Aritmetica modulare di base

Fermat's Christmas Theorem series

2025-12-14

Introduzione

Siamo alla fermata dell'autobus, in attesa che arrivi il nostro autobus. Sul tabellone è scritto che ci sono tre autobus in arrivo a breve:

- L'autobus A arriva tra 2 minuti;
- L'autobus B arriva tra 5 minuti;
- L'autobus C arriva tra 10 minuti.

Ovviamente non siamo fortunati, e dobbiamo aspettare l'autobus C. Mentre guardiamo gli autobus arrivare e ripartire, ci chiediamo:

Domanda: Gli autobus A, B e C arriveranno mai simultaneamente?

Leggiamo sul tabellone che:

- L'autobus A passa ogni 3 minuti;
- L'autobus B passa ogni 24 minuti;
- L'autobus C passa ogni 23 minuti.

Abbiamo con noi il quaderno, quindi affrontiamo il problema nel modo brutale. Elenchiamo tutti gli istanti in cui passano gli autobus A, B e C (i numeri sono i tempi di attesa in minuti):

- L'autobus A passerà tra
$$2, 5, 8, 11, 14, 17, \ldots$$
- L'autobus B passerà tra
$$5, 29, 53, 77, 101, \ldots$$
- L'autobus C passerà tra
$$10, 33, 56, 79, 102, \ldots$$

Non sappiamo se, continuando questa lista, troveremo un numero comune a tutte e tre le liste (il che significherebbe un arrivo simultaneo). Questo metodo è tedioso, quindi vogliamo un modo più efficiente per risolvere il problema in generale.

Traduciamo il problema in un contesto matematico. Che cosa significa che l'autobus A passa ogni 3 minuti e arriva tra 2 minuti? Significa che i possibili istanti (in minuti) in cui l'autobus A passerà sono della forma $3 \cdot n + 2$, dove n è un intero non negativo (cioè $n = 0, 1, 2, \ldots$; convinciti di questo). Infatti, tutti i numeri che abbiamo elencato per A sono di questa forma.

Allo stesso modo, i tempi di attesa per l'autobus B sono della forma $24 \cdot k + 5$ e i tempi di attesa per l'autobus C sono della forma $23 \cdot \ell + 10$. Quindi, trovare un tempo x (sempre in minuti) in cui A, B e C arrivano simultaneamente significa trovare tre interi non negativi n, k, ℓ tali che

$$x = 3 \cdot n + 2, \qquad x = 24 \cdot k + 5, \qquad x = 23 \cdot \ell + 10.$$

In altre parole, il tempo totale di attesa x deve essere di tutte e tre le forme nello stesso momento.

Congruenze di interi

Rendiamo la notazione un po' migliore e più utile.

Definizione: Siano n, m e q interi, con $q > 0$. Scriviamo

$$n \equiv_q m$$

se il resto della divisione di n per q e il resto della divisione di m per q sono uguali.

La scrittura $n \equiv_q m$ si legge: "n è *congruente* a m *modulo* q".

Example 0.1. Consideriamo $n = 14$ e $q = 3$. Allora $14 \equiv_3 2$. Infatti

$$14 = 3 \cdot 4 + 2$$

ha resto 2, e anche 2 ha resto 2 quando viene diviso per 3.

Remark 0.1. Per ogni intero n e ogni q con $q > 0$, se r è il resto della divisione di n per q, allora $n \equiv_q r$.

Ora arriva il fatto fondamentale che rende le congruenze davvero utili.

Proposition 0.1. *Siano n, m e q interi con $q > 0$. Allora $n \equiv_q m$ se e solo se q divide $n - m$.*

Proof. Supponiamo che $n \equiv_q m$. Allora il resto della divisione di n per q è lo stesso del resto della divisione di m per q. Chiamiamo questo resto comune r.

Per la divisione euclidea, esistono interi k e ℓ tali che

$$n = q \cdot k + r, \qquad m = q \cdot \ell + r,$$

con $0 \leq r < q$.

Sottraiamo la seconda equazione dalla prima:

$$n - m = (q \cdot k + r) - (q \cdot \ell + r).$$

Ora semplifichiamo:

$$n - m = q \cdot k + r - q \cdot \ell - r,$$

e cancellando r a destra otteniamo

$$n - m = q \cdot k - q \cdot \ell.$$

Raccogliamo q:

$$n - m = q \cdot (k - \ell).$$

Questo significa esattamente che q divide $n - m$.

