n = 102, 204, 306, 408$. ∎

Il prodotto $P(n)$ delle cifre di n è un po' meno ricorrente. Una diseguaglianza immediata che può essere utile è, con le notazioni in (1.5),

$$n \cdot 9^{c-1} \geq P(n) \cdot 10^{c-1}. \tag{1.7}$$

Problema 33 (IMO, Mosca 1968)**.** *Trovare tutti gli interi positivi n tali che*

$$P(n) = n^2 - 10n - 22.$$

SOLUZIONE. Sia n un intero positivo con $P(n) = n^2 - 10n - 22$. Allora

$$n \geq P(n) = n^2 - 10n - 22 > 0$$

da cui

$$\begin{cases} n^2 - 11n - 22 \leq 0 \\ n^2 - 10n - 22 > 0. \end{cases}$$

che risolto negli interi positivi dà $n = 12$. Infine, $P(12) = 2 = 12^2 = 10 \cdot 12 - 22$; dunque il solo intero positivo n che soddisfa la richesta è $n = 12$. ∎

Dei problemi di questa sezione daremo una soluzione, alla fine, solo nei casi che sono sembrati meno semplici.

Problema 34 (Italia 2012)**.** *Determinare tutti gli interi positivi che sono uguali a 300 volte la somma delle loro cifre.*

Problema 35 (Nordic MC, 1996)**.** *Provare che esiste un multiplo n di 1996 la somma delle cifre del quale è 1996.*

Problema 36 (Baltic Way, 2006)**.** *Un intero positivo n, multiplo di 37, ha rappresentazione decimale composta di 12 cifre, che appartengono a $\{1, 5, 9\}$. Provare che $S(n) \neq 76$.*

Problema 37 (Nordic MC, 2005)**.** *Determinare tutti gli interi positivi k tali che*

$$P(k) = \frac{25}{8}k - 211.$$

Problema 38 (IMO, Sofia 1975)**.** *Sia $n = 4444^{4444}$ scritto in notazione decimale. Sia $A = S(n)$; calcolare $S(S(A))$.*

Problema 39 (IMO, Bucarest 1960)**.** *Determinare tutti gli interi positivi $n < 1000$ che sono multipli di 11 e tali che la somma dei quadrati delle cifre della loro rappresentazione decimale è uguale a $\frac{n}{11}$.*

Spostamenti di cifre.

Una cosa abbastanza divertente da fare con le cifre è spostarle.

Problema 40 (Gara Matematica)**.** *Determinare il più piccolo intero positivo con la seguente proprietà: se la prima cifra decimale viene trasferita all'ultimo posto (esempio* $46729 \to 67294$*) si ottiene il triplo del numero di partenza. Quali numeri hanno la proprietà precedente ?*

SOLUZIONE. Sia n un intero positivo tale che spostando all'ultimo posto la prima cifra decimale di n si ottiene $3n$. Osserviamo che, poiché il numero di cifre di $3n$ è uguale a quello di n, la prima cifra a di n deve essere al più 3; inoltre, n ha almeno due cifre, quindi

$$n = a \cdot 10^k + m$$

con $a \in \{1, 2, 3\}$, $k \geq 1$ e $m < 10^k$. Spostando a a destra si deve avere,

$$10m + a = 3n = 3a \cdot 10^k + 3m,$$

dunque, $7m + a = 3a \cdot 10^k$. Questo consente di escludere il caso $a = 3$ perché se così fosse si avrebbe $7m > 9 \cdot 10^k$, che è assurdo perché $m > 10^k$. Dunque $a = 1, 2$ e

$$3a \cdot 10^k \equiv a \pmod 7; \qquad (*)$$

ovvero, poiché a è coprimo con 7, $3 \cdot 10^k \equiv 1 \pmod 7$.
Per il teorema di Fermat, $10^6 \equiv 1 \pmod 7$, mentre $10^2 \equiv 2 \pmod 7$ e $10^3 \equiv 6 \pmod 7$. Quindi

$$3 \cdot 10^5 \equiv 3 \cdot 10^3 \cdot 10^2 \equiv 3 \cdot 12 \equiv 1 \pmod 7,$$

e la congruenza $(*)$ è verificata se e solo se $k = 5 + 6t$, con $t \geq 0$.
Il minimo per $n = a \cdot 10^k + m$ si ha quindi con $a = 1$, $k = 5$; si trova $m = \frac{3 \cdot 10^5 - 1}{7} = 42857$, per cui $n = 142857$.
La risposta alla seconda domanda è di fatto già ricavata dall'analisi della congruenza $(*)$; si tratta dei numeri $n = a \cdot 10^k + m$, dove $a = 1, 2$, $0 < k \equiv 5 \pmod 6$ e $m = \frac{a(3 \cdot 10^k - 1)}{7}$. ∎

Problema 41 (Baltic Way, 2011)**.** *Trovare tutti gli interi positivi d tali che ogni qual volta d divide un intero positivo n, allora d divide ogni intero ottenuto riordinando le cifre decimali di n.*

Problema 42 (Nordic MC, 1988)**.** *L'intero positivo n ha la proprietà che levando le ultime tre cifre a destra nella rappresentazione decimale di n rimane $\sqrt[3]{n}$. Trovare n.*

Problema 43 (Italia 1997)**.** *Sia X l'insieme degli interi positivi che in base dieci non si scrivono con una sola cifra ripetuta (una o) più volte. Per ogni $n \in X$ definiamo A_n come l'insieme dei numeri ottenuti permutando in tutti i modi possibili le cifre di n e sia d_n il massimo comun divisore di tutti i numeri di A_n. Ad esempio*

$$A_{1120} = \{112, 121, 211, 1012, 1021, 1102, 1120, 1201, 1210, 2011, 2101, 2110\}$$

e $d_{1120} = 1$ (112 e 121 sono coprimi). Si determini il massimo valore possibile di d_n.

Problema 44 (UK 1997)**.** (a) *Siano N e M due interi positivi di 9 cifre decimali con la proprietà che se una cifra di M è rimpiazzata dalla cifra di N che occupa il posto corrispondente, il numero che risulta è un multiplo d 7. Provare che ogni numero ottenuto rimpiazzando una cifra di N con la corrispondente cifra di M è anche un multiplo di 7.*
(b) *Trovare un intero $d > 9$ tale che il risultato di sopra rimane valido quando M ed N sono due interi positivi con d cifre.*

Condizioni speciali sulle cifre.

In questo genere di problemi si considerano condizioni specifiche sulla natura o la disposizione delle cifre nelle rappresentazioni decimali; una buona parte delle questioni che vengono proposte si può grossolanamente ripartire in due tipi: in uno si chiede di determinare un certo ristretto insieme di numeri le cui rappresentazioni decimali soddisfano le condizioni volute, nell'altro di provare che certe classi di numeri contengono elementi le cui rappresentazioni decimali soddisfano le condizioni date. Vediamo un esempio di ciascun tipo.

Problema 45 (Centroamerica[16], 2001)**.** *Trovare tutti i numeri naturali n tali che:*

1. La rappresentazione decimale di n ha solo due cifre diverse da zero, e una di queste è 3.

2. n è un quadrato in $\mathbb{N}$.

Soluzione. Sia n come cercato; poiché solo due cifre della sua rappresentazione decimale sono non zero, ed una di queste è la cifra 3, esistono $0 \leq t < k$ ed $1 \leq a \leq 9$, tali che

$$n = 3 \cdot 10^k + a \cdot 10^t \quad \text{oppure} \quad n = a \cdot 10^k + 3 \cdot 10^t.$$

Osserviamo che, poiché n è un quadrato, t è un numero pari; dividendo allora per 10^t abbiamo ancora un intero m che soddisfa le condizioni per n:

$$\text{(i) } m = 3 \cdot 10^s + a \quad \text{oppure} \quad \text{(ii) } m = a \cdot 10^s + 3,$$

con $s \geq 1$. Se $s = 1$ si verifica facilmente che il solo caso buono è $m = 36$.
Sia quindi $s \geq 2$. Allora $m \equiv a, 3 \pmod 4$ (a seconda dei casi); d'altra parte, poiché m è un quadrato, $m \equiv 0, 1 \pmod 4$. Questo esclude il caso (ii) e, nel caso (i), implica $a \in \{1, 4, 5, 8, 9\}$. Un'ulteriore riduzione si ricava considerando m modulo 9: infatti $m \equiv S(m) = 3 + a \pmod 9$, quindi, poiché i quadrati modulo 9 sono $0, 1, 4, 7$, si deve avere $a \in \{1, 4, 6, 7\}$. Dunque $a = 1, 4$.
Ora, possiamo porre $a = b^2$ (con $b = 1, 2$) e $m = 3 \cdot 10^s + b^2 = x^2$, per qualche $x \in \mathbb{N}^*$; quindi

$$3 \cdot 10^s = (x - b)(x + b).$$

Poiché $mcd(x + b, x - b) = 1, 2, 4$, se - ad esempio - $5 \mid x + b$, allora $5^s \mid x + b$, e quindi

$$5^s - 4 \leq (x + b) - 2b = x - b \leq 3 \cdot 2^s,$$

[16] La *Olimpiada Matemática de Centroamérica y El Caribe* si disputa dal 1999.

che forza $s = 1$, caso che è già stato escluso. Assumendo, invece, che 5 divida $x - b$ si perviene ad una simile contraddizione.
In conclusione, rimangono solo i casi in cui $s = 1$; ovvero, risalendo a n, $n = 36 \cdot 10^t$ con t un numero pari. ∎

Problema 46 (USA 2003)**.** *Provare che per ogni intero positivo n esiste un multiplo di 5^n la cui rappresentazione decimale consiste di n cifre tutte dispari.*

Soluzione. Fissato il numero n, sia X l'insieme di tutti gli interi positivi la cui rappresentazione decimale consiste di n cifre tutte dispari. Siano $a = a_{n-1}10^{n-1} + \dots a_1 10 + a_0$, $b = b_{n-1}10^{n-1} + \dots b_1 10 + b_0$ elementi di X, tali che $a \equiv b \pmod{5^n}$. Se $a \neq b$ esiste un minimo $0 \leq k \leq n-1$ tale che $a_k \neq b_k$, e si ha

$$a - b = a_{n-1}10^{n-1} + \dots a_k 10^k - b_{n-1}10^{n-1} + \dots b_k 10^k = c \cdot 10^k,$$

con $c = a_{n-1}10^{n-k-1} + \dots a_k - b_{n-k-1}10^{n-1} + \dots b_k$,. Da $5^n \mid a - b$ segue allora $5^{n-k} \mid c$, di conseguenza l'ultima cifra decimale c_0 di c è 0 oppure 5, dunque $a_k - b_k \equiv 0, 5 \pmod{10}$. Siccome a_k e b_k sono dispari compresi tra 1 e 9, la loro differenza è un numero pari, e questo forza la contraddizione $a_k = b_k$.
Abbiamo dunque provato che elementi distinti di X appartengono a classi di resto distinte modulo 5^n. Poiché $|X| = 5^n$ si conclude che X è un sistema di rappresentanti delle classi di resto modulo 5^n. In particolare esiste $x \in X$ tale che $x \equiv 0 \pmod{5^n}$, che è quello che si voleva provare. ∎

Tra i problemi che seguono si trovano anche altri generi di domande.

Problema 47 (IMO, Canberra 1988)**.** *Diciamo che un intero positivo è* doppio *se la sua rappresentazione decimale consiste in un blocco di cifre, la prima delle quali non è zero, seguito da un blocco identico. Ad esempio,* 360360 *è doppio, mentre* 36036 *non lo è. Provare che esistono infiniti quadrati perfetti che sono numeri doppi.*

Problema 48 (Centroamerica, 2016)**.** *Trovare tutti gli interi positivi n la cui rappresentazione decimale ha 4 cifre, ognuna delle quali è un quadrato perfetto, e tali che n è divisibile per $2, 3, 5$ e 7.*

Problema 49 (Italia 1999)**.** *Diciamo che un numero naturale è* equilibrato *se si scrive con tante cifre quanti sono i suoi divisori primi distinti (per esempio 15 è equilibrato mentre 49 non lo è). Dimostrare che esiste solo un numero finito di numeri equilibrati.*

Problema 50 (IMO, Pechino 1990)**.** *Trovare tutti gli interi positivi n per cui ogni intero positivo la cui rappresentazione decimale è formata da $n-1$ cifre uguali a 1 e da una cifra uguale a 7 è primo.*

Un problema sui numeri palindromi.

Un numero intero positivo si dice *palindromo* se invertendo l'ordine delle cifre nella sua rappresentazione decimale si ottiene lo stesso numero: ad esempio il numero 14641 è palindromo. Pur essendo uno dei temi pblueiletti della cosiddetta matematica ricreativa, i numeri palindromi non compaiono molto di frequente nelle gare.

Problema 51 (EM Cup, 2013)**.** *Provare che la successione*

$$x_n = 2013 + 317n$$

contiene infiniti numeri palindromi.

SOLUZIONE. Dopo aver osservato che 317 è un numero primo, ci proponiamo di dare una soluzione più generale. Proviamo che

• *Per ogni primo p ed ogni intero positivo a, la successione $\{np + a \mid n \in \mathbb{N}\}$ contiene infiniti numeri palindromi.*

1) Sia p un numero primo $p \neq 2, 5$. Fissato un qualunque $k \in \mathbb{N}^*$, $10^{k(p-1)} \equiv 1 \pmod{p}$ per il Teorema di Fermat. Se a è un qualsiasi intero positivo poniamo

$$m_{p,k}(a) = 10^{k(p-1)(b-1)} + 10^{k(p-1)(b-2)} + \ldots + 10^{k(p-1)} + 1.$$

$m_{p,k}(a)$ è un numero palindromo e

$$m_{p,k}(a) \equiv a \pmod{p}.$$

Dunque $m_{p,k}(a) - a = mp$ per qualche $m \in \mathbb{N}^*$, e quindi

$$mp + a = m_{p,k}(a)$$

è un numero palindromo che appartiene alla successione $\{np + a \mid n \in \mathbb{N}\}$. Questa successione contiene dunque infiniti numeri palindromi $m_{p,k}(a)$, con $k \in \mathbb{N}^*$.

2) Se $p = 2, 5$ la cosa è più elementare. Sia a un intero positivo e c il numero di cifre della sua scrittura decimale. Se a non è un multiplo di 10, poniamo $\bar{a}$ il numero ottenuto invertendo le cifre di a; allora per ogni $m \geq c$ il numero

$$\bar{a} \cdot 10^m + a$$

è un numero palindromo che appartiene alla successione $\{10n+a \mid \in \mathbb{N}\}$, dunque anche alle successioni $\{2n + a \mid n \in \mathbb{N}\}$ e $\{5n + a \mid n \in\}$. Se a è un multiplo di 10, sia $a = b10^t$ con $t \geq 1$ e b che non è multiplo di 10. Per quanto appena visto, la successione $\{5n+b \mid n \in \mathbb{N}\}$ contiene infiniti numeri palindromi; se K è uno di questi, il numero ottenuto aggiungendo a destra e a sinistra di K una sequenza di t cifre uguali a 5, è un numero palindromo che appartiene alla successione $\{5n + b \mid n \in \mathbb{N}\}$. Per il primo 2 si fa la stessa cosa. ∎

Altre basi.

Vediamo infine qualche problema riguardante le rappresentazioni in basi diverse da 10.

Problema 52 (Italia, 2013)**.** *In quali basi $b > 6$ la scrittura* 5654 *rappresenta una potenza di un numero primo?*

SOLUZIONE. Il numero rappresentato dalla scrittura 5654 nella base b è

$$5b^3 + 6b^2 + 5b + 4 = 5b^3 + 5b^2 + b^2 + b + 4b + 4 = (5b^2 + b + 4)(b + 1).$$

Poiché sicuramente uno tra i due fattori $b+1$ e $5b^2+b+4$ è un numero pari, se tale numero è la potenza di un primo deve necessariamente essere una potenza di 2. In particolare $b+1 = 2^m$ per qualche $m \geq 3$ (dato che $b \geq 7$). Dunque $b = 2^m - 1$ che, sostituito nell'atro fattore dà, per qualche $k \geq 0$

$$2^k = 5b^2 + b + 4 = 5(2^{2m} - 2^{m+1} + 1) + (2^m - 1) + 4 = 5 \cdot 2^{2m} - 9 \cdot 2^m + 8.$$

Questo forza $m = 3$ e, di conseguenza, $b = 7$. Infatti, facendo una verifica

$$5 \cdot 7^3 + 6 \cdot 7^2 + 5 \cdot 7 + 4 = 5 \cdot 343 + 6 \cdot 49 + 35 + 4 = 2048 = 2^{11}.$$

Dunque la sola base $b > 6$ in cui la scrittura 5654 rappresenta una potenza di un numero primo è $b = 7$. ∎

Problema 53 (UK 1999). *Per ogni intero positivo m denotiamo con $c(m)$ la somma dei cubi delle cifre nella rappresentazione in base 3 di m; dunque, per esempio,*

$$c(98) = 1^3 + 0^3 + 1^3 + 2^3 + 2^3 = 18.$$

Fissato un intero positivo n, definiamo la successione $\{u_r\}_{r\geq 1}$ ponendo $u_1 = n$, e $u_r = c(u_{r-1})$ per $r \geq 2$. Provare che esiste un intero positivo r tale che $u_r = 1, 2,$ o 17.

Problema 54 (Irlanda 1998). *Provare che nessun numero la cui rappresentazione decimale è del tipo $xyxy$ (x, y cifre) è il cubo di un numero intero. Trovare quindi il minimo $b \geq 2$ per cui esiste il cubo di un numero intero la cui rappresentazione in base b è del tipo $xyxy$.*

Problema 55 (Putnam, 2002). *Sia $b \geq 2$; un intero positivo si dice palindromo in base b se la sua rappresentazione in base b è palindroma; per esempio il numero 200 in base decimale non è palindromo, ma è palindromo in base 3 (2112), in base 9 (242), ed in base 7 (404). Dimostrare che esiste un intero positivo la cui rappresentazione in base b è un palindromo di tre cifre per almeno 2002 diversi valori di b.*

Problema 56 (IMO, Hong Kong 1994). *Per ogni intero positivo k, sia $f(k)$ il numero di elementi dell'insieme $\{k+1, k+2, \ldots, 2k\}$ la cui rappresentazione binaria (cioè in base 2) contiene esattamente tre 1.*

(a) *Provare che per ogni intero positivo m, esiste un intero positivo k tale che $f(k) = m$.*

(b) *Determinare tutti gli interi positivi m per i quali esiste un solo $k \in \mathbb{N}^*$ con $f(k) = m$.*

Soluzioni.

Problema 34. Il solo intero positivo n per cui $n = 300S(n)$ è $n = 2700$.

Problema 35. Ad esempio $n = 2 \cdot 10^{498} + 1994$ (tener presente che $1996 = 4 \cdot 499$, che 499 è primo, e Fermat).

PROBLEMA 36. Sia n un intero positivo come nel testo. Osserviamo subito che $3 \cdot 37 = 111$, e quindi il numero $k = 111.111.111.111 = 111 \cdot (10^9 + 10^6 + 10^3 + 1)$ è un multiplo di 37. Inoltre, si ha $1000 \equiv 1 \pmod{37}$.
Sia n un multiplo di 37 la cui rappresentazione decimale ha 12 cifre tutte appartenenti a $\{1, 5, 9\}$. Allora anche $m = n - k$ è un multiplo di 37 e le sue cifre sono $0, 4$ o 8; in particolare, m è un multiplo di 4. Scriviamo m in base 10^3,

$$m = m_3 10^9 + m_2 10^6 + m_1 10^3 + m_0 \qquad (*)$$

con $0 < m_i \leq 999$ $(i = 1, 2, 3, 4)$; allora

$$M = m_3 + m_2 + m_1 + m_0 \equiv m \equiv 0 \pmod{37}.$$

Osserviamo anche che M è un multiplo di 4; quindi $M = 37 \cdot 4 \cdot t = 148t$ con $t \in \mathbb{N}^*$.
Supponiamo, per assurdo, $S(n) = 76$; allora

$$S(m) = S(m_3) + S(m_2) + S(m_1) + S(m_0) = 76 - 12 = 64.$$

Ora, per la regola del 9, $M \equiv m \equiv S(m) \pmod{9}$, e dunque

$$148t = M \equiv 1 \pmod{9}.$$

Poiché $148 \equiv 4 \pmod{9}$, questo comporta $4t \equiv 1 \pmod{9}$, ovvero $t = 9s + 7$ per qualche $s \in \mathbb{N}$. D'altra parte, $M \leq 888 \cdot 4 = 3552$, e dunque

$$9s + 7 = t \leq \frac{3552}{148} = 24.$$

Quindi $t = 7, 16$. Ora osserviamo che, per ogni $i = 0, 1, 2, 3$, anche ogni m_i è un multiplo di 4 e che le cifre di $m_i/4$ sono $0, 1$ o 2. Quindi, 9 non compare tra le cifre di $M/4$. Ma, per quanto provato sopra

$$M/4 = 37 \cdot t \in \{37 \cdot 7, 37 \cdot 16\} = \{259, 592\},$$

e dunque la contraddizione.

PROBLEMA 37. Le sole soluzioni sono $k = 72$, $k = 88$.

PROBLEMA 38. Posto $n = 4444^{4444}$ e $A = S(n)$, si ha

$$n < (10^4)^{4444} = 10^{17776},$$

dunque il numero di cifre decimali di n è al più 17776, e pertanto $A \leq 9 \cdot 17776 < 160000$. Quindi, A è un numero di al più 6 cifre decimali e dunque $S(A) \leq 9 \cdot 6 = 54$. Da ciò segue facilmente $S(S(A)) \leq 13$. Ora sfruttiamo il fatto che $S(S(A)) \equiv S(A) \equiv A \equiv n \pmod{9}$. Poiché $4444 \equiv 7 \pmod{9}$ e $7^3 = 343 \equiv 1 \pmod{9}$, si ha

$$n \equiv 7^{4444} \equiv 7^{3 \cdot 1481 + 1} \equiv 7 \pmod{9}.$$

Quindi, $S(S(A)) \leq 13$ e $S(S(A)) \equiv 7 \pmod{9}$ e pertanto $S(S(A)) = 7$.

PROBLEMA 39. $n = 550,608$.

PROBLEMA 41. $d = 1, 3, 9$.

PROBLEMA 42. $n = 32768$.

PROBLEMA 43. Sia $c \geq 2$ il numero di cifre della rappresentazione decimale di $n \in X$, e siano a, b due cifre distinte di n, con $a > b$; allora l'insieme A_n contiene due numeri $A = m10^2 + a10 + b$ e $B = m10^2 + b10 + a$, con m un certo numero di $c - 2$ cifre. Il massimo comun divisore d_n divide

$$A - B = 9(a - b) \leq 81;$$

quindi il valore massimo possibile per d_n è 81.
Ora, qualsiasi coppia a, b di cifre distinte di intero $n \in X$ per cui $d_n = 81$ deve soddisfare $|a - b| = 9$, dunque le cifre di n possono essere solo $0, 9$. Inoltre , n deve essere un multiplo di 81, ovvero $n = 9k$ dove k è un multiplo di 9 le cui cifre sono tutte 0 o 1. Per il criterio del 9 un tale numero k deve un numero di cifre uguali a 1 che è un multiplo di 9, e almeno una cifra uguale a 0; il più piccolo k con tale proprietà è $k = 1.011.111.111$, a cui corrisponde $n = 9.099.999.999$, valore per il quale si verifica facilmente che $d_n = 81$.

PROBLEMA 44. (a) Scriviamo

$$M = a_8 10^8 + \ldots + a_1 10 + a_0, \quad N = b_8 10^8 + \ldots + b_1 10 + b_0,$$

e, per ogni $i = 0, \ldots, 8$, e denotiamo con M_i (rispettivamente N_i) il numero ottenuto rimpiazzando in M la cifra a_i con b_i (rispettivamente, in N la cifra b_i con a_i). Per ipotesi $7 \mid M_i$ per ogni $i = 0, \ldots, 8$; quindi, fissato $i \in \{0, \ldots, 8\}$, 7 divide

$$\sum_{j \neq i} M_j = (7a_8 + b_8)10^8 + \ldots + (8a_i)10^i + \ldots + (7a_0 + b_0) = 7M + N_i$$

e dunque $7 \mid N_i$.
(b) Come si vede facilmente, l'argomento utilizzato per il punto (a) funziona allo stesso modo per numeri di d cifre con $d = 7k + 2$.

PROBLEMA 47. Un intero positivo è doppio se e solo se si può scrivere nella forma

$$a \cdot 10^n + a = a(10^n + 1)$$

dove $n \geq 1$ ed a è un numero la cui rappresentazione decimale consiste in n cifre, quindi $10^{n-1} \leq a < 10^n$. L'idea è quella di individuare un insieme infinito di esponenti n per cui $10^n + 1$ sia diviso da un quadrato $b^2 \neq 1$, e quindi di adattare a in modo da ottenere che $a(10^n + 1)$ risulti a sua volta un quadrato. Scelgo $b = 11$; questo perché, per ogni $t \geq 0$,

$$10^t \equiv (-1)^t \pmod{11}.$$

Quindi, con un po' di facili conti

$$10^{11} + 1 = (10 + 1)(10^{10} - 10^9 + \ldots + 10^2 - 10 + 1) \equiv 0 \pmod{11^2},$$

cioè $10^{11} \equiv -1 \pmod{11^2}$. Dunque, per ogni k dispari, $10^{11k} \equiv -1 \pmod{11^2}$, ovvero 11^2 divide $10^{11k}+1$. Fissato un tale k dispari, e $n = 11k$, si ha $10^n + 1 = c(11)^2$, con $c \geq 1$. Poniamo $a = 10^2 c$; allora

$$a = \left(\frac{10}{11}\right)^2 (10^n + 1),$$

e con semplici diseguaglianze, tenendo conto che $10^3 > 11^2$, si vede che $10^{n-1} < a < 10^n$, dunque a è un numero di n cifre decimali. Infine,

$$a \cdot 10^n + a = a(10^n + 1) = 10^2 \cdot c \cdot 11^2 \cdot c = c^2 \cdot 10^2 \cdot 11^2$$

è un quadrato perfetto.

PROBLEMA 48. C'è un solo caso, $n = 4410$.

PROBLEMA 49. I numeri primi minori del numero 20 sono 8; quindi, se n è un numero equilibrato di $c \geq 8$ cifre decimali, poiché per definizione n ha c divisori primi distinti, si ha

$$10^c > n \geq 2^8 \cdot 20^{c-8},$$

da cui $10^8 > 2^c$ e quindi (poiché $2^7 > 10^2$) $c < 28$. Questo mostra che i numeri equilibrati sono tutti minori di 10^{28}. Infatti, con un po' di conti si vede che il più grande numero equilibrato è il prodotto $2 \cdot 3 \cdot \ldots \cdot 29$ dei primi dieci numeri primi, ed ha 10 cifre decimali.

PROBLEMA 50. Se $n = 1, 2$ si hanno i numeri $7, 17, 71$ che sono primi. Proviamo che questi sono i soli casi buoni.
Se $3 \mid n$ allora $(n-1) + 7 \equiv 0 \pmod{3}$ e quindi ogni numero la cui rappresentazione decimale contiene $n-1$ cifre 1 e una cifra 7 è multiplo di 3. Per $n = 4, 5$ si trovano i numeri 1711 e 11711 che sono, rispettivamente, multipli di 29 e di 7.
Possiamo quindi supporre $n \geq 7$ (e n non multiplo di 3); i numeri la cui rappresentazione decimale contiene $n-1$ cifre 1 e una cifra 7 sono quelli del tipo, al variare di $0 \leq t \leq n-1$

$$y_t = b_n + 6 \cdot 10^t \qquad (*)$$

dove b_n è il numero di n cifre decimali tutte uguali a 1. Ora, per Fermat, $10^6 \equiv 1 \pmod{7}$; inoltre si verifica direttamente che per ogni $x \not\equiv 0 \pmod{7}$ esiste un esponente $1 \leq t \leq 6$ tale che $10^t \equiv x \pmod{7}$.
In particolare, se in $(*)$ $7 \nmid b_n$, esiste $1 \leq t \leq 6$ tale che $b \equiv 10^t \pmod{7}$ e dunque

$$y_t \equiv b_n - 10^t \equiv 0 \pmod{7}$$

ovvero b_t è un multiplo di 7.
Rimangono quindi da trattare i casi in cui b_n è un multiplo di 7; cioè

$$7 \mid 10^{n-1} + 10^{n-2} + \ldots + 10 + 1 = \frac{10^n - 1}{9},$$

quindi $10^n \equiv 1 \pmod{7}$. Ma allora, per quanto detto sopra, $6 \mid n$, e questo è un caso già scartato all'inizio.

COMMENTO. Abbiamo di fatto provato che per ogni intero positivo $n \neq 2, 4$ esiste un numero di n cifre, di cui $n-1$ sono uguali a 1 e una uguale a 7, che è divisibile per 3 oppure per 7.

PROBLEMA 53. Poiché $c(17) = 1^2 + 2^2 + 2^2 = 17$ se la successione $\{u_r\}$ arriva a 17, diventa poi stazionaria, lo stesso se arriva ad 1. Se $1 \leq n \leq 16$ si verifica direttamente che la successione $\{u_r\}$ associata a n arriva a 1 o 2 a seconda n sia dispari o pari (dopo pochi passi: la sequenza più lunga che si trova è $6 \to 8 \to 16 \to 10 \to 2$).
A questo punto, si prova che per $n > 17$, $c(n) < n$; quindi la successione che parte da $n > 17$, dopo un numero finito di passi arriva ad un termine $u_r \leq 17$; se $u_r = 17$ la successione diventa stazionaria, altrimenti $u_r < 17$ e, per quanto detto sopra, la successione arriva a 2 o 1.
Resta da provare $c(n) < n$ per $n > 17$. Sia t il numero di cifre di n in base 3 (quindi $t \geq 3$). Sia $t \geq 4$; se la prima cifra di n (in base 3) è 2, allora

$$n \geq 2 \cdot 3^{t-1} > 8t \geq c(n);$$

se invece prima cifra di n è 1,

$$n \geq 3^{t-1} > 8(t-1) + 1 \geq c(n).$$

Rimane il caso in cui $n > 17$ ha tre cifre nella rappresentazione in base 3; allora $18 \leq n \leq 26$, e la dieseguaglianza $c(n) < n$ si verifica direttamente.

PROBLEMA 54. Sia $2 \leq b \in \mathbb{N}$ e siano $x, y \in \{0, \ldots, b-1\}$, non entrambi nulli. Sia N il numero rappresentato in base b dalla scrittura $xyxy$,

$$N = xb^3 + yb^2 + xb + y = (b^2 + 1)(xb + y).$$

Se N è il cubo di un numero naturale, allora $b^2 + 1$ deve essere un multiplo del quadrato di un numero intero positivo $\neq 1$.
Questa condizione non è soddisfatta da $b = 10$; infatti $10^2 + 1 = 101$ è un numero primo; quindi in base dieci nessun cubo è rappresentato da una scrittura del tipo $xyxy$.
Il più piccolo intero positivo b tale che b^2+1 è diviso da un quadrato diverso da 1 è 7: si ha $7^2 + 1 = 50 = 2 \cdot 5^2$. Per completare $2 \cdot 5^2$ a un cubo si moltiplica per il fattore $2^2 \cdot 5 = 20$ che è minore di 7^2, e dunque si scrive in base 7 in due cifre $20 = 2 \cdot 7 + 6$. Quindi $x = 2$ e $y = 6$; verificando,

$$2 \cdot 7^3 + 6 \cdot 7^2 + 2 \cdot 7 + 6 = 50 \cdot 20 = 1000 = 10^3.$$

La risposta alla seconda domanda è quindi $b = 7$.
[Il successivo intero b tale che $b^2 + 1$ è diviso da un quadrato $\neq 1$ è $b = 18$, che però non va bene; infatti, $18^2 + 1 = 5^2 \cdot 13$ e per completare il cubo occorre moltiplicare per $5 \cdot 13^2$ che in base 18 è un numero di tre cifre. Con un po' di conti, si trova che il primo $b > 7$ tale che un cubo intero si rappresenta in base b con $xyxy$ è $b = 57$.]

PROBLEMA 55. Siano x, b interi positivi con $b \geq 2$ e $2x^2 < b$; allora il numero

$$N^2 := x^2(b+1)^2 = x^2b^2 + 2x^2b + x^2$$

è tale che la sua scrittura in base b è un palindromo di tre cifre: $x^2(2x^2)x^2$. Il problema si risolve quindi trovando un intero positivo N che abbia un numero sufficientemente grande di divisori x con

$$2x^2 < \frac{N}{x} - 1. \qquad (*)$$

Questo si può fare in tanti modi. Ad esempio, fissato $k \geq 1$, sia $N = 2^{2k}$; allora tutti i numeri $x = 2^t$ con $0 \leq t \leq k-1$ sono divisori di N che soddisfano la condizione $(*)$; quindi il numero $N^2 = 2^{4k}$ è rappresentato da una scrittura palindroma di tre cifre in ogni base

$$b = \frac{N}{x} - 1 = 2^{2k-t} - 1$$

con $0 \leq t \leq k-1$. Per rispondere alla domanda posta dal problema, il numero $2^{4(2002)}$ ha una rappresentazione palindroma di tre cifre in almeno 2002 basi diverse.

PROBLEMA 56. Posto X l'insieme di tutti i numeri interi positivi la cui rappresentazione binaria contiene esattamente tre cifre 1, la funzione $f : \mathbb{N}^* \to \mathbb{N}$ del quesito è definita da,

$$f(k) = |X \cap \{k+1, \ldots, 2k\}|$$

per ogni $k \in \mathbb{N}^*$. Ad esempio, per $n \geq 1$,

$$f(2^n) = \binom{n+1}{3} - \binom{n}{3} = \frac{n(n-1)}{2}.$$

Ora, $\{k+2, \ldots, 2k+2\} \setminus \{k+1, \ldots, 2k\} = \{2k+1, 2k+2\}$; poiché il numero di cifre 1 nella rappresentazione binaria di $k+1$ è lo stesso che in quella di $2k+2 = 2(k+1)$, si deduce che

$$f(k+1) - f(k) = \begin{cases} 1 \text{ se } 2k+1 \in X \\ 0 \text{ se } 2k+1 \notin X \end{cases} \qquad (*)$$

Quindi, la funzione f è crescente per differenze di al più una unità; inoltre, f è illimitata (vedi esempio di sopra) e $f(4) = 1$. Si conclude che f è suriettiva, e questo risponde alla prima questione.

(b) Sia $m \in \mathbb{N}^*$ tale che $f(k) = m$ per un unico $k \in \mathbb{N}^*$. Poiché la funzione f è crescente questo è equivalente a

$$f(k-1) < f(k) < f(k+1)$$

(poiché $f(1) = f(2) = 0$, possiamo assumere $k \geq 3$), che a sua volta, per $(*)$, è equivalente a

$$2k-1, 2k+1 \in X.$$

Poiché l'ultima cifra nella rappresentazione binaria di $2k$ è 0, mentre quella di $2k+1$ è 1, da $2k+1 \in X$ segue che la rappresentazione binaria di $2k$ ha solo due cifre 1, quindi $2k = 2^{s+1} + 2^t$ con $s \geq t \geq 1$.
Poiché la rappresentazione binaria di $2^t - 1$ è un sequenza di t cifre uguali a 1, da

$$2k - 1 = 2^s + 2^t - 1 \in X$$

segue quindi $t = 2$. Pertanto $k = 2^s + 2$, con $s > 1$.

Viceversa, se $k = 2^s + 2$ con $s > 1$ allora $2k - 1, 2k + 1 \in X$. Per concludere la risposta resta da valutare il valore assunto da f in tali interi. Poiché $2^s + 1, 2^s + 2, 2^{s+1} + 1, 2^{s+1} + 2$ non appartengono a X mentre $2^{s+1} + 3 = 2k - 1 \in X$, si ha

$$f(k) = f(2^s + 2) = f(2^s) + 1 = \frac{s(s-1)}{2} + 1.$$

In conclusione esiste un unico k tale che $f(k) = m$ se e solo se $m = 1 + \binom{s}{2}$ con $s \geq 2$.

2

Un po' di funzioni

In questo capitolo introduciamo due funzioni, la *parte intera* di un numero reale e la *valutazione p-adica* di un intero (con p un primo fissato), che pur essendo molto semplici nella definizione e nelle loro proprietà di base, costituiscono, come vedremo nei prossimi capitoli, degli strumenti molto utili in teoria dei Numeri.
L'ultima sezione del capitolo è invece un'antologia di un tipo specifico di problemi, nei quali si chiede di determinare funzioni con date proprietà, che si incontra molto di frequente nelle competizioni matematiche.

2.1. Parte intera

Dato un numero reale x, esiste un unico numero intero n tale che $n \leq x < n+1$; tale intero n è chiamato la *parte intera* di x e si denota con $\lfloor x \rfloor$. Questo definisce una funzione (detta appunto *parte intera*) $\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z}$.
Si ha, ad esempio, $\lfloor \pi \rfloor = 3, \lfloor -5,61 \rfloor = -6$, $\lfloor 34/5 \rfloor = 6$; in generale se $a, n \in \mathbb{Z}$ e $n > 0$, la parte intera $\lfloor a/n \rfloor$ è il quoziente della divisione euclidea di a per n:

$$a = \left\lfloor \frac{a}{n} \right\rfloor \cdot n + r$$

con $0 \leq r < n$. Altre semplici proprietà della parte intera, da dimostrare per esercizio, sono le seguenti.

Lemma 2.1. (1) *Per ogni* $x, y \in \mathbb{R}$, $\lfloor x+y \rfloor - 1 \leq \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor$*;*

(2) *per ogni* $x \in \mathbb{R}$ *e* $n \in \mathbb{Z}$*:* $\lfloor x+n \rfloor = \lfloor x \rfloor + n$*;*

(3) *per ogni* $x \in \mathbb{R} \setminus \mathbb{Z}$*:* $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$*;*

(4) *per ogni* $x \in \mathbb{R}$ *e* $n \in \mathbb{N}^*$*:* $\lfloor \lfloor x \rfloor / n \rfloor = \lfloor x/n \rfloor$.

Per $x \in \mathbb{R}$ il numero $x - \lfloor x \rfloor$ (che chiaramente appartiene all'intervallo reale $[0,1)$ si chiama *parte frazionale* di x e in genere si denota con $\{x\}$.

Esercizio 2.1. Si dimostri il Lemma 2.1.

Esercizio 2.2. Siano $x.y \in \mathbb{R}$; si discuta in quali casi si ha $\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor$.

Un'identità classica è data dalla seguente proposizione.

Teorema 2.2 (C. Hermite[1])**.** *Siano x un numero reale e n un intero positivo; allora*

$$\lfloor nx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor.$$

Dimostrazione. (Matsuoka [4]) Fissato n intero positivo, per ogni $x \in \mathbb{R}$ poniamo

$$f(x) = \lfloor nx \rfloor - \lfloor x \rfloor - \left\lfloor x + \frac{1}{n} \right\rfloor - \left\lfloor x + \frac{2}{n} \right\rfloor - \cdots - \left\lfloor x + \frac{n-1}{n} \right\rfloor.$$

Osserviamo che $f(y) = 0$ se $0 \leq y < \frac{1}{n}$. Inoltre

$$\begin{aligned} f\left(x + \frac{1}{n}\right) &= \lfloor nx + 1 \rfloor - \left\lfloor x + \frac{1}{n} \right\rfloor - \left\lfloor x + \frac{2}{n} \right\rfloor - \cdots - \left\lfloor x + \frac{n-1}{n} \right\rfloor - \lfloor x + 1 \rfloor = \\ &= \lfloor nx \rfloor + 1 - \left\lfloor x + \frac{1}{n} \right\rfloor - \left\lfloor x + \frac{2}{n} \right\rfloor - \cdots - \left\lfloor x + \frac{n-1}{n} \right\rfloor - \lfloor x \rfloor - 1 = \\ &= f(x). \end{aligned}$$

Dunque $f(x)$ è costante su $x + \frac{1}{n}\mathbb{Z} = \{x + z\frac{1}{n} \mid z \in \mathbb{Z}\}$; ora, esiste $y \in x + \frac{1}{n}\mathbb{Z}$ tale che $0 \leq y < 1/n$, e quindi

$$f(x) = f(y) = 0$$

che è quello che si voleva. □

Esempio 1. *Determinare per quali numeri reali $x \geq 0$ si ha*

$$\left\lfloor \frac{x}{13} \right\rfloor = \left\lfloor \frac{x}{14} \right\rfloor.$$

Soluzione. La risposta è

$$x \in \bigcup_{k=0}^{12} [14k, 13k + 13).$$

Infatti, sia $0 \leq k \leq 12$ e $14k \leq x < 13k + 13$; allora

$$k \leq \frac{x}{14} \leq \frac{x}{13} < k + 1, \tag{2.1}$$

e dunque $k = \lfloor x/14 \rfloor = \lfloor x/13 \rfloor$. Viceversa, sia $x \geq 0$ tale che $\lfloor x/14 \rfloor = \lfloor x/13 \rfloor = k$; allora, sussistono le diseguaglianze come in (2.1), per cui

$$14k \leq x < 13k + 13$$

ed anche, necessariamente, $0 \leq k \leq 12$. ∎

[1] Charles Hermite (1822-1901), matematico francese che ha fornito contributi importanti in diverse aree della matematica.

ESEMPIO 2.(S. Ramanujan[2]) *Si provi che per ogni intero positivo n si ha*

$$\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{4n+2} \rfloor.$$

SOLUZIONE. Posto $a = \sqrt{n} + \sqrt{n+1}$, si ha $a^2 = 2n + 1 + 2\sqrt{n(n+1)}$, dunque

$$4n + 1 < a^2 < 4n + 3.$$

Ora, né $4n+2$ né $4n+3$ sono quadrati interi, dato che un quadrato intero è congruo a 0 o 1 modulo 4. Dunque nessun numero intero è compreso tra $\sqrt{4n+2}$ ed $\sqrt{4n+3}$, quindi

$$\lfloor \sqrt{4n+3} \rfloor = \lfloor \sqrt{4n+2} \rfloor \leq \sqrt{4n+1} < a < \sqrt{4n+3},$$

da cui l'enunciato. ■

ESEMPIO 3. *Si provi che per ogni intero positivo n, il numero intero*

$$\lfloor (2+\sqrt{3})^n \rfloor$$

è dispari.

SOLUZIONE. Sia n un intero positivo; sviluppando le potenze n-esime si trova

$$\begin{aligned} u := (2+\sqrt{3})^n + (2-\sqrt{3})^n &= \sum_{i=0}^{n} 2^{n-i}(\sqrt{3})^i + \sum_{i=0}^{n} 2^{n-i}(-1)^i(\sqrt{3})^i = \\ &= 2 \cdot \sum_{j=0}^{\lfloor n/2 \rfloor} 2^{n-2j} 3^j \in 2\mathbb{N} \end{aligned}$$

D'altra parte, $0 < (2-\sqrt{3})^n < 1$, e dunque $\lfloor (2+\sqrt{3})^n \rfloor = u - 1$, che è un numero dispari. ■

Problemi

Come già si capisce dagli esempi di sopra, solo a partire dalla definizione e dalle sue immediate conseguenze (Lemma 2.1) è possibile produrre problemi elementari ma non banali; ed infatti la parte intera occorre con una certa frequenza nei quesiti delle competizioni matematiche.

Problema 57 (Canada, 1998)**.** *Determinare il numero di soluzioni reali x di*

$$\left\lfloor \frac{x}{2} \right\rfloor + \left\lfloor \frac{x}{3} \right\rfloor + \left\lfloor \frac{x}{5} \right\rfloor = x.$$

SOLUZIONE. Poiché $\lfloor x/2 \rfloor, \lfloor x/3 \rfloor, \lfloor x/5 \rfloor$ sono interi, anche x è un numero intero. Consideriamo allora la divisione euclidea di x per 30: $x = 30q + r$ con $0 \leq r \leq 29$. Allora

$$x = \left\lfloor \frac{x}{2} \right\rfloor + \left\lfloor \frac{x}{3} \right\rfloor + \left\lfloor \frac{x}{5} \right\rfloor = 15q + \left\lfloor \frac{r}{2} \right\rfloor + 10q + \left\lfloor \frac{r}{3} \right\rfloor + 6q + \left\lfloor \frac{r}{5} \right\rfloor,$$

[2]Srinivasa Ramanujan (1887-1920), matematico indiano, in particolare scopritore di migliaia di identità in analisi e in teoria dei numeri.

quindi

$$30q + r = x = 31q + f(r),$$

dove $f(r) = \lfloor r/2 \rfloor + \lfloor r/3 + \lfloor r/5 \rfloor$. Dunque $q = r - f(r)$ e, in conclusione,

$$x = 30q + r = 31r - 30f(r)$$

al variare di $r \in \mathbb{N}$, $0 \leq r \leq 29$. Vi sono pertanto 30 soluzioni. ∎

Problema 58 (Gauss)**.** *Siano p, q interi positivi coprimi, con p dispari. Provare che*

$$\sum_{k=1}^{p-1} \left\lfloor \frac{kq}{p} \right\rfloor = \frac{(p-1)(q-1)}{2}.$$

Soluzione. Osserviamo che per ogni $1 \leq k \leq p-1$, p non divide kq, dato che p, q sono coprimi e $k < p$; dunque

$$\frac{kq}{p} - 1 < \left\lfloor \frac{kq}{p} \right\rfloor < \frac{kq}{p}.$$

Sia $1 \leq k \leq (p-1)/2$, allora

$$q - 2 < \left\lfloor \frac{kq}{p} \right\rfloor + \left\lfloor \frac{(p-k)q}{p} \right\rfloor < q,$$

dunque

$$\left\lfloor \frac{kq}{p} \right\rfloor + \left\lfloor \frac{(p-k)q}{p} \right\rfloor = q - 1.$$

Quindi,

$$\sum_{k=1}^{p-1} \left\lfloor \frac{kq}{p} \right\rfloor = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor + \left\lfloor \frac{(p-k)q}{p} \right\rfloor = \frac{p-1}{2} \cdot (q-1),$$

come si voleva. ∎

* * *

• Ora i problemi da risolvere (le soluzioni nella sezione 2.4).

Problema 59 (Romania, 2003)**.** *Provare che per ogni intero positivo n si ha*

$$\sqrt{4n^2 + n} - \lfloor \sqrt{4n^2 + n} \rfloor < 1/4.$$

Problema 60 (Baltic Way 2015)**.** *Per ogni intero $n \geq 2$ denotiamo con $P(n)$ il più grande divisore primo di n. Trovare tutti gli interi $n \geq 2$ tali che*

$$P(n) + \lfloor \sqrt{n} \rfloor = P(n+1) + \lfloor \sqrt{n+1} \rfloor$$

Problema 61 (Italia 1998)**.** *Calcolare il valore della seguente somma:*

$$\sum_{k=1}^{10.000} \lfloor \sqrt{k} \rfloor.$$

Problema 62 (Iberoamericana, 1997). *Sia $x \geq 1$ un numero reale che soddisfa la seguente proprietà: per ogni coppia di interi positivi n, m, con n multiplo di m, si ha che $\lfloor nx \rfloor$ è un multiplo di $\lfloor mx \rfloor$. Si dimostri che x è un numero intero.*

Problema 63 (IMO, Mosca 1968). *Sia n un intero positivo. Provare che*

$$n = \sum_{i=1}^{\infty} \left\lfloor \frac{n + 2^{i-1}}{2^i} \right\rfloor.$$

Problema 64 (Putnam, 1983). *Sia n un intero positivo e $f(n) = n + \lfloor \sqrt{n} \rfloor$: si provi che la sequenza*

$$n, f(n), f^2(n), f^3(n), \ldots$$

contiene almeno un quadrato (intero).

