6 Congruenze quadratiche e legge di reciprocità

Il punto centrale di questo paragrafo è la dimostrazione della Legge di Reciprocità Quadratica (abbreviata LRQ). La prima dimostrazione completa di tale legge risale a Gauss, che la terminò nell'aprile del 1796 (e successivamente lo stesso Gauss ne ha dato almeno altre otto dimostrazioni differenti). Il primo a congetturare la validità della LQR era stato comunque Euler (nel 1745), che ne aveva poi dato anche una dimostrazione (sbagliata) nel 1783, nel suo *Opuscula Analytica*. Infine, A.M. Legendre nel suo lavoro *Recherches d'Analyse Indéterminée* (1785) dapprima, e poi nel volume *Essai sur la Théorie des Nombres* (1798), aveva ridimostrato la LRQ (in forma però incompleta), introducendo una nuova notazione (cioè, il *simbolo di Legendre*), che ne permetteva una formulazione più elegante.

Questa pluralità di contributi doveva quindi scatenare un'accesa disputa tra Euler, Legendre e Gauss, per l'attribuzione di priorità e meriti nella dimostrazione della LRQ. Informazioni più precise al riguardo si trovano in un libro di Bachmann [B], che si è ispirato ad un famoso articolo di Kronecker [K] del 1875.

La teoria delle congruenze quadratiche, cioè delle congruenze del tipo:

$$aX^2 + bX + c \equiv 0 \pmod{p} \tag{1}$$

con $a, b, c \in \mathbb{Z}$ e p primo, è certamente più complessa della teoria delle congruenze lineari, sviluppata nel Paragrafo 2 (ricordiamo che l'ipotesi che p sia primo non è restrittiva, perché possiamo sempre ricondurci a tale caso in base a quanto esposto nel Paragrafo 4). In effetti, la congruenza (1) può non essere risolubile e, se è risolubile, può non essere facile calcolarne le soluzioni. In questo paragrafo illustreremo un procedimento che permetterà di stabilire se (1) è o non è risolubile, ma non forniremo alcun metodo specifico pratico, veramente efficace, per il calcolo delle soluzioni, rinviando per questo alle tecniche generali del paragrafo precedente.

Nel considerare (1) possiamo senz'altro supporre che $p \nmid a$ (in caso contrario, (1) è una congruenza lineare) e che $p \neq 2$ (se $p = 2$, la ricerca delle soluzioni di (1) si riduce ad una banale verifica, cfr. anche il successivo Esercizio 6.1). In tali ipotesi $p \nmid 4a$ e, dunque, (1) è equivalente alla congruenza:

$$4a(aX^2 + bX + c) = (2aX + b)^2 - (b^2 - 4ac) \equiv 0 \pmod{p}.$$

Ponendo $Y := 2aX + b$ e $d := b^2 - 4ac$, (1) è equivalente a

$$Y^2 \equiv d \pmod{p}. \tag{2}$$

La risoluzione di (1) si riduce alla risoluzione di (2) e successivamente, nel caso in cui y_0 sia soluzione di (2), alla risoluzione della congruenza lineare:

$$2aX + b \equiv y_0 \pmod{p}.$$

Si noti che tale congruenza, fissato y_0 ha un'unica soluzione (mod p) data da:

$$x_0 := \frac{p+1}{2}\, a^*(y_0 - b),$$

essendo a^* un inverso aritmetico di $a \pmod p$ e $\frac{p+1}{2}$ un inverso aritmetico di $2 \pmod p$.

Nella prima parte di questo paragrafo ci occuperemo di congruenze quadratiche della forma:

$$X^2 \equiv a \pmod p \tag{3}$$

con p primo dispari ed a intero tale che $\mathrm{MCD}(a,p) = 1$.

Proposizione 6.1. *Se la congruenza* (3) *è risolubile, allora essa ha due soluzioni distinte (cioè incongruenti* (mod p)*).*

Dimostrazione. Il Teorema di Lagrange (cfr. Teorema 4.19) assicura che (3) ha al più due soluzioni. Se x_0 è una soluzione di (3), anche $p - x_0 =: x_1$ è soluzione di (3) (infatti $(p - x_0)^2 \equiv x_0^2 \equiv a \pmod p$).
Inoltre $x_0 \not\equiv x_1 \pmod p$ (altrimenti risulterebbe $p - x_0 \equiv x_0 \pmod p$, da cui $2x_0 \equiv 0 \pmod p$, mentre $p \nmid 2$ e $p \nmid x_0$, perché $p \nmid a$). □

Definizione 6.2. Sia p un primo dispari ed a un intero tale che si abbia $\mathrm{MCD}(a,p) = 1$. Se la congruenza (3) è risolubile, si dirà che a è un *residuo quadratico* di p; in caso contrario, si dirà che a è un *non residuo quadratico* di p.

Proposizione 6.3. *Sia p un primo dispari ed a un intero tale che si abbia* $\mathrm{MCD}(a,p) = 1$. *Allora a è un residuo quadratico di p se, e soltanto se, a è congruente* (mod p) *ad uno dei seguenti interi:*

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

Quindi, tra gli interi $1, 2, \ldots, p-1$, esattamente $\frac{p-1}{2}$ sono residui quadratici di p, mentre gli altri $\frac{p-1}{2}$ non lo sono.

Dimostrazione. È sufficiente osservare che, se a è un residuo quadratico di p, una delle due soluzioni della congruenza (3) è congruente ad uno degli interi $1, 2, \ldots, \frac{p-1}{2}$ (ciò segue immediatamente dalla dimostrazione della Proposizione 6.1). L'implicazione inversa è ovvia.

Per quanto concerne l'ultima affermazione, basta verificare che gli interi $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ sono a due a due incongruenti (mod p) (cfr. anche la dimostrazione del Lemma 4.12). □

Per caratterizzare quando un intero a è un residuo quadratico di p è conveniente introdurre la seguente notazione, dovuta a Legendre:

Definizione 6.4. Sia p un primo dispari ed a un intero tale che si abbia $\mathrm{MCD}(a,p)=1$. Si chiama *simbolo di Legendre* il simbolo così definito:

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{se } a \text{ è un residuo quadratico di } p \\ -1, & \text{se } a \text{ non è un residuo quadratico di } p \end{cases}$$

Se $p=2$ e se a è dispari, allora si pone:

$$\left(\frac{a}{2}\right) = \left(\frac{1}{2}\right) := 1\,.$$

A volte, per avere una definizione valida per ogni intero a, si pone $(\frac{a}{p}) := 0$ se $p \mid a$.

Un primo importante risultato, che otteniamo riformulando il Corollario 5.19, per $m=2$, è il seguente:

Proposizione 6.5. (Criterio di Euler). *Sia p un primo dispari ed a un intero tale che* $\mathrm{MCD}(a,p)=1$. *Risulta:*

$$\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \qquad \square$$

Proposizione 6.6. *Sia p un primo dispari ed siano $a,b \in \mathbb{Z}$ tali che si abbia* $\mathrm{MCD}(a,p)=1=\mathrm{MCD}(b,p)$. *Allora:*

(a) $a \equiv b \pmod{p} \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$;

(b) $(\frac{a^2}{p}) = 1$;

(c) $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$;

(d) $(\frac{a}{p}) = (-1)^{\mathrm{ind}_r(a)}$, *dove r è una radice primitiva* $\pmod{p}$;

(e) $(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$;

(f) $(\frac{1}{p}) = 1$;

(g) $(\frac{a}{p}) = (\frac{a^*}{p})$, *dove a^* è un inverso aritmetico di a* $\pmod{p}$;

(h) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \pmod 4, \\ -1 & \text{se } p \equiv 3 \pmod 4; \end{cases}$

(i) $(\frac{ab^2}{p}) = (\frac{a}{p})$.

Dimostrazione. **(a)**: è del tutto ovvio. **(b)**: basta osservare che a è soluzione della congruenza $X^2 \equiv a^2 \pmod{p}$. **(c)**: dal "Piccolo" Teorema di Fermat segue che $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$ e dunque $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Per concludere basta utilizzare il Criterio di Euler (cfr. Proposizione 6.5). **(d)**: è un'immediata conseguenza del Teorema 5.23 ovvero dell'Osservazione 5.25(2). Infatti, $X^2 \equiv a \pmod{p}$ è risolubile se e soltanto se $2 = \mathrm{MCD}(2, p-1) \mid \mathrm{ind}_r(a)$. **(e)**: risulta $(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \cdot (\frac{b}{p}) \pmod{p}$. Poiché il simbolo di Legendre assume soltanto valori ± 1 e $p > 2$, la congruenza $(\frac{ab}{p}) \equiv (\frac{a}{p}) \cdot (\frac{b}{p}) \pmod{p}$ è un'uguaglianza. **(f)**: è immediata. **(g)**: risulta: $(\frac{a}{p}) \cdot (\frac{a^*}{p}) = (\frac{aa^*}{p}) = (\frac{1}{p}) = 1$. Da ciò segue l'asserto. **(h)**: da (c) segue che $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Ragionando come in (e), essendo $p > 2$, si ha l'uguaglianza. Infine, si osservi che $\frac{p-1}{2}$ è pari (rispettivamente dispari) se, e soltanto se, $p \equiv 1 \pmod{4}$ (rispettivamente, $p \equiv 3 \pmod{4}$). **(i)**: risulta $(\frac{ab^2}{p}) = (\frac{a}{p}) \cdot (\frac{b^2}{p}) = (\frac{a}{p})$. □

Si noti che l'affermazione **(a)** della proposizione precedente non si inverte. Infatti $2 \not\equiv 3 \pmod{5}$, mentre $X^2 \equiv 2 \pmod{5}$ e $X^2 \equiv 3 \pmod{5}$ non sono risolubili, quindi:

$$\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Oppure, $1 \not\equiv 4 \pmod{5}$, però come è subito visto:

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Corollario 6.7. *Nella situazione della Proposizione 6.6, si ha:*

$$\left(\frac{-a^2}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$$

In altre parole la congruenza $X^2 + a^2 \equiv 0 \pmod{p}$ è risolubile se, e soltanto se, $p \equiv 1 \pmod{4}$. □

Corollario 6.8. *Sia p un primo dispari ed a un intero tale che $\mathrm{MCD}(a, p) = 1$. La congruenza:*

$$aX^2 + bX + c \equiv 0 \pmod{p} \tag{1}$$

è risolubile se, e soltanto se, l'intero $b^2 - 4ac$ è un residuo quadratico di p oppure è congruente a zero $\pmod{p}$. □

Dimostrazione. L'enunciato segue dalla "riduzione" discussa all'inizio del paragrafo. □

Corollario 6.9. *Sia p un primo dispari ed $a = \pm p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ un intero tale che* $\mathrm{MCD}(a,p) = 1$. *Allora:*

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \left(\frac{p_1}{p}\right)^{e_1} \cdot \left(\frac{p_2}{p}\right)^{e_2} \cdot \ldots \cdot \left(\frac{p_r}{p}\right)^{e_r}. \quad \square$$

Dal precedente corollario discende che per calcolare $(\frac{a}{p})$ è sufficiente saper calcolare i simboli di Legendre del tipo $(\frac{\pm 1}{p})$ e $(\frac{q}{p})$, con p, q primi distinti. La Legge di Reciprocità Quadratica, come vedremo, riguarderà il calcolo del simbolo $(\frac{q}{p})$, nel caso in cui p, q siano primi distinti *entrambi dispari*.

