Algebra

Alessandro D'Andrea

Reciprocità quadratica e teorema di Solovay-Strassen

Richiami

- Simbolo di Legendre e simbolo di Jacobi
- Il simbolo di Jacobi si calcola rapidamente grazie alle proprietà di reciprocità quadratica
- La rapidità nel calcolo del simbolo di Jacobi permette di verificare rapidamente la primalità di un numero grande (algoritmo di Solovay-Strassen)
- Oggi: **Dimostrazione combinatoria del teorema di reciprocità quadratica**
- **Dimostrazione della correttezza dell'algoritmo di Solovay-Strassen**
- **Perché il simbolo di Jacobi soddisfa le stesse proprietà del simbolo di Legendre**

Calcolo di $\left(\frac{2}{p}\right)$

In tutto quello che segue, p e q sono primi dispari. Abbiamo visto come calcolare $\left(\frac{2}{p}\right)$. Si scrive

$$\begin{aligned} 2^{(p-1)/2} \cdot \left(\frac{p-1}{2}\right)! & \\ &= 2 \cdot 4 \cdot \ldots \cdot (p-3) \cdot (p-1) \\ &\equiv 2 \cdot 4 \cdot \ldots \cdot (-3) \cdot (-1) \\ &\equiv (-1)^{\frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor} \left(\frac{p-1}{2}\right)! \mod p, \end{aligned}$$

per ottenere

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv (-1)^{\frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor} \mod p.$$

Calcolo di $\left(\frac{q}{p}\right)$

Proviamo a fare lo stesso per calcolare $\left(\frac{q}{p}\right)$.

$$q^{(p-1)/2} \cdot \left(\frac{p-1}{2}\right)!$$
$$= q \cdot 2q \cdot \ldots \cdot \left(\frac{p-3}{2} \cdot q\right) \cdot \left(\frac{p-1}{2} \cdot q\right)$$

Se riduco tutto modulo p, e riscrivo ogni $(p+1)/2 \leq m < p$ come $-(p-m)$, allora il secondo membro diventa

$$q \cdot 2q \cdot \ldots \cdot \left(\frac{p-3}{2} \cdot q\right) \cdot \left(\frac{p-1}{2} \cdot q\right) \equiv \pm \left(\frac{p-1}{2}\right)! \mod p.$$

Se troviamo un modo di stimare il segno, abbiamo calcolato il simbolo di Legendre.

Calcolo di $\left(\frac{7}{23}\right)$ - I

$$\begin{aligned} 7^{11} \cdot 11! &= 7 \cdot 14 \cdot 21 \cdot 28 \cdot 35 \cdot 42 \cdot 49 \cdot 56 \cdot 63 \cdot 70 \cdot 77 \\ &\equiv 7 \cdot 14 \cdot 21 \cdot 5 \cdot 12 \cdot 19 \cdot 3 \cdot 10 \cdot 17 \cdot 1 \cdot 8 \\ &\equiv 7 \cdot (-9) \cdot (-2) \cdot 5 \cdot (-11) \cdot (-4) \cdot 3 \cdot 10 \cdot (-6) \cdot 1 \cdot 8 \\ &\equiv (-1)^5 11! \mod 23. \end{aligned}$$

Il segno di ciascun fattore è $+$ quando $7n \mod 23$ si trova nella metà inferiore $1, \ldots, 11$; equivalentemente, quando la parte frazionaria di $7n/23$ è compresa tra 0 e $1/2$ (esclusi).

Il segno è $-$ quando $7n \mod 23$ si trova nella metà superiore $12, \ldots, 22$; equivalentemente, quando la parte frazionaria di $7n/23$ è compresa tra $1/2$ e 1 (esclusi).

Calcolo di $\left(\frac{7}{23}\right)$ - II

Il segno è $+$ quando $7n \mod 23$ si trova nella metà inferiore $1, \ldots, 11$; equivalentemente, quando la parte frazionaria di $7n/23$ è compresa tra 0 e $1/2$ (esclusi).

Il segno è $-$ quando $7n \mod 23$ si trova nella metà superiore $12, \ldots, 22$; equivalentemente, quando la parte frazionaria di $7n/23$ è compresa tra $1/2$ e 1 (esclusi).

Possiamo tradurre tutto in questo modo: il segno è $+$ se $\lfloor 14n/23 \rfloor$ è pari, mentre è $-$ se $\lfloor 14n/23 \rfloor$ è dispari. In conclusione, il segno di ciascun fattore è

$$(-1)^{\lfloor 14n/23 \rfloor}.$$

Nel caso generale del calcolo di $\left(\frac{q}{p}\right)$, il segno di ciascun fattore è

$$(-1)^{\lfloor 2qn/p \rfloor}.$$

Espressione esplicita per $\left(\frac{q}{p}\right)$ - I

$$
\begin{aligned}
& q^{(p-1)/2} \cdot \left(\frac{p-1}{2}\right)! \\
& \quad = q \cdot 2q \cdot \ldots \cdot \left(\frac{p-3}{2} \cdot q\right) \cdot \left(\frac{p-1}{2} \cdot q\right) \\
& \quad \equiv (-1)^{\lfloor 2q/p \rfloor} \cdot (-1)^{\lfloor 4q/p \rfloor} \cdot \ldots \cdot (-1)^{\lfloor (p-1)q/p \rfloor} \cdot \left(\frac{p-1}{2}\right)! \\
& \quad \equiv (-1)^{\lfloor 2q/p \rfloor + \lfloor 4q/p \rfloor + \ldots + \lfloor (p-1)q/p \rfloor} \cdot \left(\frac{p-1}{2}\right)! \mod p.
\end{aligned}
$$

