Teoria dei Numeri
Legge di reciprocità quadratica

Alessandra Bernardi

Cfr. Note di "Teoria dei Numeri" di Ph. Ellia, 2013–2014

20 marzo 2018, Trento

Legge di reciprocià quadratica

Il teorema dei 2 quadrati si può interpretare come un risultato sulle forme binarie quadratiche:

Quali sono gli interi rappresentati dalla forma $x^2 + y^2$*?*

Più generalmente ci si può chiedere

Quali sono gli interi rappresentati dalla forma $x^2 + ay^2$ *(con* $a \neq 0$*)?*

Eulero: il problema è moltiplicativo:

$$n = t^2 + ak^2,\ m = u^2 + av^2 \Rightarrow mn = x^2 + ay^2.$$

Il problema si riduce a trovare i primi p che si possono scrivere nella forma

$$x^2 + ay^2.$$

Legge di reciprocià quadratica

Il teorema dei 2 quadrati si può interpretare come un risultato sulle forme binarie quadratiche:

Quali sono gli interi rappresentati dalla forma $x^2 + y^2$*?*

Più generalmente ci si può chiedere

Quali sono gli interi rappresentati dalla forma $x^2 + ay^2$ *(con* $a \neq 0$*)?*

Eulero: il problema è moltiplicativo:

$$n = t^2 + ak^2,\ m = u^2 + av^2 \Rightarrow mn = x^2 + ay^2.$$

Il problema si riduce a trovare i primi p che si possono scrivere nella forma

$$x^2 + ay^2.$$

Legge di reciprocià quadratica

Il teorema dei 2 quadrati si può interpretare come un risultato sulle forme binarie quadratiche:

Quali sono gli interi rappresentati dalla forma $x^2 + y^2$*?*

Più generalmente ci si può chiedere

Quali sono gli interi rappresentati dalla forma $x^2 + ay^2$ *(con* $a \neq 0$*)?*

Eulero: il problema è moltiplicativo:

$$n = t^2 + ak^2,\ m = u^2 + av^2 \Rightarrow mn = x^2 + ay^2.$$

Il problema si riduce a trovare i primi p che si possono scrivere nella forma

$$x^2 + ay^2.$$

Legge di reciprocià quadratica

Il teorema dei 2 quadrati si può interpretare come un risultato sulle forme binarie quadratiche:

Quali sono gli interi rappresentati dalla forma $x^2 + y^2$*?*

Più generalmente ci si può chiedere

Quali sono gli interi rappresentati dalla forma $x^2 + ay^2$ *(con* $a \neq 0$*)?*

Eulero: il problema è moltiplicativo:

$$n = t^2 + ak^2,\ m = u^2 + av^2 \Rightarrow mn = x^2 + ay^2.$$

Il problema si riduce a trovare i primi p che si possono scrivere nella forma

$$x^2 + ay^2.$$

Legge di reciprocià quadratica

Cerchiamo i primi p che si possono scrivere nella forma $x^2 + ay^2$.

Chiaramente $p = x^2 + ay^2 \Rightarrow p \mid x^2 + ay^2$. Quindi il primo problema è:

Determinare i primi p t.c. un loro multiplo si scriva nella forma $x^2 + ay^2$.

Per $a = 1$ questo è quello che abbiamo fatto nel caso dei due quadrati.
Ovviamente il caso interessante è se $p \nmid x$ (altrim. sol. banali $p(x^2p + ay^2p) = (xp)^2 + a(yp)^2$). Ossia

Quand'è che la congruenza

$$x^2 + ay^2 \equiv 0 (mod\ p)$$

ha delle soluzioni non banali?

Legge di reciprocià quadratica

Cerchiamo i primi p che si possono scrivere nella forma $x^2 + ay^2$.

Chiaramente $p = x^2 + ay^2 \Rightarrow p \mid x^2 + ay^2$. Quindi il primo problema è:

Determinare i primi p t.c. un loro multiplo si scriva nella forma $x^2 + ay^2$.

Per $a = 1$ questo è quello che abbiamo fatto nel caso dei due quadrati.
Ovviamente il caso interessante è se $p \nmid x$ (altrim. sol. banali $p(x^2p + ay^2p) = (xp)^2 + a(yp)^2$). Ossia

Quand'è che la congruenza

$$x^2 + ay^2 \equiv 0 (mod\ p)$$

ha delle soluzioni non banali?

Legge di reciprocià quadratica

Cerchiamo i primi p che si possono scrivere nella forma $x^2 + ay^2$.

Chiaramente $p = x^2 + ay^2 \Rightarrow p \mid x^2 + ay^2$. Quindi il primo problema è:

Determinare i primi p t.c. un loro multiplo si scriva nella forma $x^2 + ay^2$.

Per $a = 1$ questo è quello che abbiamo fatto nel caso dei due quadrati.

Ovviamente il caso interessante è se $p \nmid x$ (altrim. sol. banali $p(x^2p + ay^2p) = (xp)^2 + a(yp)^2$). Ossia

Quand'è che la congruenza

$$x^2 + ay^2 \equiv 0 (mod\ p)$$

ha delle soluzioni non banali?

Legge di reciprocià quadratica

Cerchiamo i primi p che si possono scrivere nella forma $x^2 + ay^2$.

Chiaramente $p = x^2 + ay^2 \Rightarrow p \mid x^2 + ay^2$. Quindi il primo problema è:

Determinare i primi p t.c. un loro multiplo si scriva nella forma $x^2 + ay^2$.

Per $a = 1$ questo è quello che abbiamo fatto nel caso dei due quadrati.
Ovviamente il caso interessante è se $p \nmid x$ (altrim. sol. banali $p(x^2p + ay^2p) = (xp)^2 + a(yp)^2$). Ossia

Quand'è che la congruenza

$$x^2 + ay^2 \equiv 0 (mod\ p)$$

ha delle soluzioni non banali?

Legge di reciprocià quadratica

Cerchiamo i primi p che si possono scrivere nella forma $x^2 + ay^2$.

Chiaramente $p = x^2 + ay^2 \Rightarrow p \mid x^2 + ay^2$. Quindi il primo problema è:

Determinare i primi p t.c. un loro multiplo si scriva nella forma $x^2 + ay^2$.

Per $a = 1$ questo è quello che abbiamo fatto nel caso dei due quadrati.
Ovviamente il caso interessante è se $p \nmid x$ (altrim. sol. banali $p(x^2p + ay^2p) = (xp)^2 + a(yp)^2$). Ossia

Quand'è che la congruenza

$$x^2 + ay^2 \equiv 0 (mod\ p)$$

ha delle soluzioni non banali?

Legge di reciprocià quadratica

Quand'è che la congruenza $x^2 + ay^2 \equiv 0 (mod\ p)$ ha delle soluzioni non banali?

Se $p \mid a$, la congruenza si riduce a $x^2 \equiv 0 \pmod{p}$, i.e. $x \equiv 0 \pmod{p}$. In conclusione il nostro problema diventa

> *Per quali primi p, con $(a, p) = 1$ la congruenza $x^2 + ay^2 \equiv 0\ (mod\ p)$ ammette soluzioni non banali? (i.e. $xy \not\equiv 0\ (mod\ p)$)*

Osserviamo che se $x^2 + ay^2 \equiv 0 \pmod{p}$, con $xy \not\equiv 0 \pmod{p}$, allora $x^2 \equiv -ay^2 \pmod{p}$ e moltiplicando per $(y^{-1})^2$ si ottiene $-a \equiv (xy^{-1})^2 \pmod{p}$, cioè $-a$ è un quadrato modulo p.
Viceversa se $-a \equiv b^2 \pmod{p}$ allora $mp = b^2 + a \cdot 1^2$ e mp si scrive nella forma $x^2 + ay^2$. Quindi

> *$x^2 + ay^2 \equiv 0\ (mod\ p)$ se e solo se $-a$ è un quadrato modulo p.*

Legge di reciprocià quadratica

Quand'è che la congruenza $x^2 + ay^2 \equiv 0 (mod\ p)$ ha delle soluzioni non banali?

Se $p \mid a$, la congruenza si riduce a $x^2 \equiv 0 \pmod{p}$, i.e. $x \equiv 0 \pmod{p}$. In conclusione il nostro problema diventa

> *Per quali primi p, con $(a, p) = 1$ la congruenza $x^2 + ay^2 \equiv 0\ (mod\ p)$ ammette soluzioni non banali? (i.e. $xy \not\equiv 0\ (mod\ p)$)*

Osserviamo che se $x^2 + ay^2 \equiv 0 \pmod{p}$, con $xy \not\equiv 0 \pmod{p}$, allora $x^2 \equiv -ay^2 \pmod{p}$ e moltiplicando per $(y^{-1})^2$ si ottiene $-a \equiv (xy^{-1})^2 \pmod{p}$, cioè $-a$ è un quadrato modulo p.
Viceversa se $-a \equiv b^2 \pmod{p}$ allora $mp = b^2 + a \cdot 1^2$ e mp si scrive nella forma $x^2 + ay^2$. Quindi

> *$x^2 + ay^2 \equiv 0\ (mod\ p)$ se e solo se $-a$ è un quadrato modulo p.*

Legge di reciprocià quadratica

Quand'è che la congruenza $x^2 + ay^2 \equiv 0 (mod\ p)$ ha delle soluzioni non banali?

Se $p \mid a$, la congruenza si riduce a $x^2 \equiv 0 \pmod{p}$, i.e. $x \equiv 0 \pmod{p}$. In conclusione il nostro problema diventa

> *Per quali primi p, con $(a, p) = 1$ la congruenza $x^2 + ay^2 \equiv 0\ (mod\ p)$ ammette soluzioni non banali? (i.e. $xy \not\equiv 0\ (mod\ p)$)*

Osserviamo che se $x^2 + ay^2 \equiv 0 \pmod{p}$, con $xy \not\equiv 0 \pmod{p}$, allora $x^2 \equiv -ay^2 \pmod{p}$ e moltiplicando per $(y^{-1})^2$ si ottiene $-a \equiv (xy^{-1})^2 \pmod{p}$, cioè $-a$ è un quadrato modulo p.

Viceversa se $-a \equiv b^2 \pmod{p}$ allora $mp = b^2 + a \cdot 1^2$ e mp si scrive nella forma $x^2 + ay^2$. Quindi

> *$x^2 + ay^2 \equiv 0\ (mod\ p)$ se e solo se $-a$ è un quadrato modulo p.*

Legge di reciprocià quadratica

Quand'è che la congruenza $x^2 + ay^2 \equiv 0 (mod\ p)$ ha delle soluzioni non banali?

Se $p \mid a$, la congruenza si riduce a $x^2 \equiv 0 \pmod{p}$, i.e. $x \equiv 0 \pmod{p}$. In conclusione il nostro problema diventa

> *Per quali primi p, con $(a, p) = 1$ la congruenza $x^2 + ay^2 \equiv 0\ (mod\ p)$ ammette soluzioni non banali? (i.e. $xy \not\equiv 0\ (mod\ p)$)*

Osserviamo che se $x^2 + ay^2 \equiv 0 \pmod{p}$, con $xy \not\equiv 0 \pmod{p}$, allora $x^2 \equiv -ay^2 \pmod{p}$ e moltiplicando per $(y^{-1})^2$ si ottiene $-a \equiv (xy^{-1})^2 \pmod{p}$, cioè $-a$ è un quadrato modulo p.

