TEORIA DEI NUMERI

ARITMETICA

Bézout, congruenze e divisori:
l'aritmetica delle olimpiadi

Prof. A. Perna

IllogicoMatematico

Indice

1 Cosa serve prima di partire

Questo capitolo è diverso dagli altri: non serve a essere promossi. Serve a chi fa le **olimpiadi di matematica**, dove la teoria dei numeri è una delle quattro aree di gara, e a chi ha finito il biennio e ha il sospetto che la matematica sia qualcosa di più dei conti.

Qui per la prima volta ci sono **teoremi con le dimostrazioni**. Sono corte e si capiscono: leggile, non saltarle. È la parte che vale il capitolo.

Cosa devi già sapere

- **La divisione con resto**: $47 = 5 \cdot 9 + 2$. Il resto è sempre $0 \leq r < d$ (minore del divisore, e mai negativo).
- **Numeri primi e scomposizione**: $360 = 2^3 \cdot 3^2 \cdot 5$. Un numero è primo se ha esattamente due divisori, 1 e sé stesso — quindi 1 non è primo.
- **MCD e mcm** come si facevano alle medie: dalla scomposizione, fattori comuni con l'esponente minore (per il MCD) e tutti con l'esponente maggiore (per il mcm).
- **Le potenze**: $a^m \cdot a^n = a^{m+n}$ e $(a^m)^n = a^{mn}$. Qui servono a ogni riga.

Basta questo. Non serve il principio di induzione: dove capita, la dimostrazione è scritta senza.

2 Divisibilità e divisione euclidea

Formula 2.1: Divisibilità: Dati due interi a e b, si scrive

$$a \mid b$$

e si legge «a **divide** b», se esiste un intero k tale che $b = ak$. Se non è così si scrive $a \nmid b$. La barra **non è una frazione**: $a \mid b$ è un'affermazione (vera o falsa), non un numero.

Esempio Svolto 2.1: Leggere la notazione:
$3 \mid 12$ è vero: $12 = 3 \cdot 4$.
$12 \mid 3$ è falso: non c'è nessun intero k con $3 = 12k$.
$5 \mid 0$ è vero: $0 = 5 \cdot 0$. Ogni numero divide zero.
$0 \mid 5$ è falso: $5 = 0 \cdot k$ non ha soluzioni.

Il verso della barra

«$a \mid b$» vuol dire che **la cosa piccola sta a sinistra**: a è il divisore, b il multiplo. Chi legge $12 \mid 3$ come «12 diviso 3» sbaglia metà degli esercizi del capitolo, perché la notazione dice un'altra cosa.

Formula 2.2: Proprietà della divisibilità: Per ogni a, b, c interi:

1. se $a \mid b$ e $b \mid c$, allora $a \mid c$;
2. se $a \mid b$ e $a \mid c$, allora $a \mid (bx + cy)$ per **ogni** x, y interi.

La seconda è la più usata di tutte: si chiama proprietà delle *combinazioni lineari*.

Esempio Svolto 2.2: Dimostrare la seconda proprietà:
Ipotesi: $a \mid b$ e $a \mid c$, cioè $b = ah$ e $c = ak$ per certi interi h e k.
Conto:

$$bx + cy = ahx + aky = a(hx + ky)$$

Conclusione: $hx + ky$ è un intero, quindi $bx + cy$ è a per qualcosa: $\mathbf{a \mid (bx + cy)}$.
È una dimostrazione di tre righe, e la userai in mezzo capitolo.

Formula 2.3: Divisione euclidea: Dati a intero e $d > 0$, esistono **unici** q (quoziente) e r (resto) tali che

$$a = dq + r \qquad \text{con } 0 \leq r < d$$

La condizione sul resto è ciò che rende la coppia unica.

Esempio Svolto 2.3: Anche con i negativi:
$47 : 5$ dà $47 = 5 \cdot 9 + 2$, con $q = 9$ e $r = 2$.
$-47 : 5$ **non** dà $q = -9$, $r = -2$: il resto dev'essere positivo. Si scrive

$$-47 = 5 \cdot (-10) + 3$$

con $\mathbf{q = -10,\ r = 3}$. Il resto di -47 modulo 5 è 3, non -2.

