Congruenze ($\mathtt{mod}\ n$), congruenze lineari e teorema cinese del resto

Un fondamentale esempio di relazione di equivalenza è descritto nel seguente risultato.

Proposizione 1. Sia $n \in \mathbb{N}^*$, $n \neq 1$. La relazione

$$\mathcal{R}_n = \{(a,b) \in \mathbb{Z} \times Z : a \equiv b (\mathtt{mod}\ n)\}$$

è una relazione di equivalenza su $\mathbb{Z}$, che si dice *congruenza modulo* n.

Dimostrazione. Si deve provare che

(1) $\mathcal{R}_n$ è riflessiva: $\forall a \in \mathbb{Z}$, $a \equiv a\ (\mathtt{mod}\ n)$

(2) $\mathcal{R}_n$ è simmetrica: $\forall a, b \in \mathbb{Z}$, $a \equiv b\ (\mathtt{mod}\ n) \Rightarrow b \equiv a\ (\mathtt{mod}\ n)$

(3) $\mathcal{R}_n$ è transitiva: $\forall a, b, c \in \mathbb{Z}$, $\big(a \equiv b\ (\mathtt{mod}\ n)\ \wedge\ b \equiv c\ (\mathtt{mod}\ n)\big) \Rightarrow a \equiv c\ (\mathtt{mod}\ n)$

(1) Poiché per ogni $a \in \mathbb{Z}$, $n \mid a - a$, sicuramente $(a,a) \in \mathcal{R}_n$, ovvero $a \equiv a\ (\mathtt{mod}\ n)$.
(2) Siano $a, b \in \mathbb{Z}$, con $a \equiv b\ (\mathtt{mod}\ n)$. Questo vuol dire che $n \mid a-b$, quindi $n \mid -(a-b)$, cioè $n \mid b - a$, per cui $b \equiv a\ (\mathtt{mod}\ n)$.
(3) Siano $a, b, c \in \mathbb{Z}$, con $a \equiv b\ (\mathtt{mod}\ n)$ e $b \equiv c\ (\mathtt{mod}\ n)$, ovvero $n \mid a - b$ e $n \mid b - c$. Allora $n \mid (a-b) + (b-c)$, vale a dire $n \mid a - c$ e quindi $a \equiv c\ (\mathtt{mod}\ n)$.

Notazione Per ogni $a, b \in \mathbb{Z}$, invece che $(a,b) \in \mathcal{R}_n$ si scrive

$$a \equiv b\ (\mathtt{mod} n)$$

e si legge "a congruo b modulo n".

Lemma 1. Siano $a, b, c, d \in \mathbb{Z}$, $k, n \in \mathbb{N}^*$, $n \neq 1$. Si ha:

(1) $(a \equiv b\ (\mathtt{mod}\ n) \wedge c \equiv d\ (\mathtt{mod}\ n)) \Longrightarrow a + c\ \equiv b + d\ (\mathtt{mod}\ n)$

(2) $(a \equiv b\ (\mathtt{mod}\ n) \wedge c \equiv d\ (\mathtt{mod}\ n)) \Longrightarrow ac\ \equiv bd\ (\mathtt{mod}\ n)$

(3) $a \equiv b\ (\mathtt{mod}\ n) \Longrightarrow a^k \equiv b^k\ (\mathtt{mod}\ n)$

Dimostrazione. Da $a \equiv b\ (\mathtt{mod}\ n)$ e $c \equiv d\ (\mathtt{mod}\ n)$ segue $n \mid (a-b)$ e $n \mid (c-d)$. Allora $n \mid a - b + c - d$, ovvero $a \mid (a+c) - (b+d)$ e ciò vuol dire che $a + c\ \equiv b + d\ (\mathtt{mod}\ n)$, per cui (1) è provata.
Poichè $a \equiv b\ (\mathtt{mod}\ n)$ e $c \equiv d\ (\mathtt{mod}\ n)$, allora $n \mid (a-b)$ e $n \mid (c-d)$ e quindi $n \mid (a-b)c$ e $n \mid (c-d)b$. Pertanto $n \mid (a-b)c + (c-d)b$, cioé $n \mid ac - bd$, ovvero $ac\ \equiv bd\ (\mathtt{mod}\ n)$, e (2) risulta verificata.
Per provare (3) si procede per induzione completa su k. Per $k = 1$, certamente $a^1\ \equiv b^1\ (\mathtt{mod}\ n)$ è verificato poiché $a^1 = a$, $b^1 = b$. Sia $k \in \mathbb{N}$, $k > 1$. Si suppone che sia $a^k \equiv b^k\ (\mathtt{mod}\ n)$ e si deve provare che $a^{k+1} \equiv b^{k+1}\ (\mathtt{mod}\ n)$. Per ipotesi di induzione si ha $a^k \equiv b^k\ (\mathtt{mod}\ n)$; inoltre, per ipotesi, $a \equiv b\ (\mathtt{mod}\ n)$. Allora, usando (2), $a^k a \equiv b^k b\ (\mathtt{mod}\ n)$ e, ricordando che per ogni numero intero x, risulta $x^{k+1} = x^k \cdot x$, si ha $a^{k+1} \equiv b^{k+1}\ (\mathtt{mod}\ n)$.

Teorema 1. L'insieme quoziente di $\mathbb{Z}$ per $\mathcal{R}_n$ ha esattamente n elementi, cioè:

$$\mathbb{Z}/\mathcal{R}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$

dove, per ogni $x \in \mathbb{Z}$, $[x]_n$ indica la classe di equivalenza di x.