Viceversa, supponiamo che q divida $n - m$. Questo significa che esiste un intero t tale che

$$n - m = q \cdot t.$$

Riordiniamo:

$$n = m + q \cdot t.$$

Ora dividiamo m per q: per la divisione euclidea esistono interi ℓ e r con $0 \leq r < q$ tali che

$$m = q \cdot \ell + r.$$

Sostituiamo nella formula precedente:

$$n = (q \cdot \ell + r) + q \cdot t = q \cdot (\ell + t) + r.$$

Quindi, dividendo m per q otteniamo resto r, e dividendo n per q otteniamo ancora resto r. Dunque $n \equiv_q m$. □

Facciamo ora qualche esempio. Osserviamo che $14 \equiv_3 2$ e che $19 \equiv_3 1$. Ci chiediamo che cosa sia

$$14 + 19 \equiv_3 \ ?$$

Forse l'hai già intuito: abbiamo

$$14 + 19 \equiv_3 2 + 1.$$

Quindi stiamo dicendo che

$$33 \equiv_3 3.$$

Ma sappiamo anche che $3 \equiv_3 0$ (infatti 3 ha resto 0 quando viene diviso per 3), quindi

$$33 \equiv_3 0.$$

Questo significa che 33 è divisibile per 3.

Chiediamoci lo stesso per il prodotto:

$$14 \cdot 19 \equiv_3 \ ?$$

Siamo di nuovo fortunati: otteniamo

$$14 \cdot 19 \equiv_3 2 \cdot 1,$$

il che significa che

$$266 \equiv_3 2,$$

cioè 266 ha resto 2 quando viene diviso per 3.

Enunciamo precisamente questo fatto nella proposizione seguente.

Proposition 0.2. *Siano n, m, n', m' e q interi con $q > 0$. Se $n \equiv_q m$ e $n' \equiv_q m'$, allora*

$$n + n' \equiv_q m + m'$$

e

$$n \cdot n' \equiv_q m \cdot m'.$$

Parte facile del Teorema di Natale di Fermat

Proposition 0.3. *Sia n un intero dispari che può essere scritto come somma di due quadrati. Allora $n \equiv_4 1$, cioè n ha resto 1 quando viene diviso per 4.*

Remark 0.2. In particolare, il teorema ci dice anche che se p è un primo dispari che può essere scritto come somma di due quadrati, allora ha resto 1 quando viene diviso per 4, che è parte di ciò che afferma il Teorema di Natale di Fermat.

Proof. Se n può essere scritto come somma di due quadrati, significa che esistono interi a, b tali che

$$n = a^2 + b^2.$$

Osserviamo che n è dispari, quindi ha resto 1 quando viene diviso per 2, cioè

$$n \equiv_2 1.$$

Quindi

$$a^2 + b^2 \equiv_2 1.$$

Se sia a sia b fossero dispari, allora $a \equiv_2 1$ e $b \equiv_2 1$, quindi

$$a^2 \equiv_2 1, \qquad b^2 \equiv_2 1,$$

il che implicherebbe

$$a^2 + b^2 \equiv_2 1 + 1 \equiv_2 2 \equiv_2 0,$$

e quindi $n \equiv_2 0$, impossibile perché n è dispari.

Allo stesso modo, se a e b fossero entrambi pari, allora $a^2 + b^2 \equiv_2 0$, che è ancora impossibile.

Dunque uno è dispari e l'altro è pari. Chiamiamo a quello dispari e b quello pari. Abbiamo

$$a \equiv_2 1, \qquad b \equiv_2 0.$$

Poiché b è pari, quando dividiamo b per 4 otteniamo resto 0 oppure resto 2 (altrimenti sarebbe dispari). Quindi

$$b \equiv_4 0 \quad \text{oppure} \quad b \equiv_4 2.$$

In entrambi i casi otteniamo

$$b^2 \equiv_4 0.$$

Allo stesso modo, poiché a è dispari, abbiamo

$$a \equiv_4 1 \quad \text{oppure} \quad a \equiv_4 3.$$

In entrambi i casi (controlla!) otteniamo

$$a^2 \equiv_4 1.$$

Quindi

$$a^2 + b^2 \equiv_4 1 + 0 \equiv_4 1,$$

il che significa che

$$n \equiv_4 1.$$

□

Numeri invertibili modulo q

Ricordiamo che cos'è il massimo comun divisore.

Definizione: Siano n e m due interi diversi da 0. Il massimo comun divisore $\gcd(n, m)$ è il prodotto dei primi comuni che compaiono nelle fattorizzazioni di n e m, presi con la potenza più piccola.

Example 0.2. Calcoliamo il massimo comun divisore tra 72 e 540. Abbiamo

$$72 = 2^3 \cdot 3^2, \qquad 540 = 2^2 \cdot 3^3 \cdot 5,$$

quindi

$$\gcd(72, 540) = 2^2 \cdot 3^2.$$

Supponiamo di avere due interi n e q con $q > 0$. Ci chiediamo quando esiste un altro intero m tale che

$$n \cdot m \equiv_q 1.$$

Proviamo qualche esempio:

- Se $n = 4$ e $q = 7$, allora
$$4 \cdot 2 \equiv_7 1.$$
- Se $n = 4$ e $q = 6$, allora non possiamo trovare un tale m.
- Se $n = 3$ e $q = 9$, non possiamo trovare un tale m.
- Se $n = 3$ e $q = 5$, allora
$$3 \cdot 2 \equiv_5 1.$$

Prova qualche esempio anche tu.