3 MCD e algoritmo di Euclide

Alle medie il MCD si trova scomponendo. Ma scomporre numeri grandi è *difficilissimo* — su questo si regge la crittografia — mentre il MCD si può trovare in fretta, con un algoritmo vecchio di 2300 anni.

Formula 3.1: Il lemma su cui si regge tutto: Se $a = dq + r$, allora

$$\text{MCD}(a, d) = \text{MCD}(d, r)$$

Cioè: il MCD non cambia se si sostituisce il numero grande con il resto.

Perché vale

Ogni divisore comune di d e r divide anche $dq + r = a$ (proprietà delle combinazioni lineari), quindi è divisore comune di a e d. E viceversa, ogni divisore comune di a e d divide $a - dq = r$. Le due coppie hanno *gli stessi* divisori comuni, quindi lo stesso massimo.

Metodo 3.1: Algoritmo di Euclide:

1. Dividi il più grande per il più piccolo e prendi il resto.
2. Ripeti con il divisore e il resto appena trovato.
3. Vai avanti finché il resto è 0.
4. L'**ultimo resto non nullo** è il MCD.

Esempio Svolto 3.1: MCD di 1071 e 462:

$$\begin{aligned} 1071 &= 2 \cdot 462 + 147 \\ 462 &= 3 \cdot 147 + 21 \\ 147 &= 7 \cdot 21 + 0 \end{aligned}$$

L'ultimo resto non nullo è **21**: $\text{MCD}(1071, 462) = 21$.
Controllo: $1071 = 21 \cdot 51$ e $462 = 21 \cdot 22$; e $51 = 3 \cdot 17$, $22 = 2 \cdot 11$ non hanno fattori comuni, quindi 21 è davvero il massimo.
Quanto è veloce: tre divisioni. Scomporre 1071 e 462 ne avrebbe richieste molte di più, e con numeri di trenta cifre sarebbe stato impossibile.

Formula 3.2: Legame fra MCD e mcm:

$$\text{MCD}(a, b) \cdot \text{mcm}(a, b) = a \cdot b$$

Trovato il MCD con Euclide, il mcm viene gratis.

4 L'identità di Bézout

Ecco il primo teorema serio del capitolo, e lo strumento che apre tutto il resto.

Formula 4.1: Identità di Bézout: Per ogni coppia di interi a, b non entrambi nulli, esistono interi x, y tali che

$$ax + by = \text{MCD}(a, b)$$

I coefficienti x e y **non sono unici**, ma esistono sempre.

Perché esistono, senza calcolarli

Si guardi l'insieme di tutti i numeri della forma $ax + by$ con x, y interi, e fra quelli *positivi* si prenda il più piccolo: chiamiamolo $e = ax_0 + by_0$.
Dividendo a per e si ha $a = eq + r$ con $0 \leq r < e$, e allora

$$r = a - eq = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0q)$$

cioè anche r è della forma $ax + by$. Ma $r < e$ ed e era il più piccolo positivo: quindi $r = 0$, cioè $e \mid a$. Allo stesso modo $e \mid b$: dunque e è un divisore comune.
D'altra parte ogni divisore comune di a e b divide $ax_0 + by_0 = e$, quindi e è proprio il *massimo* divisore comune.

Metodo 4.1: Euclide esteso: trovare x e y:

1. Fai l'algoritmo di Euclide e **tieni tutte le righe**.
2. Parti dalla penultima riga e scrivi il MCD come «resto = dividendo − quoziente × divisore».
3. Risali una riga alla volta, sostituendo ogni resto con la sua espressione, e raccogliendo a e b.
4. Alla fine resta $ax + by = \text{MCD}$: leggi x e y.