Corollario 6.10. *Sia p un primo dispari ed r una radice primitiva (modulo p). I residui quadratici di p sono congruenti alle potenze pari di r. Quindi:*

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Dimostrazione. La prima affermazione è una conseguenza immediata della Proposizione 6.6(d) e la seconda della Proposizione 6.3. $\square$

Osservazione 6.11. Siano a, n interi tali che $n > 2$ e $\mathrm{MCD}(a,n) = 1$. In analogia con quanto esposto sopra, diremo che a è un *residuo quadratico* di n se la congruenza $X^2 \equiv a \pmod{n}$ è risolubile. Si verifica facilmente (utilizzando il Teorema di Euler - Fermat) che se a è un residuo quadratico di n, allora $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}$. L'affermazione reciproca è però falsa, in generale. Infatti, se $n = 8$ e $a = 3$, si ha $\varphi(8) = 4$ e $3^2 \equiv 1 \pmod{8}$ mentre la congruenza $X^2 \equiv 3 \pmod{8}$ non è risolubile. (Questo fatto non è in disaccordo con il Corollario 5.24: infatti $n = 8$ è un intero che non ammette radici primitive!)

La maggior parte delle numerose differenti dimostrazioni della LRQ utilizza il seguente risultato, noto come "Lemma di Gauss".

Teorema 6.12. (Lemma di Gauss). *Sia p un primo dispari ed a un intero tale che* $\mathrm{MCD}(a,p) = 1$. *Consideriamo il sistema completo di residui minimo in valore assoluto (modulo p):*

$$\Sigma := \{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$$

e l'insieme

$$S(a) := \{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a\}.$$

Indicato con $\nu = \nu(a)$ il numero degli elementi di $S(a)$ congruenti (modulo p) agli interi negativi di Σ, si ha:

$$\left(\frac{a}{p}\right) = (-1)^{\nu(a)}.$$

Dimostrazione. Osserviamo dapprima che, se h e k sono interi tali che $1 \leqslant h < k \leqslant \frac{p-1}{2}$, allora $ha \not\equiv \pm ka \pmod{p}$. Infatti, se fosse $ha \equiv \pm ka \pmod{p}$, allora $h \equiv \pm k \pmod{p}$ e ciò è assurdo in base alle ipotesi fatte su h e k. Per ogni k tale che $1 \leqslant k \leqslant \frac{p-1}{2}$, esiste un unico $r_k \in \Sigma$ tale che $r_k \equiv ka \pmod{p}$ e, per quanto osservato sopra, l'insieme $\{r_1, \ldots, r_{\frac{p-1}{2}}\}$ è costituito da interi a due a due differenti in valore assoluto (cioè $|r_h| \neq |r_k|$ se $h \neq k$). Ne segue che gli insiemi $\{1, 2, \ldots, \frac{p-1}{2}\}$ e $\{|r_1|, \ldots, |r_{\frac{p-1}{2}}|\}$ coincidono e quindi, in base alla definizione di ν, si ha:

$$\prod_{i=1}^{\frac{p-1}{2}} r_i = (-1)^{\nu} \prod_{i=1}^{\frac{p-1}{2}} |r_i| = (-1)^{\nu} \left(\frac{p-1}{2}\right)!\,.$$

D'altra parte, essendo $r_k \equiv ka \pmod{p}$ $(1 \leqslant k \leqslant \frac{p-1}{2})$, si ha:

$$\left(\frac{p-1}{2}\right)!\; a^{\frac{p-1}{2}} \equiv \prod_{i=1}^{\frac{p-1}{2}} r_i = (-1)^{\nu} \left(\frac{p-1}{2}\right)! \pmod{p}$$

e pertanto, poichè $p \nmid \left(\frac{p-1}{2}\right)!$, applicando la Proposizione 6.6(c), si ha:

$$(-1)^{\nu} \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

da cui (essendo $p > 2$) segue la tesi. $\square$

Osservazione 6.13. Confrontando la Proposizione 6.6 (d) con il Teorema 6.12, si ha $(-1)^{\nu(a)} = (-1)^{\mathrm{ind}_r(a)}$ e dunque $\nu(a) \equiv \mathrm{ind}_r(a) \pmod{2}$. Non è detto però che $\nu(a) = \mathrm{ind}_r(a)$: ad esempio, ponendo $p = 7$, $r = 5$ e $a = 2$ si verifica che $\nu(2) = 2$ e $\mathrm{ind}_5(2) = 4$. (Infatti, in tal caso si ha che: $\Sigma = \{-3, -2, -1, 0, 1, 2, 3\}$, $S(2) = \{2, 4, 6\}$, $\nu(2) = 2$; inoltre, $5, 5^2 \equiv 4 \pmod{7}, 5^3 \equiv 6 \pmod{7}, 5^4 \equiv 2 \pmod{7}$ dunque $\mathrm{ind}_5(2) = 4$.)

Ci proponiamo, ora, di applicare il Lemma di Gauss per calcolare $(\frac{2}{p})$ e $(\frac{3}{p})$.

Corollario 6.14. *Sia p un primo dispari. Allora:*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se, e soltanto se, } p \equiv 1 \text{ oppure } p \equiv 7 \pmod{8}, \\ -1 & \text{se, e soltanto se, } p \equiv 3 \text{ oppure } p \equiv 5 \pmod{8}. \end{cases}$$

Ne segue che:

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

Dimostrazione. Per calcolare $\nu(2)$ basta osservare che gli elementi del tipo $2k \in S(2)$ congruenti (modulo p) agli interi negativi di Σ verificano la diseguaglianza

$$\frac{p+1}{2} \leqslant 2k \leqslant p-1 \quad \text{e cioè} \quad \frac{p+1}{4} \leqslant k \leqslant \frac{p-1}{2}.$$

Dividendo p per 8, restano individuati $m, r \in \mathbb{N}$ tali che:

$$p = 8m + r, \quad \text{con } 0 \leqslant r \leqslant 7$$

e dunque, si ha:

$$2m + \frac{r+1}{4} \leqslant k \leqslant 4m + \frac{r-1}{2}.$$

Poichè p è dispari, r assume i valori $1, 3, 5, 7$.
Se quindi $r = 1$, risulta $2m + \frac{1}{2} \leqslant k \leqslant 4m$ e, dunque, $2m + 1 \leqslant k \leqslant 4m$. Ne segue che $\nu(2) = 4m - (2m+1) + 1 = 2m$.
Procedendo in modo analogo, si ha:
se $r = 3$, $2m + 1 \leqslant k \leqslant 4m + 1$ e quindi $\nu = 2m + 1$,
se $r = 5$, $2m + 2 \leqslant k \leqslant 4m + 2$ e quindi $\nu = 2m + 1$,
se $r = 7$, $2m + 2 \leqslant k \leqslant 4m + 3$ e quindi $\nu = 2m + 2$.
Pertanto $\nu(2)$ è pari se, e soltanto se, $r = 1, 7$ cioè $p \equiv 1, 7 \pmod 8$.

Relativamente all'ultima parte dell'enunciato, basta verificare che:
se $p \equiv 1, 7 \pmod 8$, allora $\frac{p^2-1}{8}$ è pari, mentre se $p \equiv 3, 5 \pmod 8$, allora $\frac{p^2-1}{8}$ è dispari. $\square$

Corollario 6.15. *Sia p un primo, $p \geqslant 5$. Allora:*

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \textit{se, e soltanto se, } p \equiv 1, 11 \pmod{12}, \\ -1 & \textit{se, e soltanto se, } p \equiv 5, 7 \pmod{12}. \end{cases}$$

Dimostrazione. Procedendo in modo analogo alla dimostrazione precedente, si vede che $\nu = \nu(3)$ coincide con il numero degli interi k tali che

$$\frac{p+1}{2} \leqslant 3k \leqslant p \quad \text{e cioè} \quad \frac{p+1}{6} \leqslant k \leqslant \frac{p}{3}.$$

Dividendo p per 12, per le restrizioni poste su p si ha che:

$$p = 12m + r \quad \text{con } r = 1, 5, 7, 11,$$

($r \neq 3, 9$ perché altrimenti p sarebbe divisibile per 3).
Pertanto, si ha:
se $r = 1$, $2m + 1 \leqslant k \leqslant 4m$ e, quindi, $\nu = 2m$,
se $r = 5$, $2m + 1 \leqslant k \leqslant 4m + 1$ e, quindi, $\nu = 2m + 1$,
se $r = 7$, $2m + 2 \leqslant k \leqslant 4m + 2$ e, quindi, $\nu = 2m + 1$,
se $r = 11$, $2m + 2 \leqslant k \leqslant 4m + 3$ e, quindi, $\nu = 2m + 2$.
Da ciò discende la tesi. $\square$

Osservazione 6.16. Riotterremo il risultato precedente come semplice applicazione della LRQ (cfr. il successivo Esempio 6.24). Questa dimostrazione risulterà quindi superflua, ma ci sembra, comunque, particolarmente istruttiva in vista della dimostrazione della LRQ.

Richiamiamo, ora, alcuni concetti e proprietà che saranno utili per dimostrare la LRQ.

