Algebra

Alessandro D'Andrea

11. L'algoritmo di primalità di Solovay-Strassen

Richiami

- Congruenze lineari
- Congruenze quadratiche
- Simbolo di Legendre e reciprocità quadratica
- Oggi: **Simbolo di Jacobi**
  - Calcolo del simbolo di Legendre per mezzo di un algoritmo euclideo
  - Algoritmo probabilistico di Solovay-Strassen per stabilire la primalità di un numero (grande)

Simbolo di Legendre - I

Il simbolo di Legendre $\left(\frac{a}{p}\right)$ è moltiplicativo in a.

Dipende solo dalla classe di congruenza di a modulo p, quindi posso ridurre a ad un numero $0 \leq r < p$.

Ne conosciamo il valore quando $a = -1, 2$, un quadrato.

Quando $a = q$ è un primo dispari, sappiamo che

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{se } p \equiv q \equiv 3 \mod 4 \\ \left(\frac{p}{q}\right) & \text{altrimenti.} \end{cases}$$

Questo ci permette di calcolare induttivamente il simbolo di Legendre.

Simbolo di Legendre - II

3253 e 1979 sono entrambi primi. Calcoliamo $\left(\frac{1979}{3253}\right)$.

$$\begin{aligned}\left(\frac{1979}{3253}\right) &= \left(\frac{3253}{1979}\right)\\ &= \left(\frac{1274}{1979}\right) = \left(\frac{2\cdot 7^2\cdot 13}{1979}\right)\\ &= \left(\frac{2}{1979}\right)\cdot\left(\frac{13}{1979}\right)\\ &= -1\cdot\left(\frac{1979}{13}\right) = -1\cdot\left(\frac{3}{13}\right)\\ &= -\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1.\end{aligned}$$

Si fa rapidamente, ma bisogna fattorizzare. E non sono noti metodi rapidi per fattorizzare numeri grandi!!

Simbolo di Legendre - III

$$\begin{aligned}
\left(\frac{1979}{3253}\right) &= \left(\frac{3253}{1979}\right) \\
&= \left(\frac{-705}{1979}\right) = \left(\frac{-1\cdot 3\cdot 5\cdot 47}{1979}\right) \\
&= \left(\frac{-1}{1979}\right)\cdot\left(\frac{3}{1979}\right)\cdot\left(\frac{5}{1979}\right)\cdot\left(\frac{47}{1979}\right) \\
&= (-1)\cdot -\left(\frac{1979}{3}\right)\cdot\left(\frac{1979}{5}\right)\cdot -\left(\frac{1979}{47}\right) \\
&= -\left(\frac{-1}{3}\right)\cdot\left(\frac{-1}{5}\right)\cdot\left(\frac{5}{47}\right) = \left(\frac{5}{47}\right) \\
&= \left(\frac{47}{5}\right) = \left(\frac{2}{5}\right) = -1.
\end{aligned}$$

Simbolo di Jacobi - I

E' possibile calcolare il simbolo di Legendre ancora più rapidamente introducendo il cosiddetto simbolo di Jacobi.

Se $n = p_1^{h_1} \cdot \ldots \cdot p_r^{h_r}$ è dispari, allora

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{h_1} \left(\frac{a}{p_2}\right)^{h_2} \ldots \left(\frac{a}{p_r}\right)^{h_r}$$

- Quando n è primo, il simbolo di Jacobi coincide con il simbolo di Legendre.
- Il simbolo di Jacobi è moltiplicativo sia in a che in n.
- Se a è un quadrato modulo n, allora è un quadrato modulo ogni p_i, e quindi

$$\left(\frac{a}{n}\right) = 1.$$

Simbolo di Jacobi - II

- Se
$$\left(\frac{a}{n}\right) = -1,$$
allora a non è un quadrato modulo qualche p_i, e quindi a non è un quadrato modulo n.
- Se a non è un quadrato modulo n, allora il simbolo di Jacobi può valere sia 1 che -1.
- $$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \qquad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}};$$
- $$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}.$$