Esempio Svolto 4.1: Bézout per 1071 e 462:
1. Le righe di Euclide (dall'esempio precedente):

$$1071 = 2 \cdot 462 + 147 \qquad 462 = 3 \cdot 147 + 21$$

2. Parto dalla penultima e isolo il resto:

$$21 = 462 - 3 \cdot 147$$

3. Risalgo: dalla prima riga, $147 = 1071 - 2 \cdot 462$. Sostituisco:

$$21 = 462 - 3\,(1071 - 2 \cdot 462)$$

4. Raccolgo 1071 e 462:

$$21 = 462 - 3 \cdot 1071 + 6 \cdot 462 = -3 \cdot 1071 + 7 \cdot 462$$

$$\mathbf{21 = 1071 \cdot (-3) + 462 \cdot 7}$$

5. Controllo: $-3213 + 3234 = 21$. Torna.

Non si semplificano i numeri mentre si risale

Nel passaggio 4 la tentazione è calcolare $3 \cdot 1071 = 3213$ e andare avanti coi numeri. Non farlo: si perde di vista chi è a e chi è b, e alla fine non si sa più leggere x e y. Si tengono 1071 e 462 scritti così come sono, e si sommano solo i *coefficienti*.

Formula 4.2: Il corollario più utile:

$$\mathrm{MCD}(a,b) = 1 \iff \text{esistono } x, y \text{ con } ax + by = 1$$

Due numeri con MCD 1 si dicono **coprimi**. Questa equivalenza è il motore dell'inverso modulare (par. 10).

5 Equazioni diofantee lineari

Un'equazione diofantea è un'equazione di cui si cercano le soluzioni **intere**. La più semplice è $ax + by = c$, e Bézout dice tutto quello che serve.

Formula 5.1: Quando $ax + by = c$ ha soluzioni: L'equazione ha soluzioni intere **se e solo se**

$$\mathrm{MCD}(a,b) \mid c$$

e in quel caso ne ha **infinite**. Detto $d = \mathrm{MCD}(a,b)$ e (x_0, y_0) una soluzione qualsiasi, tutte le altre sono

$$x = x_0 + \frac{b}{d}\,t \qquad y = y_0 - \frac{a}{d}\,t \qquad t \in \mathbb{Z}$$

Esempio Svolto 5.1: Una che si risolve:
1. Risolvo $6x + 15y = 9$.
2. Esiste? $\text{MCD}(6, 15) = 3$, e $3 \mid 9$: sì.
3. Semplifico dividendo tutto per 3: $2x + 5y = 3$.
4. Una soluzione a occhio: $x = -1$, $y = 1$ dà $-2 + 5 = 3$.
5. Tutte le soluzioni:

$$\mathbf{x = -1 + 5t}, \quad \mathbf{y = 1 - 2t}, \qquad t \in \mathbb{Z}$$

6. Controllo con $t = 2$: $x = 9$, $y = -3$, e $6 \cdot 9 + 15 \cdot (-3) = 54 - 45 = 9$. Torna.

Esempio Svolto 5.2: Una che non si risolve:
$6x + 15y = 7$: il primo membro è sempre multiplo di 3 (lo sono sia $6x$ sia $15y$), mentre 7 non lo è.

Nessuna soluzione intera

Non serve provare: il criterio $\text{MCD}(6, 15) = 3 \nmid 7$ chiude la questione in una riga.

Una soluzione non è la soluzione

Trovato $x = -1$, $y = 1$, l'esercizio **non è finito**: le soluzioni sono infinite e la risposta è la famiglia con il parametro t. Scriverne una sola è come rispondere «2» a «quali numeri sono pari?».

6 Primi e fattorizzazione unica

Formula 6.1: Teorema fondamentale dell'aritmetica: Ogni intero $n > 1$ si scrive in modo **unico** (a meno dell'ordine) come prodotto di potenze di primi:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$$

È il motivo per cui tutto il capitolo funziona: la fattorizzazione è una carta d'identità del numero.

Formula 6.2: Il lemma di Euclide: Se p è primo e $p \mid ab$, allora $p \mid a$ oppure $p \mid b$.
Attenzione: è **falso** per i non primi. $6 \mid 4 \cdot 9 = 36$, ma $6 \nmid 4$ e $6 \nmid 9$.

Esempio Svolto 6.1: Fino a dove provare:
Per sapere se 211 è primo non serve provare tutti i numeri fino a 210: basta arrivare a $\sqrt{211} \approx 14{,}5$.
Se $n = ab$ con $a \leq b$, allora $a \leq \sqrt{n}$: un divisore piccolo c'è sempre, se ce n'è uno.
Provo i primi fino a 14: $2, 3, 5, 7, 11, 13$. Nessuno divide 211 (è dispari, la somma delle cifre è 4, non finisce per 0 o 5, e le divisioni per 7, 11, 13 danno resto). Quindi 211 è primo.