Viceversa se $-a \equiv b^2 \pmod{p}$ allora $mp = b^2 + a \cdot 1^2$ e mp si scrive nella forma $x^2 + ay^2$. Quindi

> *$x^2 + ay^2 \equiv 0\ (mod\ p)$ se e solo se $-a$ è un quadrato modulo p.*

Legge di reciprocià quadratica

Quand'è che la congruenza $x^2 + ay^2 \equiv 0 (mod\ p)$ ha delle soluzioni non banali?
Se $p \mid a$, la congruenza si riduce a $x^2 \equiv 0 \pmod{p}$, i.e. $x \equiv 0 \pmod{p}$. In conclusione il nostro problema diventa

> *Per quali primi p, con $(a, p) = 1$ la congruenza $x^2 + ay^2 \equiv 0\ (mod\ p)$ ammette soluzioni non banali? (i.e. $xy \not\equiv 0\ (mod\ p)$)*

Osserviamo che se $x^2 + ay^2 \equiv 0 \pmod{p}$, con $xy \not\equiv 0 \pmod{p}$, allora $x^2 \equiv -ay^2 \pmod{p}$ e moltiplicando per $(y^{-1})^2$ si ottiene $-a \equiv (xy^{-1})^2 \pmod{p}$, cioè $-a$ è un quadrato modulo p.
Viceversa se $-a \equiv b^2 \pmod{p}$ allora $mp = b^2 + a \cdot 1^2$ e mp si scrive nella forma $x^2 + ay^2$. Quindi

> *$x^2 + ay^2 \equiv 0\ (mod\ p)$ se e solo se $-a$ è un quadrato modulo p.*

Legge di reciprocià quadratica

Bisognerebbe quindi vedere per tutti i primi modulo p che non dividono a, se $-a$ è un quadrato modulo p.

Questa è la direzione verso cui va il risultato di Eulero che si era accorto che per due primi dispari p, q c'è un legame tra il fatto che p sia un quadrato modulo q e il fatto che q sia un quadrato modulo p. Questo legame è la legge di reciprocità quadratica.

Definition

Diciamo che in *carattere quadratico* di $p \pmod q$ è 1 se p è un quadrato modulo q, ed è -1 se p non è un quadrato modulo q.

Theorem (Legge di reciprocità quadratica)

Siano p, q due primi dispari. Allora p, q hanno lo stesso carattere quadratico tranne se sono entrambi congrui a 3 (mod 4) e in tal caso i caratteri sono opposti.

Legge di reciprocià quadratica

Bisognerebbe quindi vedere per tutti i primi modulo p che non dividono a, se $-a$ è un quadrato modulo p.
Questa è la direzione verso cui va il risultato di Eulero che si era accorto che per due primi dispari p, q c'è un legame tra il fatto che p sia un quadrato modulo q e il fatto che q sia un quadrato modulo p. Questo legame è la legge di reciprocità quadratica.

Definition

Diciamo che in *carattere quadratico* di $p \pmod q$ è 1 se p è un quadrato modulo q, ed è -1 se p non è un quadrato modulo q.

Theorem (Legge di reciprocità quadratica)

Siano p, q due primi dispari. Allora p, q hanno lo stesso carattere quadratico tranne se sono entrambi congrui a 3 (mod 4) e in tal caso i caratteri sono opposti.

Legge di reciprocià quadratica

Bisognerebbe quindi vedere per tutti i primi modulo p che non dividono a, se $-a$ è un quadrato modulo p.
Questa è la direzione verso cui va il risultato di Eulero che si era accorto che per due primi dispari p, q c'è un legame tra il fatto che p sia un quadrato modulo q e il fatto che q sia un quadrato modulo p. Questo legame è la legge di reciprocità quadratica.

Definition

Diciamo che in *carattere quadratico* di $p \pmod q$ è 1 se p è un quadrato modulo q, ed è -1 se p non è un quadrato modulo q.

Theorem (Legge di reciprocità quadratica)

Siano p, q due primi dispari. Allora p, q hanno lo stesso carattere quadratico tranne se sono entrambi congrui a 3 (mod 4) e in tal caso i caratteri sono opposti.

Legge di reciprocià quadratica

Bisognerebbe quindi vedere per tutti i primi modulo p che non dividono a, se $-a$ è un quadrato modulo p.
Questa è la direzione verso cui va il risultato di Eulero che si era accorto che per due primi dispari p, q c'è un legame tra il fatto che p sia un quadrato modulo q e il fatto che q sia un quadrato modulo p. Questo legame è la legge di reciprocità quadratica.

Definition

Diciamo che in *carattere quadratico* di $p \pmod q$ è 1 se p è un quadrato modulo q, ed è -1 se p non è un quadrato modulo q.

Theorem (Legge di reciprocità quadratica)

Siano p, q due primi dispari. Allora p, q hanno lo stesso carattere quadratico tranne se sono entrambi congrui a 3 (mod 4) e in tal caso i caratteri sono opposti.

Legge di reciprocià quadratica

Bisognerebbe quindi vedere per tutti i primi modulo p che non dividono a, se $-a$ è un quadrato modulo p.
Questa è la direzione verso cui va il risultato di Eulero che si era accorto che per due primi dispari p, q c'è un legame tra il fatto che p sia un quadrato modulo q e il fatto che q sia un quadrato modulo p. Questo legame è la legge di reciprocità quadratica.

Definition

Diciamo che in *carattere quadratico* di $p \pmod q$ è 1 se p è un quadrato modulo q, ed è -1 se p non è un quadrato modulo q.

Theorem (Legge di reciprocità quadratica)

Siano p, q due primi dispari. Allora p, q hanno lo stesso carattere quadratico tranne se sono entrambi congrui a 3 (mod 4) e in tal caso i caratteri sono opposti.

Legge di reciprocià quadratica

Più precisamente:

Simbolo di Legendre: $\left(\frac{p}{q}\right) =$ il carattere quadratico di $p \pmod q$.

Con questa notazione

Theorem (Legge di reciprocità quadratica)

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}.$$

Nel caso di -1 e 2 si ha

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}.$$

Legge di reciprocià quadratica

Più precisamente:

Simbolo di Legendre: $\left(\frac{p}{q}\right) =$ il carattere quadratico di $p \pmod q$.

Con questa notazione

Theorem (Legge di reciprocità quadratica)

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}.$$

Nel caso di -1 *e* 2 *si ha*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}.$$

Legge di reciprocià quadratica

In realtà il simbolo di Legendre $\left(\frac{a}{p}\right)$ viene definito per ogni $a \in \mathbb{Z}$ con $(a, p) = 1$ e p primo dispari per rappresentare il carattere quadratico di a (mod p) (1 se a è un quadrato (mod p), -1 altrimenti).

Grazie al criterio di Eulero (lo vedremo) il carattere quadratico è moltiplicativo, quindi se $a = \prod p_i$, $\left(\frac{a}{q}\right) = \prod \left(\frac{p_i}{q}\right)$ ma grazie alla reciprocità quadratica e ai complementi possiamo calcolare i $\left(\frac{p_i}{q}\right)$ in funzione di $\left(\frac{q}{p_i}\right)$. Quindi per sapere se a è un quadrato modulo q, basta trovare il carattere quadratico di q (mod p_i) dove i p_i sono i primi che dividono a.

Legge di reciprocià quadratica

In realtà il simbolo di Legendre $\left(\frac{a}{p}\right)$ viene definito per ogni $a \in \mathbb{Z}$ con $(a, p) = 1$ e p primo dispari per rappresentare il carattere quadratico di a (mod p) (1 se a è un quadrato (mod p), -1 altrimenti).
Grazie al criterio di Eulero (lo vedremo) il carattere quadratico è moltiplicativo, quindi se $a = \prod p_i$, $\left(\frac{a}{q}\right) = \prod \left(\frac{p_i}{q}\right)$ ma grazie alla reciprocità quadratica e ai complementi possiamo calcolare i $\left(\frac{p_i}{q}\right)$ in funzione di $\left(\frac{q}{p_i}\right)$. Quindi per sapere se a è un quadrato modulo q, basta trovare il carattere quadratico di q (mod p_i) dove i p_i sono i primi che dividono a.

Legge di reciprocià quadratica

In realtà il simbolo di Legendre $\left(\frac{a}{p}\right)$ viene definito per ogni $a \in \mathbb{Z}$ con $(a, p) = 1$ e p primo dispari per rappresentare il carattere quadratico di a (mod p) (1 se a è un quadrato (mod p), -1 altrimenti).
Grazie al criterio di Eulero (lo vedremo) il carattere quadratico è moltiplicativo, quindi se $a = \prod p_i$, $\left(\frac{a}{q}\right) = \prod \left(\frac{p_i}{q}\right)$ ma grazie alla reciprocità quadratica e ai complementi possiamo calcolare i $\left(\frac{p_i}{q}\right)$ in funzione di $\left(\frac{q}{p_i}\right)$. Quindi per sapere se a è un quadrato modulo q, basta trovare il carattere quadratico di q (mod p_i) dove i p_i sono i primi che dividono a.

Legge di reciprocià quadratica

In realtà il simbolo di Legendre $\left(\frac{a}{p}\right)$ viene definito per ogni $a \in \mathbb{Z}$ con $(a, p) = 1$ e p primo dispari per rappresentare il carattere quadratico di a (mod p) (1 se a è un quadrato (mod p), -1 altrimenti).
Grazie al criterio di Eulero (lo vedremo) il carattere quadratico è moltiplicativo, quindi se $a = \prod p_i$, $\left(\frac{a}{q}\right) = \prod \left(\frac{p_i}{q}\right)$ ma grazie alla reciprocità quadratica e ai complementi possiamo calcolare i $\left(\frac{p_i}{q}\right)$ in funzione di $\left(\frac{q}{p_i}\right)$. Quindi per sapere se a è un quadrato modulo q, basta trovare il carattere quadratico di q (mod p_i) dove i p_i sono i primi che dividono a.

Legge di reciprocià quadratica

In realtà il simbolo di Legendre $\left(\frac{a}{p}\right)$ viene definito per ogni $a \in \mathbb{Z}$ con $(a, p) = 1$ e p primo dispari per rappresentare il carattere quadratico di a (mod p) (1 se a è un quadrato (mod p), -1 altrimenti).
Grazie al criterio di Eulero (lo vedremo) il carattere quadratico è moltiplicativo, quindi se $a = \prod p_i$, $\left(\frac{a}{q}\right) = \prod \left(\frac{p_i}{q}\right)$ ma grazie alla reciprocità quadratica e ai complementi possiamo calcolare i $\left(\frac{p_i}{q}\right)$ in funzione di $\left(\frac{q}{p_i}\right)$. Quindi per sapere se a è un quadrato modulo q, basta trovare il carattere quadratico di q (mod p_i) dove i p_i sono i primi che dividono a.

Legge di reciprocià quadratica

In realtà il simbolo di Legendre $\left(\frac{a}{p}\right)$ viene definito per ogni $a \in \mathbb{Z}$ con $(a, p) = 1$ e p primo dispari per rappresentare il carattere quadratico di a (mod p) (1 se a è un quadrato (mod p), -1 altrimenti).
Grazie al criterio di Eulero (lo vedremo) il carattere quadratico è moltiplicativo, quindi se $a = \prod p_i$, $\left(\frac{a}{q}\right) = \prod \left(\frac{p_i}{q}\right)$ ma grazie alla reciprocità quadratica e ai complementi possiamo calcolare i $\left(\frac{p_i}{q}\right)$ in funzione di $\left(\frac{q}{p_i}\right)$. Quindi per sapere se a è un quadrato modulo q, basta trovare il carattere quadratico di q (mod p_i) dove i p_i sono i primi che dividono a.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato $(\text{mod } p)$, cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7 \,(mod\, 8) \\ -1 & \text{se } p \equiv 3, 5 \,(mod\, 8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

Ora $(-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7\,(mod\,8) \\ -1 & \text{se } p \equiv 3, 5\,(mod\,8) \end{cases}$.

Questa esaurisce tutte le possibilità perché p è primo dispari.

