Quanti numeri primi ci sono?

Serie "Fermat's Christmas Theorem"

2025-12-08

ENG ITA

Introduzione

Nel post precedente ci siamo posti alcune domande sui numeri primi, ad esempio:

- Quali numeri possono essere scritti come prodotto di numeri primi?
- Quanti numeri primi esistono?

Lo scopo di questo post è dare una risposta precisa a queste due domande.

La prima persona a rispondere rigorosamente a queste domande fu il matematico greco Euclide, e seguiremo a grandi linee il suo ragionamento.

Che cos'è un primo?

Iniziamo con un breve ripasso. A scuola abbiamo imparato che un intero positivo è primo se i suoi soli divisori sono 1 e se stesso (1 non è considerato primo). Quindi $2, 3, 5, \ldots$ sono primi.

Consideriamo il primo 2. Osserviamo che ogni volta che 2 divide un prodotto di due interi $a \cdot b$, divide uno dei due fattori (cioè o 2 divide a oppure 2 divide b). Prova qualche esempio per convincerti. Per esempio, 2 divide il prodotto $4 \cdot 5 = 20$ e infatti 2 divide 4. Puoi provare con qualunque prodotto e la proprietà continuerà a valere. Tuttavia, non c'è nulla di speciale in 2; in realtà ogni numero primo soddisfa questa proprietà (cioè, se un numero primo p divide un prodotto $a \cdot b$ allora p divide a oppure p divide b). In realtà questa proprietà caratterizza i numeri primi. Per esempio, 6 (che non è primo) divide il prodotto $3 \cdot 4 = 12$, ma non divide né 3 né 4.

Poiché questa proprietà è importante, definiamo i numeri primi nel modo seguente:

Definizione: Un intero p è *primo* se ogni volta che p divide un prodotto $a \cdot b$, allora p divide a oppure p divide b.

Useremo invece il termine *irriducibile* per l'altra definizione che conosciamo:

Definizione: Un intero q è *irriducibile* se i suoi soli divisori sono se stesso, 1 e -1.

Includiamo -1 perché permettiamo anche interi negativi; ad esempio -3 è irriducibile poiché i suoi soli divisori sono -1, 1 e -3.

Per gli interi, un numero è irriducibile se e solo se è primo, quindi le due definizioni coincidono. Per questo usiamo spesso la definizione tramite irriducibilità per i numeri primi.

Ritorno a scuola: la divisione euclidea

Sappiamo come funziona la divisione tra interi. Per esempio, per dividere 7 per 2 contiamo quante volte possiamo sommare 2 senza superare 7. Vediamo che $2 + 2 + 2 = 6$, quindi il quoziente è 3 e il resto è 1. Scriviamo in simboli

$$7 = 2 \cdot 3 + 1$$

Un altro esempio: dividendo 17 per 15 otteniamo quoziente 1 e resto 2, cioè

$$17 = 15 \cdot 1 + 2$$

Come ultimo esempio, supponiamo di voler dividere 3 per 12. Poiché 12 è troppo grande, il quoziente è 0 e il resto è 3, cioè

$$3 = 12 \cdot 0 + 3$$

Abbiamo imparato che possiamo sempre eseguire la divisione con resto: per interi positivi n, m possiamo scrivere

$$n = m \cdot q + r$$

dove q è il quoziente e r è il resto. Siamo pronti a enunciare questo fatto come un teorema:

Theorem 0.1 (Divisione euclidea.)**.** *Per ogni coppia di interi $n \geq 0$ e $m > 0$ (non possiamo dividere per 0), esistono interi $q, r \geq 0$ tali che*

$$n = m \cdot q + r$$

dove $r < m$. Inoltre q e r sono determinati in modo unico.