Dimostrazione. Si dimostra prima che le classi di equivalenza $[0]_n, [1]_n, \ldots, [n-1]_n$ sono distinte fra loro. Siano $a, b \in \mathbb{N}$, con $a \neq b$, $0 \leq a \leq n-1$, $0 \leq b \leq n-1$, e si può supporre che sia $a < b$. Se fosse $[a]_n = [b]_n$ allora sarebbe $b \equiv a \ (\mathtt{mod} n)$ cioè $n \mid b-a$. Però $b - a \leq n-1$ e quindi n potrebbe essere un divisore di $b-a$ solo se $b-a = 0$, il che contraddice l'ipotesi $a \neq b$.
Resta da provare che non ci sono classi di equivalenza diverse da $[0]_n, [1]_n, \ldots, [n-1]_n$ in $\mathbb{Z}/\mathcal{R}_n$. A tale scopo, sia $m \in \mathbb{Z}$. Per il teorema sulla divisione, esistono $q, r \in \mathbb{Z}$, con $0 \leq r < n$ tali che $m = nq + r$. Allora $m - r = nq$, per cui $n \mid m - r$, ovvero $m \equiv r \ (\mathtt{mod} n)$ e quindi $[m]_n = [r]_n$. Segue che:

$$\forall [m]_n \in \mathbb{Z}/\mathcal{R}_n \ \exists r \in \mathbb{N}, \text{ con } 0 \leq r \leq n-1 \text{ tale che } [m]_n = [r]_n$$

e ciò conclude la dimostrazione.

Definizione 1. L'insieme quoziente di $\mathbb{Z}$ per $\mathcal{R}_n$ si chiama *insieme dei resti modulo n* e si indica con il simbolo $\mathbb{Z}_n$.

Definizione 2. Siano $a, b \in \mathbb{Z}$, $a \neq 0$, $n \in \mathbb{N} - \{0, 1\}$. Si dice *congruenza lineare* l'espressione

$$ax \equiv b \ (\mathtt{mod}\ n). \tag{1}$$

Si dice soluzione di (1) ogni intero x_0 tale che $ax_0 \equiv b \ (\mathtt{mod}\ n)$.

Teorema 2. *Siano $a, b \in \mathbb{Z}$, $a \neq 0$, $n \in \mathbb{N} - \{0, 1\}$ e sia $d = M.C.D.(a, n)$. Allora*

1. *la congruenza lineare* (1) *ammette soluzioni se e solo se $d \mid b$.*
2. *se x_0 è una soluzione di* (1)*, posto $\bar{n} = \frac{n}{d}$, tutte le altre soluzioni di* (1) *sono $x_0 + k\bar{n}$, al variare di $k \in \mathbb{Z}$*
3. *ci sono esattamente d soluzioni non congrue tra loro* mod n*, cioè $x_0, x_0+\bar{n}, \ldots, x_0+(d-1)\bar{n}$.*

Dimostrazione. Per provare 1, si osserva che, affermare che la congruenza lineare (1) ha soluzioni equivale a dire che esiste $x_0 \in \mathbb{Z}$ tale che

$$n \mid ax_0 - b,$$

ovvero che esistono $x_0, y_0 \in \mathbb{Z}$ tali che

$$ax_0 - b = ny_0,$$

ossia

$$ax_0 + n(-y_0) = b. \tag{2}$$

Questo vuol dire che l'equazione diofantea $ax + ny = b$ ammette soluzione $(x_0, -y_0)$. Il Teorema sulle equazioni diofantee assicura che (2) ha soluzioni se e solo se $M.C.M.(a, n)|b$. Anche 2 segue subito dal Teorema . La dimostrazione della proprietà 3 si tralascia.

Teorema 3. *(Teorema cinese del resto) Un sistema si congruenze lineari della forma:*

$$\begin{cases} x \equiv b_1 (\mathtt{mod}\ n_1) \\ x \equiv b_2 (\mathtt{mod}\ n_2) \\ \vdots \\ x \equiv b_h (\mathtt{mod}\ n_h) \end{cases} \tag{3}$$

dove $\forall i, j = 1, \ldots, h$, $M.C.D.(n_i, n_j) = 1$, *ha sempre soluzioni. Inoltre c'è un'unica soluzione modulo* $R = n_1 \cdot \ldots \cdot n_h$.

Dimostrazione. Si da soltanto un cenno della dimostrazione: si prova che una soluzione del sistema (3) è data da:

$$x_0 = R_1 \cdot \bar{x}_1 + R_2 \cdot \bar{x}_2 + \cdots + R_h \cdot \bar{x}_h$$

dove per ogni $i = 1, \ldots, h$

$$R_i = \frac{n_1 \cdot n_2 \cdot \ldots \cdot n_h}{n_i},$$

mentre $\bar{x}_i$ è una soluzione della congruenza lineare

$$R_i x \equiv b_i (\mathtt{mod}\ n_i).$$

Esempio 1.

$$\begin{cases} x \equiv 3(\mathtt{mod}\ 5) \\ x \equiv 4(\mathtt{mod}\ 3) \\ x \equiv 2(\mathtt{mod}\ 7) \\ x \equiv 5(\mathtt{mod}\ 2) \end{cases}$$