Legge di reciprocià quadratica

Vediamo con un esempio come questo ci può aiutare nel nostro problema iniziale.

Cerchiamo i primi $p > 3$ t.c. un loro multiplo sia della forma $x^2 + 6y^2$ con $xy \not\equiv 0 \pmod{p}$.

Questo corrisponde a vedere se -6 è o no un quadrato (mod p), cioè a calcolare $\left(\frac{-6}{p}\right)$.

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}(-1)^{\frac{(p^2-1)}{8}}\left(\frac{3}{p}\right).$$

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)}{2}\frac{3-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)}{2}}\left(\frac{p}{3}\right).$$

$$\left(\frac{-6}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}\left(\frac{p}{3}\right).$$

$$\text{Ora } (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} +1 & \text{se } p \equiv 1,7\,(mod\,8) \\ -1 & \text{se } p \equiv 3,5\,(mod\,8) \end{cases}.$$

Questa esaurisce tutte le possibilità perché p è primo dispari.

(Rimane da calcolare $\left(\frac{p}{3}\right)$.)

I quadrati (mod 3) sono: $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1 \pmod 3$.

Quindi

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & \text{se } p \equiv 1\,(mod\,3) \\ -1 & \text{se } p \equiv 2\,(mod\,3) \end{cases}$$

Questo esaurisce tutti i casi per $p > 3$ primo ($p \not\equiv 0 \pmod 3$).

Quindi se $p > 3$ primo,

$$\left(\frac{-6}{p}\right) = 1 \text{ se } p \equiv 1, 7\,(mod\,8) \text{ e } p \equiv 1\,(mod\,3)$$

$$\text{oppure se } p \equiv 3, 5\,(mod\,8) \text{ e } p \equiv 2\,(mod\,3).$$

In conclusione se $p > 3$ primo, un multiplo di p è della forma $x^2 + 6y^2$ se e solo se $p \equiv 1, 5, 7, 11 \pmod{24}$.

Legge di reciprocià quadratica

(Rimane da calcolare $\left(\frac{p}{3}\right)$.)
I quadrati (mod 3) sono: $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1 \pmod 3$.
Quindi

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & \text{se } p \equiv 1\,(mod\,3) \\ -1 & \text{se } p \equiv 2\,(mod\,3) \end{cases}$$

Questo esaurisce tutti i casi per $p > 3$ primo ($p \not\equiv 0 \pmod 3$).
Quindi se $p > 3$ primo,

$$\left(\frac{-6}{p}\right) = 1 \text{ se } p \equiv 1,7\,(mod\,8) \text{ e } p \equiv 1\,(mod\,3)$$

$$\text{oppure se } p \equiv 3,5\,(mod\,8) \text{ e } p \equiv 2\,(mod\,3).$$

In conclusione se $p > 3$ primo, un multiplo di p è della forma $x^2 + 6y^2$ se e solo se $p \equiv 1,5,7,11 \pmod{24}$.

Legge di reciprocià quadratica

(Rimane da calcolare $\left(\frac{p}{3}\right)$.)
I quadrati (mod 3) sono: $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1 \pmod 3$.
Quindi

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & \text{se } p \equiv 1\,(mod\,3) \\ -1 & \text{se } p \equiv 2\,(mod\,3) \end{cases}$$

Questo esaurisce tutti i casi per $p > 3$ primo ($p \not\equiv 0 \pmod 3$).
Quindi se $p > 3$ primo,

$$\left(\frac{-6}{p}\right) = 1 \text{ se } p \equiv 1, 7\,(mod\,8) \text{ e } p \equiv 1\,(mod\,3)$$

oppure se $p \equiv 3, 5\,(mod\,8)$ e $p \equiv 2\,(mod\,3)$.

In conclusione se $p > 3$ primo, un multiplo di p è della forma $x^2 + 6y^2$ se e solo se $p \equiv 1, 5, 7, 11 \pmod{24}$.

(Rimane da calcolare $\left(\frac{p}{3}\right)$.)
I quadrati (mod 3) sono: $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1 \pmod 3$.
Quindi

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & \text{se } p \equiv 1 \,(mod\, 3) \\ -1 & \text{se } p \equiv 2 \,(mod\, 3) \end{cases}$$

Questo esaurisce tutti i casi per $p > 3$ primo ($p \not\equiv 0 \pmod 3$).
Quindi se $p > 3$ primo,

$$\left(\frac{-6}{p}\right) = 1 \text{ se } p \equiv 1, 7 \,(mod\, 8) \text{ e } p \equiv 1 \,(mod\, 3)$$

$$\text{oppure se } p \equiv 3, 5 \,(mod\, 8) \text{ e } p \equiv 2 \,(mod\, 3).$$

In conclusione se $p > 3$ primo, un multiplo di p è della forma $x^2 + 6y^2$ se e solo se $p \equiv 1, 5, 7, 11 \pmod{24}$.

(Rimane da calcolare $\left(\frac{p}{3}\right)$.)
I quadrati (mod 3) sono: $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1 \pmod 3$.
Quindi

$$\left(\frac{p}{3}\right) = \begin{cases} +1 & \text{se } p \equiv 1 \,(mod\, 3) \\ -1 & \text{se } p \equiv 2 \,(mod\, 3) \end{cases}$$

Questo esaurisce tutti i casi per $p > 3$ primo ($p \not\equiv 0 \pmod 3$).
Quindi se $p > 3$ primo,

$$\left(\frac{-6}{p}\right) = 1 \text{ se } p \equiv 1, 7 \,(mod\, 8) \text{ e } p \equiv 1 \,(mod\, 3)$$

$$\text{oppure se } p \equiv 3, 5 \,(mod\, 8) \text{ e } p \equiv 2 \,(mod\, 3).$$

In conclusione se $p > 3$ primo, un multiplo di p è della forma $x^2 + 6y^2$ se e solo se $p \equiv 1, 5, 7, 11 \pmod{24}$.

Legge di reciprocià quadratica

Una volta che sappiamo quali sono i primi t.c. uno loro multiplo sia della forma $x^2 + ay^2$, con un argomento di discesa, possiamo sperare di determinare gli interi rappresentanti della forma $x^2 + ay^2$, risolvendo completamente il nostro problema iniziale.
Questo mostra la potenza della legge di reciprocità quadratica (individuata da Eulero, formulata da Legendre ma dim. da Gauss).

Il primo a proporre una dim. della legge di reciprocità quadratica fu Legendre, ma la sua dim. assumeva un risultato ben più profondo: il thm. di Dirichlet sui primi in una progressione aritmetica:

Se $(a, b) = 1$, *esistono infiniti primi della forma* $ax + b$.

Questo teorema è uno dei più profondi della teoria dei numeri e fu dim. da Dirichlet nel 1837.
La dim. di Legendre (1752–1833) era quindi incompleta.

Legge di reciprocià quadratica

Una volta che sappiamo quali sono i primi t.c. uno loro multiplo sia della forma $x^2 + ay^2$, con un argomento di discesa, possiamo sperare di determinare gli interi rappresentanti della forma $x^2 + ay^2$, risolvendo completamente il nostro problema iniziale.
Questo mostra la potenza della legge di reciprocità quadratica (individuata da Eulero, formulata da Legendre ma dim. da Gauss).

Il primo a proporre una dim. della legge di reciprocità quadratica fu Legendre, ma la sua dim. assumeva un risultato ben più profondo: il thm. di Dirichlet sui primi in una progressione aritmetica:

$$\textit{Se } (a, b) = 1, \textit{ esistono infiniti primi della forma } ax + b.$$

Questo teorema è uno dei più profondi della teoria dei numeri e fu dim. da Dirichlet nel 1837.
La dim. di Legendre (1752–1833) era quindi incompleta.

Legge di reciprocià quadratica

La prima dimostrazione della legge di reciprocità quadratica fu data da Gauss nelle "Disquisitiones".

Per Gauss questo teorema era fondamentale, "il gioiello della matematica", quello che gli faceva dire che la teoria dei numeri è la regina della matematica (Gauss ne diede 8 dimostrazioni diverse).

Oggigiorno ci sono circa 200 dimostrazioni più o meno diverse della legge di reciprocità quadratica (dopo il thm. di Pitagora è il risultato più dim. della matematica).

I tentativi di generalizzare questo risultato a leggi di reciprocità cubiche o biquadratiche sono all'origine della teoria algebrica dei numeri.

Al momento il risultato più generale riguardo questa questione sono le leggi di reciprocità di Emil Artin.

Legge di reciprocià quadratica

La prima dimostrazione della legge di reciprocità quadratica fu data da Gauss nelle "Disquisitiones".

Per Gauss questo teorema era fondamentale, "il gioiello della matematica", quello che gli faceva dire che la teoria dei numeri è la regina della matematica (Gauss ne diede 8 dimostrazioni diverse).

Oggigiorno ci sono circa 200 dimostrazioni più o meno diverse della legge di reciprocità quadratica (dopo il thm. di Pitagora è il risultato più dim. della matematica).

I tentativi di generalizzare questo risultato a leggi di reciprocità cubiche o biquadratiche sono all'origine della teoria algebrica dei numeri.

Al momento il risultato più generale riguardo questa questione sono le leggi di reciprocità di Emil Artin.

Legge di reciprocià quadratica

La prima dimostrazione della legge di reciprocità quadratica fu data da Gauss nelle "Disquisitiones".

Per Gauss questo teorema era fondamentale, "il gioiello della matematica", quello che gli faceva dire che la teoria dei numeri è la regina della matematica (Gauss ne diede 8 dimostrazioni diverse).

Oggigiorno ci sono circa 200 dimostrazioni più o meno diverse della legge di reciprocità quadratica (dopo il thm. di Pitagora è il risultato più dim. della matematica).

I tentativi di generalizzare questo risultato a leggi di reciprocità cubiche o biquadratiche sono all'origine della teoria algebrica dei numeri.

Al momento il risultato più generale riguardo questa questione sono le leggi di reciprocità di Emil Artin.

Legge di reciprocià quadratica

La prima dimostrazione della legge di reciprocità quadratica fu data da Gauss nelle "Disquisitiones".

Per Gauss questo teorema era fondamentale, "il gioiello della matematica", quello che gli faceva dire che la teoria dei numeri è la regina della matematica (Gauss ne diede 8 dimostrazioni diverse).

Oggigiorno ci sono circa 200 dimostrazioni più o meno diverse della legge di reciprocità quadratica (dopo il thm. di Pitagora è il risultato più dim. della matematica).

I tentativi di generalizzare questo risultato a leggi di reciprocità cubiche o biquadratiche sono all'origine della teoria algebrica dei numeri.

Al momento il risultato più generale riguardo questa questione sono le leggi di reciprocità di Emil Artin.

Legge di reciprocià quadratica

La prima dimostrazione della legge di reciprocità quadratica fu data da Gauss nelle "Disquisitiones".

Per Gauss questo teorema era fondamentale, "il gioiello della matematica", quello che gli faceva dire che la teoria dei numeri è la regina della matematica (Gauss ne diede 8 dimostrazioni diverse).

Oggigiorno ci sono circa 200 dimostrazioni più o meno diverse della legge di reciprocità quadratica (dopo il thm. di Pitagora è il risultato più dim. della matematica).

I tentativi di generalizzare questo risultato a leggi di reciprocità cubiche o biquadratiche sono all'origine della teoria algebrica dei numeri.

Al momento il risultato più generale riguardo questa questione sono le leggi di reciprocità di Emil Artin.