Pertanto

$$
q^{(p-1)/2} \equiv (-1)^{\lfloor 2q/p \rfloor + \lfloor 4q/p \rfloor + \ldots + \lfloor (p-1)q/p \rfloor} \mod p.
$$

Espressione esplicita per $\left(\frac{q}{p}\right)$ - II

$$q^{(p-1)/2} \equiv (-1)^{\lfloor 2q/p \rfloor + \lfloor 4q/p \rfloor + \ldots + \lfloor (p-1)q/p \rfloor} \mod p.$$

Di conseguenza

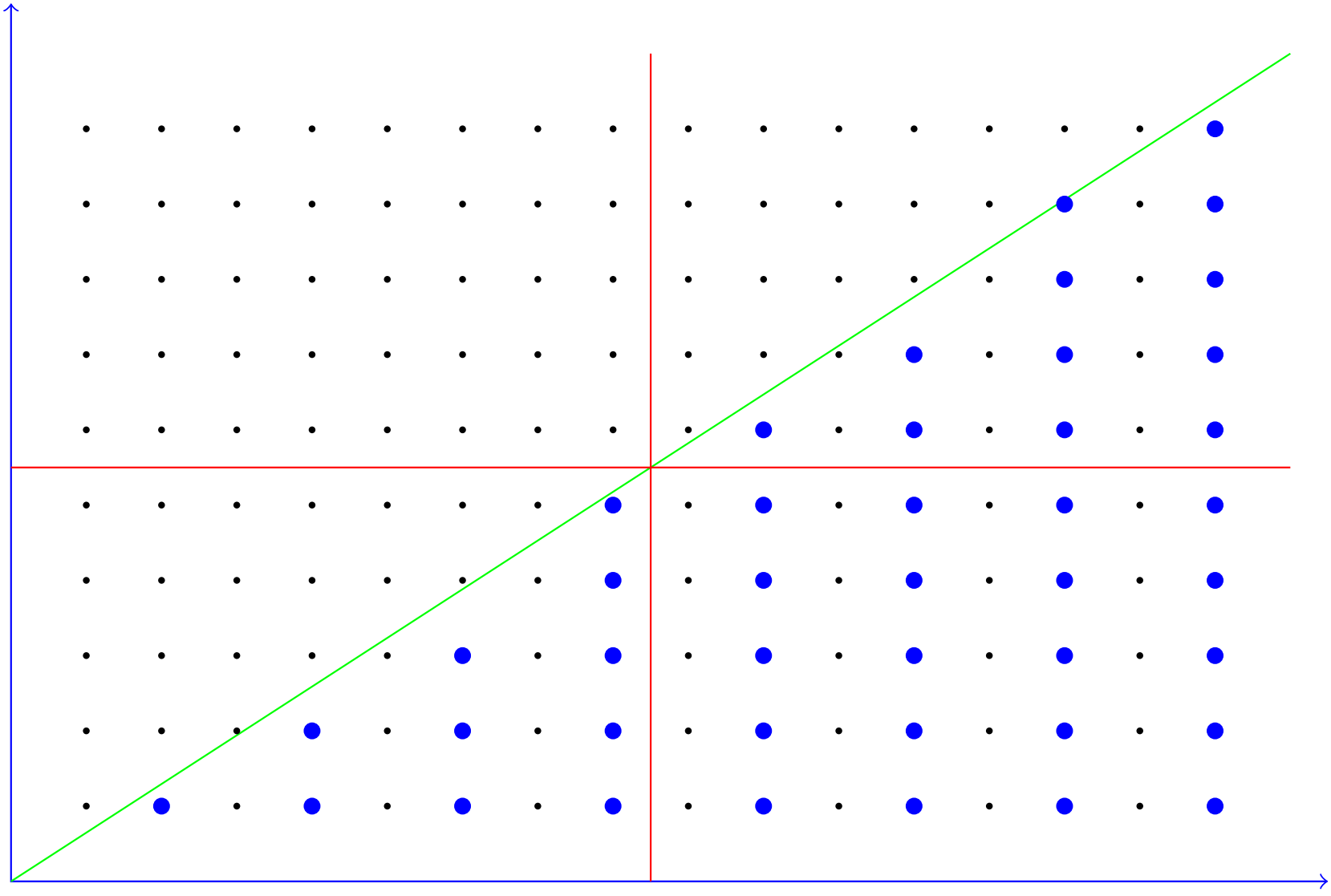
$$\left(\frac{p}{q}\right) = (-1)^{\lfloor 2p/q \rfloor + \lfloor 4p/q \rfloor + \ldots + \lfloor (q-1)p/q \rfloor},$$
$$\left(\frac{q}{p}\right) = (-1)^{\lfloor 2q/p \rfloor + \lfloor 4q/p \rfloor + \ldots + \lfloor (p-1)q/p \rfloor}.$$