Perché funziona? - I

Perché vale

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \ ?$$

Se è vero per a, b entrambi dispari, è vero anche per il loro prodotto ab. In effetti

$$(-1)^{\frac{ab-1}{2}} \quad \text{e} \quad (-1)^{\frac{a-1}{2}}(-1)^{\frac{b-1}{2}}$$

coincidono non appena

$$\frac{ab-1}{2} \quad \text{e} \quad \frac{a-1}{2} + \frac{b-1}{2}$$

differiscono per un pari. La differenza vale

$$\frac{ab-1-(a-1)-(b-1)}{2} = \frac{(a-1)(b-1)}{2},$$

che è pari.

Perché funziona? - II

Perché vale

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} \ ?$$

Se è vero per a, b entrambi dispari, è vero anche per il loro prodotto ab. In effetti

$$(-1)^{\frac{a^2b^2-1}{8}} \quad \text{e} \quad (-1)^{\frac{a^2-1}{8}}(-1)^{\frac{b^2-1}{8}}$$

coincidono non appena

$$\frac{a^2b^2-1}{8} \quad \text{e} \quad \frac{a^2-1}{8} + \frac{b^2-1}{8}$$

differiscono per un pari. La differenza vale

$$\frac{a^2b^2-1-(a^2-1)-(b^2-1)}{8} = \frac{(a-1)(a+1)(b-1)(b+1)}{8},$$

che è pari.

Perché funziona? - III

Perché vale

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \quad ?$$

Se è vero quando $m = a, b$ entrambi dispari, è vero anche quando $m = ab$. In effetti

$$(-1)^{\frac{(ab-1)(n-1)}{4}} \quad \text{e} \quad (-1)^{\frac{(a-1)(n-1)}{4}}(-1)^{\frac{(b-1)(n-1)}{4}}$$

coincidono non appena

$$\frac{(ab-1)(n-1)}{4} \quad \text{e} \quad \frac{(a-1)(n-1)}{4} + \frac{(b-1)(n-1)}{4}$$

differiscono per un pari. La differenza vale

$$\frac{(ab-1-(a-1)-(b-1))(n-1)}{4} = \frac{(a-1)(b-1)(n-1)}{4},$$

che è pari. Ora si scambia il ruolo di m ed n.

Simbolo di Jacobi - III

Se m, n sono dispari, per calcolare il simbolo di Jacobi $\left(\frac{m}{n}\right)$:

- Si sostituisce m con il suo resto modulo n, calcolandolo con una divisione euclidea;
- Si rimuove da m la massima potenza di 4 che lo divide: è un quadrato, e non altera il valore del simbolo di Jacobi;
- Se $m = 2d$, con d dispari, allora

$$\left(\frac{m}{n}\right) = \left(\frac{2d}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{d}{n}\right) = (-1)^{\frac{d^2-1}{8}}\left(\frac{d}{n}\right).$$

- Se d è dispari, si usa

$$\left(\frac{d}{n}\right) = \left(\frac{n}{d}\right) \cdot (-1)^{\frac{(d-1)(n-1)}{4}},$$

e si ricomincia dall'inizio.

Simbolo di Jacobi - IV

$$\begin{aligned}
\left(\frac{1979}{3253}\right) &= \left(\frac{3253}{1979}\right) \\
&= \left(\frac{1274}{1979}\right) = \left(\frac{2}{1979}\right)\left(\frac{637}{1979}\right) \\
&= -\left(\frac{637}{1979}\right) = -\left(\frac{1979}{637}\right) = -\left(\frac{68}{637}\right) \\
&= -\left(\frac{4}{637}\right)\cdot\left(\frac{17}{637}\right) = -\left(\frac{17}{637}\right) \\
&= -\left(\frac{637}{17}\right) = -\left(\frac{8}{17}\right) = -\left(\frac{4}{17}\right)\cdot\left(\frac{2}{17}\right) \\
&= -\left(\frac{2}{17}\right) = -1.
\end{aligned}$$