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.
" $\Leftarrow$ " Se a non è un quadrato $\pmod q$, allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).
L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \pmod q$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x + x' \not\equiv 0 \pmod q$ perchè $x + x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato $\pmod q$, a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.
" $\Leftarrow$ " Se a non è un quadrato $\pmod q$, allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).
L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x + x' \not\equiv 0 \pmod q$ perchè $x + x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato $\pmod q$, a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato $\pmod q$, allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \pmod q$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato $\pmod q$, a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato $\pmod q$, allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \pmod q$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato $\pmod q$, a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato $\pmod q$, allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \pmod q$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x + x' \not\equiv 0 \pmod q$ perchè $x + x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato $\pmod q$, a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x + x' \not\equiv 0 \pmod q$ perchè $x + x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x + x' \not\equiv 0 \pmod q$ perchè $x + x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x + x' \not\equiv 0 \pmod q$ perchè $x + x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \pmod q$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \,(mod\, q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.

" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).

L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \pmod q$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.
" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).
L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \pmod q$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.
" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).
L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.
" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).
L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.
" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).
L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x + x' \not\equiv 0 \pmod q$ perchè $x + x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.
" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).
L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x + x' \not\equiv 0 \pmod q$ perchè $x + x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Il criterio di Eulero

Il problema centrale è determinare se un dato a sia un $\square \pmod p$, $(a,p)=1$.

Theorem (Teorema di Eulero)

Sia q primo, $a \in \mathbb{Z}$, $(a,q)=1$. Allora a è un $\square \pmod q$ sse $a^{\frac{q-1}{2}} \equiv 1 \pmod q$.

Dimostrazione.

" $\Rightarrow$ " Se $a \equiv b^2 \pmod q$ allora $a^{\frac{(q-1)}{2}} \equiv b^{q-1} \equiv 1 \pmod q$ per il Piccolo Teorema di Fermat.
" $\Leftarrow$ " Se a non è un quadrato (mod q), allora $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$ (allora $a^{\frac{(q-1)}{2}} \equiv -1 \pmod q$ perché $a^{\frac{(q-1)}{2}} a^{\frac{(q-1)}{2}} = a^{q-1} \equiv 1 \pmod q$).
L'equazione $x^{\frac{(q-1)}{2}} - 1 \equiv 0 \pmod q$ ha al più $\frac{q-1}{2}$ soluzioni nel campo $\mathbb{F}_q$. Se $x \in \{1,2,\ldots,\frac{q-1}{2}\}$, allora $y = x^2$ verifica $y^{\frac{q-1}{2}} = x^{q-1} \equiv 1 \pmod q$. Può succedere che due quadrati di el. di $\{1,2,\ldots,\frac{q-1}{2}\}$ siano uguali? NO: Se $x, x' \in \{1,2,\ldots,\frac{q-1}{2}\}$ allora $x^2 \not\equiv x'^2 \ (mod\ q)$ altrimenti si avrebbe $x^2 - x'^2 = (x-x')(x+x') \equiv 0 \pmod q$ ma $x+x' \not\equiv 0 \pmod q$ perchè $x+x' \leq q-1$ quindi $x = x'$. In conclusione $p(x) = x^{\frac{q-1}{2}} - 1$ ha tutte le sue radici in $\mathbb{F}_q$ e ogni sua radice è un quadrato. Se a non è un quadrato (mod q), a non è radice di $p(x)$ e $a^{\frac{(q-1)}{2}} \not\equiv 1 \pmod q$. $\square$

Simbolo di Legendre

Definition (Simbolo di Legendre)

Sia q un primo dispari e $n \in \mathbb{Z}$, $n \not\equiv 0 \pmod{q}$. Il simbolo di Legendre è $\left(\frac{n}{q}\right)$ definito da:

$$\left(\frac{n}{q}\right) = \begin{cases} 1 \text{ se } n \text{ è un quadrato } (\mathrm{mod}\ q) \\ -1 \text{ se } n \text{ non è un quadrato } (\mathrm{mod}\ q) \end{cases}.$$

Il criterio di Eulero $\Rightarrow$ simbolo di Legendre è moltiplicativo:

Proposition

Sia q un primo dispari e siano $n_1, n_2 \in \mathbb{Z}$ con $n_1 \cdot n_2 \not\equiv 0 \pmod{q}$, allora:

$$\left(\frac{n_1 \cdot n_2}{q}\right) = \left(\frac{n_1}{q}\right)\left(\frac{n_2}{q}\right)$$

Dimostrazione.

Eulero $\Rightarrow \left(\frac{n_1}{q}\right)\left(\frac{n_2}{q}\right) \equiv n_1^{\frac{q-1}{2}} n_2^{\frac{q-1}{2}} \equiv (n_1 n_2)^{\frac{q-1}{2}} \equiv \left(\frac{n_1 n_2}{q}\right)$. □

Simbolo di Legendre

Definition (Simbolo di Legendre)

Sia q un primo dispari e $n \in \mathbb{Z}$, $n \not\equiv 0 \pmod{q}$. Il simbolo di Legendre è $\left(\frac{n}{q}\right)$ definito da:

$$\left(\frac{n}{q}\right) = \begin{cases} 1 \text{ se } n \text{ è un quadrato } (\text{mod } q) \\ -1 \text{ se } n \text{ non è un quadrato } (\text{mod } q) \end{cases}.$$

Il criterio di Eulero $\Rightarrow$ simbolo di Legendre è moltiplicativo:

Proposition

Sia q un primo dispari e siano $n_1, n_2 \in \mathbb{Z}$ con $n_1 \cdot n_2 \not\equiv 0$ (mod q), allora:

$$\left(\frac{n_1 \cdot n_2}{q}\right) = \left(\frac{n_1}{q}\right)\left(\frac{n_2}{q}\right)$$

Dimostrazione.

Eulero $\Rightarrow \left(\frac{n_1}{q}\right)\left(\frac{n_2}{q}\right) \equiv n_1^{\frac{q-1}{2}} n_2^{\frac{q-1}{2}} \equiv (n_1 n_2)^{\frac{q-1}{2}} \equiv \left(\frac{n_1 n_2}{q}\right)$. □

Simbolo di Legendre

Definition (Simbolo di Legendre)

Sia q un primo dispari e $n \in \mathbb{Z}$, $n \not\equiv 0 \pmod{q}$. Il simbolo di Legendre è $\left(\frac{n}{q}\right)$ definito da:

$$\left(\frac{n}{q}\right) = \begin{cases} 1 \text{ se } n \text{ è un quadrato } (\text{mod } q) \\ -1 \text{ se } n \text{ non è un quadrato } (\text{mod } q) \end{cases}.$$

Il criterio di Eulero $\Rightarrow$ simbolo di Legendre è moltiplicativo:

Proposition

Sia q un primo dispari e siano $n_1, n_2 \in \mathbb{Z}$ con $n_1 \cdot n_2 \not\equiv 0$ (mod q), allora:

$$\left(\frac{n_1 \cdot n_2}{q}\right) = \left(\frac{n_1}{q}\right)\left(\frac{n_2}{q}\right)$$

Dimostrazione.

Eulero $\Rightarrow \left(\frac{n_1}{q}\right)\left(\frac{n_2}{q}\right) \equiv n_1^{\frac{q-1}{2}} n_2^{\frac{q-1}{2}} \equiv (n_1 n_2)^{\frac{q-1}{2}} \equiv \left(\frac{n_1 n_2}{q}\right)$. □

Simbolo di Legendre

Questa proposizione riconduce il calcolo del simbolo di Legendre al caso in cui n è primo (positivo o negativo). Per limitarsi al caso in cui n è primo dispari (positivo) bisogna conoscere $\left(\frac{-1}{q}\right)$ e $\left(\frac{2}{q}\right)$ (i **complementi della legge di reciprocità quadratica**).
Abbiamo già visto il caso -1 (thm. dei 2 quadrati) ma rivediamolo alla luce del criterio di Eulero.

Proposition

Sia q un primo dispari, allora

$$\left(\frac{-1}{q}\right) = \begin{cases} 1 \text{ se } q \equiv 1 \pmod 4 \\ -1 \text{ se } q \equiv 3 \pmod 4 \end{cases}.$$

Dimostrazione.

Per il criterio di Eulero abbiamo $\left(\frac{-1}{q}\right) \equiv (-1)^{\frac{(q-1)}{2}} \pmod q$. Se $q = 4m+1$, viene $(-1)^{2m} = 1$, invece se $q = 4m+3$, viene $(-1)^{2m+1} = -1$. □

Simbolo di Legendre

Questa proposizione riconduce il calcolo del simbolo di Legendre al caso in cui n è primo (positivo o negativo). Per limitarsi al caso in cui n è primo dispari (positivo) bisogna conoscere $\left(\frac{-1}{q}\right)$ e $\left(\frac{2}{q}\right)$ (i **complementi della legge di reciprocità quadratica**).

Abbiamo già visto il caso -1 (thm. dei 2 quadrati) ma rivediamolo alla luce del criterio di Eulero.

Proposition

Sia q un primo dispari, allora

$$\left(\frac{-1}{q}\right) = \begin{cases} 1 \text{ se } q \equiv 1 \pmod 4 \\ -1 \text{ se } q \equiv 3 \pmod 4 \end{cases}.$$

Dimostrazione.

Per il criterio di Eulero abbiamo $\left(\frac{-1}{q}\right) \equiv (-1)^{\frac{(q-1)}{2}} \pmod q$. Se $q = 4m+1$, viene $(-1)^{2m} = 1$, invece se $q = 4m+3$, viene $(-1)^{2m+1} = -1$. □

Simbolo di Legendre

Questa proposizione riconduce il calcolo del simbolo di Legendre al caso in cui n è primo (positivo o negativo). Per limitarsi al caso in cui n è primo dispari (positivo) bisogna conoscere $\left(\frac{-1}{q}\right)$ e $\left(\frac{2}{q}\right)$ (i **complementi della legge di reciprocità quadratica**).
Abbiamo già visto il caso -1 (thm. dei 2 quadrati) ma rivediamolo alla luce del criterio di Eulero.

Proposition

Sia q un primo dispari, allora

$$\left(\frac{-1}{q}\right) = \begin{cases} 1 \text{ se } q \equiv 1 \pmod 4 \\ -1 \text{ se } q \equiv 3 \pmod 4 \end{cases}.$$

Dimostrazione.

Per il criterio di Eulero abbiamo $\left(\frac{-1}{q}\right) \equiv (-1)^{\frac{(q-1)}{2}} \pmod q$. Se $q = 4m+1$, viene $(-1)^{2m} = 1$, invece se $q = 4m+3$, viene $(-1)^{2m+1} = -1$. □

Simbolo di Legendre

Questa proposizione riconduce il calcolo del simbolo di Legendre al caso in cui n è primo (positivo o negativo). Per limitarsi al caso in cui n è primo dispari (positivo) bisogna conoscere $\left(\frac{-1}{q}\right)$ e $\left(\frac{2}{q}\right)$ (i **complementi della legge di reciprocità quadratica**).
Abbiamo già visto il caso -1 (thm. dei 2 quadrati) ma rivediamolo alla luce del criterio di Eulero.

Proposition

Sia q un primo dispari, allora

$$\left(\frac{-1}{q}\right) = \begin{cases} 1 \text{ se } q \equiv 1 \pmod 4 \\ -1 \text{ se } q \equiv 3 \pmod 4 \end{cases}.$$

Dimostrazione.

Per il criterio di Eulero abbiamo $\left(\frac{-1}{q}\right) \equiv (-1)^{\frac{(q-1)}{2}} \pmod q$. Se $q = 4m+1$, viene $(-1)^{2m} = 1$, invece se $q = 4m+3$, viene $(-1)^{2m+1} = -1$. □

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Sia $p > 2$ primo e

$$P := (p-1)/2,$$

allora $-P, \ldots, -1, 0, 1, \ldots, P$ è un sistema completo di residui (mod p).