7 Numero e somma dei divisori

Ecco la prima applicazione seria della fattorizzazione: contare i divisori *senza elencarli*.

Formula 7.1: Le due funzioni: Se $n = p_1^{a_1} \cdots p_k^{a_k}$, allora il numero dei divisori è

$$d(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

e la loro somma è

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

dove ogni fattore è la somma $1 + p_i + p_i^2 + \cdots + p_i^{a_i}$.

Perché $d(n)$ è quel prodotto

Un divisore di n è fatto *solo* con i primi di n, ciascuno con esponente da 0 ad a_i. Quindi costruire un divisore vuol dire fare k scelte indipendenti: $a_1 + 1$ possibilità per il primo esponente, $a_2 + 1$ per il secondo, e così via. Il totale è il prodotto.
Per $\sigma(n)$ è lo stesso conto, ma invece di contare le scelte se ne sommano i risultati: sviluppando il prodotto $(1 + p_1 + \dots)(1 + p_2 + \dots)$ si ottengono esattamente tutti i divisori, una volta ciascuno.

Esempio Svolto 7.1: Contare e sommare i divisori di 360:
1. Fattorizzo: $360 = 2^3 \cdot 3^2 \cdot 5$.
2. Quanti sono:

$$d(360) = (3 + 1)(2 + 1)(1 + 1) = 4 \cdot 3 \cdot 2 = \mathbf{24}$$

3. Quanto fanno sommati:

$$\sigma(360) = (1 + 2 + 4 + 8)(1 + 3 + 9)(1 + 5) = 15 \cdot 13 \cdot 6 = \mathbf{1170}$$

4. Controllo parziale: fra i 24 divisori ci sono 1 e 360, e la loro somma da sola fa 361; il totale 1170 è plausibile.

Esempio Svolto 7.2: Perché i quadrati sono speciali:
$36 = 2^2 \cdot 3^2$, quindi $d(36) = 3 \cdot 3 = 9$: un numero **dispari** di divisori.
Non è un caso. I divisori si accoppiano: se $a \mid n$ anche n/a è un divisore, e i due sono diversi *tranne* quando $a = n/a$, cioè $n = a^2$.
Quindi: $\mathbf{d(n)}$ è dispari se e solo se $\mathbf{n}$ è un quadrato perfetto. È un classico da gara.

Contare a occhio

Elencare i divisori di 36 di fretta $(1, 2, 3, 4, 6, 9, 12, 18, 36)$ funziona, ma per 360 o 1260 se ne perde sempre qualcuno. La formula non sbaglia: prima si fattorizza, poi si moltiplicano gli esponenti aumentati di uno.

8 Congruenze

L'idea è semplice e cambia il modo di guardare i numeri: invece del numero, interessa il **resto**.

Formula 8.1: Congruenza modulo m: Dati a, b interi e $m > 1$:

$$a \equiv b \pmod{m} \iff m \mid (a - b)$$

e si legge «a è congruo a b modulo m». Equivale a dire che a e b danno lo **stesso resto** nella divisione per m.

Formula 8.2: Le regole di calcolo: Se $a \equiv b$ e $c \equiv e \pmod{m}$, allora

$$a + c \equiv b + e \qquad a - c \equiv b - e \qquad ac \equiv be \pmod{m}$$

e di conseguenza $a^n \equiv b^n \pmod{m}$ per ogni n naturale.
Somma, sottrazione, prodotto e potenza si comportano bene. La **divisione no**: è il prossimo riquadro.

Esempio Svolto 8.1: Calcolare con i resti:
1. Che resto dà $17 \cdot 23$ diviso per 5?
2. Invece di moltiplicare: $17 \equiv 2$ e $23 \equiv 3 \pmod{5}$, quindi

$$17 \cdot 23 \equiv 2 \cdot 3 = 6 \equiv \mathbf{1} \pmod{5}$$

3. Controllo: $17 \cdot 23 = 391 = 5 \cdot 78 + 1$. Torna, e non ho mai calcolato 391.
4. È tutta qui l'utilità: si lavora con numeri piccoli.

