12 maggio 2020 - lezione unica

Avvertenza importante!

Questo pdf contiene alcuni esercizi, che costituiscono formalmente un’ora di lezione “virtuale” di martedì 12 maggio 2020. La motivazione per questa ora è principalmente burocratica, perché in un insegnamento di 9 crediti mi sembra corretto che vengano svolte 90 ore di lezione, e questa è appunto la novantesima.

Al di là della motivazione burocratica, non è comunque male che gli studenti abbiano la possibilità di vedere qualche esercizio (facile) in più, del tipo che potrebbe essere proposto in una prova scritta preliminare (anche se al momento non è ancora chiaro il modo in cui questa prova scritta preliminare potrà tenersi nei prossimi appelli!).

Cominciamo con un problema di “calcolo combinatorio”. Vogliamo contare quante sono le sequenze ordinate di otto caratteri alfanumerici, dei quali esattamente quattro (ma non necessariamente i primi quattro!) sono caratteri numerici (anche ripetuti, scelti fra le dieci cifre usuali $0, 1, \ldots, 9$, e disposti in ordine non decrescente) e i rimanenti sono caratteri alfabetici (tutti diversi fra loro, scelti tra i 21 dell’alfabeto italiano, disposti in qualsiasi ordine).

Conviene applicare il “principio di moltiplicazione”: calcoliamo in quanti modi possono essere scelti i posti occupati dai caratteri numerici, in quanti modi possono essere scelti i caratteri numerici, in quanti modi possono essere scelti i caratteri alfabetici, e facciamo il prodotto.

I posti occupati dai quattro caratteri numerici possono essere scelti in

$$\binom{8}{4} = \tfrac{8\cdot 7\cdot 6\cdot 5}{4\cdot 3\cdot 2} = 70$$

modi diversi; i caratteri numerici possono essere scelti in

$$\binom{10+4-1}{4} = \; = \tfrac{13\cdot 12\cdot 11\cdot 10}{4\cdot 3\cdot 2} = 715$$

modi diversi; infine, i caratteri alfabetici (ancora per il principio di moltiplicazione) possono essere scelti in

$$21 \cdot 20 \cdot 19 \cdot 18$$

modi diversi.

In tutto, dunque, si possono scrivere

$$70 \cdot 715 \cdot 21 \cdot 20 \cdot 19 \cdot 18 = 7\,189\,182\,000$$

diverse sequenze ordinate che rispettano le condizioni del problema.

Vediamo ora un facilissimo problema sulle permutazioni. Siano α, β le permutazioni sull'insieme {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14} così definite:

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 6 & 7 & 2 & 5 & 9 & 12 & 8 & 4 & 3 & 14 & 1 & 11 & 10 & 13 \end{pmatrix}$$

$$\beta := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 8 & 10 & 6 & 7 & 3 & 2 & 4 & 9 & 5 & 1 & 12 & 11 & 14 & 13 \end{pmatrix}$$

e sia σ la permutazione ottenuta applicando prima α e poi β.

Vogliamo scrivere σ come prodotto di cicli disgiunti e poi stabilire se σ è una permutazione pari oppure una permutazione dispari.

Si ha

$$\sigma = (1\ 2\ 4\ 3\ 10\ 13)(6\ 11\ 8\ 7\ 9) = (1\ 2)(1\ 4)(1\ 3)(1\ 10)(1\ 13)(6\ 11)(6\ 8)(6\ 7)(6\ 9)\,.$$

Poiché σ si può scrivere come prodotto di 9 trasposizioni, e 9 è un numero dispari, σ è una permutazione dispari.

Adesso consideriamo tre equazioni di primo grado nell'anello $\mathbb{Z}_{4\,697}$ delle classi di resto modulo $4\,697$ per chiederci quante soluzioni ha ciascuna di esse. Come al solito, per ogni $z \in \mathbb{Z}$ indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{4\,697}$ a cui z appartiene.

Le equazioni da considerare sono:

$$[793]\,x = [122]\,; \qquad [121]\,x = [793]\,; \qquad [427]\,x = [0]\,.$$

Indichiamo con δ_1 il massimo comun divisore fra $4\,697$ e 793. L'equazione

$$[793]\,x = [122]$$

ha soluzione in $\mathbb{Z}_{4\,697}$ se e soltanto se δ_1 divide 122, e in tal caso ha esattamente δ_1 soluzioni. Calcoliamo δ_1 utilizzando l'algoritmo di Euclide:

$4\,697 = 793 \cdot 5 + 732\,;$
$793 = 732 \cdot 1 + 61\,;$
$732 = 61 \cdot 12 + 0\,.$

Dunque $\delta_1 = 61\,.$

Poiché 61 divide 122 (infatti $122 = 61 \cdot 2$), l’equazione $[793]\,x = [122]$ ha esattamente 61 soluzioni in $\mathbb{Z}_{4\,697}$.

Indichiamo ora con δ_2 il massimo comun divisore fra $4\,697$ e 121 . L’equazione

$$[121]\,x = [793]$$

ha soluzione in $\mathbb{Z}_{4\,697}$ se e soltanto se δ_2 divide 793, e in tal caso ha esattamente δ_1 soluzioni. Calcoliamo δ_2 utilizzando l’algoritmo di Euclide:

$4\,697 = 121 \cdot 38 + 99\,;$
$121 = 99 \cdot 1 + 22\,;$
$99 = 22 \cdot 4 + 11\,;$
$22 = 11 \cdot 2 + 0\,.$

Dunque $\delta_2 = 11$.