Lemma (Gauss)

Sia $p > 2$ primo e sia $a \in \mathbb{Z}$, $(a, p) = 1$. Consideriamo i P numeri $a, 2a, 3a, \ldots, Pa$. Per ogni k, $1 \leq k \leq P$, $ka \equiv \pm x \pmod{p}$ con $x \in \{1, 2, \ldots, P\}$. Sia ν il numero di interi negativi così ottenuti, allora:

$$a^{(p-1)/2} \equiv (-1)^{\nu} \pmod{p}.$$

Dimostrazione.

Osserviamo che se $1 \leq k, t \leq P$, $k \neq t$, allora $ka \not\equiv ta \pmod{p}$ (visto che a è invertibile mod p si dovrebbe avere $k \equiv t \pmod{p}$). Se $ka \equiv -ta \pmod{p}$, allora $a(k+t) \equiv 0 \pmod{p}$, ma questo è impossibile perché a è invertibile e $2 \leq k + t \leq 2P = (p-1)$. (continua →) □

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Sia $p > 2$ primo e

$$P := (p-1)/2,$$

allora $-P, \ldots, -1, 0, 1, \ldots, P$ è un sistema completo di residui (mod p).

Lemma (Gauss)

Sia $p > 2$ primo e sia $a \in \mathbb{Z}$, $(a, p) = 1$. Consideriamo i P numeri $a, 2a, 3a, \ldots, Pa$. Per ogni k, $1 \leq k \leq P$, $ka \equiv \pm x \pmod{p}$ con $x \in \{1, 2, \ldots, P\}$. Sia ν il numero di interi negativi così ottenuti, allora:

$$a^{(p-1)/2} \equiv (-1)^{\nu} \pmod{p}.$$

Dimostrazione.

Osserviamo che se $1 \leq k, t \leq P$, $k \neq t$, allora $ka \not\equiv ta \pmod{p}$ (visto che a è invertibile mod p si dovrebbe avere $k \equiv t \pmod{p}$). Se $ka \equiv -ta \pmod{p}$, allora $a(k+t) \equiv 0 \pmod{p}$, ma questo è impossibile perché a è invertibile e $2 \leq k + t \leq 2P = (p-1)$. (continua →) □

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Sia $p > 2$ primo e

$$P := (p-1)/2,$$

allora $-P, \ldots, -1, 0, 1, \ldots, P$ è un sistema completo di residui (mod p).

Lemma (Gauss)

Sia $p > 2$ primo e sia $a \in \mathbb{Z}$, $(a, p) = 1$. Consideriamo i P numeri $a, 2a, 3a, \ldots, Pa$. Per ogni k, $1 \leq k \leq P$, $ka \equiv \pm x \pmod{p}$ con $x \in \{1, 2, \ldots, P\}$. Sia ν il numero di interi negativi così ottenuti, allora:

$$a^{(p-1)/2} \equiv (-1)^{\nu} \pmod{p}.$$

Dimostrazione.

Osserviamo che se $1 \leq k, t \leq P$, $k \neq t$, allora $ka \not\equiv ta \pmod{p}$ (visto che a è invertibile mod p si dovrebbe avere $k \equiv t \pmod{p}$). Se $ka \equiv -ta \pmod{p}$, allora $a(k+t) \equiv 0 \pmod{p}$, ma questo è impossibile perché a è invertibile e $2 \leq k + t \leq 2P = (p-1)$. (continua $\rightarrow$) $\square$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Sia $p > 2$ primo e

$$P := (p-1)/2,$$

allora $-P, \ldots, -1, 0, 1, \ldots, P$ è un sistema completo di residui (mod p).

Lemma (Gauss)

Sia $p > 2$ primo e sia $a \in \mathbb{Z}$, $(a, p) = 1$. Consideriamo i P numeri $a, 2a, 3a, \ldots, Pa$. Per ogni k, $1 \leq k \leq P$, $ka \equiv \pm x \pmod{p}$ con $x \in \{1, 2, \ldots, P\}$. Sia ν il numero di interi negativi così ottenuti, allora:

$$a^{(p-1)/2} \equiv (-1)^{\nu} \pmod{p}.$$

Dimostrazione.

Osserviamo che se $1 \leq k, t \leq P$, $k \neq t$, allora $ka \not\equiv ta \pmod{p}$ (visto che a è invertibile mod p si dovrebbe avere $k \equiv t \pmod{p}$). Se $ka \equiv -ta \pmod{p}$, allora $a(k+t) \equiv 0 \pmod{p}$, ma questo è impossibile perché a è invertibile e $2 \leq k + t \leq 2P = (p-1)$. (continua $\rightarrow$) □

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Sia $p > 2$ primo e

$$P := (p-1)/2,$$

allora $-P, \ldots, -1, 0, 1, \ldots, P$ è un sistema completo di residui (mod p).

Lemma (Gauss)

Sia $p > 2$ primo e sia $a \in \mathbb{Z}$, $(a, p) = 1$. Consideriamo i P numeri $a, 2a, 3a, \ldots, Pa$. Per ogni k, $1 \leq k \leq P$, $ka \equiv \pm x \pmod{p}$ con $x \in \{1, 2, \ldots, P\}$. Sia ν il numero di interi negativi così ottenuti, allora:

$$a^{(p-1)/2} \equiv (-1)^{\nu} \pmod{p}.$$

Dimostrazione.

Osserviamo che se $1 \leq k, t \leq P$, $k \neq t$, allora $ka \not\equiv ta \pmod{p}$ (visto che a è invertibile mod p si dovrebbe avere $k \equiv t \pmod{p}$). Se $ka \equiv -ta \pmod{p}$, allora $a(k+t) \equiv 0 \pmod{p}$, ma questo è impossibile perché a è invertibile e $2 \leq k + t \leq 2P = (p-1)$. (continua →) □

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Sia $p > 2$ primo e

$$P := (p-1)/2,$$

allora $-P, \ldots, -1, 0, 1, \ldots, P$ è un sistema completo di residui (mod p).

Lemma (Gauss)

Sia $p > 2$ primo e sia $a \in \mathbb{Z}$, $(a, p) = 1$. Consideriamo i P numeri $a, 2a, 3a, \ldots, Pa$. Per ogni k, $1 \leq k \leq P$, $ka \equiv \pm x \pmod{p}$ con $x \in \{1, 2, \ldots, P\}$. Sia ν il numero di interi negativi così ottenuti, allora:

$$a^{(p-1)/2} \equiv (-1)^{\nu} \pmod{p}.$$

Dimostrazione.

Osserviamo che se $1 \leq k, t \leq P$, $k \neq t$, allora $ka \not\equiv ta \pmod{p}$ (visto che a è invertibile mod p si dovrebbe avere $k \equiv t \pmod{p}$). Se $ka \equiv -ta \pmod{p}$, allora $a(k+t) \equiv 0 \pmod{p}$, ma questo è impossibile perché a è invertibile e $2 \leq k + t \leq 2P = (p-1)$. (continua $\rightarrow$) $\square$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Sia $p > 2$ primo e

$$P := (p-1)/2,$$

allora $-P, \ldots, -1, 0, 1, \ldots, P$ è un sistema completo di residui (mod p).

Lemma (Gauss)

Sia $p > 2$ primo e sia $a \in \mathbb{Z}$, $(a, p) = 1$. Consideriamo i P numeri $a, 2a, 3a, \ldots, Pa$. Per ogni k, $1 \leq k \leq P$, $ka \equiv \pm x \pmod{p}$ con $x \in \{1, 2, \ldots, P\}$. Sia ν il numero di interi negativi così ottenuti, allora:

$$a^{(p-1)/2} \equiv (-1)^{\nu} \pmod{p}.$$

Dimostrazione.

Osserviamo che se $1 \leq k, t \leq P$, $k \neq t$, allora $ka \not\equiv ta \pmod{p}$ (visto che a è invertibile mod p si dovrebbe avere $k \equiv t \pmod{p}$). Se $ka \equiv -ta \pmod{p}$, allora $a(k+t) \equiv 0 \pmod{p}$, ma questo è impossibile perché a è invertibile e $2 \leq k + t \leq 2P = (p-1)$. (continua $\rightarrow$) $\square$

Dimostrazione.

Abbiamo detto che $ka \not\equiv \pm ta \pmod{p}$ (con $1 \leq k, t \leq P$ e $k \neq t$).
Quindi quando riduciamo mod p i P numeri $a, 2a, \ldots, Pa$, con dei rappresentati x, $-P \leq x \leq P$, ogni elemento di $\{1, 2, 3, \ldots, P\}$ compare una sola volta con un segno ben determinato, cioè:

$$\{a, 2a, \ldots, Pa\} \equiv \{\varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \ldots, \varepsilon_P \cdot P\} \ (mod\ p),\ \varepsilon_i \in \{-1, 1\},\ \forall i.$$

Pertanto:

$$a(2a)\cdots(Pa) \equiv (\varepsilon_1 \cdot 1)(\varepsilon_2 \cdot 2)\cdots(\varepsilon_P \cdot P) \ (mod\ p)$$

semplificando per $P!$ viene:

$$a^{(p-1)/2} = a^P \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_P = (-1)^\nu \ (mod\ p).$$

Dimostrazione.

Abbiamo detto che $ka \not\equiv \pm ta \pmod{p}$ (con $1 \leq k, t \leq P$ e $k \neq t$). Quindi quando riduciamo mod p i P numeri $a, 2a, \ldots, Pa$, con dei rappresentati x, $-P \leq x \leq P$, ogni elemento di $\{1, 2, 3, \ldots, P\}$ compare una sola volta con un segno ben determinato, cioè:

$$\{a, 2a, \ldots, Pa\} \equiv \{\varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \ldots, \varepsilon_P \cdot P\} \ (mod\ p),\ \varepsilon_i \in \{-1, 1\},\ \forall i.$$

Pertanto:

$$a(2a) \cdots (Pa) \equiv (\varepsilon_1 \cdot 1)(\varepsilon_2 \cdot 2) \cdots (\varepsilon_P \cdot P) \ (mod\ p)$$

semplificando per $P!$ viene:

$$a^{(p-1)/2} = a^P \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_P = (-1)^\nu \ (mod\ p).$$

□

Dimostrazione.

Abbiamo detto che $ka \not\equiv \pm ta \pmod{p}$ (con $1 \leq k, t \leq P$ e $k \neq t$). Quindi quando riduciamo mod p i P numeri $a, 2a, \ldots, Pa$, con dei rappresentati x, $-P \leq x \leq P$, ogni elemento di $\{1, 2, 3, \ldots, P\}$ compare una sola volta con un segno ben determinato, cioè:

$$\{a, 2a, \ldots, Pa\} \equiv \{\varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \ldots, \varepsilon_P \cdot P\} \ (mod\ p),\ \varepsilon_i \in \{-1, 1\},\ \forall i.$$

Pertanto:

$$a(2a)\cdots(Pa) \equiv (\varepsilon_1 \cdot 1)(\varepsilon_2 \cdot 2)\cdots(\varepsilon_P \cdot P) \ (mod\ p)$$

semplificando per $P!$ viene:

$$a^{(p-1)/2} = a^P \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_P = (-1)^\nu \ (mod\ p).$$

Dimostrazione.

Abbiamo detto che $ka \not\equiv \pm ta \pmod{p}$ (con $1 \leq k, t \leq P$ e $k \neq t$). Quindi quando riduciamo mod p i P numeri $a, 2a, \ldots, Pa$, con dei rappresentati x, $-P \leq x \leq P$, ogni elemento di $\{1, 2, 3, \ldots, P\}$ compare una sola volta con un segno ben determinato, cioè:

$$\{a, 2a, \ldots, Pa\} \equiv \{\varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \ldots, \varepsilon_P \cdot P\} \ (mod\ p),\ \varepsilon_i \in \{-1, 1\},\ \forall i.$$

Pertanto:

$$a(2a)\cdots(Pa) \equiv (\varepsilon_1 \cdot 1)(\varepsilon_2 \cdot 2)\cdots(\varepsilon_P \cdot P) \ (mod\ p)$$

semplificando per $P!$ viene:

$$a^{(p-1)/2} = a^P \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_P = (-1)^\nu \ (mod\ p).$$

Dimostrazione.