Definizione 6.17. Sia α un numero reale. Si chiama *parte intera di* α (e si denota $[\alpha]$) il più grande intero $\leqslant \alpha$. Si chiama *parte residuale di* α il numero reale $\alpha_1 := \alpha - [\alpha]$ (ovviamente $0 \leqslant \alpha_1 < 1$ e $\alpha = [\alpha] + \alpha_1$).

Proposizione 6.18. *Siano α, β numeri reali tali che $\alpha \leqslant \beta$. Allora:*
(a) *il numero degli interi k tali che $\alpha \leqslant k \leqslant \beta$ è uguale a $[\beta]-[\alpha]$, se $\alpha \notin \mathbb{Z}$, oppure a $[\beta]-[\alpha]+1$ se $\alpha \in \mathbb{Z}$;*
(b) *per ogni intero n, $[n+\beta] = n + [\beta]$;*
(c) *siano n_1, n_2 interi tali che $n_1 \leqslant n_2$. Si ponga:*

$$\nu := \#\{k \in \mathbb{Z}; 2n_1 + \alpha \leqslant k \leqslant 2n_2 + \beta\} \quad e$$

$$\mu := \#\{h \in \mathbb{Z} : \alpha \leqslant h \leqslant \beta\}.$$

Allora:

$$\mu \equiv \nu \pmod 2.$$

Dimostrazione. **(a)**: gli interi cercati sono $[\alpha]+1, [\alpha]+2, \ldots, [\beta]$ e dunque sono esattamente $[\beta]-[\alpha]$ se $\alpha \notin \mathbb{Z}$; se $\alpha \in \mathbb{Z}$, agli interi sopra elencati si deve aggiungere $[\alpha] = \alpha \in \mathbb{Z}$. **(b)**: sia $\beta_1 := \beta - [\beta]$. Allora $n + \beta = (n + [\beta]) + \beta_1$ ed $n + [\beta]$ è un intero. Da ciò segue la tesi. **(c)**: da (a) e (b) segue che $\nu = [2n_2 + \beta] - [2n_1 + \alpha] = 2n_2 + [\beta] - 2n_1 - [\alpha] = 2(n_2 - n_1) + \mu$ se $\alpha \notin \mathbb{Z}$. Ad analoga conclusione si perviene se $\alpha \in \mathbb{Z}$. $\square$

Proposizione 6.19. *Siano p un primo dispari ed a un intero anch'esso dispari tale che* $\mathrm{MCD}(a,p) = 1$. *Allora*

$$\left(\frac{a}{p}\right) = (-1)^{\sigma_{a,p}} \quad con \quad \sigma_{a,p} := \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$$

Dimostrazione. Come nel Teorema 6.12, sia $S(a) := \{ka : 1 \leqslant k \leqslant \frac{p-1}{2}\}$. Dividendo gli elementi di $S(a)$ per p, si ottiene:

$$ka = q_k p + t_k \quad \text{con} \quad q_k, t_k \in \mathbb{N} \quad \text{e} \quad 1 \leqslant t_k \leqslant p-1.$$

Ne segue che $\frac{ka}{p} = q_k + \frac{t_k}{p}$ e quindi $\left[\frac{ka}{p}\right] = q_k$; pertanto si ha:

$$ka = \left[\frac{ka}{p}\right] \cdot p + t_k, \quad 1 \leqslant k \leqslant \frac{p-1}{2}.$$

Si denoti con $\{s_1, \ldots, s_\mu\}$ l'insieme $\{t_k$: con $1 \leqslant t_k \leqslant \frac{p-1}{2}$, al variare di k e con $1 \leqslant k \leqslant \frac{p-1}{2}\}$ e con $\{r_1, \ldots, r_\nu\}$ l'insieme $\{t_k$: e con $\frac{p+1}{2} \leqslant t_k \leqslant p-1$, al variare di k e con $1 \leqslant k \leqslant \frac{p-1}{2}\}$. Si noti che ν è lo stesso intero, $\nu(a)$, considerato nel Lemma di Gauss (cfr. Teorema 6.12).
Vogliamo verificare che l'insieme $\{s_1, \ldots, s_\mu, p-r_1, \ldots, p-r_\nu\}$ coincide con l'insieme $\{1, 2, \ldots, \frac{p-1}{2}\}$. A tale scopo basta provare che $s_{i'} \not\equiv p - r_{j'} \pmod{p}$ (con $1 \leqslant i' \leqslant \mu$ e $1 \leqslant j' \leqslant \nu$). Se infatti $s_{i'} \equiv ia \pmod{p}$ e $r_{j'} \equiv ja \pmod{p}$; dove $1 \leqslant i \neq j \leqslant \frac{p-1}{2}$), allora $(i+j)a \equiv s_{i'} + r_{j'} \pmod{p}$; se, per assurdo, fosse $s_{i'} \equiv p - r_{j'} \pmod{p}$, allora $(i+j)a \equiv 0 \pmod{p}$ e dunque $i + j \equiv 0 \pmod{p}$, il che è ovviamente assurdo.
Si ha allora:

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{\mu} s_i + \sum_{j=1}^{\nu} (p - r_j) = p\nu + \sum_{i=1}^{\mu} s_i - \sum_{j=1}^{\nu} r_j$$

ed anche:

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] \cdot p + \sum_{i=1}^{\mu} s_i + \sum_{j=1}^{\nu} r_j$$

da cui, sottraendo la prima uguaglianza dalla seconda, si ottiene:

$$(a-1) \sum_{k=1}^{\frac{p-1}{2}} k = p(\sigma_{a,p} - \nu) + 2 \sum_{j=1}^{\nu} r_j.$$

Tenendo presente che $p \equiv a \equiv 1 \pmod{2}$, si ha $0 \equiv \sigma_{a,p} - \nu \pmod{2}$ e dunque, applicando il Teorema 6.12, si ha la tesi. □

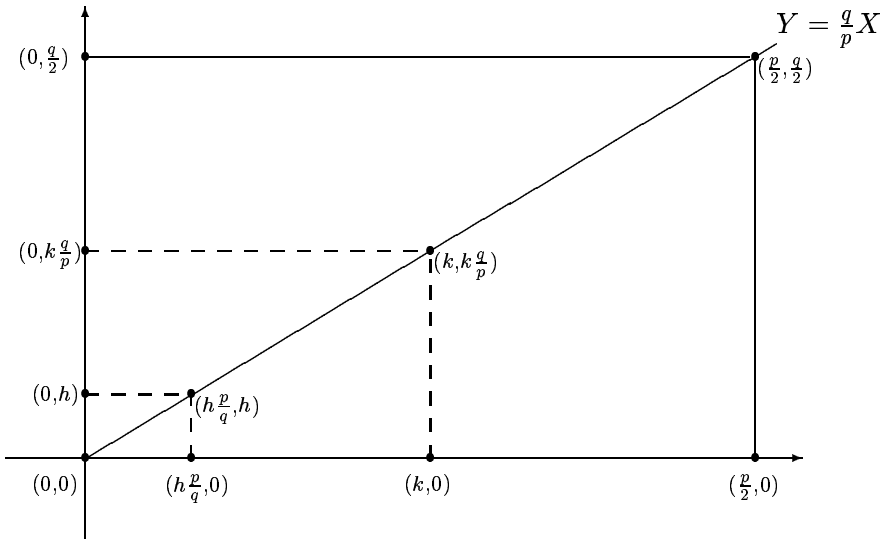
Veniamo finalmente alla LRQ. La dimostrazione che ne daremo è dovuta a F. G. Eisenstein (allievo di Gauss) ed è, in pratica, una semplificazione di una delle varie dimostrazioni che Gauss dette di tale legge.

Osservazione 6.20. Si noti che ormai la prima dimostrazione di Gauss, scritta "in a very repulsive form", come scrisse H. J. Smith, è stata rivisitata e riscritta in maniera estremamente chiara da E. Brown (cfr. Amer. Math. Montly, **88** (1981), 257-263). Altre semplici dimostrazioni sono state date da M. Gersternhaber (cfr. Amer. Math. Montly, **70** (1963), 397-398) e da J.S. Frame (cfr. Amer. Math. Montly, **85** (1978), 818-819).
Per un esame comparativo di varie dimostrazioni classiche della LRQ va infine segnalato un articolo di Frobenius del 1914 (cfr. Gesamm. Abh., **3** (1914), 628-647; Springer, 1968).

Teorema 6.21. (Legge di Reciprocità Quadratica). *Siano p, q due primi dispari distinti. Allora:*

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

Dimostrazione. Nel piano cartesiano consideriamo il rettangolo di vertici $(0,0), (\frac{p}{2},0), (0,\frac{q}{2}), (\frac{p}{2},\frac{q}{2})$.



e denotiamo con R l'interno di tale rettangolo. L'idea della dimostrazione consiste nel contare, in due modi distinti, i punti a coordinate intere giacenti in R.

Sia (n,m) un punto del piano a coordinate intere: è chiaro che $(n,m) \in R$ se, e soltanto se, risulta

$$1 \leqslant n \leqslant \frac{p-1}{2} \quad \text{e} \quad 1 \leqslant m \leqslant \frac{q-1}{2}$$

essendo $\frac{p-1}{2} = \left[\frac{p}{2}\right]$ e $\frac{q-1}{2} = \left[\frac{q}{2}\right]$. Pertanto i punti cercati sono in numero di $\left(\frac{p-1}{2}\right) \cdot \left(\frac{q-1}{2}\right)$.