Vogliamo mostrare che se $p \neq q$ sono primi dispari, allora

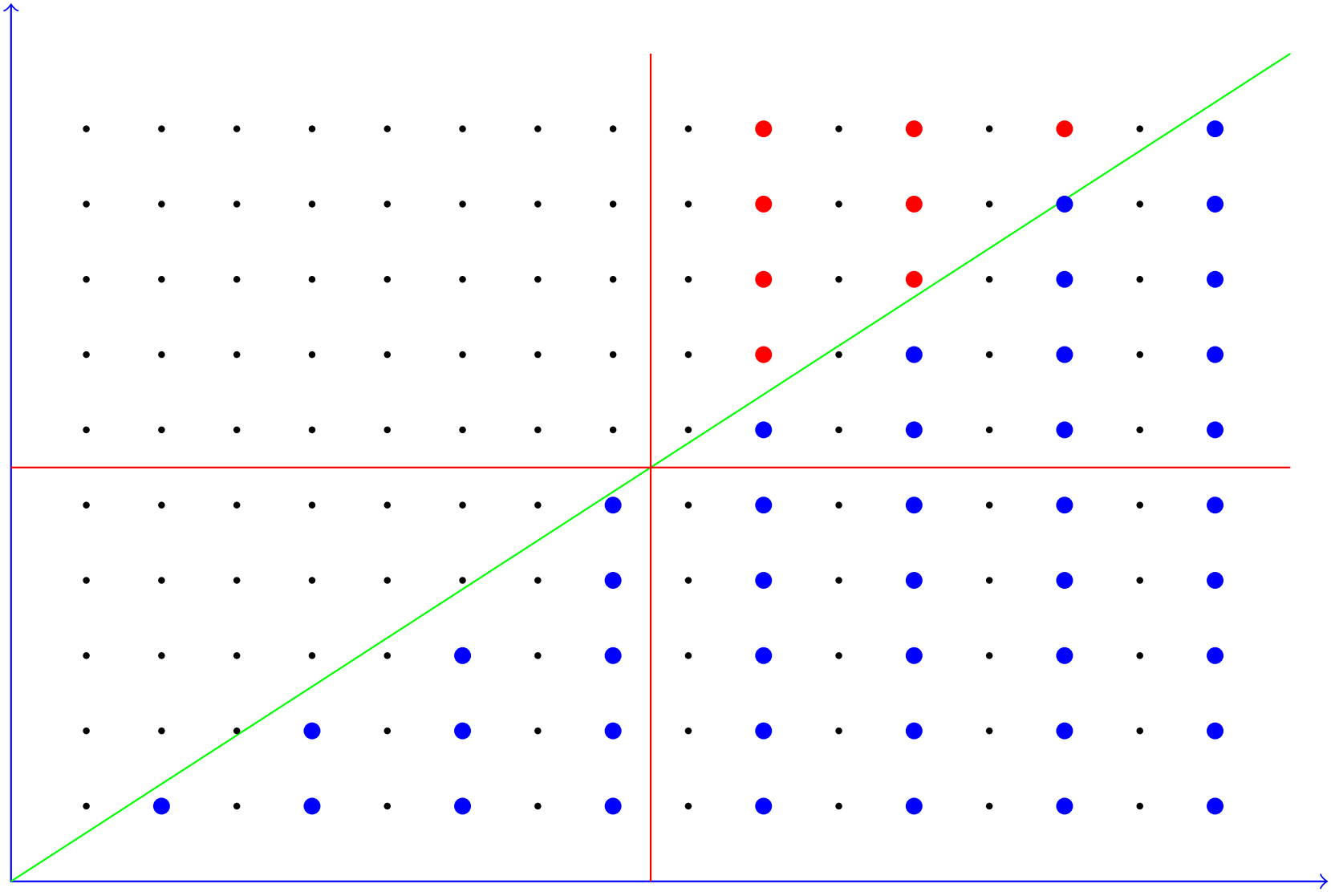
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Daremo di questo fatto una dimostrazione grafica.