Si vede facilmente che

$$R_1 = 42,\ R_2 = 70,\ R_3 = 30,\ R_4 = 105.$$

Si cercano le soluzioni delle congruenze lineari previste nel teorema:

$$42x \equiv 3(\mathtt{mod}\ 5)$$

ha soluzione $x_1 = -6$, (si trova eseguendo l'algoritmo delle divisioni successive)

$$70x \equiv 4(\mathtt{mod}\ 3)$$

ha soluzione $x_2 = 1$ ($70 - 4 = 66$ che è multiplo di 3)

$$30x \equiv 2(\mathtt{mod}\ 7)$$

ha soluzione $x_3 = 1$ ($30 - 2 = 28$ che è multiplo di 4)

$$105x \equiv 5(\mathtt{mod}\ 2)$$

ha soluzione $x_4 = 1$ ($105 - 5 = 100$ che è multiplo di 2). Allora una soluzione è

$$\bar{x} = 42 \cdot (-6) + 70 + 30 + 105 = -47,$$

mentre la più piccola soluzione positiva è 163 e tutte le soluzioni del sistema sono

$$163 + 210h, \quad h \in \mathbb{Z}.$$

Numeri in base n e criteri di divisibilità

Teorema 4. *Sia $n \in \mathbb{N}^*$, $n \neq 1$. Allora $\forall a \in \mathbb{N}, \exists | r_0, \ldots, r_h \in \mathbb{N}$ tali che*

$$a = r_h n^h + r_{h-1} n^{h-1} + \cdots + r_1 n + r_0. \tag{4}$$

Dimostrazione. (cenno) Si eseguono le seguenti divisioni:

$$\begin{array}{rcll} a & = & q_0\ n + r_0, & r_0 < n \\ q_0 & = & q_1\ n + r_1, & r_1 < n \\ q_1 & = & q_2\ n + r_2. & r_2 < n \\ \vdots & & & \\ q_{h-2} & = & q_{h-1}\ n + r_{h-1} & r_{h-1} < n \\ q_{h-1} & = & 0\ n + r_h & r_h < n \end{array}$$

Poichè si tratta di numeri naturali, si ha $q_0 > q_1 > \ldots$, per cui, ad un certo punto il quoziente di una divisione si deve azzerare.
Si ha, quindi:

$$\begin{aligned} a = q_0 n + r_0 = (q_1 n + r_1) n + r_0 = q_1 n^2 + r_1 n + r_0 \\ = (q_2 n + r_2) n^2 + r_1 n + r_0 = q_2 n^3 + r_2 n^2 + r_1 n + r_0 \\ = \cdots = r_h n^h + r_{h-1} n^{h-1} + \cdots + r_1 n + r_0. \end{aligned}$$

Osservazione 1. Per comoditá, invece di usare l'espressione (4), si scrive:

$$(a)_n = r_h r_{h-1} \ldots r_1 r_0.$$

che si dice *scrittura del numero a in base n.*

Osservazione 2. Sia $n \in \mathbb{N}^*$, $n \neq 1$. Poiché risulta:

$$\begin{array}{rcl} n & = & 1\ n + 0 \\ 1 & = & 0\ n + 1, \end{array}$$

si ha $(n)_{10} = (10)_n$

Esempio 2. Si vuole scrivere 11 in base 2. Si effettuano le divisioni, come suggerisce il Teorema 4

$$\begin{array}{rcl} 11 & = & 5 \cdot \mathbf{2} + 1 \\ 5 & = & 2 \cdot \mathbf{2} + 1 \\ 2 & = & 1 \cdot \mathbf{2} + 0 \\ 1 & = & 0 \cdot \mathbf{2} + 1. \end{array}$$

Allora si ha:

$$\begin{array}{rcl} (11)_{10} & = & 5 \cdot \mathbf{2} + 1 = (2 \cdot \mathbf{2} + 1)\mathbf{2} + 1 = 2 \cdot \mathbf{2}^2 + 1 \cdot \mathbf{2} + 1 \\ & = & (1 \cdot \mathbf{2} + 0)\mathbf{2}^2 + 1 \cdot \mathbf{2} + 1 \\ & = & 1 \cdot \mathbf{2}^3 + 0 \cdot \mathbf{2}^2 + 1 \cdot \mathbf{2} + 1 \\ & = & (1011)_2 \end{array}$$

Osservazione 3. Siano $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$, $n \neq 1$, con $a \equiv b \pmod{n}$. Allora

$$n \mid a \iff n \mid b.$$

Dimostrazione. Se $n \mid a$, poichè per ipotesi $a \equiv b \pmod{n}$, risulta $n \mid a - b$ e quindi $n \mid a - (a - b)$, cioè $n \mid b$. L'altra implicazione è del tutto analoga: se $n \mid b$, poichè dall'ipotesi segue $n \mid a - b$, si ha $n \mid b + (a - b)$, cioè $n \mid a$.