Procediamo, ora, al calcolo degli stessi punti seguendo un altro metodo. La diagonale del rettangolo (condotta dal vertice $(0,0)$) ha equazione:

$$Y = \frac{q}{p}X$$

e si verifica subito che nessun punto di R a coordinate intere (n,m) giace su tale diagonale. In caso contrario, risulterebbe $m = \frac{q}{p}n$, dunque $pm = qn$ e pertanto $p \mid n$ e $q \mid m$. Ciò è in contrasto con le limitazioni $1 \leqslant n \leqslant \frac{p-1}{2}$ e $1 \leqslant m \leqslant \frac{q-1}{2}$.
Se denotiamo allora con T_1 (rispettivamente T_2) il sottoinsieme triangolare di R giacente al di sotto (rispettivamente al di sopra) della diagonale, è evidente che i punti cercati sono quelli giacenti in T_1 più quelli giacenti in

T_2. Ora, se k è un intero tale che $1 \leqslant k \leqslant \frac{p-1}{2}$, il numero degli interi y tali che $0 < y < \frac{qk}{p}$ è dato da $[qk/p]$ e pertanto i punti di T_1 a coordinate intere e con ascissa k sono esattamente $[qk/p]$. Ne segue che i punti a coordinate intere in T_1 sono:

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right].$$

Analogamente, i punti a coordinate intere in T_2 sono:

$$\sum_{h=1}^{\frac{q-1}{2}} \left[\frac{ph}{q}\right].$$

In definitiva, abbiamo:

$$\left(\frac{p-1}{2}\right) \cdot \left(\frac{q-1}{2}\right) = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] + \sum_{h=1}^{\frac{q-1}{2}} \left[\frac{ph}{q}\right].$$

Applicando due volte la Proposizione 6.19, abbiamo:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\sum_{h=1}^{\frac{q-1}{2}} \left[\frac{ph}{q}\right]} \cdot (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right]} = (-1)^{(\frac{p-1}{2})\cdot(\frac{q-1}{2})}. \ \square$$

Corollario 6.22. *Siano p, q due primi dispari distinti. Allora:*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \begin{cases} 1 & \text{se} \quad p \equiv 1 \pmod 4 \quad o/e \quad q \equiv 1 \pmod 4, \\ -1 & \text{se} \quad p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Dimostrazione. Basta osservare che $(\frac{p-1}{2}) \cdot (\frac{q-1}{2})$ è pari se, e soltanto se, almeno uno dei due primi p, q è congruente a $1 \pmod 4$. $\square$

Corollario 6.23. *Siano p, q due primi dispari distinti. Allora:*

$$\left(\frac{p}{q}\right) = \begin{cases} (\frac{q}{p}) & \text{se} \quad p \equiv 1 \pmod 4 \quad o/e \quad q \equiv 1 \pmod 4, \\ -(\frac{q}{p}) & \text{se} \quad p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Dimostrazione. Basta moltiplicare per $(\frac{q}{p})$ ambo i membri dell'uguaglianza del Corollario 6.22, tenendo conto del fatto che $(\frac{q}{p})^2 = 1$ $\square$

Algoritmo per il calcolo del simbolo di Legendre. A questo punto è opportuno chiarire come i risultati precedenti possono essere utilizzati per calcolare $(\frac{a}{p})$, dove p è un primo dispari ed a un intero tale che $\mathrm{MCD}(a, p) = 1$. Se $a = \pm 2^{e_0} p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ (con $p_1, \ldots, p_r$ primi dispari distinti), dal Corollario 6.9 segue che:

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{2}{p}\right)^{e_0} \left(\frac{p_1}{p}\right)^{e_1} \left(\frac{p_2}{p}\right)^{e_2} \cdot \ldots \cdot \left(\frac{p_r}{p}\right)^{e_r}.$$

La LRQ permette di ricondurre il calcolo di ogni $(\frac{p_i}{p})$ al calcolo di $(\frac{p}{p_i})$ (nel caso in cui $p_i < p$), rinviando quindi al calcolo del simbolo di Legendre con "denominatore" più piccolo di quello di partenza. Dividendo p per p_i si ha:

$$p = h_i p_i + r_i, \text{ con } h_i, r_i \in \mathbb{N} \quad \text{e} \quad 1 \leqslant r_i \leqslant p_i,$$

dunque $p \equiv r_i \pmod{p_i}$ e pertanto $(\frac{p}{p_i}) = (\frac{r_i}{p_i})$. A questo punto si fattorizza r_i nel prodotto di primi e si itera il procedimento sopra esposto. In questo modo, per il calcolo di un qualsiasi simbolo di Legendre $(\frac{p_i}{p})$, ci si riduce, in ultima analisi, al calcolo di simboli di Legendre del tipo:

$$\left(\frac{1}{q}\right), \quad \left(\frac{-1}{q}\right), \quad \left(\frac{2}{q}\right) \ ,$$

dove q è un qualunque primo dispari; i valori di tali simboli di Legendre sono stati già calcolati.

Esemplifichiamo le considerazioni ora svolte.

Esempio 6.24. Calcolo di $(\frac{3}{p})$ con p primo dispari, $p > 3$.
Si ha, ponendo $r \equiv p \pmod{3}, 1 \leqslant r \leqslant 2$:

$$\left(\frac{3}{p}\right) = \begin{cases} (\frac{p}{3}) = (\frac{r}{3}) & \text{se } p \equiv 1 \pmod 4, \\ -(\frac{p}{3}) = -(\frac{r}{3}) & \text{se } p \equiv 3 \pmod 4, \end{cases}$$

$$= \begin{cases} (\frac{1}{3}) = 1 & \text{se } p \equiv 1 \pmod 4 \text{ e } p \equiv 1 \pmod 3, \\ -(\frac{1}{3}) = -1 & \text{se } p \equiv 3 \pmod 4 \text{ e } p \equiv 1 \pmod 3, \\ (\frac{2}{3}) = -1 & \text{se } p \equiv 1 \pmod 4 \text{ e } p \equiv 2 \pmod 3, \\ -(\frac{2}{3}) = 1 & \text{se } p \equiv 3 \pmod 4 \text{ e } p \equiv 2 \pmod 3, \end{cases}$$

$$= \begin{cases} 1 & \text{se } p \equiv 1, 11 \pmod{12}, \\ -1 & \text{se } p \equiv 5, 7 \pmod{12}. \end{cases}$$

Esempio 6.25. Calcolo di $(\frac{4}{p})$ con p primo dispari.
Risulta, ovviamente:

$$\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right)^2 = 1.$$

Esempio 6.26. Calcolo di $(\frac{5}{p})$ con p dispari, $p \neq 5$.
Se $p = 3$, $(\frac{5}{3}) = (\frac{2}{3}) = -1$. Sia $p > 5$: in tal caso $(\frac{5}{p}) = (\frac{p}{5})$ e risulta:

$$p = 5k + r \text{ con } k, r, \in \mathbb{N} \quad \text{e} \quad 1 \leqslant r \leqslant 4.$$

Pertanto:

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{r}{5}\right) = \begin{cases} (\frac{1}{5}) = 1 & \text{se } p \equiv 1 \pmod 5, \\ (\frac{2}{5}) = -1 & \text{se } p \equiv 2 \pmod 5, \\ (\frac{3}{5}) = (\frac{5}{3}) = (\frac{2}{3}) = -1 & \text{se } p \equiv 3 \pmod 5, \\ (\frac{4}{5}) = (\frac{2}{5})^2 = 1 & \text{se } p \equiv 4 \pmod 5, \end{cases}$$

$$= \begin{cases} 1 & \text{se } p \equiv 1, 4 \pmod 5, \\ -1 & \text{se } p \equiv 2, 3 \pmod 5. \end{cases}$$

Esempio 6.27. Calcolo di $(\frac{6}{p})$ con $p \geqslant 5$, p primo.
Poiché $(\frac{6}{p}) = (\frac{2}{p}) \cdot (\frac{3}{p})$, allora, $(\frac{6}{p}) = -1$ se, e soltanto se, uno soltanto tra i simboli $(\frac{2}{p})$ e $(\frac{3}{p})$ vale -1. A partire dai valori già noti di $(\frac{2}{p})$ e $(\frac{3}{p})$ si ottiene facilmente che:

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1, 5, 19, 23 \pmod{24}, \\ -1 & \text{se } p \equiv 7, 11, 13, 17 \pmod{24}. \end{cases}$$

Esempio 6.28. Calcolo di $(\frac{7}{p})$ con p primo dispari, $p \neq 7$.
Se $p = 3$, $(\frac{7}{3}) = (\frac{1}{3}) = 1$; se $p = 5$, $(\frac{7}{5}) = (\frac{2}{5}) = -1$. Sia ora $p > 7$; in tal caso si ha:

$$\left(\frac{7}{p}\right) = \begin{cases} (\frac{p}{7}) & \text{se } p \equiv 1 \pmod 4, \\ -(\frac{p}{7}) & \text{se } p \equiv 3 \pmod 4. \end{cases}$$

Ora, $p = 7k + r$ con $k, r \in \mathbb{N}$ e $1 \leqslant r \leqslant 6$; conseguentemente:

$$\left(\frac{p}{7}\right) = \begin{cases} (\frac{1}{7}) = 1 & \text{se } p \equiv 1 \pmod 7, \\ (\frac{2}{7}) = 1 & \text{se } p \equiv 2 \pmod 7, \\ (\frac{3}{7}) = -1 & \text{se } p \equiv 3 \pmod 7, \\ (\frac{4}{7}) = 1 & \text{se } p \equiv 4 \pmod 7, \\ (\frac{5}{7}) = -1 & \text{se } p \equiv 5 \pmod 7, \\ (\frac{6}{7}) = -1 & \text{se } p \equiv 6 \pmod 7. \end{cases}$$

Ne segue che:

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}, \\ -1 & \text{se } p \equiv 5, 11, 13, 15, 17, 23 \pmod{28}. \end{cases}$$

Concludiamo questo paragrafo studiando la risolubilità di congruenze quadratiche di tipo:

$$X^2 \equiv a \pmod n \tag{4}$$

dove n è un intero arbitrario $\geqslant 2$ ed a un intero tale che $\mathrm{MCD}(a,n)=1$. Tenuto conto delle considerazioni svolte all'inizio del Paragrafo 4 e supposto che n ammetta la seguente fattorizzazione in numeri primi distinti:

$$n = 2^{e_0} p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r},$$

la risolubilità di (4) equivale alla risolubilità del sistema:

$$\begin{cases} X^2 \equiv a \pmod{2^{e_0}}, \\ X^2 \equiv a \pmod{p_i^{e_i}}, \\ 1 \leqslant i \leqslant r \end{cases}$$

Ci occuperemo quindi separatamente dei seguenti problemi:

I Problema: studio della risolubilità di congruenze del tipo:

$$X^2 \equiv a \pmod{p^e}$$

con p primo dispari, $e \geqslant 1$ ed a intero tale che $\mathrm{MCD}(a,p)=1$.

II Problema: studio della risolubilità di congruenze del tipo:

$$X^2 \equiv a \pmod{2^e}$$

con $e \geqslant 1$ ed a intero dispari.