Ok, fermiamoci un attimo: questo teorema sembra più complicato di quanto dovrebbe. Prima di tutto, dovrebbe essere chiaro che possiamo scrivere il nostro n come

$$n = m \cdot q + r$$

per qualche q e r. Perché r deve essere strettamente minore di m? Perché, se così non fosse, potremmo dividere ancora. Per esempio, supponiamo di scrivere

$$15 = 4 \cdot 2 + 6$$

Questo non è ammesso, perché $6 = 4 + 2$; possiamo ancora dividere per 4 e ottenere

$$15 = 4 \cdot 3 + 2$$

Ora, poiché 2 è più piccolo di 4, non possiamo più dividerlo, quindi abbiamo finito e ciò che otteniamo è la divisione.

L'altra domanda è: che cosa significa che q e r sono determinati in modo unico? Significa che c'è un solo modo di scrivere n come $m \cdot q + r$, con $r < m$. Prendi carta e penna e prova a convincerti che questa scrittura è unica facendo qualche esempio.

Il teorema fondamentale dell'aritmetica

Ora vogliamo rispondere alla domanda su quali numeri possono essere scritti come prodotto di primi. Il teorema seguente ci dà la risposta.

Theorem 0.1 (Teorema fondamentale dell'aritmetica.)**.** *Ogni intero n strettamente maggiore di uno (cioè $n > 1$) può essere scritto in modo* unico *come prodotto di numeri primi.*

Questo ci aiuta a capire perché i numeri primi sono così importanti. In questo senso sono i mattoni fondamentali degli interi. Possiamo sempre decomporre un intero come prodotto di primi e questo avviene in modo unico.

Facciamo alcuni esempi per chiarire il teorema. Consideriamo 15. I suoi divisori primi sono 3 e 5, quindi $15 = 3 \cdot 5$. Un altro esempio può essere 4; è divisibile solo per 2, quindi $4 = 2^2$.

Come si fattorizza un numero in pratica? Prendiamo un intero, per esempio 36. Guardiamo i primi iniziali

$$2, 3, 5, 7, 11, ...$$

e testiamo la divisibilità per i primi successivi:

- 36 è divisibile per 2? Sì: $36 = 2 \cdot 18$.
- 18 è divisibile per 2? Sì: $18 = 2 \cdot 9$.
- 9 è divisibile per 2? No: passiamo al primo successivo.
- 9 è divisibile per 3? Sì: $9 = 3 \cdot 3$.

Otteniamo quindi

$$36 = 2 \cdot 18 = 2 \cdot (2 \cdot 9) = 2 \cdot (2 \cdot (3 \cdot 3)) = 2^2 \cdot 3^2$$

Con questo procedimento possiamo fattorizzare qualunque intero positivo. Per gli interi negativi, basta aggiungere un segno meno davanti; ad esempio $-36 = -(2^2 \cdot 3^2)$.

Consideriamo ora 7. Poiché è primo, non può essere fattorizzato ulteriormente. Diremo quindi che la sua fattorizzazione è semplicemente se stesso, cioè

$$7 = 7$$

dove a destra stiamo scrivendo i fattori (solo 7) della fattorizzazione.

Vogliamo convincerci che una fattorizzazione esiste sempre, quindi entriamo nel dettaglio della dimostrazione.

Esistenza della fattorizzazione in primi. Supponiamo che alcuni interi positivi non possano essere fattorizzati. Prendiamo il più piccolo tra questi interi e chiamiamolo m. L'intero m non può essere un numero primo, perché se lo fosse la sua fattorizzazione sarebbe $m = m$ (come abbiamo fatto nel caso di 7). Poiché m non è primo, deve esistere un numero s diverso da m e da 1 che lo divide. Possiamo quindi scrivere $m = s \cdot t$ per qualche altro intero t. Osserviamo ora che s e t sono entrambi minori di m. Dal momento che m era il più piccolo numero che non poteva essere fattorizzato, sia s che t possono essere fattorizzati in fattori primi. In particolare otteniamo

$$m = s \cdot t = (\text{fattorizzazione in primi di } s) \cdot (\text{fattorizzazione in primi di } t)$$