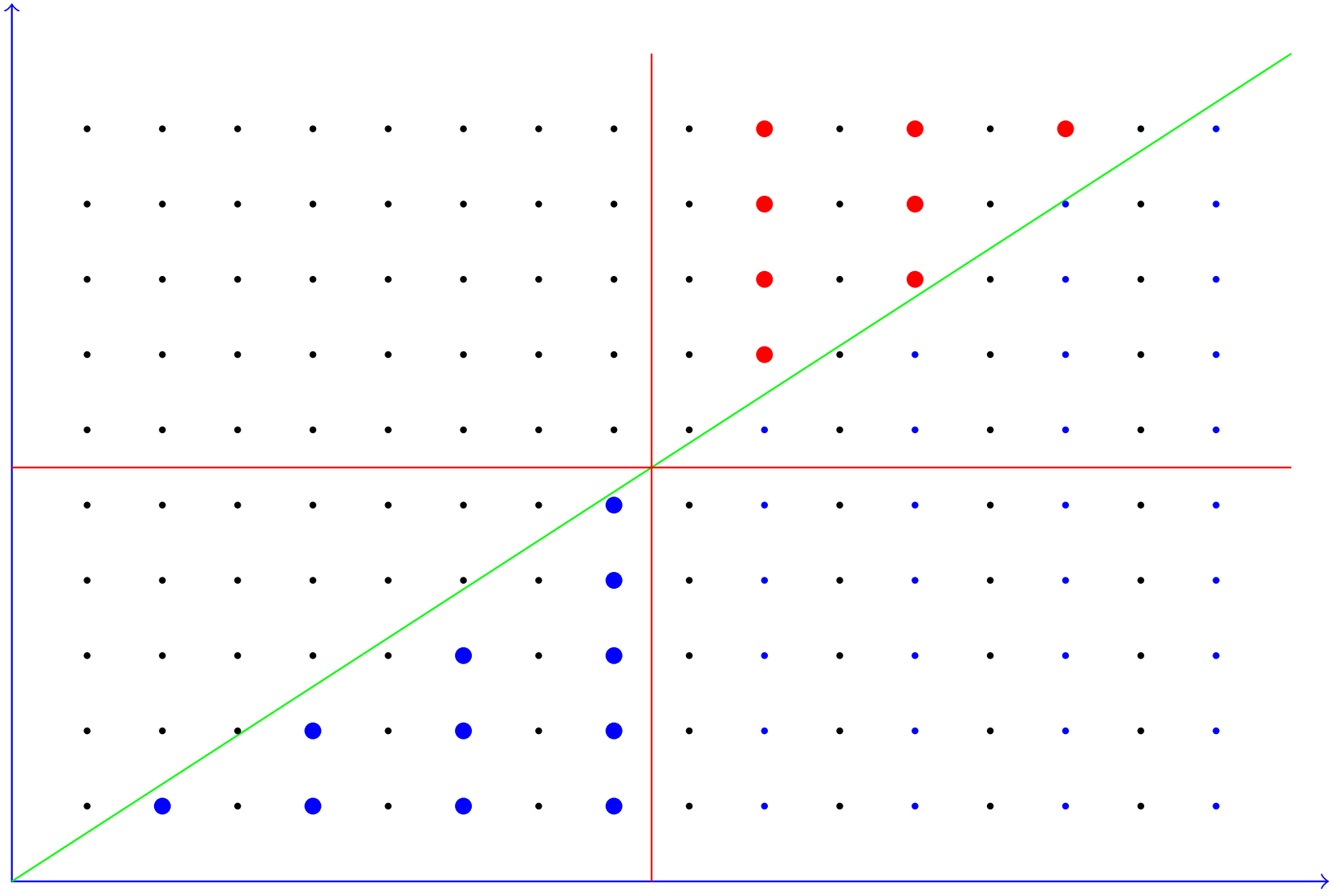
Dimostrazione grafica - I ($p = 11, q = 17$)



