10. – Soluzione degli esercizi su: ***equazioni esponenziali in $\mathbb{Z}_n$***.

Esercizio 10.1

Calcolare il resto della divisione per 77 di $2^{100\,000}$.

Soluzione – Poiché MCD$(2, 77) = 1$, si può applicare il teorema di Euler-Fermat, per ottenere che $2^{\varphi(77)} \equiv 1 \pmod{77}$.

È $77 = 7 \cdot 11$, con 7 e 11 numeri primi; pertanto $\varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$. Sappiamo così che $2^{60} \equiv 1 \pmod{77}$.

Poiché $100\,000 = 60 \cdot 1\,666 + 40$, si ha che

$$2^{100\,000} = 2^{60 \cdot 1\,666 + 40} = (2^{60})^{1\,666} \cdot 2^{40} \equiv 1 \cdot 2^{40} \pmod{77}.$$

Siamo dunque ricondotti a calcolare il resto della divisione di 2^{40} per 77, cosa che si può fare ad esempio osservando che

$$2^{40} = (2^8)^5$$

e che

$$2^8 = (2^4)^2 = 16 \cdot 16 = 256 \equiv 25 \pmod{77}.$$

Dunque

$$2^{40} \equiv 25^5 = 625 \cdot 625 \cdot 25 \equiv 9 \cdot 9 \cdot 25 = 2025 \equiv 23 \pmod{77}$$

poiché $625 = 77 \cdot 8 + 9$ e $2025 = 77 \cdot 26 + 23$.

Pertanto, il resto della divisione per 77 di $2^{100\,000}$ è 23.

Esercizio 10.2

Risolvere uno dei seguenti problemi:

(i) si calcoli il resto della divisione di $101\,420^{222}$ per 363;
(ii) si calcoli il resto della divisione di $912\,141^{444}$ per 363;
(iii) si calcoli il resto della divisione di $2\,843\,018^{222}$ per 363;
(iv) si calcoli il resto della divisione di $13\,765\,543^{444}$ per 363.

Soluzione – Per affrontare questo tipo di problemi conviene utilizzare il teorema di Euler-Fermat, in base al quale $a^{\varphi(n)} \equiv 1 \pmod{n}$ quando MCD$(a, n) = 1$.

Poiché $363 = 3 \cdot 11^2$, l'ipotesi del teorema di Euler-Fermat per $n := 363$ è verificata solo per $a := 2\,843\,018$ (infatti dai noti criteri di divisibilità si ricava immediatamente che $101\,420$ e $13\,765\,543$ sono divisibili per 11 e che $912\,141$ è divisibile per 3).

Poiché

$$\varphi(363) = \varphi(3 \cdot 11^2) = \varphi(3) \cdot \varphi(11^2) = 2 \cdot 11 \cdot 10 = 220$$

si ha

$$2\,843\,018^{222} = 2\,843\,018^{220+2} = 2\,843\,018^{220} \cdot 2\,843\,018^2 =$$
$$= 2\,843\,018^{\varphi(363)} \cdot 2\,843\,018^2 \equiv 1 \cdot 2\,843\,018^2 \pmod{363}.$$

D'altro lato, $2\,843\,018 = 7\,832 \cdot 363 + 2$ ossia $2\,843\,018 \equiv 2 \pmod{363}$ cosicché

$$2\,843\,018^2 \equiv 2^2 \pmod{363}$$

e quindi il resto della divisione di $2\,843\,018^{222}$ per 363 è 4.

Esercizio 10.3

Sia $\mathbb{Z}_{685}$ l'anello delle classi di resto modulo 685. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{685}$ a cui z appartiene. Si trovi una soluzione in $\mathbb{Z}^+$ per una delle seguenti equazioni esponenziali in $\mathbb{Z}_{685}$ (a scelta del candidato):

$$[137]^x = [3]; \qquad [375]^x = [7]; \qquad [521]^x = [1].$$

Soluzione – Conviene cercare di utilizzare il teorema di Euler – Fermat, secondo il quale

$$[a]^{\varphi(n)} \equiv 1 \pmod{n}$$

se MCD$(a, n) = 1$.

Quest'ultima condizione, fra i casi proposti, è verificata soltanto per $a := 521$ e $n := 685$. In questo caso, poiché $685 = 5 \cdot 137$ con 5 e 137 numeri primi, si ha

$$\varphi(685) = \varphi(5) \cdot \varphi(137) = 4 \cdot 136 = 544$$

cosicché $x := 544$ è la soluzione cercata.