Criteri di divisibilità per 10, per 5, per 2

Sia $a \in \mathbb{N}^*$. Se $a = r_h r_{h-1} \dots r_1 r_0$ (ovviamente in base 10), allora si può scrivere:

$$a = r_h 10^h + r_{h-1} 10^{h-1} \dots r_1 10 + r_0. \tag{5}$$

È noto che a è divisibile per 2 se e solo se l'ultima cifra r_0 è pari, è divisibile per 5 se e solo se r_0 è uguale a 5 oppure a 0, è divisibile per 10 se e solo se r_0 è 0. Si osseva che (5) può essere scritta come

$$a = 10(r_h 10^{h-1} + r_{h-1} 10^{h-2} \dots r_1) + r_0$$

e quindi:

$$a - r_0 = 10(r_h 10^{h-1} + r_{h-1} 10^{h-2} \dots r_1).$$

Dunque $10 \mid a - r_0$ per cui anche $5 \mid a - r_0$ e $2 \mid a - r_0$. Allora $a \equiv r_0 \pmod{10}$, $a \equiv r_0 \pmod{5}$, $a \equiv r_0 \pmod{2}$ e quindi, per l'Osservazione 3:

$$10 \mid a \iff 10 \mid r_0,$$

$$5 \mid a \iff 5 \mid r_0,$$

$$2 \mid a \iff 2 \mid r_0,$$

Criteri di divisibilità per 3, per 9

Poichè $10 \equiv 1 \pmod{3}$, allora risulta $10^k \equiv 1^k \equiv 1 \pmod{3}$, per ogni $k \in \{1, \dots, h\}$, e quindi

$$a \equiv r_h + r_{h-1} + \dots + r_0 \pmod{3},$$

da cui, per l'Osservazione 3, si ricava il noto criterio di divisibilità per 3:

$$3 \mid a \iff 3 \mid r_h + r_{h-1} + \dots + r_0.$$

Analogamente si ottiene il criterio di divisibilità per 9, osservando che $10 \equiv 1 \pmod{9}$.

Criterio di divisibilità per 11

Si osserva che $10 \equiv -1 \pmod{11}$ e quindi:

$$10^k \equiv (-1)^k \pmod{11},$$

cioè $10^k \equiv 1 \pmod{11}$ se k è pari $10^k \equiv -1 \pmod{11}$ se k è dispari. Allora usando ancora l'Osservazione 3 si ha

$$a \equiv r_h(-1)^h + r_{h-1}(-1)^{h-1} + \dots + r_1(-1) + r_0(-1)^0 \pmod{11},$$

cioè

$$11 \mid a \iff 11 \mid r_h(-1)^h + r_{h-1}(-1)^{h-1} + \dots + r_1(-1) + r_0(-1)^0.$$

Esempio 3. Risulta che $11 \mid 939115309$, perchè $9-3+9-1+1-5+3-0+9=22$ che è un multiplo di 11.

Metodi di fattorizzazione

CRIVELLO DI ERATOSTENE Sia $n \in \mathbb{N}$, $n \geq 4$ (si può sempre studiare la scomposizione dei numeri interi riferendosi ai numeri positivi, senza ledere la generalità dei ragionamenti). Per determinare i numeri primi minori o uguali di n, si scrive una tabella con tutti i numeri fino ad n e si procede cancellando per primi tutti i multipli di 2. Finita questa operazione, si eliminano tutti i multipli del primo numero non cancellato, ovvero 3; dopo i multipli di 5, che è il primo numero non cancellato, dopo tutti i multipli di 7 e così via. È importante osservare che il procedimento si ferma al più grande numero primo q più piccolo di $\sqrt{n}$.

Osservazione 4. Tra i fattori primi di un numero naturale n non primo $n \geq 4$ ce n'è almeno uno minore o uguale di $\sqrt{n}$. Sia infatti

$$n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s}$$

la scomposizione di n in fattori primi. Se fosse

$$p_1 > \sqrt{n}, \ldots, p_s > \sqrt{n},$$

allora sarebbe

$$n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s} > \sqrt{n}^{h_1} \cdot \ldots \cdot \sqrt{n}^{h_s} \geq n$$

il che è una contraddizione.

Esempio 4. Si vuole trovare l'eventuale scomposizione in fattori primi del numero $n = 4187$. Si considera la sua radice $\sqrt{n} \backsim 64,707$ e quindi si prendono in esame tutti i numeri primi minori di 64, che sono:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61.$$

Effettuando (se necessario) le divisioni con la calcolatrice si ottiene un eventuale primo fattore. Se non si trova nessun fattore, per l'Osservazione 4, il numero è certamente primo.
In queso caso si vede che n è divisibile per 53 e precisamente $n = 53 \cdot 79$.

Esempio 5. Si vuole trovare l'eventuale scomposizione in fattori primi del numero $n = 613$. Si considera la sua radice $\sqrt{n} \backsim 24,758$ e quindi si prendono in esame tutti i numeri primi minori di 24, che sono:

$$2, 3, 5, 7, 11, 13, 17, 19, 23.$$

Effettuando le divisioni necessarie con la calcolatrice, si vede che il numero non è divisibile per alcuno dei numeri primi minori di 24, per cui, per l'Osservazione 4, 613 è certamente un numero primo.

METODO DI FATTORIZZAZIONE DI FERMAT Questo metodo si basa sul seguente risultato:

Proposizione 2. *Sia $n \in \mathbb{N}^*$, $n \neq 1$, n dispari (se n fosse pari, si potrebbe dividere per 2 anche più volte, fino ad ottenenere un numero dispari). Sussiste la seguente equivalenza:*

$$(\exists\ a, b \in \mathbb{N} \text{ tali che } n = ab) \Longleftrightarrow (\exists\ x, y \in \mathbb{N} \text{ tali che } n = x^2 - y^2).$$

Dimostrazione. Se $n = ab$, allora a e b sono due numeri dispari, per cui la loro somma, come la loro differenza, è pari. Quindi $\frac{a+b}{2} \in \mathbb{N}$, e, se per esempio si suppone che sia $a \geq b$, anche $\frac{a-b}{2} \in \mathbb{N}$. Si vede facilmente che

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2,$$

per cui $\exists\ x = \frac{a+b}{2},\ y = \frac{a-b}{2} \in \mathbb{N}$ tali che $n = x^2 - y^2$.
Il viceversa è ovvio, perchè se esistono $x, y \in \mathbb{N}$ tali che $n = x^2 - y^2 = (x+y) \cdot (x-y)$, certamente è $x \geq y$ per cui $a = x + y \in \mathbb{N},\ b = x - y \in \mathbb{N}$ e si ha $n = ab$.