Semplificare è pericoloso

Da $6 \equiv 2 \pmod 4$ **non** segue $3 \equiv 1 \pmod 4$ (sarebbe falso: $3-1=2$ non è multiplo di 4).
La regola giusta: da $ac \equiv bc \pmod m$ si può semplificare c solo se $\text{MCD}(c,m)=1$. Se no, si divide anche il modulo per il MCD.

Esempio Svolto 8.2: Le potenze diventano cicliche:
Qual è l'ultima cifra di 7^{100}? L'ultima cifra è il resto modulo 10.
1. Calcolo le prime potenze modulo 10:

$$7^1 \equiv 7, \quad 7^2 \equiv 49 \equiv 9, \quad 7^3 \equiv 63 \equiv 3, \quad 7^4 \equiv 21 \equiv 1 \pmod{10}$$

2. Da $7^4 \equiv 1$ in poi si ricomincia: il ciclo è lungo 4.
3. $100 = 4 \cdot 25$, quindi $7^{100} = (7^4)^{25} \equiv 1^{25} = \mathbf{1} \pmod{10}$.
L'ultima cifra di 7^{100} è 1 — e non ho calcolato un numero di 85 cifre.

9 I criteri di divisibilità, dimostrati

Alle medie si imparano a memoria. Con le congruenze si *dimostrano* in due righe, e si capisce da dove vengono.

Esempio Svolto 9.1: Il criterio del 3 (e del 9):
1. L'osservazione: $10 \equiv 1 \pmod 3$, e quindi $10^k \equiv 1^k = 1 \pmod 3$ per ogni k.
2. Un numero $n = c_k 10^k + \cdots + c_1 10 + c_0$ diventa

$$n \equiv c_k + \cdots + c_1 + c_0 \pmod 3$$

3. Conclusione: n e la somma delle sue cifre danno lo stesso resto modulo 3. Quindi **3 | n** $\iff$ **3** | somma delle cifre.
4. Con 9 è identico, perché anche $10 \equiv 1 \pmod 9$.
5. Esempio: 4 725 ha somma cifre 18, divisibile per 9: quindi 4725 è divisibile per 9.

Esempio Svolto 9.2: Il criterio dell'11:
1. Qui $10 \equiv -1 \pmod{11}$, e allora $10^k \equiv (-1)^k$: vale 1 per k pari, -1 per k dispari.
2. Quindi n è congruo alla somma delle cifre **a segni alterni**, partendo da destra col più.
3. Esempio: 918 082 dà

$$2-8+0-8+1-9=-22$$

che è multiplo di 11: quindi **11 | 918082**.
4. Controllo: $918082 = 11 \cdot 83462$. Torna.

E il criterio del 7?

Non c'è un criterio comodo, ed è per questo che a scuola non si insegna: modulo 7 le potenze di 10 fanno $1, 3, 2, 6, 4, 5$ e poi si ripetono, un ciclo di sei numeri senza simmetria. Il «criterio del 7» che gira (togliere il doppio dell'ultima cifra) funziona, ma è più lento di una divisione.

10 Inverso modulare ed equazioni congruenziali

Dividere modulo m non si può; moltiplicare per l'inverso sì — quando esiste.

Formula 10.1: Inverso modulare: L'inverso di a modulo m è un intero a^{-1} con

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

Esiste **se e solo se** $\text{MCD}(a, m) = 1$, e in quel caso è unico modulo m.

Il legame con Bézout

Se $\text{MCD}(a, m) = 1$, Bézout dà $ax + my = 1$. Guardando l'uguaglianza modulo m, il termine my sparisce e resta $ax \equiv 1$: quel x *è* l'inverso. Ecco perché l'inverso esiste esattamente quando i due numeri sono coprimi — e come si calcola: con Euclide esteso.