Veniamo al I Problema:

Teorema 6.29. *Sia p primo dispari ed a un intero tale che* $\mathrm{MCD}(a,p)=1$. *Allora la congruenza:*

$$X^2 \equiv a \pmod{p^e} \text{ con } e \geqslant 1 \tag{5}$$

è risolubile se, e soltanto se, $\left(\frac{a}{p}\right)=1$.

Dimostrazione. Se la congruenza (5) è risolubile, ogni sua soluzione risolve anche la congruenza $X^2 \equiv a \pmod{p}$: dunque $\left(\frac{a}{p}\right)=1$.

Viceversa, assumiamo che $\left(\frac{a}{p}\right)=1$ e procediamo per induzione su e. Il caso $e=1$ è assunto per ipotesi. Sia $e \geqslant 2$ e supponiamo che la congruenza $X^2 \equiv a \pmod{p^{e-1}}$ sia risolubile. Se y ne è una soluzione, esiste $b \in \mathbb{Z}$ tale che $y^2 = a + bp^{e-1}$. Poiché $\mathrm{MCD}(p,2y)=1$, la seguente congruenza lineare nell'indeterminata T:

$$2yT \equiv -b \pmod{p} \tag{$\bullet_y$}$$

ammette un'unica soluzione t. (Osserviamo che, a meno di un ovvio adattamento di notazione relativo all'esponente, tale congruenza lineare coincide

con quella considerata nella dimostrazione del Teorema 4.6; cfr. anche la successiva Osservazione 6.30.) Poniamo allora

$$x := x_t := y + tp^{e-1}\,.$$

Già sappiamo che x è soluzione di (5) (cf. dimostrazione del Teorema 4.6). Infatti, ripetendo il ragionamento già fatto (Teorema 4.6) si ha:

$$x^2 = a + bp^{e-1} + 2ytp^{e-1} + t^2p^{2e-2} \equiv a + bp^{e-1} - bp^{e-1} \pmod{p^e}$$

in quanto $2ytp^{e-1} \equiv -bp^{e-1} \pmod{p^e}$ e $2e - 2 \geqslant e$, per $e \geqslant 2$. □

Osservazione 6.30. Si noti che il Teorema 4.7 permette di ottenere la seconda implicazione del teorema precedente. Sia infatti $f(X) := X^2 - a$ e y una soluzione di $f(X) \equiv 0 \pmod{p^{e-1}}$, quindi se $y^2 = a + bp^{e-1}$ allora $f(y)/p^{e-1} = b$. Poichè p è dispari, si dimostra per induzione su $e \geqslant 2$ che $f'(y) = 2y \not\equiv 0 \pmod{p}$ dunque si è nella situazione descritta nel I Caso del Teorema 4.7 (cioè che y è una soluzione non singolare; cfr. anche Esercizio 4.1). Ne segue che (5) è risolubile.
Si noti che questo ragionamento non si può ripetere nel caso del successivo Teorema 6.32(3), per il quale sarà necessario sviluppare una dimostrazione "ad hoc".

Corollario 6.31. *Con le notazioni del Teorema 6.29, se la congruenza* (5) *è risolubile, essa ammette esattamente due soluzioni distinte (cioè non congruenti* $\pmod{p^e}$*).*

Dimostrazione. Alla conclusione si può pervenire (ragionando come nella Osservazione 6.30), applicando il Teorema 4.7. Diamo, comunque, una dimostrazione esplicita (ispirata a quella del Teorema 4.7), che poi tornerà utile per dimostrare il successivo Corollario 6.34.
Se x_0 è una soluzione di (5), è chiaro che x_0 e $x_1 := p - x_0$ sono due soluzioni distinte di (5). Proviamo, per induzione su e, che (5) ammette soltanto due soluzioni distinte. Se $e = 1$, l'asserto è vero (cfr. Proposizione 6.1). Supponiamo che $e \geqslant 2$ e che la congruenza:

$$X^2 \equiv a \pmod{p^{e-1}} \tag{6}$$

ammetta soltanto due soluzioni y_0, y_1. Dalla dimostrazione del Teorema 6.29 segue che y_i $(0 \leqslant i \leqslant 1)$ determina la soluzione $x_i := y_i + t_ip^{e-1}$ di (5), dove $y_i^2 = a + b_ip^{e-1}$ per un qualche $b_i \in \mathbb{Z}$ e t_i è la soluzione della congruenza lineare $2y_iT \equiv -b_i \pmod{p}$.

Per concludere basta verificare che se x è una soluzione della congruenza (5), allora $x \equiv x_0 \pmod{p^e}$ oppure $x \equiv x_1 \pmod{p^e}$. Poiché x è una soluzione di (6), allora $x \equiv y_i \pmod{p^{e-1}}$, con $i = 0$ oppure $i = 1$. Posto

$x = y_i + \tau p^{e-1}$ per un qualche $\tau \in \mathbb{Z}$, dalla congruenza $x^2 \equiv a \equiv (x_i)^2 \pmod{p^e}$ discende che:

$$y_i^2 + 2y_i\tau p^{e-1} + \tau^2 p^{2e-2} \equiv y_i^2 + 2y_i t_i p^{e-1} + t_i^2 p^{2e-2} \pmod{p^e}.$$

Da ciò di ricava facilmente che $\tau \equiv t_i \pmod{p}$ e quindi si conclude che $x \equiv x_i \pmod{p^e}$. □

Veniamo ora al II Problema:

Teorema 6.32. *Sia a un intero dispari. Allora:*

(1) *La congruenza $X^2 \equiv a \pmod 2$ è sempre risolubile;*

(2) *La congruenza $X^2 \equiv a \pmod 4$ è risolubile se, e soltanto se, $a \equiv 1 \pmod 4$;*

(3) *La congruenza $X^2 \equiv a \pmod{2^e}$, $e \geqslant 3$ è risolubile se, e soltanto se, $a \equiv 1 \pmod 8$.*

Dimostrazione. (1). È del tutto ovvio. **(2).** Sia $x_0 \in \mathbb{Z}$ una soluzione della congruenza $X^2 \equiv a \pmod 4$. Essendo a dispari, anche x_0 è dispari e poiché il quadrato di ogni intero dispari è congruente ad 1 (mod 4), si ha $a \equiv x_0^2 \equiv 1 \pmod 4$. Viceversa, se $a \equiv 1 \pmod 4$, allora 1 e 3 sono soluzioni della congruenza in questione. **(3).** È facile verificare che il quadrato di ogni intero dispari è congruente ad 1 (mod 8) (cfr. Esercizio 1.3 (b)). Se, quindi, la congruenza $X^2 \equiv a \pmod{2^e}$ ($e \geqslant 3$) è risolubile, anche la congruenza $X^2 \equiv a \pmod 8$ è risolubile e pertanto, procedendo come sopra, si ottiene che $a \equiv 1 \pmod 8$. Viceversa, assumiamo che $a \equiv 1 \pmod 8$ e procediamo per induzione su e. Se $e = 3$, la congruenza $X^2 \equiv a \pmod 8$ è certamente risolubile (ed ha quattro soluzioni 1, 3, 5, 7 (mod 8)). Supponiamo ora che $e \geqslant 4$ e che $X^2 \equiv a \pmod{2^{e-1}}$ sia risolubile. Se y ne è una soluzione, si ha $y^2 = a + b2^{e-1}$, per un qualche $b \in \mathbb{Z}$. Poichè a è dispari, anche y è dispari e, pertanto, la seguente congruenza lineare nell'indeterminata T:

$$yT \equiv -b \pmod 2$$

ammette un'unica soluzione $t \pmod 2$. Si pone allora:

$$x := x_t := y + t2^{e-2}$$

e si verifica, facilmente, che x è una soluzione della congruenza $X^2 \equiv a \pmod{2^e}$. Infatti, si ha $yt2^{e-1} \equiv -b \cdot 2^{e-1} \pmod{2^e}$, $2e - 4 \geqslant e$ e dunque $x^2 = a + b2^{e-1} + yt2^{e-1} + t^2 2^{2e-4} \equiv a \pmod{2^e}$. □

Osservazione 6.33. Si noti che nella dimostrazione del punto (3) del Teorema 6.32 si ha che se b è pari allora risulta $t \equiv 0 \pmod 2$; se b è dispari, $t \equiv 1 \pmod 2$. Ne primo caso $x = y$ e nel secondo $x = y + 2^{e-2}$.

Corollario 6.34. *Sia a un intero dispari. Allora:*

(1) *La congruenza $X^2 \equiv a \pmod 2$ ha un'unica soluzione;*

(2) *Se la congruenza $X^2 \equiv a \pmod 4$ è risolubile, allora ha esattamente due soluzioni distinte (cioè incongruenti (modulo 4));*

(3) *Se la congruenza $X^2 \equiv a \pmod{2^e}$, $e \geqslant 3$ è risolubile, allora ha esattamente quattro soluzioni distinte (cioè incongruenti (modulo 2^e)).*

Dimostrazione. **(1)** e **(2)** sono del tutto evidenti. Dimostriamo **(3)** seguendo la linea dimostrativa del Corollario 6.31.