Poiché 11 non divide 793 (infatti $793 = 11 \cdot 72 + 1$), l’equazione $[793]\,x = [122]$ non ha soluzioni in $\mathbb{Z}_{4\,697}$.

Infine, è chiaro che l’equazione

$$[427]\,x = [0]$$

ha almeno una soluzione in $\mathbb{Z}_{4\,697}$ (perché $[427] \cdot [0] = [0]$); ma noi vogliamo sapere quante soluzioni ha, quindi dobbiamo comunque calcolare il massimo comun divisore fra $4\,697$ e 427. Utilizziamo ancora una volta l’algoritmo di Euclide:

$4\,697 = 427 \cdot 11 + 0\,.$

Dunque il massimo comun divisore fra $4\,697$ e 793 è 427 e l’equazione $[427]\,x = [0]$ ha esattamente 427 soluzioni in $\mathbb{Z}_{4\,697}$.

Adesso andiamo a lavorare nell’anello $\mathbb{Z}_{1\,813}$ delle classi di resto modulo $1\,813$. Come sopra, per ogni $z \in \mathbb{Z}$ indichiamo con $[z]$ l’elemento di $\mathbb{Z}_{1\,813}$ a cui z appartiene.

Per ciascuna delle seguenti due equazioni esponenziali nell’incognita x ci chiediamo quante soluzioni ha in $\mathbb{N}\backslash\{0\}$, e se ne ha ne vogliamo trovare almeno una:

$$[245]^x = [1]\,; \qquad\qquad [605]^x = [1]\,.$$

Dobbiamo considerare separatamente le due equazioni.

L’equazione

$$[245]^x = [1]$$

ha soluzione in $\mathbb{N}\backslash\{0\}$ se e soltanto se il massimo comun divisore fra $1\,813$ e 245 è 1, e in tal caso ha infinite soluzioni.. Calcoliamo il massimo comun divisore fra $1\,813$ e 245 utilizzando l’algoritmo di Euclide:

$1\,813 = 245 \cdot 7 + 98\,;$
$245 = 98 \cdot 2 + 49\,;$
$98 = 49 \cdot 2 + 0\,.$

Dunque il massimo comun divisore fra $1\,813$ e 245 è $49 \neq 1$, e l’equazione considerata non ha soluzioni in $\mathbb{N}\backslash\{0\}$.

Analogamente, l’equazione

$$[605]^x = [1]$$

ha soluzione in $\mathbb{N}\backslash\{0\}$ se e soltanto se il massimo comun divisore fra $1\,813$ e 605 è 1, e in tal caso ha infinite soluzioni.. Calcoliamo il massimo comun divisore fra $1\,813$ e 605 utilizzando l’algoritmo di Euclide:

$1\,813 = 605 \cdot 2 + 603\,;$
$605 = 603 \cdot 1 + 2\,;$
$603 = 2 \cdot 301 + 1\,;$
$2 = 1 \cdot 2 + 0\,.$

Dunque il massimo comun divisore fra $1\,813$ e 605 è 1, e l’equazione considerata ha infinite soluzioni in $\mathbb{N}\backslash\{0\}$. Una di esse è $\varphi(1\,813)$; per calcolare questo numero dobbiamo esprimere $1\,813$ come prodotto di numeri primi.

Dai calcoli effettuati in precedenza, sappiamo che $1\,813$ è multiplo di 49 $(=7^2)$; in effetti,

$$1\,813 = 49 \cdot 37 = 7^2 \cdot 37$$

con 37 numero primo; dunque

$$\varphi(1\,813) = \varphi(7^2 \cdot 37) = \varphi(7^2) \cdot \varphi(37) = 7 \cdot 6 \cdot 36 = 1\,512\,.$$

Pertanto, $1\,512$ è una soluzione non nulla dell’equazione $[605]^x = [1]$.

Infine, un problema sul cambiamento di base nel sistema di notazione dei numeri naturali (un *must* per chi vuole lavorare in informatica!).

Sia n il numero che in base *tredici* si scrive $184\text{A}94$, cioè

$$n := 184\text{A}94_{tredici},$$

e scriviamo invece n in base *quindici*.

Dobbiamo prima trovare l’espressione di n in base *dieci*. Si ha

$$n = 4 + 9 \cdot 13 + 10 \cdot 13^2 + 4 \cdot 13^3 + 8 \cdot 13^4 + 1 \cdot 13^5 =$$

$$= 4 + 9 \cdot 13 + 10 \cdot 169 + 4 \cdot 2\,197 + 8 \cdot 28\,561 + 1 \cdot 371\,293 =$$

$$= 4 + 117 + 1\,690 + 8\,788 + 228\,488 + 371\,293 = 610\,380_{dieci}\,.$$

Per scrivere n in base *quindici*, effettuiamo divisioni successive per *quindici* come segue (la notazione è in base *dieci*):

$610\,380 = 40\,692 \cdot 15 + 0\,;$

$40\,692 = 2\,712 \cdot 15 + 12\,;$

$2\,712 = 180 \cdot 15 + 12\,;$

$180 = 12 \cdot 15 + 0\,;$

$12 = 0 \cdot 15 + 12$

e prendiamo (in ordine inverso) le "cifre" che rappresentano i resti ottenuti. Si ottiene dunque che

$$n = \mathrm{C0CC0}_{\textit{quindici}}\,.$$

E adesso, buon lavoro a tutti! Vi ricordo che, per qualsiasi dubbio e/o richiesta di chiarimenti sul programma svolto, siete invitati a contattarmi per email

marco.barlotti@unifi.it.