Esempio Svolto 10.1: Trovare l'inverso di 7 modulo 26:
1. Esiste? $\text{MCD}(7, 26) = 1$: sì.
2. Euclide: $26 = 3 \cdot 7 + 5$; $7 = 1 \cdot 5 + 2$; $5 = 2 \cdot 2 + 1$.
3. Risalgo:

$$1 = 5 - 2 \cdot 2 = 5 - 2(7 - 5) = 3 \cdot 5 - 2 \cdot 7 = 3(26 - 3 \cdot 7) - 2 \cdot 7 = 3 \cdot 26 - 11 \cdot 7$$

4. Modulo 26: $-11 \cdot 7 \equiv 1$, quindi l'inverso è $-11 \equiv \mathbf{15} \pmod{26}$.
5. Controllo: $7 \cdot 15 = 105 = 4 \cdot 26 + 1$. Torna.

Metodo 10.1: Risolvere $ax \equiv b \pmod{m}$:

1. Calcola $d = \text{MCD}(a, m)$.
2. Se $d \nmid b$: **nessuna soluzione**, e hai finito.
3. Se $d = 1$: moltiplica per l'inverso di a, e la soluzione è $x \equiv a^{-1}b \pmod{m}$ (una classe sola).

4. Se $d > 1$ e $d \mid b$: dividi tutto per d — compreso il modulo — e risolvi la congruenza più piccola. Le soluzioni modulo m diventano d.

Esempio Svolto 10.2: Una congruenza risolta:
1. Risolvo $7x \equiv 3 \pmod{26}$.
2. $\text{MCD}(7, 26) = 1$: c'è una sola classe di soluzioni.
3. Moltiplico per l'inverso, che è 15:

$$x \equiv 15 \cdot 3 = 45 \equiv \mathbf{19} \pmod{26}$$

4. Controllo: $7 \cdot 19 = 133 = 5 \cdot 26 + 3$. Torna.

11 Piccolo Fermat e teorema di Eulero

Due teoremi che rendono banali certi calcoli mostruosi.

Formula 11.1: Piccolo teorema di Fermat: Se p è **primo** e $p \nmid a$, allora

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

In forma sempre valida (anche se $p \mid a$): $a^p \equiv a \pmod{p}$.

Esempio Svolto 11.1: Una potenza mostruosa:
1. Quanto fa 2^{100} modulo 13?
2. 13 è primo e non divide 2, quindi $2^{12} \equiv 1 \pmod{13}$.
3. Divido l'esponente per 12: $100 = 12 \cdot 8 + 4$.

$$2^{100} = (2^{12})^8 \cdot 2^4 \equiv 1^8 \cdot 16 \equiv 16 \equiv \mathbf{3} \pmod{13}$$

4. Il conto vero sarebbe stato su un numero di 31 cifre.

Formula 11.2: Funzione di Eulero e suo teorema: $\varphi(m)$ conta gli interi da 1 a m coprimi con m. Se $m = p_1^{a_1} \cdots p_k^{a_k}$:

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Teorema di Eulero: se $\text{MCD}(a, m) = 1$, allora

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

Con $m = p$ primo si ha $\varphi(p) = p - 1$: si ritrova Fermat.

Esempio Svolto 11.2: Eulero con modulo non primo:
1. Le ultime due cifre di 3^{40}? Sono il resto modulo 100.
2. $100 = 2^2 \cdot 5^2$, quindi

$$\varphi(100) = 100\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{5}\right) = 100 \cdot \tfrac{1}{2} \cdot \tfrac{4}{5} = \mathbf{40}$$

3. $\mathrm{MCD}(3, 100) = 1$, quindi per Eulero $3^{40} \equiv \mathbf{1} \pmod{100}$: le ultime due cifre sono 01.

Le ipotesi contano

Fermat vuole il modulo **primo**: $a^{m-1} \equiv 1 \pmod{m}$ è falso in generale. Con $m = 4$ e $a = 3$: $3^3 = 27 \equiv 3$, non 1.
Ed entrambi i teoremi vogliono a **coprimo** col modulo: senza quell'ipotesi non c'è nessun inverso e nessun ciclo.

12 Teorema cinese del resto

Il problema è antico: trovare un numero conoscendo i resti che dà con divisori diversi.

Formula 12.1: Teorema cinese del resto: Se $m_1, m_2, \ldots, m_k$ sono **a due a due coprimi**, il sistema

$$x \equiv r_1 \pmod{m_1}, \quad \ldots, \quad x \equiv r_k \pmod{m_k}$$

ha una e una sola soluzione modulo $m_1 m_2 \cdots m_k$.