Simbolo di Jacobi - V

$$\left(\frac{1979}{3253}\right) = \left(\frac{3253}{1979}\right)$$
$$= \left(\frac{1274}{1979}\right) = \left(\frac{2}{1979}\right)\left(\frac{637}{1979}\right) = -\left(\frac{637}{1979}\right)$$
$$= -\left(\frac{1979}{637}\right) = -\left(\frac{1342}{637}\right) = -\left(\frac{2}{637}\right)\cdot\left(\frac{671}{637}\right) = \left(\frac{671}{637}\right)$$
$$= \left(\frac{34}{637}\right) = \left(\frac{2}{637}\right)\left(\frac{17}{637}\right) = -\left(\frac{637}{17}\right) = -\left(\frac{620}{17}\right)$$
$$= -\left(\frac{4}{17}\right)\left(\frac{155}{17}\right) = -\left(\frac{155}{17}\right) = -\left(\frac{138}{17}\right) = -\left(\frac{2}{17}\right)\left(\frac{69}{17}\right)$$
$$= -\left(\frac{52}{17}\right) = -\left(\frac{13}{17}\right) = -\left(\frac{17}{13}\right) = -\left(\frac{4}{13}\right) = -1.$$

Algoritmo di Solovay-Strassen

Se n è primo, sappiamo che

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \mod n.$$

Teorema (Solovay-Strassen)

Se n non è primo, per almeno la metà delle scelte di a

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \mod n.$$

Provo valori di a a caso. Se dopo k prove ho sempre ottenuto l'uguaglianza, allora n è primo con probabilità almeno $1 - 1/2^k$.

Dopo aver verificato positivamente i primi $3(\log n)^2$ valori di a, si è certi che n sia primo (se vale l'ipotesi di Riemann generalizzata).

Come si usa Solovay-Strassen?

Nei casi concreti, si verifica la primalità con un metodo probabilistico veloce.

Se si ha il dubbio concreto che il numero possa essere primo, si controlla con un metodo non probabilistico.

La verifica con Solovay-Strassen della non primalità di un numero è molto rapida.

Nella prossima lezione (facoltativa), fornirò dimostrazioni della reciprocità quadratica e del teorema di Solovay-Strassen.

Un esempio - I

Stabiliamo con l'algoritmo di Solovay-Strassen se $n = 1247$ è primo.

Provo con $a = 97$.

$$\begin{aligned}\left(\frac{97}{1247}\right) &= \left(\frac{1247}{97}\right) \\ &= \left(\frac{-14}{97}\right) \\ &= \left(\frac{-1}{97}\right)\left(\frac{2}{97}\right)\left(\frac{7}{97}\right) \\ &= 1 \cdot 1 \cdot \left(\frac{97}{7}\right) = \left(\frac{-1}{7}\right) = -1.\end{aligned}$$

Un esempio - II

$$
\begin{aligned}
97^2 &= 680,\\
97^4 &= 680^2 = 1010,\\
97^8 &= 1010^2 = 54,\\
97^{16} &= 54^2 = 422,\\
97^{32} &= 422^2 = 1010,\\
97^{64} &= 1010^2 = 54,\\
97^{128} &= 54^2 = 422,\\
97^{256} &= 422^2 = 1010,\\
97^{512} &= 1010^2 = 54.
\end{aligned}
$$

$$
\begin{aligned}
97^{623} &= 97^{512+64+32+8+4+2+1}\\
&= 54 \cdot 54 \cdot 1010 \cdot 54 \cdot 1010 \cdot 680 \cdot 97\\
&= 1119 \neq -1 = \left(\frac{97}{1247}\right).
\end{aligned}
$$

Per la cronaca, scegliendo a caso, solo un elemento ogni 12 fornisce lo stesso risultato, mentre gli altri dimostrano la non primalità di 1247.