Abbiamo detto che $ka \not\equiv \pm ta \pmod{p}$ (con $1 \leq k, t \leq P$ e $k \neq t$). Quindi quando riduciamo mod p i P numeri $a, 2a, \ldots, Pa$, con dei rappresentati x, $-P \leq x \leq P$, ogni elemento di $\{1, 2, 3, \ldots, P\}$ compare una sola volta con un segno ben determinato, cioè:

$$\{a, 2a, \ldots, Pa\} \equiv \{\varepsilon_1 \cdot 1, \varepsilon_2 \cdot 2, \ldots, \varepsilon_P \cdot P\} \ (mod\ p),\ \varepsilon_i \in \{-1, 1\},\ \forall i.$$

Pertanto:

$$a(2a)\cdots(Pa) \equiv (\varepsilon_1 \cdot 1)(\varepsilon_2 \cdot 2)\cdots(\varepsilon_P \cdot P) \ (mod\ p)$$

semplificando per $P!$ viene:

$$a^{(p-1)/2} = a^P \equiv \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_P = (-1)^\nu \ (mod\ p).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Per il criterio di Eulero otteniamo

Corollary

Con le notazioni precedenti

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \nu \text{ è pari.}$$

Vediamo come questo risultato ci permette di calcolare $\left(\frac{2}{p}\right)$.

Lemma

Siano $\alpha < \beta$ due numeri reali e siano $s, t \in \mathbb{N}$. Sia $I =]\alpha, \beta[$, $J =]\alpha + 2s, \beta + 2s + 2t[$. Sia $i(I)$ il numero di interi contenuti nell'intervallo I. Allora $i(J) = i(I) + 2t$, in particolare $i(I) \equiv i(J) \pmod 2$.

Dimostrazione.

Esercizio. □

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Per il criterio di Eulero otteniamo

Corollary

Con le notazioni precedenti

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \nu \text{ è pari.}$$

Vediamo come questo risultato ci permette di calcolare $\left(\frac{2}{p}\right)$.

Lemma

Siano $\alpha < \beta$ due numeri reali e siano $s, t \in \mathbb{N}$. Sia $I =]\alpha, \beta[$, $J =]\alpha + 2s, \beta + 2s + 2t[$. Sia $i(I)$ il numero di interi contenuti nell'intervallo I. Allora $i(J) = i(I) + 2t$, in particolare $i(I) \equiv i(J)$ (mod 2).

Dimostrazione.

Esercizio. □

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$.

Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$.

Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Cerchiamo di calcolare $\left(\frac{2}{p}\right)$.

Consideriamo i numeri $2, 4, 6, \ldots, 2P = p - 1$. Quando li riduciamo (mod p) con dei rappresentanti tra $-P$ e P, quelli che hanno dei rappresentanti negativi sono i multipli di 2 (son tutti pari) t.c. $P < 2n \leq 2P = p - 1$ (quelli più grandi di P). Siccome n è intero questa disuguaglianza è equivalente a $p/2 < 2n < p$, cioè $p/4 < n < p/2$. Per il Lemma di Gauss con $a = 2$, dobbiamo quindi trovare la parità del numero di interi in $J =]p/4, p/2[$. Poniamo $p = 8k + r$ con $r \in \{1, 3, 5, 7\}$. Abbiamo $J =]2k + r/4, 4k + r/2[$. Per l'ultimo Lemma la parità di $i(J)$ è uguale alla parità di $i(I)$ dove $I =]r/4, r/2[$, $(i(J) = i(I) + 2k)$. Siccome il numero di interi in I è

- 0 se $r = 1$,
- 1 se $r = 3, 5$,
- 2 se $r = 7$,

otteniamo $i(J)$ è pari se e solo se $p \equiv 1, 7 \pmod 8$. Ora per il Lemma di Gauss segue che:

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ (mod 8).

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12), \ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Proposition (Secondo complemento)

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 8)$$

cioè 2 è un quadrato (mod p) se e solo se $p \equiv 1, 7$ *(mod 8).*

Esattamente nello stesso modo si dimostra che

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \ (mod\, 12),\ p > 3.$$

Si considera $3, 6, \ldots, 3P = 3(p-1)/2$. Nella riduzione (mod p) con rappresentanti tra $-P$ e P avremo dei termini negativi per multipli di 3 che $P < 3n < p$. Infatti i $(p-1)/2$ successivi $p+1, \ldots, p+P = (3p-1)/2$ hanno tutti rappresentanti positivi e $3(p-1)/2 < (3p-1)/2$. Quindi dobbiamo trovare la parità di $i(J)$ dove $J =]p/6, p/3[$. Dividiamo p per $12 = 3 \cdot 4$: $p = 12k + r$, $0 < r < 12$, quindi $J =]2k + r/6, 4k + r/3[$. Per l'ultimo lemma la parità di $i(J)$ è la stessa di quella di $i(I)$ dove $I =]r/6, r/3[$. I resti possibili sono $r = 1, 5, 7, 11$. Nel secondo e terzo caso $i(I) = 1$, nel primo $i(I) = 0$, nell'ultimo $i(I) = 2$ e il risultato segue.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:

- Determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/(2a) < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/(2a), p/a[$.
- Si divide p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per l'ultimo lemma basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. In particolare se p, q sono due primi che hanno lo stesso resto nella divisione per $4a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione vale se i resti sono r e $4a - r$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:

- Determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/(2a) < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/(2a), p/a[$.
- Si divide p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per l'ultimo lemma basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. In particolare se p, q sono due primi che hanno lo stesso resto nella divisione per $4a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione vale se i resti sono r e $4a - r$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:

- Determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/(2a) < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/(2a), p/a[$.
- Si divide p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per l'ultimo lemma basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. In particolare se p, q sono due primi che hanno lo stesso resto nella divisione per $4a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione vale se i resti sono r e $4a - r$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:

- Determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/(2a) < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/(2a), p/a[$.
- Si divide p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per l'ultimo lemma basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. In particolare se p, q sono due primi che hanno lo stesso resto nella divisione per $4a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione vale se i resti sono r e $4a - r$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:

- Determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/(2a) < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/(2a), p/a[$.
- Si divide p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per l'ultimo lemma basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. In particolare se p, q sono due primi che hanno lo stesso resto nella divisione per $4a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione vale se i resti sono r e $4a - r$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:

- Determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/(2a) < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/(2a), p/a[$.
- Si divide p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per l'ultimo lemma basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. In particolare se p, q sono due primi che hanno lo stesso resto nella divisione per $4a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione vale se i resti sono r e $4a - r$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:

- Determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/(2a) < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/(2a), p/a[$.
- Si divide p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per l'ultimo lemma basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. In particolare se p, q sono due primi che hanno lo stesso resto nella divisione per $4a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione vale se i resti sono r e $4a - r$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:

- Determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/(2a) < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/(2a), p/a[$.
- Si divide p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per l'ultimo lemma basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. In particolare se p, q sono due primi che hanno lo stesso resto nella divisione per $4a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione vale se i resti sono r e $4a - r$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se analizziamo queste dimostrazioni (casi $a = 2, 3$ del calcolo di $\left(\frac{a}{p}\right)$) vediamo che abbiamo seguito lo schema seguente:

- Determinare la parità del numero di "termini negativi" è equivalente a conoscere la parità del numero di multipli di a che si trovano nell'intervallo $]p/2, p[$, cioè $p/2 < an < p$, quindi $p/(2a) < n < p/a$. Pertanto dobbiamo determinare la parità di $i(J)$ dove $J =]p/(2a), p/a[$.
- Si divide p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Allora $J =]2k + r/2a, 4k + r/a[$. Per l'ultimo lemma basta determinare la parità di $i(I)$ dove $I =]r/2a, r/a[$. In particolare se p, q sono due primi che hanno lo stesso resto nella divisione per $4a$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Eulero ha anche osservato che la stessa conclusione vale se i resti sono r e $4a - r$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Eulero era arrivato a questa conclusione

> $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ *se e solo se* p *e* q *hanno lo stesso resto nella divisione per* $4a$ *o hanno resti "opposti" (i.e.* r *e* $4a - r$*);*
> *negli altri casi* $\left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) = -1$.

Questo enunciato (di Eulero!) è (vedremo) equivalente alla legge di reciprocità quadratica. La dimostrazione generale secondo le linee precedenti si complica perché i "termini negativi" non sono necessariamente in un unico intervallo, ma rimane comunque elementare. Vediamola.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti (mod p) tra $-P$ e P sono negativi. Se prendiamo un **multiplo di** p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, \ldots, cp+P$ sono risp. congrui a $1, 2, \ldots, P$ (mod p). I successivi P numeri $cp+P+1, cp+P+2, \ldots, \mathbf{cp+2P}$ sono congrui a $-P, -P+1 \ldots, -1 (P+1 = p-P)$. Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, $\mathbf{cp+2P} \leq aP$, cioè $c+1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c+1 = a/2$ se a è pari ($c+1 = (a-1)/2$ se a è dispari). In conclusione dobbiamo determinare la parità ν del numero di multipli di a contenuti negli intervalli

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, \ldots,](2b-1)p/2, bp[, \ldots,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti (mod p) tra $-P$ e P sono negativi. Se prendiamo un **multiplo di** p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, \ldots, cp+P$ sono risp. congrui a $1, 2, \ldots, P$ (mod p). I successivi P numeri $cp+P+1, cp+P+2, \ldots, \mathbf{cp+2P}$ sono congrui a $-P, -P+1 \ldots, -1 (P+1 = p-P)$. Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, $\mathbf{cp+2P} \leq aP$, cioè $c+1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c+1 = a/2$ se a è pari ($c+1 = (a-1)/2$ se a è dispari). In conclusione dobbiamo determinare la parità ν del numero di multipli di a contenuti negli intervalli

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, \ldots,](2b-1)p/2, bp[, \ldots,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti (mod p) tra $-P$ e P sono negativi. Se prendiamo un **multiplo di** p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, \ldots, cp+P$ sono risp. congrui a $1, 2, \ldots, P$ (mod p). I successivi P numeri $cp+P+1, cp+P+2, \ldots, \mathbf{cp+2P}$ sono congrui a $-P, -P+1 \ldots, -1 (P+1 = p-P)$. Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, $\mathbf{cp+2P} \leq aP$, cioè $c+1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c+1 = a/2$ se a è pari ($c+1 = (a-1)/2$ se a è dispari). In conclusione dobbiamo determinare la parità ν del numero di multipli di a contenuti negli intervalli

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, \ldots,](2b-1)p/2, bp[, \ldots,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti (mod p) tra $-P$ e P sono negativi. Se prendiamo un **multiplo di** p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, \ldots, cp+P$ sono risp. congrui a $1, 2, \ldots, P$ (mod p). I successivi P numeri $cp+P+1, cp+P+2, \ldots, \mathbf{cp+2P}$ sono congrui a $-P, -P+1 \ldots, -1 (P+1 = p-P)$. Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, $\mathbf{cp+2P} \leq aP$, cioè $c+1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c+1 = a/2$ se a è pari ($c+1 = (a-1)/2$ se a è dispari). In conclusione dobbiamo determinare la parità ν del numero di multipli di a contenuti negli intervalli