Definizione: Siano n e q interi con $q > 0$. Diciamo che n è *invertibile modulo* q se esiste un intero m tale che

$$n \cdot m \equiv_q 1.$$

La risposta alla domanda è data dalla proposizione seguente.

Proposition 0.4. *Siano n e q interi con $q > 0$. Allora n è invertibile modulo q se e solo se* $\gcd(n, q) = 1$.

Teorema Cinese del Resto

Ora enunciamo il teorema che ci permetterà di risolvere in modo efficiente il problema degli autobus.

Theorem 0.1. *Siano* $s, t > 1$ *interi con* $\gcd(s,t) = 1$*. Allora per ogni intero* a *e ogni intero* b *esiste un intero* x *tale che*

$$x \equiv_s a \qquad e \qquad x \equiv_t b.$$

Proof. Vogliamo

$$x \equiv_s a \qquad \text{e} \qquad x \equiv_t b.$$

La prima congruenza $x \equiv_s a$ significa che $x - a$ è divisibile per s, quindi x è della forma

$$x = a + s \cdot n$$

per qualche intero n.

Ora imponiamo la seconda congruenza. Vogliamo $x \equiv_t b$, cioè

$$a + s \cdot n \equiv_t b.$$

Sottraiamo a da entrambi i membri:

$$s \cdot n \equiv_t b - a.$$

Quindi l'intero problema diventa: possiamo risolvere

$$s \cdot n \equiv_t (b - a)?$$

Poiché $\gcd(s,t) = 1$, per Proposition 0.4 il numero s è invertibile modulo t. Questo significa che esiste un intero u tale che

$$s \cdot u \equiv_t 1.$$

Ora moltiplichiamo la congruenza $s \cdot n \equiv_t (b - a)$ per u:

$$(s \cdot u) \cdot n \equiv_t u \cdot (b - a).$$

Ma $s \cdot u \equiv_t 1$, quindi il lato sinistro diventa

$$1 \cdot n \equiv_t u(b - a),$$

cioè

$$n \equiv_t u(b - a).$$

Quindi, se scegliamo $n := u(b - a)$, otteniamo una soluzione, che è

$$x = a + s \cdot u(b - a).$$

$\square$

Remark 0.3. Osserviamo che Theorem 0.1 ci dice che una soluzione *esiste*. Tuttavia, in generale la soluzione non è unica. Infatti, supponiamo di avere una soluzione x. Allora anche $x + st$ è una soluzione, perché

$$x + st \equiv_s x, \qquad x + st \equiv_t x.$$

In particolare, dopo aver trovato una soluzione x, tutte le altre soluzioni sono della forma $x + st \cdot k$ con k un intero.

Soluzione del problema degli autobus

Sia x il tempo di attesa (in minuti) fino a un arrivo simultaneo.

Dai dati, otteniamo:

- Autobus A: passa ogni 3 minuti e arriva tra 2 minuti, quindi $x = 3 \cdot n + 2$, cioè

$$x \equiv_3 2.$$

- Autobus B: passa ogni 24 minuti e arriva tra 5 minuti, quindi

$$x \equiv_{24} 5.$$

- Autobus C: passa ogni 23 minuti e arriva tra 10 minuti, quindi

$$x \equiv_{23} 10.$$

Quindi vogliamo capire se esiste un x tale che

$$x \equiv_3 2, \qquad x \equiv_{24} 5, \qquad x \equiv_{23} 10.$$

Poiché 24 è un multiplo di 3, da $x \equiv_{24} 5$ otteniamo che 24 divide $x - 5$. In particolare, 3 divide $x - 5$, quindi $x \equiv_3 5$.

Ma $5 \equiv_3 2$, quindi $x \equiv_3 2$ automaticamente.

Dunque la condizione per l'autobus A è già implicata dalla condizione per l'autobus B, e il problema si riduce a risolvere soltanto

$$x \equiv_{24} 5, \qquad x \equiv_{23} 10.$$

Una volta trovato un tale x, anche l'autobus A arriverà al tempo x. Theorem 0.1 ci dice che una tale soluzione esiste, poiché $\gcd(24, 23) = 1$. Quindi gli autobus arriveranno simultaneamente prima o poi (puoi verificare che $x = 125$ funziona).

Questo articolo fa parte della serie *Fermat's Christmas Theorem*.

Precedente: How many primes are there?