Osservazione 5. Quando n è primo si ha la fattorizzazione banale:

$$n = \left(\frac{n+1}{2} + \frac{n-1}{2}\right) \cdot \left(\frac{n+1}{2} - \frac{n-1}{2}\right) = n \cdot 1.$$

In virtù della Osservazione 2, cercare una fattorizzazione di n equivale a cercare x tale che $x^2 - n$ sia un quadrato (cioè y^2). Allora si usa il seguente procedimento: si determina il più piccolo intero positivo $t \geq \sqrt{n}$ e si calcolano

$$t^2 - n;\quad (t+1)^2 - n;\quad (t+2)^2 - n; \ldots\ldots$$

e così via, finché si trova un quadrato.

Esempio 6. $n = 1183$, $\sqrt{n} \backsim 34, 39$, $t = 35$ allora si ha:

$$\begin{aligned}
t^2 - n &= 35^2 - 1183 = 1225 - 1183 = 42 \quad \text{non quadrato} \\
(t+1)^2 - n &= 36^2 - 1183 = 1296 - 1183 = 113 \quad \text{" "} \\
(t+2)^2 - n &= 37^2 - 1183 = 1369 - 1183 = 186 \quad \text{" "} \\
(t+3)^2 - n &= 38^2 - 1183 = 1444 - 1183 = 261 \quad \text{" "} \\
(t+4)^2 - n &= 39^2 - 1183 = 1521 - 1183 = 338 \quad \text{" "} \\
(t+5)^2 - n &= 40^2 - 1183 = 1600 - 1183 = 417 \quad \text{" "} \\
(t+6)^2 - n &= 41^2 - 1183 = 1681 - 1183 = 498 \quad \text{" "} \\
(t+7)^2 - n &= 42^2 - 1183 = 1764 - 1183 = 581 \quad \text{" "} \\
(t+8)^2 - n &= 43^2 - 1183 = 1849 - 1183 = 646 \quad \text{" "} \\
(t+9)^2 - n &= 44^2 - 1183 = 1936 - 1183 = 753 \quad \text{" "} \\
(t+10)^2 - n &= 45^2 - 1183 = 2052 - 1183 = 842 \quad \text{" "} \\
(t+11)^2 - n &= 46^2 - 1183 = 2116 - 1183 = 933 \quad \text{" "} \\
(t+12)^2 - n &= 47^2 - 1183 = 2209 - 1183 = 1026 \quad \text{" "} \\
(t+13)^2 - n &= 48^2 - 1183 = 2304 - 1183 = 1121 \quad \text{" "} \\
(t+14)^2 - n &= 49^2 - 1183 = 2401 - 1183 = 1218 \quad \text{" "} \\
(t+15)^2 - n &= 50^2 - 1183 = 2500 - 1183 = 1317 \quad \text{" "} \\
(t+16)^2 - n &= 51^2 - 1183 = 1601 - 1183 = 1481 \quad \text{" "} \\
(t+17)^2 - n &= 52^2 - 1183 = 2704 - 1183 = 1521 = 39^2.
\end{aligned}$$

Quindi: $52^2 - 1183 = 39^2$, cioè

$$1183 = 52^2 - 39^2 = (52 + 39)(52 - 39) = 91 \cdot 13$$

Bisogna scomporre 91, per esempio iterando il procedimento di Fermat: $m = 91$, $\sqrt{91} \backsim 9, 53$, $k = 10$,

$$k^2 - 91 = 100 - 91 = 9 = 3^2.$$

Segue che

$$91 = 10^2 - 3^2 = (10 + 3)(10 - 3) = 13 \cdot 7.$$

Allora

$$1183 = 13^2 \cdot 7.$$

Il procedimento di Fermat è un algoritmo, ovvero ha sempre una conclusione (anche se non si sa a priori qual è il numero dei passaggi da effettuare); nel caso in cui il numero n è primo, si conclude con $(\frac{n+1}{2})^2 - n = (\frac{n-1}{2})^2$.

Teorema di Eulero-Fermat

Proposizione 3. *Siano $x, y \in \mathbb{Z}$, $p \in \mathbb{N}$, p primo. Allora*

$$(x + y)^p \equiv x^p + y^p (\mathtt{mod}\ p).$$

La dimostrazione viene omessa.