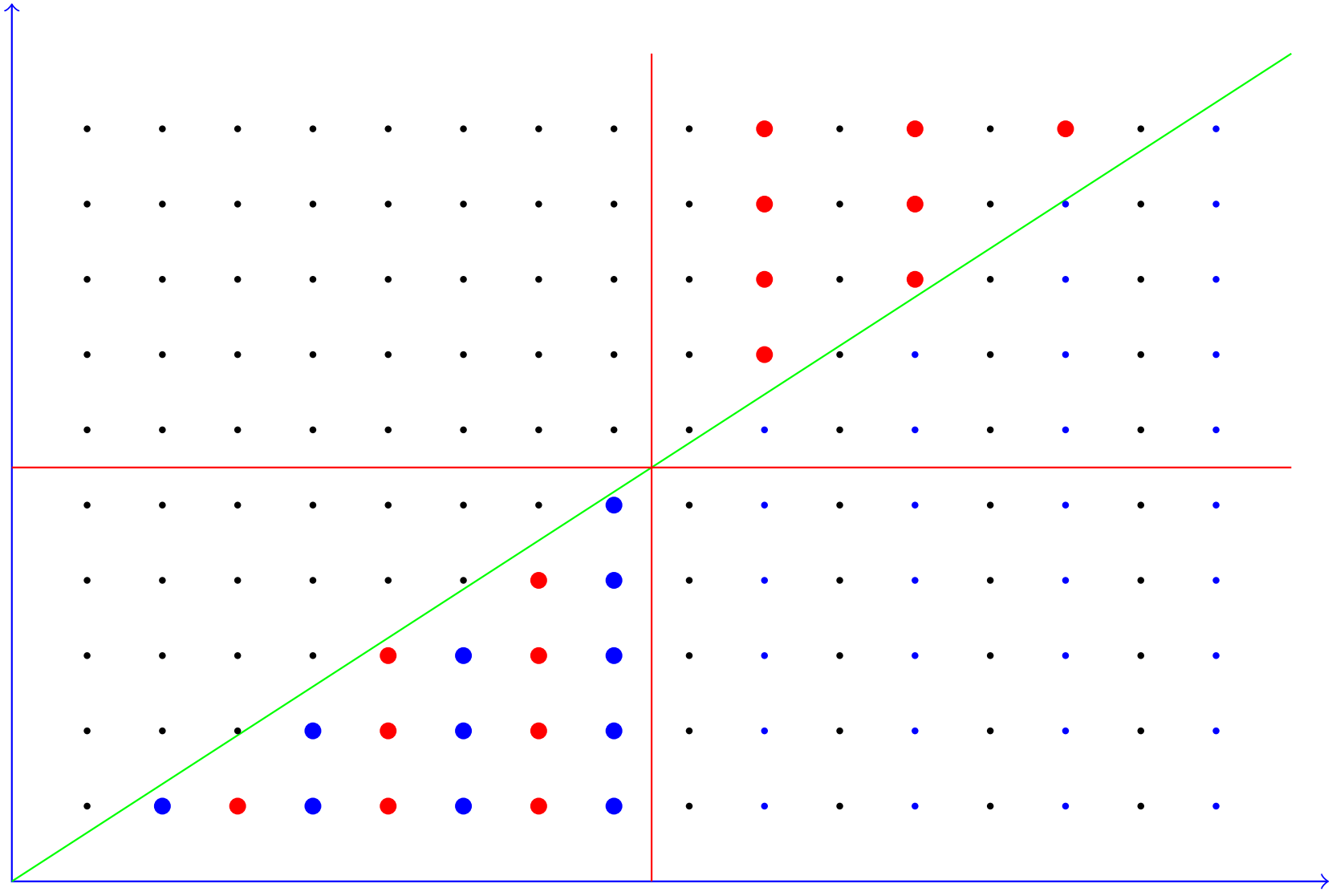
Dimostrazione grafica - II



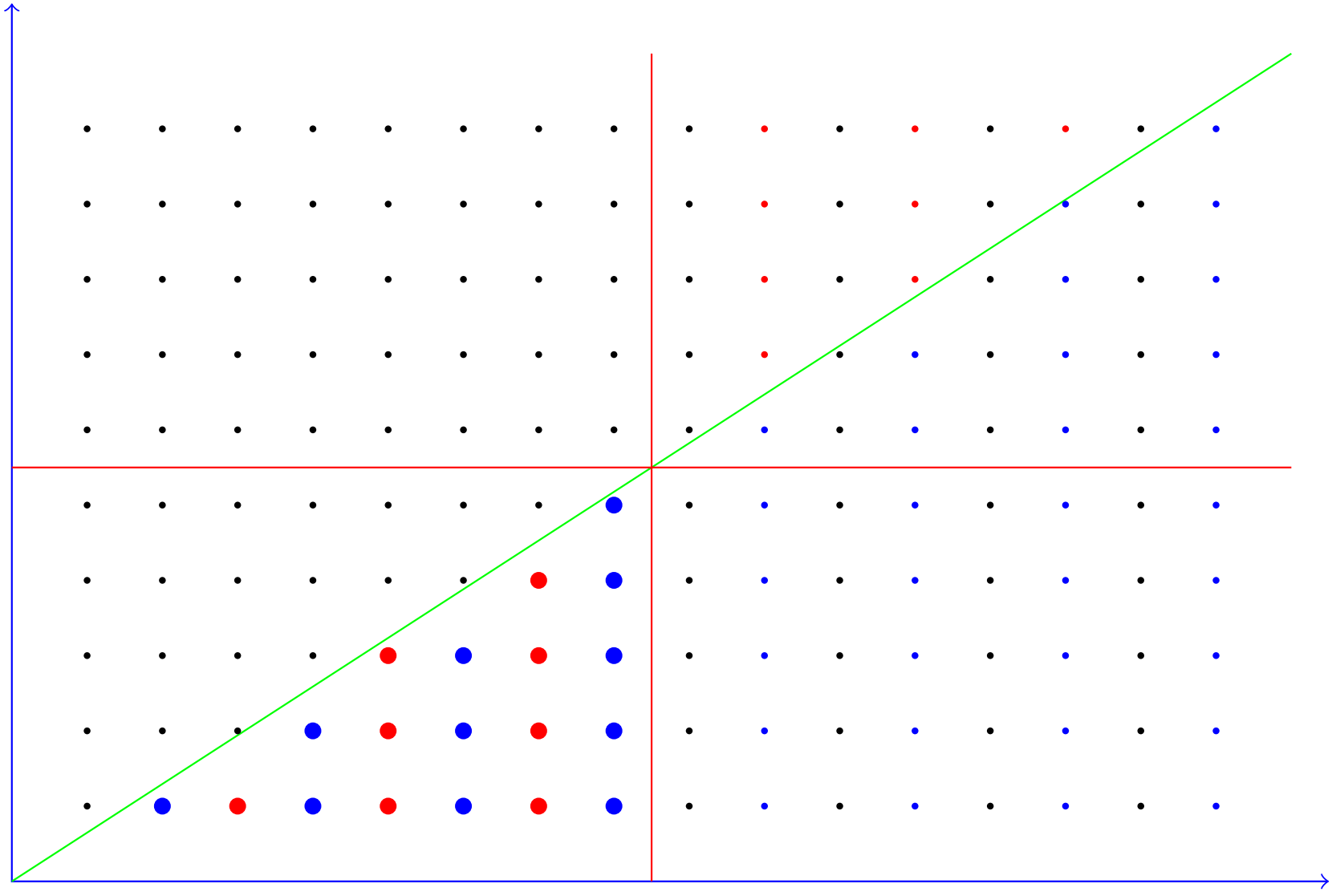
Dimostrazione grafica - III



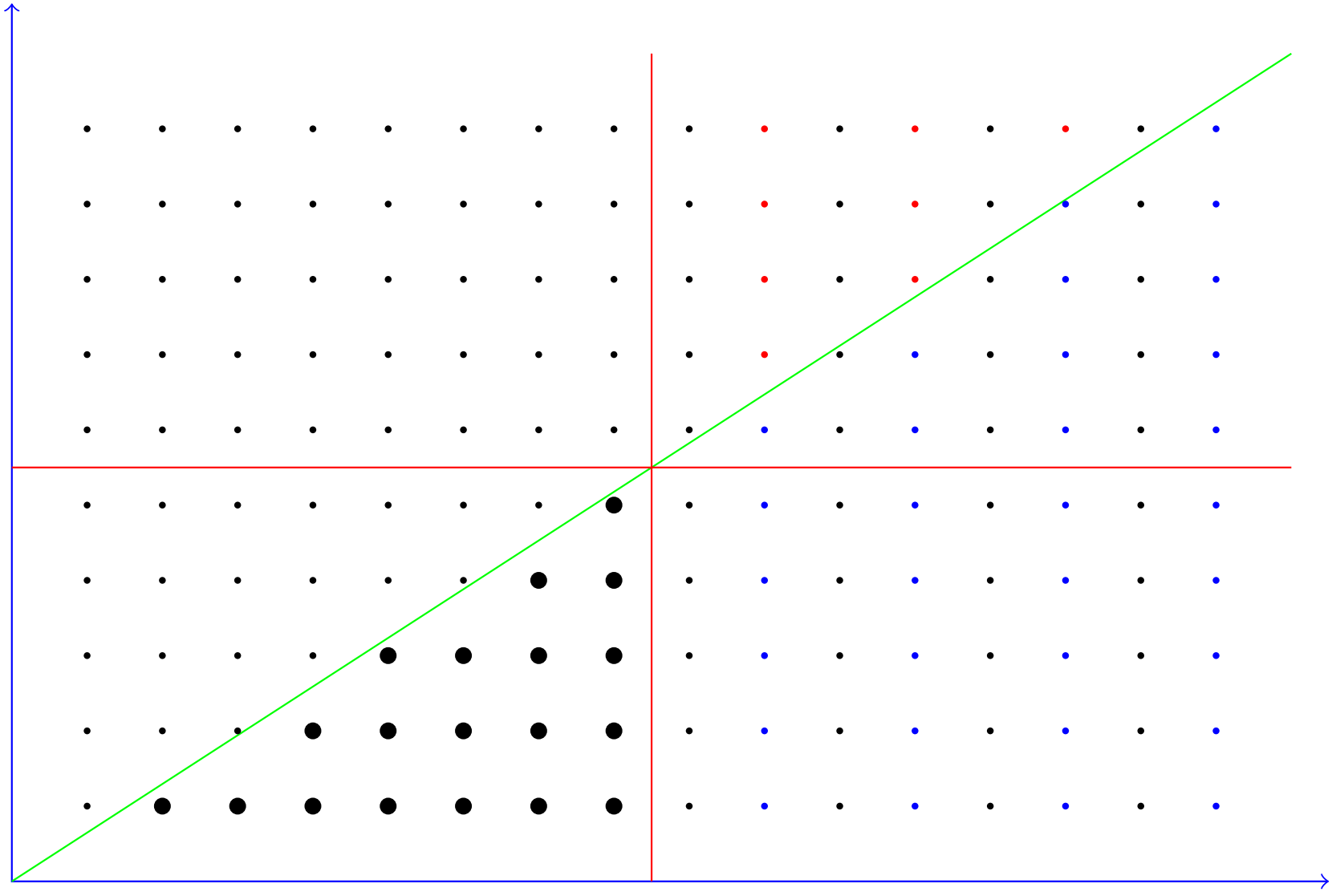
Dimostrazione grafica - IV



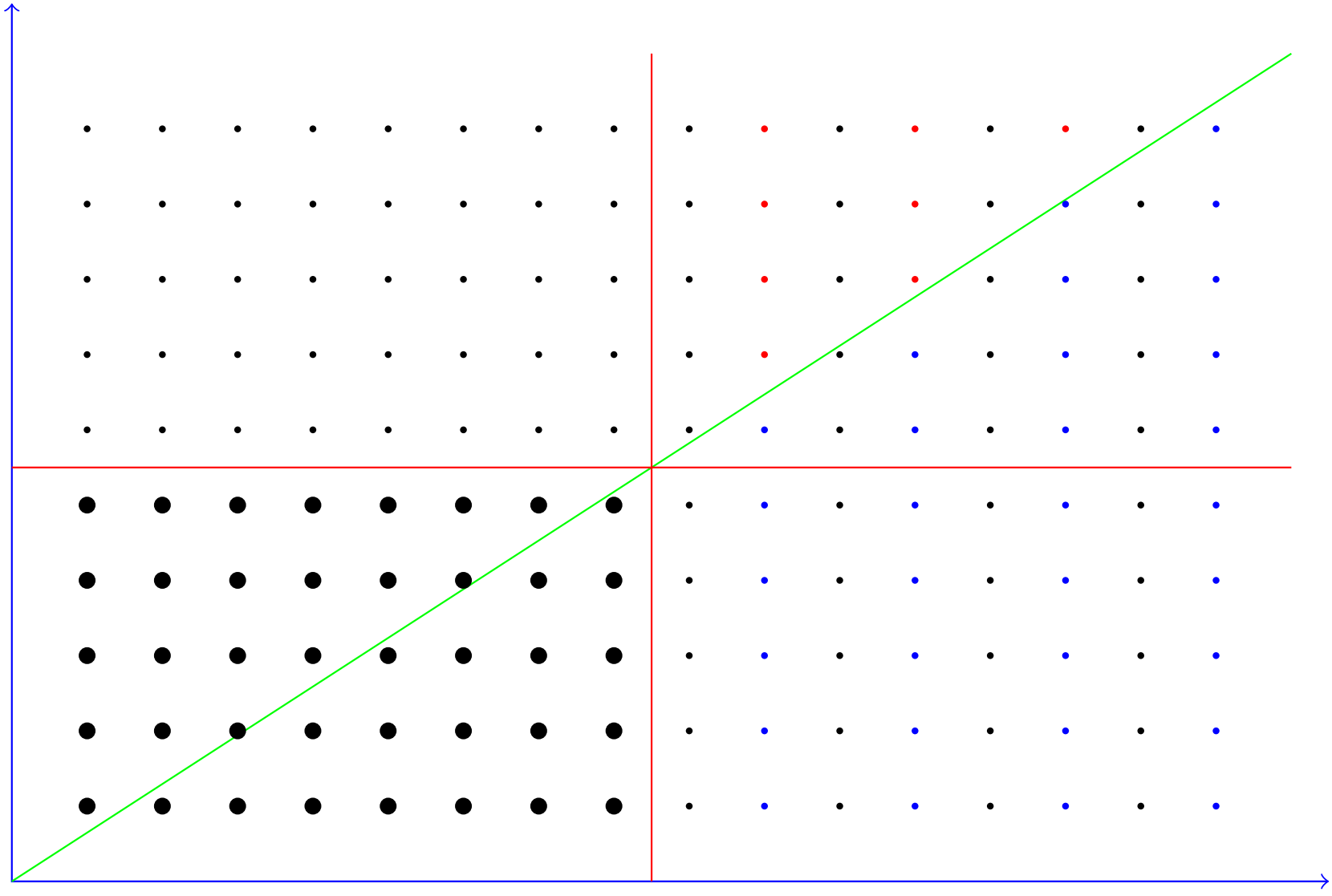
Dimostrazione grafica - V



Dimostrazione grafica - VI



Dimostrazione grafica - VII



Solovay-Strassen - I

Cerchiamo ora di capire per quale motivo l'algoritmo di Solovay-Strassen dia la risposta desiderata.

Innanzitutto, notiamo che il simbolo di Jacobi

$$\left(\frac{a}{n}\right)$$

vale ± 1 ogni volta che $\mathrm{MCD}(a, n) = 1$ e vale 0 altrimenti.

Fissato n, mentre il simbolo di Legendre produce sicuramente anche il valore -1, il simbolo di Jacobi può valere sempre 1.
In effetti

$$\left(\frac{a}{p^2}\right) = \left(\frac{a}{p}\right)^2 = 1,$$

non appena $\mathrm{MCD}(a, p) = 1$.

