

FUNZIONE TOTIENTE,
TEOREMA DI EULERO,
PICCOLO TEOREMA DI FERMAT

In queste brevi note vogliamo vedere alcune applicazioni della funzione totiente (teorema di Eulero) e del piccolo teorema di Fermat. Gli ingredienti sono:

- **Il Gruppo U_m** degli elementi invertibili di $\mathbb{Z}_m$. Sono tutte le classi $[a] \in \mathbb{Z}_m$ tali che a ed m sono coprimi.
- **Funzione totiente.** È la funzione $\phi : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}$ data $\phi(m) = |U_m|$, quindi $\phi(m)$ è data dal numero di elementi $a \in \mathbb{Z}$ tali che $0 < a < m$ e a ed m sono coprimi.
- **Teorema di Eulero.** Per ogni $a \in \mathbb{Z}$ tale che a ed m sono coprimi, vale:

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

- **Piccolo teorema di Fermat.** Se p è primo e $a \in \mathbb{Z}$ è tale che p non divide a , allora

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

o, anche, per qualunque $a \in \mathbb{Z}$,

$$a^p \equiv a \pmod{p}$$

Esempi:

- Trovare 2^{389} modulo 11 (evitando il conto diretto, non molto agevole).
Dal piccolo teorema di Fermat abbiamo che $2^{10} \equiv 1$ modulo 11. Allora anche $2^{390} \equiv 1$ modulo 11 in quanto $2^{390} = (2^{10})^{39} \equiv 1^{39} \equiv 1$. Poiché $2^{390} = 2^{389+1}$, abbiamo che $2^{389} \cdot 2 \equiv 1$, cioè in $\mathbb{Z}_{11}$ la classe di 2^{389} è l'inversa della classe di 2. Il problema allora diventa trovare l'inverso di [2] in $\mathbb{Z}_{11}$. Siccome 2 e 11 sono coprimi, il problema ha soluzione e si può usare l'identità di Bezout. Si vede subito che $1 = 2 \cdot (-5) + 11 \cdot 1$, quindi l'inverso di [2] in $\mathbb{Z}_{11}$ è $[-5] = [6]$. In conclusione, $2^{389} \equiv 6$ modulo 11.
Una soluzione alternativa potrebbe essere la seguente: $389 = 38 \cdot 10 + 9$, quindi $2^{389} \equiv (2^{10})^{38} \cdot 2^9 \equiv 2^9$. Ora $2^9 = 2^4 \cdot 2^4 \cdot 2^1$ e, modulo 11 si ottiene $2^9 \equiv 5 \cdot 5 \cdot 2 \equiv 6$ modulo 11.
- Trovare 7^{314} modulo 20.
Contando gli elementi invertibili di $\mathbb{Z}_{20}$, abbiamo che $\phi(20) = 8$ (i numeri primi con 20 e minori di 20 sono infatti 8 e cioè: 1, 3, 7, 9, 11, 13, 17, 19), pertanto, per il teorema di Eulero: $7^8 \equiv 1$ modulo 20. Inoltre $314 = 39 \cdot 8 + 2$, quindi $7^{314} = (7^8)^{39} \cdot 7^2$ e quindi $7^{314} \equiv 49 \equiv 9$ modulo 20.

- Trovare l'ultima cifra del numero 13^{4587} .
Si tratta quindi di trovare quanto vale 13^{4587} modulo 10. Poiché $\phi(10) = 4$ e $4587 = 1146 \cdot 4 + 3$, abbiamo da calcolare 13^3 modulo 10. Inoltre $13 \equiv 3$ modulo 10, quindi $13^{4587} \equiv 13^3 \equiv 3^3$ modulo 10, pertanto l'ultima cifra è l'ultima cifra di $3^3 = 27$, cioè vale 7.
- Provare che il numero 511 non è un numero primo.
Supponiamo che 511 sia primo. Allora, per il piccolo teorema di Fermat, deve valere: $2^{510} \equiv 1$ modulo 511. Si tratta allora di calcolare 2^{510} modulo 511. In base 2 il numero 510 si scrive così: 111111110, quindi $510 = 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1$. Allora $2^{510} = 2^{2^8} + 2^{2^7} + 2^{2^6} + 2^{2^5} + 2^{2^4} + 2^{2^3} + 2^{2^2} + 2^{2^1}$. Calcolare 2^{2^i} modulo 511 non è complicato: si ottiene, per $i = 0, 1, \dots, 8$, rispettivamente: 2, 4, 16, 256, 128, 32, 2, 4, 16, quindi $2^{510} \equiv 4 \cdot 16 \cdot 256 \cdot 128 \cdot 32 \cdot 2 \cdot 4 \cdot 16$ modulo 511 e si ottiene che $2^{510} \equiv 64$ modulo 511. Pertanto 2^{510} modulo 511 non è il numero 1 e quindi 511 non è primo. Un altro modo per calcolare 2^{510} modulo 511 è il seguente: si vede subito che $2^9 = 512$. Pertanto $2^9 \equiv 1$ modulo 511. Poiché $510 = 9 \cdot 56 + 6$, allora $2^{510} \equiv 2^6 \equiv 64$ modulo 511.
- Provare che il numero $n^9 + 2n^7 + 3n^3 + 4n$ è sempre divisibile per 5 (per ogni $n \in \mathbb{Z}$).
Infatti, se $5|n$ il risultato è vero. Se 5 non divide n allora, per il piccolo teorema di Fermat, $n^4 \equiv 1$ modulo 5 e quindi $n^9 + 2n^7 + 3n^3 + 4n \equiv n^4 \cdot n^4 \cdot n + 2n^4 \cdot n^3 + 3n^3 + 4n \equiv n + 2n^3 + 3n^3 + 4n \equiv 5n^3 + 5n \equiv 0$ modulo 5.
- Sapendo che il numero 167 è un numero primo, provare che nel gruppo U_{167} degli elementi invertibili di $\mathbb{Z}_{167}$ l'ordine di $[7]$ è almeno 80.
Si ricordi che, se $(G, \cdot)$ è un gruppo moltiplicativo, l'ordine di un elemento $g \in G$ è il più piccolo $n \in \mathbb{N} \setminus \{0\}$ (se esiste) tale che $g^n = 1$ (se G è finito, l'ordine di un elemento esiste sempre ed è un divisore dell'ordine del gruppo). Inoltre si ricordi anche che se $g \in G$ è tale che $g^m = 1$ e se g ha ordine n , allora n divide m . Tornando all'esercizio, sia n l'ordine di $[7]$. Per Fermat abbiamo che $[7]^{166} = 1$, allora n deve dividere $166 = 2 \cdot 83$. Siccome l'ordine di $[7]$ non è né 1, né 2, deve essere o 83 o 166. In particolare è superiore ad 80.
- Per ogni $n \in \mathbb{Z}$, trovare il resto della divisione di

$$P(n) = 5n^{13} + 8n^9 - n^3 + 2n + 10$$

quando viene diviso per 7.

Per Fermat abbiamo che, per ogni n vale: $n^7 \equiv n$ modulo 7. Pertanto, considerando le congruenze modulo 7, abbiamo: $n^{13} \equiv n^7 \cdot n^6 \equiv n^7 \equiv n$; $n^9 \equiv n^3$ e quindi $P(n) \equiv 5n + 8n^3 - n^3 + 2n + 10 \equiv 7n + 7n^3 + 10 \equiv 10 \equiv 3$. In conclusione, il resto della divisione di $P(n)$ per 7 vale sempre 3.