Innanzitutto, se x_0 è una soluzione di

$$X^2 \equiv a \pmod{2^e} \quad e \geqslant 3, \tag{7}$$

si verifica subito che:

$$x_0, \quad -x_0, \quad x_0 + 2^{e-1}, \quad -x_0 + 2^{e-1}$$

sono quattro soluzioni distinte di (7). Proviamo, per induzione su e, che (7) ammette soltanto quattro soluzioni distinte. Se $e = 3$, allora possiamo porre $a = 1$ (in quanto, $a \equiv 1 \pmod 8$, cfr. Teorema 6.32 (3)), ed è evidente che $X^2 \equiv 1 \pmod 8$ ha soltanto quattro soluzioni distinte (cioè: $1, 3, 5, 7 \pmod 8$). Sia $e \geqslant 4$ e supponiamo che l'asserto sia vero per l'esponente $e - 1$. Denotiamo con y_0, y_1, y_2, y_3 le quattro soluzioni distinte di

$$X^2 \equiv a \pmod{2^{e-1}} \tag{8}$$

Procedendo come nel Teorema 6.32, y_i $(0 \leqslant i \leqslant 3)$ determina la soluzione di (7):

$$x_i := y_i + t_i 2^{e-2},$$

dove si è posto $y_i^2 = a + b_i 2^{e-1}$ $(b_i \in \mathbb{Z})$ e t_i soluzione della congruenza $y_i T \equiv -b_i \pmod 2$. A partire da una qualsiasi scelta di i, con $0 \leqslant i \leqslant 3$, gli interi $x_i, -x_i, x_i + 2^{e-1}, -x_i + 2^{e-1}$ sono quattro soluzioni distinte di (7) (cfr. anche Osservazione 6.33). Per concludere basta verificare che se x è una soluzione di (7), allora x è congruente (modulo 2^e) ad una di tali soluzioni. Poiché x è anche soluzione di (8), esiste un unico intero i $(0 \leqslant i \leqslant 3)$ tale che $x \equiv y_i \pmod{2^{e-1}}$. Inoltre non è restrittivo assumere che $1 \leqslant x < 2^e$ e $1 \leqslant y_i < 2^{e-1}$ e quindi risulta necessariamente $x = y_i$ oppure $x = y_i + 2^{e-1}$. Nel primo caso, $y_i^2 \equiv a \pmod{2^e}$, quindi si vede facilmente che $x_i = y_i$ e, pertanto, $x \equiv x_i \pmod{2^e}$. Nel secondo caso si hanno due alternative:

(a) se $x_i = y_i$, allora $x \equiv x_i + 2^{e-1} \pmod{2^e}$;

(b) se $x_i = y_i + 2^{e-2}$, allora dal fatto che $x^2 \equiv (x_i)^2 \pmod{2^e}$ si ricava facilmente che $y_i \equiv 0 \pmod 2$ e ciò è assurdo in quanto a (e, quindi, y_i) è dispari. $\square$

Osservazione 6.35. Vogliamo commentare la dimostrazione del teorema precedente, anche alla luce del Teorema 4.7.
Innanzitutto, osserviamo che, con le notazioni sopra introdotte, per ogni j fissato, con $0 \leqslant j \leqslant 3$, risulta:

$$\{x_j, -x_j, x_j+2^{e-1}, -x_j+2^{e-1}\} = \{x_i, -x_i, x_i+2^{e-1}, -x_i+2^{e-1} : 0 \leqslant i \leqslant 3\}.$$

Inoltre, notiamo che $\{x_0, x_1, x_2, x_3\}$ è un sottoinsieme dell'insieme sopra considerato $\{x_j, -x_j, x_j + 2^{e-1}, -x_j + 2^{e-1}\}$ di tutte le soluzioni distinte di $X^2 \equiv a \pmod{2^e}$ ed, in generale, non coincide con quest'ultimo.
Per esemplificare quanto osservato sopra, descriviamo più dettagliatamente, il passaggio dalla congruenza $X^2 \equiv a \pmod 8$ alla congruenza $X^2 \equiv a \pmod{16}$.
Nel caso risolubile, cioè $a \equiv 1 \pmod 8$, denotiamo con $\{y_0 = 1, y_1 = 3, y_2 = 5, y_3 = 7\}$ le soluzioni della congruenza $X^2 \equiv 1 \pmod 8$. Quindi se $a \equiv 1 \pmod 8$ abbiamo due congruenze risolubili $\pmod{16}$.

Caso 1: $X^2 \equiv 1 \pmod{16}$.
Conserviamo le notazioni della dimostrazione del Corollario 6.34. Allora, $b_0 = 0, b_1 = 1, b_2 = 3, b_3 = 6$, quindi $t_0 = 0, t_1 = 1, t_2 = 1, t_3 = 0$, pertanto $x_0 = 1, x_1 = 7, x_2 = 9, x_3 = 7$. Mentre l'insieme delle soluzioni distinte $X^2 \equiv 1 \pmod{16}$ è dato da:

$$\{1, -1, 9, -9\} = \{1, 15, 9, 7\} = \{x_j, -x_j, x_j + 8, -x_j + 8\}$$

per ogni scelta di j, con $0 \leqslant j \leqslant 3$. Inoltre, esaminando il problema con l'ottica del Teorema 4.7, abbiamo che $y_0 = 1$ e $y_3 = 7$ sono anche soluzioni della congruenza $\pmod{2^4}$ e quindi ciascuna di queste determina due soluzioni $\pmod{2^4}$ date da:

$$y_0 = 1, y_0 + 2^3 = 8, y_1 = 7, y_1 + 2^3 = 15$$

(II Caso del Teorema 4.7). Mentre $y_1 = 3$ e $y_2 = 5$ non sono soluzioni della congruenza $\pmod{2^4}$ e, quindi, non determinano alcuna soluzione della congruenza $\pmod{2^4}$ (III Caso del Teorema 4.7).

Caso 2: $X^2 \equiv 9 \pmod{16}$.
In questo caso, $b_0 = 1, b_1 = 0, b_2 = 2, b_3 = 5$, quindi $t_0 = 1, t_1 = 0, t_2 = 0, t_3 = 1$, pertanto $x_0 = 5, x_1 = 3, x_2 = 5, x_3 = 11$. Mentre l'insieme delle soluzioni distinte $X^2 \equiv 9 \pmod{16}$ è dato da:

$$\{3, -3, 11, -11\} = \{3, 13, 11, 5\} = \{x_j, -x_j, x_j + 8, -x_j + 8\}$$

per ogni scelta di j, con $0 \leqslant j \leqslant 3$. Inoltre le soluzioni $y_1 = 3$ e $y_2 = 5$ della congruenza $X^2 \equiv 1 \pmod 8$ determinano ciscuna due soluzioni della congruenza $X^2 \equiv 9 \pmod{16}$ e cioè

$$y_1 = 3, y_1 + 2^3 = 11, y_2 = 5, y_2 + 2^3 = 13.$$

Mentre le soluzioni y_0 e y_3 non determinano soluzioni della congruenza $X^2 \equiv 9 \pmod{16}$.

Possiamo riassumere nel seguente teorema i risultati sopra ottenuti.

Teorema 6.36. *Sia n un intero $\geqslant 2$ che ammette la seguente fattorizzazione in primi distinti:*

$$n = 2^{e_0} p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}.$$

Sia a un intero tale che $\mathrm{MCD}(a, n) = 1$. *Allora, la congruenza*

$$X^2 \equiv a \pmod{n} \tag{4}$$

è risolubile se, e soltanto se, le seguenti due condizioni sono soddisfatte:
(1) $(\frac{a}{p_1}) = \cdots = (\frac{a}{p_r}) = 1$;
(2) $\begin{cases} a \text{ dispari}, & \text{se } e_0 = 1; \\ a \equiv 1 \pmod 4, & \text{se } e_0 = 2 \ (\text{cioè se } 4 \mid n \text{ e } 8 \nmid n); \\ a \equiv 1 \pmod 8, & \text{se } e_0 \geqslant 3 \ (\text{cioè se } 8 \mid n). \end{cases}$

Dimostrazione. È una semplice congruenza dei Teoremi 4.1, 6.29, 6.32. □

Corollario 6.37. *Con le notazioni del Teorema 6.36, se la congruenza* (4) *è risolubile, il numero delle sue soluzioni distinte (cioè, incongruenti* (mod n)*) è dato da:*

$$\begin{cases} 2^r & \text{se } e_0 \leqslant 1, \\ 2^{r+1} & \text{se } e_0 = 2, \\ 2^{r+2} & \text{se } e_0 \geqslant 3. \end{cases}$$

Dimostrazione. È una semplice conseguenza dell'Osservazione 4.2 e dei Corollari 6.31 e 6.34. □

Osservazione 6.38. Come applicazione del Teorema 6.36, vogliamo studiare la risolubilità dell'equazione diofantea in due indeterminate X e Y:

$$aX^2 + bY + c = 0 \quad \text{con } a, b, c \in \mathbb{Z} \tag{9}$$

Se $a = 0$ (e $b \neq 0$), (9) è risolubile se, e soltanto se, $b \mid c$; se $b = 0$ (e $a \neq 0$), (9) è risolubile se, e soltanto se, $\frac{-c}{a}$ è il quadrato di un numero intero. Supponiamo, ora, che $a \neq 0$ e $b \neq 0$. In tal caso (9) è risolubile se, e soltanto se,

$$aX^2 \equiv -c \pmod{b} \tag{10}$$

è risolubile.
Supponiamo allora che la congruenza quadratica (10) sia risolubile e poniamo $d :=\mathrm{MCD}(a, b)$. Allora risulta che $d \mid c$ e perciò, indicati con $\bar{a}, \bar{b}, \bar{c}$ gli interi tali che

$$a = \bar{a}d, \qquad b = \bar{b}d, \qquad c = \bar{c}d,$$

è immediato che la risolubilità di (9) equivale alla risolubilità di:

$$\bar{a}X^2 + \bar{b}Y + \bar{c} = 0 \quad \text{con MCD}(\bar{a}, \bar{b}) = 1. \tag{11}$$

In tal caso, la risolubilità di (11) equivale alla risolubilità della congruenza: $\bar{a}X^2 \equiv -\bar{c} \pmod{\bar{b}}$. Denotiamo, allora, con $\bar{a}^*$ un inverso aritmetico di $\bar{a}$ (mod $\bar{b}$) e posto $-\bar{c} \cdot \bar{a}^* =: e$, questa ultima congruenza è equivalente alla congruenza:

$$X^2 \equiv e \pmod{\bar{b}} \tag{12}$$

e per stabilire se (12) è risolubile basta applicare il Teorema 6.36.

In particolare, l'equazione diofantea:

$$X^2 \pm pY - c = 0,$$

con p primo dispari e $c \in \mathbb{Z}$, è risolubile se, e soltanto se, $(\frac{c}{p}) = 1$. Ad esempio, quindi, l'equazione diofantea $X^2 \pm 3Y + 1 = 0$ non è risolubile; mentre $X^2 \pm pY - 5 = 0$ è risolubile per un primo p dispari se e soltanto se, $p \equiv 1, 4 \pmod 5$.

"Geometricamente" questo fatto si traduce nell'esistenza di parabole del piano che non contengono alcun punto a coordinate intere (ad esempio $X^2 \pm 3Y - 5 = 0$) oppure che ne contengono infiniti (ad esempio $X^2 \pm 11Y - 5 = 0$).

Il matematico tedesco C.G. Jacobi (1804 - 1851) ha introdotto un simbolo (noto come simbolo di Jacobi) che generalizza il simbolo di Legendre e ne estende alcune proprietà.