Metodo 12.1: Risolverlo per sostituzione:

1. Scrivi la prima congruenza in forma di equazione: $x = r_1 + m_1 t$.
2. Sostituiscila nella seconda e risolvi in t (è una congruenza lineare: par. 10).
3. Rimetti t trovato dentro x: ora hai una congruenza sola, modulo $m_1 m_2$.
4. Ripeti con le congruenze rimaste.

Esempio Svolto 12.1: Il problema classico:

Trovare x con

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5, \qquad x \equiv 2 \pmod 7$$

1. Dalla prima: $x = 2 + 3t$.
2. Nella seconda: $2 + 3t \equiv 3 \pmod 5$, cioè $3t \equiv 1 \pmod 5$. L'inverso di 3 modulo 5 è 2 (perché $3 \cdot 2 = 6 \equiv 1$), quindi $t \equiv 2 \pmod 5$, cioè $t = 2 + 5s$.
3. Sostituisco: $x = 2 + 3(2 + 5s) = 8 + 15s$. Ho unito le prime due: $x \equiv 8 \pmod{15}$.
4. Nella terza: $8 + 15s \equiv 2 \pmod 7$. Siccome $8 \equiv 1$ e $15 \equiv 1$, diventa $1 + s \equiv 2$, cioè $s \equiv 1 \pmod 7$): $s = 1 + 7u$.
5. Rimetto dentro: $x = 8 + 15(1 + 7u) = 23 + 105u$.

$$\mathbf{x \equiv 23 \pmod{105}}$$

6. Controllo: $23 = 3 \cdot 7 + 2$ ✓, $23 = 5 \cdot 4 + 3$ ✓, $23 = 7 \cdot 3 + 2$ ✓.

I moduli devono essere coprimi

Con $x \equiv 1 \pmod 4$ e $x \equiv 2 \pmod 6$ il teorema non si applica (4 e 6 non sono coprimi), e infatti non c'è soluzione: la prima chiede x dispari, la seconda x pari. Prima di partire si controllano i MCD.

13 Tecniche da gara, e come si controlla

Tre mosse che risolvono buona parte dei problemi di teoria dei numeri alle gare.

Metodo 13.1: Le tre mosse:

1. **Guarda i resti.** Se un problema parla di divisibilità, lavora modulo qualcosa: spesso modulo 3, 4, 8 o 9. Molte dimostrazioni di impossibilità si fanno così.
2. **Cerca il ciclo.** Le potenze modulo m si ripetono: trova il periodo con Fermat o a mano, poi riduci l'esponente.
3. **Fattorizza.** Se compaiono divisori, quadrati o prodotti, la fattorizzazione dice quasi sempre la risposta — come per $d(n)$ e per i quadrati perfetti.

Esempio Svolto 13.1: Una dimostrazione di impossibilità:
Dimostra che $n^2 + 1$ non è mai divisibile per 3.
1. Guardo i resti di n modulo 3: può essere 0, 1 o 2.

2. Calcolo n^2 nei tre casi:

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 = 4 \equiv 1 \pmod 3$$

Quindi un quadrato è sempre $\equiv 0$ o 1 modulo 3, mai 2.
3. Allora $n^2 + 1 \equiv 1$ oppure 2: non è **mai** $\equiv 0$.

$$\mathbf{3 \nmid n^2 + 1} \text{ per ogni } \mathbf{n}$$

4. Tre casi controllati, e vale per infiniti numeri: è la potenza dell'aritmetica modulare.

Metodo 13.2: Il controllo, qualunque sia l'esercizio:

1. **Bézout**: sostituisci x e y e verifica che $ax + by$ faccia il MCD.
2. **Diofantee**: prendi due valori di t e controlla che le coppie risolvano davvero.
3. **Congruenze**: sostituisci la soluzione trovata e controlla il resto con una divisione vera.
4. **Divisori**: se $d(n)$ è piccolo, elencali; se no, rifai la fattorizzazione.

Nessuno di questi controlli costa più di un minuto, e in gara un risultato controllato vale il doppio di uno veloce.

Indice analitico