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, \ldots,](2b-1)p/2, bp[, \ldots,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti (mod p) tra $-P$ e P sono negativi. Se prendiamo un **multiplo di** p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, \ldots, cp+P$ sono risp. congrui a $1, 2, \ldots, P$ (mod p). I successivi P numeri $cp+P+1, cp+P+2, \ldots, \mathbf{cp+2P}$ sono congrui a $-P, -P+1 \ldots, -1 (P+1 = p-P)$. Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, $\mathbf{cp+2P} \leq aP$, cioè $c+1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c+1 = a/2$ se a è pari ($c+1 = (a-1)/2$ se a è dispari). In conclusione dobbiamo determinare la parità ν del numero di multipli di a contenuti negli intervalli

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, \ldots,](2b-1)p/2, bp[, \ldots,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti (mod p) tra $-P$ e P sono negativi. Se prendiamo un **multiplo di** p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, \ldots, cp+P$ sono risp. congrui a $1, 2, \ldots, P$ (mod p). I successivi P numeri $cp+P+1, cp+P+2, \ldots, \mathbf{cp+2P}$ sono congrui a $-P, -P+1 \ldots, -1 (P+1 = p-P)$. Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, $\mathbf{cp+2P} \leq aP$, cioè $c+1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c+1 = a/2$ se a è pari ($c+1 = (a-1)/2$ se a è dispari). In conclusione dobbiamo determinare la parità ν del numero di multipli di a contenuti negli intervalli

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, \ldots,](2b-1)p/2, bp[, \ldots,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti (mod p) tra $-P$ e P sono negativi. Se prendiamo un **multiplo di** p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, \ldots, cp+P$ sono risp. congrui a $1, 2, \ldots, P$ (mod p). I successivi P numeri $cp+P+1, cp+P+2, \ldots,$ **$cp+2P$** sono congrui a $-P, -P+1 \ldots, -1 (P+1 = p-P)$. Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, **$cp+2P$** $\leq aP$, cioè $c+1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c+1 = a/2$ se a è pari ($c+1 = (a-1)/2$ se a è dispari). In conclusione dobbiamo determinare la parità ν del numero di multipli di a contenuti negli intervalli

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, \ldots,](2b-1)p/2, bp[, \ldots,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti (mod p) tra $-P$ e P sono negativi. Se prendiamo un **multiplo di** p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, \ldots, cp+P$ sono risp. congrui a $1, 2, \ldots, P$ (mod p). I successivi P numeri $cp+P+1, cp+P+2, \ldots, \mathbf{cp+2P}$ sono congrui a $-P, -P+1 \ldots, -1 (P+1 = p-P)$. Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, $\mathbf{cp+2P} \leq aP$, cioè $c+1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c+1 = a/2$ se a è pari ($c+1 = (a-1)/2$ se a è dispari). In conclusione dobbiamo determinare la parità ν del numero di multipli di a contenuti negli intervalli

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, \ldots,](2b-1)p/2, bp[, \ldots,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Si tratta quindi di determinare la parità del numero di multipli di a, $\leq aP$, che ridotti (mod p) tra $-P$ e P sono negativi. Se prendiamo un **multiplo di** p, cp, i successivi $(p-1)/2 = P$ numeri, $cp+1, cp+2, \ldots, cp+P$ sono risp. congrui a $1, 2, \ldots, P$ (mod p). I successivi P numeri $cp+P+1, cp+P+2, \ldots, \mathbf{cp+2P}$ sono congrui a $-P, -P+1 \ldots, -1 (P+1 = p-P)$. Il numero successivo è $cp+2P+1 = (c+1)p$ e si ricomincia. Siamo quindi interessati ai multipli di a contenuti in intervalli del tipo $\tilde{J} = [cp+(p+1)/2, (c+1)p-1] = [(2c+1)p/2+1/2, (c+1)p-1]$. Gli interi contenuti in $\tilde{J}$ sono gli stessi di quelli contenuti in $J =](2c+1)p/2, (c+1)p[$. Siccome siamo interessati ai multipli $\leq aP$, $\mathbf{cp+2P} \leq aP$, cioè $c+1 \leq a/2$ e l'ultimo intervallo da considerare sarà per $c+1 = a/2$ se a è pari ($c+1 = (a-1)/2$ se a è dispari). In conclusione dobbiamo determinare la parità ν del numero di multipli di a contenuti negli intervalli

$$]p/2, p[,]3p/2, 2p[,]5p/2, 3p[, \ldots,](2b-1)p/2, bp[, \ldots,](2B-1)p/2, Bp[$$

dove $B = a/2$ se a è pari e $B = (a-1)/2$ se a è dispari.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.

Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$. Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, ν (mod 2) dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a, p) = (a, q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$. Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, ν (mod 2) dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a, p) = (a, q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$. Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, ν (mod 2) dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a, p) = (a, q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$. Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$. Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, ν (mod 2) dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a, p) = (a, q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$.
Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, ν (mod 2) dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a, p) = (a, q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$.
Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, ν (mod 2) dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a, p) = (a, q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$.
Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, ν (mod 2) dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a, p) = (a, q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$.
Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, $\nu \pmod 2$ dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a,p) = (a,q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$.
Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, $\nu \pmod 2$ dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a,p) = (a,q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$. Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, ν (mod 2) dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a, p) = (a, q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Se $\nu \equiv 0 \pmod 2$, allora $\left(\frac{a}{p}\right) = 1$, altrimenti $\left(\frac{a}{p}\right) = -1$.
Dividiamo p per $4a$: $p = 4ak + r$, $0 < r < 4a$. Abbiamo

$$an \in](2b-1)p/2, bp[\Leftrightarrow n \in]4kb - 2k + \frac{r}{2a}(2b-1), 4kb + \frac{r}{a}b[:= J_b.$$

Stiamo quindi cercando la parità del numero di interi contenuti negli intervalli J_b, $1 \leq b \leq B$.Cioè $\nu \equiv i(J_1) + \cdots + i(J_B) \pmod 2$. Sia $I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[$. Per l'ultimo lemma $i(I_b) = i(J_b)$. Quindi $\nu \equiv i(I_1) + \cdots + i(I_B) \pmod 2$. Per b e a fissati, $i(I_b)$ dipende solo da r. Siccome B dipende solo da a, concludiamo che, **fissato a, ν (mod 2) dipende solo da r**. Questo dimostra:

Lemma

Se p, q sono due primi dispari, con $(a,p) = (a,q) = 1$, che hanno lo stesso resto nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Vediamo adesso che se p ha resto r e q ha resto $4a - r$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Per quanto appena visto questo di nuovo si riduce a **mostrare** che la parità del numero di interi negli intervalli

$$I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[,\ 1 \leq b \leq B$$

è la stessa di quella del numero di interi negli intervalli

$$T_b =]\frac{4a-r}{2a}(2b-1), \frac{4a-r}{a}b[,\ 1 \leq b \leq B.$$

Abbiamo $T_b =]4b - 2 - \frac{r}{2a}(2b-1), 4b - \frac{r}{a}b[:=]X, Y[$. Sia $\tilde{T}_b =]4b - Y, 4b - X[$. Allora $\tilde{T}_b =]\frac{r}{a}b, 2 + \frac{r}{2a}(2b-1)[$. Chiaramente $i(T_b) = i(\tilde{T}_b)$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Vediamo adesso che se p ha resto r e q ha resto $4a - r$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
Per quanto appena visto questo di nuovo si riduce a **mostrare** che la parità del numero di interi negli intervalli

$$I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[,\ 1 \leq b \leq B$$

è la stessa di quella del numero di interi negli intervalli

$$T_b =]\frac{4a-r}{2a}(2b-1), \frac{4a-r}{a}b[,\ 1 \leq b \leq B.$$

Abbiamo $T_b =]4b - 2 - \frac{r}{2a}(2b-1), 4b - \frac{r}{a}b[:=]X, Y[$. Sia $\tilde{T}_b =]4b - Y, 4b - X[$. Allora $\tilde{T}_b =]\frac{r}{a}b, 2 + \frac{r}{2a}(2b-1)[$. Chiaramente $i(T_b) = i(\tilde{T}_b)$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Vediamo adesso che se p ha resto r e q ha resto $4a - r$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
Per quanto appena visto questo di nuovo si riduce a **mostrare** che la parità del numero di interi negli intervalli

$$I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[,\ 1 \leq b \leq B$$

è la stessa di quella del numero di interi negli intervalli

$$T_b =]\frac{4a-r}{2a}(2b-1), \frac{4a-r}{a}b[,\ 1 \leq b \leq B.$$

Abbiamo $T_b =]4b - 2 - \frac{r}{2a}(2b-1), 4b - \frac{r}{a}b[:=]X, Y[$. Sia $\tilde{T}_b =]4b - Y, 4b - X[$. Allora $\tilde{T}_b =]\frac{r}{a}b, 2 + \frac{r}{2a}(2b-1)[$. Chiaramente $i(T_b) = i(\tilde{T}_b)$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Vediamo adesso che se p ha resto r e q ha resto $4a - r$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
Per quanto appena visto questo di nuovo si riduce a **mostrare** che la parità del numero di interi negli intervalli

$$I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[,\ 1 \leq b \leq B$$

è la stessa di quella del numero di interi negli intervalli

$$T_b =]\frac{4a-r}{2a}(2b-1), \frac{4a-r}{a}b[,\ 1 \leq b \leq B.$$

Abbiamo $T_b =]4b - 2 - \frac{r}{2a}(2b-1), 4b - \frac{r}{a}b[:=]X, Y[$. Sia $\tilde{T}_b =]4b - Y, 4b - X[$. Allora $\tilde{T}_b =]\frac{r}{a}b, 2 + \frac{r}{2a}(2b-1)[$. Chiaramente $i(T_b) = i(\tilde{T}_b)$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Vediamo adesso che se p ha resto r e q ha resto $4a - r$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
Per quanto appena visto questo di nuovo si riduce a **mostrare** che la parità del numero di interi negli intervalli

$$I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[,\ 1 \leq b \leq B$$

è la stessa di quella del numero di interi negli intervalli

$$T_b =]\frac{4a-r}{2a}(2b-1), \frac{4a-r}{a}b[,\ 1 \leq b \leq B.$$

Abbiamo $T_b =]4b - 2 - \frac{r}{2a}(2b-1), 4b - \frac{r}{a}b[:=]X, Y[$. Sia $\tilde{T}_b =]4b - Y, 4b - X[$. Allora $\tilde{T}_b =]\frac{r}{a}b, 2 + \frac{r}{2a}(2b-1)[$.
Chiaramente $i(T_b) = i(\tilde{T}_b)$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Vediamo adesso che se p ha resto r e q ha resto $4a - r$, allora $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
Per quanto appena visto questo di nuovo si riduce a **mostrare** che la parità del numero di interi negli intervalli

$$I_b =]\frac{r}{2a}(2b-1), \frac{r}{a}b[,\ 1 \leq b \leq B$$

è la stessa di quella del numero di interi negli intervalli

$$T_b =]\frac{4a-r}{2a}(2b-1), \frac{4a-r}{a}b[,\ 1 \leq b \leq B.$$

Abbiamo $T_b =]4b - 2 - \frac{r}{2a}(2b-1), 4b - \frac{r}{a}b[:=]X, Y[$. Sia $\tilde{T}_b =]4b - Y, 4b - X[$. Allora $\tilde{T}_b =]\frac{r}{a}b, 2 + \frac{r}{2a}(2b-1)[$.
Chiaramente $i(T_b) = i(\tilde{T}_b)$.