Problema 65 (AMM, D. Doster). *Si provi che per ogni primo $p \geq 2$,*

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^3}{p} \right\rfloor = \frac{(p+1)(p-1)(p-2)}{4}.$$

Il prossimo problema è strettamente collegato al Problema di Frobenius che abbiamo descritto nel precedente capitolo (sezione 1.5).

Problema 66 (Sylvester). *Siano p, q interi positivi coprimi; provare che il numero di interi positivi non rappresentabili com $ap + bq$ con a, b interi non negativi è*

$$h(p, q) = \frac{1}{2}(p-1)(q-1).$$

Suggerimenti. I Problemi 59 e 60 che, come alcuni degli esempi fatti sopra, riguardano la parte intera delle radici, sono tutto sommato facili. Per il primo si può iniziare con l'osservazione, quasi banale, che $2n = \lfloor \sqrt{4n^2 + n} \rfloor \ldots$; per il secondo basta fare attenzione a quello che la questione richiede.

Anche il Problema 61 è abbastanza semplice nell'impostazione; per la soluzione può essere utile ricordare la seguente identità, valida per ogni intero $n \geq 1$,

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \tag{2.2}$$

Questa identità, che si dimostra facilmente per induzione, sarà utile anche nel Problema 65.

Il punto del Problema 62 è intuire la giusta impostazione: una è la seguente. Sia $x \geq 1$ un numero reale non intero; allora esiste un numero naturale (primo) $p \geq 2$ tale che px non è un intero; quindi $0 < px - \lfloor px \rfloor < 1$ e dunque esiste un intero positivo m tale che

$$\frac{1}{2m} < px - \lfloor px \rfloor < \frac{1}{m}.$$

Da ciò segue, con semplici argomenti, $\lfloor mpx \rfloor = m\lfloor px \rfloor$ e $\lfloor 2mpx \rfloor = 2m\lfloor px \rfloor + 1 \ldots$

Quanto al Problema 63, si parta dall'identità di Hermite nel caso $n = 2$.

Per il Problema 64, fare induzione sul numero intero $n - \lfloor \sqrt{n} \rfloor^2$, applicando una o due volte la funzione f per il passo induttivo.

Problema 65: accoppiare opportunamente gli addendi della sommatoria.

Problema 66: ricordarsi della dimostrazione del Teorema 1.22 ed applicare la formula di Gauss (problema 58).

2.2. Valutazioni p-adiche

Sia p un numero primo fissato. Per ogni numero intero $z \neq 0$ La *valutazione p-adica* di z è il massimo intero $\nu_p(z)$ (maggiore o uguale a zero) tale che $p^{\nu_p(z)}$ divide z. Si pone inoltre, per qualsiasi primo p, $\nu_p(0) = \infty$.
Si osserva quindi che se n è un intero positivo, allora

$$n = \prod_{p \leq n} p^{\nu_p(n)}$$

è la decomposizione di n come prodotto di potenze di primi distinti. Dal Teorema fondamentale dell'Aritmetica segue che, dati due numeri interi n, m, si ha $n \mid m$ se e solo se $\nu_p(n) \leq \nu_p(m)$ per ogni primo p.
Dalla definizione si ricavano facilmente le seguenti prime proprietà delle valutazioni p-adiche:

Lemma 2.3. *Sia p un primo positivo; per ogni $a, b \in \mathbb{Z}$, si ha*

(i) $\nu_p(ab) = \nu_p(a) + \nu_p(b)$;

(ii) $\nu(a + b) \geq \min(\nu_p(a), \nu_p(b))$ *e vale l'uguaglianza se* $\nu_p(b) \neq \nu_p(a)$.

Molto importante è poi la formula seguente.

Teorema 2.4. *Sia $n \geq 2$, e sia p un numero primo (minore od uguale a n). Allora*

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

(Osserviamo che la sommatoria del membro di destra è di fatto una somma finita; infatti se $i > [\log_p n]$ allora $[n/p^i] = 0$.)

Dimostrazione. Sia $n \in \mathbb{N}^*$ e p un numero primo. Denotiamo con $I = \{1, 2, \ldots, [\log_p n]\}$ l'insieme dei numeri naturali compresi tra 1 e $[\log_p n]$, poniamo $T = \{1, 2, \ldots, n\}$, e consideriamo l'insieme delle coppie,

$$S = \{\ (i, m) \in I \times T \mid p^i \text{ divide } m\ \} .$$

Sia $i \in I$; allora il numero di elementi di S che hanno i come prima componente è uguale al numero di interi minori o uguali ad n che sono multipli di p^i, cioè $[n/p^i]$. Dunque, il numero di elementi di S (che si può ottenere sommando, per ogni $i \in I$ il numero di coppie di cui essa è la prima componente) è

$$|S| = \sum_{i=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

Viceversa, fissato un $m \in T$, il numero di elementi di S che hanno m come seconda componente è il numero di potenze di p che dividono m, cioè $\nu_p(m)$; quindi

$$|S| = \sum_{m=1}^{n} \nu_p(m) \ .$$

Poichè, per l'osservazione fatta sopra,

$$\sum_{m=1}^{n} \nu_p(m) = \nu_p \left(\prod_{m=1}^{n} m \right) = \nu_p(n!)$$

dal confronto delle due espressioni di $|S|$ si ottiene l'enunciato. □

Corollario 2.5 (Legendre)**.** *Siano n un intero positivo e p un primo positivo; allora*

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}$$

dove $s_p(n)$ è la somma delle cifre della rappresentazione in base p di n.

Dimostrazione. Sia $t = \lfloor \log_p n \rfloor$ e sia $n = a_t p^t + \ldots + a_1 p + a_0$ la rappresentazione di n in base p, dove $0 \le a_i \le p-1$ per ogni $0 \le i \le t$, e $a_t \neq 0$. Allora, per ogni $0 \le i \le t$,

$$\left\lfloor \frac{n}{p^i} \right\rfloor = a_t p^{t-i} + \ldots + a_{i+1} p + a_i$$

quindi, con qualche considerazione sulla doppia sommatoria,

$$\sum_{i=1}^{t} \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=1}^{t} \Big(\sum_{j=0}^{t-i} a_{i+j} p^j \Big) = \sum_{k=0}^{t} a_k \Big(\sum_{j=0}^{k-1} p^j \Big) = \sum_{k=1}^{t} a_k \frac{p^k - 1}{p-1}.$$

Quindi, per il Teorema 2.4,

$$(p=1)\nu_p(n!) = \sum_{k=0}^{t} a_k (p^k - 1) = \sum_{k=0}^{t} a_k p^k - \sum_{k=0}^{t} a_k = n - s_p(n),$$

da cui l'identità nell'enunciato. □

Un caso interessante di applicazione di questi risultati, che ricorrerà spesso in un prossimo capitolo (intanto si veda l'esempio 6 qui di seguito), riguarda la valutazione dei coefficienti binomiali; infatti per ogni coppia di interi positivi $1 \leq k \leq n$, ed ogni primo p,

$$\nu_p\left[\binom{n}{k}\right] = \nu_p(n!) - \nu_p(k!) - \nu_p((n-k)!). \tag{2.3}$$

Esercizio 2.3. Siano p, m interi positivi con p primo. Calcolare $v_p((p^m)!)$.

Esempio 4. *Siano n un intero positivo e p un primo positivo. Provare che $p^{n-1} \mid n!$ se e solo $p = 2$ e n è una potenza di 2.*

Infatti, $p^{n-1} \mid n!$ se e solo $\nu_p(n!) \geq n-1$. Sia $s - s_p(n)$ la somma delle cifre nella rappresentazione di n in base p. Per il Corollario 2.5

$$\nu_p(n!) = \frac{n-s}{p-1}$$

e quindi $n - 1 \leq \nu_p(n!)$ se e solo se $s = 1$ (quindi n è una potenza di p) e $p - 1 = 1$ (quindi $p = 2$). ■

Esempio 5. *Dire con quanti zeri termina la scrittura decimale di* 1005!.

Si tratta di trovare il massimo $n \in \mathbb{N}$ tale che 10^n divide 1005!; qualche secondo di riflessione porta a concludere che

$$n = \min\{\nu_2(1005!), \nu_5(1005!)\}$$

Per il Teorema 2.4:

$$\nu_2(1005!) = \lfloor 1005/2 \rfloor + \lfloor 1005/4 \rfloor + \ldots + \lfloor 1005/512 \rfloor = 502 + 251 + \ldots + 3 + 1 = 997;$$

$$\nu_5(1005!) = \lfloor 1005/5 \rfloor + \lfloor 1005/25 \rfloor + \lfloor 1005/125 \rfloor + \lfloor 1005/625 \rfloor = 201 + 40 + 8 + 1 = 250.$$

Dunque la rappresentazione decimale di 1005! termina con $n = 250$ zeri. ■

Un'utile formula. Il prossimo è un risultato molto utile; nei testi in inglese è chiamato *"Lifting the exponent Lemma"*.

Teorema 2.6. *Sia p un primo positivo dispari e siano x, y numeri interi entrambi non divisibili per p, e tali che $\nu_p(x-y) \geq 1$. Allora per ogni intero $n \geq 0$,*

$$\nu_p(x^n - y^n) = \nu_p(x-y) + \nu_p(n).$$

Dimostrazione. Siano p, x, y, n come nelle ipotesi. Allora $x \equiv y \pmod{p}$; possiamo inoltre chiaramente supporre inoltre $x > y$.
Iniziamo con il caso $n = p$; ponendo $v = \nu_p(x-y)$ possiamo scrivere

$$x = y + p^v b$$

con $v \geq 1$, $b \in \mathbb{N}^*$ e p non divide b. Dunque

$$x^p - y^p = x^p - (x + p^v b)^p = p \cdot x^{p-1} p^v b + \binom{p}{2} x^{p-2} p^{2v} b^b + \cdots + p^{pv} b^p.$$

Ricordando che per ogni $1 \leq i \leq p-1$ il coefficiente binomiale $\binom{p}{i}$ è un multiplo di p (e che $p \geq 3$ per ipotesi), si osserva che p^{v+2} divide ogni addendo

$$\binom{p}{i} x^{p-1} p^{iv} b^i$$

per $2 \leq i \leq p$; mentre $\nu_p(p \cdot x^{p-1} p^v b) = \nu_p(p^{v+1} x^{p-1} b) = v + 1$. Dunque, per il punto (ii) del Lemma 2.3,

$$\nu_p(x^p - y^p) = \nu_p\Big(p^{v+1} x^{p-1} b + \sum_2^p \binom{p}{i} x^{p-i} p^{iv} b^i\Big) = \nu_p(p^{v+1} x^{p-1} b) = v + 1, \qquad (2.4)$$

come si voleva.
Procediamo ora alla dimostrazione del lemma per induzione su $k = \nu_p(n)$. Se $k = 0$, allora $p \not| n$, dunque $p \not| n x^{n-1}$ e dall'identità

$$\frac{x^n - y^n}{x - y} = x^{n-1} + x^{n-2} y + \ldots x y^{n-2} + y^{n-1} \equiv n x^{n-1} \pmod{p}$$

segue l'uguaglianza voluta:

$$\nu_p(x^n - y^n) = \nu_p(x - y).$$

Sia ora $\nu_p(n) \geq 1$ ed assumiamo l'ipotesi induttiva. Sia $m = n/p$, che è un intero positivo e $\nu_p(m) = k - 1$. Per ipotesi induttiva,

$$\nu_p(x^m - y^m) = \nu_p(x - y) + k - 1;$$

dunque, per la (2.4)

$$\nu_p(x^n - y^n) = \nu_p((x^m)^p - (y^m)^p) = \nu_p(x^m - y^m) + 1 = \nu_p(x - y) + k,$$

e la dimostrazione è completa. □

Corollario 2.7. *Sia p un primo positivo dispari e siano x, y numeri interi entrambi non divisibili per p, e tali che $\nu_p(x + y) \geq 1$. Allora per ogni intero positivo dispari n,*

$$\nu_p(x^n + y^n) = \nu_p(x + y) + \nu_p(n).$$

Dimostrazione. Basta osservare che se n è intero dispari, allora $x^n + y^n = x^n - (-y)^n$, quindi applicare il Teorema 2.6. □

Osserviamo che per $p = 2$ il Teorema 2.6, com'è, non vale: se $m \geq 2$, $x = 2^m - 1$ e $y = 1$, allora $\nu_2(x - y) = 1$, mentre

$$\nu_2(x^2 - y^2) = \nu_2(x - y) + \nu_2(x + y) = 1 + \nu_2(2^m) = m + 1.$$

Riferiamo, lasciando la dimostrazione per esercizio, cosa si può dire in questo caso.

Teorema 2.8. *Siano x, y interi dispari tali che $4 \mid x - y$, allora*

$$\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(n)$$

per ogni intero positivo n.

Esercizio 2.4. Trovare il minimo intero positivo n tale che

$$3^{1001} \mid 19^n - 1.$$

ESEMPIO 6. *Siano x, y, n interi positivi, con $x \neq y$ ed n dispari, tali che n divide $x^n - y^n$; provare che n divide $\frac{x^n - y^n}{x - y}$.*

Se $n = 1$ la cosa è ovvia; assumiamo quindi $n \geq 2$. Sia p un divisore primo di n. Se p non divide $x - y$ allora, poiché $n \mid x^n - y^n$,

$$p^{\nu_p(n)} \Big| \frac{x^n - y^n}{x - y}.$$

Se $p \mid x - y$ allora, per il Teorema 2.6,

$$\nu_p(x^n - y^n) - \nu_p(x - y) = \nu_p(n)$$

e quindi $p^{\nu_p(n)}$ divide $\frac{x^n - y^n}{x - y}$. Poiché $n = \prod_{p|n} p^{\nu_p(n)}$, si conclude.

NOTA: Non è difficile provare che la stessa conclusione dell'esempio vale se n è pari.

Problemi

I problemi svolti riguardano: uno la valutazione p-adica dei fattoriali, due (e sono tra i miei preferiti) l'applicazione delle formule di sollevamento.

Problema 67 (IMO, Torùn 1972)**.** *Provare che $(2m)!(2n)!$ è un multiplo di $m!n!(m+n)!$ per ogni coppia di interi positivi m, n.*

SOLUZIONE. Siano $m, n \in \mathbb{N}^*$, e sia p un numero primo. Allora

$$\nu_p(m!n!(m+n)!) = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor + \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor + \sum_{i=1}^{\infty} \left\lfloor \frac{m+n}{p^i} \right\rfloor,$$

mentre,

$$\nu_p((2m)!(2n)!) = \sum_{i=1}^{\infty} \left\lfloor \frac{2m}{p^i} \right\rfloor + \sum_{i=1}^{\infty} \left\lfloor \frac{2n}{p^i} \right\rfloor.$$

Osserviamo quanto segue. Siani a, numeri reali positivi. Se $\lfloor a + b \rfloor = \lfloor a \rfloor + \lfloor b \rfloor$, allora

$$\lfloor 2a \rfloor + \lfloor 2b \rfloor \geq 2\lfloor a \rfloor + 2\lfloor b \rfloor = \lfloor a + b \rfloor + \lfloor a \rfloor + \lfloor b \rfloor.$$

Se invece $\lfloor a + b \rfloor > \lfloor a \rfloor + \lfloor b \rfloor$, allora

$$1 \leq (a - \lfloor a \rfloor) + (b - \lfloor b \rfloor)$$

e quindi $2 \leq (2a - 2\lfloor a \rfloor) + (2b - 2\lfloor b \rfloor)$. Dal Lemma 2.1 segue

$$\lfloor 2a \rfloor - 2\lfloor a \rfloor + \lfloor 2b \rfloor - 2\lfloor b \rfloor = \lfloor 2a - 2\lfloor a \rfloor \rfloor + \lfloor 2b - 2\lfloor b \rfloor \rfloor \geq 1,$$

e poiché $1 = \lfloor a + b \rfloor - \lfloor a \rfloor - \lfloor b \rfloor$, si ha ancora

$$\lfloor 2a \rfloor + \lfloor 2b \rfloor \geq \lfloor a + b \rfloor + \lfloor a \rfloor + \lfloor b \rfloor.$$

Tornando quindi al nostro problema, per ogni $i \geq 1$,

$$\left\lfloor \frac{2m}{p^i} \right\rfloor + \left\lfloor \frac{2n}{p^i} \right\rfloor \geq \left\lfloor \frac{m+n}{p^i} \right\rfloor + \left\lfloor \frac{m}{p^i} \right\rfloor + \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Dunque, per quanto detto all'inizio,

$$\nu_p((2m)!(2n)!) \geq \nu_p(m!n!(m+n)!)$$

per ogni primo p, e quindi $m!n!(m+n)!$ divide $(2m)!(2n)!$ ■

Problema 68 (IMO, Pechino 1990). *Trovare tutti gli interi positivi n tali che*

$$\frac{2^n + 1}{n^2}$$

è un numero intero.

SOLUZIONE. Una soluzione è senz'altro $n = 1$. Supponiamo quindi $n \geq 2$ sia un'altra soluzione, ed osserviamo che, poiché $2^n + 1$ è dispari, n deve essere dispari.
Sia p il minimo divisore primo di n. Allora p divide $2^n + 1$ e dunque p divide $2^{2n-1} - 1$; d'altra parte p divide $2^{p-1} - 1$ per il teorema di Fermat, quindi (vedi Proposizione 1.11) p divide $2^r - 1$ dove $r = MCD(p-1, 2n)$. Dalla minimalità di p tra i divisori primi di n si deduce $r = 2$; qjuindi $p \mid 2^2 - 1$ e pertanto $p = 3$.
Ora, affinché $\frac{2^n+1}{n^2}$ sia un numero intero, si deve avere $\nu_3(2^n + 1) \geq \nu_3(n^2)$, quindi, per il Corollario 2.7,

$$2\nu_3(n) = \nu_3(n^2) \leq \nu_3(2^n + 1) = \nu_3(2 + 1) + \nu_3(n) = 1 + \nu_3(n),$$

da cui $\nu_3(n) = 1$. Pertanto $n = 3m$ con m un numero dispari non diviso da 3. Se $m = 1$ si ha $n = 3$, che è una soluzione (infatti $2^3 + 1 = 9 = 3^2$). Supponiamo $m > 1$ e sia q il minimo divisore primo di m. Osserviamo che $q \neq 7$; infatti $2^n + 1 = 8^m + 1 \equiv 2 \pmod 7$ e dunque 7 non può dividere n^2. D'altra parte, ragionando come fatto per p, si trova che q divide $8^{2m} - 1$ e $8^{q-1} - 1$; quindi q divide $8^s - 1$ dove $s = MCD(2m, q-1) = 2$. Quindi

$$q \mid 8^2 - 1 = 63$$

e dunque, dato che $q \neq 3$, risulta $q = 7$, che è una contraddizione.
In conclusione, le soluzioni sono $n = 1, 3$. ■

Problema 69 (Italia 2014). *Per ogni intero positivo n, sia d_n il massimo comune divisore di tutti i numeri della forma $a^n + (a+1)^n + (a+2)^n$ al variare di $a \in \mathbb{N}^*$.*

(a) Dimostrare che per ogni n, $d_n = 3^k$ per qualche $k \in \mathbb{N}$.

(b) Dimostrare che per ogni $k \in \mathbb{N}$ esiste n tale che $d_n = 3^k$.

SOLUZIONE. (a) Sia $n \in \mathbb{N}^*$ e sia d_n il massimo comun divisore di tutti i numeri del tipo $a^n + (a+1)^n + (a+2)^n$ con $a \geq 1$. Sostituendo d_n e $d_n + 1$ per a si trova che d_n divide sia $d_n^n + (d_n+1)^n + (d_n+2)^n$ che $(d_n+1)^n + (d_n+2)^n + (d_n+3)^n$, dunque divide la loro differenza $(d_n+3)^n - d_n^3$, e quindi

$$d_n | (d_n+3)^n.$$

Se $d_n = 1 = 3^0$ siamo a posto. Altrimenti, sia p un divisore primo di d_n; allora p divide $(d_n+3)^n$ e quindi, essendo un primo, p divide $d_n + 3$. Dunque, $p = 3$, provando che d_n è una potenza di 3.

Per il punto (b) cominciamo osservando che, siccome d_2 è una potenza di 3 e $1^2+2^2+3^2 = 14$, di ha $d_2 = 1$, e il caso $k = 0$ è stabilito.
Supponiamo quindi $k \geq 1$, e proviamo che $d_{3^t} = 3^{t+1}$ per ogni $t \geq 0$.
Per $t = 0$ la cosa è banale. Sa quindi $t \geq 1$ e poniamo $b = 1^{3^t} + 2^{3^t} + 3^{3^t}$. Per il Corollario 2.7

$$\nu_3(1^{3^t} + 2^{3^t}) = t + 1.$$

Poiché certamente $t + 1 < 3^t$, per il punto (ii) del Lemma 2.3 si conclude che $\nu_3(b) = t + 1$. Quindi $d_{3^t} \leq 3^{t+1}$. Per provare che, viceversa, $d_{3^t} \geq 3^{t+1}$ (e quindi completare la dimostrazione), mostriamo per induzione su $a \geq 1$ che 3^{t+1} divide $a^{3^t} + (a+1)^{3^t} + (a+2)^{3^t}$ per ogni $a \in \mathbb{N}^*$. La cosa è stata verificata sopra per $a = 1$. Per $a \geq 1$, si ha che

$$(a+1)^{3^t} + (a+2)^{3^t} + (a+3)^{3^t} = a^{3^t} + (a+1)^{3^t} + (a+2)^{3^t} + [(a+3)^{3^t} - a^{3^t}].$$

Ora, $a^{3^t} + (a+1)^{3^t} + (a+2)^{3^t}$ è un multiplo di 3^{t+1} per ipotesi induttiva; mentre $(a+3)^{3^t} - a^{3^t}$ lo è per il Teorema 2.6 se a non è un multiplo di 3, e banalmente se 3 divide a. Quindi 3^{t+1} divide $(a+1)^{3^t} + (a+2)^{3^t} + (a+3)^{3^t}$; e, in conclusione, $d_{3^t} = 3^{t+1}$ per ogni $t \geq 0$. ∎

* * *

• Problemi da risolvere:

Problema 70 (AIME 1983)**.** *Trovare il massimo primo $p \leq 100$ che divide $\binom{200}{100}$.*

Problema 71 (Putnam, 2003)**.** *Si provi che per ogni intero positivo n vale*

$$n! = \prod_{i=1}^{n} mcm(1, 2, \ldots, \lfloor n/i \rfloor).$$

Problema 72 (U.S.A. 1975)**.** (a) *Si provi che, per ogni $x, y \in R$, $x, y \geq 0$,*

$$\lfloor 3x + y \rfloor + \lfloor 3y + x \rfloor + \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor 5x \rfloor + \lfloor 5y \rfloor.$$

(b) *Applicando* (a) *o in altro modo, si provi che per ogni coppia di interi positivi m, n,*

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

è un numero intero.

Problema 73 (Austria 2010). *Per ogni intero n poniamo $f(n) = \sum_{k=0}^{2010} n^k$. Provare che se m è un intero e $2 \leqslant m \leqslant 2010$, allora non esiste n tale che $f(n)$ è un multiplo di m.*

Problema 74 (Czech-Polish-Slovak MO, 1996). *Determinare tutte le coppie di interi positivi (m, n) tali che $p^m - n^p = 1$ con p un numero primo dispari.*

Problema 75 (Bulgaria, 1997). *Sia n un intero positivo tale che $3^n - 2^n$ è la potenza di un numero primo. Si provi che n è un numero primo.*

Problema 76 (Irlanda, 1996). *Siano p un numero primo e k, n interi positivi tali che*

$$2^p + 3^p = k^n.$$

Si provi che allora $n = 1$.

Problema 77 (Balkan MO 1993). *Siano p un numero primo e $m \geq 2$ un intero. Si provi che se l'identità*

$$\frac{x^p + y^p}{2} = \left(\frac{x+y}{2}\right)^m$$

è verificata per qualche coppia di interi positivi x, y, con $(x, y) \neq (1, 1)$, allora $p = m$.

2.3. Valori assoluti

In questa sezione deviamo temporaneamente dal percorso elementare ma insieme problematico tenuto fin qui, per trattare un argomento teorico che potreste considerare un poco più 'avanzato' rispetto a quanto fatto sinora. Questo argomento si sviluppa anche a partire dalla nozione di valutazione p-adica, vista nella sezione precedente, ma per il resto non avrà alcuna ricaduta nello svolgimento dei capitoli a seguire: dunque la lettura di questa sezione può essere saltata, o rinviata, senza compromettere la comprensione del resto.

DEFINIZIONE. Sia F un campo; una funzione $|\cdot| : F \to \mathbb{R}$ si dice un *valore assoluto* su F se soddisfa le seguenti proprietà:

(v1) $|x| \geq 0$ per ogni $x \in F$;

(v2) $|x| = 0$ se e solo se $x = 0$;

(v3) $|xy| = |x||y|$ per ogni $x, y \in F$;

(v4) $|x + y| \leq |x| + |y|$ per ogni $x, y \in F$.

La proprietà (v4) è detta *diseguaglianza triangolare*. Un valore assoluto $|\ |$ sul campo F si dice *non-archimedeo* se soddisfa la proprietà più forte:

(v4.1) $|x + y| \leq \max\{|x|, |y|\}$ per ogni $x, y \in F$.

Se tale proprietà non è soddisfatta il valore assoluto si dice *archimedeo*.

Dalle proprietà nella definizione, se $|\ | : F \to \mathbb{R}$ è un valore assoluto sul campo F, allora

i) $|1| = 1$. Infatti $|1||1| = |1 \cdot 1| = |1|$ da cui, poiché $|1| \neq 0$, segue l'asserto.

ii) $|-x| = |x|$ per ogni $x \in F$. Infatti, $|-x| \geq 0$ e $|-x|^2 = |(-x)(-x)| = |x|^2$.

iii) $|x^{-1}| = |x|^{-1}$ per ogni $0 \neq x \in F$. Infatti $|x^{-1}||x| = |x^{-1}x| = |1| = 1$.

• L'usuale valore assoluto su $\mathbb{R}$, o su $\mathbb{Q}$, che chiameremo valore assoluto *standard*, così come il modulo su $\mathbb{C}$, sono valori assoluti archimedei.

• Per ogni campo F, la funzione definita da $|x| = 0$ per ogni $0 \neq x \in F$, e $|0| = 0$, è un valore assoluto (non-archimedeo) detto valore assoluto *banale*.

Esercizio 2.5. Sia F un campo finito. Si provi che quello banale è l'unico valore assoluto definito su F.

Lemma 2.9. *Sia $|\ | : F \to \mathbb{R}$ un valore assoluto sul campo F e sia $P = \{z1_F \mid z \in \mathbb{Z}\}$ il sottoanello fondamentale di F. Sono equivalenti*

(i) $|\ |$ è non-archimedeo;

(ii) $|x| \leq 1$ per ogni $x \in P$.

(iii) esiste $0 > R \in \mathbb{R}$ tale che $|x| \leq R$ per ogni $x \in P$.

Dimostrazione. (i) $\Rightarrow$ (ii). Sia $|\ |$ non-archimedeo. Allora, per ogni $1 \leq n \in \mathbb{N}$,

$$|(-n)1_F| = |-n1_F| = |n1_F| = |1_F + \ldots + 1_F| \leq \max\{|1_F|, \ldots, |1_F|\} = 1,$$

e quindi la condizione (ii) è soddisfatta.

(ii) $\Rightarrow$ (i). Supponiamo $|n1_F| \leq 1$ pe ogni $n \in \mathbb{N}$. Allora per ogni $x \in F$ e $n \in \mathbb{N}$,

$$|nx| = |(n1_F)x| = |n1_F||x| \leq |x|.$$

Siano $x, y \in F$ e $M = \max\{|x|, |y|\}$; per ogni $1 \leq n \in \mathbb{N}$ si ha

$$|x+y|^n = |(x+y)^n| \leq \sum_{i=0}^{n} \left| \binom{n}{i} x^{n-i} y^i \right| \leq \sum_{i=0}^{n} \left| x^{n-i} y^i \right| \leq (n+1)M^n.$$

Quindi, per ogni $n \in \mathbb{N}$,

$$|x+y| \leq M \sqrt[n]{n+1}.$$

Poiché $\lim_{n\to\infty} \sqrt[n]{n+1} = 1$, si deduce $|x+y| \leq M$, provando che il valore assoluto $|\ |$ è non-archimedeo.

(ii) $\Leftrightarrow$ (iii). Se esiste $x \in P$ tale che $|x| > 1$, allora per ogni $R \in \mathbb{R}$ esiste un intero positivo n tale che $|x^n| = |x|^n > R$ (per $n \geq 0$, $x^n \in P$, poiché P è sottoanello di F); quindi (iii) $\Rightarrow$ (ii). Il viceversa è banale. □

Valore assoluto p-adico. Sia p un numero primo fissato. Ssi può estendere al campo $\mathbb{Q}$ dei razionali la valutazione p-adica ponendo, per ogni $q = \frac{m}{n}$, con $m, n \in \mathbb{Z}$ e $n \neq 0$,

$$\nu_p(q) = \nu_p(m/n) = \nu_p(m) - \nu_p(n),$$

che è una buona definizione, dato che chiaramente non dipende dai particolari rappresentanti m, n del numero razionale q.
Si definisce quindi il *valore assoluto p-adico* ponendo, per ogni $m, n \in \mathbb{Z}$, $n \neq 0$,

$$|m/n|_p = p^{-\nu_p(m/n)} = p^{\nu_p(n)-\nu_p(m)}.$$

Si verifica piuttosto agevolmente che per ogni primo p, il valore assoluto p-adico è un valore assoluto non-archimedeo su $\mathbb{Q}$.

Equivalenza. Valori assoluti $|\ |_1$ e $|\ |_2$ sul campo F si dicono *equivalenti* se, per ogni $x \in F$,

$$|x|_1 < 1 \iff |x|_2 < 1.$$

Per chi conosce un poco di topologia, diciamo qualcosa sulle ragioni di questa definizione. Sia $|\ | : F \to \mathbb{R}$ un valore assoluto sul campo F, allora ponendo, per ogni $(x, y) \in F \times F$,

$$d(x, y) = |x - y|$$

resta definita una distanza su F, e dunque una topologia su F, dedotta naturalmente dallo spazio metrico (F, d)), che si chiama la topologia associata la valore assoluto $|\ |$. Rispetto a tale topologia sono continue le funzioni di opposto (definita da F in F) $x \mapsto -x$, la funzione reciproco (definita da F^* in F^*) $x \mapsto x^{-1}$, e sono continue le funzioni (definite da $F \times F$ in F), somma $(x, y) \mapsto x + y$, e prodotto $(x, y) \mapsto xy$.
Non è difficile provare che due valori assoluti sul campo F sono equivalenti secondo la definizione data sopra se e solo se inducono la stessa topologia su F.

Veniamo al risultato principale di questa sezione.

Teorema 2.10 (Ostrowski[3])**.** *Sia $|\ |$ un valore assoluto non banale su $\mathbb{Q}$; allora $|\ |$ è equivalente al valore assoluto standard, oppure ad un valore assoluto p-adico per un qualche primo p.*

Dimostrazione. (1) Supponiamo che esista $1 < n \in \mathbb{N}$ tale che $|n| \leq 1$, e poniamo $N = \max\{|0|, |1|, \ldots, |n-1|\}$. Sia $m \in \mathbb{N}^*$, rappresentato in base n,

$$m = a_r n^r + \ldots a_1 n + a_0,$$

con $r = \left\lfloor \frac{\log m}{\log n} \right\rfloor$, $0 \leq a_i \leq n-1$ $(1 = 1, \ldots, r)$, $a_r \neq 0$. Allora

$$|m| \leq \sum_{i=0}^{r} |a_i||n|^i \leq \sum_{i=0}^{r} |a_i| \leq N \frac{\log m}{\log n},$$

disuguaglianza che applicata a m^k, per ogni $k \in \mathbb{N}^*$,

$$|m|^k = |m^k| \leq N \frac{k \log m}{\log n}$$

[3]Alexander Ostrowski (1893–1986), matematico di origine ucraina, studiò e lavorò in Germania ed in seguito a Basilea.

quindi

$$|m| \leq \lim_{k\to\infty} \sqrt[k]{N\frac{k\log m}{\log n}} = 1.$$

Quindi, $|z| \leq 1$ per ogni $z \in \mathbb{Z}$ e dunque, per il Lemma 2.9, $|\ |$ è non-archimedeo.

Sia $J = \{z \in \mathbb{Z} \mid |z| < 1\}$. Per ogni $x, y \in J$ e $a \in \mathbb{Z}$,

$$|x - y| \leq \max\{|x|, |y|\} < 1 \quad \text{e} \quad |ax| = |a||x| < |a| \leq 1,$$

quindi $x - y, ax \in J$; inoltre se $a, b\mathbb{Z} \setminus J$, $|ab| = |a||b| = 1$, quindi $ab \notin J$. Dunque, J è un ideale primo di $\mathbb{Z}$ e non è l'ideale nullo: infatti, se $J = \{0\}$ allora $|\ |$ è il valore assoluto banale, che è escluso per ipotesi. Dunque esiste un primo positivo p tale che $J = p\mathbb{Z}$.

Mostriamo che $|\ |$ è equivalente al valore assoluto p-adico. Sia $m/n \in \mathbb{Q}$ con m, n interi coprimi e $n \neq 0$; osserviamo che la coprimità di m e n implica che al più uno di essi appartiene a $J = p\mathbb{Z}$ (e dunque l'altro ha modulo uguale a 1). Allora

$$1 > \left|\frac{m}{n}\right| = |m||n|^{-1}$$

se e solo se $m \in pZ$ e $n \notin p\mathbb{Z}$, e questo equivale a

$$\left|\frac{m}{n}\right|_p = p^{-\nu_p(m)} < 1.$$

Dunque, $|\ |$ è equivalente al valore assoluto p-adico.

(2) Supponiamo $|n| > 1$ per ogni $1 < n \in \mathbb{N}$. Siano $m, n \in \mathbb{N}$ entrambi maggiori di 1, e poniamo $c(n) = \log_n |n| = \frac{\log|n|}{\log n}$. Si osservi che c è un numero reale positivo.
Dalla rappresentazione di m in base n, $m = a_r n^r + \ldots a_1 n + a_0$, con $0 \leq a_i \leq n - 1$ $(1 = 1, \ldots, r)$ e $r = \left\lfloor \frac{\log m}{\log n} \right\rfloor$, e tenendo conto che dalla proprietà (v4) segue $|k| \leq k$ per ogni $k \in \mathbb{N}$, si ricava

$$|m| \leq \sum_{i=0}^{r} |a_i||n|^i \leq \sum_{i=0}^{r} n|n|^i = n\sum_{i=0}^{r} |n|^i \leq n|n|^{r+1} \leq n^2|n|^r;$$

dunque, $\log|m| \leq 2\log n + r\log|n|$, da cui

$$c(m) = \frac{\log|m|}{\log m} \leq \frac{2\log n}{\log m} + \frac{\log m}{\log n} \cdot \frac{\log|n|}{\log m} = \frac{2\log n}{\log m} + c(n).$$

Per ogni $k \geq 1$, facendo le stesse considerazioni con m^k al posto di m, si ricava

$$c(m) = \frac{\log\left(|m|^k\right)}{\log\left(m^k\right)} = \frac{\log|m^k|}{\log\left(m^k\right)} = c(m^k) \leq \frac{2\log n}{k\log m} + c(n);$$

quindi, passando al limite $k \to \infty$,

$$c(m) \leq c(n).$$

Scambiando i ruoli tra m e n, si ricava allo stesso modo $c(n) \leq c(m)$. Concludiamo dunque che per ogni m, n interi maggiori o uguali a 2,

$$c(n) = c(m) =: c.$$

Dunque, per ogni $n \geq 1$, $|n| = n^c$, da cui segue, per le proprietà dei valori assoluti,

$$|x| = |x|_1^c \quad \text{per ogni } x \in \mathbb{Q},$$

dove $|x|_1$ è il valore assoluto standard di x. In particolare, poiché $c > 0$, per ogni $x \in \mathbb{Q}$ si ha $|x| \leq 1$ se e solo se $|x|_1 \leq 1$, e dunque $|\ |$ è equivalente al valore assoluto standard. □

2.4. Soluzioni dei problemi

PROBLEMA 59. Sia n un intero positivo; basterà osservare che

$$(2n)^2 < 4n^2 + n < \left(2n + \frac{1}{4}\right)^2,$$

quindi

$$2n < \sqrt{4n^2 + n} < 2n + \frac{1}{4},$$

da cui $\lfloor \sqrt{4n^2 + n} \rfloor = 2n$ e l'asserto.

* * *

PROBLEMA 60. Sia $n \geq 2$; chiaramente, $P(n) \neq P(n+1)$ e $\lfloor \sqrt{n} \rfloor \leq \lfloor \sqrt{n+1} \rfloor \leq \lfloor \sqrt{n} \rfloor + 1$. L'unica possibilità perché si abbia l'uguaglianza richiesta è dunque:

$$\begin{cases} \lfloor \sqrt{n+1} \rfloor = \lfloor \sqrt{n} \rfloor + 1 \\ P(n) = P(n+1) + 1 \end{cases}$$

Ora, $P(n+1)$ e $P(n)$ sono numeri primi; si deve dunque avere $P(n+1) = 2$ e $P(n) = 3$, e quindi n è una potenza di 3. Inoltre, la condizione $\lfloor \sqrt{n+1} \rfloor = \lfloor \sqrt{n} \rfloor + 1$ implica che, posto $b = \lfloor \sqrt{n} \rfloor$, si ha $n = b^2 + 2b = b(b+2)$, che è una potenza di 3 se e solo se $b = 1$. Dunque, $n = b^2 + 2b = 3$ è l'unico intero positivo che soddisfa la condizione posta.

* * *

PROBLEMA 61. Siano k, n interi positivi; allora $k = \lfloor \sqrt{n} \rfloor$ se e solo se

$$k^2 \leq n < (k+1)^2 = k^2 + 2k + 1,$$

dunque $n = k^2 + t$ cone $0 \leq t \leq 2k$. In altri termini, ci sono esattamente $2k + 1$ numeri interi positivi (consecutivi) la cui radice quadrata ha parte intera uguale a k. Dunque, se $M \geq 1$,

$$\sum_{n=1}^{M^2} \lfloor \sqrt{n} \rfloor = M + \sum_{n=1}^{M^2-1} \lfloor \sqrt{n} \rfloor = M + \sum_{k=1}^{M-1} k(2k+1) = M + 2 \cdot \sum_{k=1}^{M-1} k^2 + \sum_{k=1}^{M-1} k;$$

quindi, applicando in particolare l'identità (2.2),

$$\sum_{n=1}^{M^2} \lfloor \sqrt{n} \rfloor = M + \frac{(M-1)M(2M-1)}{3} + \frac{(M-1)M}{2} = M + \frac{(M-1)M(4M+1)}{6}.$$

Nel caso specifico del problema, cioè $M = 100$, si ottiene $100 + 33 \cdot 50 \cdot 401 = 661750$.

* * *

PROBLEMA 62. Sia $x \geq 1$ un numero reale non intero; mostriamo che x non soddisfa la condizione del testo. Poiché x non è intero, esiste un numero naturale $p \geq 2$ tale che px non è un intero. Quindi $0 < px - \lfloor px \rfloor < 1$ e dunque esiste un intero positivo m tale che

$$\frac{1}{2m} < px - \lfloor px \rfloor < \frac{1}{m}. \tag{2.5}$$

Moltiplicando per m si ha $0 < mpx - m\lfloor px \rfloor < 1$ e dunque $\lfloor mpx \rfloor = m\lfloor px \rfloor$. D'altra parte, moltiplicando la (2.5) per $2m$, si ottiene

$$1 < 2mpx - 2m\lfloor px \rfloor < 2.$$

e da ciò segue $\lfloor 2mpx \rfloor = 2m\lfloor px \rfloor + 1$. Ora, poiché $x \geq 1$ e $p \geq 2$, $m\lfloor px \rfloor \geq 2$ e dunque

$$\lfloor mpx \rfloor = m\lfloor px \rfloor \text{ non divide } \lfloor 2mpx \rfloor$$

mentre mp divide $2mp$.

* * *

PROBLEMA 63. Cominciamo osservando che l'identità di Hermite (Teorema 2.2) implica in particolare che, per ogni numero reale x,

$$\lfloor 2x \rfloor - \lfloor x \rfloor = \left\lfloor x + \frac{1}{2} \right\rfloor.$$

Dunque, per ogni coppia n, i di interi positivi

$$\left\lfloor \frac{n + 2^{i-1}}{2^i} \right\rfloor = \left\lfloor \frac{n}{2^i} + \frac{1}{2} \right\rfloor = \left\lfloor \frac{n}{2^{i-1}} \right\rfloor - \left\lfloor \frac{n}{2^i} \right\rfloor. \tag{2.6}$$

Ora, posto t il massimo intero positivo tale che $2^t \leq n$ ($t = \lfloor \log_2 n \rfloor$), si ha

$$S := \sum_{i=1}^{\infty} \left\lfloor \frac{n + 2^{i-1}}{2^i} \right\rfloor = \sum_{i=1}^{t+1} \left\lfloor \frac{n + 2^{i-1}}{2^i} \right\rfloor$$

e, applicando (2.6),

$$S = \sum_{i=1}^{t+1} \left(\left\lfloor \frac{n}{2^{i-1}} \right\rfloor - \left\lfloor \frac{n}{2^i} \right\rfloor \right) = \left\lfloor \frac{n}{2^0} \right\rfloor - \left\lfloor \frac{n}{2^{t+1}} \right\rfloor = n - 0 = n.$$

* * *

PROBLEMA 64. Sia n un intero positivo e $m = \lfloor\sqrt{n}\rfloor$; allora (vedi soluzione Problema 61) $n = m^2 + t$ per qualche intero $0 \le t \le 2m$.
Dimostriamo l'asserto del Problema per induzione su $t = n - \lfloor\sqrt{n}\rfloor^2$. Se $t = 0$ allora n è un quadrato e siamo a posto. Sia dunque $t \ge 1$, scriviamo $m = \lfloor\sqrt{n}\rfloor$, ed assumiamo l'ipotesi induttiva.
Supponiamo $t \le m$. Allora

$$f(n) = n + m = m^2 + t + m \le m^2 + 2m < (m+1)^2,$$

quindi $\lfloor\sqrt{f(n)}\rfloor = m$. Ora,

$$b = f^2(n) = f(n) + \lfloor\sqrt{f(n)}\rfloor = n + 2m = m^2 + 2m + t \ge (m+1)^2;$$

dunque $\lfloor b\rfloor = m + 1$ e $b - \lfloor b\rfloor^2 = n + 2m - m^2 - 2m - 1 = t = 1$. Per ipotesi induttiva esiste $t \ge 0$ tale che $f^{t+2}(n) = f^t(b)$ è un quadrato.
Assumiamo ora $t > m$. Allora $f(n) = m^2 + m + t \ge (m+1)^2$, quindi $\lfloor\sqrt{f(n)}\rfloor = m + 1$ e

$$f^2(n) = f(n) - \lfloor\sqrt{f(n)}\rfloor = n + m - (m+1)^2 = t - m - 1 \le 2m - m - 1 < m < t,$$

che consente di concludere per ipotesi induttiva.

* * *

PROBLEMA 65. Sia $1 \le k \le \frac{p-1}{2}$; allora $p - k \le p - 1$ e, applicando opportunamente le proprietà (2) e (4) del Lemma 2.1,

$$\left\lfloor \frac{(p-k)^3}{p} \right\rfloor = \left\lfloor p^2 - 3pk + 3k^2 - \frac{k^3}{p} \right\rfloor = p^2 - 3pk + 3k^2 - 1 - \left\lfloor \frac{k^3}{p} \right\rfloor.$$

Quindi,

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^3}{p} \right\rfloor = \sum_{k=1}^{(p-1)/2} (p^2 - 3pk + 3k^2 - 1);$$

ponendo $N = (p-1)/2$ ed applicando l'identità (2.2), si ha

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^3}{p} \right\rfloor = N(p^2-1) - 3p\cdot\sum_{k=1}^{N} k + 3\cdot\sum_{k=1}^{N} k^2 = N(p^2-1) - \frac{3N(N+1)}{2} + \frac{N(N+1)(2N+1)}{2}.$$

Da ciò, con semplici calcoli, si ricava

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^3}{p} \right\rfloor = \frac{(p+1)(p-1)(p-2)}{4}$$

che è l'identità voluta.

* * *

PROBLEMA 66. Siano p, q interi positivi coprimi. Abbiamo visto nella dimostrazione del Teorema 1.22 che ogni numero intero n si scrive in modo unico come $n = a(n)p + b(n)q$, con $0 \leq a(n) \leq p-1$. Ne segue che un intero positivo n non è rappresentabile come combinazione a coefficienti non negativi di p, q se e solo se

$$-a(n)p \leq b(n)q < 0$$

(la diseguaglianza di sinistra viene da $n \geq 0$, quella di destra dalla non rappresentabilità di n), ovvero

$$0 < -b(n) \leq \frac{a(n)p}{q}.$$

Quindi, per ogni $0 \leq k \leq p-1$, il numero di interi positivi distinti non rappresentabili come combinazione a coefficienti non negativi di p, q e tali che $a(n) = k$ è $\left\lfloor \frac{kp}{q} \right\rfloor$; dunque, per l'identità del problema 58 il numero totale $h(p, q)$ di interi positivi non rappresentabili è

$$h(p,q) = \sum_{k=0}^{p-1} \left\lfloor \frac{kp}{q} \right\rfloor = \frac{(p-1)(q-1)}{2}.$$

* * *

PROBLEMA 70. Come osservato (formula (2.3)), per ogni primo p si ha

$$\nu_p\left[\binom{200}{100}\right] = \nu_p(200!) - 2\nu_p(100!) = \sum_{i=1}^{\infty} \left\lfloor \frac{200}{p^i} \right\rfloor - 2\sum_{i=1}^{\infty} \left\lfloor \frac{100}{p^i} \right\rfloor$$

Se $\lfloor \sqrt{200} \rfloor < p < 100$ allora

$$\nu_p(200!) - 2\nu_p(100!) = \left\lfloor \frac{200}{p} \right\rfloor - 2\left\lfloor \frac{100}{p} \right\rfloor,$$

dunque p divide $\binom{200}{100}$ se e solo se $\left\lfloor \frac{200}{p} \right\rfloor > 2\left\lfloor \frac{100}{p} \right\rfloor$. Se $66 = \lfloor 200/3 \rfloor < p < 100$, allora $\left\lfloor \frac{200}{p} \right\rfloor = 2 = 2\left\lfloor \frac{100}{p} \right\rfloor$, mentre per $50 < p \leq 66$ si ha

$$\left\lfloor \frac{200}{p} \right\rfloor = 3 > 2\left\lfloor \frac{100}{p} \right\rfloor.$$

Il più grande primo in questo intervallo, che è anche la risposta al quesito, è $p = 61$.

* * *

PROBLEMA 71. Per ogni $1 \leq i \leq n$ denotiamo $M(i) = mcm(1, 2, \ldots, \lfloor n/i \rfloor)$. Sia p un numero primo. Poiché $M(i)$ è il minimo comune multiplo di titti gli interi compresi tra 1 e $\lfloor \frac{n}{i} \rfloor$, $k = \nu_p(M(i))$ è l'esponente della massima potenza di p minore o uguale a $\frac{n}{i}$. Ora

$$p^k \leq n/i < p^{k+1}$$

se e solo se

$$\left\lfloor \frac{n}{p^{k+1}} \right\rfloor < i \leq \left\lfloor \frac{n}{p^k} \right\rfloor;$$

quindi, il numero di termini i tali che $k = \nu_p(M(i))$ è uguale a

$$\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor.$$

Possiamo dunque calcolare

$$\nu_p\Big(\prod_{i=1}^{n} M(i)\Big) = \sum_{i=1}^{n} \nu_p(M(i)) = \sum_{k=1}^{\lfloor \log_p n \rfloor} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) = \sum_{k=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor = \nu_p(n!).$$

Questo vale per ogni primo p, da cui l'uguaglianza cercata.

* * *

PROBLEMA 72. Punto (a). Assumiamo prima $0 \leq x, y \leq 1$, quindi $\lfloor x \rfloor = 0 = \lfloor y \rfloor$, e proviamo

$$\lfloor 3x + y \rfloor + \lfloor 3y + x \rfloor \leq \lfloor 5x \rfloor + \lfloor 5y \rfloor. \tag{2.7}$$

Sia $y \leq x$; e supponiamo per assurdo $\lfloor 3x + y \rfloor + \lfloor 3y + x \rfloor \geq \lfloor 5x \rfloor + \lfloor 5y \rfloor + 1$. Poiché $\lfloor 3x + y \rfloor \leq \lfloor 4x \rfloor \leq \lfloor 5x \rfloor$, si ha

$$\begin{cases} \lfloor 3y + x \rfloor = \lfloor 5y \rfloor + 1 \\ \lfloor 3x + y \rfloor = \lfloor 5x \rfloor \end{cases}$$

da cui,

$$\begin{cases} 3y + x \geq \lfloor 5y \rfloor + 1 \\ 3x + y > 5x - 1 \end{cases}$$

Da questo si deduce in particolare, $2y < x < 2/3$ e $2x < y + 1$. Ma allora

$$\lfloor 5x \rfloor + \lfloor 5y \rfloor < \lfloor 3x + y \rfloor + \lfloor 3y + x \rfloor \leq \lfloor 2 + 1/3 \rfloor + \lfloor 3y + 2/3 \rfloor \leq 2 + 0 = 2,$$

e dunque, $\lfloor 5y \rfloor = 0$. A questo punto $y < 1/5$, e allora, da $3y + x \geq 1$ e $2x < y + 1$, segue $2/5 < x < 3/5$, per cui la contraddizione

$$2 > \lfloor 3x + y \rfloor = \lfloor 5x \rfloor \geq 2.$$

La diseguaglianza (2.7) è quindi provata per $0 \leq x, y < 1$.

Veniamo al caso generale del punto (a), e dato $0 \leq x \in \mathbb{R}$, scriviamo $x - \lfloor x \rfloor = \{x\} < 1$. Si verifica facilmente che, per $0 \leq x, y \in \mathbb{R}$ e m, n interi positivi:

$$\lfloor nx + my \rfloor = n\lfloor x \rfloor + m\lfloor y \rfloor + \lfloor n\{x\} + m\{y\} \rfloor.$$

Quindi

$$\lfloor 3x + y \rfloor + \lfloor 3y + x \rfloor + \lfloor x \rfloor + \lfloor y \rfloor = 5\lfloor x \rfloor + 5\lfloor y \rfloor + \lfloor 3\{x\} + \{y\} \rfloor + \lfloor 3\{y\} + \{x\} \rfloor,$$

e, per il caso discusso prima,

$$\lfloor 3x+y\rfloor+\lfloor 3y+x\rfloor+\lfloor x\rfloor+\lfloor y\rfloor\leq 5\lfloor x\rfloor+5\lfloor y\rfloor+\lfloor 5\{x\}\rfloor+\lfloor 5\{y\}\rfloor=\lfloor 5x\rfloor+\lfloor 5y\rfloor.$$

Il punto (b) del Problema si tratta ora come nella soluzione del Problema 67. Pwer ogni primo p e intero positivo i, si ha, per il punto (a),

$$\left\lfloor\frac{m}{p^i}\right\rfloor+\left\lfloor\frac{n}{p^i}\right\rfloor+\left\lfloor\frac{3m+n}{p^i}\right\rfloor+\left\lfloor\frac{3n+n}{p^i}\right\rfloor\leq\left\lfloor\frac{5m}{p^i}\right\rfloor+\left\lfloor\frac{5n}{p^i}\right\rfloor.$$

Da ciò segue, per il Teorema 2.4,

$$\nu_p(m!n!(3m+n)!(3n+m)!)\leq\nu_p((5m)!(5n)!).$$

Questo vale per ogni primo p, dunque $m!n!(3m+n)!(3n+m)!$ divide $(5m)!(5n)!$.

* * *

PROBLEMA 73. Sia $f(n)=\sum_{k=0}^{2010}n^k$; allora

$$f(n)=\frac{n^{2011}-1}{n-1}.$$

Sia m un intero, $2\leqslant m\leqslant 2010$; proviamo che non esiste n tale che $f(n)$ è un multiplo di m. Chiaramente, possiamo supporre che $m=p$ sia un numero primo. Supponiamo, per assurdo, $p\mid f(n)$ per un intero positivo n. Osserviamo che $p\neq 2$; infatti, poiché 2010 è pari, $f(n)$ è dispari per ogni intero positivo n.
Ora, p divide $n^{2011}-1$ e, per il Teorema di Fermat, p divide $n^{p-1}-1$, e quindi p divide n^d-1, dove $d=MCD(2011,p-1)$; ma 2011 è un numero primo maggiore di p e pertanto $d=1$. Dunque, p divide $n-1$. Per il Teorema 2.6,

$$\nu_p(n^{2011}-1)=\nu_p(n-1)++\nu_p(2001)=\nu_p(n-1)+0$$

il che implica che p non divide $f(n)$, contraddizione.

* * *

PROBLEMA 74. Siano m,n interi positivi tali che $p^m-n^p=1$, con p un numero primo dispari. Allora $p^m=n^p+1$, e $p\mid n+1$: infatti, dato che p è un primo, $n\equiv n^p\equiv -1 \pmod p$. Allora, per il Corollario 2.7,

$$m=\nu_p(n^p+1)=\nu_p(n+1)+1.$$

Dunque, $\nu_p(n+1)=m-1$, e questo forza $n+1=p^{m-1}$. Allora

$$p^m>n^p\geq(p^{m-1}-1)^3=p^{3m-3}-3p^{2m-2},$$

che, con semplici considerazioni, implica $m=2$, $n=2$, $p=3$. Questa è infatti una soluzione: $2^3+1=3^2$.

* * *

PROBLEMA 75. Sia $n \in \mathbb{N}^*$ tale che $3^n - 2^n = q^k$ dove k è un numero primo q e $k \geq 1$. Chiaramente $n \geq 2$. Sia p un divisore primo di n e $n = pm$. Poiché

$$3^p - 2^p \mid 3^{pm} - 2^{pm} = (3^p)^m = (2^p)^m$$

deve essere $3^p - 2^p = q^v$ per qualche $v \geq 1$. Poiché $q \neq 2, 3$, il Teorema 2.6 fornisce

$$k = \nu_q(3^n - 2^n) = \nu_q(3^p - 2^p) + \nu_q(m) = v + \nu_q(m).$$

Se $\nu_q(m) = 0$, allora $3^n - 2^n = q^k = q^v = 3^p - 2^p$ e quindi $n = p$.
Altrimenti, q divide m (quindi divide n), dunque $1 < 3^q - 2^q$ divide $3^n - 2^n = q^k$, il che è assurdo dato che, poiché certamente $q \neq 2, 3$,

$$3^n - 2^n \equiv 3 - 2 = 1 \pmod{q}.$$

Si osservi che $3^2 - 2^2 = 5$, $3^3 - 2^3 = 19$, $3^5 - 2^5 = 211$ sono numeri primi, ma $3^7 - 2^7 = 29 \cdot 71$.

* * *

PROBLEMA 76. Siano p un numero primo, e k, n interi positivi tali che $2^p + 3^p = k^n$. Per $p = 2$ si ha $2^2 + 3^2 = 13$. Sia quindi p dispari; allora $5 = 2 + 3$ divide $2^p + 3^p = k^n$, dunque 5 divide k e, per il Corollario 2.7,

$$n \geq \nu_5(k^n) = \nu_5(2 + 3) + \nu_5(p).$$

Per $p = 5$ si ha $2^5 + 3^5 = 11 \cdot 5^2$, che non è un quadrato. Altrimenti, p è un primo diverso da 5, dunque $\nu_5(p) = 0$, e quindi $n = \nu_5(2 + 3) = 1$.

* * *

PROBLEMA 77. Siano p un numero primo e $m \geq 2$ un intero, e supponiamo esistano interi positivi x, y con $(x, y) \neq (1, 1)$, tali che

$$\frac{x^p + y^p}{2} = \Big(\frac{x + y}{2}\Big)^m.$$

Se $p = 2$ allora, poiché $(x, y) \neq (1, 1)$, controllato che il caso $x + y = 3$ non si verifica, si può supporre $x + y \geq 4$ e quindi

$$\frac{x^2 + y^2}{2} < \frac{(x + y)^2}{2} < \frac{x + y}{4} \cdot \frac{(x + y)^2}{2} = \Big(\frac{x + y}{2}\Big)^3,$$

quindi la sola possibilità è $m = 2$ (che di fatto si verifica per $x = y$).
Sia p dispari. Supponiamo esista un primo dispari q che divide $x + y$ e sia $v = \nu_q(x + y)$; allora, per il Corollario 2.7,

$$\nu_q\Big(\frac{x^p + y^p}{2}\Big) = \nu_q(x^p + y^p) = v + \nu_q(p).$$

D'altra parte,

$$\nu_q\Big(\Big(\frac{x + y}{2}\Big)^m\Big) = \nu_q((x + y)^m) = mv.$$

Dal confronto, tenendo conto che $m \geq 2$, si ricava $q = p$, $v = 1$ e $m = 2$; questo (dato che $p \geq 3$) si vede facilmente non può essere il caso.
Dunque, $x + y$ e $x^p + y^p$ sono potenze di 2. Se $x \neq y$ allora, per qualche $t \geq 0$, $x + y = 2^t(x_1 + y_1)$ con x_1, y_1 dispari e $(x_1, y_1) \neq (1, 1)$. Ora

$$x^p + y^p = 2^{tp}(x_1^p + y_1^p) = (x_1 + y_1)(x_1^{p-1} + x_1^{p-2}y_1 + \ldots + y_1^{p-1})$$

ma, poiché p è dispari, $x_1^{p-1} + x_1^{p-2}y_1 + \ldots + y_1^{p-1}$ è dispari, contro il fatto che $x^p + y^p$ è una potenza di 2. Quindi, $x = y = 2^k$ per qualche $k \geq 1$, e

$$2^{kp} = \frac{x^p + y^p}{2} = \left(\frac{x + y}{2}\right)^m = (2^k)^m = 2^{km}$$

pertanto $m = p$.

2.5. Speciale problemi di funzioni

Problemi in cui si chiede di determinare le funzioni (in genere definite su $\mathbb{R}$, $\mathbb{Z}$ o $\mathbb{N}^*$) che soddisfano a certe condizioni (prevalentemente di tipo aritmetico, anche se spesso sembrano un po' strampalate) sono tra i favoriti di chi prepara i testi delle competizioni matematiche: molti dei temi proposti contiengono almeno una questione del genere. Si tratta, normalmente, di problemi la cui soluzione non richiede particolari conoscenze, ma molto ingegno, assieme alla capacità di intuire i giusti percorsi.

Se f è una funzione da un insieme X in se stesso, denotiamo con f^2 la composizione di f con se stessa (ovvero, $f^2(x) = f(f(x))$ per ogni $x \in X$), e in generale, per $n \geq 1$ un intero positivo, f^n denota la n-esima iterazione di f.
Come primo esempio, vediamo un problema che ha a che fare con uno degli argomenti di questo capitolo.

Problema 78 (IMO 2010). *Determinare tutte le funzioni $f : \mathbb{R} \to \mathbb{R}$ tali che*

$$f(\lfloor x \rfloor y) = f(x) \lfloor f(y) \rfloor$$

per ogni $x, y \in \mathbb{R}$.

Soluzione. Ponendo $x = y = 1$ sia ha $f(1) = f(1)^2$, quindi $f(1) \in \{0, 1\}$; il medesimo argomento fornisce $f(0) \in \{0, 1\}$.
Se $f(1) = 0$ allora, per ogni $x \in \mathbb{R}$, $f(x) = f(\lfloor 1 \rfloor x) = f(1)\lfloor f(x) \rfloor = 0$, e f è la costante 0.
Se $f(0) = 1$ allora, per ogni $x \in \mathbb{R}$, $f(x) = f(x)\lfloor f(0) \rfloor = f(\lfloor x \rfloor 0) = f(0) = 1$, dunque f è la funzione costante 1.
Supponiamo quindi $f(0) = 0$ e $f(1) = 1$. Allora per ogni $x \in \mathbb{R}$,

$$f(x) = f(x)\lfloor f(1) \rfloor = f(\lfloor x \rfloor 1) = f(\lfloor x \rfloor);$$

in particolare, se $0 \leq x < 1$, $f(x) = f(\lfloor x \rfloor) = f(0) = 0$. Ma allora

$$1 = f(1) = f(\lfloor 2 \rfloor 2^{-1}) = f(2)\lfloor f(2^{-1} \rfloor = f(2) \cdot 0 = 0,$$

una contraddizione. In conclusione, le sole funzioni che soddisfano la proprietà richiesta sono le funzioni costanti 0 e 1. ∎

Come in questo esempio, un primo passo sovente utile è stabilire - se le condizioni date lo consentono - i valori che la funzione assume in particolari punti: in genere, $f(0)$ e/o $f(1)$ per funzioni definite su $\mathbb{R}$, $f(1)$ (o a volte $f(p)$ quando p è un numero primo) per funzioni definite su $\mathbb{N}$. Un altro passo iniziale consigliabile (ma non sempre attuabile facilmente) è quello di trovare una (o qualche) funzione che soddisfi le proprietà richieste: in molti casi le soluzioni sono poche e può essere utile avere un'idea di dove andare a parare. Il problema seguente è un buon esempio: la tecnica di soluzione è elementare ma non immediata da trovare.

Problema 79 (Nordic, 2003). *Sia $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Determinare tutte le funzioni $f : \mathbb{R}^* \to \mathbb{R}^*$ tali che*

$$f(x) + f(y) = f(xy \cdot f(x + y))$$

per ogni $x, y \in \mathbb{R}^*$ con $x + y \neq 0$.

Soluzione. La funzione $\phi(x) = \frac{1}{x}$ (che è definita per ogni $x \in \mathbb{R}^*$ ed è una biezione di $\mathbb{R}^*$) è una soluzione; infatti per ogni $x, y \in \mathbb{R}^*$ con $x + y \neq 0$,

$$\phi(x) + \phi(y) = \frac{1}{x} + \frac{1}{y} = \frac{x+y}{xy} = \left(\frac{xy}{x+y}\right)^{-1} = \phi(xy\phi(x+y)).$$

Sia ora $f : \mathbb{R}^* \to \mathbb{R}^*$ che soddisfa la condizione data e $x \in \mathbb{R}$. Poiché $\mathbb{R}^* = \{1/y \mid y \in \mathbb{R}^*\}$, $f(x) = \frac{1}{y}$ per qualche $y \in \mathbb{R}^*$. Supponiamo per assurdo $y \neq x$; allora $x - y \neq 0$ e

$$f(y) + f(x - y) = f((x - y)y \cdot f(x)) = f((x - y)y \cdot y^{-1}) = f(x - y),$$

da cui segue l'assurdo $f(y) = 0$. Dunque $f(x) = \frac{1}{x}$ pr ogni $x \in \mathbb{R}^*$ e $f = \phi$ è la sola funzione con la proprietà richiesta. ∎

Problema 80 (Nordic 1998). *Determinare le funzioni $f : \mathbb{Q} \to \mathbb{Q}$ tali che*

$$f(x + y) + f(x - y) = 2f(x) + 2f(y)$$

per ogni $x, y \in \mathbb{Q}$.

Soluzione. Per ogni $b \in \mathbb{Q}$ sia $f_b : \mathbb{Q} \to \mathbb{Q}$ la funzione definita da $f_b(x) = ax^2$, per ogni $x \in \mathbb{Q}$; allora per $x, y \in \mathbb{Q}$:

$$f_b(x+y) = f_b(x-y) = b(x^2+2xy+y^2)+b(x^2-2xy+y^2) = 2bx^2+2by^2 = 2f_b(x)+2f_b(y).$$

Viceversa, sia $f : \mathbb{Q} \to \mathbb{Q}$ che soddisfa l'equazione data; ponendo in essa $n = m = 0$ si ottiene $2f(0) = 4f(0)$, da cui $f(0) = 0$. Scriviamo $b = f(1)$ e mostriamo che $f = f_b$. Cominciamo provando che, per ogni $x \in \mathbb{Q}$ ed ogni $z \in \mathbb{Z}$,

$$f(nx) = n^2 f(x). \tag{2.8}$$

Per $n = 0$ questo è già stato visto e per $n = 1$ è banale. Sia $n \geq 1$; dall'equazione si ricava

$$f((n+1)x) = f(nx + x) = 2f(nx) + 2f(x) - f(nx - x)$$

e per ipotesi induttiva,

$$f((n+1)x) = 2n^2 f(x) + 2f(x) - (n-1)^2 f(x) = (n+1)^2 f(x);$$

dunque (2.8) è provata per ogni $n \in \mathbb{N}$. Dalla equazione si ottiene anche, per ogni $x \in \mathbb{Q}$,

$$f(-x) = 2f(0) + 2f(x) - f(x) = f(x),$$

e dunque (2.8) vale per ogni $z \in \mathbb{Z}$. Sia ora $\mathbb{Q} \ni x = \frac{z}{m}$ con $z \in \mathbb{Z}$ e $n \in \mathbb{N}^*$. Allora, per quanto visto sinora, $n^2 f(x) = f(z) = f(z \cdot 1) = z^2 b$; quindi,

$$f(x) = \frac{z^2}{n^2} b = x^2 b = f_b(x)$$

come si voleva. ■

Altri problemi sulle funzioni reali.

Problema 81 (Gran Bretagna, 2008)**.** *Determinare tutte le funzioni $f : \mathbb{R} \to \mathbb{R}$ tali che*

$$f(x)f(y) = f(x+y) + xy$$

per ogni $x, y \in \mathbb{R}$.

Problema 82 (Vietnam 2005)**.** *Trovare tutte le funzioni $f : \mathbb{R} \to \mathbb{R}$ tali che*

$$f(f(x-y)) = f(x) \cdot f(y) - f(x) + f(y) - xy$$

per ogni $x, y \in \mathbb{R}$.

Problema 83 (Czech-Polish-Slovak 2009)**.** *Sia $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ l'insieme dei numeri reali positivi. Trovare tutte le funzioni $f : \mathbb{R}^+ \to \mathbb{R}^+$ tali che*

$$\Big(1 + yf(x)\Big)\Big(1 - yf(x+y)\Big) = 1$$

per ogni $x, y \in \mathbb{R}^+$.

Problema 84 (Gran Bretagna, 2009)**.** *Determinare tutte le funzioni $f : \mathbb{R} \to \mathbb{R}$ tali che*

$$f(x^3) + f(y^3) = (x+y)(f(x^2) + f(y^2) - f(xy)),$$

per ogni $x, y \in \mathbb{R}$.

Problema 85 (Baltic Way 2011)**.** *Sia $f : \mathbb{R} \to \mathbb{R}$ una funzione che soddisfa*

$$f(f(x)) = x^2 - x + 1$$

per ogni $x \in \mathbb{R}$. Determinare $f(0)$.

Problema 86 (Filippine 2010). *Provare che non esistono funzioni $f : \mathbb{R} \to \mathbb{R}$ tali che*

$$f(f(x)) + xf(x) = 1$$

per ogni $x \in \mathbb{R}$.

Veniamo ora a funzioni definite sui numeri naturali (o interi): in questo contesto sono da considerare, come possibili strumenti da utilizzare o carte da giocare, induzione, buon ordine (minimi), divisione, ordinamento, etc.

Iniziamo con una osservazione generale. Sia $f : M \to M$ (dove $M = \mathbb{N}^*, \mathbb{N}$ o $\mathbb{Z}$), tale che

$$f(m+n) = f(m) + f(n) \quad \text{per ogni} \quad m, n \in M. \tag{2.9}$$

Nei casi $M = \mathbb{N}, \mathbb{Z}$, ponendo $m = n = 0$ si ha $f(0) = 2f(0)$, da cui si ricava $f(0) = 0$. Scriviamo $b = f(1)$. Allora, per ogni $n \in \mathbb{N}$

$$f(n+1) = f(n) + f(1) = f(n) + 1$$

e dunque, per un ovvio argomento induttivo, $f(n) = nb$ per ogni $n \in \mathbb{N}$.
Infine, nel caso $M = \mathbb{Z}$, da

$$0 = f(0) = f(n + (-n)) = f(n) + f(-n)$$

segue $f(-n) = -f(n)$, per ogni $n \in M$. Abbiamo quindi provato che se f soddisfa (2.9) allora

$$f(x) = f(1)x,$$

per ogni $x \in M$.

Il prossimo esempio, oltre a proporre una variazione di quanto appena visto, illustra come a volte possa essere utile stabilire che le funzioni che stiamo cercando godono di proprietà quali l'iniettività e/o la suriettività

Problema 87 (Sudafrica 1997). *Trovare tutte le funzioni $f : \mathbb{Z} \to \mathbb{Z}$ che soddisfano*

$$f(m + f(n)) = f(m) + n$$

per ogni $m, n \in \mathbb{Z}$.

Soluzione. Ponendo $m = 0$ si ha $f(f(n)) = f(0) + n$, da cui segue che f è una funzione iniettiva (se $f(n) = f(n')$, allora $f(0) + n = f(0) + n'$ e $n = n'$).
Ponendo ora $n = 0$, risulta $f(m + f(0)) = f(m)$ e quindi (poiché f è iniettiva), $f(0) = 0$. Dunque, per quanto osservato all'inizio, $f^2(n) = n$ per ogni $n \in \mathbb{Z}$. Quindi, per ogni $m, n \in \mathbb{Z}$ si ha

$$f(f(m) + f(n)) = f^2(m) + n = m + n = f^2(m + n)$$

da cui, per iniettività,

$$f(m) + f(n) = f(m + n).$$

Da questo segue (vedi le osservazioni che precedono) che $f(a) = f(1)a$, per ogni $a \in \mathbb{Z}$. In particolare $1 = f(f(1)) = f(1)^2$, quindi $f(1) \in \{1, -1\}$, e i due casi forniscono le uniche

due diverse funzioni che soddisfano la condizione; ovvero $f(a) = a$, per ogni $a \in \mathbb{Z}$, oppure $f(a) = -a$, per ogni $a \in \mathbb{Z}$. ∎

Il caso di funzioni $f : \mathbb{N}^* \to \mathbb{N}^*$ che conservano il prodotto, cioè tali che

$$f(mn) = f(n)f(m) \quad \text{per ogni} \quad m, n \in \mathbb{N}^*$$

è più complesso (a parte la semplice osservazione che da $f(1) = f(1)f(1)$ segue necessariamente $f(1) = 1$). Vediamo due problemi molto affini.

Problema 88 (Canada). *Trovare tutte le funzioni $f : \mathbb{N}^* \to \mathbb{N}^*$ tali che*

(i) $f(n + 1) > f(n)$ *per ogni* $n \in \mathbb{N}^*$,

(ii) $f(mn) = f(m)f(n)$ *per ogni* $m, n \in \mathbb{N}^*$,

(iii) $f(2) = 2$.

Problema 89 (Nordic, 1987). *Sia $f : \mathbb{N}^* \to \mathbb{N}^*$ tale che*

(i) $f(n + 1) > f(n)$ *per ogni* $n \in \mathbb{N}^*$,

(ii) $f(mn) = f(m)f(n)$ *per ogni* $m, n \in \mathbb{N}^*$,

(iii) $f(2) > 2$,

Determinare il valore minimo di $f(2)$.

Soluzione. Sia $f : \mathbb{N}^* \to \mathbb{N}^*$ con le proprietà (i) e (ii) nei due testi. Allora $f(1) = f(1)f(1)$ e quindi $f(1) = 1$.

Problema 88. Dalle (ii) e (iii) segue $f(4) = 4$; quindi, da (i), $2 = f(2) < f(3) < f(4) = 4$ e $f(3) = 3$. Osserviamo poi che, per ogni $m \in \mathbb{N}^*$,

$$f(2m) = f(2)f(m) = 2f(m). \tag{2.10}$$

A questo punto dimostriamo, procedendo per induzione su n, che $f(n) = n$ per ogni $n \in \mathbb{N}^*$. Abbiamo già verificato questo per $n \leq 4$. Sia $n \geq 5$. Se $n = 2m$ è pari, allora per (2.10) e l'ipotesi induttiva, $f(n) = 2f(m) = 2m = n$. sia $n = 2m + 1$; allora $m + 1 < m$, quindi

$$2m = f(2m) < f(n) < f(2(m + 1)) = 2f(m + 1) = 2m + 2,$$

da cui $f(n) = 2m + 1 = n$.

Problema 89. La funzione $f(x) = x^2$ soddisfa le proprietà (i) e (ii), inoltre $f(2) = 4$. Mostriamo che questo è il valore cercato, supponendo per assurdo che esista $f : \mathbb{N}^* \to \mathbb{N}^*$ che soddisfa (i) e (ii) e tale che $f(2) = 3$. Allora, per le proprietà (i) e (ii),

$$f(3)^2 = f(9) > f(8) = f(2)^3 = 27$$

e dunque $f(3) \geq 6$. Ora,

$$6^5 \leq f(3)^5 = f(3^5) = f(243) < f(256) = f(2^8) = f(2)^8 = 3^8,$$

da cui $2^5 < 3^3$, che è assurdo. ∎

Un problema che un poco chiarisce come possono essere definite funzioni $\mathbb{N}^* \to \mathbb{N}^*$ che conservano il prodotto, è il primo della seguente collezione (la soluzioni si trovano più avanti).

Problema 90 (Turchia 1995). *Trovare tutte le funzioni suriettive $f : \mathbb{N}^* \to \mathbb{N}^*$ tali che*

$$m \mid n \;\Leftrightarrow\; f(m) \mid f(n)$$

per ogni $m, n \in \mathbb{N}^*$.

Problema 91 (Canada, 2015). *Trovare tutte le funzioni $f : \mathbb{N}^* \to \mathbb{N}^*$, tali che*

$$(n-1)^2 < f(n)f^2(n) < n^2 + n$$

per ogni intero positivo n.

Problema 92 (IMO 2013, Colombia). *Trovare tutte le funzioni $f : \mathbb{N}^* \to \mathbb{N}^*$ tali che*

$$m^2 + f(n) \mid mf(m) + n$$

per ogni $m, n \in \mathbb{N}^*$.

Problema 93 (Indonesia 1999). *Trovare tutte le funzioni $f : \mathbb{N}^* \to \mathbb{N}^*$ tali che*

$$f(mn) + f(m+n) = f(m)f(n) + 1$$

per ogni $m, n \in \mathbb{N}^*$.

Problema 94 (Spagna 2000). *Si provi che non esiste alcuna funzione $f : \mathbb{N} \to \mathbb{N}$ tale che $f(f(n)) = n + 1$ per ogni $n \in \mathbb{N}$,*

I seguenti problemi hanno a che fare con la funzione parte intera, sono quindi particolarmente raccomandati.

Problema 95 (Spagna 2010). *Sia $f : \mathbb{N} \to \mathbb{Z}$ la funzione definita da, per ogni $n \in \mathbb{N}$,*

$$f(n) = -f\left(\left\lfloor \frac{n}{3} \right\rfloor\right) - 3\left\{\frac{n}{3}\right\}$$

(dove, per ogni $x \in \mathbb{R}$, $\{x\} = x - \lfloor x \rfloor$). Trovare il minimo intero n tale che $f(n) = 2010$.

Problema 96 (IMO 1982). *Sia $f : \mathbb{N}^* \to \mathbb{N}$ tale che $f(2) = 0, f(3) > 0, f(9999) = 3333$, e*

$$f(m+n) - f(m) - f(n) \in \{0, 1\}$$

per ogni $m, n \in \mathbb{N}^*$. Determinare $f(1982)$.

Per quest'ultimo problema, si osservi che la condizione imposta su f si può riscrivere come

$$f(m) + f(n) \leq f(m+n) \leq f(m) + f(n) + 1,$$

che richiama una delle proprietà (Lemma 2.1 punto (1)) della funzione parte intera.

Problemi impegnativi possono essere quelli in cui le funzioni che soddisfano le condizioni richieste dal testo sono diverse. Vediamo alcuni esempi.

Problema 97 (IMO, 1996). *Trovare tutte le funzioni $f : \mathbb{N} \to \mathbb{N}$ tali che*

$$f(m + f(n)) = f(f(m)) + f(n)$$

per ogni $m, n \in \mathbb{N}$.

Soluzione. Sia $f : \mathbb{N} \to \mathbb{N}$ una funzione che soddisfa la condizione richiesta; ponendo $m = 0$ nell'equazione, si ha

$$f^2(n) = f^2(0) + f(n) \tag{2.11}$$

per ogni $n \in \mathbb{N}$. In particolare, per $n = 0$, $f^2(0) = f^2(0) + f(0)$, quindi $f(0) = 0$. La funzione costante $f(n) = 0$ è una soluzione. D'ora in avanti supponiamo f non sia la costante nulla.
Da (2.11) segue

$$f^2(n) = f(n) \quad \text{per ogni } n \in \mathbb{N}.$$

Quindi ogni elemento dell'immagine $f(\mathbb{N}) = \{f(n) \mid n \in \mathbb{N}\}$ è fissato da f; dunque $f(\mathbb{N})$ è l'insieme degli elementi di $\mathbb{N}$ che sono fissati da f.
Poiché f non è costantemente 0, esiste $b = \min\{n \mid 1 \leq n = f(n)\}$. Proviamo, per induzione su $q \in \mathbb{N}^*$, che $f(qb) = qb$. Questo è per definizione se $n = 1$ (infatti $f(b) = b$); sia $q \geq 2$, allora, per l'ipotesi induttiva,

$$f(qb) = f((q-1)b + b) = f^2((q-1)b) + b = f((q-1)b) + b = (q-1)b + b = qb,$$

come si voleva. Ora, per un generico $n \in \mathbb{N}$, la divisione euclidea dà $n = qb + r$, con $q, r \in \mathbb{N}$ e $0 \leq r \leq b - 1$; per cui

$$f(qb + r) = f(r + f(qb)) = f^2(r) + f(qb) = qb + f(r). \tag{2.12}$$

Questo implica in particolare che $f(\mathbb{N}) = b\mathbb{N} = \{bx \mid x \in \mathbb{N}\}$; infatti sia $x = qb + r \in \mathbb{N}$, con $0 \leq r \leq b-1$, allora $x \in f(\mathbb{N})$ se e solo se $x = f(x)$, se e solo se (dalla (2.12)) $r = f(r)$, se e solo se (per la scelta di b) $r = 0$.
A questo punto, per ogni $0 \leq r \leq b-1$, $f(r) \in f(\mathbb{N})$ quindi esiste $u_r \in \mathbb{N}$ (e $u_0 = 0$) tale che $f(r) = bu_r$. Per (2.12) la funzione f verifica quindi, per ogni $q \in \mathbb{N}^*$ e ogni $0 \leq r \leq b - 1$,

$$f(qb + r) = qb + f(r) = b(q + u_r).$$

Viceversa, proviamo che ogni funzione definita in questo modo, verifica la condizione. Quindi, siano fissati $b \in \mathbb{N}$ e $u_r \in \mathbb{N}^*$ per ogni $0 \leq r \leq b-1$, con $u_0 = 0$, e sia $f : \mathbb{N}^* \to \mathbb{N}^*$ definita da, per ogni $q \in \mathbb{N}$ e $0 \leq r \leq b - 1$:

$$f(qb + r) = b(q + u_r).$$

Si verifica agevolmente che f soddisfa la condizione, e la soluzione è completa. ∎

Problema 98 (Vietnam 1996)**.** *Trovare tutte le funzioni* $f : \mathbb{N}^* \to \mathbb{N}^*$ *tali che*

$$f(n) + f(n+1) = f(n+2)f(n+3) - 1996$$

per ogni $n \in \mathbb{N}^*$.

SOLUZIONE. Per $n \in \mathbb{N}^*$, sia $P(n)$ l'identità $f(n) + f(n+1) = f(n+2)f(n+3) - 1996$. Sottraendo membro a membro $P(n)$ da $P(n+1)$ si ottiene

$$f(n+2) - f(n) = f(n+3)(f(n+4) - f(n+2))$$

per ogni $n \in \mathbb{N}^*$. Da questo segue per induzione che, per ogni $m \geq 2$,

$$f(3) - f(1) = f(4)f(6)\cdots f(2m)[f(2m+1) - f(2m-1)] \tag{2.13}$$

e similmente

$$f(4) - f(2) = f(5)f(7)\cdots f(2m+1)[f(2m+2) - f(2m) \tag{2.14}$$

Osserviamo anche che dalla condizione imposta segue subito che per ogni $n_0 \in \mathbb{N}$ esiste $k \geq n_0$ tale che $f(k) > 1$. Poniamo $a = f(3) - f(1)$, $b = f(4) - f(2)$. Notiamo che se $a \neq 0$ segue allora dalla (2.13) che $f(2m) = 1$ tranne che per un numero finito di valori $m \geq 2$; similmente, se $b \neq 0$, si ha che $f(2m+1) = 1$ tranne che per un numero finito di casi. Per quanto osservato poco sopra, concludiamo che questi due casi non possono presentarsi assieme. Studiamo quindi separatamente i tre casi rimasti.

(i) $a = 0 = b$. Da (2.13) e (2.14) segue $f(2m) = f(2)$ e $f(2m+1) = f(1)$, per ogni $m \geq 1$. In particolare, per la condizione data,

$$f(1) + f(2) = f(1)f(2) - 1996. \tag{2.15}$$

Per quanto osservato, $f(1)$ e $f(2)$ non possono essere entrambi 1. Supponiamo $f(1) \neq 1$, allora da (2.15) segue che $f(1) - 1$ divide $f(1) + 1996 - (f(1) - 1) = 1997$. Poiché 1997 è un numero primo, risulta $f(1) - 1 \in \{1, 1997\}$, cioè $f(1) = 2$ oppure $f(1) = 1998$. Nei due casi, da (2.15) segue, rispettivamente, $f(2) = 1998$ e $f(2) = 2$. Risultano quindi due funzione: per la prima $f(2m+1) = f(1) = 2$ e $f(2m) = f(2) = 1998$, per ogni $m \geq 1$; per la seconda, $f(2m+1) = 1998$, $f(2m) = 2$ per ogni $m \geq 1$.

(ii) $a \neq 0$ (e $b = 0$). Poiché $b = 0$ si ha, come prima, $f(2m) = f(2)$ per ogni $m \geq 1$; allora da (2.14) e da $a \neq 0$ segue $f(2m+1) - f(2m-1) = a$ e quindi, con una semplice induzione, $f(2m+1) - f(1) = ma$, per ogni $m \geq 1$. Inoltre, dalla condizione imposta in partenza

$$f(1) + 1 = f(3) \cdot 1 - 1996 = f(1) + a - 1996,$$

da cui $a = 1997$. Ricapitolando, la funzione f è definita da

$$f(n) = \begin{cases} f(1) + 1997 \cdot \frac{n-1}{2} & \text{se } n \text{ dispari} \\ 1 & \text{se } n \text{ pari} \end{cases}$$

e si controlla facilmente che le funzioni così definite, al variare di $f(1)$ in $\mathbb{N}^*$ soddisfano la condizione data.

(iii) $b \neq 0$ (e $a = 0$). Si fanno gli stessi ragionamenti del caso precedente, scambiando a con b (e $f(1)$ con $f(2)$), e si arriva alla conclusione che le funzioni cercate sono quelle del tipo

$$f(n) = \begin{cases} f(1) + 1997 \cdot \frac{n}{2} & \text{se } n \text{ pari} \\ 1 & \text{se } n \text{ dispari} \end{cases}$$

al variare di $f(1)$ in $\mathbb{N}^*$. ■

Problema 99 (IMO 1998, Taipei)**.** *Determinare il minimo valore possibile di* $f(1998)$*, dove* $f : \mathbb{N}^* \to \mathbb{N}^*$ *è una funzione tale che, per ogni* $m, n \in \mathbb{N}^*$*,*

$$f\left(n^2 f(m)\right) = m\left(f(n)\right)^2.$$

Soluzione. Sia f come nel testo, e poniamo $f(1) = b$. Allora $f(b) = f(f(1)) = f(1)^2 = b^2$, da cui, per ogni $m \in \mathbb{N}^*$,

$$f^2(m) = f(1 \cdot f(m)) = mb^2 \quad \text{e} \quad f(m^2 b) = f(m)^2.$$

In particolare (dalla identità di sinistra) f è una funzione iniettiva. Ora, per ogni $m, n \in \mathbb{N}^*$,

$$f(m)^2 f(n)^2 = f(m)^2 f(n^2 b) = f(f^2(n^2 b)m^2) = f(m^2 n^2 b^3) = f(mnb)^2,$$

quindi

$$f(m)f(n) = f(mnb). \tag{2.16}$$

In particolare, ponendo $m = 1$, si ha $f(nb) = f(n)b$.
Proviamo che $b \mid f(n)$, per ogni $n \in \mathbb{N}^*$. Sia p^v la massima potenza del primo p che divide b (cioè $v = \nu_p(q)$), e sia $n \in \mathbb{N}^*$ tale che $\alpha = \nu_p(f(n))$ sia minima possibile. Allora,

$$2\alpha = \nu_p(f(n)^2) = \nu_p(f(n^2 b)) = \nu_p(f(n^2)b) = \nu_p(f(n^2)) + v \geq \alpha + v,$$

quindi $\alpha \geq v$, il che prova che $b \mid f(n)$ per ogni $n \in \mathbb{N}^*$.
Ponendo, $f_1(n) = \frac{f(n)}{b}$, si verifica facilmente che f_1 soddisfa la condizione richiesta; inoltre $f_1(1) = 1$ e $f_1(n) \leq f(n)$ per ogni $n \in \mathbb{N}^*$, per cui possiamo supporre $f = f_1$, ovvero $b = f(i) = 1$. In tal caso, da (2.16) segue $f(nm) = f(n)f(m)$, e inoltre $f^2(n) = n$, per ogni $n, m \in \mathbb{N}^*$. In particolare, f è una biezione, e dalla condizione di moltiplicatività segue facilmente che $f(p)$ è un numero primo se e solo se p è un numero primo. Sia $\mathbb{P}$ l'insieme dei numeri primi; per quanto appena osservato f induce una permutazione σ di $\mathbb{P}$, tale che σ^2 è l'identità.
Viceversa, sia σ una permutazione di $\mathbb{P}$ tale che σ^2 è l'identità e definiamo $g : \mathbb{N}^* \to \mathbb{N}^*$ ponendo $g(1) = 1$ e, per ogni $p_1, p_2, \ldots, p_k$ (primi non necessariamente distinti)

$$g(p_1 p_2 \cdots p_k) = p_{\sigma(1)} p_{\sigma(2)} \cdots p_{\sigma(k)}.$$

Chiaramente, $g^2(n) = n$ e $g(nm) = g(n)g(m)$ per ogni $n, m \in \mathbb{N}$; quindi

$$g(n^2 g(m)) = g(n)^2 g^2(m) = mg(n)^2$$

e g soddisfa la condizione.

Venendo alla domanda specifica: dato che $1998 = 2 \cdot 3^3 \cdot 37$, il valore minimo di $g(1998)$ si ottiene considerando la permutazione σ tale che $\sigma(2) = 3, \sigma(3) = 2, \sigma(37) = 5$ e $\sigma(5) = 37$, per cui $g(1998) = 3 \cdot 2^3 \cdot 5 = 120$ che è la risposta al quesito. ■

Ultimo gruppo di problemi da risolvere, alcuni piuttosto difficili.

Problema 100 (Balkan M.O. 2017)**.** *Trovare tutte le funzioni* $f : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ *tali che*

$$n + f(m) \mid f(n) + nf(m)$$

per ogni $m, n \in \mathbb{N}^*$.

Problema 101 (Spagna 2002)**.** *Determinare tutte le funzioni* $f : \mathbb{N}^* \to \mathbb{N}^*$ *che sono strettamente crescenti (cioè* $m < n \Rightarrow f(m) < f(n)$ *per ogni* $m, n \in \mathbb{N}^*$*) e tali che*

$$f(n + f(n)) = 2f(n)$$

per ogni intero positivo n.

Problema 102 (Vietnam 1997)**.** *Dire quante sono le funzioni* $f : \mathbb{N}^* \to \mathbb{N}^*$ *che soddisfano:*

$$\text{(i) } f(1) = 1, \qquad \text{(ii) } f(n)f(n+2) = f(n+1)^2 + 1997,$$

per ogni $n \in \mathbb{N}^*$.

Problema 103 (Bulgaria 2014)**.** *Siano* $\mathbb{Q}^+$ *e* $\mathbb{R}^+$*, rispettivamente, l'insieme dei numeri razionali positivi e quello dei numeri reali positivi. Trovare tutte le funzioni* $f : \mathbb{Q}^+ \to \mathbb{R}^+$ *tali che*

$$f(xy) = f(x + y)(f(x) + f(y))$$

per ogni $x, y \in \mathbb{Q}^+$.

Problema 104 (IMO, 2010)**.** *Trovare tutte le funzioni* $g : \mathbb{N}^* \to \mathbb{N}^*$ *tali che*

$$(g(m) + n)\,(g(n) + m)$$

è un quadrato intero per ogni $m, n \in \mathbb{N}^*$.

Soluzioni.

Problema 81. Sia $f : \mathbb{R} \to \mathbb{R}$ che soddisfa la condizione data. Chiaramente f non è la funzione costante 0; sia $u \in \mathbb{R}$ tale che $f(u) \neq 0$, allora $f(0)f(u) = f(u) + 0 = f(u)$, e dunque $f(0) = 1$. Ma allora $f(1)f(-1) = f(0) - 1 = 0$ e quindi $f(1) = 0$ oppure $f(-1) = 0$. Sia $f(1) = 0$; allora per ogni $x \in \mathbb{R}$,

$$f(x) = f(x - 1 + 1) = f(x - 1)f(1) - (x - 1) = 1 - x.$$

Questa funzione soddisfa la condizione; infatti, per ogni $x, y \in \mathbb{R}$,

$$f(x)f(y) = (1 - x)(1 - y) = 1 - (x + y) + xy = f(x + y) + xy.$$

Se $f(-1) = 0$ si ha, per ogni $x \in \mathbb{R}$,

$$f(x) = f(x+1-1) = f(x+1)f(-1) + (x+1) = x+1;$$

e anche questa funzione soddisfa la condizione voluta. La soluzione è completata.

* * *

PROBLEMA 82. Sia $f : \mathbb{R} \to \mathbb{R}$ con la proprietà richiesta, e sia $b = f^2(0) = f(f(0))$. Allora, per ogni $x \in \mathbb{R}$, ponendo nell'equazione $y = x$, si ha $b = f(x)^2 - x^2$; quindi

$$f(x)^2 = x^2 + b$$

per ogni $x \in \mathbb{R}$. In particolare, $f(0)^2 = b$ e, per $x = f(0)$,

$$b^2 = f(f(0))^2 = f(0)^2 + b = 2b.$$

Dunque, $b = 0$ (e $f(0) = 0$) oppure $b = 2$.
Nel primo caso $f(x)^2 - x^2$ per ogni $x \in \mathbb{R}$, quindi $f(x) = \pm x$. Supponiamo $f(x) = x$; allora dall'equazione (con $y = 0$) si ricava la contraddizione

$$x = f(f(x)) = -f(x) = -x;$$

dunque, in questo caso, $f(x) = -x$ per ogni $x \in \mathbb{R}$, e questa funzione soddisfa la proprietà.
Caso $b = 2$. In questo caso $c = f(0) = \pm\sqrt{2}$. Inoltre, per ogni $x \in \mathbb{R}$, $f(x)^2 = x^2 + 2$ e $f^2(x)^2 = f(x)^2 + 2 = x^2 + 4$. Sostituendo nell'equazione $x = \sqrt{2}$, $y = 0$,

$$f^2(\sqrt{2}) + f(\sqrt{2}) = f(\sqrt{2})c + c;$$

quindi, tenendo conto che $f(\sqrt{2}) = \pm\sqrt{2+2} = \pm 2$ e $f^2(\sqrt{2}) = \pm\sqrt{2+4} = \pm\sqrt{6}$, ed elevando al quadrato:

$$10 \pm 4\sqrt{6} = (5 \pm 4)c^2 = (5 \pm 4)2,$$

che è chiaramente un assurdo.
Dunque, l'unica soluzione rimane la funzione $f(x) = -x$, per ogni $x \in \mathbb{R}$.

* * *

PROBLEMA 83. Sia $f : \mathbb{R}^+ \to \mathbb{R}^+$ che soddisfa la condizione posta, e siano $x, y \in \mathbb{R}$ con $0 < x < y$. Allora

$$\big(1 + (y-x)f(x)\big)\big(1 - (y-x)f(y)\big) = 1,$$

e svolgendo il prodotto si trova

$$(y-x)f(x) - (y-x)f(y) = (y-x)^2 f(x)f(y)$$

da cui

$$\frac{1}{f(y)} - \frac{1}{f(x)} = y - x. \tag{2.17}$$

Sia $a \in \mathbb{R}^+$; se $x < 1$ poniamo in (2.17) $(x, y) = (a, 1)$, se invece $a > 1$ poniamo $(x, y) = (1, a)$. Sosituendo in ogni caso si ottiene,

$$\frac{1}{f(a)} - a = \frac{1}{f(1)} - 1.$$

Posto $C = \frac{1}{f(1)} - 1$, si ricava, per ogni $1 \neq a \in \mathbb{R}^+$,

$$f(a) = \frac{1}{a + C},$$

che chiaramente vale anche per $a = 1$, e definisce una funzione $\mathbb{R}^+ \to \mathbb{R}^+$ se e solo se $C \geq 0$. In tali casi si verifica facilmente che la funzione è una soluzione.

* * *

PROBLEMA 84. Sia $f : \mathbb{R} \to \mathbb{R}$ una funzione che soddisfa la condizione posta. Da questa, ponendo $x = y = 0$, si deduce subito $f(0) = 0$. Con $x \in \mathbb{R}$ e $y = 0$ si ottiene quindi:

$$f(x^3) = xf(x^2),$$

che consente di riscrivere l'uguaglianza come

$$xf(x^2) + yf(y^2) = (x + y)(f(x^2) + f(y^2) - f(xy)),$$

da cui, per ogni $x, y \in \mathbb{R}$,

$$xf(y^2) + yf(x^2) = (x + y)f(xy). \tag{2.18}$$

Sia $0 < a \in \mathbb{R}$; ponendo $x = \sqrt{a}$, $y = \sqrt{a^3}$ in (2.18)

$$\sqrt{a}f(a^3) + \sqrt{a^3}f(a) = (\sqrt{a} + \sqrt{a^3})f(a^2),$$

da cui, tenendo conto che $f(a^3) = af(a^2)$,

$$\sqrt{a^3}f(a^2) + \sqrt{a^3}f(a) = \sqrt{a}f(a^2) + \sqrt{a^3}f(a^2),$$

ottenendo quindi, per ogni $a > 0$,

$$f(a^2) = af(a).$$

Sostituendo in (2.18) $(x, y) = (a, 1)$,

$$af(1) + af(a) = (a + 1)f(a);$$

concludendo che $f(a) = f(1)a$ per ogni $0 \leq a \in \mathbb{R}$.
Questo implica che per ogni $x \in \mathbb{R}$, ponendo $y = \sqrt[3]{x}$,

$$f(x) = f(y^3) = yf(y^2) = f(1)y^3 = f(1)x$$

In conclusione, la funzione f è data da $f(x) = f(1)x$, per ogni $x \in \mathbb{R}$, che si verifica subito soddisfare la condizione data.

* * *

PROBLEMA 85. Sia $f : \mathbb{R} \to \mathbb{R}$ come nel testo, e siano $x, y \in \mathbb{R}$ tali che $f(x) = f(y)$; allora

$$x^2 - x + 1 = y^2 - y + 1$$

da cui segue $y = x$ oppure $y = 1 - x$. Poniamo $b = f(0)$. Allora, $f(b) = f^2(0) = 1$ e anche

$$f(b^2 - b + 1) = f(f^2(b)) = f^2(f(b)) = f^2(1) = 1.$$

Quindi, per quanto osservato, $b^2 - b + 1 = b$ oppure $b^2 - b + 1 = 1 - b$; nel primo caso $b = 1$, nel secondo $b = 0$.

* * *

PROBLEMA 86. Supponiamo, per assurdo, che $f : \mathbb{R} \to \mathbb{R}$ sia tale che $f^2(x)) + xf(x) = 1$ per ogni $x \in \mathbb{R}$, e sia $b = f(0)$. Allora $1 = f^2(0) = f(b)$; inoltre $b \neq 0$, perché se così fosse si avrebbe $f^2(0) = 0$. Ora

$$f(1) = f^2(b) = 1 - bf(b) = 1 - b,$$

quindi $f^2(1) = 1 - f(1) = b$. Ma allora

$$f(1)b = f(1)f^2(1) = 1 - f^3(1) = 1 - f(b) = 0,$$

e poiché $b \neq 0$, $0 = f(1) = 1 - b$, quindi $b = 1$, il che conduce all'assurdo

$$1 = f^2(0) + 0f(0) = f(1) = 0.$$

* * *

PROBLEMA 90. Sia $f : \mathbb{N}^* \to \mathbb{N}^*$ con la proprietà richiesta. Poiché f è suriettiva, si ha $f(1) \mid n$ per ogni $n \in \mathbb{N}^*$, e dunque $f(1) = 1$. Osserviamo anche che la condizione posta implica che f è iniettiva (dunque una biezione).
Sia $\mathbb{P}$ l'insieme di tutti i numeri primi positivi. Da quanto detto, segue facilmente che per ogni $p \in \mathbb{N}^*$, $p \in \mathbb{P}$ se e solo se $f(p) \in \mathbb{P}$. Quindi la restrizione di f a $\mathbb{P}$ è una biezione.
Un'altra facile conseguenza della condizione e del fatto che f è una biezione è che, se m, n sono interi coprimi, allora

$$f(mn) = f(m)f(n).$$

Infatti $f(m)$ ed $f(n)$ sono entrambi divisori di $f(mn)$ e sono coprimi per la condizione, dunque $b = f(m)f(n) \mid f(mn)$; essendo f suriettiva, $b = f(k)$ per qualche $k \in \mathbb{N}^*$, con $k \mid mn$; ma allora m e n dividono k, per cui $mn \mid k$ e $k = mn$. Infine, proviamo, per induzione su n, che per ogni primo p ed $n \geq 1$, $f(p^n) = f(p)^n$; questo è dato per $n = 1$, per $n \geq 2$, $f(p^{n-1}) = f(p)^{n-1}$ per ipotesi induttiva, da cui $f(p^n) = f(p)^{n-1}q$ con $q = f(k) \in \mathbb{N}$, e $k \mid p$ ovvero $k = p^t$ (per $t \geq 1$)' segue subito $t = 1$ e pertanto $ff(p^n) = f(p)^n$.
In conclusione, $f(1) = 1$, e se $n = p_1p_2 \cdots p_n$, con $p_1, \ldots, p_t$ primi, allora

$$f(n) = f(p_1)f(p_2) \cdots f(p_n).$$

Viceversa, se $\pi : \mathbb{P} \to \mathbb{P}$ una biezione (quindi una permutazione di $\mathbb{P}$), si verifica facilmente che la funzione $f : \mathbb{N}^* \to \mathbb{N}^*$, definita da $f(1) = 1$ e

$$f(p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}) = \pi(p_1)^{k_1} \pi(p_2)^{k_2} \cdots \pi(p_t^{k_t}),$$

soddisfa la condizione richiesta.

* * *

PROBLEMA 91. Per $n = 1$ si ha $0 < f(1)f^2(1) < 2$, da cui $f(1) = 1$.
Proviamo che $f(n) \geq n$ per ogni $n \in \mathbb{N}^*$; supponiamo che ciò si falso e sia n minimo tale che $f(n) < n$; allora $n > 1$ e $f^2(n) = f(f(n)) \geq f(n)$; quindi

$$(n-1)^2 < f(n)f(f(n)) \leq f(n)^2$$

da cui la contraddizione $n > f(n) > n - 1$.
Supponiamo ora che esista $n \in \mathbb{N}^*$ tale che $f(n) > n$; allora

$$n^2 + n > f(n)f(f(n)) \geq (n+1)f(n) \geq (n+1)n = n^2 + n,$$

che ancora è assurdo. In conclusione si deve avere $f(n) = n$ per ogni $n \in \mathbb{N}^*$, cioè f è la funzione identica, che si verifica banalmente soddisfare la condizione data.

* * *

PROBLEMA 92. Osserviamo che la funzione identica $f(n) = n$ soddisfa la condizione. Viceversa, sia f una funzione con la proprietà richiesta. Ponendo $m = f(n)$ si ha

$$f(n)^2 + f(n) \mid f^2(n)f(n) + n$$

per ogni $n \in \mathbb{N}^*$; in particolare, $f(n) \mid n$, e dunque $f(n) \leq n$, per ogni $n \in \mathbb{N}^*$. Applicato a $n = 1$ si ha $f(1) = 1$. In generale, per $m \in \mathbb{N}^*$ si ha (con $n = 1$)

$$m^2 + 1 \mid mf(m) + 1$$

e quindi $m^2 + 1 \leq mf(m) + 1 \leq m \cdot m + 1$; dunque $m^2 = mf(m)$ da cui $f(m) = m$.

* * *

PROBLEMA 93. Sia $f : \mathbb{N}^* \to \mathbb{N}^*$ con la proprietà richiesta. Ponendo nell'equazione $m = 1$ si trova, per ogni $n \in \mathbb{N}^*$,

$$f(n+1) = (f(1) - 1)f(n) + 1. \tag{2.19}$$

Se $f(1) = 1$, risulta quindi $f(n) = 1$ per ogni $n \in \mathbb{N}^*$, e questa funzione costante soddisfa infatti la condizione.
Sia $f(1) > 1$ e poniamo $b = f(1) - 1$; dall'identità (2.19) si dimostra mediante una facile induzione, che per ogni $n \in \mathbb{N}^*$,

$$f(n) = b^n + b^{n-1} + \ldots + b + 1. \tag{2.20}$$

In particolare $f(4) = b^4+b^3+b^2+b+1$. Per un altro verso, dall'equazione che caratterizza f segue

$$2f(4) = f(2\cdot 2) + f(2+2) = f(2)^2 + 1 = (b^2+b+1)^2 + 1.$$

Uguagliando le due espressioni,

$$2(b^4+b^3+b^2+b+1) = (b^2+b+1)^2 + 1,$$

si ricava $b^4 = b^2$, da cui, poiché $b \geq 0$: $b = 0$ oppure $b = 1$. Nel primo caso, $f(1) = 1$, che abbiamo già visto portare alla funzione cotante $f(n) = 1$. Nel secondo caso, da (2.20) si ricava

$$f(n) = 1^n + 1^{n-1} + \ldots + 1 = n+1$$

per ogni $n \in \mathbb{N}^*$, che si verifica definisce una funzione che soddisfa la condizione.

* * *

Problema 94. Supponiamo, per assurdo, che esista $f : \mathbb{N}^* \to \mathbb{N}^*$, e poniamo $b = f(1)$. Proviamo che, per ogni $n \in \mathbb{N}^*$, $f(n) = b+n = 1$. Questo è vero per definizione per $n = 1$; procedendo per induzione supponiamo $f(n) = b+n-1$; allora

$$f(n+1) = f(f^2(n)) = f^2(f(n)) = f(n)+1 = b+n-1+1 = b+(n+1)-1,$$

e l'affermazione è provata. Se $b = 1$, allora, per ogni $n \in \mathbb{N}^*$, $f(n) = n$ e la contraddizione $n = f(f(n)) = n+1$. Quindi $b \geq 2$ e, per quanto già provato,

$$b = f(f(b-1)) = f(2b-2) = 3b-3$$

da cui $b = 3/2$. Che non è possibile.

Nota. Variazioni sullo stesso tema, sono

[IMO 1987]: *provare che non esiste* $f : \mathbb{N} \to \mathbb{N}$ *tale che* $f(f(n)) = n+1987$ *per ogni* $n \in \mathbb{N}$.

[Slovenia 1997]: *trovare tutte le funzioni* $f : \mathbb{Z} \to \mathbb{Z}$ *tali che* $f(f(n)) = n+1$ *per ogni* $n \in \mathbb{Z}$.

A questo punto, viene naturale porsi l'obiettivo seguente: *trovare tutte le funzioni* $f : \mathbb{Q} \to \mathbb{Q}$ *tali che* $f(f(x)) = x+1$ *per ogni* $x \in \mathbb{Q}$.

* * *

Problema 95. Sia $f : \mathbb{N} \to \mathbb{Z}$ la funzione definita da, per ogni $n \in \mathbb{N}$,

$$f(n) = -f\left(\left\lfloor \frac{n}{3} \right\rfloor\right) - 3\left\{\frac{n}{3}\right\}.$$

Sia $n = 3q+r$, con $q, r \in \mathbb{N}$, $0 \leq r \leq 2$; allora $\lfloor n/3 \rfloor = q$ e $\{n/3\} = r/3$, quindi

$$f(n) = -f(q) - r.$$

Chiaramente, $f(0) = 0$. Sia $1 \leq n \in \mathbb{N}$ e sia

$$n = a_k 3^k + \ldots + a_1 3 + a_0$$

la scrittura in base 3 di n, con $k \geq 1$, $a_i \in \{0,1,2\}$ per $i = 0, \ldots, k$, e $a_k \neq 0$. Proviamo che

$$f(n) = \sum_{i=o}^{k} (-1)^{i+1} a_i. \tag{2.21}$$

Questo è chiaramente vero per $0 \leq n \leq 2$. Sia $n \geq 3$, allora $n = (a_k 3^{k-1} + \ldots + a_1)3 + a_0$; quindi, per quanto osservato all'inizio ed assumendo l'ipotesi induttiva

$$f(n) = -f(a_k 3^{k-1} + \ldots + a_1) - a_0 = -\sum_{i=1}^{k} (-1)^i a_i - a_0 = \sum_{i=o}^{k} (-1)^{i+1} a_i.$$

Dunque la (2.21) è provata. A questo punto, non è difficile vedere che il minimo n per cui $f(n) = 2010$ si realizza quando, nella scrittura in base 3 di n, tutte le cifre di posto dispari sono 2, quelle di posto pari 0. Quindi

$$n = \sum_{i=0}^{1004} 2 \cdot 3^{2i+1}$$

è il numero cercato.

* * *

Problema 96. Sia $f : \mathbb{N}^* \to \mathbb{N}$ tale che $f(2) = 0, f(3) > 0, f(9999) = 3333$, e

$$f(m) + f(n) \leq f(m+n) \leq f(m) + f(n) + 1,$$

per ogni $m, n \in \mathbb{N}^*$. Chiaramente, f è crescente (cioè $f(n+1) \geq f(n)$ per ogni $n \in \mathbb{N}^*$); da $f(2) = 0$ segue dunque $f(1) = 0$. Quindi $0 = f(2) + f(1) \leq f(3) \leq 1$ e dunque, dalla condizione $f(3) > 0$ si ricava $f(3) = 1$.
Osserviamo poi che per ogni $k, n \in \mathbb{N}^*$ si ha $f(kn) \geq k \cdot f(n)$. Infatti, questo è banale per $k = 1$ e, procedendo per induzione, per $k \geq 2$,

$$f(kn) = f((k-1)n + n) \geq f((k-1)n) + f(n) \geq (k-1)f(n) + f(n) = kf(n).$$

In particolare, $f(3n) \geq nf(3) \geq n$ per ogni $n \in \mathbb{N}^*$.
Posto $M = 3333$, proviamo che, per ogni $1 \leq m \leq M$,

$$f(3m) = m. \tag{2.22}$$

Questo è vero per $m = 1$ e, per ipotesi, per $m = M = 3333$. Dato un generico $1 \leq m \leq M$, per quanto osservato prima, si ha $f(3m) \geq 3f(m) \geq$

$$m \leq f(3m) \leq f(3M) - f(3M - 3m) = M - f(3(M-m)) \leq M - (M-m) = m,$$

e quindi la (2.22). Proviamo ora che, per ogni $1 \leq n \leq M$

$$f(n) = \left\lfloor \frac{n}{3} \right\rfloor.$$

Scriviamo $n = 3q + r$ con $q \in \mathbb{N}$ e $r \in \{0, 1, 2\}$. Se $r = 0$ allora, come abbiamo appena visto $f(n) = q = \frac{n}{3}$. Sia $r = 1, 2$ e supponiamo per assurdo $f(n) \neq q = \lfloor \frac{n}{3} \rfloor$. Dunque

$$f(n) = 1 + f(3q) + f(r) = 1 + q + 0 = 1 + q;$$

ma allora, da (2.22) segue la contraddizione

$$n = f(3n) = 3f(n) = 3q + 3 > 3q + r = n.$$

Dunque, $f(n) = \lfloor n/3 \rfloor$ per ogni $1 \leq n \leq 3333$. In particolare, $f(1982) = \lfloor \frac{1982}{3} \rfloor = 660$.

* * *

PROBLEMA 100. Sia $f : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ tali che per ogni $m, n \in \mathbb{N}^*$,

$$n + f(m) \mid f(n) + nf(m).$$

Allora, ponendo $m = n = 1$, $1 + f(1) \mid 2f(1)$, da cui segue $f(1) = 1$. Notiamo anche il seguente fatto

($*$) *Sia $m \in \mathbb{N}^*$ tale che $f(m) \neq 1$, allora $f(m) > m + 1$.*

Infatti, poiché $1 = f(1)$, si ha $1 + m \mid f(m) + m$, quindi

$$1 + m \mid f(m) + m - (1 + m) = f(m) - 1$$

perciò, se $f(m) \neq m$, $1 + m \leq f(m) - 1$ da cui ($*$).

Osserviamo a questo punto che la funzione costante $n \mapsto 1$ e la funzione definita da $n \mapsto n^2$, per ogni $n \in \mathbb{N}^*$, soddisfano la condizione. Proviamo che non ve ne sono altre. Sia quindi $f : \mathbb{N}^* \to \mathbb{N}^*$ che soddisfa la condizione e tale che esiste $n \in \mathbb{N}^*$ con $f(n) \neq n^2$ (osserviamo che $n \neq 1$). Allora, per ogni $m \in \mathbb{N}^*$,

$$n + f(m) \mid f(n) + nf(m) - n(n + f(m)) = f(n) - n^2,$$

in particolare, $n + f(m) \leq |f(n) - n^2|$, per ogni $m \in \mathbb{N}^*$. Dunque,

$$f(m) < C = |f(n) - n^2| \text{ per ogni } m \in \mathbb{N}^*.$$

Sia $m \in \mathbb{N}^*$, e poniamo $k = Cf(m)$; poiché $f(k) < C \leq k$, da ($*$) segue $f(k) = 1$. Ma allora

$$(C + 1)f(m) = k + f(m) \mid f(k) + kf(m) = 1 + kf(m),$$

dunque $f(m) = 1$. Questo prova che f è la funzione costante 1, e completa la soluzione.

* * *

PROBLEMA 101. Sia $f : \mathbb{N}^* \to \mathbb{N}^*$ strettamente crescente e tale che, per ogni $n \in \mathbb{N}^*$,

$$f(n + f(n)) = 2f(n).$$

L'ipotesi che f sia strettamente crescente imlpica che, per ogni $m, n \in \mathbb{N}^*$ con $n \geq m$, $f(n) - f(m) \geq n - m$, e quindi

$$f(n) - n \geq f(m) - m.$$

Poniamo $a = f(1)$ e, per ogni $m \in \mathbb{N}$, $b_m = 1 + (2^m - 1)a$. Proviamo, per induzione su m che

$$f(b_m) = 2b_m = b_m + (a - 1). \tag{2.23}$$

L'asserto è infatti vero per definizione per $b_0 = 1$. Sia $m \geq 0$, allora, per l'ipotesi induttiva e la proprietà della funzione f,

$$f(b_{m+1}) = f(b_m + 2^a b_m) = f(b_m + f(b_m)) = 2f(b_m) = 2^{m+1}a,$$

e dunque (2.23) è provata. Dato ora $n \in \mathbb{N}^*$ esiste un unico $b \geq 0$ tale che $b_m \leq n < b_{m+1}$. Per quanto osservato all'inizio, si ha

$$a - 1 = f(b_m) - b_m \leq f(n) - n \leq f(b_{m+1}) - b_{m+1} = a - 1,$$

quindi $f(n) = n + (a - 1)$.

Viceversa, se $c \in \mathbb{N}$ la funzione $f_c : \mathbb{N}^*\mathbb{N}^*$, definita da $f(n) = n+c$, è strettamente crescente e per ogni $n \in \mathbb{N}^*$,

$$f_c(n + f_c(n)) = f_c(2n + a) = 2n + 2a = 2(f_c(n)).$$

La soluzione al problema è pertanto $f = f_c$ per qualche numero intero c.

* * *

Problema 102. Problema 102. Cominciamo considerando funzioni $f : \mathbb{N}^* \to \mathbb{Q}^+$ tali che $f(1) = 1$ e

$$f(n)f(n + 2) = f(n + 1)^2 + 1997, \tag{2.24}$$

per ogni $n \in \mathbb{N}^*$. Fissato $b \in \mathbb{N}^*$, le relazioni (2.24) definiscono ricorsivamente un'unica funzione $f_b : \mathbb{N}^* \to \mathbb{Q}^+$ mediante $f_b(1) = 1$, $f_b(2) = b$ e, per ogni $n \geq 3$,

$$f_b(n) = \frac{f_b(n - 1)^2 + 1997}{f_b(n - 2)}. \tag{2.25}$$

Poiché tale funzione verifica (2.24) per costruzione, il problema si risolve determinando per quanti valori di $b \in \mathbb{N}^*$, la funzione f_b assume tutti valori interi. Scriviamo $f = f_b$ e, per comodità, $p = 1997$ (che è un numero primo). Da (2.25) si ricava

$$f(3) = b^2 + p, \qquad f(4) = \frac{f(3)^2 + p}{b} = \frac{(b^2 + p)^2 + p}{b},$$

quindi

$$f(5) = \frac{f(4)^2 + p}{f(3)} = \frac{f(3)^4 + 2pf(3)^2 + p^2 + b^2p}{b^2f(3)} = \frac{f(3)^3 + 2pf(3) + p}{b^2},$$

che è un intero se e solo se b^2 divide $f(3)^3 + 2pf(3) + p = (b^2 + p)^3 + 2p(b^2 + p) + p$, il che si verifica se e solo se

$$b^2 \mid p^3 + 2p^2 + p = p(p + 1)^2.$$

Poiché p è un numero primo, concludiamo che $f(5) = f_b(5) \in \mathbb{N}^*$ se e solo se $b \mid p + 1$.

Verifichiamo ora che, viceversa, se $b \mid p+1$ allora $f(n) = f_b(n)$ è un intero positivo per ogni $n \in \mathbb{N}^*$. Ora, per dato $n \in \mathbb{N}^*$, $n \geq 2$, si ha

$$\frac{f(n+2)+f(n)}{f(n+1)} = \frac{f(n+1)^2+p+f(n)^2}{f(n+1)f(n)} = \frac{f(n+1)^2+f(n+1)f(n-1)}{f(n+1)f(n)}$$

dunque

$$\frac{f(n+2)+f(n)}{f(n+1)} = \frac{f(n+1)+f(n-1)}{f(n)},$$

per cui, iterando il passaggio (o facendo induzione) si ricava che, per ogni $n \in \mathbb{N}^*$,

$$\frac{f(n+2)+f(n)}{f(n+1)} = \frac{f(3)+f(1)}{f(2)} = \frac{b^2+p+1}{p} = b+m$$

dove $mb = p+1$. Quindi $f(n+2) = f(n+1)(b+m)+f(n)$, e da ciò segue facilmente per induzione che, se m è un intero (cioè se $b \mid p+1$), $f(n)$ è un intero per ogni $n \in \mathbb{N}^*$.

In conclusione, il numero di funzioni che soddisfano le condizioni del problema è uguale al numero di divisori distinti di $p+1 = 1998$. Con un po' di conti (oppure consultando il prossimo capitolo) si trova che tale numero è 16.

* * *

PROBLEMA 103. $f : \mathbb{Q}^+ \to \mathbb{R}^+$ tali che, per ogni $x, y \in \mathbb{Q}^+$,

$$f(xy) = f(x+y)(f(x)+f(y)).$$

Poniamo $b = f(1)$ e, per ogni $x \in \mathbb{Q}^+$, $g(x) = f(x)^{-1}$. La funzione g verifica

$$g(xy)(g(x)+g(y)) = g(x+y)g(x)g(y), \tag{2.26}$$

per ogni $x, y \in \mathbb{Q}^+$. In particolare, per ogni $x \in \mathbb{Q}^+$,

$$g(x)(g(x)+g(1)) = g(x+1)g(x)g(1),$$

ovvero $g(x)+b^{-1} = g(x+1)b^{-1}$, e dunque

$$g(x+1) = 1+bg(x)$$

Con una semplice induzione segue che, per ogni $x \in \mathbb{Q}^+$ e ogni $n \in \mathbb{N}^*$,

$$g(x+n) = 1+b+\ldots+b^{n-1}+b^n g(x). \tag{2.27}$$

Partendo da $g(1) = b^{-1}$ si trova che per ogni $n \in \mathbb{N}^*$,

$$g(n) = 1+b+\ldots+b^{n-3}+2b^{n-2},$$

(si osservi, $g(2) = 2$), In particolare

$$g(6) = 1+b+b^2+b^3+2b^4. \tag{2.28}$$

D'altra parte, da (2.29) si ha

$$g(6) = g(2 \cdot 3) = \frac{g(5)g(2)g(3)}{g(2) + g(3)} = \frac{(1 + b + b^2 + 2b^3)2g(1 + 2b)}{3 + 2b}. \tag{2.29}$$

Confrontando le espressioni per $g(6)$ date da (2.28) e (2.29), con qualche calcolo, si ricava $b = 1$.
Dunque $f(1) = g(1) = 1$. Da (2.27) segue allora, per ogni $n \in \mathbb{N}^*$,

$$g(n) = n.$$

Applicando (2.26) e (2.27) su ricava, per ogni $n \in \mathbb{N}^*$,

$$n + g(n^{-1}) = g(n) + g(n^{-1}) = g(n + n^{-1})g(n)g(n^{-1}) = (n + g(n^{-1}))ng(n^{-1}),$$

per cui, ponendo $t = g(n^{-1})$,

$$nt^2 + (n^2 - 1)t - n = 0,$$

che, risolta in t (e mantenendo solo la soluzione positiva), fornisce

$$g(n^{-1}) = n^{-1}.$$

Infine, sia $\frac{m}{n} \in \mathbb{Q}^+$, con $m, n \in \mathbb{N}^*$; da (2.26) e quanto provato sinora, si ricava

$$g\Big(\frac{m}{n}\Big)\Big(m + \frac{1}{n}\Big) = g\Big(m + \frac{1}{n}\Big)m \cdot \frac{1}{n} = \Big(m + \frac{1}{n}\Big)\frac{m}{n}$$

da cui

$$g\Big(\frac{m}{n}\Big) = \frac{m}{n}.$$

In conclusione g è la funzione identica $g(x) = x$, per ogni $x \in \mathbb{Q}^+$, e quindi f è la funzione reciproca: $f(x) = x^{-1}$ per ogni $x \in \mathbb{Q}^+$.

* * *

PROBLEMA 104. Siano x, y numeri interi con $x \geq y$, e p un numero primo che divide $x - y$; allora $x = y + p^k b$, con $k \geq 1$ e p non divide b. Se $k = 1$, scegliamo $t \geq 2$, t dispari e tale che $p^t b > x$, e poniamo $a = p^t b - x$; allora

$$\nu_p(a + y) = \nu_p(p^t b - pb) = 1, \quad \text{e} \quad \nu_p(a + x) = \nu_p(p^t b) = t.$$

Se $k \geq 2$, si prende $t \geq k$ tale che $p^t \geq x$ e si pone $a = p^t + p - x$; allora,

$$\nu_p(a + y) = \nu_p(p^t + p - p^k b) = 1, \quad \text{e} \quad \nu_p(a + x) = \nu_p(p^t + p) = 1.$$

Abbiamo dunque provato che se $x, y \in \mathbb{N}^*$ sono tali che $x \equiv y \pmod{p}$, con p un primo, allora esiste un intero positivo a tale che $\nu_p(a + x)$ e $\nu_p(a + y)$ sono entrambi dispari.

Veniamo ora al problema. Sia $g : \mathbb{N}^* \to \mathbb{N}^*$ tale che

$$(g(m) + n)\,(g(n) + m)$$

è un quadrato intero per ogni $m, n \in \mathbb{N}^*$. Sia $n \in \mathbb{N}^*$; se, per assurdo, $g(n) = g(n+1) = b$, dalla condizione su g si avrebbe che $(b+n)(b+n+1)$ è un quadrato, e questo è impossibile perchè $b+n$ e $b+n+1$ sono coprimi e non possono essere entrambi quadrati interi. Dunque

$$g(n+1) \neq g(n)$$

per ogni $n \in \mathbb{N}^*$. Supponiamo ora (ancora per assurdo) che esiste un divisore primo p di $g(n+1) - g(n)$. Per quanto provato sopra, esiste $a \in \mathbb{N}^*$ tale che $\nu_p(a + g(n))$ e $\nu_p(a + g(n+1))$ sono entrambi dispari. Allora, dalla condizione che $(a + g(n))(n + g(a))$ e $(a + g(n+1))(n + 1 + g(a))$ sono entrambi quadrati, segue che p divide $n + g(a)$ e divide $n + 1 + g(a)$, da cui l'assurdo

$$p \mid (n + 1 + g(a)) - (n + g(a)) = 1.$$

Dunque, $|g(n+1) - g(n)| = 1$ per ogni $n \in \mathbb{N}^*$.
Ancora, supponiamo che per qualche $n \in \mathbb{N}^*$ $g(n+1) = g(n) - 1$, allora

$$(g(n) + n + 1)(g(n+1) + n) = (g(n) + n + 1)(g(n) + n - 1) = (g(n) + n)^2 - 1$$

che non è un quadrato. In conclusione, per ogni $n \in \mathbb{N}^*$,

$$g(n+1) = g(n) + 1,$$

da cui segue facilmente $g(n) = n + (g(1) - 1)$, per ogni $n \in \mathbb{N}^*$.
Viceversa, fissato $b \in \mathbb{N}$, la funzione definita da $f(n) = n + b$, per ogni $n \in \mathbb{N}^*$, sodisfa la condizione richiesta.

3

Funzioni moltiplicative

In questo capitolo definiamo e studiamo altre funzioni definite su $\mathbb{N}$, che sono fondamentali in Teoria dei Numeri. Come introduzione, discutiamo un problema classico di quella che viene chiamata 'matematica ricreativa'.

Problema 105. *Le celle di una prigione sono numerate da* 1 *a* 100 *e le loro porte sono controllate da un pulsante centrale. Quando viene premuto, il pulsante attiva alcune delle porte, aprendole se sono chiuse, chiudendole se aperte. Partendo dallo stato in cui tutte le porte sono chiuse il pulsante viene premuto* 100 *volte, attivando alla k-esima pressione tutte e sole le porte che sono numerate con un multiplo di k. Quali porte saranno aperte alla fine?*

Soluzione. La porta numerata con n (per $1 \leq n \leq 100$) si attiva un numero di volte pari al numero di divisori positivi di n, numero che si denota con $\tau(n)$; poiché la porta è inizialmente chiusa, sarà alla fine aperta se e solo se $\tau(n)$ è dispari. Ora, si verifica (per il momento direttamente) che l'insieme dei numeri $1 \leq n \leq 100$ che hanno un numero dispari di divisori positivi è $\{1, 4, 9, 16, 25, 36, 49, 64, 81, 100\}$. Le porte numerate con uno di tali numeri saranno al termine aperte, tutte le altre chiuse. ∎

Oltre ad esemplificare quelle tante situazioni in cui risulta fondamentale assumere fin dalla partenza il giusto punto di vista (cosa non troppo difficile in questo caso), questo problema evidenzia l'utilità che potrebbe avere una conoscenza più generale delle proprietà e dei valori della funzione $\tau(n)$, che eviti di dover eseguire ogni volta lunghe verifiche dirette. Questo è quello che, in parte, faremo nella prima sezione del capitolo.

3.1. Funzioni moltiplicative

Definizione. Una funzione $f : \mathbb{N}^* \to \mathbb{C}$, si dice *moltiplicativa*[1] se $f(1) \neq 0$ e, per ogni $n, m \in \mathbb{N}^*$,

$$\mathrm{mcd}(n, m) = 1 \quad \Rightarrow \quad f(nm) = f(n)f(m). \tag{3.1}$$

[1] Nei casi che esamineremo il codominio sarà di fatto $\mathbb{N}$; d'altra parte, le proprietà generali sono facilmente estendibili al caso in cui il codominio della funzione è un dominio d'integrità qualsivoglia.

Osserviamo subito che se f è una funzione moltiplicativa, $f(1) = 1$. Infatti, da (3.1) segue $f(1) = f(1)f(1)$ e poiché $f(1) \neq 0$, ciò implica $f(1) = 1$.

ESEMPI. Sono moltiplicative la funzione costante $f(n) = 1$, e la funzione identica $f(n) = n$.

Definiamo ora formalmente le funzioni che ci interessano per prime. Sia $n \in \mathbb{N}^*$, si pone

$$\begin{aligned} \tau(n) &= \text{ numero di divisori positivi di } n \\ \sigma(n) &= \text{ somma dei divisori positivi di } n \end{aligned}$$

Ad esempio, poiché l'insieme dei divisori di 100 è $\{1, 2, 4, 5, 10, 20, 25, 50, 100\}$ si ha $\tau(100) = 9$ e $\sigma(100) = 217$.

Proposizione 3.1. *Le funzioni τ, σ sono moltiplicative.*

Questo non è difficile da provare direttamente dalle definizioni; d'altra parte discende anche come applicazione immediata del seguente principio generale. Per semplificare le notazioni, d'ora in avanti adotteremo la convenzione che se n è un intero positivo, la scrittura $\sum_{d|n}$ indica la somma eseguita al variare di d fra tutti i divisori interi positivi di n.

Teorema 3.2. *Sia f una funzione moltiplicativa; allora la funzione $F : \mathbb{N}^* \to \mathbb{C}$, definita ponendo, per ogni $n \in \mathbb{N}^*$,*

$$F(n) = \sum_{d|n} f(d),$$

è moltiplicativa.

Dimostrazione. Siano $n, m \in \mathbb{N}^*$ tali che $mcd(n, m) = 1$. Osserviamo che i divisori di nm sono in corrispondenza biunivoca con le coppie (d_1, d_2), dove d_1 e d_2 sono, rispettivamente, divisori di n e di m: ogni divisore d di nm si scrive infatti *in modo unico* come prodotto $d = d_1 d_2$ con dove $d_1 | n$ e $d_2 | m$. Quindi, tenendo presente che ogni divisore di n è coprimo con ogni divisore di m,

$$F(nm) = \sum_{d|nm} f(d) = \sum_{d_1|n\, d_2|m} f(d_1 d_2) = \sum_{d_1|n\, d_2|m} f(d_1) f(d_2) =$$

$$= \sum_{d_1|n} \Big(f(d_1) \sum_{d_2|m} f(d_2) \Big) = \sum_{d_1|n} f(d_1) \cdot \sum_{d_2|m} f(d_2) = F(n)F(m),$$

così provando che F è moltiplicativa. □

Poiché per ogni $n \in \mathbb{N}^*$ si ha

$$\tau(n) = \sum_{d|n} 1 \quad \text{e} \quad \sigma(n) = \sum_{d|n} d,$$

dal Teorema 3.2 segue subito, come anticipato, che le funzioni τ e σ sono moltiplicative.

Ad esempio, poiché $100 = 4 \cdot 25$, si ha

$$\tau(100) = \tau(4)\tau(25) = 3 \cdot 3 = 9 \quad \text{e} \quad \sigma(100) = \sigma(4)\sigma(25) = 7 \cdot 31 = 217.$$

Ma possiamo fare di meglio. Infatti, la moltiplicatività di una funzione consente di determinarne i valori a partire da quelli che essa assume sulle potenze dei numeri primi. Infatti, se f è una funzione moltiplicativa, e $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ dove i p_i sono primi distinti e gli α_i interi maggiori o uguali a 1, allora chiaramente

$$f(n) = \prod_{i=1}^{k} f(p_i^{\alpha_k}). \tag{3.2}$$

Ora, se p è un primo positivo e $\alpha \in \mathbb{N}^*$, i divisori positivi di p^α sono $1, p, \ldots, p^\alpha$; dunque

$$\begin{aligned} \tau(p^\alpha) &= 1 + \alpha \\ \sigma(p^\alpha) &= 1 + p + p^2 + \cdots + p^\alpha = \tfrac{p^{\alpha+1}-1}{p-1} \end{aligned} \tag{3.3}$$

Possiamo dunque concludere con le seguenti formule per il calcolo dei valori di τ e σ.

Proposizione 3.3. *Sia $n \in \mathbb{N}^*$, e sia $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ la fattorizzazione di n in potenze di primi distinti; allora*

$$\tau(n) = \prod_{i=1}^{k}(1 + \alpha_i) = \prod_{p|n}(\nu_p(n) + 1) \qquad e \qquad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}. \tag{3.4}$$

Evidenziamo un semplice corollario, con il fine di risolvere definitivamente il Problema posto all'inizio del capitolo.

Corollario 3.4. *Un intero positivo ha un numero dispari di divisori positivi se e solo se è un quadrato intero.*

Dimostrazione. Sia $n > 1$ un intero positivo (il caso $n = 1$ è ovvio); dalla prima formula in (3.4), $\tau(n)$ è dispari se e solo se $\nu_p(n)$ è pari per ogni primo p che divide n, e questo è equivalente all'essere n un quadrato intero. □

Gli esercizi che seguono (a parte forse il primo) potranno tornare utili nella soluzione di alcuni dei problemi che proporremmo poi.

Esercizio 3.1. Si provi che per ogni $n \geq 1$,

$$\sum_{d|n} \tau^3(d) = \Big(\sum_{d|n} \tau(d)\Big)^2$$

Esercizio 3.2. Si provi che per ogni $n \in \mathbb{N}^*$, $\tau(n) < 2\sqrt{n}$.

Esercizio 3.3. Si provi che per ogni $n \geq 1$,

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

Esercizio 3.4. Si provi che per ogni $n \geq 2$,

$$\frac{\sigma(n)}{n} < \prod_{p|n} \frac{p}{p-1}.$$

dove p varia nell'insieme dei divisori primi di n.

Esercizio 3.5. Sia $n \in \mathbb{N}^*$; si provi che se $\sigma(n)$ è dispari, allora $n = a^2$ oppure $n = 2a^2$, per qualche $a \in \mathbb{N}^*$.

Esercizio 3.6. Si provi che per ogni $n \geq 2$,

$$\sigma(n) \geq \tau(n)\sqrt{n}.$$

Numeri perfetti. Un numero $n \in \mathbb{N}^*$ si dice perfetto se $\sigma(n) = 2n$, ovvero se n è uguale alla somma dei suoi divisori positivi diversi da se stesso. I primi due numeri perfetti sono 6 e 28.

Proposizione 3.5 (L. Eulero)**.** *Un numero intero positivo pari n è perfetto se e solo se $n = 2^{p-1}(2^p - 1)$, dove p e $2^p - 1$ sono numeri primi.*

Dimostrazione. Il verso facile: sia $n = 2^{p-1}(2^p - 1)$, con p e $2^p - 1$ numeri primi, allora per la Proposizione 3.3

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)2^p = 2n,$$

e dunque n è perfetto.

Viceversa, sia n un numero perfetto pari, e scriviamo $n = 2^{k-1}m$ con $k \geq 2$ e m dispari; allora

$$2^k m = 2n = \sigma(n) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m).$$

Dunque, $2^k - 1$ divide m, sia $m = (2^k - 1)m'$; quindi

$$\sigma(m) = 2^k m 2^k - 1 = 2^k m' \ .$$

Poiché m e m' sono distinti e dividono entrambi m si ha

$$\sigma(m) \geq m + m' = (2^k - 1)m' + m' = 2^k m' = \sigma(m)$$

da cui $m' = 1$. Di conseguenza m è primo, e pertanto, per quanto richiamato sopra, $m = 2^p - 1$ per qualche primo p. □

COMMENTI. Il risultato stabilito nel Proposizione 3.5, parzialmente già noto ai matematici greci (ma anche al nostro matematico arabo Ibn al-Haytham), e provato definitivamente da Eulero, stabilisce una corrispondenza biunivoca tra numeri perfetti pari e primi di Mersenne (vedi sezione 1.2). Dunque anche per i numeri perfetti pari non è noto se il loro numero sia finito o infinito. Il problema dell'esistenza di numeri perfetti dispari diversi da 1 è invece tuttora aperto, anche se la congettura prevalente è che non ve ne siano; una cosa nota è, ad esempio, che se esiste un numero perfetto dispari, esso deve avere almeno sette divisori primi distinti.

Esercizio 3.7. Si provi che se n è un numero perfetto dispari, allora n è diviso da almeno 3 primi distinti.

Esercizio 3.8. Siano $p, n \in \mathbb{N}^*$ con p un primo; si provi che $\sigma(p^n) = 2q$ con q dispari se e soltanto se sia p che n sono congrui a 1 modulo 4. Dedurre che se $a > 1$ è un numero perfetto dispari, allora $a = p^t m^2$ con p un primo, m un numero dispari non diviso da p e p, t entrambi congrui a 1 modulo 4.

Problemi

Vediamo qualche esempio risolto di problema da gara,

Problema 106 (Bielorussia 1999)**.** *Sia n un intero positivo dispari; provare che $\sigma(n)^3 < n^4$.*

SOLUZIONE. Per la moltiplicatività della funzione σ è sufficiente provare l'asserto quando $n = p^a$, con p un numero primo dispari e $a \geq 1$. In tal caso

$$\sigma(n) < \frac{p^{a+1}}{p-1} \leq p^a \frac{p}{p-1} \leq p^a \frac{3}{2};$$

dunque, se $n = p^a \geq 5$, $\sigma(n)^3 < p^{3a}\frac{27}{8} < p^{4a} = n^4$. Rimane il solo caso $n = 3$, per il quale si ha direttamente $\sigma(3)^3 = 4^3 < 3^4$. ∎

Problema 107 (Iberoamericana, 2007)**.** *Diciamo che un intero positivo n è* atresvido *se l'insieme dei suoi divisori positivi si può ripartire in tre sottoinsiemi tali che la somma degli elementi di ciascuno è la stessa. Si dica qual è il minimo numero di divisori positivi che un numero atresvido può avere.*

SOLUZIONE. Sia n un numero atresvido. Poiché n compare in uno dei tre sottoinsiemi in cui si ripartiscono i suoi divisori, si ha $\sigma(n) \geq 3n$. Per l'esercizio 3.4,

$$3 \leq \frac{\sigma(n)}{n} < \prod_{p|n} \frac{p}{p-1}, \qquad (*)$$

il che comporta immediatamente che n è diviso da almeno tre primi distinti p, q, r. Se n è diviso da 4 primi distinti allora $\tau(n) \geq 2^4 = 16$.

Supponiamo n sia diviso da 3 primi distinti; se questi sono tutti dispari, da $(*)$ segue l'assurdo

$$3 < \frac{p}{p-1} \cdot \frac{q}{q-1} \cdot \frac{r}{r-1} \leq \frac{3}{2} \cdot \frac{5}{4} \cdot \frac{7}{6} = \frac{35}{16} < 3.$$

Dunque $2|n$. Con un argomento analogo (dato che $2 \cdot \frac{5}{4} \cdot \frac{7}{6} = \frac{35}{12} < 3$) si prova che $3|n$. Quindi $n = 2^a 3^b p^c$, con $p \geq 5$, e $a, b, c \geq 1$. Supponiamo $(a+1)(b+1)(c+1) = \tau(n) \leq 16$; quindi al più uno dei tre esponenti a, b, c è maggiore o uguale a 2, ed è al più 3
Se $n = 6p^c$, con $1 \leq c \leq 3$, si ha la contraddizione

$$\sigma(n) = 12 \cdot \frac{p^{c+1} - 1}{p-1} \leq 12 \cdot 2p^c < 3n.$$

Un calcolo simile si applica per escludere i casi $12p$, $18p$ e $54p$.
Dunque rimane il caso $n = 24p$. Il più piccolo numero del genere è 120, per il quale si ha $\tau(120) = 16$, e che è un numero atresvido. Infatti $\sigma(120) = 360$ e i divisori di 120 si possono ripartire nei tre sottoinsiemi

$$A = 120, \quad B = \{d \mid d \text{ divide } 24\} \cup \{60\}, \quad C = \{5d \mid d = 1, 2, 3, 4, 6, 8\}$$

la somma degli elementi di ciascuno dei quali è 120.
In conclusione, il minimo numero di divisori che può aver un numero atresvido è 16, e 120 è il più piccolo numero atresvido. ∎

Commento. L'aggettivo *atresvido* non esiste nella lingua spagnola; il termine è stato probabilmente coniato per incastro tra le parole *tres* (tre) e *atrevido* (audace, osé).

* * *

• Problemi da risolvere.

Problema 108 (San Pietroburgo 2001)**.** *Siano $n, m, k \in \mathbb{N}^*$ con $n \geq 2$, e $\sigma(n)$ definita come nel problema precedente. Si provi che*

$$\sigma(n)^k \neq n^m.$$

Problema 109 (Stati Uniti 2008)**.** *Quanti sono i divisori positivi di 2004^{2004} che sono divisibili per esattamente 2004 interi positivi?*

Problema 110 (San Pietroburgo 1998)**.** *Per $n \in \mathbb{N}^*$ sia $\tau(n)$ il numero di divisori interi positivi di n Si provi che la successione $\tau(n^2+1)$ non diviene mai strettamente monotona a partire da alcun $n \in \mathbb{N}^*$.*

Problema 111 (IMO, Taipei 1998)**.** *Sia $k \in \mathbb{N}^*$. Con le notazione del problema precedente, si provi che esiste $n \in \mathbb{N}^*$ tale che*

$$\frac{\tau(n^2)}{\tau(n)} = k$$

se e solo se k è dispari.

Altri tre problemi sulla funzione τ.

Problema 112 (IMO, Taejon 2000)**.** *Dire per quali interi positivi n si ha $\tau(n)^3 = 4n$.*

Problema 113 (IMO, Atene 2004)**.** *Provare che esistono infiniti interi positivi a tali che l'identità $\tau(an) = n$ non è soddisfatta da alcun $n \in \mathbb{N}^*$.*

Problema 114 (Baltic Way 2011)**.** *Determinare tutte le terne di interi positivi (n, k, p) con p un numero primo, tali che*

$$n^{\tau(n)} - 1 = p^k.$$

SUGGERIMENTI. Diamo di seguito qualche suggerimento, a cui ricorrere nei casi ostinati, prima di guardare le soluzioni che si trovano, assieme a qualche commento integrativo, nella sezione 3.4.

Problema 108: osservare che $\sigma(n) > n$, quindi applicare la formula in (3.4).

Problema 109: poiché $2004 = 4 \cdot 3 \cdot 167$ (e 167 è primo), ogni divisore di 2004^{2004} ha una fattorizzazione in primi del tipo $2^a 3^b 167^c$.

Problema 110: questo è il più difficile, anche perché la soluzione non è agevolata dalla conoscenza delle proprietà di τ che abbiamo visto, ed il primo suggerimento è proprio questo: mettete da parte quella conoscenza e cercate un'idea diversa. Il secondo suggerimento è che l'idea giusta sta nel provare preliminarmente che se n è pari allora $\tau(n^2 + 1) \leq n$; quindi notare che, siccome $n^2 + 1$ non è mai un quadrato perfetto, $\tau(n^2 + 1)$ è pari per ogni $n \in \mathbb{N}^*$; assumete infine che per $n \geq N$ la funzione $\tau(n^2 + 1)$ sia strettamente crescente e giungete ad una contraddizione con l'osservazione pdi prima.

Problema 111: anche questo è tosto. Sia $\mathcal{S} = \{\tau(n^2)/\tau(n) \mid n \in \mathbb{N}^*\}$; si vuole provare che $\mathcal{S} \cap \mathbb{N}^*$ è l'insieme D dei numeri dispari. L'inclusione $\mathcal{S} \cap \mathbb{N}^* \subseteq D$ è facile; per il viceversa, si osservi che $\mathcal{S}$ è moltpilicativamente chiuso, quindi si proceda per induzione su $k \in D$, osservando che, se $k > 1$, $k = 1 + 2^a d$ con $a \geq 1$ e $d \in D$, e provando che allora $k/d \in S$, quindi... (per capire come fare, può essere utile eseguire degli esperimenti, scrivendo i primi numeri dispari, $3, 5, 7$, nella forma $\tau(n^2)/\tau(n)$).

Problema 112: Sia $\tau(n)^3 = 4n$, e per ogni primo p, sia $\nu_p(n)$ l'esponente della massima potenza di p che divide n; osservare che $3 \mid \nu_p(n)$ se $p \geq 3$ mentre $\nu_2(n) \equiv 1 (\mathrm{mod}\ 3)$. Dedurre che $3 \nmid n$, quindi, usando le formule e diseguaglianze abbastanza ovvie, provare a concludere che $n = 2, 2^7, 2^4 5^3$.

Problema 113: Occorre intuire un insieme infinito di interi positivi a che soddisfi la condizione richiesta; e la cosa più maneggevole è pensare ai numeri primi o, eventualmente, alle loro potenze; conviene fare qualche esperimento, che mostrerà che 2 non funziona e che, inoltre, se $p \geq 3$, $\tau(p \cdot 8) = 8$. Si passa quindi a considerare potenze di primi, ma ancora si trova, ad esempio, che se $p \geq 5$, $\tau(p^2 \cdot 18) = 18$ e $\tau(p^3 \cdot 36) = 36$. Se, dato un primo p (che conviene prender maggiore o uguale a 5) trovate un giusto esponente, dipendente da p, per il quale i casi coprimi (come sono quelli degli ultimi esempi) non danno uguaglianza, siete già a buon punto (e ho detto troppo).

Problema 114: ricordarsi dell'esercizio 3.3.

3.2. Altre funzioni moltiplicative

La funzione di Möbius. La *funzione di Möbius* classica è l'applicazione $\mu : \mathbb{N}^* \to \{0, 1, -1\}$, definita nel modo seguente

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se esiste un primo } p \text{ tale che } p^2 | n \\ (-1)^s & \text{se } n = p_1 p_2 \dots p_s \text{ con } p_i \text{ primi distinti} \end{cases}$$

Chiaramente μ è una funzione moltiplicativa. Inoltre si ha

Lemma 3.6. *Per ogni intero positivo n,*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & se \quad n = 1 \\ 0 & se \quad n > 1 \end{cases}$$

Dimostrazione. Poniamo $\Delta(n) = \sum_{d|n} \mu(d)$. Allora Δ è moltiplicativa per il Teorema 3.2, e $\Delta(1) = 1$. Sia p un numero primo, e $a \geq 1$; allora

$$\Delta(p^a) = \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^a) = \mu(1) + \mu(p) = 1 - 1 = 0 \ ;$$

poichè Δ è moltiplicativa, si conclude che, se $n > 1$, $\Delta(n) = 0$. □

Prodotto di convoluzione e formula di inversione. Un'applicazione $f : \mathbb{N}^* \to \mathbb{C}$ si dice *funzione aritmetica*. Sull'insieme di tutte le funzione aritmetiche si definisce il *prodotto di convoluzione* $*$, ponendo, per ogni $f, g : \mathbb{N}^* \to \mathbb{C}$, ed ogni $n \in \mathbb{N}^*$,

$$(f * g)(n) = \sum_{d|n} f(d) g(n/d).$$

Enunciamo ora alcune proprietà di base di questa importante operazione, la cui dimostrazioni, non troppo difficili, lasciamo per esercizio.

Proposizione 3.7. *Sia Ω l'insieme di tutte le funzioni aritmetiche; e sia $\mathfrak{e} \in \Omega$ definita da $\mathfrak{e}(1) = 1$ e $\mathfrak{e}(n) = 0$ per ogni $n \geq 2$.*

(1) Il prodotto di convoluzione è un operazione associativa e commutativa in Ω.

(2) $\mathfrak{e}$ è (l'unico) elemento neutro, cioè $f * \mathfrak{e} = f = \mathfrak{e} * f$ per ogni $f \in \Omega$.

(3) Se $f, g \in \Omega$ sono moltiplicative, allora $f * g$ è moltiplicativa.

I primi due punti della Proposizione dicono che $(\Omega, *)$ è un monoide commutativo. Si prova poi che $f \in \Omega$ ammette un'inversa per convoluzione (cioè esiste $h \in \Omega$ tale che $f * h = \mathfrak{e}$) se e solo se $f(1) \neq 0$. Demandando la dimostrazione generale ad un esercizio (il 3.11), ci limitiamo ad osservare il caso per noi particolarmente interessante.

Denotiamo con $\underline{1}$ la funzione costante definita da $\underline{1}(n) = 1$ per ogni $n \in \mathbb{N}^*$; si osservi che, per ogni $f \in \Omega$ e $n \in \mathbb{N}^*$,

$$(f * \underline{1})(n) = \sum_{d|n} f(d)$$

(quindi, la Proposizione 3.2 è un caso particolare del punto (3) della Proposizione 3.7).

Lemma 3.8. *Sia μ la funzione di Möbius, allora $\mu * \underline{1} = \mathfrak{e} = \underline{1} * \mu$.*

Dimostrazione. Per ogni $n \in \mathbb{N}^*$ si ha infatti, per il Lemma 3.6,

$$(\mu * \underline{1})(n) = \sum_{d|n} \mu(d) = \mathfrak{e}(n),$$

come si voleva. □

Questo Lemma è una delle forme equivalenti della proprietà più importante della funzione di Möbius, la *Formula di Inversione di Möbius*, che è il contenuto del prossimo Teorema.

Teorema 3.9. *Sia f una funzione aritmetica e per ogni $n \in \mathbb{N}^*$ sia $F(n) = \sum_{d|n} f(d)$. Allora, per ogni $n \in \mathbb{N}^*$,*

$$f(n) = \sum_{d|n} \mu(n/d)F(d) = \sum_{d|n} \mu(d)F(n/d). \tag{3.5}$$

Dimostrazione. Per quanto osservato, $F = f * \underline{1}$; quindi, per il Lemma 3.8 e l'associatività del prodotto di convoluzione,

$$f = f * \mathfrak{e} = f * (\underline{1} * \mu) = (f * \underline{1}) * \mu) = F * \mu,$$

che è esattamente la (3.5). □

In particolare, è possibile invertire la Proposizione 3.2.

Corollario 3.10. *Sia f una funzione aritmetica tale che la funzione $F(n) = \sum_{d|n} f(d)$ è moltiplicativa. Allora f è moltiplicativa.*

Dimostrazione. Per il Teorema precedente, $f = F * \mu$, che è un prodotto di funzioni moltiplicative. Dunque f è moltiplicativa per il punto (3) della Proposizione 3.7. □

La funzione di Möbius può essere generalizzata in modo da venire definita per insiemi parzialmente ordinati in cui per ogni elemento c'è un numero finito di elementi più piccoli: quella che abbiamo esposto è la versione classica, in cui l'insieme parzialmente ordinato è $\mathbb{N}^*$ con la relazione di divisibilità. Applicata all'insieme ordinato per inclusione dei sottoinsiemi di un insieme finito, dà luogo al ben noto principio di *esclusione–inclusione*. Nel suo aspetto più generale, è però argomento del corso di enumerabilità, ai ricordi del quale si rimanda per le numerose interessanti applicazioni.

Esercizio 3.9. Si dimostrino le seguenti proprietà della funzione di Möbius:

1) $\sum_{d^2|n} \mu(d) = |\mu(n)|$

2) $\sum_{i\le n} \mu(i)[n/i] = 1$ e quindi $\left|\sum_{i\le n}(\mu(i)/i)\right| \le 1$.

Esercizio 3.10. Si provi che per ogni $n \in \mathbb{N}^*$,

$$\sum_{d|n} |\mu(d)| = 2^{\omega(n)},$$

dove $\nu(1) = 0$, e per $n > 1$, $\omega(n)$ è uguale al numero di fattori primi, non necessariamente distinti, di n (ad esempio, $\omega(24) = 4$).

Esercizio 3.11. Si provi che una ogni funzione aritmetica f ammette un'inversa per convoluzione (cioè esiste una funzione aritmetica g tale che $f * g = \mathfrak{e}$) se e solo se $f(1) \neq 0$; si provi quindi che se f è moltiplicativa allora anche la sua inversa per convoluzione lo è. [sugg.: per la prima parte, sia $f : \mathbb{N}^* \to \mathbb{C}$ con $f(1) \neq 0$ e g la sua inversa, ancora da determinare; si osservi che $g(1) = f(1)^{-1}$, quindi si proceda per induzione a definire $g(n)$.]

Esercizio 3.12. [La funzione λ di Liouville.] La funzione λ di Liouville è definita ponendo, per ogni $n \in \mathbb{N}^*$,

$$\lambda(n) = (-1)^{\nu(n)},$$

dove ν è la funzione definita nell'esercizio 3.10.

1) Si provi che λ è moltiplicativa, e che per ogni $n \in \mathbb{N}^*$,

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{se } n \text{ è un quadrato} \\ 0 & \text{altrimenti} \end{cases}$$

2) Si determini l'inversa di λ rispetto al prodotto di convoluzione.

La funzione di Eulero. Dato $n \in \mathbb{N}^*$, si indica con $\phi(n)$ il numero di interi compresi tra 1 e n che sono coprimi con n. La funzione ϕ così definita si chiama *funzione di Eulero* (o anche funzione *toziente*). Riscrivendo la definizione in modo formale,

$$\phi(n) = |\{a \in \mathbb{N} \ ; \ 1 \le a \le n \ \text{ e } \ (a, n) = 1\}|.$$

Lemma 3.11. *Per ogni $n \in \mathbb{N}^*$,*

$$\sum_{d|n} \phi(d) = n \ .$$

Dimostrazione. Poniamo $A = \{1, 2, \ldots, n\}$ e $\Delta_n = \{d \mid 1 \le d \text{ e } d \text{ divide n}\}$. Definiamo una applicazione $c : A \to \Delta_n$ ponendo, per ogni $a \in A$, $c(a) = (a, n)$. Allora, chiaramente,

$$n = \sum_{d|n} |c^{-1}(d)| \ .$$

D'altra parte, per ogni $d \in \Delta_n$,

$$|c^{-1}(d)| = |\{a \in A \mid (a,n) = d\}| = |\{1 \le a \le n/d \mid (a, n/d) = 1\}| = \phi(n/d).$$

Dunque

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi(d/n) = \sum_{d|n} |c^{-1}(d)| = n,$$

come si voleva. □

Teorema 3.12. *La funzione ϕ di Eulero è moltiplicativa. Inoltre, per ogni $n \in \mathbb{N}^*$ si ha*

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Dimostrazione. La prima affermazione discende immediatamente dal Corollario 3.10, poiché la funzione $n = \sum_{d|n} \phi(d)$ è ovviamente moltiplicativa.
La seconda affermazione è un'altra facile applicazione della formula di inversione di Möbius all'uguaglianza del Lemma 3.11; infatti da queste segue che, per ogni $n \in \mathbb{N}^*$,

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

□

La moltiplicatività della funzione di Eulero consente di determinarne i valori. Innanzi tutto supponiamo che $n = p^\alpha$ sia la potenza di un numero primo. Allora, per ogni $a \in \mathbb{N}^*$, $(a,n) = 1$ se e solo se $(a,p) = 1$; ora i multipli di p compresi tra 1 e p^α sono in numero di $p^{\alpha-1}$, e quindi

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1).$$

Ne segue che se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ è la fattorizzazione in potenze di primi distinti di n, allora

$$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = n \cdot \prod_{i=1}^{k} \Big(\frac{p_i - 1}{p_i}\Big). \tag{3.6}$$

Quest'ultima espressione consente, con ovvia manipolazione, di concludere che per ogni $n \ge 2$,

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

dove p varia nell'insieme dei numeri primi che dividono n.

Osserviamo che, se p è un primo, il valore di ϕ in p^α si può anche ricavare immediatamente dall'uguaglianza del Teorema 3.12; infatti da questa si ha

$$\phi(p^\alpha) = p^\alpha \sum_{i=0}^{\alpha} \frac{\mu(p^i)}{p^i} = p^\alpha \left(\frac{\mu(1)}{1} + \frac{\mu(p)}{p}\right) = p^\alpha \left(1 - \frac{1}{p}\right).$$

Esercizio 3.13. Si provi che per ogni $a, b \in \mathbb{N}^*$, $\phi(ab) \leq \phi(a)b$ (on particolare $\phi(2n) \leq n$).

Esercizio 3.14. Si provi che, per ogni $n \geq 2$,

$$\sum_{i \leq n,\, (i,n)=1} i = \frac{1}{2} n\phi(n).$$

Esercizio 3.15. Si provi che la disuguaglianza $\phi(x) \geq x - \sqrt{x}$ ha come sole soluzioni intere i numeri p e p^2, con p primo.

Problemi

Problema 115 (Corea 1998)**.** *Sia n un intero positivo diviso da al più 3 primi distinti. Si provi che se $\phi(n)$ divide $n-1$ allora n è un numero primo.*

Soluzione. Sia $n \in \mathbb{N}^*$; dalla formula (3.6) segue subito che se n è diviso dal quadrato di un numero primo p, allora p divide $\phi(n)$, che quindi non divide $n-1$. Dunque, se n è la potenza di un primo p, allora $\phi(n)|n-1$ se e solo se $n = p$. Un altro caso generale che si esclude facilmente è quando n è un numero pari ma non una potenza di 2; allora $n-1$ è dispari mentre, poiché n è diviso da un primo $q \geq 3$, $\phi(n)$ è pari.
Ai fini del nostro problema resta da provare che se il numero di divisori primi distinti di n è 2 o 3, e questi sono dispari, allora $\phi(n)$ non divide $n-1$. Distinguiamo i due casi.
Sia $n = pq$, con p, q primi dispari distinti; dunque $\phi(n) = (p-1)(q-1)$. Se $\phi(n)|n-1$ allora $p-1$ divide $n-1-(p-1) = pq - p = p(q-1)$, quindi, dato che $p \neq 2$, si ha $p-1|q-1$; ma, simmetricamente, $q-1|p-1$, e dunque la contraddizione $p = q$.
Sia $n = pqr$, con $p < q < r$ primi dispari distinti; dunque $\phi(n) = (p-1)(q-1)(r-1)$. Supponiamo $p = 3$; allora

$$\frac{(q-1)(r-1)}{qr} \geq \frac{4}{5} \cdot \frac{6}{7} > \frac{1}{2}$$

e dunque $3\phi(n) = 3 \cdot 2(q-1)(r-1) > 3qr = n$. Se $\phi(n)|n-1$ si deve quindi avere

$$3qr - 1 = n - 1 = 2\phi(n) = 4(q-1)(r-1),$$

da cui

$$r(q-4) = 4q - 5 = 4(q-4) + 11,$$

che non ha soluzioni con q, r primi.
Sia ora $3 < p < q < r$. Ragionando come sopra si ha

$$\frac{\phi(n)}{n} = \frac{p-1}{p} \cdot \frac{q-1}{q} \cdot \frac{r-1}{r} \geq \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11} = \frac{48}{77} > \frac{1}{2},$$

dunque $2\phi(n) > n$. Quindi, se $\phi(n)$ divide $n-1$ si ha $\phi(n) = n-1$, che è assurdo. ∎

Commento. C'è una congettura, dovuta a Lehmer e tuttora aperta nella sua generalità, la quale afferma che per ogni $n > 1$, se $\phi(n)$ divide $n-1$ allora n è un numero primo.

Problema 116 (A. Schinzel)**.** *Si dimostri che esistono infiniti numeri pari positivi k tali che $\phi(n) \neq k$ per ogni $n \in \mathbb{N}^*$.*

SOLUZIONE. Sia $k = 2 \cdot 7^m$ con $m \geq 1$ e supponiamo, per assurdo che esista $n \in \mathbb{N}^*$ tale che $\phi(n) = k$. Poiché $2|p-1$ per ogni primo dispari p, dalla formula (3.6) segue che n deve essere della forma $2^\epsilon p^b$, con $\epsilon \in \{0,1\}$, p un numero primo dispari e $b \geq 1$. Ma allora $\phi(n) = b^{b-1}(p-1) = 2 \cdot 7^m$, da cui

$$7^m = p^{b-1}\frac{p-1}{2};$$

quindi, $b = 1$ e $\frac{p-1}{2} = 7^m$, cioè $p = 2 \cdot 7^m + 1$. Questo non è possibile: infatti, $7 \equiv 1 \pmod 3$ e dunque $7^m \equiv 1 \pmod 3$ per ogni $m \geq 1$, il che significa che 3 divide $2 \cdot 7^m + 1$, che non è pertanto un numero primo. ∎

COMMENTO. In questo caso, la cosa principale è stata congetturare la natura di un insieme infinito di numeri pari k che non coincidano con alcun valore della funzione di Eulero. Dalla formula (3.6) segue che se t è il numero di divisori primi dispari distinti di n, allora 2^t divide $\phi(n)$; è quindi naturale provare a prendere $k = 2c$ con c dispari: se $\phi(n) = k$ allora $n = 2^\epsilon p^b$ per qualche primo dispari p e $\epsilon \in \{0,1\}$. Se $p > 3$ e $b \geq 2$ allora $\phi(n)$ è divisa da p e inoltre o da 2^2 (che non va bene) oppure da un altro primo dispari $q \neq p$, quindi $qp|c$. Questo suggerisce di prendere $k = 2q^m$ com q un primo dispari, per cui $n = 2^\epsilon p$.

* * *

• Problemi da risolvere.

Problema 117 (Nordic MC, 2010). *Sia $f : \mathbb{N}^* \to \mathbb{N}^*$ una funzione moltiplicativa crescente. Si provi che $f(8)f(13) \geq (f(10))^2$.*

Problema 118 (Math. Magazine). *Siano n, p interi con p un primo positivo e $1 < n \leq p$. Si provi che*

$$p \mid \phi(n^{p-1} + \ldots + n + 1).$$

Problema 119 (Bulgaria 2011). *Trovare tutti gli interi positivi n tali che n ha esattamente due divisori primi distinti e soddisfa $\tau(\phi(n)) = \phi(\tau(n))$.*

Infine, un problema olimpico nel quale la funzione di Eulero c'entra solo di striscio.

Problema 120 (IMO, Sigtuna 1991). *Sia $6 < n \in \mathbb{N}$ e siano $a_1, a_2, \ldots, a_k$ tutti gli interi positivi minori di n e coprimi con esso. Si provi che se $a_2 - a_1 = a_3 - a_2 = \ldots = a_k - a_{k-1} > 0$ allora n è un numero primo oppure una potenza di 2.*

3.3. Media di $\phi(n)$

Anche in questo capitolo, lasciamo per una sezione la via dei problemi, per dimostrare un interessante risultato sul comportamento asintotico del valore medio della funzione ϕ di Eulero; cosa che ci consentirà di valutare con esattezza (Teorema 3.17) la probabilità che, presi due numeri positivi a caso, essi risultino coprimi.

Nel seguito, se f è una funzione aritmetica e $1 \leq x \in \mathbb{R}$, con la scrittura

$$\sum_{i \leq x} f(i)$$

intenderemo la somma sui numeri interi positivi i che sono minori di x.

La funzione *Zeta di Riemann* ζ è definita per numeri complessi z tali che $Re(z) > 1$ da

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}.$$

Si tratta di una funzione estremamente importante in teoria dei numeri, così come in altri settori della matematica. Ad esempio, Eulero ha dimostrato (chiaramente prima degli studi di B. Riemann) che, se $\mathbb{P}$ è l'insieme di tutti i numeri primi positivi, allora

$$\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

In questa sezione, siamo interessati al valore che essa assume in $z = 2$.

Lemma 3.13 (L. Eulero)**.**

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Dimostrazione. Dimostrazioni di questa classica identità[2] ce ne sono a decine: per il suo carattere elementare ho scelto quella proposta da J. Hofbauer in [3].

Ricordando che $\sin x = 2 \sin \frac{x}{2} \cos \frac{x}{2}$, si ottiene la seguente identità,

$$(\sin^2 x)^{-1} = \frac{1}{4 \sin^2 \frac{x}{2} \cos^2 \frac{x}{2}} = \frac{1}{4} \left[\frac{1}{\sin^2 \frac{x}{2}} + \frac{1}{\cos^2 \frac{x}{2}} \right] = \frac{1}{4} \left[\frac{1}{\sin^2 \frac{x}{2}} + \frac{1}{\sin^2 \frac{\pi + x}{2}} \right].$$

In particolare,

$$1 = \left(\sin^2 \frac{\pi}{2} \right)^{-1} = \frac{1}{4} \left[\frac{1}{\sin^2 \frac{\pi}{4}} + \frac{1}{\sin^2 \frac{3\pi}{4}} \right].$$

Applicando ripetutamente questa uguaglianza (cioè, facendo induzione su n) si prova che, per ogni $n \geq 2$,

$$1 = \frac{1}{4^n} \sum_{k=0}^{2^n - 1} \left(\sin^2 \frac{(2k+1)\pi}{2^{n+1}} \right)^{-1} = \frac{2}{4^n} \sum_{k=0}^{2^{n-1} - 1} \left(\sin^2 \frac{(2k+1)\pi}{2^{n+1}} \right)^{-1}. \tag{3.7}$$

Ora, per $0 < x < \pi/2$, si ha $\sin x < x < \tan x$, e quindi

$$\frac{1}{\sin^2 x} > \frac{1}{x^2} > \frac{1}{\tan^2 x} = \frac{1}{\sin^2 x} - 1.$$

[2] Il problema di valutare la somma dei quadrati degli inversi degli interi positivi, divenuto noto come Problema di Basilea, fu proposto da Pietro Mengoli nel 1644, e resistette all'attacco dei migliori matematici fino alla soluzione data da Leonardo Eulero nel 1735.

Ponendo $N = 2^n$, e $x = (2k+1)\pi/2N$ (con $k = 0, 1, \ldots, N/2-1$), con semplici calcoli, dalla (3.7) segue

$$1 > \frac{8}{\pi^2} \sum_{k=0}^{\frac{N}{2}-1} \frac{1}{(2k+1)^2} > 1 - \frac{1}{N}.$$

Passando al limite per $n \to \infty$ si ottiene,

$$1 = \frac{8}{\pi^2} \sum_{k=0}^{\infty} \frac{1}{(2k+1)^2}.$$

Da tale identità segue quella per $\zeta(2)$. Infatti

$$\zeta(2) = \sum_{i=1}^{\infty} \frac{1}{i^2} = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^2} + \sum_{k=1}^{\infty} \frac{1}{(2k)^2} = \frac{\pi^2}{8} + \frac{1}{4}\zeta(2),$$

e quindi $\zeta(2) = \pi^2/6$. □

Lemma 3.14. *Se $1 < s \in \mathbb{R}$, allora*

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Dimostrazione. Poiché $s > 1$, la serie $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ è assolutamente convergente. Quindi, per un noto risultato di Analisi[3],

$$\zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{m=1}^{\infty} \frac{1}{m^s} \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{m,n=1}^{\infty} \frac{\mu(n)}{(mn)^s}.$$

Ponendo $i = mn$ e ricordando il Lemma 3.6, possiamo scrivere

$$\zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{i=1}^{\infty} \left(\frac{1}{i^s} \sum_{d|i} \mu(d) \right) = 1,$$

che è quello che si voleva. □

Lemma 3.15.

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}\ .$$

Dimostrazione. Questo discende immediatamente dai due Lemmi precedenti. □

[3]Il prodotto di due serie convergenti, di cui almeno una assolutamente convergente, è convergente e la sua somma vale il prodotto delle somme delle serie date.

Possiamo ora descrivere il comportamento asintotico della media della funzione ϕ di Eulero, ovvero dei valori

$$\frac{1}{n}\sum_{i\leq n}\phi(i).$$

Poiché utilizzeremo strumenti di Analisi, risulta conveniente trattare funzioni definite su intervalli di numeri reali; nel caso specifico, la funzione $\sum_{i\leq x}\phi(i)$, per $1\leq x\in\mathbb{R}$.

Teorema 3.16. *Per ogni* $1\leq x\in\mathbb{R}$,

$$\sum_{i\leq x}\phi(i)=\frac{3x^2}{\pi^2}+R(x),$$

dove $|R(x)|\leq x+x\log(x+1)$.

Dimostrazione. Per il Teorema 3.12,

$$\sum_{i\leq x}\phi(i)=\sum_{i\leq x}\Big(i\cdot\sum_{d|i}\frac{\mu(d)}{d}\Big);$$

abbiamo quindi,

$$\sum_{i\leq x}\phi(i)=\sum_{d\leq x}\frac{\mu(d)}{d}\sum_{i\leq x/d}di=\sum_{d\leq x}\Big(\mu(d)\sum_{i\leq x/d}i\Big). \tag{3.8}$$

Ricordando che, per ogni $k\in\mathbb{N}^*$, $\sum_{i\leq k}i=k(k+1)/2$, possiamo riscrivere la (3.8) come

$$\sum_{i\leq x}\phi(i)=\sum_{d\leq x}\frac{\mu(d)}{2}\left\lfloor\frac{x}{d}\right\rfloor\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right). \tag{3.9}$$

Ora, per ogni $d\leq x$,

$$\frac{x}{d}-1<\left\lfloor\frac{x}{d}\right\rfloor\leq\frac{x}{d};$$

quindi,

$$\left(\frac{x}{d}\right)^2-\frac{x}{d}=\left(\frac{x}{d}-1\right)\frac{x}{d}<\left\lfloor\frac{x}{d}\right\rfloor\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right)\leq\frac{x}{d}\left(\frac{x}{d}+1\right)=\left(\frac{x}{d}\right)^2+\frac{x}{d},$$

e pertanto possiamo scrivere

$$\left\lfloor\frac{x}{d}\right\rfloor\left(\left\lfloor\frac{x}{d}\right\rfloor+1\right)=\left(\frac{x}{d}\right)^2+R_d,$$

dove $R_d=R(x,d)$ è un numero reale tale che

$$|R_d|\leq\frac{x}{d}. \tag{3.10}$$

Sostituendo nell'identità (3.9) otteniamo

$$\sum_{i\le x}\phi(i) = \frac{1}{2}\sum_{d\le x}\mu(d)\frac{x^2}{d^2} + \frac{1}{2}\sum_{d\le x}\mu(d)R_d =$$
$$= \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2} + \frac{1}{2}\sum_{d\le x}\mu(d)R_d = \frac{x^2}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} + R(x),$$

dove

$$R(x) = -\frac{x^2}{2}\sum_{d>x}\frac{\mu(d)}{d^2} + \frac{1}{2}\sum_{d\le x}\mu(d)R_d. \tag{3.11}$$

Quindi, applicando il Lemma 3.15,

$$\sum_{i\le x}\phi(i) = \frac{3x^2}{\pi^2} + R(x).$$

Rimane da verificare la limitazione in modulo per $R(x)$. Osserviamo innanzi tutto i seguenti fatti; per ogni $1 \le x \in \mathbb{R}$ si ha

$$\sum_{d\le x}\frac{1}{d} \le 1 + \int_1^x \frac{\mathrm{d}t}{t} = 1 + \log(x+1),$$

e anche, per $x > 1$ (dove, come sopra, la somma è sugli interi positivi d),

$$\sum_{d>x}\frac{1}{d^2} \le \int_{x-1}^{\infty}\frac{\mathrm{d}t}{t^2} = \frac{1}{x-1}.$$

Applicando queste disuguaglianze nella (3.11), tenendo conto di (3.10) e del fatto che che, per ogni $n \in \mathbb{N}^*$, $|\mu(n)| \le 1$, si ottiene (per $x \ge 2$),

$$|R(x)| \le \frac{x^2}{2}\sum_{d>x}\frac{1}{d^2} + \frac{1}{2}\sum_{d\le x}|R_d| \le \frac{x^2}{2}\cdot\frac{1}{x-1} + \frac{x}{2}\sum_{d\le x}\frac{1}{d} \le x + x\log(x+1)$$

(facendo i calcoli, ricordate che, per ogni $x > -1$, $\log(x+1) \ge x/(x+1)$). Con questo, la dimostrazione è completa. □

Utilizzando la notazione con gli infiniti, si usa scrivere

$$\sum_{i\le x}\phi(i) = \frac{3x^2}{\pi^2} + O(x\log x).$$

Concludiamo con l'annunciata applicazione del Teorema 3.16.

Teorema 3.17. *La probabilità che due interi positivi siano coprimi è* $6/\pi^2$.

Dimostrazione. Fissato $n \in \mathbb{N}^*$, il numero di coppie di interi (r, s) tali che $1 \leq r \leq s \leq n$ è $n(n+1)/2$. Il numero di tali coppie che sono costituite da numeri coprimi è, chiaramente, $\sum_{i \leq n} \phi(i)$. Quindi, denotata con $P(n)$ la probabilità che due numeri interi positivi minori di n siano coprimi, si ha

$$P(n) = \frac{2}{n(n+1)} \sum_{i \leq n} \phi(i).$$

La probabilità che due interi positivi qualsiasi siano coprimi è

$$P = \lim_{n \to \infty} P(n) = \lim_{n \to \infty} \frac{2}{n(n+1)} \sum_{i \leq n} \phi(i),$$

per cui, applicando il Teorema precedente,

$$P = \lim_{n \to \infty} \frac{6n^2}{\pi^2 n^2} = \frac{6}{\pi^2},$$

come si voleva. □

3.4. Soluzioni dei problemi e commenti

Problema 108. Sia $2 \leq n \in \mathbb{N}^*$ e supponiamo, per assurdo, che esistano $m, k \in \mathbb{N}$ tali che $\sigma(n)^k = n^m$. Dalla Proposizione 3.3 segue isubito $\sigma(n) > n$, e quindi se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ è la fattorizzazione di n in potenze di primi distinti, allora $\sigma(n) = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$, con $\beta_i \geq \alpha_i + 1$ per ogni $i = 1, \ldots, t$. Dunque

$$\sigma(n) \geq p_1^{\alpha_1+1} p_2^{\alpha_2+1} \cdots p_t^{\alpha_t+1} > \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_t^{\alpha_t+1} - 1}{p_t - 1} = \sigma(n).$$

Commento. Si osservi che, essenzialmente con la stesso metodo, si dimostra che per ogni $n \geq 2$, $\sigma(n)$ ha almeno un divisore primo strettamente maggiore di n (quindi, i numeri primi sono infiniti!).

* * *

Problema 109. Poiché $2004 = 4 \cdot 3 \cdot 167$ (dove 167 è primo), ogni divisore di 2004^{2004} è della forma $d = 2^a 3^b 167^c$, con $0 \leq c \leq 4008$ e $0 \leq b, c \leq 2004$. Per la formula (3.4) il problema si riduce a trovare per quante terne (a, b, c) si ha

$$\tau(d) = (1+a)(1+b)(1+c) = 2004 = 2 \cdot 2 \cdot 3 \cdot 167,$$

(ad esempio, $(a, b, c) = (2 \cdot 167 - 1, 2 \cdot 3 - 1, 0)$). Si tratta quindi di stabilire in quante maniere diverse è possibile distribuire i numeri $2, 2, 3, 167$ nelle tre 'scatole' $[1+a]$, $[1+b]$ e $[1+c]$. Ora, i due numeri uguali 2 e 2 si possono distribuire in 6 modi diversi: in tre dei quali entrambi finiscono nella stessa scatola, ed altri tre in cui vanno in due scatole diverse; a questo punto, per il numero 3, così come per il numero 167, abbiamo 3 scelte. In conclusione, il numero di modi diversi per distribuire i quattro numeri, e dunque la risposta al nostro problema è:

$$6 \times 3 \times 3 = 54.$$

COMMENTO. La risoluzione di questo problema risulta piuttosto facile, conoscendo la formula (3.2) e con un minimo addestramento alle, semplicissime, considerazioni combinatorie della parte conclusiva.

* * *

PROBLEMA 110. Per $n \in \mathbb{N}^*$, ogni divisore di n^2+1 è elemento di un'unica coppia ordinata (x, y) con $xy = n$ e $1 \leq x < n$, $n < y \leq n^2 + 1$; da questa osservazione abbastanza elementare, si deduce subito

$$\textit{per ogni } n \in \mathbb{N}^*,\ \tau(n^2+1) \textit{ è un numero pari.} \qquad (*)$$

Inoltre, se n è pari, i divisori di $n^2 + 1$ sono dispari; e poiché i numeri dispari minori di n sono $n/2$, si ha

$$\textit{se } n \in \mathbb{N}^* \textit{ è pari, allora } \tau(n^2+1) \leq n. \qquad (**)$$

Assumiamo, per assurdo, che a partire da un certo $N \in \mathbb{N}^*$ la funzione $\tau(n^2 + 1)$ sia strettamente crescente (non può essere strettamente decrescente perché in tal caso finirebbe con l'assumere valori negativi). Dal punto $(*)$ segue allora che, per ogni $n \geq N$,

$$\tau((n+1)^2+1) \geq \tau(n^2+1) + 2;$$

in particolare, per ogni $t \geq 1$, $\tau((N+t)^2+1) \geq \tau(N^2+1) + 2t$. Dal punto $(**)$ si deduce che, siccome $N + N$ è pari,

$$2N = N + N \geq \tau((N+N)^2+1) \geq \tau(N^2+1) + 2N,$$

e pertanto

$$\tau(N^2+1) \leq 0$$

il che è assurdo.

COMMENTO. Come avvisato, la soluzione di questo problema non si appella alla proprietà moltiplicativa della funzione τ; la mossa giusta è provare che, per ragioni che poi si rivelano del tutto elementari, se la successione $\tau(n^2 + 1)$ è strettamente crescente allora cresce abbastanza rapidamente $(*)$, ed insieme che non può crescere troppo $(**)$. L'importanza di porre attenzione su cosa 'esattamente' ci viene chiesto di provare, è una possibile morale. Il problema, il cui autore è A. Golovanov, fu proposto ai Giochi Matematici di San Pietroburgo del 1998, e risolto correttamente da solo due concorrenti[4].

* * *

PROBLEMA 111. Poniamo

$$\mathcal{S} = \left\{ \frac{\tau(n^2)}{\tau(n)} \;\middle|\; n \in \mathbb{N}^* \right\}$$

e proviamo che $\mathcal{S} \cap \mathbb{N}^*$ coincide l'insieme D dei numeri positivi dispari. L'inclusione $\mathcal{S} \cap \mathbb{N}^* \subseteq D$ è ovvia, dato che dalla formula (3.4) segue che $\tau(n^2)$ è dispari per ogni $n \in \mathbb{N}^*$.

[4]Riferito in [7].

Per l'inclusione inversa, cominciamo con l'osservare che l'insieme $\mathcal{S}$ è moltiplicativamente chiuso. Infatti il valore di $\tau(n)$ dipende solo dagli esponenti dei primi nella fattorizzazione di n e non dai primi stessi; quindi, se $a, b \in \mathcal{S}$, possiamo trovare due numeri coprimi $n, m \in \mathbb{N}^*$ tali che $a = \tau(n^2)/\tau(n)$ e $b = \tau(m^2)/\tau(m)$, e poiché τ è moltiplicativa,

$$ab = \frac{\tau(n^2)\tau(m^2)}{\tau(n)\tau(m)} = \frac{\tau((nm)^2)}{\tau(nm)} \in \mathcal{S}.$$

Ora, osservato che $1 = \tau(1^2)/\tau(1) \in S$, proviamo per induzione che ogni numero positivo dispari k appartiene a $\mathcal{S}$. Sia dunque $3 \leq k \in D$; allora $k + 1 = 2^r s$, con $r \geq 1$, $s \in D$ e $s < k$. Poniamo $w = k - s = s(2^r - 1) - 1$ e, per $i = 1, \ldots, r$, $a_i = 2^{r-i}w$; osserviamo che, per ogni $i = 2, \ldots r$

$$1 + 2a_i = 1 + 2 \cdot 2^{r-i} = 1 + 2^{r-(i-1)}w = 1 + a_{i-1}.$$

Ora $\mathcal{S}$ contiene il numero razionale

$$\frac{1 + 2a_1}{1 + a_1} \cdot \frac{1 + 2a_2}{1 + a_2} \cdots \frac{1 + 2a_r}{1 + a_r} = \frac{1 + 2a_1}{1 + a_r};$$

quindi, facendo i calcoli,

$$\mathcal{S} \ni \frac{1 + 2a_1}{1 + a_r} = \frac{1 + 2^r w}{1 + w} = \frac{(2^r s - 1)(2^r - 1)}{s(2^r - 1)} = \frac{k}{s}.$$

Ma, per ipotesi induttiva, s appartiene a $\mathcal{S}$, che, per quanto visto, è moltiplicativamente chiuso; dunque $k = (k/s)s \in \mathcal{S}$, completando la dimostrazione.

Commento. Il problema originale, proposto alle Olimpiadi Internazionali di Matematica del 1998, chiedeva di determinare quali fossero i numeri interi della forma $\tau(n^2)/\tau(n)$; ho preferito fornire già la risposta per semplificare un poco (in verità, molto poco) la questione. Per la soluzione, si è rivelato opportuno allargare l'ambito, passando ai numeri razionali in modo da avere un'istanza di moltiplicatività, mentre per l'argomento che stabilisce il passo induttivo è stata utile (almeno nel mio caso) un po' di sperimentazione.

* * *

Problema 112. Sia n intero positivo tale che $4n = \tau(n)^3$. Allora, $3 \mid \nu_p(n)$ per ogni primo $p \geq 3$, mentre $\nu_2(n) \equiv 1 \pmod 3$. Quindi,

$$\tau(n) = \prod_{p|n} (\nu_p(n) + 1) \equiv \nu_2(n) \equiv 1 \pmod 3;$$

da cui $n = 4\tau(n)^3 \equiv 2 \pmod 3$ (in particolare, 3 non divide n).
Se $n = 2^k$, allora $2^{k+2} = (k+1)^3$, da cui $k = 1, 7$. Supponiamo da qui in avanti che n non sia una potenza di 2. Osserviamo ora che, se p è un primo $p \geq 7$ e $m \geq 1$, oppure $p = 5$ e $m \geq 2$,

$$p^{3m} > 4(3m + 1)^3.$$

Supponiamo che n sia diviso da q un primo $q \geq 7$, oppure da $q = 5$ con $\nu_5(n) \geq 4$; allora, tenendo conto che per p dispari $\nu_p(n)$ è un multiplo di 3,

$$\prod_{p|n}(\nu_p(n)+1)^3 = \tau(n)^3 = 4n = 2^{\nu_2(n)+2}q^{\nu_q(n)}\prod_{p\neq 2,q} p^{\nu_p(n)} > 2^{\nu_2(n)+4}\prod_{p\neq 2}(\nu_p(n)+1)^3,$$

da cui

$$(\nu_2(n)+1)^3 > 2^{\nu_2(n)+4},$$

che, come si verifica facilmente, non è soddisfatta per alcun $\nu_2(n) \geq 1$. Dunque $n = 2^m 5^3$, e allora

$$2^{m+2}5^3 = 4n = \tau(n)^3 = (m+1)^3 4^3,$$

da cui si ricava $m + 1 = 5^3$ e pertanto $n = 2^4 5^3$. In conclusione, la risposta al problema è $n = 2, 2^7, 2^4 5^3$.

* * *

Problema 113. Una famiglia infinita che soddisfa le richieste del problema è

$$\{p^{p-1} \mid p \text{ primo},\ p \geq 5\}$$

Proviamo, infatti che se $p \geq 5$ è primo allora $\tau(p^{p-1}n) \neq n$ per ogni $n \in \mathbb{N}^*$.
Se $p \nmid n$, $\tau(p^{p-1}n) = \tau(p^{p-1})\tau(n) = p\tau(n) \neq n$ (dato che $p \nmid n$). Supponiamo allora $p \mid n$, e premettiamo la seguente facile osservazione: sia $k \geq 2$, allora

$$k^a \geq a+1 \text{ per ogni } a \geq 1, \quad \text{e} \quad k^a > 2(a+1) \text{ per ogni } a \geq 4. \tag{$*$}$$

Sia $n = p^a p_1^{a_1} \dots p_t^{a_t}$, con $p_1, \dots, p_t$ primi distinti diversi da p (eventualmente non ce ne sono) e $a, a_1, \dots, a_t \in \mathbb{N}^*$. Per $(*)$,

$$\tau(p^{p-1}n) = (a+p)(a_1+1)\cdots(a_t+1) \leq (a+p)p_1^{a_1}\cdots p_t^{a_t}; \tag{3.12}$$

quindi se, per assurdo, $\tau(p^{p-1}n) = n$, allora $p + a \geq p^a$, che implica $a = 1$ dato che $p \geq 5$. Ciò comporta che p divide qualche $a_i + 1$ con $i \in \{1, \dots, t\}$; in particolare $a_i \geq 4$. Ma allora, per $(*)$ la (3.12) diventa

$$n = \tau(p^{p-1}n) < \frac{1}{2}(p+1)p_1^{a_1}\cdots p_t^{a_t},$$

e dunque $p + 1 > 2p$ che è assurdo.

* * *

Problema 114. Sia n un intero positivo, e supponiamo che, per qualche primo p e un $k \geq 1$, sia $n^{\tau(n)} - 1 = p^k$. Un caso possibile è $n = 2$: infatti $2^{\tau(2)} - 1 = 2^2 - 1 = 3$. Sia $n > 2$; abbiamo

$$p^k = (n^{\frac{\tau(n)}{2}} - 1)(n^{\frac{\tau(n)}{2}} + 1)$$

dove i fattori del termine di destra sono interi positivi (vedi esercizio 3.3). Poiché $n > 2$ nessuno di questi fattori è 1 e quindi, dato che il loro massimo comun divisore è 1 o 2,

si deve avere che entrambi sono potenze di 2. Il solo caso è quando $n^{\tau(n)} - 1 = 2^3$, cioè $n = 3$.
Le terne (n, k, p) cercate sono dunque $(2, 1, 3)$ e $(3, 3, 2)$.

* * *

PROBLEMA 117. Poiché f è moltiplicativa e crescente si ha

$$f(7)^2 f(10)^2 = f(70)^2 \leq f(70)f(71) = f(70 \cdot 71) = f(4970),$$

e, dall'altra parte,

$$f(7)^2 f(8)f(13) = f(7 \cdot 8)f(7 \cdot 13) = f(56)f(91) \geq f(55)f(91) = f(55 \cdot 91) = f(5005).$$

Quindi, $f(7)^2 f(8)f(13) \geq f(5005) \geq f(4970) \geq f(7)^2 f(10)^2$; e poiché $f(7)^2 > 0$ segue la conclusione desiderata.

COMMENTO. Nessun commento...

* * *

PROBLEMA 118. Siano n, p interi con p un primo e $1 < n \leq p$; poniamo $M = n^{p-1} + \ldots + n + 1$. Osserviamo che se t è un divisore primo di $n - 1$, allora $M \equiv p \pmod{t}$ e quindi (poichè $t \leq n - 1 < p$) $t \nmid M$. Dunque $mcd(M, n - 1) = 1$, e pertanto

$$\phi(n^p - 1) = \phi(n - 1)\phi(M).$$

Poichè $p > n - 1$, e quindi certamente $p \nmid \phi(n - 1)$, ci siamo ricondotti a provare che p divide $\phi(n^p - 1)$. Questo è quasi immediato (vedi anche un'osservazione a pagina 11): sia infatti q è un divisore primo di $n^p - 1$; allora, per Fermat, $n^p \equiv 1 \equiv n^{q-1} \pmod{q}$ e dunque $p \mid q - 1$, il che comporta in particolare che p divide $\phi(n^p - 1)$.

* * *

PROBLEMA 119. Sia $n = p^a q^b$ con $p > q$ numeri primo e $a, b \in \mathbb{N}^*$, e supponiamo

$$\phi(\tau(n)) = \tau(\phi(n)).$$

Poiché $p > q$, $q - 1$ è coprimo con p, mentre sia q^s, con $s \geq 0$, la massima potenza di q che divide $p - 1$; allora $(p - 1)(q - 1) = q^s x$ con x coprimo con pq (osserviamo che $q - 1 \mid x$). Dunque

$$\tau(\phi(n)) = \tau(p^{a-1}(p - 1)q^{b-1}(q - 1)) = \tau(p^{a-1}q^{b+s-1}x) = a(b + s)\tau(x). \qquad (*)$$

Osserviamo che se $\tau(x) = 1$ allora $x = 1$; in particolare $q - 1 = 1$, cioè $q = 2$ e dunque $s \geq 1$. In ogni caso, quindi, $\tau(\phi(n)) \geq a(b + 1)$.
D'altra parte, usando anche l'esercizio 3.13,

$$\phi(\tau(n)) = \phi((a + 1)(b + 1)) \leq \phi(a + 1)(b + 1).$$

Poiché $\phi(a + 1) \leq a$, dal confronto con la $(*)$ e quanto osservato subito dopo, si ricavano nell'ordine le seguenti conseguenze:

(1) $\phi(a+1) = a$, quindi $a+1$ è un numero primo;
(2) $\phi(\tau(n)) = a(b+1)$;
(3) $b = 1$ oppure $x = 1$: quindi $q = 2$ e $p - 1 = 2^s$.

Se $b = 1$, allora $b + 1 = 2$ e da (2), riutilizzando l'esercizio 3.13, $2a = \phi(\tau(n)) \leq a + 1$, da cui $a = 1$. Ma allora

$$\tau((p-1)(q-1)) = \tau(\phi(n)) = \phi(\tau(n)) = \phi(4) = 2,$$

quindi $(p-1)(q-1)$ è un numero primo; cosa che si verifica solo per $q = 2, p = 3$, cioè $n = 6$. In effetti $\phi(\tau(6)) = 2 = \tau(\phi(6))$, e $n = 6$ è una soluzione.

Sia $b > 1$. Allora, per (3), $q = 2$ e $p = 2^s$. In particolare $s \geq 1$ e dunque da (2) segue necessariamente $s = 1$, cioè $p = 3$. Inoltre, da (1) $r = a + 1$ è un numero primo. Sia $b + 1 = r^k m$ con $k \geq 0$ e $mcd(r, m) = 1$; allora

$$a(b+1) = \phi(\tau(n)) = \phi((a+1)(b+1)) = \phi(r^{k+1}m) = (r-1)r^k\phi(m) = ar^k\phi(m),$$

dunque $m = 1$ e $b + 1 = r^k$.
A questo punto, formuliamo la ipotesi che sono soluzioni tutti numeri del tipo $n = 3^a 2^b$, con $a = r - 1$, $b = r^k - 1$ dove r è un primo e $k \geq 1$. Infatti è così:

$$\tau(\phi(n)) = \tau(3^{a-1}2^b) = a(b+1) = (r-1)r^k = \phi(r^{k+1}) = \phi((a+1)(b+1)) = \phi(\tau(n)).$$

Anche la soluzione $n = 6$, precedentemente trovata, rientra in questa casistica, che quindi è condizione necessaria e sufficiente.

* * *

Problema 120. Chiaramente la condizione data implica $a_1 < a_2 < \ldots < a_k$, quindi $a_1 = 1$ e $a_k = n - 1$ (si osservi anche che, poiché $n > 6$, $k = \phi(n) \geq 3$). Se n è dispari, $a_2 = 2$, ed allora $a_t = t$ per ogni $1 \leq t \leq k$, dunque $k = n - 1$ e n è un numero primo.
Possiamo assumere ora che n sia pari. Poiché a_2 è il più piccolo intero $\neq 1$ che è coprimo con n, $a_2 = p$ è un numero primo (dispari); inoltre, dato che $a_2 - a_1 = p - 1$, per ogni $2 \leq t \leq k$ si ha $a_t = 1 + (t-1)(p-1)$. In particolare,

$$n = a_k + 1 = (k-1)(p-1) + 2. \qquad (*)$$

Sia q un divisore primo di $p - 1$. Poiché $a_1 < q < p = a_2$, p divide n, e dalla $(*)$ segue allora $q = 2$. Pertanto $p = 2^m + 1$ con m una potenza di 2, dato che p è primo.
Se $p = 3$, allora $a_1, \ldots, a_k$ sono tutti e soli i numeri dispari minori di n e dunque n è necessariamente una potenza di 2.
Se $p > 3$, allora 3 divide n; d'altra parte, poiché $m+1$ è dispari, 3 divide anche $2^{m+1}+1 = 2p - 1 = a_3$, che è una contraddizione.

3.5. Altri problemi

Problema 121 (L. Carlitz, Amer. Math. Monthly[5]). *Una funzione aritmetica f si dice* totalmente moltiplicativa *se*

$$f(nm) = f(n)f(m) \quad \textit{per ogni } n, m \in \mathbb{N}^*.$$

[5] La rivista *American Mathematica Monthly* è

Si provi che una funzione aritmetica f è totalmente moltiplicativa se e solo se, per ogni $n \in \mathbb{N}^*$,

$$(f * f)(n) = f(n)\tau(n).$$

SUGGERIMENTO. In un verso, l'affermazione discende facilmente dalla definizione di prodotto di convoluzione. Per il viceversa, si assuma che f sia una funzione aritmetica tale che si abbia $f * f = f\tau$: si provi che $f(1) = 1$, quindi che $f(p^n) = f(p)^n$ per ogni primo p e $n \geq 1$; a questo punto basta provare che f è moltiplicativa.

Problema 122 (Russia 2001)**.** *Si dica se esiste un intero positivo tale che l'espressione decimale del prodotto dei suoi divisori termina con esattamente* 2001 *zeri.*

SUGGERIMENTO. Si applichi l'esercizio 3.3 (la risposta è affermativa).

Problema 123 (Romania 2002)**.** *Siano p, q due primi distinti. Si provi che esistono interi positivi a, b tali che il valore medio dei divisori di $p^a q^b$ è un numero intero.*

SUGGERIMENTO. Questo è facile.

Problema 124 (Baltic Way 2010)**.** *Con $S(k)$ denotiamo la somma delle cifre nella rappresentazione decimale dell'intero positivo k. L'intero positivo n si dice* divertente *se esiste un $k \in \mathbb{N}^*$ tale che $\tau(k) = S(k) = n$. Dire qual è il più piccolo intero dispari divertente maggiore di* 1*.*

SUGGERIMENTO. I numeri dispari $3, 5, 7$ sono anche primi; quindi coincidono con $\tau(k)$ solo se k è la potenza di un primo. Tenuto conto di questo, escludere che $3, 5, 7$ siano divertenti. Quindi, provare con $9\ldots$

Problema 125 (Irlanda 1998)**.** *Siano $1 = d_1 < d_2 < \ldots < d_{16} = n$ i divisori positivi di $n \in \mathbb{N}^*$. Sapendo che $d_6 = 18$ e che $d_9 - d_8 = 17$, si determini n.*

SUGGERIMENTO. Poiché $\tau(n) = 16$, se p^a è la massima potenza di un primo p che divide n, allora $a = 1, 3, 7$ o 15. Dal fatto che $d_6 = 18$ divide n si deduce che se n è diviso da un primo $p \neq 2, 3$ allora $n = 2 \cdot 3^3 \cdot p$, inoltre, dato che $\tau(d_6) = \tau(18) = 6$, $p \geq 19$; usare la seconda condizione ($d_9 - d_8 = 17$) per provare che $p = 37$ oppure $p = 71$. Altrimenti, i soli primi che dividono n sono 2 e 3, e si presentano i due soli casi $n = 2^3 \cdot 3^3$ e $n = 2 \cdot 3^7 \ldots$

Problema 126 (EM Cup, 2014)**.** *Si provi che esistono infiniti numeri interi positivi che non possono essere scritti nella forma*

$$a^{\tau(a)} + b^{\tau(b)}$$

cone $a, b \in \mathbb{N}^*$

SUGGERIMENTO. Provare che per ogni $n \in \mathbb{N}^*$, se 3 non divide n allora $n^{\tau(n)} \equiv 1 \pmod 3$. Da ciò dedurre che se $n = a^{\tau(a)} + b^{\tau(b)}$ e $3|n$ allora $3|a$ e $3|b$; trarne una immediata conseguenza e concludere esibendo un insieme infinito di numeri positivi che non si può scrivere nella forma $a^{\tau(a)} + b^{\tau(b)}$.
A questo punto potete cimentarvi con una versione più difficile: provare che esistono infiniti $n \in \mathbb{N}^*$ che non possono essere scritti nella forma $a^{\tau(b)} + b^{\tau(a)}$, con $a, b \in \mathbb{N}^*$.

Problema 127 (Putnam, 1969)**.** *Sia n intero positivo; provare che se $24 \mid n$ allora $24 \mid \sigma(n-1)$.*

SUGGERIMENTO. Mettete da parte le formule: se $24 \mid n$ allora $n-1$ non è un quadrato in $\mathbb{N}$ (perché?), quindi i suoi divisori possono essere raggruppati a coppie $\{d, (n-1)/d\}$ di elementi distinti; a questo punto,

$$d + \frac{n-1}{d} = \frac{d^2 - 1 + n}{d},$$

e siccome $mcd(d, 24) = 1$ basterà provare che 24 divide $d^2 - 1 \ldots$

Problema 128 (IMO, Glasgow 2002)**.** *Per ogni intero $n \geq 2$, se $1 = d_1 < d_2 < \ldots < d_t = n$ sono i divisori positivi di n, poniamo $g(n) = d_1 d_2 + d_2 d_3 + \ldots + d_{t-1} d_t$.*

1) Si provi che $g(n) \leq n^2$ per ogni $n \geq 2$.

2) Si determinino tutti gli interi $n \geq 2$ tali che $g(n)$ divide n^2.

SUGGERIMENTO. Per il punto (1), dopo aver provato che

$$g(n) = \frac{n^2}{d_1 d_2} + \ldots + \frac{n^2}{d_{t-1} d_t}, \qquad (*)$$

potrà essere utile rispolverare l'espressione delle somme parziali nelle serie di Mengoli:

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

Per il punto (2), si osservi che da $(*)$ segue

$$\frac{n^2}{d_1 d_2} \leq g(n) \leq n^2,$$

quindi, se $g(n)$ divide n^2 ...

Problema 129 (San Pietroburgo, 2014)**.** *Si provi che, per ogni $n \in \mathbb{N}^*$, il numero di divisori positivi di n la cui ultima cifra è 1 o 9 è maggiore o uguale a quello dei divisori positivi di n la cui ultima cifra è 3 o 7.*

SUGGERIMENTO. Se i, j sono cifre da 0 a 9, per ogni $n \in \mathbb{N}^*$ si denoti con $\tau_{i,j}(n)$ il numero di divisori positivi di n la cui ultima cifra in rappresentazione decimale è i o j. Si studi il, mutuo, comportamento delle funzioni $\tau_{1,9}$ e $\tau_{3,7}$, quando applicate alle potenza di un primo, e quando al prodotto di due interi tra loro coprimi. Si dimostri quindi l'asserto del Problema ragionando per induzione su n.

Problema 130 (EGMO[6], 2014)**.** *Per ogni $n \in \mathbb{N}^*$, $\omega(n)$ denota il numero di primi distinti che dividono n. Si provi che per ogni $k \in \mathbb{N}^*$ esistono infiniti interi positivi n tali che $\omega(n) = k$ e $\tau(n)$ non divide $\tau(a^2 + b^2)$ per ogni coppia di interi positivi a, b tali che $a + b = n$.*

[6] *European Girls' Mathematical Olympiad.* Si disputa dal 2012.

SUGGERIMENTO. L'idea è di fare in modo che $\tau(n)$ sia diviso da un primo p che non divida alcun valore $\tau(a^2+b^2)$, con $a+b=n$; e p andrà scelto abbastanza grande in modo da rendere possibile l'analisi che lo escluda dai divisori di $\tau(a^2+b^2)$. Si considera quindi

$$n = 2^{p-1}p_1 \cdots p_{k-1},$$

con p un primo sufficientemente grande e $p_1, \ldots, p_{k-1}$ primi distinti dispari (prendere $p_i \geq 5$ per ognuno di questi primi non è strettamente necessario ma semplifica qualche passaggio). Allora $\omega(n) = k$ e $\tau(n) = p2^{k-1}$. Siano $a, b \in \mathbb{N}^*$ tali che $a+b=n$ e $p|\tau(a^2+b^2)$; allora esiste un primo q tale che $a^2+b^2 = q^s c$ con $(q,c)=1$ e $s \equiv -1 \pmod{p}$. Si proceda provando che, per p sufficientemente grande, $q=2$ e $s=p-1$; dopo di che si pervenga ad un assurdo: l'analisi è abbastanza elementare, ma va fatta con attenzione. [Poiché questo problema è piuttosto artificioso, più sotto trovate la soluzione scritta per esteso.]

Problema 131 (Czech-Polish-Slovak, 2012)**.** *Trovare tutti gli interi positivi n tali che uno dei tre numeri $n, \tau(n), \phi(n)$ è la media aritmetica degli altri due.*

SUGGERIMENTO. $n \geq \tau(n)$, $n \geq \phi(n)$. Ci sono quindi due casi; nel caso in cui $\tau(n)$ è il valore medio, si ha $\tau(n) > n/2$; nell'altro caso è $\phi(n) > n/2$ ... [anche di questo trovate la soluzione completa più sotto.]

Per ultimo, un problema che riguarda i numeri primi (soluzione più sotto).

Problema 132 (Canada 2017)**.** *Sia $f : \mathbb{N}^* \to \mathbb{N}^*$ tale che $f(f(n)) = \tau(n)$ per ogni $n \in \mathbb{N}^*$. Provare che se p è un primo allora $f(p)$ è un primo.*

* * *

SOLUZIONE (del problema 130). Per $k \geq 1$, siano $p_1, \ldots, p_{k-1}$ primi distinti maggiori o uguali a 5 (fissati), e consideriamo $n = 2^{p-1}p_1 \cdots p_{k-1}$, con p un primo sufficientemente grande. Poiché $\lim_{m\to\infty} \frac{4^m}{5^m} = 0$ possiamo scegliere p in modo che $n^2 < 5^{p-1}$ (e di tali p ce ne sono infiniti).
Siano $a, b \in \mathbb{N}^*$ con $a+b=n$ e supponiamo, per assurdo che p divida a^2+b^2. Allora esiste un primo q tale che $a^2+b^2 = q^s c$ con $(q,c)=1$ e $s \equiv -1 \pmod{p}$. In particolare $q^{p-1} \leq a^2+b^2 < n^2$ e dunque, per la scelta di p fatta sopra, $q < 5$.
Sia $q=3$, allora poiché $x^2 \equiv 0, 1 \pmod{3}$ per ogni intero x, si deduce che 3 divide sia a che b, dunque 3 divide $a+b=n$, contro la scelta dei primi p_i.
Dunque, $q=2$ e $s=p-1$ oppure $s=2p-1$. Poiché, per ogni intero x, $x^2 \equiv 0, 1 \pmod{4}$, si ha che a e b sono entrambi pari; scriviamo

$$a = 2^{\nu_2(a)}x, \quad b = 2^{\nu_2(b)}y,$$

con $1 \leq \nu_2(a) \leq \nu_2(b)$, e x, y dispari. Allora,

$$n = a+b = 2^{\nu_2(a)}(x + 2^{\nu_2(b)-\nu_2(a)}y). \tag{$*$}$$

Se $\nu_2(a) < \nu_2(b)$ allora da $(*)$ segue $\nu_2(a) = p-1$, e conseguentemente,

$$p^s c = a^2+b^2 = 2^{p-1}(x^2 + 2^{2\nu_2(b)-2\nu_2(a)}y^2)$$

da cui la contraddizione $s = 2p - 2$.
Dunque $\nu_2(a) = \nu_2(b)$; ma allora, poiché $x^2 + y^2 \equiv 2 \pmod 4$,

$$2^s c = 2^{2\nu_2(a)}(x^2 + y^2) = 2^{2\nu_2(a)+1} c < n^2 = 2^{2p-2}(p_1 \cdots p_{k-1})^2,$$

quindi $2\nu_2(a) + 1 = s = p - 1$, che è ancora una contraddizione, dato che $p - 1$ è pari. ∎

Soluzione (del problema 131). Sia $n \in \mathbb{N}^*$ tale che uno tra $n, \phi(n), \tau(n)$ è la media aritmetica degli altri due. Come detto nel suggerimento, si presentano due casi.
(1) $\tau(n) = (n + \phi(n))/2$. In questo caso, $\tau(n) > n/2$. Ma allora, per l'esercizio 3.2,

$$4\sqrt{n} \geq 2\tau(n) > n,$$

quindi $n < 16$ ed esaminando direttamente i casi possibili si trova che la richiesta è soddisfatta per $n = 4, 6$.
(1) $\phi(n) = (n + \tau(n))/2$. In questo caso, $\phi(n) > n/2$. E si vede subito (esercizio 3.13) che n deve essere dispari; quindi, anche $\tau(n)$ è dispari. Sia

$$n = p_1^{a_1} \cdots p_t^{a_t},$$

con $p_1 < p_2 < \ldots < p_t$ primi e $a_1, \ldots, a_t \in \mathbb{N}^*$. Poichè $\tau(n) = (a_1 + 1) \ldots (a_t + 1)$ è dispari, $a_i = 2x_i$ è pari per ogni indice $i = 1, \ldots, t$. Da ciò segue che $M = p_1^{2x_i - 1} \cdots p_t^{2x_t - 1}$ divide $\phi(n)$ e quindi divide $\tau(n)$; in particolare $M \leq \tau(n)$. Ora, si verifica facilmente (ad esempio per induzione su x_i) che, poichè $p_i \geq 3$,

$$p_i^{2x_i - 1} \geq 2x_i + 1$$

per ogni $i = 1, \ldots, t$, e che si ha l'eguaglianza soltanto nel caso $p_i = 3$ e $x_i = 1$. Quindi, $M \leq \tau(n)$ si verifica solo per $n = 3^2$.
Poichè in effetti $(9 + \tau(9))/2 = 6 = \phi(9)$, concludiamo la soluzione dicendo che gli interi n cercati sono $n = 4, 6, 9$. ∎

Soluzione (del Problema 132). Per ogni $n \in \mathbb{N}^*$, scriviamo $f^2(n) = f(f(n))$; per ipotesi $f^2(n) = \tau(n)$. Per ogni primo p si ha

$$\tau(f(p)) = f^2(f(p)) = f(f^2(p)) = f(\tau(p)) = f(2). \qquad (*)$$

Ora,

$$f(2) = f(\tau(2)) = f(f^2(2)) = f^2(f(2)) = \tau(f(2)),$$

e dunque $f(2) \in \{1, 2\}$. Se $f(2) = 1$, allora $f(1) = f^2(2) = \tau(2) = 2$ e $\tau(f(3)) = 1$ per $(*)$; quindi

$$1 = f(3) = f(\tau(4)) = f(f^2(4)) = f^2(f(4)) = \tau(f(4)),$$

cioè $f(4) = 1$, e infine la contraddizione $3 = \tau(4) = f^2(4) = f(1) = 2$.
Dunque $f(2) = 2$; ma allora da $(*)$ segue che, per ogni primo p, $\tau(f(p)) = 2$, il che implica che $f(p)$ è un primo. ∎

4

Congruenze

In questo capitolo, intraprendiamo uno studio più approfondito delle congruenze (dopo aver ricordato alcune proprietà fondamentali nella sezione 1.3), iniziando dalla generalizzazione, dovuta a Eulero, del Teorema di Fermat, per arrivare al celebre Teorema di Reciprocità Quadratica di Gauss.
Un certo avanzamento nella comprensione di quel che succede si avrebbe utilizzando, in modo più sistematico di quanto faremo, la struttura algebrica degli insiemi di classi di resto $\mathbb{Z}/n\mathbb{Z}$, che, come sappiamo dal corso di Algebra 1, costituiscono naturalmente un anello commutativo e, in particolare, un campo quando n è un numero primo. Cercheremo, però, di rimanere fedeli al proposito di mantenere i prerequisiti ad un livello quanto possibile pre-universitario (daremo per conosciuto il fatto che se $0 \neq f(x)$ è un polinomio a coefficienti interi e $a \in \mathbb{Z}$, allora $f(x) - f(a) = (x-a)g(x)$ con $g(x)$ un polinomio a coefficienti interi). Affideremo poi a qualche "nota algebrica" la spiegazione (per chi - come voi - già conosce questi concetti) di come trattare le stesse cose utilizzando semplici nozioni relative ai gruppi ed ai campi.

4.1. Teorema di Eulero

Il Teorema di Eulero generalizza il Teorema di Fermat.

Teorema 4.1 (Eulero)**.** *Sia n un intero positivo, e sia $a \in \mathbb{Z}$ tale che $mcd(n,a) = 1$. Allora*

$$a^{\phi(n)} \equiv 1 \, (mod\, n)$$

Il caso particolare in cui $m = p$ è il Teorema 1.14 di Fermat.

Dimostrazione. La dimostrazione è analoga a quella del Teorema di Fermat vista nel corso di Algebra I. Sia $n \geq 2$ e sia $B = \{b_1, b_2, \ldots, b_{\phi(n)}\}$ l'insieme di tutti i numeri interi compresi tra 1 e $n-1$ che sono coprimi con n. Sia a un numero intero con $mcd(a,n) = 1$. Per ogni $i = 1, \ldots, \phi(n)$, si ha $mcd(ab_i, n) = 1$, dunque

$$ab_i \equiv b_{\alpha(i)} \pmod{n},$$

con $\alpha(i) \in \{1, \dots, \phi(n)\}$. Sia $b_{\alpha(i)} = b_{\alpha(j)}$, per qualche $b_i, b_j \in B$; allora $ab_i \equiv ab_j \pmod{n}$, ovvero n divide $a(b_i - b_j)$; dunque, poiché $mcd(a, n) = 1$, n divide $b_i - b_j$, il che implica $b_i = b_j$. Dunque la funzione $B \to B$ definita da $b_i \mapsto b_{\alpha(i)}$ è una biezione.
Posto $b = b_1 b_2 \cdots b_{\phi(n)}$, si ricava quindi

$$a^{\phi(n)} b = (ab_1)(ab_2) \cdots (ab_{\phi(n)}) \equiv b_1 b_2 \cdots b_{\phi(n)} = b \pmod{n}.$$

Dunque, n divide $(a^{\phi(n)} - 1)b$. Poiché n e b sono coprimi, n divide $a^{\phi(n)} - 1$. □

Siano a, n interi coprimi, con n positivo; il minimo $d \geq 1$ tale che $a^d \equiv 1 \pmod{n}$ si chiama ordine di a modulo n e si denota con $o_n(a)$. Per il Teorema 4.1, $o_n(a) \leq \phi(n)$. Infatti,

Proposizione 4.2. *Siano a un intero, n, t interi positivi tali che*

$$a^t \equiv 1 \pmod{n}.$$

Allora $o_n(a) \mid t$; in particolare per ogni $a \in \mathbb{Z}$ con $mcd(a, n) = 1$, $o_n(a) \mid \phi(n)$.

Dimostrazione. Siano n, t, a come nelle ipotesi, e $d = o_n(a)$. Allora n divide sia $a^d - 1$ che $a^t - 1$. Se $a = 1$, non c'è nulla da provare. Se $a \neq 1$, per la Proposizione 1.11, n divide $a^{mcd(d,t)} - 1$. Per la minimalità di d si ha per forza $mcd(d, t) = d$, cioè $d \mid t$.
Poiché, per il Teorema di Eulero, per ogni intero a coprimo con n, $a^{\phi(n)} - 1$, si ricava in particolare $o_n(a) \mid \phi(n)$. □

Esempio 1. *Siano a, n interi positivi, $a \geq 2$. Provare che $n \mid \phi(a^n - 1)$.*

Questo arriva quasi per definizione; infatti, a e $a^n - 1$ sono coprimi, inoltre, chiaramente, $n = o_{a^n-1}(a)$, e la conclusione segue dalla Proposizione 4.2.

Esempio 2. *Siano a, b interi positivi coprimi. Provare che esistono interi positivi n, m tali che $a^n + b^m \equiv 1 \pmod{ab}$.*

Basta prendere $n = \phi(b)$ e $m = \phi(a)$. Infatti, poiché $mcd(a, b) = 1$, per il Teorema di Eulero,

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{a} \quad \text{e} \quad a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{b}$$

dunque $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$.

Esempio 3. *Poniamo $b_1 = 7$ e, per ogni $n \geq 1$, $b_{n+1} = 7^{b_n}$. Determinare le ultime tre cifre nella rappresentazione decimale di b_n, per $n \geq 2$.*

Avendo in animo di applicare il Teorema di Eulero, e poiché $\phi(1000) = \phi(2^3)\phi(5^3) = 400$, cerchiamo di studiare il residuo modulo 400 di b_n.
Iniziamo da $7^4 - 1 = (7^2 - 1)(7^2 + 1)$, che è un multiplo di 400. Osserviamo poi che, poiché $7 \equiv -1 \pmod{4}$ e, per ogni $n \geq 1$, b_n è dispari, si ha $b_n \equiv -1 \equiv 3 \pmod{4}$, per ogni $n \geq 1$. Quindi, per $n \geq 2$, $b_{n-1} = 4k + 3$ per qualche $k \in \mathbb{N}^*$, e dunque

$$b_n = 7^{b_{n-1}} = (7^4)^k \cdot 7^3 \equiv 7^3 = 343 \pmod{400}.$$

A questo punto, osserviamo che $5^2 \mid 7^4 - 1$; dunque per il Teorema 2.6, 5^3 divide $7^{20} - 1$. Quindi,

$$7^{20} \equiv 1 \pmod{2^3 \cdot 5^3}.$$

Concludendo, sia $n \geq 3$; allora $b_{n-1} = 400r + 343$ per qualche $r \in \mathbb{N}$; per il Teorema di Eulero e quanto sopra osservato,

$$b_n = 7^{b_{n-1}} = (7^{400})^r \cdot 7^{343} \equiv 7^{343} = (7^{20})^{17} \cdot 7^3 \equiv 7^3 = 343 \pmod{1000}.$$

Siano a, n interi coprimi con $n \geq 2$, e sia $d = 0_n(a)$, allora per ogni $1 \leq i \leq j \leq d-1$,

$$a^i \equiv a^j \pmod{n} \quad \Leftrightarrow \quad i = j.$$

Infatti, se $a^i \equiv a^j \pmod{n}$ allora $n \mid a^i(a^{j-i} - 1)$, quindi, poiché a, n sono coprimi, $n \mid a^{j-i} - 1$, e siccome $0 \leq j - i < d = o_n(a)$ deve essere $j = i$ per definizione di ordine di a modulo n.

Ci restringiamo ora al caso in cui il modulo è un numero primo. Il prossimo Lemma è la versione per congruenze sul massimo numero di soluzioni distinte di un equazione polinomiale.

Lemma 4.3 (Teorema di Lagrange)**.** *Sia p un primo positivo, e sia $f \in \mathbb{Z}[x]$ un polinomio di grado $n \geq 1$ a coefficienti interi, non tutti multipli di p. Allora il numero di elementi $a \in \{0, 1, \ldots, p-1\}$ tali che*

$$f(a) \equiv 0 \pmod{p} \tag{4.1}$$

è al più n.

Dimostrazione. Poniamo $A = \{0, \ldots, p-1\}$ l'insieme dei residui modulo p e procediamo per induzione su n. Se $n = 1$ l'equazione è lineare e sappiamo dalla teoria precedente che essa ammette al più una soluzione nell'insieme A.
Sia $n \geq 2$, e supponiamo che esista $a \in A$ con $f(a) \equiv 0 \pmod{p}$ (se non esiste non resta più nulla da provare). Poiché $x - a \in \mathbb{Z}[x]$ è monico, si può scrivere, nell'anello dei polinomi $\mathbb{Z}[x]$,

$$f(x) = (x - a)g(x) + f(a)$$

cone $g(x) \in \mathbb{Z}[x]$, di grado $n - 1$. Sia ora $b \in A$ tale che $f(b) \equiv 0 \pmod{p}$, e $b \neq a$ (quindi $b \not\equiv a \pmod{p}$); allora

$$0 \equiv f(b) - f(a) = (b - a)g(a) \pmod{p}$$

e quindi, poiché p è un primo e non divide $b - a$, $g(a) \equiv 0 \pmod{p}$; osserviamo anche che, siccome $p \mid f(a)$, p non divide tutti i coefficienti di $g(x)$. Dunque, per ipotesi induttiva, vi sono al più $n - 1$ elementi di A, diversi da a, che verificano (4.1), che fornisce quel che si voleva. □

Fissiamo ora la seguente convenzione (valida per il resto di questa sezione): dato p è un primo fissato, per ogni $a \in \mathbb{Z}$ scriviamo $[a]$ il resto della divisione di a per p (ovvero l'unico elemento appartenente a $\{0, 1, \ldots, p-1\}$ che è congruo ad a modulo p.

Proposizione 4.4. *Siano p un numero primo e d un divisore positivo di $p - 1$; allora*

(i) il numero di interi $1 \leq a \leq p - 1$ tali che $o_p(a) = d$ è $\phi(d)$;

(ii) la congruenza $x^d \equiv 1 \pmod{p}$ ha esattamente d soluzioni (a meno di congruenza modulo p).

Dimostrazione. Sia $A = \{1, 2, \ldots, p-1\}$; per ogni divisore positivo d di $p-1$ poniamo $E_d = \{a \in A \mid a^d \equiv 1 \pmod{p}\}$, e $\psi(d) = \{a \in A \mid o_p(a) = d\}$. Chiaramente, $\psi(d) \subseteq E_d$; inoltre, per la Proposizione 4.2,

$$\sum_{d|p-1} |\psi(d)| = |A| = p - 1.$$

Supponiamo $\psi(d) \neq \emptyset$, allora esiste un elemento $a \in A$ tale che $o_p(a) = d$, e per ogni $0 \leq i \leq d-1$ si ha $(a^i)^d \equiv 1 \pmod{p}$. Ora $1 = a^0, a, \ldots, a^{d-1}$ sono d elementi che, per l'osservazione che precede il Lemma 4.3, sono a due a due non congruenti modulo p, dunque, per il Lemma 4.3 stesso, costituiscono un insieme di rappresentanti di tutte le soluzioni di $x^d \equiv 1 \pmod{p}$. Quindi $E_d = \{[1], [a], \ldots, [a^{d-1}]\}$.
Ora, per $0 \leq j \leq d-1$, posto $t = mcd(j, d)$ si ha

$$(a^j)^{\frac{d}{t}} = (a^d)^{\frac{j}{t}} \equiv 1 \pmod{p}$$

e dunque $o_p(a^j) \leq \frac{d}{t}$. Pertanto

$$\psi(d) \subseteq \{[a^j] \mid 0 \leq j \leq d-1,\ mcd(k, d) = 1\}.$$

Abbiamo così provato che, per ogni divisore positivo d di $p-1$,

$$|\psi(d)| \leq \phi(d)$$

(questo include il caso eventuale in cui $\psi(d)$ sia vuoto). Ma allora, ricordando il Lemma 3.11,

$$p - 1 = \sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \phi(d) = p - 1.$$

Dunque, non può che essere $\psi(d) = \phi(d)$ per ogni divisore positivo d di $p-1$, il che prova il punto (ii).
Per il punto (ii) basterà osservare che, per ogni $d \mid p-1$, $\psi(d) \neq \emptyset$ e concludere, ragionando come sopra, che $|E_d| = d$. □

In particolare, si ha che se p è un numero primo allora esistono $\phi(p-1)$ interi $1 \leq a \leq p-1$ tali che $o_p(a) = p-1$. Un intero a tale che $o_p(a) = p-1$ si dice *primitivo* (o radice primitiva) modulo p. Fissato un primo p è però cosa assai difficile determinare esplicitamente i numeri primitivi modulo p.

Vediamo altre immediate conseguenze della Proposizione 4.4.

Corollario 4.5. *Siano p, n interi positivi, p un numero primo, e $d = mcd(n, p-1)$. Allora la congruenza*

$$x^n \equiv 1 \pmod{p}$$

ha esattamente d soluzioni (a meno di congruenza modulo p).

Dimostrazione. Se $a \in \mathbb{Z}$ è soluzione di $x^n \equiv 1 \pmod{p}$, allora in particolare $p \nmid a$, e quindi, per il Teorema di Fermat p divide $a^{p-1} - 1$; dunque, per la Proposizione 1.11, p divide

$$mcd(a^n - 1, a^{p-1} - 1) = a^d - 1,$$

ovvero a è soluzione di $x^d \equiv 1 \pmod{p}$. Viceversa, poiché $d \mid n$, è chiaro che le soluzioni di quest'ultima congruenza sono soluzioni di $x^n \equiv 1 \pmod{p}$. Si conclude quindi per la Proposizione 4.4. □

Corollario 4.6. *Siano p un numero primo e n un intero positivo coprimo con $p-1$; allora per ogni intero a la congruenza*

$$x^n \equiv a \pmod{p}$$

ammette una e una sola soluzione a meno di congruenza modulo p.

Dimostrazione. Se $p \mid a$, allora, a meno di congruenza modulo p, l'unica soluzione è $x = 0$. Suppongo a coprimo con p. Siano b, c interi coprimi con p e tali che $b^n \equiv c^n \pmod{p}$, e sia $c' \in \{1, 2, \ldots, p-1\}$ tale che $cc' \equiv 1 \pmod{p}$. Allora

$$(bc')^n \equiv (cc')^n \equiv 1 \pmod{p}$$

e dunque $bc' \equiv 1 \pmod{p}$: per il Corollario 4.5 la congruenza $x^n \equiv 1 \pmod{p}$ ha, a meno di congruenza modulo p, un'unica soluzione $x = 1$. Dunque $b \equiv c \pmod{p}$. Questo mostra che l'insieme $\{0^n, 1^n, 2^n, \ldots, (p-1)^n\}$ è un sistema di rappresentanti delle classi di congruenza modulo p, e da ciò deriva immediatamente il Corollario. □

Esercizio 4.1. Si trovino le soluzioni di $x^2 \equiv 1 \pmod{35}$. Si concluda che la Proposizione 4.4 non è validea in generale se il modulo non è un numero primo.

NOTA ALGEBRICA. Sia $n \geq 2$, allora l'insieme $\mathbb{Z}/n\mathbb{Z}$ delle classi di congruenza modulo n è un anello commutativo; per ogni intero a, denotiamo con $\bar{a}$ la classe di congruenza di a modulo n. L'insieme degli elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$, $U(\mathbb{Z}/n\mathbb{Z}) = \{\bar{a} \mid 1 \leq a \leq n-1 \mid mcd(a, n) = 1\}$, è un gruppo moltiplicativo di ordine $\phi(n)$; quindi per ogni $a \in \mathbb{Z}$ coprimo con n, $\bar{a}^{\phi(n)} = \bar{1}$, e questo è il teorema 4.1 di Eulero.
Se p è un numero primo, $\mathbb{Z}/p\mathbb{Z}$ è un campo e quindi $U(\mathbb{Z}/p\mathbb{Z}) = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ è un gruppo ciclico di ordine $p-1$ (la dimostrazione è essenzialmente quella del punto (i) della Proposizione 4.4). Sia d un divisore positivo di $p-1$ e $\overline{u}$ un generatore di $U(\mathbb{Z}/p\mathbb{Z})$, e sia $p-1 = de$; allora $\langle \overline{u}^e \rangle$ è un sottogruppo di F^* di ordine esattamente d, ed è l'insieme degli elementi $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ tali che $\bar{a}^d = \bar{1}$ (questa è la Proposizione 4.4).

Problemi

Problema 133 (Sierpinski[1]). *Si provi che per ogni intero positivo k esiste un intero positivo n tale che k è la somma delle cifre decimali di n (cioè $k = S(n)$) e $k \mid n$.*

[1] Waclaw Sierpinski (1882–1969), matematico polacco.

SOLUZIONE. Se $mcd(10,k)=1$, si prende

$$n = 10^{k\phi(k)} + 10^{(k-1)\phi(k)} + \ldots + 10^{2\phi(k)} + 10^{\phi(k)}.$$

Allora (poiché n ha k cifre uguali a 1 e le altre 0) $S(n)=k$. Inoltre, per il Teorema di Eulero, $n \equiv k \equiv 0 \pmod{k}$, ovvero $k \mid n$.
Nel caso generale, si scrive $k=md$ con $d=2^i5^j$, per $i,j \in \mathbb{N}$, e $mcd(m,10)=1$; posto $r=\max\{i,j\}$, si prende

$$n = 10^r(10^{k\phi(d)} + 10^{(k-1)\phi(d)} + \ldots + 10^{2\phi(d)} + 10^{\phi(d)})$$

e funziona. ■

Problema 134 (IMO, Tokio 2003)**.** *Sia p un numero primo. Si provi che esiste un numero primo q tale che, per ogni intero positivo n, $n^p - p$ non è divisibile per q.*

SOLUZIONE. Sia p un numero primo; vogliamo provare che esiste un primo q tale che la congruenza

$$x^p \equiv p \pmod{q}$$

non ha soluzioni. Per il Corollario 4.6, si deve avere $mcd(p, q-1) > 1$, quindi $p \mid q-1$. Allora, per il Teorema di Eulero, per ogni intero n,

$$1 \equiv (n^p)^{\frac{q-1}{p}} \equiv p^{\frac{q-1}{p}} \pmod{q}.$$

Quindi, cerchiamo un primo q tale che $p \mid q-1$ e l'ordine di p modulo q non divida $\frac{q-1}{p}$. Consideriamo il numero

$$k = \frac{p^p - 1}{p-1} = p^{p-1} + \ldots + p + 1,$$

ed osserviamo che, poiché $k \equiv p+1 \pmod{p^2}$, esiste almeno un divisore primo q di k tale che $q \not\equiv 1 \pmod{p^2}$. Allora $o_q(p) = p$, poichè $q \mid p^p - 1$ e $q \nmid p-1$, e p non divide $\frac{q-1}{p}$; quindi

$$p^{\frac{q-1}{p}} \not\equiv 1 \pmod{q}$$

e q è un primo come cercato. ■

Problema 135 (Romania 1996)**.** *Trovare tutte le coppie di numeri primi (p,q) tali che*

$$a^{3pq} \equiv a \pmod{3pq} \tag{4.2}$$

per ogni intero a.

SOLUZIONE. Sia p,q una coppia di primi con la proprietà voluta. Da

$$2^{3pq} \equiv 2 \pmod{3pq}$$

segue, in particolare, $3 \mid 2^{3pq}-2$, e questo forza p,q dispari. Sia a un intero primitivo modulo p (cioè tale che $o_p(a)=p-1$, vedi commento dopo la Proposizione **??**); dalla (4.2) segue $a^{3pq-1}\equiv 1 \pmod p$ e quindi, per la Proposizione 4.2, $p-1 \mid 3pq-1$ e pertanto

$$p-1 \mid 3pq-1-3q(p-1)=3q-1.$$

Simmetricamente, si ricava $q-1 \mid 3p-1$.
Se $p=q$, allora $p=q=3$, e questo non è il caso, dato che $\phi(27)=2\cdot 9$ e quindi

$$4^{27}=2^{2\cdot 27}=(2^3)^{\phi(27)}\equiv 1 \pmod{27}.$$

Sia $p\neq q$, e possiamo supporre $q>p$; allora $q\geq p+2$ e dunque

$$1<\frac{3p-1}{q-1}<3.$$

Poiché è un intero, $\frac{3p-1}{q-1}=2$; quindi $2q=3p+1$. Infine, $p-1$ divide $3q-1=(9p+1)/2$, e dunque

$$p-1 \mid 9p+1-9(p-1)=10.$$

Quindi $(p,q)=(3,5)$ oppure $(p,q)=(10,17)$. Il primo caso non soddisfa la richiesta, infatti $3pq=9\cdot 5=45$, e

$$4^{45}=(2^{15})^6=(2^{15})^{\phi(9)}\equiv 1 \pmod 9.$$

La coppia $(p,q)=(11,17)$ va bene. In tal caso $3pq=561$; ora, $561-1=560$ è un multiplo di $\phi(t)$ per $t\in\{3,11,17\}$, quindi, per ogni intero a,

$$a^{561}=a^{560}a\equiv a \pmod t$$

per ciascun primo $t=3,11,17$, e dunque $a^{561}\equiv a \pmod{3\cdot 11\cdot 17}$. ∎

Numeri di Carmichel. Un intero positivo $n\geq 2$ si dice *numero di Carmichel* se non è primo e soddisfa

$$a^n\equiv a \pmod n$$

per ogni numero intero a. Quindi, per definizione, un numero di Carmichel è diviso da almeno due primi, e si vede facilmente che deve essere dispari. Nel Problema 135 abbiamo provato che $561=3\cdot 11\cdot 17$ è un numero di Carmichel (ed è l'unico numero di Carmichel con tre divisori primi, multiplo di 3). Infatti, 561 è il più piccolo numero di Carmichel (il successivo è 1105).
Si dimostra che $n=p_1p_2\cdots p_k$ (con $k\geq 2$ e $p_1,\ldots,p_k$ primi non necessariamente distinti) è un numero di Carmichel se e solo se i primi $p_1,\ldots,p_k$ sono tutti distinti e tali che $p_i-1 \mid n-1$ per ogni $i=1,\ldots,k$. Soltanto nel 1994, Alford, Granville e Pomerance hanno dimostrato che esistono infiniti numeri di Carmichel.

* * *

• Problemi da risolvere.

Problema 136 (Baltic Way, 2002)**.** *Siano p un numero primo e n un intero positivo. Sia q un divisore positivo di $(n+1)^p-n^p$. Si provi che p divide $q-1$.*

Problema 137 (Canada 2002)**.** *Determinare le ultime tre cifre decimali del numero*

$$n = 2003^{2002^{2001}}.$$

Problema 138 (USA 2003)**.** *Trovare tutte le terne di numeri primi (p, q, r) tali che*

$$p \mid q^r + 1, \quad q \mid r^p + 1, \quad r \mid p^q + 1.$$

Problema 139 (Bulgaria 1996)**.** *Trovare tutte le coppie di primi (non necessariamente distinti) p, q tali che*

$$pq \mid (5^p - 2^p)(5^q - 2^q).$$

Problema 140 (Taiwan, 1997)**.** *Sia X l'insieme di tutti i numeri interi della forma*

$$a_{2k}10^{2k} + a_{2k-2}10^{2k-2} + \ldots + a_2 10^2 + a_0$$

con $k \in \mathbb{N}$ e $a_{2i} \in \{1, 2, \ldots, 9\}$ per ogni $0 \leq i \leq k$. Si provi che ogni numero intero del tipo $2^m 3^n$, con $n, m \in \mathbb{N}$ divide qualche elemento di X.

Problema 141 (Cina 2009)**.** *Trovare tutte le coppie di numeri primi p, q tali che*

$$pq \mid 5^p + 5^q.$$

Problema 142 (Korea 2003)**.** *Fissato un primo p, per ogni intero positivo n sia*

$$f_p(n) = n^{p-1} + n^{p-2} + \ldots + n + 1.$$

(a) Sia $p \mid n$; si provi che esiste un divisore primo di $f_p(n)$ che è coprimo con $n(n-1)$.

(b) Si provi che esistono infiniti interi positivi k tali che $pk + 1$ è un numero primo.

4.2. Residui quadratici

Siano p un primo dispari, $a, b, c \in \mathbb{Z}$ con $p \nmid a$, e studiamo la congruenza quadratica

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{4.3}$$

Si può argomentare come si fa con le equazioni di grado 2 sui reali. Si considera l'identità

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac);$$

poiché p è dispari e coprimo con a, $p \nmid 4a$; inoltre la congruenza è risolubile per ogni b. Si conclude che la congruenza (4.3) è risolubile in $\mathbb{Z}$ se e soltanto è risolubile la congruenza

$$y^2 \equiv \Delta \pmod{p},$$

dove $\Delta = b^2 - 4ac$.

Esercizio 4.2. Calcolare le eventuali soluzioni della congruenza

$$x^2 - 3x + 11 \equiv 0 \pmod{13}.$$

Questa sezione e la seguente sono dedicate ad alcuni risultati classici che riguardano congruenze di questo tipo.

DEFINIZIONE. Siano a, b interi, con b positivo e $b \neq 1$. Allora a si dice un *Residuo Quadratico (RQ) modulo* b se esiste un $c \in \mathbb{Z}$ tale che

$$c^2 \equiv a \pmod{b}$$

(ovvero se $a + b\mathbb{Z}$ è un quadrato nell'anello $\mathbb{Z}/b\mathbb{Z}$).

Il caso in cui $b = p$ è un numero primo è particolarmente interessante. Se $p = 2$, per ogni intero a si ha $a^2 \equiv a \pmod{2}$, dunque ogni intero è un RQ modulo 2. Se invece p è un primo dispari le cose sono più complicate: cominciamo con una semplice ma fondamentale osservazione.

Sia p un primo dispari e $A = \{0, 1, \ldots, p-1\}$ un sistema di rappresentanti delle classi modulo p; per ogni $a \in A$ denotiamo con a_2 l'unico elemento di A tale che $a_2 \equiv a^2 \pmod{p}$; allora $a_2 = 0$ se e solo se $a = 0$, mentre, per $a \neq 0$ si ha (Proposizione 4.4) che le soluzioni in A di $x^2 \equiv a_2 \pmod{p}$ sono a e $p - a$. Da ciò si deduce che il numero di RQ in A, cioè la cardinalità dell'immagine della funzione $A \to A$ definita da $a \mapsto a_2$ è

$$1 + \frac{p-1}{2} = \frac{p+1}{2}.$$

A questo punto è conveniente introdurre la seguente notazione.

Simbolo di Legendre. Sia p un numero primo dispari, e $a \in \mathbb{Z}$. Si pone

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \mid a; \\ 1 & \text{se } p \nmid a \text{ ed } a \text{ è un RQ modulo } p; \\ -1 & \text{se } a \text{ non è un RQ modulo } p. \end{cases}$$

Proposizione 4.7 (Criterio di Eulero)**.** *Siano p un primo dispari e $a \in \mathbb{Z}$, con $mcd(a, p) = 1$. Allora.*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Dimostrazione. Sia p un primo dispari, e sia $a \in \mathbb{Z}$, con $mcd(a, p) = 1$. Dal Teorema di Fermat segue che $a^{\frac{p-1}{2}}$ è una soluzione dell'equazione

$$x^2 \equiv 1 \pmod{p},$$

e poiché tale equazione ha esattamente due soluzioni modulo p, che sono 1 e -1 si ha

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}. \tag{4.4}$$

Se $\left(\frac{a}{p}\right) = 1$, cioè a è un RQ modulo p, esiste $c \in \mathbb{Z}$ tale che $c^2 \equiv a \pmod{p}$. Chiaramente, c è coprimo con p, quindi

$$a^{\frac{p-1}{2}} \equiv c^{p-1} \equiv 1 \pmod{p}.$$

Ora, per quanto osservato in precedenza, il numero di quadrati non nulli modulo p è esattamente $\frac{p-1}{2}$, che è anche (Proposizione 4.4) il numero di soluzioni (a meno di congruenza modulo p) della congruenza

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Dunque, se $a \in \mathbb{Z}$ (con $mcd(a,p) = 1$) non è un RQ modulo p, a non è una soluzione della congruenza di sopra, quindi, per (4.4)

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

provando così la Proposizione. □

Seguono facilmente le seguenti proprietà del simbolo di Legendre.

Lemma 4.8. *Sia p un primo dispari, e siano $a, b \in \mathbb{Z}$. Allora*

(1) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *se* $a \equiv b \pmod{p}$;

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(3) $\left(\frac{a^2}{p}\right) = 1$;

(4) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Dimostrazione. I punti (1) e (3) discendono immediatamente dalle definizioni.
Per il punto (3), la cosa è ovvia se p divide ab. Altrimenti, per il criterio di Eulero,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

provando così l'affermazione (dato che p è dispari).
Anche il punto (4) segue dal criterio di Eulero; infatti

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

e quindi l'asserto. □

Osserviamo che se p è un primo dispari, allora $p \equiv 1, 3 \pmod{4}$. Il punto (4) del Lemma precedente può quindi essere riformulato affermando che, per un primo dispari p,

$$\left(\frac{-1}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1 \pmod{4},$$

cosa che avevamo già provato nel Capitolo 1 (Lemma 1.20).

* * *

Sia n un intero positivo; allora l'insieme dei numeri interi x con $-\frac{n}{2} < x \leq \frac{n}{2}$ è un sistema di rappresentanti delle classi di congruenza modulo n. Dato un intero a chiamiamo *residuo assoluto* di a modulo n quell'unico intero $-\frac{n}{2} < b \leq \frac{n}{2}$ tale che $a \equiv b \pmod{n}$.

Lemma 4.9 (Lemma di Gauss)**.** *Siano p un primo dispari e a un intero positivo con $p \nmid a$. Sia t il numero di elementi nell'insieme*

$$Q = \{a,\, 2a, \ldots,\, ((p-1)/2)a\}$$

il cui residuo assoluto modulo p è negativo. Allora

$$\left(\frac{a}{p}\right) = (-1)^t.$$

Dimostrazione. Osserviamo che, poiché $(a, p) = 1$, gli elementi di Q sono a due a due non congrui modulo p.
Sia $k = (p-1)/2 - t$. Siano $r_1, r_2, \ldots, r_k$ i residui assoluti positivi degli elementi di Q, e siano $-s_1, -s_2, \ldots, -s_t$ quelli negativi. Supponiamo che esistano $1 \le i \le k$ e $1 \le j \le t$ tali che $r_i \equiv s_j \pmod p$. Ora, esistono $1 \le n_i, n_j \le (p-1)/2$, tali che $an_i \equiv r_i \pmod p$ e $an_j \equiv -s_j \pmod p$. Ma allora

$$a(n_i - n_j) \equiv 0 \pmod p,$$

quindi p divide $n_i - n_j$, il che è possibile solo se $n_i = n_j$, come invece non è. Dunque gli elementi dell'insieme $R = \{r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_t\}$ sono a due a due non congrui modulo p, e di conseguenza $R = \{1, 2, \ldots, (p-i)/2\}$. Da ciò segue

$$a^{\frac{p-1}{2}}((p-1)/2)! = a \cdot 2a \cdots ((p-1)/2)a \equiv (-1)^t((p-1)/2)! \pmod p,$$

e quindi, poiché p non divide $((p-1)/2)!$,

$$a^{\frac{p-1}{2}} \equiv (-1)^t \pmod p,$$

e la dimostrazione si completa applicando il criterio di Eulero. □

Esempio 4. Il Lemma di Gauss può essere impiegato per calcolare il valore del simbolo di Legendre. Ad esempio, determiniamo $\left(\frac{5}{13}\right)$ (nella tabella di sotto i residui assoluti sono ovviamente intesi modulo 13).

	res. ass.
$1 \cdot 5 = 5$	5
$2 \cdot 5 = 10$	-3
$3 \cdot 5 = 15$	2
$4 \cdot 5 = 20$	-6
$5 \cdot 5 = 25$	-1
$6 \cdot 5 = 30$	4

quindi il numero t di residui assoluti negativi per i multipli di 5 da considerare è 3 e pertanto, per il Lemma di Gauss,

$$\left(\frac{3}{13}\right) = (-1)^3 = -1.$$

Esercizio 4.3. Calcolare, usando il Lemma di Gauss, $\left(\frac{7}{17}\right)$ e $\left(\frac{3}{23}\right)$.

Naturalmente, il Lemma di Gauss ha applicazioni ben più generali; come la seguente, che stabilisce per quali primi dispari, il numero 2 è un residuo quadratico.

Proposizione 4.10. *Sia p un primo dispari. Allora*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Dimostrazione. Applichiamo il Lemma di Gauss (e le stesse notazioni) con $a = 2$, e quindi $Q = \{2, 4, \ldots, p-1\}$. In questo caso, gli elementi di Q il cui residuo assoluto modulo p è negativo sono quelli maggiori di $p/2$, ovvero (in ordine decrescente)

$$p-1,\ p-3,\ \ldots,\ p-(2t-1),$$

dove quindi t è il massimo tale che $p-(2t-1) > p/2$, e cioè

$$t = \left\lfloor \frac{p+2}{4} \right\rfloor.$$

Se $p \equiv \pm 1 \pmod 8$, allora $\frac{p^2-1}{8}$ è pari; inoltre, per qualche k, $p = 8k \pm 1$, quindi

$$t = \left\lfloor \frac{p+2}{4} \right\rfloor = 2k$$

è pari, e dunque

$$\left(\frac{2}{p}\right) = (-1)^t = 1 = (-1)^{\frac{p^2-1}{8}}.$$

Se invece $p \equiv 3, 5 \pmod 8$, allora $\frac{p^2-1}{8}$ è dispari, $p = 8k+3$ oppure $p = 8k+5$ (per qualche intero k), quindi

$$t = \left\lfloor \frac{p+2}{4} \right\rfloor = 2k+1$$

è dispari, e dunque

$$\left(\frac{2}{p}\right) = (-1)^t = -1 = (-1)^{\frac{p^2-1}{8}},$$

concludendo la dimostrazione. □

Nei prossimi esempi vediamo due applicazioni ai numeri di Mersenne e di Fermat.

Esempio 5. *Sia p un numero primo e $p \equiv 3 \pmod 4$. Provare che $2p+1$ è primo se e solo se $2^p \equiv 1 \pmod{2p+1}$; dedurre che se $2p+1$ è numero primo, allora il numero di Mersenne $M_p = 2^p - 1$ non è primo.*

Osserviamo che $2p+1 \equiv 7 \pmod 8$. Se $2p+1$ è un primo, allora, per la Proposizione 4.10,

$$\left(\frac{2}{2p+1}\right) = (-1)^{\frac{(2p+1)^2-1}{8}} = (-1)^{\frac{49-1}{8}} = 1,$$

e quindi, dal criterio di Eulero,

$$2^p = 2^{\frac{(2p+1)-1}{2}} \equiv 1 \pmod{(2p+1)}.$$

Viceversa, sia $2^p \equiv 1 (\mathrm{mod}\ (2p+1))$, e sia $2p+1 = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ è la fattorizzazione di $2p+1$ in potenze di primi distinti. Allora, poiché $(2, 2p+1) = 1$, si ha che p divide l'ordine di 2 modulo $2p+1$, e quindi p divide

$$\phi(2p+1) = \prod_{i=1}^{s} p_i^{a_1 - 1}(p_i - 1),$$

Dunque, $p \mid p_i$ per qualche $i = 1, 2, \ldots, s$. Sia, per assurdo, $2p+1 \neq p_i$; allora $2p+1 = p_i m$ con $m \geq 3$, e quindi (essendo $p \neq 2$) $2p+1 \geq (p_i - 1)3 > 3p$, una contraddizione. Pertanto, $2p+1 = p_i$ è un numero primo.

L'ultimo punto segue subito, tenendo conto che, poiché $p > 3$, $2p+1 \neq 2^p - 1$.

Esempio 6. *Siano $n \geq 2$ e p un divisore primo del numero di Fermat $F_n = 2^{2^n} + 1$; allora*

$$p \equiv 1 \pmod{2^{n+2}}.$$

Sia p un divisore primo di F_n. Allora (esempio 6 del Capitolo 1) esiste $k \geq 1$ tale che

$$p = 2^{n+1}k + 1.$$

In particolare, poiché $n \geq 2$, 2^4 divide $p^2 - 1$; quindi, per la Proposizione 4.10, 2 è un RQ modulo p, ovvero esiste un intero a tale che $a^2 \equiv 2 \pmod{p}$. Dunque

$$a^{2^{n+1}} = (a^2)^{2^n} \equiv 2^{2^n} \equiv -1 \pmod{p}.$$

Inoltre $a^{2^{n+2}} \equiv 1 \pmod{p}$; pertanto $o_p(a) \mid 2^{n+2}$. Ma $o_p(a) \neq 2^{n+1}$, e dunque $o_p(a) = 2^{n+2}$. Per la Proposizione 4.2, 2^{n+2} divide $\phi(p) = p - 1$, e quindi $p \equiv 1 \pmod{2^{n+2}}$.

Problemi

Problema 143 (Vietnam 2004)**.** *Sia n un intero positivo. Provare che $2^n + 1$ non ha divisori primi della forma $8k + 7$ (con $k \in \mathbb{N}$).*

Problema 144 (Czech-Polish-Slovak 2011)**.** *Sia a un numero intero. Provare che esistono infiniti numeri primi p tali che*

$$p \mid n^2 + 3 \qquad e \qquad p \mid m^3 - a$$

per qualche coppia di interi n e m.

4.3. Reciprocità Quadratica

La *Legge di Reciprocità Quadratica*, dimostrata da K. F. Gauss, è uno dei più celebri e importanti teoremi della teoria dei numeri classica. In qualche modo, non proprio intuitivo: se p e q sono primi dispari distinti, la risolubilità della congruenza $x^2 \equiv p \pmod{q}$ (ovvero, se p sia o meno un residuo quadratico modulo q), sembrebbe, a prima vista, non avere molto a che fare con la la risolubilità di quella che si ottiene scambiando p con q, ovvero $x^2 \equiv q \pmod{p}$. La legge di Reciprocità Quadratica dice che non è così.

Teorema 4.11 (Legge di reciprocità quadratica di Gauss)**.** *Siano p, q due primi dispari distinti. Allora*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Esistono molte dimostrazioni diverse di questo Teorema (pare ne siano state proposte almeno 150), e lo stesso Gauss ne fornì sette distinte. Quella che vedremo è di carattere elementare ed ed è sostanzialmente la terza delle dimostrazioni proposte da Gauss.

Dimostrazione. Siano p e q numeri primi dispari distinti, e poniamo

$$P = \{1, 2, \ldots, (p-1)/2\}, \qquad Q = \{1, 2, \ldots, (q-1)/2\}.$$

Sia s il numero di elementi dell'insieme $Pq = \{xq \mid x \in P\}$ il cui residuo assoluto modulo p è negativo, e sia t il numero di elementi dell'insieme $Qp = \{xp \mid x \in Q\}$ il cui residuo assoluto modulo q è negativo. Per il Lemma di Gauss (Lemma 4.9),

$$\left(\frac{q}{p}\right) = (-1)^s \left(\frac{q}{p}\right) = (-1)^{s+t}.$$

La Legge di reciprocità quadratica equivale quindi ad affermare che

$$s + t \text{ è dispari} \quad \Leftrightarrow \quad p \equiv q \equiv 3 \pmod{4}.$$

Consideriamo l'insieme N di tutte le coppie $(u, v) \in P \times Q$ tali che

$$-q/2 < vp - uq < 0. \tag{4.5}$$

Queste coppie, (in un usuale piano cartesiano, sono i punti a coordinata intera che giacciono all'interno del trapezio di vertici

$$A_0 = (0, 0) \quad A_1 = (p/2,\, q/2) \quad B_1 = (0,\, 1/2) \quad B_2 = (p/2,\, q(p-1)/2p).$$

La condizione (4.5) implica che se $(u, v) \in N$, allora il residuo assoluto di vp modulo q è negativo. Pertanto $|N| \leq t$.

Viceversa, se $j \in Q$ è tale che il residuo assoluto di jp modulo q è negativo, allora esiste un intero k tale che $-q/2 < jp - kq < 0$. Quindi, $jp < kq < jp + q/2$; siccome $1 \leq j \leq (q-1)/2$ si ha

$$p < kq < \frac{(q-1)p}{2} + \frac{q}{2}$$

da cui segue,

$$\frac{p}{q} < k < \frac{q-1}{q} \cdot \frac{p}{2} + \frac{1}{2} < \frac{p+1}{2},$$

ed essendo k intero e p dispari

$$1 \leq k \leq (p-1)/2,$$

ovvero $k \in P$. In conclusione per ogni $j \in Q$ tale che il residuo assoluto di jp modulo q è negativo esiste uno ed un solo punto $(j,k) \in N$.
Pertanto $|N| \geq t$, e dunque $|N| = t$.

Allo stesso modo si prova che il numero di coppie $(u,v) \in P \times Q$ tali che

$$-p/2 < uq - vp < 0 \tag{4.6}$$

è uguale a s. In questo caso si tratta dei punti a coordinate intere che giacciono all'interno del trapezio di vertici

$$A_0 = (0,0) \quad A_1 = (p/2,\, q/2) \quad C_1 = (0,0) \quad C_2 = (p/2,\, p(q-1)/2q).$$

Quindi, $s+t$ è uguale alla cardinalità dell'insieme U di tutti i punti a coordinata intera che giacciono all'interno dell'esagono di vertici A_0, B_1, B_2, A_1, C_2, C_1.

Ora, si verifica facilmente che $X = (x_0, y_0) \in U$ se e solo se $\sigma(X) = (x_1, y_1) \in U$, dove

$$\begin{cases} x_1 = \frac{p+1}{2} - x_0 \\ \\ y_1 = \frac{q+1}{2} - y_0. \end{cases}$$

Dunque, la funzione $\sigma : U \to U$ è una biezione, ed è tale che $\sigma(\sigma(X)) = X$ per ogni $X \in U$. Supponiamo che $X = (x_0, y_0)$ sia un punto fisso per σ (ovvero $\sigma(X) = X$). Allora

$$\begin{cases} 2x_0 = \frac{p+1}{2} \\ \\ 2y_0 = \frac{q+1}{2} \end{cases}$$

Ne segue, in particolare, che esiste al più un punto fisso per σ. Siccome le orbite di σ contengono uno (se si tratta di un punto fisso) o due elementi, il numero di elementi di U che non sono fissati da σ è pari. Quindi, un punto fisso esiste se e solo se $|U| = s+t$ è dispari. D'altra parte, dalle due equazioni che lo caratterizzano, si deduce che, essendo x_0 e y_0 numeri interi, un punto fisso per σ esiste se e solo se $p \equiv q \equiv 3 \pmod 4$.
Ciò conclude la dimostrazione. □

Esempio 7. *Provare che la congruenza* $x^2 \equiv 257 \pmod{269}$ *non ha soluzioni.*

Infatti, 257 e 269 sono numeri primi e $269 = 257 + 12$. Per le proprietà del simbolo di Legendre e la Legge di reciprocità quadratica,

$$\left(\frac{257}{269}\right) = \left(\frac{269}{257}\right) = \left(\frac{12}{257}\right) = \left(\frac{3}{257}\right)\left(\frac{4}{257}\right) = \left(\frac{3}{257}\right) = \left(\frac{257}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Quindi, 257 non è un RQ modulo 269.

ESEMPIO 8. *Sia p un primo dispari. Provare che 3 è un residuo quadratico modulo p se e solo se $p \equiv \pm 1 \pmod{12}$.*

Infatti, se $p \neq 3$ è un primo dispari, allora, per il Teorema di reciprocità quadratica,

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right).$$

Pertanto 3 è un RQ modulo p se e solo se $\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}$.
Se $p \equiv 1 \pmod 3$, allora $\left(\frac{p}{3}\right) = 1$, e quindi la condizione è soddisfatta se e solo se $4|p-1$, ovvero se e solo se $p \equiv 1 \pmod{12}$.
Altrimenti, $p \equiv 2 \pmod 3$, e $\left(\frac{p}{3}\right) = -1$, e la condizione è soddisfatta se e solo se 4 non divide $p-1$ (cioè, essendo p dispari, $p \equiv -1 \pmod 4$), ovvero se e solo se $p \equiv -1 \pmod{12}$.

Problemi

Problema 145 (Taiwan 1997)**.** *Sia n un intero positivo. Si provi che il numero di Fermat $F_n = 2^{2^n} + 1$ è un numero primo se e solo se F_n divide $3^{(F_n-1)/2} + 1$.*

Problema 146 (Amer. Math. Monthly)**.** *Trovare tutti gli interi positivi n tali che $2^n - 1 \mid 3^n - 1$.*

Problema 147 (IMO 1996)**.** *Siano a e b interi positivi tali che i numeri $15a + 16b$ e $16a - 15b$ sono entrambi quadrati. Qual; è il minimo valore possibile che può assumere il più piccolo di questi quadrati ?*

4.4. Soluzioni dei problemi

PROBLEMA 136. Dati p un primo ed n un intero positivo, vogliamo provare che per ogni divisore positivo q di $(n+1)^p - n^p$ si ha

$$q \equiv 1 \pmod p. \qquad (*)$$

Osserviamo per prima cosa che per il carattere moltiplicativo delle congruenze, è sufficiente provare $(*)$ nel caso in cui q è un numero primo. Sia quindi q un primo dove, per ipotesi, $(n+1)^p \equiv n^p \pmod q$. Poiché certamente $n + 1 \not\equiv n \pmod q$, il Corollario 4.6 implica $mcd(p, q-1) > 1$ e dunque, siccome è un primo, p divide $q - 1$.

* * *

PROBLEMA 137. Per determinare le ultime tre cifre decimali di $n = 2003^{2002^{2001}}$, osserviamo intanto che

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod{1000}. \qquad (4.7)$$

Poiché, chiaramente, $\phi(8) = 4 \mid 2002^{2001}$, si ha

$$3^{2002^{2001}} \equiv 1 \pmod 8.$$

Studiamo quindi la congruenza (4.7) modulo $5^3 = 125$. Si ha $\phi(125) = 4 \cdot 5^2 = 100$ e

$$2002^{2001} \equiv 2^{2001} \pmod{100}.$$

Chiaramente, $2^{2001} \equiv 0 \pmod 4$; mentre, poiché $\phi(25) = 20$, $2^{2001} \equiv 2 \pmod{25}$. applicando il metodo per il teorema Cinese dei Resti, si ricava

$$2^{2001} \equiv 52 \pmod{100}.$$

Allora, sempre per il teorema di Eulero,

$$3^{2002^{2001}} \equiv 3^{52} \pmod{125}.$$

Ora, $\nu_5(3^2 + 1) = 1$ e dunque per il Corollario 2.7,

$$\nu_5(3^{50} + 1) = \nu_5(3^2 + 1) + \nu_5(25) = 3;$$

in particolare, $3^{50} \equiv -1 \pmod{125}$ e dunque

$$3^{52} \equiv -9 \equiv 116 \pmod{125}.$$

Abbiamo in conclusione trovato

$$\begin{cases} 3^{2002^{2001}} \equiv 1 \pmod 8 \\ 3^{2002^{2001}} \equiv 116 \pmod{125} \end{cases}$$

Con il teorema Cinese dei Resti si conclude

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \equiv 241 \pmod{1000}.$$

Le ultime tre cifre decimali di $2003^{2002^{2001}}$ sono quindi 241.

* * *

Problema 138. Chiaramente p, q, r sono tutti distinti. Osserviamo che, ad esempio, da $p \mid q^r + 1$ segue $p \mid q^{2r} - 1$, quindi $o_p(q) \mid 2r$; inoltre, $q^r \equiv -1 \pmod p$, dunque $o_p(q) \in \{2, 2r\}$. Similmente $o_q(r) \in \{2, 2p\}$ e $o_r(p) \in \{2, 2q\}$.
Sia $p = 2$; se $o_r(2) = o_r(p) = 2$, si ha $r = 3$ e di conseguenza $q = 5$, e la terna $(2, 5, 3)$ soddisfa in effetti le condizioni. Altrimenti, $o_r(2) = 2q$, quindi $2q \mid r - 1$, e segue l'assurdo

$$2q \mid r^p + 1 - r(r - 1) = r^2 + 1 - r(r - 1) = 2.$$

Allo stesso modo si procede nei casi $q = 2$ e $r = 2$.
Possiamo ora assumere che p, q, r sono tutti dispari. Sia $o_p(q) = 2$, allora $p \mid q + 1$, quindi

$$o_q(r) \mid 2(q + 1) - 2(q - 1) = 4,$$

e dunque $o_q(r) = 2$; da questo segue, allo stesso modo, $o_r(p) = 2$. Ma allora

$$p \mid q + 1, \quad q \mid r + 1, \quad r \mid p + 1$$

che è assurdo. Dunque $o_p(q) = 2r$, $o_q(r) = 2p$ e $o_r(p) = 2q$, che però implica l'altro assurdo

$$2r \mid p-1, \quad 2p \mid q-1, \quad 2q \mid r-1.$$

In conclusione, le soluzioni sono $(2,5,3), (5,3,2), (3,2,5)$.

* * *

PROBLEMA 139. Supponiamo $p \mid 5^p - 2^p$; allora per il teorema di Fermat,

$$0 \equiv 5^p - 2^p \equiv 5 - 2 = 3 \pmod{p}.$$

e dunque $p = 3$. La coppia $(p,q) = (3,3)$ è una soluzione; se $q \neq 3$ allora

$$q \mid 5^p - 2^p = 5^3 - 2^3 = 117 = 9 \cdot 13,$$

e quindi $q = 13$. Sono perciò soluzioni $(p,q) = (3,13)$ e, simmetricamente $(p,q) = (13,3)$. Rimane il caso in cui $p \nmid 5^p - 2^p$ e $q \nmid 5^q - 2^q$; dunque $p \neq 3 \neq q$, $p \nmid 5^q - 2^q$ e $q \nmid 5^p - 2^p$. Poiché p, q sono primi e, certamente, $p, q \neq 2, 5$, dal Corollario 4.6 segue la contraddizione $p \mid q-1$ e $q \mid p-1$. In conclusione, le soluzioni sono $(p,q) = (3,3), (3,13), (13,3)$.

* * *

PROBLEMA 140. Sia X l'insieme di tutti i numeri interi della forma

$$a_{2k}10^{2k} + a_{2k-2}10^{2k-2} + \ldots + a_2 10^2 + a_0$$

con $k \in \mathbb{N}$ e $a_{2i} \in \{1, 2, \ldots, 9\}$ per ogni $0 \leq i \leq k$.
Cominciamo col provare, per induzione su j, che 2^{2j} divide un elemento $x_j \in X$ con al più j cifre (con le notazioni di sopra, il numero di cifre di un elemento di X è $k+1$, quindi $x_j < 10^{2j}$). Questo è ovvio per $j = 1$; supponiamo vero per un certo $j \geq 1$, quindi $2^{2j} \mid x_j \in X$ (scrivo $x_j = 2^{2j}x'$) con $x_j < 10^{2j}$. Poiché $2^{2j} \mid 10^{2j}$, esiste una cifra $a \in \{1,2,3,4\}$ tale che

$$a10^{2j} + x_j = 2^{2j}(a5^{2j} + x') \equiv 0 \pmod{2^{2j+2}}.$$

Ponendo $x_{j+1} = a10^{2j} + x_j$, si ha $2^{2(j+1)} \mid x_{j+1} \in X$, e x_{j+1} ha al più $j+1$ cifre.
Nel caso generale, sia $a = 2^m 3^n$. Chiaramente, possiamo supporre $m = 2j$ per qualche $j \geq 1$. Sia k il numero di cifre di x_j come individuato sopra; quindi

$$x_j = a_{2(k-1)}10^{2(k-1)} + a_{2k-2}10^{2k-2} + \ldots + a_2 10^2 + a_0.$$

Osserviamo che allora per ogni $s \geq 2$,

$$x_j \frac{10^{2ks} - 1}{10^{2k} - 1} = x_j 10^{2k(s-1)} + x_j 10^{2k(s-2)} + \ldots + x_j 10^{2k} + x_j \in X. \tag{4.8}$$

Infine, sia $v = \nu_3(10^{2k} - 1)$: si ha allora, per il Teorema di Eulero, che

$$3^n \text{ divide } \frac{10^{2k\phi(3^{n+v})} - 1}{10^{2k} - 1}.$$

Quindi $a = 2^m 3^n$ divide l'elemento di X che si ottiene in (4.8) ponendo $s = \phi(3^{n+v})$.

* * *

PROBLEMA 141. Siano p, q numeri primi tali che $pq \mid 5^p + 5^q$.
Se $p = 2$ allora, poiché (Teorema di Fermat) $q \mid 5^q - 5$, si ha che q divide $5^2 + 5 = 30$. Ora, $q \neq 2$ dato che $5^2 + 5^2 = 50$ non è multiplo di 4; rimane quindi $q = 3, 5$, casi che si verifica essere entrambi accettabili. Si ragiona in modo simmetrico se $q = 2$.
Similmente, se $p = 5$, allora q divide $5^5 + 5 = 5(5^4 + 1)$, quindi $q = 5$, che va bene, oppure $q \mid 5^4 + 1 = 626$ e dunque $q = 2, 313$. Lo stesso si fa per $q = 5$.

Supponiamo quindi che né p né q siano uguali a 2 oppure a 5. In tal caso si ha anche $p \neq q$. Ora, p divide $5^p + 5^q \equiv 5(5^{q-1} + 1) \pmod p$, e dunque $p \mid 5^{q-1} + 1$ (similmente, $q \mid 5^{p-1} + 1$). Allora

$$p \mid (5^{q-1} + 1)(5^{q-1} - 1) = 5^{2(q-1)} - 1,$$

quindi $o_p(5)$ divide $2(q-1)$. Inoltre, poiché $5^{q-1} \equiv -1 \pmod p$, $o_p(5)$ non divide $q - 1$. Dato che $2(q-1)$ e $q-1$ differiscono per un fattore uguale a 2, ne segue che

$$\nu_2(o_p(5)) = \nu_2(q-1) + 1.$$

D'altra parte $o_p(5) \mid p - 1$, pertanto

$$\nu_2(q-1) < \nu_2(o_p(5)) \leq \nu_2(p-1).$$

Scambiando i ruoli di p e q si ottiene però $\nu_2(p-1) < \nu_2(o_q(5)) \leq \nu_2(q-1)$, che è un assurdo.
In conclusione, soluzioni sono le coppie $(p, q) = (2, 3), (3, 2), (2, 5), (5, 2), (5, 5), (5, 313), (313, 5)$.

* * *

PROBLEMA 142. (a) Siano p un primo e n intero con $p \mid n$. Sia q un divisore primo di

$$f_p(n) = n^{p-1} + n^{p-2} + \ldots + n + 1.$$

Allora chiaramente $mcd(q, n) = 1$. Supponiamo $q \mid n - 1$, cioè $n \equiv 1 \pmod q$, allora

$$0 \equiv n^{p-1} + n^{p-2} + \ldots + n + 1 \equiv p \pmod q,$$

dunque $q = p$ divide n, che è assurdo. Abbiamo quindi provato che se $p \mid n$ allora ogni divisore primo di $f_p(n)$ è coprimo con $n(n-1)$.
(b) Proseguiamo l'analisi del punto (a) e proviamo che se $p \mid n$ allora ogni divisore primo q di $f_p(n)$ è del tipo $q = pk + 1$ (cioè $q \equiv 1 \pmod p$). Infatti, q divide $(n-1)f_p(n) = n^p - 1$, quindi $o_q(n) \mid p$. Ma al punto (a) abbiamo visto che $q \nmid n - 1$, quindi $o_q(n) = p$, il che implica (Proposizione 4.2) $p \mid \phi(q) = q - 1$.
Supponiamo ora di aver trovato $q_1, q_2, \ldots, q_n$ primi distinti tali che $p \mid q_i - 1$, per ogni indice $i = 1, 2, \ldots, n$. Sia q_{n+1} un divisore primo di $f_p(pq_1q_2 \cdots q_n)$. Per il punto (a), q_{n+1} non divide $q_1 q_2 \cdots q_n$, quindi $q_{n+1} \neq q_i$ per ogni $i = 1, \ldots, n$. Inoltre per quanto visto sopra $p \mid q_{n+1} - 1$. Questo prova che il numero di primi q con $p \mid q - 1$ è infinito.

* * *

PROBLEMA 143. Sia n un intero positivo e sia p un divisore primo di $2^n + 1$.

Se n è pari, allora da $p \mid 2^n + 1$ segue che -1 è un RQ modulo p; quindi, per il punto (4) del Lemma 4.8, $p \equiv 1 \pmod 4$, e dunque $p \equiv 1, 5 \pmod 8$.

Se n è dispari, poiché $p \mid 2^{n+1} + 2$ e quindi -2 è un RQ modulo p. Per il Lemma 4.8 e la Proposizione 4.10 si ha allora

$$1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}};$$

quindi $p \equiv 1, 3 \pmod 8$.

In ogni caso $p \not\equiv 7 \pmod 8$.

* * *

PROBLEMA 144. Sia a un numero intero. Se p è un primo dispari, la condizione che esista n intero tale che $p \mid n^2 + 3$ equivale a richiedere che -3 sia un RQ modulo p, ovvero $\left(\frac{-3}{p}\right) = 1$.

Sia t un intero positivo dispari; poniamo $m = -3^t a$, per cui $m^3 - a = -a(3^{3t}a^2 + 1)$. Sia p un divisore primo dispari di $3^{3t}a^2 + 1$. Allora $p \mid m^3 - a$ e, tenendo conto che t è dispari,

$$\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{3^{3t}a^2}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{3}{p}\right) = 1,$$

per cui esiste un intero n tale che $p \mid n^2 + 3$.

Si tratta a questo punto di provare che, al variare di t nell'insieme dei numeri positivi dispari, è possibile scegliere, come sopra, infiniti primi distinti p. Ora, se t, k sono interi dispari distinti, con $t < k$,

$$3^{3(k-t)}(3^{3t}a^2 + 1) - (3^{3k}a^2 + 1) = 3^{3(k-t)} - 1$$

* * *

PROBLEMA 145. Scriviamo $b = F_n = 2^{2^n} + 1$.

Se $b \mid 3^{(b-1)/2} + 1$, allora $b \mid 3^{b-1} - 1$; quindi $o_b(3) \mid b - 1$ ma $o_b(3) \nmid \frac{b-1}{2}$, e pertanto $o_b(3) = b - 1$. Per il Teorema di Eulero, $b - 1 \mid \phi(b)$, dunque $\phi(b) = b - 1$ e b è un numero primo.

Viceversa, sia b un primo. Allora, per il Teorema 4.11 di reciprocità quadratica,

$$\left(\frac{3}{b}\right) = \left(\frac{b}{3}\right) = \left(\frac{2^{2^n} + 1}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Per il criterio di Eulero (Proposizione 4.7),

$$-1 \equiv 3^{\frac{b-1}{2}} \pmod b$$

ovvero $b \mid 3^{(b-1)/2} + 1$.

* * *

PROBLEMA 146. Dimostriamo che l'unico intero positivo n tale che $2^n-1 \mid 3^n-1$ è $n=1$. Sia $n>1$. Se n è pari, $3 \mid 2^n-1$ mentre $3 \nmid 3^n-1$. Possiamo dunque assumere n dispari. Allora $2^n \equiv 0 \pmod 2$ e $2^n-1 \equiv 2 \pmod 3$, quindi

$$2^n \equiv 8 \pmod{12}. \tag{4.9}$$

Sia p un divisore primo di 2^n-1; allora p è dispari e $p \neq 3$, e da (4.9) segue

$$p \equiv \pm 1, \pm 5 \pmod{12}.$$

Ora, se p è un primo con $p = 12k \pm 5$ (per qualche $k \geq 0$), allora, per la legge di reciprocità quadratica,

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = (-1)^{\frac{\pm 5-1}{2}} \left(\frac{\pm 5}{3}\right) = -1;$$

dunque, 3 non è un quadrato modulo p, e ciò implica, poiché n è dispari, che nemmeno 3^n è un quadrato modulo p; in particolare $p \nmid 3^n-1$.
Pertanto, se $2^n-1 \mid 3^n-1$, ogni divisore primo p di 2^n-1 è tale che $p \equiv \pm 1 \pmod{12}$. Ma questo implica $2^n-1 \equiv \pm 1 \pmod{12}$, il che è assurdo dato che $2^n-1 \equiv 7 \pmod{12}$.

* * *

PROBLEMA 147. Siano a e b interi positivi tali che $15a+16b$ e $16a-15b$ sono entrambi quadrati; poniamo $15a+16b=x^2$ e $16a-15b=y^2$. Allora,

$$\begin{cases} 15x^2+16y^2 = 15^2a+240b+16^2a-240b = 481a \\ 16x^2-15y^2 = 240a+16^2b-240a+15^2b = 481b \end{cases}$$

Quindi, sommando, $31x^2-y^2 = 481(a+b) = 13 \cdot 37 \cdot (a+b)$. In particolare,

$$31x^2 \equiv y^2 \pmod{13 \cdot 37}. \tag{4.10}$$

Ora, per la legge di reciprocità quadratica

$$\left(\frac{31}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1;$$

quindi se $13 \nmid x$, $\left(\frac{31x^2}{13}\right) = \left(\frac{31}{13}\right) = -1$, che contraddice (4.10). Dunque $13 \mid x$. Similmente,

$$\left(\frac{31}{37}\right) = \left(\frac{37}{31}\right) = \left(\frac{6}{31}\right) = \left(\frac{3}{31}\right)\left(\frac{2}{31}\right) = -\left(\frac{31}{3}\right)(-1)^{\frac{31^2-1}{8}} = -1;$$

da cui, come prima, si deduce $37 \mid x$.
Quindi x, e di conseguenza y, sono multipli di $13 \cdot 37 = 481$, e dunque $x^2, y^2 \geq 481^2$. D'altra parte, ponendo $a = 31 \cdot 481$ e $b = 481$ si ottiene

$$15a+16b = (15 \cdot 31 + 16)481 = 481^2, \qquad 16a-15b = (16 \cdot 31 - 15)481 = 481^2.$$

La risposta è dunque 481^2.

5

Numeri primi.

Questo capitolo tratta, per quanto si riesca a fare in modo elementare, della fondamentale questione della distribuzione dei numeri primi. La domanda, espressa in modo certo non matematico è "quanti sono i numeri primi?" (in modo corretto: dato un numero positivo n, quanti sono i numeri primi che non superano n?); meglio ancora, è possibile descrivere come si distribuiscono i numeri primi nella successione dei numeri naturali?

5.1. La successione dei numeri primi

Il crivello di Eratostene. Si tratta del più semplice e, come suggerisce il nome, antico algoritmo per la ricerca dei numeri primi. Poiché in rete si trovano facilmente applicazioni più o meno animate e colorate che fanno vedere e comprendere l'algoritmo in maniera molto più accattivante e chiara di quanto sia capace di produrre il sottoscritto, mi limito ad illustrarlo con un esempio minimalista: trovare tutti i numeri primi positivi minori o uguali a 120.

Si prendono i numeri da 2 a 120 e li si dispone "nel crivello". Si mette da parte 2, che il minimo numero primo, e si considerano i suoi multipli,

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100	101	102	103	104	105
106	107	108	109	110	111	112	113	114	115	116	117	118	119	120

questi passano attraverso il primo filtro - il più fine - del crivello, e noi dunque li cassiamo; si prende allora il primo numero maggiore di 2 non eliminato, il numero 3, lo si mette da parte, si considerano i multipli di 3 che sono rimasti nel setaccio,

	2	3	–	5	–	7	–	9	–	11	–	13	–	15
–	17	–	19	–	21	–	23	–	25	–	27	–	29	–
31	–	33	–	35	–	37	–	39	–	41	–	43	–	45
–	47	–	49	–	51	–	53	–	55	–	57	–	59	–
61	–	63	–	65	–	67	–	69	–	71	–	73	–	75
–	77	–	79	–	81	–	83	–	85	–	87	–	89	–
91	–	93	–	95	–	97	–	99	–	101	–	103	–	105
–	107	–	109	–	111	–	113	–	115	–	117	–	119	–

questi passano attraverso il secondo filtro (con i fori un poco più larghi), e li si cassa; il più piccolo numero rimasto è un primo, che è il 5; lo si mette da parte, si considerano i suoi multipli non ancora eliminati, e li si cassa;

	2	3	–	5	–	7	–	–	–	11	–	13	–	–
–	17	–	19	–	–	–	23	–	25	–	–	–	29	–
31	–	–	–	35	–	37	–	–	–	41	–	43	–	–
–	47	–	49	–	–	–	53	–	55	–	–	–	59	–
61	–	–	–	65	–	67	–	–	–	71	–	73	–	–
–	77	–	79	–	–	–	83	–	85	–	–	–	89	–
91	–	–	–	95	–	97	–	–	–	101	–	103	–	–
–	107	–	109	–	–	–	113	–	115	–	–	–	119	–

arrivando a lasciare il prossimo numero primo, che è 7, i multipli di 7 ancora nel setaccio li si cassa;

	2	3	–	5	–	7	–	–	–	11	–	13	–	–
–	17	–	19	–	–	–	23	–	–	–	–	–	29	–
31	–	–	–	–	–	37	–	–	–	41	–	43	–	–
–	47	–	49	–	–	–	53	–	–	–	–	–	59	–
61	–	–	–	–	–	67	–	–	–	71	–	73	–	–
–	77	–	79	–	–	–	83	–	–	–	–	–	89	–
91	–	–	–	–	–	97	–	–	–	101	–	103	–	–
–	107	–	109	–	–	–	113	–	–	–	–	–	119	–

a questo punto, il più piccolo numero rimasto 11 è un primo; il suo quadrato è maggiore di 120, il che significa che non ci sono altri multipli di 11 da eliminare (perché i multipli del tipo $11 \cdot x$ con $2 \leq x \leq 10$ sono già stati cassati in precedenza). Quindi i numeri rimasti sono tutti numeri primi:

	2	3	–	5	–	7	–	–	–	11	–	13	–	–
–	17	–	19	–	–	–	23	–	–	–	–	–	29	–
31	–	–	–	–	–	37	–	–	–	41	–	43	–	–
–	47	–	–	–	–	–	53	–	–	–	–	–	59	–
61	–	–	–	–	–	67	–	–	–	71	–	73	–	–
–	–	–	79	–	–	–	83	–	–	–	–	–	89	–
–	–	–	–	–	–	97	–	–	–	101	–	103	–	–
–	107	–	109	–	–	–	113	–	–	–	–	–	–	–

Nel seguito denoteremo con $\mathbb{P}$ l'insieme dei numeri primi positivi e, quando ciò potrà contribuire alla chiarezza, intenderemo $\mathbb{P}$ ordinato in ordine crescente $p_1, p_2, p_3, \ldots$ (quindi, $p_1 = 2$, $p_2 = 3$, etc.), diremo anche che p_n è l'n-esimo numero primo.
La successione $\{p_n\}_{n\geq 1}$ tende a infinito, per il Teorema di Euclide, e ci si chiede quanto rapidamente lo faccia (o, equivalentemente, quanto rapidamente il reciproco $1/p_n$ tenda a 0). Il crivello di Eratostene sembra suggerire (per il momento sperimentalmente) che per ogni $n \geq 1$, $n < p \leq n^2$. Che la successione $\frac{1}{p_n}$ tenda a 0 più lentamente (cioè sia un infinitesimo di ordine inferiore) di $\frac{1}{n^2}$ è confermato dal seguente risultato (anche questo dovuto a Leonard Euler).

Teorema 5.1 (Eulero)**.** *La serie* $\sum_{p\in\mathbb{P}} \frac{1}{p}$ *è divergente.*

Dimostrazione. (P. Erdos) Con le notazioni introdotte sopra, supponiamo per assurdo che la serie

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \sum_{n\geq 1} \frac{1}{p_n}$$

converga. Allora esiste un k tale che $\sum_{i>k} \frac{1}{p_i} < \frac{1}{2}$; quindi, per un qualunque numero intero $N \geq 1$,

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Dato $N \geq 1$, sia N_0 il numero di interi positivi $n \leq N$ che sono divisibili per almeno un primo p_j con $j \geq k+1$, e con N_1 il numero di numeri di interi positivi $n \leq N$ che sono divisibili solo da primi p_t con $t \leq k$. Chiaramente, per definizione, $N_0 + N_1 = N$.
Osserviamo che il numero di interi $1 \leq n \leq N$ che sono multipli del primo p_i è al più $\frac{N}{p_i}$. Quindi

$$N_0 \leq \sum_{j \geq k+1} \frac{N}{p_j} < \frac{N}{2}.$$

Stimiamo ora N_1. Osserviamo che ogni numero naturale n può essere scritto in modo univoco come $n = a_n b_n^2$, dove b_n^2 è il massimo quadrato che divide n, e a_n è un prodotto di primi *distinti*. Ora, se i divisori primi di $n \leq N$ sono tutti compresi tra $p_1, p_2, \ldots, p_k$, si ha che il numero di possibili fattori a_n per tali interi n, è 2^k. D'altra parte, sempre per tali n, $b_n \leq \sqrt{n} \leq \sqrt{N}$, e dunque ci sono al più $\sqrt{N}$ possibilità per il fattore b_n. In conclusione,

$$N_1 \leq 2^k \sqrt{N}.$$

Poiché $N = N_0 + N_1$ vale per ogni $N \geq 1$, si ha

$$N < \frac{N}{2} + 2^k \sqrt{N}.$$

Ma tale relazione è falsa per $N \geq 2^{2k+2}$, e questa contraddizione dimostra che la serie $\sum_{p \in \mathbb{P}} \frac{1}{p}$ deve essere divergente. □

Come abbiamo visto (Lemma 3.13), $\sum_{n \geq 1} \frac{1}{n^2} = \zeta(2) = \frac{\pi^2}{6}$, quindi questo Teorema conferma che la successione $\frac{1}{p_n}$ tende a 0 meno rapidamente di $\frac{1}{n^2}$.

Il Teorema dei numeri primi. Un'altra maniera di presentare la stessa osservazione è dire che il Teorema 5.1 implica che, tra tutti i reciproci $\frac{1}{n}$ dei numeri interi positivi, quelli per cui n è un quadrato sono "di meno" di quelli per cui n è un numero primo.

Introduciamo ora la seguente notazione: se x è un numero reale maggiore di 1, denotiamo con $\pi(x)$ il numero di numeri primi positivi minori od uguali ad x.

Il commento di sopra può essere quindi meglio formulato dicendo che il Teorema 5.1 comporta che, almeno per x sufficientemente grande, $\pi(x)$ sia maggiore del numero di quadrati interi minori uguali ad x, cioè $\lfloor \sqrt{x} \rfloor$; ed anzi che il rapporto $\pi(x)/\sqrt{x}$ tende a infinito. Di fatto, sappiamo che per ogni numero reale $\alpha > 1$, la serie $\sum_{n \geq 1} \frac{1}{n^\alpha}$ è convergente, dunque possiamo aspettarci che per ogni $\alpha > 1$, a partire da un opprotuno valore di x, si abbia $\pi(x) \geq x^{\frac{1}{\alpha}}$, o anzi che la funzione $\pi(x)$ sia un infinito di ordine superiore a $x^{\frac{1}{\alpha}}$.
Ora, una delle prime funzioni che vengono in mente, il cui ordine di infinito si minore di quello di x e maggiore di ogni x^β per ogni $0 < \beta < 1$, è la funzione $\frac{x}{\log x}$.

Infatti, il più importante risultato concernente la funzione $\pi(x)$ è il giustamente celebre *Teorema dei Numeri Primi*, congetturato da Legendre e da Gauss e provato, indipendentemente da Hadamard e La Vallee Poussin nel 1896.

Teorema 5.2 (Teorema dei Numeri Primi)**.**

$$\pi(x) \sim \frac{x}{\log x},$$

Dove, se $f(x)$ e $g(x)$ sono funzioni reali definite su un intervallo $(x_0, +\infty)$, con la scrittura $f(x) \sim g(x)$ si intende che $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

La dimostrazione di questo Teorema è al di fuori dagli scopi di queste note, dove ci accontentiamo di provare, con i metodi elementari scoperti da P. Erdos, un precedente risultato di Čebichev[1] (1860), che afferma che esistono due costanti $A, B > 0$ tali che

$$A\frac{x}{\log x} \leq \pi(x) \leq B\frac{x}{\log x} \ .$$

5.2. Il Teorema di Čebichev

Premettiamo la seguente convenzione: quando la lettera p compare nella definizione di una somma o di un prodotto a più termini, si intende che p rappresenta un numero primo positivo (variabile). In particolare, sia $1 \leq x$ un numero reale; con le scritture

$$\sum_{p\leq x} \qquad \text{e} \qquad \sum_{p^m \leq x}$$

intenderemo, rispettivamente, la somma fatta su tutti i numeri primi positivi minori o uguali a x, e quella su tutte le potenze minori o uguali a x di numeri primi positivi.

Come detto, la dimostrazione del Teorema di Čebichev segue una tecnica introdotta da Erdos, che, in ultima analisi, consiste in una intelligente manovra di valutazione delle fattorizzazioni in potenze di primi dei coefficienti binomiali. In questa manovra, torneranno utili le considerazioni sulla valurtazione p-adica dei fattoriali viste nella sezione **??**.

Lasciamo per esercizio la facile dimostrazione della seguente diseguaglianza.

Lemma 5.3. *Sia n un numero intero positivo; allora, per ogni $0 \leq i \leq 2n$,*

$$\binom{2n}{i} \leq \binom{2n}{n}.$$

Continuiamo con un'altra stima piuttosto semplice.

Lemma 5.4. *Sia n un intero positivo; allora*

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n} < 2^{2n} \ .$$

[1] Pafnufy L. Čebichev (1821–1894), matematico russo, oltre alla teoria dei Numeri, i suoi contributi principali riguardano la probabilità e la statistica.

Dimostrazione. Sia $n \in \mathbb{N}^*$. Allora

$$2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} > \binom{2n}{n} .$$

Viceversa, dal Lemma 5.3 segue

$$2^{2n} = 2 + \sum_{i=1}^{2n-1} \binom{2n}{i} \leq 2 + (2n-1)\binom{2n}{n} \leq 2n\binom{2n}{n},$$

da cui la prima disuguaglianza. □

Definiamo ora le seguenti due funzioni ('theta' e 'psi' di Čebichev). Sia x un numero reale maggiore di 1; poniamo

$$\theta(x) = \sum_{p \leq x} \log p$$

$$\psi(x) = \sum_{p^m \leq x} \log p \ .$$

Ad esempio,

$$\theta(10) = \log 2 + \log 3 + \log 5 + \log 7$$

$$\psi(10) = 3\log 2 + 2\log 3 + \log 5 + \log 7$$

Osservazione. Per ogni $x > 1$ si ha

$$\psi(x) = \sum_{p^m \leq x} \log p = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \leq \sum_{p \leq x} \frac{\log x}{\log p} \log p = \pi(x) \log x \ .$$

Proposizione 5.5. *Per ogni* $1 < x \in \mathbb{R}$,

$$\theta(x) < 2x \log 2 \ .$$

Dimostrazione. Poichè $\theta(x) = \theta([x])$, è chiaro che è sufficiente provare l'affermazione per $x = n \in \mathbb{N}^*$.

Premettiamo una osservazione. Sia $m \in \mathbb{N}^*$, e sia

$$M = \binom{2m+1}{m} = \binom{2m+1}{m+1} = \frac{(2m+1)2m(2m-1)\cdots(m+2)}{m!} \ .$$

Ora, questo M è un intero che compare due volte come addendo nell'espansione binomiale $(1+1)^{2m+1} = 2^{2m+1}$. Quindi $2M < 2^{2m+1}$, cioè $M < 2^{2m}$. Se p è un primo tale che $m+1 < p \leq 2m+1$, allora p divide il numeratore ma non il denominatore nell'espressione di M come frazione; quindi divide M. Dunque

$$\prod_{m+1<p\leq 2m+1} p \quad \text{divide} \quad M.$$

Da ciò segue

$$\theta(2m+1) - \theta(m+1) = \sum_{m+1<p\leq 2m+1} \log p \leq \log M < 2m \log 2 \ .$$

Proviamo ora la Proposizione procedendo per induzione su n. Se $n = 2$ l'affermazione è banale. Sia $n \geq 3$ e assumiamo la proposizione vera per $m \leq n-1$.

- Se n è pari, n non è un numero primo e, applicando l'ipotesi induttiva,

$$\theta(n) = \theta(n-1) < 2(n-1)\log 2 < 2n \log 2.$$

- Se $n = 2m+1$ è dispari, $m+1 < n$; applicando l'ipotesi induttiva e l'osservazione di sopra,

$$\theta(n) = \theta(2m+1) - \theta(m+1) + \theta(m+1) < 2m \log 2 + 2(m+1)\log 2 = 2n \log 2;$$

come si voleva. □

Esercizio 5.1. Provare che per ogni numero reale $x \geq 1$, $\psi(x) = \log U(x)$, dove $U(x)$ è il minimo comune multiplo di tutti gli interi positivi minori od uguali a x.

Esercizio 5.2. Sia $1 < x \in \mathbb{R}$, e sia $t = [\log_2 x] = [\log x / \log 2]$. Si provi che

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \ldots + \theta(x^{1/t}) \ .$$

Esercizio 5.3. Sia $n \in \mathbb{N}^*$; si provi che

$$\prod_{p\leq n} p < 4^n \ .$$

Proposizione 5.6. *Per ogni* $1 < x \in \mathbb{R}$,

$$\psi(x) \geq \frac{1}{4} x \log 2 \ .$$

Dimostrazione. Sia $n \in \mathbb{N}^*$, e sia

$$N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p\leq 2n} p^{\nu_p(N)} \ .$$

Per il Teorema 2.4, e l'osservazione che lo segue,

$$\nu_p(N) = \nu_p((2n)!) - 2\nu_p(n!) = \sum_{m\geq 1} \left(\left\lfloor \frac{2n}{p^m} \right\rfloor - 2 \left\lfloor \frac{n}{p^m} \right\rfloor \right).$$

Ora, si vede facilmente che ciascun termine $\left\lfloor \frac{2n}{p^m} \right\rfloor - 2 \left\lfloor \frac{n}{p^m} \right\rfloor$ è uguale a 0 o ad 1 a seconda che $\left\lfloor \frac{2n}{p^m} \right\rfloor$ sia pari o dispari. Quindi

$$\nu_p(N) \leq \log_p(2n) \leq \left\lfloor \frac{\log 2n}{\log p} \right\rfloor$$

da cui segue

$$\log N = \sum_{p \le 2n} \nu_p(N) \log p \le \sum_{p \le 2n} \left\lfloor \frac{\log 2n}{\log p} \right\rfloor \log p = \psi(2n) \ .$$

D'altra parte, $N \ge 2^n$ e quindi

$$\psi(2n) \ge n \log 2.$$

Sia ora $2 \le x \in \mathbb{R}$. Allora, $n = \left\lfloor \frac{x}{2} \right\rfloor \ge 1$ e, per quanto visto sopra, si ha

$$\psi(x) \ge \psi(2n) \ge n \log 2 \ge \frac{1}{4} x \log 2,$$

completando la dimostrazione. □

Possiamo ora provare il risultato annunciato.

Teorema 5.7. (Čebichev). *Per ogni* $2 \le x \in \mathbb{R}$,

$$\frac{\log 2}{4} \frac{x}{\log x} \le \pi(x) \le (2 + 4 \log 2) \frac{x}{\log x}.$$

Dimostrazione. Sia $1 < x \in \mathbb{R}$. Per la proposizione 5.6, e l'osservazione che segue la definizione di $\psi(x)$, si ha

$$\frac{1}{4} x \log 2 \le \psi(x) \le \pi(x) \log x,$$

da cui si ricava la limitazione inferiore

$$\frac{\log 2}{4} \frac{x}{\log x} \le \pi(x).$$

Sia ora $\delta \in \mathbb{R}$, con $0 < \delta < 1$. Allora $x^\delta < x$, e

$$\theta(x) \ge \sum_{x^\delta < p \le x} \log p \ge \sum_{x^\delta < p \le x} \log(x^\delta) \ge \log(x^\delta) \left\lfloor \pi(x) - \pi(x^\delta) \right\rfloor,$$

e dunque

$$\pi(x) \log(x^\delta) \le \theta(x) + \pi(x^\delta) \log(x^\delta) \le \theta(x) + x^\delta \log(x^\delta).$$

Applicando la Proposizione 5.5, si ottiene

$$\pi(x) \log(x^\delta) \le 2x \log 2 + x^\delta \log(x^\delta),$$

e ancora

$$\pi(x) \le 2x \frac{\log 2}{\log(x^\delta)} + x^\delta.$$

Ponendo $\delta = \frac{1}{2}$, si ricava

$$\pi(x) \le \frac{4x \log 2}{\log x} + \sqrt{x} \ .$$

Ora, per $x \geq 2$,

$$\sqrt{x} < \frac{2x}{\log x},$$

quindi è possibile maggiorare la diseguaglianza precedente

$$\pi(x) \leq \frac{4x \log 2}{\log x} + \frac{2x}{\log x} = (4 \log 2 + 2)\frac{x}{\log x},$$

completando la dimostrazione. □

5.3. Il postulato di Bertrand

Con tecniche analoghe è possibile provare un interessante e talvolta utile risultato che, nonostante sia un teorema a tutti gli effetti, prende il nome di postulato di Bertrand, dato che per qualche anno è rimasto una congettura (formulata, appunto, da J. Bertrand nel 1845, e dimostrata poi da Čebichev)

Teorema 5.8. (Postulato di Bertrand). *Per ogni intero positivo n esiste un numero primo p tale che $n < p \leq 2n$.*

Dimostrazione. Poiché i numeri

$$2,\ 3,\ 5,\ 7,\ 13,, 23,\ 43,\ 83,\ 163,\ 317,\ 631$$

sono numeri primi, ognuno dei quali è maggiore della metà del successivo, l'affermazione dell'enunciato è vera per $n \leq 630$; in particolare è vera per $n \leq 2^9 = 512$.
Sia ora $n \geq 512$, e poniamo $N = \binom{2n}{n}$. Supponiamo per assurdo che non esista alcun numero primo p con $n < p \leq 2n$, allora

$$N = \binom{2n}{n} = \prod_{p \leq 2n} p^{\nu_p(N)} = \prod_{p \leq n} p^{\nu_p(N)}.$$

dove (si veda la dimostrazione della Proposizione 5.6)

$$\nu_p(N) = \sum_{m \geq 1} \left(\left\lfloor \frac{2n}{p^m} \right\rfloor - 2 \left\lfloor \frac{n}{p^m} \right\rfloor \right).$$

Sia p un numero primo con $\frac{2}{3}n < p \leq n$. Allora $2p \leq 2n < 3p$, e $2n < \frac{4}{9}n^2 < p^2$, e si ha

$$\nu_p(N) = \left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor = 0.$$

Dunque se p è un divisore primo di N, si ha $p \leq \frac{2}{3}n$; e quindi, per la Proposizione 5.5,

$$\sum_{p|N} \log p \leq \sum_{p \leq \frac{2}{3}n} \log p = \theta\Big(\frac{2}{3}n\Big) \leq \frac{4}{3} n \log 2.$$

Ora, sia p un primo tale che $p^2|N$ (cioè $\nu_p(N) \geq 2$); allora (si veda ancora la dimostrazione della Proposizione 5.6),

$$2 \leq \nu_p(N) \leq \left\lfloor \frac{\log 2n}{\log p} \right\rfloor \leq \frac{\log 2n}{\log p}$$

e quindi $\nu_p(N) \log p \leq \log 2n$, e in particolare $p^2 \leq 2n$, cioè $p \leq \sqrt{2n}$. Pertanto

$$\sum_{p^2|N} \nu_p(N) \log p \leq \sqrt{2n} \log 2n \ ,$$

da cui si ricava

$$\log N = \sum_{p|N} \nu_p(N) \log p = \sum_{\nu_p(N)=1} \log p + \sum_{p^2|N} \nu_p(N) \log p \leq \frac{4}{3} n \log 2 + \sqrt{2n} \log 2n \ .$$

Ma, per il Lemma 5.4,

$$\log N \geq \log \left(\frac{2^{2n}}{2n} \right) = 2n \log 2 - \log 2n \ ,$$

che, dal confronto con la diseguaglianza precedente, dà

$$2n \log 2 \leq \log N + \log 2n \leq \frac{4}{3} n \log 2 + \sqrt{2n} \log 2n$$

da cui si ricava

$$2n \log 2 \leq 3(\sqrt{2n} + 1) \log 2n$$

ed ancora

$$2n \leq 3(\sqrt{2n} + 1)(\log_2 n + 1) \ .$$

La dimostrazione si conclude provando che tale diseguaglianza non vale per $n \geq 512$. In tal caso, infatti, $\sqrt{2n} \geq 15$, e quindi $3(\sqrt{2n} + 1) \leq \frac{16}{5}\sqrt{2n}$, che, se vale la disuguaglianza di sopra, implica

$$2n \leq \frac{16}{5} \sqrt{2n} (\log_2 n + 1)$$

da cui

$$\sqrt{2n} \leq \frac{16}{5} (\log_2 n + 1) \ .$$

Siano $f(x) = \sqrt{2x}$, e $g(x) = \frac{16}{5}(\log_2 x + 1)$. Per $x = 512 = 2^9$, si ha

$$f(x) = 2^5 = 32 \qquad \text{e} \qquad g(x) = \frac{16}{5}(\log_2 2^9 + 1) = \frac{16}{5} 10 = 32 \ ,$$

mentre per $x > 512$, $f(x) > g(x)$. Questa contraddizione completa la dimostrazione. □

Questo Teorema (postulato di Bertrand) è stato generalizzato e migliorato in varie direzioni; ad esempio, si può dimostrare (Ramanujan e, indipendentemente, Erdos) che per ogni intero positivo k esiste un intero M tale che per ogni $n \geq M$ esistono k primi distinti tra n e $2n$. Invece, ancora aperta è la affine *Congettura di Legendre*:

per ogni intero positivo n esiste un numero primo p con $n^2 < p \leq (n+1)^2$.

(per questa, il Teorema dei Numeri Primi non aiuta).

5.4. Altri risultati e problemi

Il Teorema dei Numeri Primi quantifica, almeno asintoticamente, l'idea intuitiva che i numeri primi si vadano diradando man mano che si cresce: infatti, per $x \geq 1$ un numero reale (grande), la probabilità $P(x)$ che un intero positivo $n \leq x$ sia un numero primo è all'incirca $\frac{1}{\log x}$.
Questo tuttavia non dice molto riguardo l'effettiva distribuzione dei numeri primi. Ad esempio, un famoso problema aperto è quello dei *Primi gemelli*. Due numeri primi positivi p, q, con $p < q$, si dicono *gemelli* se $q = p + 2$ (in tal caso si dice che (p, q) è una coppia di primi gemelli). Ad esempio, sono coppie di primi gemelli $(3, 5), (5, 7), (11, 13), (17, 19), \ldots$
Il problema, ancora irrisolto, è:

esistono infinite coppie di primi gemelli?

Recentemente (2014) Yitang Zhang ha dimostrato l'esistenza di un numero N tale che esistono infinite coppie di numeri primi consecutivi la cui differenza non supera N;

Teorema 5.9 (Y. Zhang)**.** *Esiste un intero $N \leq 7 \times 10^6$ tale che $q - p = N$ per infinite coppie di numeri primi (p, q).*

Denotando con p_n l'n-esimo numero primo (per $n \geq 1$, nell'ordine crescente dei numeri interi), una maniera più formale per enunciare questo risultato è:

$$\liminf_{n\to\infty}(p_{n+1} - p_n) = N.$$

Il problema dei Primi Gemelli chiede appunto se si possa prendere $N = 2$. La pubblicazione dell'articolo di Zhang suscitò infatti un grosso interesse e stimolò altri ricercatori a cercare di migliorare il limite per N trovato da Zhang; nel giro di qualche anno, per il contributo di vari studiosi, tale limite è stato ridotto a 256 (e, pare, anche meno).
Si noti che dal Teorema dei numeri primi discende che, per numeri fino ad un certo n, la distanza media di un numero primo dal successivo tende ad approssimarsi a $\log n$, e quindi tende a infinito al crescere di n; anche se non risolve il problema dei gemelli, il Teorema di Y. Zhang è quindi molto significativo.

Un altro famoso problema irrisolto riguardante i numeri primi è la *Congettura di Goldbach*, della quale diremo qualche cosa nel prossimo capitolo.

* * *

Venendo un po' ai problemi, è chiaro che i risultati di questo capitolo sono di un livello superiore a quello che, giustamente, viene assunto nelle competizioni matematiche. Altrettanto chiaro è che la conoscenza e l'utilizzo di alcuni risultati più avanzati, come ad esempio il Postulato di Bertrand, può portare a soluzioni particolarmente brevi o, come nel caso del seguente esempio, eleganti.

Problema 148 (Cina 2015)**.** *Determinare tutti gli interi $k \geq 1$ tali che esistono infiniti interi positivi n con*

$$n + k \nmid \binom{2n}{n}.$$

SOLUZIONE. Per $k = 1$, è facile provare che $n + 1 \mid \binom{2n}{n}$ per ogni intero positivo n (ed è ben noto: per $n \geq 1$, $C_n = \frac{1}{n+1}\binom{2n}{n}$ è l'n-esimo numero di Catalan).
Sia $k > 1$, per il Postulato di Bertrand esiste un primo p con $k < p < 2k$. Scegliamo n del tipo $n = (p - k) + p^m$ per ogni $m \in \mathbb{N}$; allora, per il Corollario 2.5,

$$v_p\left[\binom{2n}{n}\right] = \frac{2s_p(n) - s_p(2n)}{p-1}.$$

(dove, per $k \in \mathbb{N}$, $s_p(k)$ è la somma delle cifre nella rappresentazione in base p di k). Ora, $2n = 2(p-k) + 2p^m$ e $2(p-k) < p$: quindi $s_p(2n) = 2(p-k) + 2 = 2s_p(n)$, e dunque $v_p\left[\binom{2n}{n}\right] = 0$. D'altra parte, $p \mid n + k$. Quindi $n + k \nmid \binom{2n}{n}$ per infiniti interi n. ∎

Un altro fatto che, conoscendolo, assicura un certo vantaggio è il Teorema di Zsigmondy.

Teorema 5.10 (Zsigmondy[2])**.** *Siano $1 \leq b < a$ interi coprimi. Allora per ogni intero positivo n esiste un numero primo p tale che p divide $a^n - b^n$ ma non divide $a^t - b^t$ per ogni $1 \leq t < n$, tranne nei casi seguenti*

(a) $n = 1,\ a = b + 1$;

(b) $n = 2$ *e* $a + b$ *una potenza di* 2;

(c) $n = 6,\ a = 2,\ b = 1$.

Ad esempio, avendo in mano il Teorema di Zsigmondy riesce quasi banale la soluzione del Problema 75: *Sia n un intero positivo tale che $3^n - 2^n$ è la potenza di un numero primo. Si provi che n è un numero primo.* Di fatto, questo si generalizza notevolmente,

Problema 149. *Siano a, b, n interi positivi, con $a > b$ e $n \geq 2$. Provare che se $a^n - b^n$ è la potenza di un numero primo, allora n è un numero primo e $a - b = 1$.*

SOLUZIONE. Siano a, b, n interi positivi come nelle ipotesi. Nel caso (c) dell'enunciato del Teorema di Zsigmondy, $a^n - b^n = 63$ non è la potenza di un numero primo; nel caso (b), $n = 2$ è un primo e $a^2 - b^2 = (a-b)(a+b)$ è una potenza di 2, il che si verifica non essere possibile: infine, il caso (a) non si presenta per ipotesi. Supponiamo che $a^n - b^n$ sia la potenza di un primo, e sia p un divisore primo di n; allora $a^p - b^p$ divide $a^n - b^n$ e dunque, per il Teorema di Zsigmondy, e quanto sopra escluso, si deve avere $p = n$. Allo stesso modo, poiché $a - b \mid a^n - b^n$ deve essere $a - b = 1$. ∎

Il Teorema di Dirichlet. Mentre il Teorema di Zsigmondy, utilissimo e che si incontra applicato in diverse parti della matematica, è un risultato relativamente tecnico, di fondamentale importanza, sia teorica che per le applicazioni, è il Teorema di Dirichlet sui primi nelle progressioni aritmetiche.

Teorema 5.11 (Dirichlet)**.** *Siano a, c numeri naturali tali con $c \geq 1$ e $mcd(a, c) = 1$. Allora la progressione aritmetica $\{a + cn \mid n \in \mathbb{N}\}$ contiene infiniti numeri primi.*

Problema 150 (H. Lee, Amer. Math. Monthly)**.** *Si provi che per ogni $k, m \in \mathbb{N}^*$ esiste un intero positivo n tale che $\phi(n), \phi(n+1), \ldots, \phi(n+k)$ sono tutti multipli di m.*

[2]Karl Zsigmondy (1867–1925), matematico austriaco di origini ungheresi.

SOLUZIONE. Per il Teorema di Dirichlet, la progressione aritmetica $\{1 + dm \mid d \in \mathbb{N}\}$ contiene infiniti numeri primi; siano $p_0, p_1, \ldots, p_k$ primi distinti appartenenti a tale progressione e osserviamo che $m|p_i - 1$ per ogni $i = 0, 1, \ldots, k$. Ora, per il problema **??**, esiste un intero n tale che, per ogni $i = 0, \ldots, k$, p_i divide $n + i$. Quindi $p_i - 1$ divide $\phi(n + i)$ per ogni i, e dunque m divide $\phi(n), \phi(n + 1), \ldots, \phi(n + k)$. ∎

6

Teoria additiva

Con Teoria Additiva dei Numeri si intende compendiare in modo generico diverse questioni incentrate sulla somma di numeri interi. Tra le più storicamente rilevanti in quest'ambito è quella che riguarda la possibilità di rappresentare ogni numero naturale (o ogni numero naturale sufficientemente grande, oppure appartenente ad un certo sottoinsieme notevole) come somma di due o più elementi di un fissato sottoinsieme S dei numeri interi.
Un tipico problema in tal senso è la famosa *congettura di Goldbach*, la quale afferma che ogni numero naturale pari è somma di due numeri primi (o, equivalentemente, che ogni numero naturale è somma di al più tre primi). Un altro, del quale in questo capitolo daremo i primi risultati, è la questione di quali numeri siano rappresentabili come somme di un certo numero di potenze intere (con esponente fisso).

6.1. Somme di quadrati

Il primo problema che affrontiamo chiede quali siano i numeri interi (positivi) che si ottengono come somma di due quadrati interi. Il problema fu risolto da Eulero; la dimostrazione che vedremo è di fatto molto vicina a quella originale, ed utilizza il cosiddetto "metodo della discesa", precedentemente introdotto da P. Fermat, che noi riutilizzeremo più avanti per dimostrare il Teorema di Lagrange sulla somma di quattro quadrati. L'argomento si appoggia in ultima analisi sulla prime delle seguenti identità (la seconda la useremo nella dimostrazione del Teorema di Lagrange).

Lemma 6.1. *Siano $x_1, \dots, x_4, y_1, \dots, y_4$ numeri complessi. Allora*

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2. \tag{6.1}$$

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \tag{6.2}$$

dove

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \\ z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \ . \end{aligned}$$

Per la dimostrazione basta fare i calcoli (di fatto queste identità sussistono in qualsiasi anello commutativo); c'è anche un'identità simile per somme di 8 quadrati, che non impiegheremo in queste note.

Veniamo quindi alla somma di quadrati, ed iniziamo con il caso dei numeri primi.

Teorema 6.2 (Eulero)**.** *Sia p un numero primo positivo. Allora l'equazione*

$$x^2 + y^2 = p$$

è risolubile negli interi se e solo se $p = 2$ oppure $p \equiv 1 \pmod 4$.

Dimostrazione. Poiché $2 = 1 + 1 = 1^2 + 1^2$, l'affermazione è vera per $p = 2$. Inoltre, per ogni intero a, si ha $a^2 \equiv 0, 1 \pmod 4$, quindi, per ogni $a, b \in \mathbb{N}$,

$$a^2 + b^2 \equiv 0, 1, 2 \pmod 4;$$

dunque $x^2 + y^2 = p$ non è risolubile se $p \equiv 3 \pmod 4$.

Supponiamo ora $p \equiv 1 \pmod 4$. Allora, per il Lemma 1.20, esiste un intero $0 < t < p/2$ tale che $t^2 \equiv -1 \pmod p$. Pertanto (prendendo ad esempio $x_0 = t, y_0 = 1$) esistono interi x_0, y_0, k, con $0 < k < p$, tali che

$$x_0^2 + y_0^2 = kp. \tag{6.3}$$

Tra le possibili terne di questo tipo, scegliamo una in modo che k sia minimo, e supponiamo per assurdo che sia $k > 1$. Poniamo

$$\begin{aligned} x_0 &= bk + x_1 \\ y_0 &= ck + y_1 \end{aligned}$$

dove b, c sono interi, e x_1, y_1 sono rappresentanti di x_0, y_0 modulo k che possiamo trovare in modo che

$$-\frac{k}{2} \leq x_1, y_1 \leq \frac{k}{2} .$$

Allora,

$$x_1^2 + y_1^2 = (x_0 - bk)^2 + (y_0 - ck)^2 \equiv x_0^2 + y_0^2 \equiv 0 \pmod k;$$

dunque $x_1^2 + y_1^2 = k_1 k$, con $k_1 < k$, perchè, per la scelta di x_1, y_1,

$$x_1^2 + y_1^2 \leq 2(k/2)^2 = k^2/2 .$$

Applicando l'identità (6.1) otteniamo

$$(x_0^2 + y_0^2)(x_1^2 + y_1^2) = (x_0 x_1 + y_0 y_1)^2 + (x_0 y_1 - x_1 y_0)^2 = k_1 k^2 p .$$

Ora,

$$x_0 x_1 + y_0 y_1 = x_0(x_0 - bk) + y_0(y_0 - ck) \equiv x_0^2 + y_0^2 \equiv 0 \pmod k$$

e, similmente

$$x_0 y_1 - x_1 y_0 = x_0(y_0 - ck) - (x_0 - bk)y_0 \equiv x_0 y_0 - x_0 y_0 \equiv 0 \pmod k;$$

per cui, ponendo

$$x_2 = \frac{x_0x_1 + y_0y_1}{k} \qquad y_2 = \frac{x_0y_1 - x_1y_0}{k}$$

si ha

$$x_2^2 + y_2^2 = k_1 p$$

contro la scelta di k. □

A questo punto, non è difficile pervenire al criterio generale.

Teorema 6.3. *Sia $n \in \mathbb{N}^*$. Allora l'equazione*

$$x^2 + y^2 = n$$

è risolubile se e solo se per ogni primo $p \equiv 3 \pmod 4$, la massima potenza di p che divide n ha esponente pari.

Dimostrazione. Sia $D = \{a^2 + b^2 \mid a, b \in \mathbb{N}\}$; l'identità (6.1) nel lemma 6.1 assicura che l'insieme D è moltiplicativamente chiuso. Quindi se $n = 2^{\alpha_0} p_1^{\alpha_1} \dots p_n^{\alpha_n}$, con α_k pari per i primi $p_k \equiv 3 \pmod 4$, allora $n \in D$ per il teorema precedente.
Viceversa, sia $p \equiv 3 \pmod 4$, e supponiamo che $n = p^{2k+1}m$ appartenga a D con $(p, m) = 1$ e k minimale. Siano $x, y \in \mathbb{N}$ tali che $x^2 + y^2 = n$. Si ha che p non divide xy, perchè se p divide x o y, allora p^2 divide $x^2 + y^2 = n$ e quindi anche $p^{2k-1}m$ appartiene a D, contro la scelta di k. Allora y è invertibile modulo p; sia y' un suo inverso modulo p; da $x^2 \equiv -y^2 \pmod p$ segue

$$(xy')^2 = x^2(y')^2 \equiv -(yy')^2 \equiv -1 \pmod p.$$

Per il Lemma 1.20, segue la contraddizione $p \equiv 1 \pmod 4$. □

Modulo un numero primo, la situazione è anche più semplice.

Lemma 6.4. *Sia p un numero primo. Allora per ogni intero a la congruenza*

$$x^2 + y^2 \equiv a \pmod p$$

ammette soluzioni intere (detto altrimenti: ogni elemento del campo $\mathbb{Z}/p\mathbb{Z}$ è una somma di due quadrati).

Dimostrazione. Se $p = 2$ non c'e nulla da dimostrare. Sia dunque p un primo dispari, e sia B il sottoinsieme di $A = \{0, 1, \dots, p-1\}$ costituito da quadrati modulo p. Per quanto osservato nella sezione 4, $|B| = (p+1)/2$.
Sia $a \in \mathbb{Z}$. Se $p \mid a$ allora $a \equiv 0 = 0 + 0 \pmod p$. Passiamo quindi al caso in cui a è coprimo con p e scriviamo $a - B = \{a - b \mid b \in B\}$. Se $b, b' \in B$ sono tali che $a - b \equiv a - b' \pmod p$, allora $b' \equiv b \pmod p$ e dunque $b = b'$; questo significa che gli elementi di $a - B$ rappresentano $|B| = \frac{p+1}{2}$ classi diverse modulo p. Lo stesso vale, per definizione, per l'insieme B; poiché $|B| + |a - B| = p + 1 > p$, ciò implica che esistono $b, b' \in B$ tali che $a - b$ e b' rappresentano la stessa classe modulo p; ovvero $a - b \equiv b' \pmod p$. Ma b, b' sono quadrati modulo p; ovvero esistono $x, y \in \mathbb{Z}$ tali che $x^2 \equiv b \pmod p$ e $y^2 \equiv b' \pmod p$; pertanto

$$a \equiv b + b' \equiv x^2 + y^2 \pmod p$$

che è quel che si voleva provare. □

Passiamo alle somme di 4 quadrati, osservando innanzi tutto che dall'identità (6.2) nel lemma 6.1 segue che l'insieme

$$Q = \{a^2 + b^2 + c^2 + d^2 \mid a, b, c, d \in \mathbb{Z}\}$$

è moltiplicativamente chiuso. Il fondamentale Teorema di Lagrange assicura che $Q = \mathbb{N}$.

Teorema 6.5 (Lagrange)**.** *Ogni numero naturale n è somma di 4 quadrati interi.*

Dimostrazione. Il risultato è banalmente vero per $n = 0, 1, 2$; dunque, per quanto osservato prima dell'enunciato, è sufficiente provare che ogni primo positivo $p \geq 3$ appartiene all'insieme Q definito sopra (cioè è somma di quattro quadrati interi). Sia dunque p un primo dispari.
Sappiamo che ogni intero è congruo modulo p ad una somma di due quadrati. Dunque, esistono x_0, y_0 tali che $x^2 + y^2 \equiv -1 \, (mod\, p)$. Tali interi x, y possono essere presi in modo che $0 \leq x, y \leq \frac{p-1}{2}$. Dunque sistono interi positivi x, y ed m tali che

$$1 + x^2 + y^2 = mp \tag{6.4}$$

ed inoltre $0 < 1 + x^2 + y^2 < 1 + 2(\frac{p}{2})^2 < p^2$; e quindi

$$0 < m < p \ .$$

Sia ora m_0 il più piccolo intero positivo tale che $m_0 p$ è somma di quattro quadrati. Vogliamo provare che $m_0 = 1$. Per la 6.4, si ha $0 < m_0 < p$.
Siano x_1, x_2, x_3, x_4 interi tale che

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \ . \tag{6.5}$$

Supponiamo per assurdo, $m_0 \geq 2$, ed analizziamo separatamente i due casi: I) m_0 è pari; II) m_0 è dispari.

I) Se m_0 è pari, allora $x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p$ è pari; quindi $x_1 + x_2 + x_3 + x_4$ è pari. Dunque si verifica una delle seguenti posssibilità:
i) x_1, x_2, x_3, x_4 sono tutti pari;
ii) x_1, x_2, x_3, x_4 sono tutti dispari;
iii) x_1, x_2, x_3, x_4 sono due pari e due dispari; in questo caso possiamo assumere che x_1, x_2 siano pari, e x_3, x_4 siano dispari.
In tutti e tre i casi si ha che

$$x_1 + x_2, \ x_1 - x_2, \ x_3 + x_4, \ x_3 - x_4$$

sono interi pari. Ma allora

$$\frac{m_0}{2} p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

il che, poichè $\frac{m_0}{2}$ è un intero, contraddice la scelta di m_0.

II) Sia m_0 dispari; e quindi $m_0 \geq 3$. Allora, dividendo gli x_i per m_0; è possibile trovare interi b_i e y_i, per $i = 1, 2, 3, 4$, tali che

$$y_i = x_i - b_i m_0 \qquad \text{con} \quad |y_i| < \frac{m_0}{2} \ .$$

Osserviamo che, poichè m_0 non divide p, almeno uno degli x_i non è divisibile per m_0, e quindi che almeno uno degli y_i è diverso da 0. Dunque

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 = 4\left(\frac{m_0}{2}\right)^2 = m_0^2$$

ed inoltre

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \, (mod\, m_0)$$

ovvero, mettendo insieme queste due proprietà,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 m_0 \tag{6.6}$$

per qualche $0 < m_1 < m_0$. Moltiplicando membro a membro l'uguaglianza (5) e la (6), otteniamo

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = m_0^2 m_1 p$$

dove gli z_i sono dati dall'identità di Eulero (3). Ora, si osserva che

$$z_1 = \sum_{i=1}^{4} x_i y_i = \sum_{i=1}^{4} x_i(x_i - b_i m_0) \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \, (mod\, m_0) \ .$$

Analogamente si prova che, per $i = 1, 2, 3, 4$, si ha $z_i \equiv 0 \, (mod\, m_0)$. Esistono quindi interi positivi t_1, t_2, t_3, t_4 tali che

$$z_i = m_0 t_i \qquad \text{per} \quad i = 1, 2, 3, 4 \ .$$

ma allora

$$t_1^2 + t_2^2 + t_3^2 + t_4^2 = m_1 p$$

che, ancora una volta, è in contraddizione con la scelta di m_0.
Pertanto, deve essere $m_0 = 1$, e dunque p è somma di quattro quadrati, completando così la dimostrazione del Teorema. □

6.2. Il problema di Waring

Il Teorema 6.5, enunciato da Fermat, fu dimostrato da Lagrange nel 1770 (grosso modo con la stessa tecnica che abbiamo utilizzato). In quello stesso anno, nel suo libro *Meditationes Algebricae*, Edward Waring affermò, senza provarlo, che ogni numero intero può essere espresso come somma di al più 9 cubi, e di al più 19 quarte potenze. Più tardi, nell'edizione del 1782, egli aggiunse la congettura che per ogni $k \geq 2$, esiste un intero s tale che ogni numero naturale può scriversi come somma di al più s potenze k-esime. Nella letteratura moderna, fissato un k, si suole indicare con $g(k)$ il minimo valore possibile di tale s.

La dimostrazione della congettura, ovvero dell'esistenza di $g(k)$ per ogni $k \geq 2$, fu data da Hilbert nel 1909. La determinazione dei valori esatti di $g(k)$ (che viene comunemente chiamato *problema di Waring*), richiese più tempo, e lo sforzo combinato di diversi studiosi e tecniche.

Il Teorema di Lagrange risolve il caso $k = 2$.

Corollario 6.6. $g(2) = 4$.

Dimostrazione. Per il Teorema di Lagrange $g(2) \leq 4$. D'altra parte si vede subito che $n = 7$ non è somma di 3 quadrati. Dunque $g(2) = 4$. □

Il caso $n = 3$ fu risolto indipendentemente da Wieferich e da Kemper nel 1909-1912; essi provarono che $g(3) = 9$, ovvero che ogni numero naturale può essere espresso come somma di 9 cubi interi, e che esistono numeri naturali che non sono somma di otto cubi. Più tardi, Dickson provò che 23 e 239 sono i soli numeri naturali che richiedono almeno nove cubi, e nel 1943 Linnik dimostrò che ogni numero naturale sufficientemente grande può essere rappresentato come somma di 7 cubi.
Questo porta a definire una nuova funzione $G(k)$, come il minimo valore s, tale che ogni numero naturale sufficientemente grande può essere espresso come somma di s potenze k-esime. Dal teorema di Lagrange scende che $G(2) = 4$ (vedi la proposizione seguente). Il citato risultato di Linnik dice inoltre che $G(3) \leq 7$. La determinazione dei valori di $G(k)$ è un problema in larga parte ancora aperto; i soli valori esatti conosciuti sono $G(2) = 4$, e $G(4) = 16$ (Davemport 1939).

Proposizione 6.7. $G(2) = 4$.

Dimostrazione. Proviamo che nessun numero naturale congruo a 7 modulo 8 si può scrivere come somma di tre quadrati. Infatti, sia $x \in \mathbb{N}$;

- se $x = 2m$ è pari: $x^2 = 4m^2 \equiv 0\,(mod\,4)$;
- se $x = 2m = 1$ è dispari: $x^2 = (2m = 1)^2 = 4m(m + 1) + 1 \equiv 1\,(mod\,8)$.

Dunque, per ogni $x \in \mathbb{N}$,

$$x^2 \equiv 0,\ 1,\ 4\ (mod\,8)\ .$$

Da ciò segue subito che se $x, y, z \in \mathbb{N}$,

$$x^2 + y^2 + z^2 \not\equiv 7\,(mod\,8)$$

che è quello che si voleva. □

Questa semplice dimostrazione è un pezzettino banale di un risultato di Gauss che descrive tutti i numeri interi (positivi) che sono somme di 3 quadrati interi, La dimostrazione è meno elementare di quella dei Teoremi di Eulero e Lagrange, e la omettiamo.

Teorema 6.8 (Gauss)**.** *Un intero $n \geq 0$ è uguale alla somma di 3 quadrati interi se e solo se non è del tipo*

$$n = 4^s(8t + 7)$$

con $s, t \in \mathbb{N}$.

Torniamo alla funzione $g(k)$, e proviamo una limitazione inferiore per essa.

Proposizione 6.9. *Sia $k \geq 2$, e sia $q = \left\lfloor \frac{3}{2}^k \right\rfloor$; allora*

$$g(k) \geq 2^k + q - 2 \ .$$

Dimostrazione. Con le notazioni dell'enunciato, sia $n = 2^k q - 1$. Allora

$$n \leq 2^k \Big(\frac{3}{2}\Big)^k - 1 = 3^k - 1 < 3^k.$$

Dunque, in una espressione di n come somma di potenze k-esime i soli addendi non nulli che compaiono sono 1^k e 2^k. Chiaramente, il numero minimo necessario di addendi del tipo 2^k si ottiene come quoziente della divisione di n per 2^k:

$$n = (q-1)2^k + (2^k - 1)1^k \ .$$

Ne segue che per ottenere n come somma di potenze k-esime sono necessari almeno $q-1$ addendi uguali a 2^k e $2^k - 1$ addendi uguali a $1 = 1^k$. Pertanto

$$g(k) \geq q - 1 + 2^k - 1 = 2^k + q - 2 \ .$$

□

Per $n = 2, 3, 4$ la disuguaglianza della Proposizione precedente fornisce

$$g(3) \geq 9, \quad g(4) \geq 19, \quad g(5) \geq 37$$

che sono, di fatto, i valori corretti. Se $k \geq 7$ e $r = 3^k - q2^k$ (quindi $1 \leq r \leq 2^k - 1$), è stato provato che $2^k + q - 2$ è effettivamente il valore di $g(k)$ se risulta soddisfatta la disuguaglianza

$$r + q \leq 2^k \ .$$

È noto che tale disuguaglianza non è soddisfatta per al più un numero finito di interi n, ma non se ne conoscono controesempi.

Esercizio 6.1. Sfruttando la seguente identità

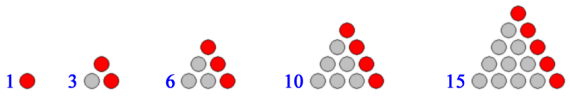
$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 \quad = \quad & (a+b)^4 + (a-b)^4 + (c+d)^4 + (c-d)^4 + \\ & (a+c)^4 + (a-c)^4 + (b+d)^4 + (b-d)^4 + \\ & (a+d)^4 + (a-d)^4 + (b+c)^4 + (b-c)^4 \end{aligned}$$

si provi che $g(4) \leq 50$.

6.3. Altri risultati e congetture

In questa sezione menzioniamo due classici problemi di Teoria additiva dei Numeri: il primo completamente risolto, il secondo ancora aperto nella sua generalità.

Numeri poligonali. Un intero positivo T si dice *numero triangolare* se rappresentando con figure omogenee (palline, per esempio) T unità, queste possono essere disposte in modo da formare una figura di triangolo isoscele (un caso di quelli che venivano chiamati *numeri figurati*; si tratta, come si comprende da una certa poetica vaghezza, di un'idea piuttosto antica[1]. La figura seguente[2] mostra i primi cinque numeri triangolari.



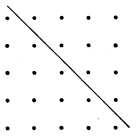
Questa stessa figura illustra chiaramente il fatto che l'n-esimo numero triangolare T_n coincide con la somma dei primi n numeri interi positivi (e questa è una definizione che non lascia scampo), e mostra anche il processo induttivo che conduce alla formula

$$T_n = \frac{n(n+1)}{2}.$$

Un intero positivo è *quadrato* (propriamente, sarebbe 'quadrangolare') se è la somma di tante unità quante se ne possono disporre a formare un quadrato. Chiaramente, l'n-esimo numero quadrato è proprio il quadrato di n, $Q_n = n^2$. Forse il più antico teorema riguardante numeri figurati è quello di Teone di Smirne (IV sec. a.c.): *ogni numero quadrato diverso da* 1 *è somma di due numeri triangolari.* La nostra dimostrazione

$$T_n + T_{n-1} = \frac{n(n+1)}{2} + \frac{n(n-1)}{2} = n^2 = Q_n;$$

quella di Teone:



Il risultato definitivo sui numeri triangolari si deve a Gauss.

Teorema 6.10 (Gauss)**.** *Ogni intero positivo è la somma di al più tre numeri triangolari.*

[1] Diofanto, che scrisse un libro sui numeri figurati, afferma che il primo a definire i numeri poligonali sia stato il matematico Ipsicle intorno al 170 a.c.

[2] Le le figure in questa sezione sono tratte da Wikipedia.

Dimostrazione. Tenendo conto che se m è un intero dispari allora $m^2 \equiv 1 \pmod 8$, dal Teorema 6.8 segue che ogni intero n con $n \equiv 3 \pmod 8$ è la somma di tre quadrati dispari. Per $n \in \mathbb{N}$ esistono dunque interi a, b, c tali che

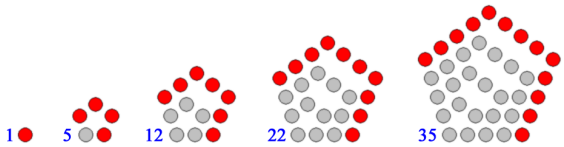
$$8n + 3 = (2a+1)^2 + (2b+1)^2 + (2c+1)^2 = 4a^2 + 4a + 4b^2 + 4b + 4c^2 + 4c + 3.$$

Quindi

$$n = \frac{a^2+a}{2} + \frac{b^2+b}{2}\frac{c^2+c}{2} = \binom{a+1}{2} + \binom{b+1}{2} + \binom{c+1}{2}$$

(intendendo $\binom{1}{2} = 0$) è la somma di al più tre numeri triangolari. □

Andando avanti con il numero di lati, ecco i primi cinque numeri pentagonali:



Non è difficile provare, seguendo il processo induttivo suggerito dalla figura, che l'n-esimo numero pentagonale è

$$P_n = \frac{3n^2 - n}{2}. \tag{6.7}$$

Estendendo ad ogni intero z la definizione (6.7) per P_z, Eulero dimostrò la seguente e bella identità:

$$\prod_{n=1}^{\infty}(1 - x^n) = \sum_{z=-\infty}^{\infty}(-1)^n x^{P_z}.$$

In generale, per $n \geq 3$, un intero positivo si dice n-gonale se è la somma di tante unità quante se ne possono disporre a formare un n-agono regolare.

Nel 1638, Pierre de Fermat affermò che ogni intero positivo si può scrivere come somma di al più n numeri n-agonali. Poiché Fermat non produsse alcuna dimostrazione, questa divenne nota come 'congettura di Fermat' sui numeri poligonali.

Il teorema 6.5 di Lagrange, del 1770, confermò la congettura nel caso $n = 4$; quello di Gauss 6.10, che risale al 1796[3], nel caso $n = 3$; mentre si deve a Cauchy la dimostrazione, nel 1814, della congettura nella sua generalità.

Teorema 6.11 (Cauchy)**.** *Sia $n \geq 3$; allora ogni intero positivo è somma di al più n numeri n-gonali.*

Una dimostrazione accessibile del Teorema di Cauchy (anzi di un risultato leggermente più forte) si trova in [5].

* * *

[3]Conosciamo la data esatta: il 10 Luglio 1796, Gauss annotò nel suo diario "EYPHKA: num = Δ + Δ + Δ".

La Congettura di Goldbach: In una lettera a Eulero, datata 7 Giugno 1742, il matematico Christian Goldbach formulò quella che oggi rimane forse la più famosa congettura irrisolta in Teoria dei Numeri:

Ogni numero intero pari maggiore o uguale a 4 *è la somma di due numeri primi.*

Una formulazione equivalente è: *ogni intero maggiore o uguale a* 6 *è la somma di tre numeri primi.* Grazie a intenso uso del computer, questa congettura è stata verificata fino a numeri molto grandi (tipo 10^{18}), ma una dimostrazione generale ancora non è stata trovata.
Nel 1930 Schnirelmann ha provato che esiste un numero $C < 8 \times 10^5$ tale che ogni numero intero positivo è la somma di al più C numeri primi. Il valore C è stato in seguito abbassato (grazie allo sforzo di diversi autori) fino a provare (Ramaré 1995) che ogni numero intero maggiore o uguale a 2 è la somma di al più sette numeri primi.
Nel 1973 J. Chen ha provato che ogni numero pari sufficientemente grande è la somma di due primi oppure di un primo e di un semiprimo (cioè il prodotto di due numeri primi).
Nel 2014, H. Helfgott ha diffuso la dimostrazione di quella che veniva chiamata *congettura di Goldbach debole*; precisamente

Teorema 6.12. *Ogni numero dispari maggiore o uguale a* 9 *è la somma di tre numeri primi dispari.*

Da ciò segue che ogni numero pari maggiore o uguale a 4 è la somma di al più quattro numeri primi. Questo risultato di Helfgott è certamente spettacolare, ma la percezione diffusa è che la congettura di Goldbach 'forte' sia molto più difficile.

6.4. Problemi inversi

Siano A e B sottoinsiemi non vuoti dell'insieme $\mathbb{Z}$ dei numeri interi. Con $A+B$ si intende l'insieme di tutte le somme $a+b$ al variare di $a \in A$ e $b \in B$. Ad esempio

$$\{2,3,4,7\} + \{2,5,6\} = \{4,5,6,7,8,9,10,12,13\}.$$

Scriviamo anche $2A = A + A$, $3A = A + A + A$, etc. I problemi classici di teoria additiva, come quelli ai quali abbiamo accennato nelle sezioni precedenti, consistono in genere nel descrivere $A + B$ (a di stabilirne alcune proprietà) a partire dalla conoscenza di A e B. Ad esempio, se indichiamo con Q l'insieme dei quadrati interi, il teorema 6.5 di Lagrange assicura che $4Q = \mathbb{N}$, mentre i Teoremi 6.3 di Eulero e 6.8 di Gauss descrivono rispettivamente $2Q$ e $3Q$; similmente, la congettura di Goldbach si può esprimere dicendo che $\mathbb{P}+\mathbb{P}$ contiene l'insieme di tutti i numeri pari maggiori o uguali a 4.

Con *problema inverso* si intende invece un problema in cui si chiede di ricavare informazioni sugli insiemi A e B , a partire da informazioni sulla loro somma $A + B$. Si tratta di un settore di ricerca che negli ultimi anni ha suscitato un notevole interesse in diversi studiosi.

Uno specifico problema che ha riscosso parecchia attenzione riguarda il caso di sottoinsiemi finiti A e B di $\mathbb{Z}$ e chiede cosa si possa dedurre intorno ad essi dalla semplice conoscenza

della cardinalità $|A+B|$. È abbastanza semplice osservare che, se A e B sono sottoinsiemi finiti e non vuoti di $\mathbb{Z}$ allora

$$\max\{|A|,|B|\} \leq |A+B| \leq |A||B|.$$

In questa sezione ci limitiamo ad esaminare il caso più semplice (e l'unico elementare), ovvero quello in cui $|A+B| < |A|+|B|$.

Chiamiamo *progressione aritmetica* un sottoinsieme finito A di $\mathbb{Z}$ del tipo

$$A = \{a, a+d, a+2d, \ldots, a+(n-1)d\} = \{a+dx \mid x = 0,1,\ldots,n-1\},$$

con $a \in \mathbb{Z}$, $d, n \in \mathbb{N}^*$. Il numero n (che altro non è che la cardinalità di A) è detto *lunghezza* della progressione, mentre l'intero positivo d si chiama *ragione* (o anche *differenza comune*) della progressione.

Siano $A = \{a+xb \mid 0 \leq x < n\}$ e $A_1 = \{a_1 + yb_1 \mid 0 \leq y < m\}$ progressioni aritmetiche di lunghezza, rispettivamente, n e m, e ragioni b e b_1. Allora,

$$A + A_1 = \big\{(a+a_1) + xb + yb_1 \mid (x,y) \in \{0,\ldots,n-1\} \times \{0,\ldots,m-1\}\big\},$$

per cui si osserva il fatto seguente

- *Se $b = b_1$, allora $A + A_1$ è una progressione aritmetica di lunghezza $n+m-1$ (e ragione b); in particolare, $|A+A_1| = |A|+|A_1|-1$.*

Da ciò segue facilmente la seguente osservazione.

Proposizione 6.13. *Sia A una progressione aritmetica, allora $A+A$ è una progressione aritmetica e $|A+A| = 2|A| = 1$; più in generale, per ogni intero $m \geq 2$, mA è una progressione aritmetica e*

$$|mA| \leq m|A| - m + 1.$$

Il risultato principale in questa sezione stabilisce che, in un certo senso, vale il viceversa.

Teorema 6.14. *Siano A, B sottoinsiemi finiti non vuoti di $\mathbb{Z}$; allora*

(i) $|A+B| \geq |A|+|B|-1$.

(ii) $|A+B| = |A|+|B|-1$ *se e solo se A e B sono progressioni aritmetiche con la stessa ragione.*

Dimostrazione. (i) Siano $a = \max A$ e $b = \min B$. Allora

$$(a+B) \cup (A+b) \subseteq A+B.$$

Siano $y \in B$ e $x \in A$ tali che $a+y = x+b$; allora $0 \leq y-b = x-a \leq 0$, e quindi $y = b, x = a$. Ciò prova che $(a+B) \cap (A+b) = \{(a,b)\}$; dunque

$$|A+B| \geq |(a+B) \cup (A+b)| = |a+B| + |A+b| - 1 = |A|+|B|-1.$$

(ii) Abbiamo già osservato che se A e B sono progressioni aritmetiche con la stessa ragione allora vale l'uguaglianza $|A+B| = |A|+|B|-1$.

Per dimostrare il viceversa, possiamo certamente assumere che sia A che B contengano almeno due elementi (il caso in cui $|A| = 1$ oppure $|B| = 1$ è banale). Sia $|A| = m > 1$, $|B| = n > 1$.
Siano $a_1 < a_2 < \ldots < a_m$ e $b_1 < b_2 < \ldots < b_n$, rispettivamente, gli elementi di A e quelli di B, e supponiamo $|A + B| = m + n - 1$. Allora, come nella dimostrazione del punto (i),

$$m + n - 1 = |A + B| \geq |(a + B) \cup (A + b)| = m + n - 1,$$

quindi

$$A + B = (A + b_1) \cup (a_m + B).$$

Inoltre l'insieme somma $A + B$ risulta ordinato nel modo seguente:

$$a_1 + b_1 < a_2 + b_1 < \ldots < a_m + b_1 < a_m + b_2 < \ldots < a_m + b_{n-1} < a_m + b_n. \tag{6.8}$$

Consideriamo l'insieme $A + b_2$; è formato da m elementi ed è contenuto nell'intervallo di numeri interi $[a_1 + b_1, a_m + b_2] \cap (A + B) = \{a_1 + b_1, a_2 + b_1, \ldots, a_m + b_2\}$, il quale pure contiene m elements; quindi, confrontando con la sequenza (6.8) si ricava

$$a_i + b_2 = a_{i+1} + b_1 \tag{6.9}$$

per ogni $i = 1, \cdots, m - 1$. Facendo simili considerazioni per l'insieme $a_{m-1} + B$, e confrontando con (6.8) si ricava inoltre

$$a_m + b_i = a_{m-1} + b_{j+1} \tag{6.10}$$

per ogni $j = 1, \cdots, n - 1$. Infine, mettendo assieme le uguaglianze (6.9) e le (6.10), si ottiene

$$a_{i+1} - a_i = b_2 - b_1 = a_m - a_{m-1} = b_{j+1} - b_j,$$

per ogni $i = 1, \cdots, m-1$ and $j = 1, \cdots, n-1$. Ciò mostra che sia A che B sono progressioni aritmetiche di ragione $d = a_2 - a_1 = b_2 - b_1$, e conclude la dimostrazione. □

Bibliografia

[1] J. L. Ramírez Alfonsín, The Diophantine Frobenius Problem. Oxford University Press, 2005.

[2] T. Andreescu, D. Andrica, Number Theory: structures, examples and problems. Birkhauser, 2009.

[3] J. Hofbauer, American Math. Monthly 109 (2002).

[4] Y. Matsuoka, American Math. Monthly 71 (1964).

[5] M. Nathanson, A short proof of Cauchy's polygonal number theorem. Proceedings American Math. Soc.,99 (1997).

[6] J. Stevens, Olympiad Number Theory through challenging problems. Disponibile on-line nel sito dell'autore: https://numbertheoryguy.com/publications/olympiad-number-theory-book/

[7] Problems in elementary number theory.

[8] artofproblemsolving.com/community/c13_contests