Teorema 5. *(Piccolo teorema di Fermat) Siano $a \in \mathbb{Z}$, $p \in \mathbb{N}$ un numero primo. Allora*

$$a^p \ \equiv \ a \ (\mathtt{mod}\ p). \tag{6}$$

Dimostrazione. Si suppone in un primo momento che sia $a \geq 0$ e si procede per induzione completa su a. Per $a = 0$, $a^p = 0$ e (6) diviene $0 \ \equiv \ 0$ $(\mathtt{mod}\ p)$, ovviamente vera. Si suppone che (6) sia vera e si prova $(a + 1)^p \ \equiv \ a + 1$ $(\mathtt{mod}\ p)$. Per la proprietà transitiva della congruenza modulo n e l'ipotesi di induzione risulta:

$$(a + 1)^p \ \equiv \ a^p + 1^p \ \equiv \ a + 1 \ (\mathtt{mod}\ p).$$

quindi (6) è verificata quando $a \geq 0$. Se $a < 0$, allora $-a > 0$ e quindi

$$(-a)^p \ \equiv \ (-a) \ (\mathtt{mod}\ p).$$

Segue che:

$$0 = (a + (-a))^p \ \equiv \ a^p + (-a)^p \ \equiv \ a^p + (-a) \ (\mathtt{mod}\ p).$$

Pertanto $a^p + (-a) \ \equiv \ 0$ $(\mathtt{mod}\ p)$ da cui$a^p \ \equiv \ a$ $(\mathtt{mod}\ p)$.

Corollario 1. Siano $a \in \mathbb{Z}$, $p \in \mathbb{N}$ un numero primo. Se $M.C.D.(a, p) = 1$ allora

$$a^{p-1} \equiv 1 (\mathtt{mod}\ p).$$

Dimostrazione. Poiché $p \mid a^p - a$, ovvero $p \mid a(a^{p-1} - 1)$, certamente $p \mid a^{p-1} - 1$, essendo p primo e non potendo essere un divisore di a, per ipotesi.

Esercizio 1. Determinare il resto della divisione di 89741^{527} per 3.

Si osserva che

$$89741 \equiv 2(\texttt{mod } 3)$$

e quindi

$$89741^{527} \equiv 2^{527}(\texttt{mod } 3).$$

Per il corollario, poichè $M.C.D.(2,3) = 1$, si ha $2^{3-1} \equiv 1(\texttt{mod } 3)$ (in questo caso è banale) e pertanto

$$89741^{527} \equiv 2^{527} = (2^2)^{263} \cdot 2 \equiv 1^{263} \cdot 2 = 2(\texttt{mod } 3)$$

per cui il resto è 2.

Esercizio 2. Determinare il resto della divisione di 57432^{1142} per 9.

Si osserva che

$$57432 \equiv 3(\texttt{mod } 9)$$

e quindi

$$57432^{1142} \equiv 3^{1142} \equiv (3^2)^{571} \equiv 0^{571} \equiv 0(\texttt{mod } 9).$$

Definizione 3. Si dice *funzione di Eulero* l'applicazione

$$\varphi : \mathbb{N} - \{0,1\} \to \mathbb{N}$$

tale che $\forall n \in \mathbb{N} - \{0,1\}$, $\varphi(n)$=numero dei numeri minori di n e primi con n.

Osservazione 6. È ovvio che per ogni numero primo p

$$\varphi(p) = p - 1.$$

risultati che seguono viene omessa. La dimostrazione dei

Proposizione 4. *La funzione di Eulero è moltiplicativa, cioè*

$$\forall n, m \in \mathbb{N} - \{0,1\},\ n > 1,\ m > 1 \text{ tali che } M.C.D.(n,m) = 1,$$

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m).$$

Proposizione 5. *Sia p un numero primo. Allora*

$$\varphi(p^h) = p^h - p^{h-1}.$$

Proposizione 6. *Sia $n \in \mathbb{N} - \{0,1\}$, e sia $n = p_1^{h_1} \cdot \ldots \cdot p_s^{h_s}$ la sua fattorizzazione in numeri primi. Allora*

$$\varphi(n) = \varphi(p_1^{h_1}) \cdot \ldots \cdot \varphi(p_s^{h_s}).$$

Teorema 6. *(Eulero) Siano $a \in \mathbb{Z}^*$, $n \in \mathbb{N} - \{0,1\}$, con $M.C.D.(a,n) = 1$. Allora*

$$a^{\varphi(n)} \equiv 1(\texttt{mod } n).$$

Esercizio 3. Determinare il resto della divisione di 190^{597} per 17.

Bisogna esprimere 190^{597} (mod 17). Si osserva prima che

$$190 \equiv 3(\text{mod } 17).$$

Inoltre, è noto che $a^{p-1} \equiv 1(\text{mod } p)$, se $M.C.D.(a,p) = 1$. Quindi nel caso in esame

$$3^{16} \equiv 1(\text{mod } 17).$$

Allora

$$3^{597} = (3^{16})^{37} \cdot 3^5 \equiv 1^{37} \cdot 3^5 = 3^5(\text{mod } 17).$$

Si vede facilmente che $3^5 = 238 \equiv 5(\text{mod } 17)$, e quindi il resto è 5.

Esercizio 4. Determinare le ultime due cifre del numero 523^{321}.

Si deve ridurre 523^{321} (mod 100). Si osserva che

$$523 \equiv 23(\text{mod } 100)$$

e quindi

$$523^{321} \equiv 23^{321}(\text{mod } 100).$$

Poichè $M.C.D.(23,100) = 1$, si può usare il teorema di Eulero, secondo il quale

$$23^{\varphi(100)} \equiv 1(\text{mod } 100). \tag{7}$$

Per le proprietà della funzione di Eulero si ha

$$\varphi(100) = \varphi(5^2)\varphi(2^2) = (5^2 - 5) \cdot (2^2 - 2) = 20 \cdot 2 = 40$$

pertanto (7) diventa

$$23^{40} \equiv 1(\text{mod } 100).$$

D'altra parte $321 = 40 \cdot 8 + 1$ e quindi

$$23^{321} = (23^{40})^8 \cdot 23 \equiv 1^8 \cdot 23 = 23(\text{mod } 100)$$

In conclusione $523^{321} \equiv 23(\text{mod } 100)$.