Solovay-Strassen - II

Dobbiamo dare una dimostrazione del

Teorema (Solovay-Strassen)

Se n non è primo, allora esiste a, primo con n, tale che

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

Dividiamo la dimostrazione in due casi:

- n non è libero da quadrati
  - Esiste p primo tale che p^2 divida n
- n è libero da quadrati

Faremo vedere che, in entrambi i casi, possiamo trovare a tale che $a^{(n-1)/2} \not\equiv \pm 1 \mod n$.

Solovay-Strassen - III

Se p^2 divide n, allora p divide $\varphi(n)$. Questo vuol dire che p divide l'ordine di $\mathbb{Z}/(n)^\times$.

Per il teorema di Cauchy, il gruppo $\mathbb{Z}/(n)^\times$ deve possedere un elemento $\overline{a}$ di ordine p. Chiaramente, $\overline{a} \neq \overline{1}$

Ma allora $a^p \equiv 1 \mod n$, e poiché n è un multiplo di p, $a^n \equiv 1 \mod n$.

Tuttavia, se $a^{(n-1)/2} \equiv \pm 1 \mod n$, allora $a^{n-1} \equiv 1 \mod n$, il che contraddice $a^n \equiv 1 \mod n$.

Se $a^n = a^{n-1}$, cancellando a^{n-1} da entrambi i membri si ottiene $a = 1$, che avevamo escluso.

Solovay-Strassen - IV

Il caso in cui n sia libero da quadrati è solo lievemente più delicato.

n è libero da quadrati solo se $n = p_1 p_2 \dots p_k$, dove i p_i sono primi diversi tra loro.

Il simbolo di Jacobi assume sicuramente entrambi i valori ± 1. Sia c un non-residuo quadratico modulo p_1 e risolviamo il sistema di congruenze

$$\begin{cases} a \equiv c & \mod p_1 \\ a \equiv 1 & \mod p_2 \\ \vdots & \\ a \equiv 1 & \mod p_k \end{cases}$$

Allora

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_k}\right) = -1 \cdot 1 \cdot \dots \cdot 1 = -1.$$

Solovay-Strassen - V

Per concludere, dobbiamo mostrare che $a^{(n-1)/2} \not\equiv -1 \mod n$.

In effetti, se $a^{(n-1)/2} \equiv -1 \mod n$, allora l'equivalenza vale anche mod p_2, ma sappiamo che $a \equiv 1 \mod p_2$, da cui segue $a^{(n-1)/2} \equiv 1$ mod p_2

Riassumendo, per tale scelta di a si ottiene

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

Solovay-Strassen - VI

Le applicazioni

$$a \mapsto \left(\frac{a}{n}\right), \qquad a \mapsto a^{(n-1)/2}$$

sono entrambe omomorfismi di gruppi $(\mathbb{Z}/n)^\times \to (\mathbb{Z}/n)^\times$.

Se $\phi, \psi : G \to H$ sono due omomorfismi di gruppi, allora $X = \{g \in G \,|\, \phi(g) = \psi(g)\}$ è sicuramente un sottogruppo di G, che non può essere tutto G se ϕ, ψ differiscono su almeno un elemento.

Ma per il teorema di Lagrange, l'ordine di un sottogruppo di G divide $|G|$, e quindi $|X| \leq |G|/2$: i due omomorfismi devono pertanto assumere valore diverso su almeno la metà dei possibili argomenti.

Simbolo di Jacobi - I

E' possibile calcolare il simbolo di Legendre 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 di un numero 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 di un numero 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

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

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 di un numero 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.

Perché funziona? - IV

In altre parole, tutto ciò che vale per numeri primi dispari vale anche per numeri dispari che ne sono prodotto (e ogni numero dispari è prodotto di primi dispari).

Il calcolo del simbolo di Legendre attraverso le proprietà del simbolo di Jacobi ha la stessa velocità di un algoritmo euclideo, nel quale possiamo tirare via ogni fattore 2.

Esercizio: stabilire se 13081 sia primo.

Un esempio concreto

Esercizio: stabilire se 13081 sia primo. ($13081 = 103 \cdot 127$)

$$\left(\frac{2}{13081}\right) = 1, \qquad 2^{6540} \equiv 2036 \mod 13081.$$

$$\left(\frac{3}{13081}\right) = 1, \qquad 3^{6540} \equiv 9231 \mod 13081.$$

$$\left(\frac{5}{13081}\right) = 1, \qquad 5^{6540} \equiv 5596 \mod 13081.$$

$$\left(\frac{7}{13081}\right) = -1, \qquad 7^{6540} \equiv 4031 \mod 13081.$$

Le uniche (poche!) scelte per le quali la congruenza è rispettata sono:

$$\pm 1, \pm 253, \pm 1396, \pm 1544, \pm 1797, \pm 1798, \pm 2940, \pm 2941, \pm 3194.$$