Esercizio 10.4

Sia $\mathbb{Z}_{3033}$ l'anello delle classi di resto modulo $3\,033$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{3033}$ a cui z appartiene. Si trovino almeno due soluzioni in $\mathbb{Z}^+$ per una delle seguenti equazioni esponenziali in $\mathbb{Z}_{3033}$ (a scelta del candidato):

$$[317]^x = [317]; \qquad [337]^x = [337]; \qquad [357]^x = [357].$$

Soluzione – Tutte le equazioni date hanno l'ovvia soluzione $x := 1$. Per trovare un'altra soluzione, è opportuno osservare che in $\mathbb{Z}_{3033}$ sono equivalenti due equazioni ottenute una dall'altra moltiplicando ambo i membri per l'inverso di $[317]$, dato che (come è immediato verificare) MCD$(317, 3\,033) = 1$. In particolare, la prima equazione diventa

$$[317]^{x-1} = [1].$$

A questo punto, ricordando ancora che MCD$(317, 3\,033) = 1$, si può utilizzare il teorema di Euler – Fermat, che ci garantisce che in $\mathbb{Z}_{3033}$

$$[317]^{\varphi(3\,033)} = [1].$$

Dunque un'altra soluzione x è data dalla relazione $x - 1 = \varphi(3\,033)$ ossia

$$x = \varphi(3\,033) + 1 = \varphi(3^2 \cdot 337) + 1 = \varphi(3^2) \cdot \varphi(337) + 1 = 6 \cdot 336 + 1 = 2\,017.$$

Esercizio 10.5

La ditta ACME ha brevettato e prodotto un nuovo utensile casalingo, il *tuttotrone*, che purtroppo non ha avuto il successo di vendita sperato. Per questo motivo la ditta ACME ha ritirato dal commercio tutti i pezzi rimasti invenduti, esattamente 55^{170}, accantonandoli in attesa di una più favorevole situazione di mercato: li ha sistemati in grandi contenitori, ciascuno dei quali contiene esattamente 147 pezzi.

Dopo aver completamente riempito molti contenitori, sono avanzati alcuni tuttotroni (insufficienti a riempire un ulteriore contenitore) che sono stati distribuiti gratuitamente ai dipendenti della ditta.

Quanti esemplari di tuttotrone sono stati così distribuiti gratuitamente?

Soluzione – Si deve calcolare il residuo modulo 147 di 55^{170}. Calcoliamo il massimo comun divisore fra 147 e 55:

$$147 = 55 \cdot 2 + 37\,; \quad 55 = 37 \cdot 1 + 18\,; \quad 37 = 18 \cdot 2 + 1\,; \quad 18 = 1 \cdot 18 + 0\,.$$

Poiché MCD $(147, 55) = 1$, possiamo applicare il teorema di Euler-Fermat, in base al quale $55^{\varphi(147)} \equiv 1 \pmod{147}$. Si ha $\varphi(147) = \varphi(3 \cdot 7^2) = \ = \varphi(3) \cdot \varphi(7^2) = 2 \cdot 42 = 84$. Dunque

$$55^{170} = 55^{2 \cdot 84 + 2} = (55^{84})^2 \cdot 55^2 \equiv 1^2 \cdot 55^2 = 3\,025 \pmod{147}$$

e poiché $3\,025 = 147 \cdot 20 + 85$ si conclude che $55^{170} \equiv 3\,025 \equiv 85 \pmod{147}$. Dunque gli esemplari di tuttotrone distribuiti gratuitamente sono 85.

Esercizio 10.6

Calcolare il resto della divisione per 77 di $4^{50\,000}$.

Soluzione – Poiché MCD$(4, 77) = 1$, si può applicare il teorema di Euler-Fermat, per ottenere che $4^{\varphi(77)} \equiv 1 \pmod{77}$.

È $77 = 7 \cdot 11$, con 7 e 11 numeri primi; pertanto $\varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$. Sappiamo così che $4^{60} \equiv 1 \pmod{77}$.

Poiché $50\,000 = 60 \cdot 833 + 20$, si ha che

$$4^{50\,000} = 4^{60 \cdot 833 + 20} = (4^{60})^{833} \cdot 4^{20} \equiv 1 \cdot 4^{20} \pmod{77}\,.$$

Siamo dunque ricondotti a calcolare il resto della divisione di 4^{20} per 77, cosa che si può fare ad esempio osservando che

$$4^{20} = (4^4)^5$$

e che

$$4^4 = 256 \equiv 25 \pmod{77}\,.$$

Dunque

$$4^{20} \equiv 25^5 = 625 \cdot 625 \cdot 25 \equiv 9 \cdot 9 \cdot 25 = 2025 \equiv 23 \pmod{77}$$

poiché $625 = 77 \cdot 8 + 9$ e $2025 = 77 \cdot 26 + 23$.

Pertanto, il resto della divisione per 77 di $4^{50\,000}$ è 23.

Esercizio 10.7

Trovare le ultime due cifre della scrittura in base 10 di $93^{28\,562}$.

Soluzione – Il numero formato dalla penultima e dall'ultima cifra (prese in quest'ordine) della scrittura in base 10 di un numero n è il resto della divisione per 100 di n.

Dato che MCD$(93, 100) = 1$, per trovare il resto della divisione per 100 di $93^{28\,562}$ possiamo utilizzare il teorema di Euler – Fermat: se φ è la funzione di Euler, $93^{\varphi(100)} \equiv 1 \pmod{100}$.

Poiché φ è moltiplicativa, $\varphi(100) = \varphi(25)\varphi(4) = (5 \cdot 4) \cdot (2 \cdot 1) = 40$; inoltre, $28\,562 = 40 \cdot 714 + 2$, cosicché

$$93^{28\,562} = 93^{40 \cdot 714 + 2} = 93^{40 \cdot 714} \cdot 93^2 = (93^{40})^{714} \cdot 93^2 \equiv 1^{714} \cdot 93^2 \equiv 93^2 \pmod{100}.$$

Da un calcolo diretto si ricava infine che

$$93^2 = 8\,649 \equiv 49 \pmod{100}$$

e dunque le due cifre cercate sono (nell'ordine) 4 e 9.

Esercizio 10.8

Sia n il numero ottenuto elevendo *sette* alla potenza *novantaseimilacinquecentosessantasei*.
Si dica, motivando la risposta, quali sono le ultime due cifre della scrittura di n in base *tredici*.

Soluzione – Il numero formato in base *tredici* dalle ultime due cifre della scrittura di n in base *tredici* è il resto della divisione di n per (da qui in avanti i numeri si intendono scritti in base *dieci*) 13^2. Poiché MCD$(7, 13^2) = 1$, per trovare tale resto possiamo utilizzare il teorema di Euler-Fermat, in base al quale

$$7^{\varphi(13^2)} \equiv 1 \pmod{13^2}.$$

Poiché $\varphi(13^2) = 13 \cdot 12 = 156$ e $96\,566 = 156 \cdot 619 + 2$, si ha

$$7^{96\,566} = 7^{156 \cdot 619 + 2} = (7^{156})^{619} \cdot 7^2 \equiv 1^{619} \cdot 7^2 = 49 \pmod{13^2}$$

e poiché 49 in base 13 si scrive 3A, le ultime due cifre cercate sono appunto 3 e A.

Esercizio 10.9

Risolvere uno dei seguenti problemi:

(i) si calcoli il resto della divisione di $84\,938^{255}$ per 147;
(ii) si calcoli il resto della divisione di $912\,141^{255}$ per 147;
(iii) si calcoli il resto della divisione di $1\,151\,306^{170}$ per 147;
(iv) si calcoli il resto della divisione di $77\,777\,777^{170}$ per 147.

Soluzione – Per affrontare questo tipo di problemi conviene utilizzare il teorema di Euler-Fermat, in base al quale $a^{\varphi(n)} \equiv 1 \pmod{n}$ quando MCD$(a, n) = 1$.

Poiché $147 = 3 \cdot 7^2$, l'ipotesi del teorema di Euler-Fermat per $n := 147$ è verificata solo per $a := 1\,151\,306$ (infatti è facile verificare che $84\,938$ e $77\,777\,777$ sono divisibili per 7 e che $912\,141$ è divisibile per 3).

Poiché

$$\varphi(147) = \varphi(3 \cdot 7^2) = \varphi(3) \cdot \varphi(7^2) = 2 \cdot 7 \cdot 6 = 84$$

si ha

$$1\,151\,306^{170} = 1\,151\,306^{2 \cdot 84 + 2} = \left(1\,151\,306^{84}\right)^2 \cdot 1\,151\,306^2 =$$

$$= \left(1\,151\,306^{\varphi(363)}\right)^2 \cdot 1\,151\,306^2 \equiv 1^2 \cdot 1\,151\,306^2 \pmod{147}.$$

D'altro lato, $1\,151\,306 = 7\,832 \cdot 147 + 2$ ossia $1\,151\,306 \equiv 2 \pmod{147}$ cosicché

$$1\,151\,306^2 \equiv 2^2 \pmod{147}$$

e quindi il resto della divisione di $1\,151\,306^{170}$ per 147 è 4.

Esercizio 10.10

Sia $\mathbb{Z}_{695}$ l'anello delle classi di resto modulo 695. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{695}$ a cui z appartiene. Si trovi una soluzione in $\mathbb{Z}^+$ per una delle seguenti equazioni esponenziali in $\mathbb{Z}_{695}$ (a scelta del candidato):

$$[137]^x = [3]; \qquad [375]^x = [7]; \qquad [521]^x = [1].$$

Soluzione – Conviene cercare di utilizzare il teorema di Euler – Fermat, secondo il quale

$$[a]^{\varphi(n)} \equiv 1 \pmod{n}$$

se MCD$(a, n) = 1$.

Quest'ultima condizione, fra i casi proposti, è certamente verificata per $a := 521$ e $n := 695$. In questo caso, poiché $695 = 5 \cdot 139$ con 5 e 139 numeri primi, si ha

$$\varphi(695) = \varphi(5) \cdot \varphi(139) = 4 \cdot 138 = 551$$

cosicché $x := 552$ è la soluzione cercata.

Esercizio 10.11

La ditta ACME ha brevettato e prodotto un nuovo utensile casalingo, il *politrone*, che purtroppo non ha avuto il successo di vendita sperato. Per questo motivo la ditta ACME ha ritirato dal commercio tutti i pezzi rimasti invenduti, esattamente 33^{170}, accantonandoli in attesa di una più favorevole situazione di mercato: li ha sistemati in grandi contenitori, ciascuno dei quali contiene esattamente 245 pezzi.

Dopo aver completamente riempito molti contenitori, sono avanzati alcuni politroni (insufficienti a riempire un ulteriore contenitore) che sono stati distribuiti gratuitamente ai dipendenti della ditta.

Quanti esemplari di politrone sono stati così distribuiti gratuitamente?

Soluzione – Si deve calcolare il residuo modulo 245 di 33^{170}. Calcoliamo il massimo comun divisore fra 245 e 33:

$$245 = 33 \cdot 7 + 14\,;$$

$$33 = 14 \cdot 2 + 5\,;$$

$$14 = 5 \cdot 2 + 4\,;$$

$$5 = 4 \cdot 1 + 1\,;$$

$$4 = 1 \cdot 4 + 0\,.$$

Poiché MCD $(245,\, 33) = 1$, possiamo applicare il teorema di Euler-Fermat, in base al quale $33^{\varphi(245)} \equiv 1 \pmod{245}$. Si ha $\varphi(245) = \varphi(5 \cdot 7^2) = \ = \varphi(5) \cdot \varphi(7^2) = 4 \cdot 42 = 168$. Dunque

$$33^{170} = 33^{168+2} = 33^{168} \cdot 33^2 \equiv 1 \cdot 33^2 = 1\,089 \pmod{245}$$

e poiché $1\,089 = 245 \cdot 4 + 105$ si conclude che $33^{170} \equiv 1\,089 \equiv 105 \pmod{245}$. Dunque gli esemplari di politrone distribuiti gratuitamente sono 105.

Esercizio 10.12

Sia $\mathbb{Z}_{2853}$ l'anello delle classi di resto modulo $2\,853$. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{2853}$ a cui z appartiene. Si trovino almeno due soluzioni in $\mathbb{Z}^+$ per una delle seguenti equazioni esponenziali in $\mathbb{Z}_{2853}$ (a scelta del candidato):

$$[317]^x = [317]\,; \qquad [337]^x = [337]\,; \qquad [357]^x = [357]\,.$$

Soluzione – Tutte le equazioni date hanno l'ovvia soluzione $x := 1$. Per trovare un'altra soluzione, è opportuno osservare che in $\mathbb{Z}_{2853}$ sono equivalenti due equazioni ottenute una dall'altra moltiplicando ambo i membri per l'inverso di $[337]$, dato che (come è immediato verificare) MCD$(337, 2\,853) = 1$. In particolare, la seconda equazione diventa

$$[337]^{x-1} = [1]\,.$$

A questo punto, ricordando ancora che MCD$(337, 2\,853) = 1$, si può utilizzare il teorema di Euler – Fermat, che ci garantisce che in $\mathbb{Z}_{2853}$

$$[337]^{\varphi(2\,853)} = [1]\,.$$

Dunque un'altra soluzione x è data dalla relazione $x - 1 = \varphi(2\,853)$ ossia

$$x = \varphi(2\,853) + 1 = \varphi(3^2 \cdot 317) + 1 = \varphi(3^2) \cdot \varphi(317) + 1 = 6 \cdot 316 + 1 = 1\,897\,.$$

Esercizio 10.13

Trovare le ultime due cifre della scrittura in base 10 di 13^{682}.

Soluzione – Il numero formato da tali cifre, prese nell'ordine, è il resto della divisione per 100 di 13^{682}, cioè il rappresentante "canonico" (quello compreso fra 0 e 99) della classe di resto modulo 100 cui appartiene 13^{682}. Poiché $\text{MCD}(13, 100) = 1$, conviene utilizzare il teorema di Euler – Fermat secondo il quale $[a]^{\varphi(n)} \equiv 1 \pmod{n}$ se $\text{MCD}(a, n) = 1$.

Si ha $\varphi(100) = \varphi(4) \cdot \varphi(25) = 2 \cdot 20 = 40$, e $682 = 40 \cdot 17 + 2$. Dunque,

$$13^{682} = 13^{40 \cdot 17 + 2} = (13^{40})^{17} \cdot 13^2 \equiv 1^{17} \cdot 69 \equiv 69 \pmod{100}.$$

Pertanto, le ultime due cifre della scrittura in base 10 di 13^{682} sono, nell'ordine, 6 e 9.

Esercizio 10.14

Trovare le ultime due cifre della scrittura in base 10 di $97^{29\,482}$.

Soluzione – Il numero formato dalla penultima e dall'ultima cifra (prese in quest'ordine) della scrittura in base 10 di un numero n è il resto della divisione per 100 di n.

Dato che $\text{MCD}(97, 100) = 1$, per trovare il resto della divisione per 100 di $97^{29\,482}$ possiamo utilizzare il teorema di Euler – Fermat: se φ è la funzione di Euler, $97^{\varphi(100)} \equiv 1 \pmod{100}$.

Poiché φ è moltiplicativa, $\varphi(100) = \varphi(25)\varphi(4) = (5 \cdot 4) \cdot (2 \cdot 1) = 40$; inoltre, $29\,482 = 40 \cdot 737 + 2$, cosicché

$$97^{29\,482} = 97^{40 \cdot 737 + 2} = 97^{40 \cdot 737} \cdot 97^2 = (97^{40})^{737} \cdot 97^2 \equiv 1^{737} \cdot 97^2 \equiv 97^2 \pmod{100}.$$

Da un calcolo diretto si ricava infine che

$$97^2 = 9\,409 \equiv 9 \pmod{100}$$

e dunque le due cifre cercate sono (nell'ordine) 0 e 9.

Esercizio 10.15

Sia

$$n := 8^{98\,438}.$$

Si dica, motivando la risposta, quali sono le ultime due cifre della scrittura di n in base 13.

Soluzione – Il numero formato in base 13 dalle ultime due cifre della scrittura di n in base 13 è il resto della divisione di n per 13^2. Poiché $\text{MCD}(8, 13^2) = 1$, per trovare tale resto possiamo utilizzare il teorema di Euler-Fermat, in base al quale $8^{\varphi(13^2)} \equiv 1 \pmod{13^2}$.

Poiché $\varphi(13^2) = 13 \cdot 12 = 156$ e $98\,438 = 156 \cdot 631 + 2$, si ha

$$8^{98\,438} = 8^{156 \cdot 631 + 2} = (8^{156})^{631} \cdot 8^2 \equiv 1^{631} \cdot 8^2 = 64 \pmod{13^2}$$

e poiché 64 in base 13 si scrive 4C, le ultime due cifre cercate sono appunto 4 e C.

Esercizio 10.16

Trovare le ultime due cifre della scrittura in base 10 di 37^{721} .

Soluzione – Si cerca il rappresentante "canonico" (cioè compreso fra 0 e 99) della classe di resto modulo 100 cui appartiene 37^{721}. Poiché $\text{MCD}(37, 100) = 1$, conviene utilizzare il teorema di Euler – Fermat secondo il quale $[a]^{\varphi(n)} \equiv 1 \pmod{n}$ se

$$\text{MCD}(a, n) = 1 .$$

Si ha $\varphi(100) = \varphi(4) \cdot \varphi(25) = 2 \cdot 20 = 40$, e $721 = 40 \cdot 18 + 1$. Dunque,

$$37^{721} = 37^{40 \cdot 18 + 1} = (37^{40})^{18} \cdot 37^1 \equiv 1^{18} \cdot 37 \pmod{100}.$$

Pertanto, le ultime due cifre della scrittura in base 10 di 37^{721} sono, nell'ordine, 3 e 7 .

Esercizio 10.17

Sia $\mathbb{Z}_{831}$ l'anello delle classi di resto modulo 831 . Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{831}$ a cui z appartiene.
Per ciascuna delle seguenti equazioni esponenziali in $\mathbb{Z}_{831}$ nella incognita x si dica, motivando la risposta, se ha soluzioni in $\mathbb{Z}^+$ e, nei casi in cui la risposta è affermativa, si precisi quante sono le soluzioni e se ne trovi almeno una:

$$[277]^x = [1] ; \qquad [278]^x = [0] ; \qquad [278]^x = [1] .$$

Soluzione – Calcoliamo con l'algoritmo di Euclide il massimo comun divisore fra 831 e 277 e poi il massimo comun divisore fra 831 e 278 .

$$831 = 277 \cdot 3 ; \quad \text{dunque } \text{MCD}(831, 277) = 277 .$$

$831 = 278 \cdot 2 + 275 ; \quad 278 = 275 \cdot 1 + 3 ; \quad 275 = 3 \cdot 91 + 2 ; \quad 3 = 2 \cdot 1 + 1 ; \quad 2 = 1 \cdot 2 ;$ dunque $\text{MCD}(831, 278) = 1$.

Poiché $\text{MCD}(831, 277) \neq 1$, l'equazione esponenziale $[277]^x = [1]$ non ha soluzioni in $\mathbb{Z}^+$ (in $\mathbb{Z}$ ha la soluzione "banale" $x := 0$). Poiché $\text{MCD}(831, 278) = 1$, l'equazione esponenziale $[278]^x = [0]$ non ha soluzioni in $\mathbb{Z}^+$ (se ne avesse, $[278]$ sarebbe $[0]$ o un divisore dello zero e quindi dovrebbe essere $\text{MCD}(831, 277) \neq 1$).

Infine, poiché $\text{MCD}(831, 278) = 1$ possiamo applicare il teorema di Euler – Fermat, in base al quale l'equazione esponenziale $[278]^x = [1]$ ha infinite soluzioni, fra le quali tutti i multipli di $\varphi(831) = \varphi(277) \cdot \varphi(3) = 276 \cdot 2 = 552$.

Esercizio 10.18

Sia $n := 11^{297}$. Si determini l'ultima cifra a destra della rappresentazione di n in base sedici.

Soluzione – La cifra cercata è quella che in base sedici rappresenta il resto della divisione per sedici di 11^{297}.

Poiché $\text{MCD}(11, 16) = 1$, per il teorema di Euler-Fermat è $11^{\varphi(16)} \equiv 1 \pmod{16}$. Si ha $\varphi(16) = \varphi(2^4) = 2^3 = 8$, quindi $11^8 \equiv 1 \pmod{16}$. D'altro lato è $297 = 8 \cdot 37 + 1$, quindi

$$11^{297} = 11^{8 \cdot 37 + 1} = (11^8)^{37} \cdot 11 \equiv 1 \cdot 11 = 11 \pmod{16}.$$

Pertanto il resto della divisione per sedici di 11^{297} è 11, e la cifra cercata è B.

Esercizio 10.19

Calcolare il resto della divisione per 77 di $3^{50\,000}$.

Soluzione – Poiché $\text{MCD}(3, 77) = 1$, si può applicare il teorema di Euler-Fermat, per ottenere che $3^{\varphi(77)} \equiv 1 \pmod{77}$.

È $77 = 7 \cdot 11$, con 7 e 11 numeri primi; pertanto $\varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$. Sappiamo così che $3^{60} \equiv 1 \pmod{77}$.

Poiché $50\,000 = 60 \cdot 833 + 20$, si ha che

$$3^{50\,000} = 3^{60 \cdot 833 + 20} = (3^{60})^{833} \cdot 3^{20} \equiv 1 \cdot 3^{20} \pmod{77}.$$

Siamo dunque ricondotti a calcolare il resto della divisione di 3^{20} per 77, cosa che si può fare ad esempio osservando che

$$3^{20} = (3^4)^5$$

e che

$$3^4 = 81 \equiv 4 \pmod{77}.$$

Dunque

$$3^{20} \equiv 4^5 = 1\,024 \equiv 23 \pmod{77}$$

poiché $1\,024 = 77 \cdot 13 + 23$.

Pertanto, il resto della divisione per 77 di $3^{50\,000}$ è 23.

Esercizio 10.20

Trovare le ultime tre cifre della scrittura in base 10 di $13^{1\,203}$.

Soluzione – Il numero formato da tali cifre, prese nell'ordine, è il resto della divisione per $1\,000$ di $13^{1\,203}$, cioè il rappresentante "canonico" (quello compreso fra 0 e 999) della classe di resto modulo $1\,000$ cui appartiene $13^{1\,203}$. Poiché $\text{MCD}(13, 1000) = 1$, conviene utilizzare il teorema di Euler – Fermat secondo il quale $[a]^{\varphi(n)} \equiv 1 \pmod{n}$ se

$$\text{MCD}(a, n) = 1.$$

Si ha $\varphi(1000) = \varphi(8) \cdot \varphi(125) = 4 \cdot 100 = 400$, e $1\,203 = 400 \cdot 3 + 3$. Dunque,

$$13^{1\,203} = 13^{400 \cdot 3 + 3} = (13^{400})^3 \cdot 13^3 \equiv 1^3 \cdot 2\,197 \equiv 197 \pmod{1\,000}.$$

Pertanto, le ultime tre cifre della scrittura in base 10 di $13^{1\,203}$ sono, nell'ordine, 1, 9 e 7.

Esercizio 10.21

Sia $\mathbb{Z}_{843}$ l'anello delle classi di resto modulo 843. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{843}$ a cui z appartiene.
Per ciascuna delle seguenti equazioni esponenziali in $\mathbb{Z}_{843}$ nella incognita x si dica, motivando la risposta, se ha soluzioni in $\mathbb{Z}^+$ e, nei casi in cui la risposta è affermativa, si precisi quante sono le soluzioni e se ne trovi almeno una:

$$[277]^x = [1]\,; \qquad [280]^x = [0]\,; \qquad [285]^x = [1]\,.$$

Soluzione – Calcoliamo con l'algoritmo di Euclide il massimo comun divisore fra 843 e 277, quello fra 843 e 280 e quello fra 843 e 285.

$$843 = 277 \cdot 3 + 12\,; \quad 277 = 12 \cdot 23 + 1\,; \quad 12 = 1 \cdot 12\,.$$

Dunque $\mathrm{MCD}(843, 277) = 1$.

$$843 = 280 \cdot 3 + 3\,; \quad 280 = 3 \cdot 93 + 1\,; \quad 3 = 1 \cdot 3\,.$$

Dunque $\mathrm{MCD}(843, 280) = 1$.

$$\begin{aligned} &843 = 285 \cdot 2 + 273\,;\\ &285 = 273 \cdot 1 + 12\,;\\ &273 = 12 \cdot 22 + 9\,;\\ &12 = 9 \cdot 1 + 3\,;\\ &9 = 3 \cdot 3\,. \end{aligned}$$

Dunque $\mathrm{MCD}(843, 285) = 3$.

Poiché $\mathrm{MCD}(843, 285) \neq 1$, l'equazione esponenziale $[285]^x = [1]$ non ha soluzioni in $\mathbb{Z}^+$ (in $\mathbb{Z}$ ha la soluzione "banale" $x := 0$). Poiché $\mathrm{MCD}(843, 280) = 1$, l'equazione esponenziale $[280]^x = [0]$ non ha soluzioni in $\mathbb{Z}^+$ (se ne avesse, $[280]$ sarebbe $[0]$ o un divisore dello zero in $\mathbb{Z}_{843}$ e quindi dovrebbe essere $\mathrm{MCD}(843, 280) \neq 1$).

Infine, poiché $\mathrm{MCD}(843, 277) = 1$ possiamo applicare il teorema di Euler – Fermat, in base al quale l'equazione esponenziale $[277]^x = [1]$ ha infinite soluzioni, fra le quali tutti i multipli di $\varphi(843) = \varphi(281) \cdot \varphi(3) = 280 \cdot 2 = 560$.

Esercizio 10.22

Sia $n := 13^{313}$. Si determini l'ultima cifra a destra della rappresentazione di n in base sedici.

Soluzione – La cifra cercata è quella che in base sedici rappresenta il resto della divisione per sedici di 13^{313}.

Poiché $\mathrm{MCD}(13, 16) = 1$, per il teorema di Euler-Fermat è $13^{\varphi(16)} \equiv 1 \pmod{16}$. Si ha $\varphi(16) = \varphi(2^4) = 2^3 = 8$, quindi $13^8 \equiv 1 \pmod{16}$. D'altro lato è $313 = 8 \cdot 39 + 1$, quindi

$$13^{313} = 13^{8 \cdot 39 + 1} = (13^8)^{39} \cdot 13 \equiv 1 \cdot 13 = 13 \pmod{16}\,.$$

Pertanto il resto della divisione per sedici di 11^{297} è 13, e la cifra cercata è D.

Esercizio 10.23

Trovare le ultime tre cifre della scrittura in base 10 di $17^{1\,604}$.

Soluzione – Si cerca il rappresentante "canonico" (cioè compreso fra 0 e 999) della classe di resto modulo $1\,000$ cui appartiene $17^{1\,604}$. Poiché MCD$(17, 1\,000) = 1$, conviene utilizzare il teorema di Euler – Fermat secondo il quale

$$[a]^{\varphi(n)} \equiv 1 \pmod{n}$$

se MCD$(a, n) = 1$.

Si ha $\varphi(1000) = \varphi(8) \cdot \varphi(125) = 4 \cdot 100 = 400$, e $1\,604 = 400 \cdot 4 + 4$. Dunque,

$$17^{1\,604} = 17^{400 \cdot 4 + 4} = (17^{400})^4 \cdot 17^4 \equiv 1^4 \cdot 83\,521 \pmod{1\,000}.$$

Pertanto, le ultime due cifre della scrittura in base 10 di $17^{1\,604}$ sono, nell'ordine, $5, 2$ e 1.

Esercizio 10.24

Sia $\mathbb{Z}_{554}$ l'anello delle classi di resto modulo 554. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{554}$ a cui z appartiene.
Per ciascuna delle seguenti equazioni esponenziali in $\mathbb{Z}_{554}$ nella incognita x si dica, motivando la risposta, se ha soluzioni in $\mathbb{Z}^+$ e, nei casi in cui la risposta è affermativa, si precisi quante sono le soluzioni e se ne trovi almeno una:

$$[277]^x = [1]; \qquad [279]^x = [0]; \qquad [281]^x = [1].$$

Soluzione – Calcoliamo con l'algoritmo di Euclide il massimo comun divisore fra 554 e 277, quello fra 554 e 279 e quello fra 554 e 281.

$554 = 277 \cdot 2$.

Dunque MCD$(554, 277) = 277$.

$554 = 279 \cdot 1 + 275$; $279 = 275 \cdot 1 + 4$; $275 = 4 \cdot 68 + 3$; $4 = 3 \cdot 1 + 1$; $3 = 1 \cdot 3$.

Dunque MCD$(554, 279) = 1$.

$554 = 281 \cdot 1 + 273$; $281 = 273 \cdot 1 + 8$; $273 = 8 \cdot 34 + 1$; $8 = 1 \cdot 8$.

Dunque MCD$(554, 281) = 1$.

Poiché MCD$(554, 277) \neq 1$, l'equazione esponenziale $[277]^x = [1]$ non ha soluzioni in $\mathbb{Z}^+$ (in $\mathbb{Z}$ ha la soluzione "banale" $x := 0$). Poiché MCD$(554, 279) = 1$, l'equazione esponenziale $[279]^x = [0]$ non ha soluzioni in $\mathbb{Z}^+$ (se ne avesse, $[279]$ sarebbe $[0]$ o un divisore dello zero e quindi dovrebbe essere MCD$(554, 279) \neq 1$).

Infine, poiché MCD$(554, 281) = 1$ possiamo applicare il teorema di Euler – Fermat, in base al quale l'equazione esponenziale $[281]^x = [1]$ ha infinite soluzioni, fra le quali tutti i multipli di $\varphi(554) = \varphi(277) \cdot \varphi(2) = 276$.

Esercizio 10.25

Sia $\mathbb{Z}_{562}$ l'anello delle classi di resto modulo 562. Per ogni $z \in \mathbb{Z}$, indichiamo con $[z]$ l'elemento di $\mathbb{Z}_{562}$ a cui z appartiene.
Per ciascuna delle seguenti equazioni esponenziali in $\mathbb{Z}_{562}$ nella incognita x si dica, motivando la risposta, se ha soluzioni in $\mathbb{Z}^+$ e, nei casi in cui la risposta è affermativa, si precisi quante sono le soluzioni e se ne trovi almeno una:

$$[277]^x = [1]\,; \qquad [279]^x = [0]\,; \qquad [281]^x = [1]\,.$$

Soluzione – Calcoliamo con l'algoritmo di Euclide il massimo comun divisore fra 562 e 277, quello fra 562 e 279 e quello fra 562 e 281.

$$562 = 277 \cdot 2 + 8;\ 277 = 8 \cdot 34 + 5;\ 8 = 5 \cdot 1 + 3;\ 5 = 3 \cdot 1 + 2;\ 3 = 2 \cdot 1 + 1;\ 2 = 1 \cdot 2.$$

Dunque $\text{MCD}(562, 277) = 1$.

$$562 = 279 \cdot 2 + 4\,; \quad 279 = 4 \cdot 69 + 3\,; \quad 4 = 3 \cdot 1 + 1\,; \quad 3 = 1 \cdot 3\,.$$

Dunque $\text{MCD}(562, 279) = 1$.

$562 = 281 \cdot 2$. Dunque $\text{MCD}(562, 281) = 281$.

Poiché $\text{MCD}(562, 281) \neq 1$, l'equazione esponenziale $[281]^x = [1]$ non ha soluzioni in $\mathbb{Z}^+$ (in $\mathbb{Z}$ ha la soluzione "banale" $x := 0$). Poiché $\text{MCD}(562, 279) = 1$, l'equazione esponenziale $[279]^x = [1]$ non ha soluzioni in $\mathbb{Z}$ (se ne avesse, 278 sarebbe $[0]$ o un divisore dello zero e quindi dovrebbe essere $\text{MCD}(562, 279) \neq 1$).

Infine, poiché $\text{MCD}(562, 277) = 1$ possiamo applicare il teorema di Euler – Fermat, in base al quale l'equazione esponenziale $[277]^x = [1]$ ha infinite soluzioni, fra le quali tutti i multipli di $\varphi(562) = \varphi(281) \cdot \varphi(2) = 280$.

Esercizio 10.26

Calcolare il resto della divisione per 143 di $2^{100\,000}$.

Soluzione – Poiché $\text{MCD}(2, 143) = 1$, si può applicare il teorema di Euler-Fermat, per ottenere che $2^{\varphi(143)} \equiv 1 \pmod{143}$.

È $143 = 11 \cdot 13$, con 11 e 13 numeri primi; quindi $\varphi(143) = \varphi(11) \cdot \varphi(13) = 10 \cdot 12 = 120$. Sappiamo così che $2^{120} \equiv 1 \pmod{143}$. Poiché $100\,000 = 120 \cdot 833 + 40$, si ha che

$$2^{100\,000} = 2^{120 \cdot 833 + 40} = (2^{120})^{833} \cdot 2^{40} \equiv 1 \cdot 2^{40} \pmod{143}\,.$$

Siamo dunque ricondotti a calcolare il resto della divisione di 2^{40} per 143, cosa che si può fare ad esempio osservando che $2^{40} = (2^8)^5$ e che

$$2^8 = (2^4)^2 = 16 \cdot 16 = 256 \equiv 113 \pmod{143}.$$

Dunque

$$2^{40} \equiv 113^5 = 12\,769 \cdot 12\,769 \cdot 113 \equiv 42 \cdot 42 \cdot 113 = 199\,332 \equiv 133 \pmod{143}$$

poiché $12\,769 = 143 \cdot 89 + 42$ e $199\,332 = 143 \cdot 1\,393 + 133$.

Pertanto, il resto della divisione per 143 di $2^{100\,000}$ è 23.