Esercizio 5. Determinare le ultime 3 cifre del numero 173^{31}.

Per determinare le ultime 3 cifre del numero 173^{31}, bisogna ridurlo (mod 1000). Si può osservare che $\varphi(1000) = 400$ e che l'esponente è $31 < 400$, per cui non si può usare il teorema di Eulero. Potrebbe essere conveniente trovare la quarta potenza di 173, in modo da avere:

$$173^{31} = 173^{28+3} = 173^{28} \cdot 173^3 = (173^4)^7 \cdot 173^3 = (895.745.041)^7 \cdot 5.177.717.$$

Ma $895.745.041 \equiv 41(\text{mod } 1000)$, $5.177.717 \equiv 717$ (mod 1000) per cui, usando compatibilità delle congruenze (mod n) ($n \in \mathbb{N}^*$) con il prodotto e la proprietà seguente:

$$\forall a, a', b \in \mathbb{Z},\ a \equiv a'\ (\text{mod } n) \implies ab \equiv a'b\ (\text{mod } n)$$

si ottiene $(895.745.041)^7 \cdot 5.177.717 \equiv (41)^7 \cdot 717 \pmod{1000}$. D'altra parte, $41^6 = 4.750.104.241 \equiv 241 \pmod{1000}$, per cui

$$173^{31} \equiv (41)^7 \cdot 717 \equiv 241 \cdot 41 \cdot 717 \pmod{1000}.$$

A questo punto, poichè $241 \cdot 41 \cdot 717 = 7.084.677 \equiv 677 \pmod{1000}$, le ultime 3 cifre di 173^{31} sono 677. Si osservi che, naturalmente, si può procedere in modo diverso, per esempio partendo dalla terza potenza di 173; si consiglia di rifare l'esercizio seguendo questa strada.

UN'APPLICAZIONE INFORMATICA DELL'ARITMETICA MODULARE: IL SISTEMA CRITTOGRAFICO RSA

Fin dall'antichità si è sentita l'esignza di trasmettere messaggi in modo nascosto: per questo nasce la crittografia. Fino a pochi decenni fa, i sistemi crittografici erano basati su sistemi di codifica e decodifica dei messaggi a chiave simmetrica: chi inviava i messaggi e chi li riceveva aveva a disposizione la stessa chiave. Il sistema crittografico RSA attualmente in uso si basa invece sul principio della *chiave asimmetrica*. Il nome RSA deriva dalle iniziali di Ronald Rivest, Adi Shamir e Leonard Adleman che lo hanno realizzato (anche se James Ellis e Clifford Cocks avevano in precedenza trovato un sistema basato sugli stessi principi, ma avevano tenuto segreto il risultato della loro scoperta).
Prima di tutto le lettere vengono rappresentate da numeri in codice. Per esempio Nell'American Standard Code for Information Interchange le lettere vengono rappresentate dai numeri da 065 a 090: quindi la parola ALA viene scritta come:

$$065076065.$$

Ogni utente B deve scegliere una coppia di numeri (n_B, e_B) in modo che n_B sia il prodotto di due numeri primi distinti molto grandi, $n_B = p_B \cdot q_B$, e inoltre

$$M.C.D.(e_B, p_B - 1) = 1, \quad M.C.D.(e_B, q_B - 1) = 1.$$

La coppia (n_B, e_B) è pubblica, ma non è pubblica la scomposizione di n_B. La segretezza di questo sistema sta proprio in questo: B deve costruire n_B scegliendo due numeri primi p_B e q_B molto grandi (anche di 13-14 cifre) e moltiplicandoli. Come si fa a trovare un numero primo? si prende un numero dispari m e si sottopone a certi test di primalità: se un test viene superato va bene, altrimenti si prova con $m + 2$. La coppia (n_B, e_B) dà a B la chiave segreta per decodificare i messaggi: si tratta del numero d_B, soluzione della congruenza lineare

$$e_B \; x \equiv 1 (\mathtt{mod}\ \varphi(n_B)) \tag{8}$$

e tale che $0 < d_B < \varphi(n_B)$. Sicuramente (8) ammette soluzione visto che

$$\varphi(n_B) = (p_B - 1)(q_B - 1)$$

e quindi

$$M.C.D.(e_B, \varphi(n_B)) = M.C.D.(e_B, (p_B - 1)(q_B - 1)) = 1.$$

Inoltre questa soluzione è unica ($\mathtt{mod}\ \varphi(n_B)$). Quindi B è l'unico che può conoscere la chiave d_B tale che:

$$e_B \; d_B \equiv 1 (\mathtt{mod}\ \varphi(n_B)), \quad 0 < d_B < \varphi(n_B)$$

perchè soltanto B conosce $\varphi(n_B)$. Da ciò segue che esiste $k \in \mathbb{Z}$ tale che

$$e_B \; d_B = 1 + \varphi(n_B).$$

Si supponga che l'utente A debba inviare il messaggio M all'utente B. Allora consulta gli elenchi ufficiali e trova la coppia (n_B, e_B). Se il messaggio è più lungo di n_B, A può spezzare M in modo standard in più messaggi. Quindi si può supporre che

$$M < n_B, \quad M.C.D.(M, n_B) = 1.$$

Il messaggio codificato che A invia a B è M' tale che

$$M' \equiv M^{e_B} (\mathtt{mod}\ n_B).$$

Il punto fondamentale è:

$$M \equiv M'^{d_B} (\mathtt{mod}\ n_B), \tag{9}$$

che si dimostra usando il Teorema di Eulero: risulta infatti che

$$M^{\varphi(n_B)} \equiv 1 (\mathtt{mod} n_B),$$

da cui segue:

$$M'^{d_B} \equiv (M^{e_B})^{d_B} = M^{e_B d_B} = M^{1+\varphi(n_B)k} = M \cdot (M^{\varphi(n_B)})^k \equiv M (\mathtt{mod}\ n_B) \tag{10}$$

Quindi B, trovando una soluzione della congruenza lineare $x \equiv M'^{d_B} (\mathtt{mod}\ n_B)$, avrà decodificato il messaggio.
Il sistema RSA viene usato anche per l'autenticazione delle firme. L'utente A manda un messaggio M all'utente B e lo fa seguire dalla propria firma F, ma nella forma:

$$M_1 \equiv F^{d_A} (\mathtt{mod}\ n_A),$$

cioè A invia $M + M_1$. B non riesce a codificare la seconda parte del messaggio, ma sa che proviene da A e ne deve controllare l'autenticità. Allora controlla che

$$M_1^{e_A} \equiv F (\mathtt{mod}\ n_A).$$

Infatti, si prova che $M_1^{e_A} \equiv (F^{d_A})^{e_A} = F^{d_A e_A} \equiv F (\mathtt{mod}\ n_A)$.

Esercizio 6. L'utente A vuole inviare il messaggio $M = 5$ all'utente B, la cui coppia identificativa è

$$(n_B = 77, e_B = 13).$$

Allora soltanto B sa che $n_B = 11 \cdot 7$ e quindi $\varphi(n_B) = \varphi(11)\varphi(7) = 10 \cdot 6 = 60$. Pertanto soluzione $d_B < 60$ della congruenza lineare

$$13x \equiv 1 (\mathtt{mod}\ 60) \tag{11}$$

è la chiave per la decodifica dei messaggi. Per risolvere (11), si può usare l'algoritmo delle divisioni successive:

$$\begin{aligned} 60 &= 13 \cdot 4 + 8 \\ 13 &= 8 \cdot 1 + 5 \\ 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Quindi:

$$\begin{aligned} 1 &= 3 + 2 \cdot (-1) = 3 + (5 + 3(-1)) \cdot (-1) = 3 + 5 \cdot (-1) + 3 = 3 \cdot 2 + 5 \cdot (-1) \\ &= (8 + 5 \cdot (-1)) \cdot 2 + \cdot(-1) = 8 \cdot 2 + 5 \cdot (-2) + 5 \cdot (-1) = 8 \cdot 2 + 5 \cdot (-3) \\ &= 8 \cdot 2 + (13 + 8 \cdot (-1)) \cdot (-3) = 8 \cdot 2 + 13 \cdot (-3) + 8 \cdot 3 = 8 \cdot 5 + 13 \cdot (-3) \\ &= (60 + 13 \cdot (-4)) \cdot 5 + 13 \cdot (-3) = 60 \cdot 5 + 13 \cdot (-23), \end{aligned}$$

Allora $1 = 13 \cdot (-23) + 60 \cdot 5$ e quindi -23 è una soluzione. La più piccola soluzione positiva è $-23 + 60 = 37$, per cui la chiave è

$$d_B = 37.$$

L'utente A dovrà inviare a B il messaggio

$$M' \equiv M^{e_B} (\mathtt{mod}\ n_B).$$

e quindi deve trovare x tale che

$$x \equiv 5^{13} (\mathtt{mod}\ 77).$$

Per esempio, usando una comune calcolatrice, si vede che $5^6 = 15.625$ e che

$$15.625 = 202 \cdot 77 + 71,$$

ovvero $15.625 \equiv 71 (\mathtt{mod}\ 77)$. Quindi

$$5^{13} = 5^{6 \cdot 2 + 1} = (5^6)^2 \cdot 5 = (15.625)^2 \cdot 5 \equiv 71^2 \cdot 5 (\mathtt{mod}\ 77).$$

Sempre effettuando il calcolo su una calcolatrice, si ha: $71^2 \cdot 5 = 25.205 = 327 \cdot 77 + 26$, per cui

$$71^2 \cdot 5 \equiv 26 (\mathtt{mod}\ 77).$$

Allora A invia a B il messaggio $M' = 26$. A questo punto B deve decodificare il messaggio ricevuto usando la sua chiave $d_B = 37$, che solo lui conosce, e usando (9). Quindi deve cercare x tale che $x \equiv 26^{37} (\mathtt{mod}\ 77)$. Si vede che $26^6 = 308.915.776 = 4.011.893 \cdot 77 + 15$, per cui $26^6 \equiv 15 (\mathtt{mod}\ 77)$. Allora:

$$26^{37} = 26^{6 \cdot 6 + 1} = (26^6)^6 \cdot 26 \equiv 15^6 \cdot 26 (\mathtt{mod}\ 77).$$

D'altra parte $15^6 = 11.390.625$ e $15^6 \cdot 26 = 296.156.250 = 3.846.185 \cdot 77 + 5$ e quindi

$$26^{37} \equiv 5 (\mathtt{mod}\ 77),$$

e quindi B ha decodificato il messaggio M'.