Prima dim. legge di reciprocità quadratica (linee di Eulero)

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p) = 1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p) = 1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \,(mod\, 2).$$

Questo dimostra

Prima dim. legge di reciprocità quadratica (linee di Eulero)

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

Prima dim. legge di reciprocità quadratica (linee di Eulero)

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

Prima dim. legge di reciprocità quadratica (linee di Eulero)

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

$$I_b \cup \tilde{T}_b =]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[\setminus\{\frac{r}{a}b\}.$$

Osserviamo che sotto le nostre ipotesi rb/a e $r(2b-1)/2a$ non sono interi. Infatti se $rb/a = m$, allora $bp = 4akb + br = a(4kb+m)$ e siccome $(a,p)=1$ segue che $a \mid b$, assurdo perché $b < a$. Nello stesso modo si vede che $r(2b-1)/2a$ non è intero. Abbiamo quindi

$$i(I_b) + i(\tilde{T}_b) = i(]\frac{r}{2a}(2b-1), 2+\frac{r}{2a}(2b-1)[).$$

Se α non è intero si ha chiaramente $i(]\alpha, 2+\alpha[) = 2$ (mentre $i(]n, n+2[) = 1$). In conclusione $i(I_b) + i(T_b) = i(I_b) + i(\tilde{T}_b) = 2$, pertanto

$$\sum_{b=1}^{B} i(I_b) \equiv \sum_{b=1}^{B} i(T_b) \ (mod\, 2).$$

Questo dimostra

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Lemma

Siano p, q due primi dispari e sia $a \in \mathbb{Z}$ t.c. $(a, p) = (a, q) = 1$. Se p ha resto r nella divisione per $4a$ e se q ha resto $4a - r$ nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Gli ultimi due lemmi dimostrano l'affermazione fatta da Eulero e sono equivalenti alla legge di reciprocità quadrtatica.

Theorem (Legge di reciprocità quadratica)

Siano p, q due primi > 2, allora

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Lemma

Siano p, q due primi dispari e sia $a \in \mathbb{Z}$ t.c. $(a, p) = (a, q) = 1$. Se p ha resto r nella divisione per $4a$ e se q ha resto $4a - r$ nella divisione per $4a$, allora

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Gli ultimi due lemmi dimostrano l'affermazione fatta da Eulero e sono equivalenti alla legge di reciprocità quadrtatica.

Theorem (Legge di reciprocità quadratica)

Siano p, q due primi > 2, allora

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k+1$ allora $(p-1)/2$ è pari, mentre se $p = 4j+3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè $(4 = 2^2)$ sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

□

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k + 1$ allora $(p-1)/2$ è pari, mentre se $p = 4j + 3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè $(4 = 2^2)$ sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

□

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k+1$ allora $(p-1)/2$ è pari, mentre se $p = 4j+3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè $(4 = 2^2)$ sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

□

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k + 1$ allora $(p-1)/2$ è pari, mentre se $p = 4j + 3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè $(4 = 2^2)$ sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

□

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k+1$ allora $(p-1)/2$ è pari, mentre se $p = 4j+3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè $(4 = 2^2)$ sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

□

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k + 1$ allora $(p-1)/2$ è pari, mentre se $p = 4j + 3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè ($4 = 2^2$) sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

□

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k+1$ allora $(p-1)/2$ è pari, mentre se $p = 4j+3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè ($4 = 2^2$) sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

□

Dimostrazione.

Osserviamo che se $p = 4k + 1$ allora $(p-1)/2$ è pari, mentre se $p = 4j + 3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè $(4 = 2^2)$ sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k+1$ allora $(p-1)/2$ è pari, mentre se $p = 4j+3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè ($4 = 2^2$) sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

□

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k+1$ allora $(p-1)/2$ è pari, mentre se $p = 4j+3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè ($4 = 2^2$) sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

Analogamente

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

Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

Osserviamo che se $p = 4k+1$ allora $(p-1)/2$ è pari, mentre se $p = 4j+3$, $(p-1)/2$ è dispari. Quindi $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ sse $p \equiv q \equiv 3 \pmod 4$.

- Supponiamo $p \equiv q \pmod 4$. Possiamo assumere $p > q$. Sia $p - q = 4a$. Quindi $p = q + 4a$ e p è un quadrato (mod q) sse $4a$ lo è. Cioè $(4 = 2^2)$ sse a è un quadrato (mod q):

$$\left(\frac{p}{q}\right) = \left(\frac{4a+q}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right).$$

  Analogamente

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

  Siccome $p \equiv q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma). Quindi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)$. Siccome $\left(\frac{-1}{p}\right) = 1$ sse $p \equiv 1 \pmod 4$, abbiamo il risultato cercato ($p \equiv q \pmod 4$ per ip.).

(continua →)

□

Dimostrazione.

- Supponiamo $p \not\equiv q \pmod 4$. In questo caso $p \equiv -q \pmod 4$. Poniamo $p + q = 4a$. Abbiamo

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

Analogamente

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

Siccome $p \equiv -q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma).

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

Dimostrazione.

- Supponiamo $p \not\equiv q \pmod 4$. In questo caso $p \equiv -q \pmod 4$.

  Poniamo $p + q = 4a$. Abbiamo

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

  Analogamente

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

  Siccome $p \equiv -q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma).

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

Prima dim. legge di reciprocità quadratica (linee di Eulero)

Dimostrazione.

- Supponiamo $p \not\equiv q \pmod 4$. In questo caso $p \equiv -q \pmod 4$. Poniamo $p + q = 4a$. Abbiamo

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

Analogamente

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

Siccome $p \equiv -q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma).

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

Dimostrazione.

- Supponiamo $p \not\equiv q \pmod 4$. In questo caso $p \equiv -q \pmod 4$. Poniamo $p + q = 4a$. Abbiamo

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

Analogamente

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

Siccome $p \equiv -q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma).

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

Dimostrazione.

- Supponiamo $p \not\equiv q \pmod 4$. In questo caso $p \equiv -q \pmod 4$. Poniamo $p + q = 4a$. Abbiamo

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

Analogamente

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

Siccome $p \equiv -q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma).

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

Dimostrazione.

- Supponiamo $p \not\equiv q \pmod 4$. In questo caso $p \equiv -q \pmod 4$. Poniamo $p + q = 4a$. Abbiamo

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

Analogamente

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

Siccome $p \equiv -q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma).

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

Dimostrazione.

- Supponiamo $p \not\equiv q \pmod 4$. In questo caso $p \equiv -q \pmod 4$. Poniamo $p + q = 4a$. Abbiamo

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

Analogamente

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

Siccome $p \equiv -q \pmod{4a}$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ (vedi lemma).

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

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod{p}$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod{2}$, viene:
$1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod{2}$. Per differenza tra questa relazione e la precedente otteniamo:
$(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu) \,(mod\, 2)$. Siccome n, p sono dispari, $M \equiv \nu \pmod{2}$ e si conclue con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod{p}$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod{2}$, viene:
$1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod{2}$. Per differenza tra questa relazione e la precedente otteniamo:
$(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu) \ (mod\, 2)$. Siccome n, p sono dispari, $M \equiv \nu \pmod{2}$ e si conclue con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod{p}$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod{2}$, viene:
$1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod{2}$. Per differenza tra questa relazione e la precedente otteniamo:
$(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu) \ (mod\, 2)$. Siccome n, p sono dispari, $M \equiv \nu \pmod{2}$ e si conclue con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod{p}$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod 2$, viene:
$1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod 2$. Per differenza tra questa relazione e la precedente otteniamo:
$(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu) \pmod 2$. Siccome n, p sono dispari, $M \equiv \nu \pmod 2$ e si conclude con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod p$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod 2$, viene:
$1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod 2$. Per differenza tra questa relazione e la precedente otteniamo:
$(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu) \pmod 2$. Siccome n, p sono dispari, $M \equiv \nu \pmod 2$ e si conclude con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod p$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod 2$, viene: $1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod 2$. Per differenza tra questa relazione e la precedente otteniamo: $(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu) \pmod 2$. Siccome n, p sono dispari, $M \equiv \nu \pmod 2$ e si conclue con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod p$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod 2$, viene:
$1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod 2$. Per differenza tra questa relazione e la precedente otteniamo:
$(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu) \pmod 2$. Siccome n, p sono dispari, $M \equiv \nu \pmod 2$ e si conclue con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod p$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod 2$, viene:
$1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod 2$. Per differenza tra questa relazione e la precedente otteniamo:
$(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu)\ (mod\ 2)$. Siccome n, p sono dispari, $M \equiv \nu \pmod 2$ e si conclue con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod p$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod 2$, viene:
$1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod 2$. Per differenza tra questa relazione e la precedente otteniamo:
$(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu) \pmod 2$. Siccome n, p sono dispari, $M \equiv \nu \pmod 2$ e si conclue con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Lemma

Sia $p > 2$ primo e $n > 0$ intero dispari con $(n, p) = 1$. Sia

$$M = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{2n}{p} \right\rfloor + \cdots + \left\lfloor \frac{Pn}{p} \right\rfloor$$

dove $P = (p-1)/2$. Allora $\left(\frac{n}{p}\right) = (-1)^M$.

Dimostrazione.

Per $1 \leq i \leq P$ dividiamo in per p: $in = p\left\lfloor \frac{in}{p} \right\rfloor + r_i$, $0 < r_1 < p$. Sommando queste P equazioni viene $n(1+2+\cdots+P) = pM + r_1 + \cdots + r_P$. Chiaramente $in \equiv r_i \pmod{p}$. Quando riduciamo (mod p) $r_1, \ldots, r_P$ otteniamo P elementi distinti e dal Lemma di Gauss sappiamo che ν tra loro sono $> P$. Se $r_j > P$ lo rimpiazziamo con $r_j - p$, il cui valore assoluto è $p - r_j$. Abbiamo quindi $\{1, 2, \ldots, P\} = \{r_i, -r_j + p\}$. Siccome $x \equiv -x \pmod 2$, viene:
$1 + 2 + \cdots + P \equiv r_1 + r_2 + \cdots + r_P + p\nu \pmod 2$. Per differenza tra questa relazione e la precedente otteniamo:
$(1 + 2 + \cdots + P)(n-1) \equiv p(M - \nu) \pmod 2$. Siccome n, p sono dispari, $M \equiv \nu \pmod 2$ e si conclue con il lemma. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.

Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.

Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

□

Seconda dim. legge di reciprocità quadratica (Eisenstein)

Dimostrazione la legge di recirocità quadratica.

Nel piano (x, y) consideriamo i punti a coordinate intere (x, y), $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$. Denotiamo I l'insieme dei punti così ottenuti. Ovviamente $\sharp(I) = \frac{p-1}{2}\frac{q-1}{2}$. Sia R il rettangolo di vertici $(0,0)$, $(0, q/2)$, $(p/2, 0)$, $(p/2, q/2)$. La diagonale di R ha equazione $y = (q/p)x$ e non contiene nessun punto di I. Infatti se $py = qx$ con x, y interi, allora $p \mid x$ e $q \mid y$.
Per $1 \leq k \leq (p-1)/2$, la retta $x = k$ contiene i punti $(k,1), (k,2), \ldots (k, \lfloor \frac{kq}{p} \rfloor)$, cioè $\lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Quindi ci sono $M = \sum_{k=1}^{(p-1)/2} \lfloor \frac{kq}{p} \rfloor$ punti di I sotto la diagonale. Per il lemma con $n = q$: $\left(\frac{q}{p}\right) = (-1)^M$. Con lo stesso ragionamento ci sono $N = \sum_{k=1}^{(q-1)/2} \lfloor \frac{jp}{q} \rfloor$ punti di I sopra alla diagonale (considerare le rette $y = j$, $1 \leq j \leq (q-1)/2$). Per il lemma con $n = p$: $\left(\frac{p}{q}\right) = (-1)^N$.
Siccome $N + M = \frac{p-1}{2}\frac{q-1}{2} = \sharp(I)$, abbiamo $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{M+N} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □