Università Roma Tre - Corso di Laurea in Matematica
AL110-Algebra 1 - A.A. 2017-2018 – prof. Cigliola
Esercizi svolti di aritmetica modulare

Esercizio 1. Calcolare l'ultima cifra del numero 57937^{458}.

Svolgimento. In base ai criteri di divisibilità studiati, sappiamo che l'ultima cifra di un numero intero a coincide con il resto della divisione di a per 10. Si tratta in altre parole di calcolare

$$x = 57937^{458} (\text{mod}.10)$$

Cominciamo con il ridurre la base della potenza richiesta, per quanto ricordato sopra:

$$57937 \equiv 7 (\text{mod}.10)$$

Quindi $x \equiv 7^{458} (\text{mod}.10)$. Poiché 7 è coprimo con il modulo $m = 10$, possiamo applicare il teorema di Euler-Fermat, riducendo l'esponente 458 modulo $\varphi(10) = 4$. Abbiamo che

$$458 \equiv 2 (\text{mod}.4)$$

pertanto

$$x \equiv 7^2 = 49 \equiv 9 (\text{mod}.10).$$

Esercizio 2. Calcolare le ultime due cifre del numero 57937^{458}.

Svolgimento. Procediamo come sopra, ricordando che le ultime due cifre di un numero sono date dal resto della divisione modulo 100. Quindi cerchiamo

$$x \equiv 57937^{458} (\text{mod}.100) \equiv 37^{458} (\text{mod}.100)$$

Poiché 37 è coprimo con 100, possiamo ridurre l'esponente modulo $\varphi(100) = \varphi(4)\varphi(25) = 2 \cdot 20 = 40$. Si ha che $458 \equiv 18 (\text{mod}.40)$ e dunque

$$x \equiv 37^{18} (\text{mod}.100)$$

Calcoliamo, per ridurre l'espressione,

$$37^2 = (30+7)^2 = (30+7)(30+7) = 900 + 420 + 49 = 69 \equiv -31 (\text{mod}.100)$$

e

$$31^3 = 31 \cdot 31^2 \equiv 31 \cdot 61 = (30+1)(60+1) = 30 + 60 + 1800 + 1 \equiv 91 \equiv -9 (\text{mod}.100)$$

Sostituendo in x, abbiamo che

$$x \equiv 37^{18} = (37^2)^9 \equiv (-31)^9 = -(31^3)^3 = -(-9)^3 = 9^3 = 81 \cdot 9 = 729 \equiv 29 (\text{mod}.100).$$

In alternativa il calcolo di $37^{18} (\text{mod}.100)$ può essere portato avanti sfruttando il teorema cinese dei resti. Infatti, essendo 100 il prodotto dei due fattori coprimi 4 e 25, abbiamo l'equivalenza

$$x \equiv 37^{18} (\text{mod}.100) \qquad \Leftrightarrow \qquad \begin{cases} x \equiv 37^{18} (\text{mod}.4) \\ x \equiv 37^{18} (\text{mod}.25) \end{cases}$$

La prima equazione diventa banale non appena si riduce la base della potenza modulo 4:

$$x \equiv 37^{18} = (36+1)^{18} \equiv 1 (\text{mod}.4).$$

L'altra diventa

$$x \equiv 37^{18} \equiv 12^{18} \equiv (-6)^9 = -6^9 \equiv -16^3 \equiv 4 (\text{mod}.25).$$

Dobbiamo allora risolvere il sistema

$$\begin{cases} x \equiv 1 (\text{mod}.4) \\ x \equiv 4 (\text{mod}.25). \end{cases}$$

Procedendo, ad esempio per sostituzioni, si trova dalla prima equazione $x = 4k+1$, per qualche $k \in \mathbb{Z}$ e

$$4k + 1 \equiv 4 (\text{mod}.25)$$

$$4k \equiv 3(\text{mod}.25) \qquad (*)$$

Poiché 4 è coprimo con 25, potremmo usare il teorema di Euler-Fermat trovando che

$$4^* \equiv 5^{\varphi(25)-1} \equiv -6$$

È più conveniente osserva che $6 \cdot 4 = 24 \equiv -1(\text{mod}.25)$ e che quindi $(-6) \cdot 4 \equiv 1(\text{mod}.25)$. Moltiplicando la (*) per -6, ricaviamo che

$$k \equiv -18 \equiv 7(\text{mod}.25).$$

Sostituendo in x abbiamo che

$$x \equiv 4 \cdot 7 + 1 = 29(\text{mod}.100).$$

Esercizio 3. Calcolare l'ultima cifra di 7^{7^7}.

Svolgimento. Poiché 7 è coprimo con 10, riduciamo dapprima l'esponente 7^7 modulo $\varphi(10) = 4$. L'espressione

$$7^7(\text{mod}.4)$$

può essere a sua volta semplificata usando il teorema di Euler-Fermat, essendo l'esponente 7 coprimo con 4. Siccome $7 \equiv 1(\text{mod}.\varphi(4) = 2)$, ne ricaviamo che

$$7^7 \equiv 7 \equiv 3(\text{mod}.4).$$

Tornando al modulo 10, abbiamo infine che

$$7^{7^7} \equiv 7^3 = 49 \cdot 7 \equiv 49 \cdot 3 \equiv 9 \cdot 3 = 27 \equiv 7(\text{mod}.10).$$

Esercizio 4. Calcolare l'ultima cifra di 2^{999}.

Svolgimento. Poiché 2 è un divisore di 10, non possiamo procedere come nel precedente esercizio applicando il teorema di Euler-Fermat. Dobbiamo trovare altre strategie di calcolo. Osserviamo a tal fine che

$$2^1 = 2 \qquad 2^2 = 4 \qquad 2^3 = 8 \qquad 2^4 \equiv 6 \qquad 2^5 \equiv 2(\text{mod}.10).$$

L'ultimo calcolo effettuato ci fa capire che periodicamente le potenze di due assumono i quattro valori 2, 4, 8, 6 quando lavoriamo modulo 10. Per calcolare allora $2^k(\text{mod}.10)$, con k intero positivo, basta prendere come esponente il resto della divisione di k modulo 4:

$$k \equiv t(\text{mod}.4) \qquad \Rightarrow \qquad 2^k \equiv 2^t(\text{mod}.10).$$

In particolare ciò ci dà un controesempio per la validità della formula di Eulero nel caso in cui la base della potenza non è coprima con il modulo. Infatti $\varphi(10) = 4$ e

$$2^4 \equiv 6 \not\equiv 1(\text{mod}.10).$$

Tornando all'esponente 999, abbiamo che

$$999 = 900 + 99 \equiv 19 \equiv 3(\text{mod}.4)$$

Pertanto $2^{999} \equiv 2^3 = 8(\text{mod}.10)$.