Questo fornisce una fattorizzazione di m. Per esempio, $144 = 4 \cdot 36$; fattorizzando otteniamo $4 = 2^2$ e $36 = 2^2 \cdot 3^2$, quindi

$$144 = 4 \cdot 36 = (2^2) \cdot (2^2 \cdot 3^2) = 2^4 \cdot 3^2$$

Abbiamo quindi dimostrato che il più piccolo numero che non poteva essere fattorizzato in realtà può essere fattorizzato. Dunque, otteniamo la tesi. □

Inoltre, il teorema ci dice che la fattorizzazione è unica: non puoi scrivere un intero (> 1) come prodotto di primi in due modi diversi. Prova qualche esempio per convincerti.

Quanti numeri primi ci sono?

Siamo finalmente pronti a rispondere a questa domanda. Probabilmente immagini già la risposta, ma voglio comunque dare un argomento pulito che ti convinca che è corretta.

Theorem 0.1. *Esistono infiniti numeri primi.*

Dimostrazione di Euclide. Supponiamo che esistano solo un numero finito di primi, chiamiamoli $p_1, \dots, p_n$. Definiamo m come il prodotto di tutti questi primi più 1, cioè

$$m = p_1 \cdot p_2 \cdots p_n + 1$$

Osserviamo che m non è divisibile da nessuno dei primi $p_1, \dots, p_n$. Per convincerci, prendiamo p_1 e scriviamo

$$m = p_1 \cdot (p_2 \cdots p_n) + 1$$

Definiamo $q := (p_2 \cdots p_n)$. Stiamo quindi dicendo

$$m = p_1 \cdot (p_2 \cdots p_n) + 1 = p_1 \cdot q + 1$$

Dunque m ha resto 1 nella divisione per p_1, quindi p_1 non divide m (se lo dividesse, il resto sarebbe 0). Non c'è nulla di speciale in p_1: possiamo ripetere lo stesso argomento per tutti gli altri primi $p_2, \dots, p_n$.

Siamo quindi convinti che nessun primo nella lista $p_1, \dots, p_n$ divide m.

Ma abbiamo detto (Theorem 0.1) che ogni numero intero può essere scritto come prodotto di numeri primi. Tuttavia, poiché m non è divisibile da nessuno dei primi nella lista $p_1, \dots, p_n$, significa che la lista non contiene tutti i numeri primi.

Quindi, ogni volta che supponiamo che una lista finita $p_1, \dots, p_n$ contenga tutti i primi, possiamo costruire un primo che non è nella lista; dunque ogni lista finita è incompleta.

Concludiamo che devono esistere infiniti numeri primi. □

Conclusione

Per dimostrare che esistono *infiniti* numeri primi abbiamo usato una strategia comune. Abbiamo capito che dimostrare l'enunciato così com'è è molto difficile. Come si può dimostrare che esistono infiniti numeri primi? L'idea naturale è: supponiamo che ce ne siano solo finiti e ricaviamo una contraddizione. Questo è ciò che chiamiamo *dimostrazione per assurdo* (dimostri la tua affermazione mostrando che la sua negazione porta ad una contraddizione).

C'è un'altra idea interessante che abbiamo usato oggi. Quando abbiamo dimostrato Theorem 0.1 abbiamo ipotizzato che esistessero numeri che non soddisfacevano il nostro enunciato. Poi abbiamo preso il minimo tra questi numeri e dimostrato che in realtà quel minimo soddisfaceva la nostra tesi. Questo tipo di argomento è spesso chiamato *dimostrazione per controesempio minimale* (una forma di induzione), ed è anch'esso molto comune.

Pensa a questi due tipi di dimostrazioni e a come li abbiamo utilizzati negli argomenti. Se vuoi esercitarti, prova a dimostrare l'unicità della fattorizzazione in primi (procedi per assurdo e usa le due definizioni di numero primo introdotte sopra).

In ogni caso, ci vediamo la prossima settimana!

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

Precedente: Introduction

Prossimo: Aritmetica modulare di base