Definizione 6.39. Siano a, n interi tali che $n > 1$ e $\text{MCD}(a, n) = 1$. Posto $n = p_1 p_2 \cdot \ldots \cdot p_r$, con $p_1, p_2, \ldots, p_r$ primi non necessariamente a due a due distinti, si chiama *simbolo di Jacobi* il simbolo così definito:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_r}\right)$$

dove $(\frac{a}{p_i})$ per $1 \leqslant i \leqslant r$ è l'usuale simbolo di Legendre.

Proposizione 6.40. *Siano n, m interi dispari tali che $n > 1, m > 1$; siano inoltre a, b interi relativamente primi con n e con m. Risulta:*

(a) $a \equiv b \pmod n \Rightarrow (\frac{a}{n}) = (\frac{b}{n})$;

(b) $(\frac{ab}{n}) = (\frac{a}{n}) \cdot (\frac{b}{n})$;

(c) $(\frac{a}{nm}) = (\frac{a}{n}) \cdot (\frac{a}{m})$;

(d) $(\frac{a}{n^2}) = (\frac{a^2}{n}) = 1$;

(e) $(\frac{1}{n}) = 1$;

(f) $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$;

(g) $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$. *In particolare,* $(\frac{2}{n}) = 1$ *se, e soltanto se* $n \equiv \pm 1 \pmod 8$.

(h) (Legge di Reciprocità Quadratica; forma generalizzata). *Siano* n, m *interi dispari tali che* $n > 1, m > 1$ *e* $\mathrm{MCD}(n, m) = 1$. *Allora:*

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

Dimostrazione. Per verificare **(a), ... , (e)** basta utilizzare la definizione del simbolo di Jacobi e le proprietà del simbolo di Legendre.
(f). Sia $n = p_1 p_2 \cdot \ldots \cdot p_r$. Tenuto conto della Proposizione 6.6 (h), basta verificare che

$$\frac{n-1}{2} \equiv \frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \cdots + \frac{p_r - 1}{2} \pmod 2.$$

Infatti, risulta $n = [(p_1 - 1) + 1][(p_2 - 1) + 1] \cdot \ldots \cdot [(p_r - 1) + 1] = 4k + 1 + (p_1 - 1) + \cdots + (p_r - 1)$ per un qualche $k \in \mathbb{N}$, perché $4 \mid (p_i - 1)(p_j - 1))$, con $1 \leqslant i, j \leqslant r$. Da ciò segue banalmente la congruenza voluta. **(g)**. Si procede come in (f). Tenuto conto del Corollario 6.14, basta verificare che:

$$\frac{n^2 - 1}{8} \equiv \frac{p_1^2 - 1}{8} + \cdots + \frac{p_r^2 - 1}{8} \pmod 2.$$

Infatti $n^2 = [(p_1^2 - 1) + 1] \ldots [(p_r^2 - 1) + 1] = 16h + 1 + (p_1^2 - 1) + \cdots + (p_r^2 - 1)$ per un qualche $h \in \mathbb{N}$, perché $4 \mid (p_i^2 - 1)$ e quindi $16 \mid (p_i^2 - 1)(p_j^2 - 1)$, con $1 \leqslant i, j \leqslant r$. Da ciò segue l'asserto. **(h)**. Sia $n = p_1 p_2 \cdot \ldots \cdot p_r$ e $m = q_1 q_2 \cdot \ldots \cdot q_s$. Tenuto conto del Teorema 6.21, si ha:

$$\begin{aligned}
\left(\frac{n}{m}\right) \cdot \left(\frac{m}{n}\right) &= \prod_{j=1}^{s} \prod_{i=1}^{r} \left(\frac{p_i}{q_j}\right) \cdot \prod_{i=1}^{r} \prod_{j=1}^{s} \left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{r} \prod_{j=1}^{s} \left(\frac{p_i}{q_j}\right) \cdot \left(\frac{q_j}{p_i}\right) = \\
&= \prod_{i=1}^{r} \prod_{j=1}^{s} (-1)^{(\frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2})} = \\
&= (-1)^{\sum_{i=1}^{r} \sum_{j=1}^{s} (\frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2})} = \\
&= (-1)^{(\sum_{i=1}^{r} (\frac{p_i - 1}{2})) \cdot (\sum_{j=1}^{s} (\frac{q_j - 1}{2}))}.
\end{aligned}$$

Per concludere basta osservare (cfr. dimostrazione di **(f)**) che:

$$\sum_{i=1}^{r} (\frac{p_i - 1}{2}) \equiv \frac{n-1}{2} \pmod 2 \quad \text{e} \quad \sum_{j=1}^{s} (\frac{q_j - 1}{2}) \equiv \frac{m-1}{2} \pmod 2. \ \square$$

Osservazione 6.41. Si consideri la congruenza:

$$X^2 \equiv a \pmod{n} \tag{13}$$

con n dispari, $n > 1$ e $\mathrm{MCD}(a, n) = 1$. È chiaro che (cfr. Teorema 6.36) se (13) è risolubile, allora $(\frac{a}{n}) = 1$. Il viceversa è invece falso (anche se n è un intero per il quale esiste una radice primitiva dell'unità). Basta porre $n = 9$ (cfr. Teorema 5.17) ed osservare che $(\frac{2}{9}) = (\frac{2}{3^2}) = 1$, mentre $X^2 \equiv 2 \pmod{9}$ non è risolubile (in quanto $(\frac{2}{3}) = -1$, cfr. Teorema 6.29).

Si noti la parziale analogia tra queste considerazioni e quelle svolte nell'Osservazione 6.11.

Possiamo, ora, applicare il simbolo di Jacobi e le sue proprietà per dimostrare il seguente risultato:

Proposizione 6.42. (S. Chowla). *L'equazione diofantea quadratica in una indeterminata X*

$$X^2 = a, \quad \textit{con } a \in \mathbb{Z} \tag{14}$$

è risolubile se, e soltanto se, per ogni primo p la congruenza

$$X^2 \equiv a, \pmod{p} \tag{15}$$

è risolubile.

Dimostrazione. È chiaro che se (14) è risolubile, ogni (15) è risolubile. Viceversa, ammettiamo per assurdo che $a \neq b^2$, per ogni $b \in \mathbb{Z}$. Verificheremo che esiste un intero dispari n tale che $(\frac{a}{n}) = -1$ (e, dunque, che esiste un primo dispari p con $p \mid n$ e tale che $(\frac{a}{p}) = -1$).

Distinguiamo tre casi, che insieme coprono tutte le possibilità per le quali a non è quadrato:

(a) Sia $a = \pm 2^e b$, con b, e interi positivi dispari. Sia n una soluzione del sistema:

$$\begin{cases} X \equiv 5 \pmod{8} \\ X \equiv 1 \pmod{b} \end{cases}$$

Si verifica con facilità che $(\frac{\pm 2}{n}) = -1$ (Proposizione 6.40 (f) e (g)), $(\frac{2^{e-1}}{n}) = 1$ e $(\frac{b}{n}) = (\frac{n}{b}) = (\frac{1}{b}) = 1$. Allora $(\frac{a}{n}) = -1 \cdot 1 \cdot 1 = -1$.

(b) Sia $a = \pm 2^{2h} q^k b$, con q, k, b interi dispari, q primo e $q \nmid b$. Sia n una soluzione del sistema:

$$\begin{cases} X \equiv 1 \pmod{4b} \\ X \equiv c \pmod{q} \end{cases}$$

dove c è un intero tale che $(\frac{c}{q}) = -1$. Allora si ha: $(\frac{\pm 1}{n}) = 1$, $(\frac{2^{2h}}{n}) = 1$, $(\frac{b}{n}) = (\frac{n}{b}) = 1$, $(\frac{q^k}{n}) = (\frac{q}{n}) = (\frac{n}{q}) = (\frac{c}{q}) = -1$ e pertanto $(\frac{a}{n}) = -1$.

(c) sia $a = -b^2$, con b intero dispari. Scelto $n \equiv 3 \pmod 4$ tale che $\mathrm{MCD}(a, n) = 1$, è chiaro che $(\frac{a}{n}) = (\frac{-1}{n}) = -1$. □

Osservazione 6.43. Più generalmente, si dimostra che *l'equazione diofantea $X^n = a$ è risolubile se, e soltanto se, $X^n \equiv a \pmod{p^k}$ è risolubile per ogni p primo e per ogni $k \geqslant 1$.* Anzi, più precisamente è noto che *se $X^n \equiv a \pmod p$ è risolubile per ogni p primo, due casi sono possibili:*

1. *Se $8 \nmid n$, allora $X^n = a$ è risolubile;*

2. *Se $8 \mid n$, allora $X^n = a$ è risolubile, oppure $2^{\frac{n}{2}} X^n = a$ è risolubile.*

Il secondo caso, nell'enunciato precedente, si presenta effettivamente, come mostra il seguente esempio: $X^8 \equiv 16 \pmod p$ è risolubile, per ogni primo p, però l'equazione diofantea $X^8 = 16$ non è risolubile, mentre è ovviamente risolubile $2^4 X^8 = 16$.

Per maggiori dettagli si veda: E. Trost, Niew Arch. Wisk. **18** (1934), 58-61 od, anche, N.C. Ankeny - C.A. Rogers, Ann. Math. **53** (1951), 541-550. Una prova più algebrica di un caso particolare di tale risultato è stata data più recentemente da J. Kraft e M. Rosen, Amer. Math. Montly, **88** (1981), 269-270.

6. Esercizi e Complementi

6.1. Siano $a, b, c \in \mathbb{Z}, a \equiv 1 \pmod 2$. Determinare quando la congruenza $aX^2 + bX + c \equiv 0 \pmod 2$ è risolubile.
[Soluzione. La tabella seguente descrive i vari casi possibili:

b	c	x
0	0	0
0	1	1
1	0	0, 1
1	1	−

.]

6.2. Verificare che, per ogni primo p, la congruenza $X^2 \equiv 0 \pmod p$ ha un'unica soluzione (mod p).

6.3. Sia a un intero positivo che scriviamo nella forma $a = b^2 d$, con $b, d \in \mathbb{Z}$ e d privo di fattori quadratici. Mostrare che, per ogni p primo dispari tale che $p \nmid a$, risulta $(\frac{a}{p}) = (\frac{d}{p})$.

6.4. (a). Se q è un primo dispari ed r è una radice primitiva (mod q), si ha $(\frac{r}{q}) = -1$.
(b). Siano p, q primi dispari tali che $q = 2p + 1$ e si consideri l'insieme $T := \{a \in \mathbb{Z} : 1 \leqslant a \leqslant q - 1 \text{ e } (\frac{a}{q}) = -1\}$. Verificare che $\#(T) = p$, che $p - 1$ elementi di T sono radici primitive (mod q) e infine che $2p$ è l'unico elemento di T che non è radice primitiva (mod q).
(c). Utilizzando (b), calcolare le radici primitive modulo $7, 11, 23, 47$.
(Si noti che 11 e 23 sono gli unici primi q, tra 7 e 47, del tipo $q = 2p + 1$, con p primo.)
(d). Con le notazioni di (b), dimostrare che $2(-1)^{\frac{p-1}{2}}$ è una radice primitiva (mod q).
(e). Verificare che 2 è una radice primitiva modulo $11, 59$, e 107, mentre -2 è una radice primitiva modulo $7, 23, 47, 159$ e 167.
[Suggerimento. **(a)** segue dalle Proposizioni 6.6 (d) e 5.22 (d). **(b)** Il primo asserto è conseguenza della Proposizione 6.3 e del fatto che $\frac{q-1}{2} = p$. Per il secondo, cfr. (a) e la Proposizione 5.8. Infine, per il terzo si verifichi che, necessariamente, $q \equiv 3 \pmod 4$ da cui segue che $(\frac{q-1}{q}) = -1$ e $\mathrm{ord}_q(q-1) = 2$. **(c)** Se $q = 7$, $T = \{3, 5, 6\}$, $r = 3, 5$. Se $q = 11$, $T = \{2, 6, 7, 8, 10\}$, $r = 2, 6, 7, 8$. Se $q = 23$, $T = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$, $r = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21$. Se $q = 47$, $T = \{5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45, 46\}$, $r = 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45$. **(d)** Se $p \equiv 1 \pmod 4$, $\frac{p-1}{2}$ è pari e bisogna quindi provare che $\mathrm{ord}_q(2) = 2p$. A priori, $\mathrm{ord}_q(2) = 1, 2, p, 2p$ e bisogna pertanto escludere le prime tre eventualità. Per le prime due è ovvio essendo $q \geqslant 7$, per la terza, si ha $2^p = 2^{\frac{q-1}{2}} \equiv (\frac{2}{q}) \pmod q$ e, essendo $p \equiv 1 \pmod 4$ allora $q \equiv 3 \pmod 8$, dunque $2^p \equiv -1 \pmod q$. Se invece $p \equiv 3 \pmod 4$, bisogna provare che $\mathrm{ord}_q(-2) = 2p$. Procedendo come sopra, essendo $q \equiv 7 \pmod 8$, si ha: $(-2)^p \equiv (\frac{-2}{q}) = (\frac{-1}{q}) \cdot (\frac{2}{q}) \equiv -1 \pmod q$, e da ciò segue l'asserto. **(e)** È una semplice conseguenza di (d).]

6.5. Sia p un primo dispari ed a un intero tale che $\mathrm{MCD}(a,p)=1$. Se $(\frac{a}{p})=1$, allora

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

[Suggerimento: $(\frac{p-a}{p})\equiv(p-a)^{\frac{p-1}{2}}\equiv(-a)^{\frac{p-1}{2}}\equiv(-1)^{\frac{p-1}{2}} \pmod p$.]

6.6. Sia p un primo dispari ed a un intero tale che $\mathrm{MCD}(a,p)=1$. Mostrare che:

$$(p-1)!\equiv -\left(\frac{a}{p}\right)a^{\frac{p-1}{2}} \pmod p.$$

[Suggerimento. Dal Criterio di Eulero segue che $(\frac{a}{p})\equiv a^{\frac{p-1}{2}} \pmod p$, quindi $(\frac{a}{p})a^{\frac{p-1}{2}}\equiv 1 \pmod p$; la conclusione è conseguenza del Lemma di Wilson.]

6.7. Sia p un primo dispari e siano $a,b\in\mathbb{Z}$ tali che $\mathrm{MCD}(a,p)=\mathrm{MCD}(b,p)=1$. Se $(\frac{a}{p})=(\frac{b}{p})$, allora $aX^2\equiv b \pmod p$ è risolubile (e viceversa).
[Suggerimento. Se a^* è l'inverso aritmetico di $a \pmod p$, allora $X^2\equiv a^*b \pmod p$ è risolubile $\iff (\frac{a^*b}{p})=1 \iff (\frac{a}{p})=(\frac{b}{p})$.]

6.8. Mostrare che esistono infiniti primi di tipo $4k+1$.
[Suggerimento. Per assurdo, siano $p_1,\ldots,p_n$ i soli primi di tipo $4k+1$. L'intero dispari $N:=4(p_1p_2\cdot\ldots\cdot p_n)^2+1$ è divisibile per un primo dispari p. Utilizzando la Proposizione 6.6 (h), si verifica che $p\equiv 1 \pmod 4$ e che da ciò segue un assurdo.]

6.9. Mostrare che esistono infiniti primi di tipo $8k-1$.
[Suggerimento. Per assurdo, siano $p_1,\ldots,p_n$ i soli primi di tipo $8k-1$. L'intero $N:=(4p_1\cdot\ldots\cdot p_n)^2-2$ ammette certamente un divisore primo p dispari. Ne segue che $(\frac{2}{p})=1$, quindi $p\equiv 1,7 \pmod 8$. Se tutti i divisori primi dispari di N fossero della forma $8k+1$, siccome N è pari risulterebbe $N\equiv 2 \pmod{16}$, mentre $N\equiv -2 \pmod{16}$. Se invece fosse $p\equiv 7\equiv -1 \pmod 8$, allora $p\mid(N-(4p_1p_2\cdot\ldots\cdot p_n)^2)=2$ e ciò è ugualmente assurdo.]

6.10. Mostrare che esistono infiniti primi del tipo:

(a) $8k+3$;

(b) $8k+5$;

(c) $8k+7$;

(d) $6k+1$.

[Suggerimento. Per ciascuna parte si assuma che esistano un numero finito di primi del tipo indicato. Per la parte **(a)** prendere in esame $N:=(4p_1p_2\cdot\ldots\cdot p_n)^2-2$; per la parte **(b)** prendere in esame $N:=(p_1p_2\cdot\ldots\cdot p_n)^2+2$; per la parte **(d)** $N:=(2p_1p_2\cdot\ldots\cdot p_n)^2+3$. Per **(c)** si noti che $8k+7\equiv 8k-1 \pmod 8$ (cfr. Esercizio 6.9).]

6.11. Sia n un intero dispari ed a un intero tale che $\mathrm{MCD}(a,n)=1$. Mostrare che la risolubilità della congruenza $aX^2+bX+c\equiv 0 \pmod n$ può essere ricondotta alla risolubilità di una congruenza del tipo: $Y^2\equiv d \pmod n$.
[Suggerimento. Si proceda come già fatto all'inizio del Paragrafo 6 per ogni fattore primo p (necessariamente dispari) di n e si tenga conto del Teorema 6.36.]

6.12. Determinare se le seguenti congruenze sono risolubili:

(a) $2X^2 - 5X + 7 \equiv 0 \pmod{21}$

(b) $X^2 + X - 2 \equiv 0 \pmod{35}$

[Soluzione. **(a)** Sia $a = 2, b = -5, c = 7, d = b^2 - 4ac = -31, Y = 2aX + b = 4X - 5$. Poiché $21 = 3 \cdot 7$ è dispari, allora le soluzioni della congruenza data si determinano dalle soluzioni della congruenza

$$Y^2 \equiv -31 \pmod{21} \quad \text{cioè} \quad Y^2 \equiv 11 \pmod{21}.$$

Poiché $(\frac{11}{21}) = (\frac{21}{11}) = (\frac{10}{11}) = (\frac{2}{11})(\frac{5}{11}) = -(\frac{11}{5}) = -(\frac{1}{5}) = -1$, $Y^2 \equiv 11 \pmod{21}$ non è risolubile, pertanto non è risolubile la congruenza data. **(b)** In tal caso $d = 9, Y = 2X + 1, Y^2 \equiv 9 \pmod{35}$ è risolubile in quanto $(\frac{9}{5}) = 1$ e $(\frac{9}{7}) = 1$. Precisamente le soluzioni sono $x = 1, 8, 26, 33 \pmod{35}$.]

6.13. Sia p primo, $p \neq 3$ ed a un intero tale che $\text{MCD}(a, p) = 1$. Mostrare che la congruenza: $aX^3 + bX^2 + cX + d \equiv 0 \pmod{p}$ può essere ricondotta ad una congruenza del tipo: $Y^3 + eY + f \equiv 0 \pmod{p}$.
[Suggerimento. Si moltiplichi la congruenza assegnata per a^* e si ponga $X = Y - 3^* a^* b$.]

6.14. Mostrare che p è un qualsiasi primo dispari, allora:

$$\left(\frac{2}{p}\right) = \left(\frac{8-p}{p}\right) = \left(\frac{p}{p-8}\right) = \left(\frac{2}{p-8}\right).$$

[Suggerimento. Utilizzando la Proposizione 6.40 si ha: $(\frac{8-p}{p}) = (\frac{8}{p}) = (\frac{2 \cdot 4}{p}) = (\frac{2}{p})$, $(\frac{p}{p-8}) = (\frac{8}{p-8}) = (\frac{2}{p-8})$, $(\frac{2}{p}) = (\frac{2}{p-8})$ perché $p \equiv 8 \pmod{p-8}$.]

6.15. Sia $k \geqslant 2$ e sia $p = 4k + 3$ un numero primo. Mostrare che:

(a) $2p + 1$ è primo $\iff 2^p \equiv 1 \pmod{(2p+1)}$.

(b) Se $2p+1$ è primo, il numero $M_p := 2^p - 1$ (detto *p-esimo numero di Mersenne*) è composto.

[Suggerimento. **(a, $\Rightarrow$)**. Basta osservare che $2^p = 2^{\frac{2p+1-1}{2}} \equiv (\frac{2}{2p+1}) = 1$ (modulo $2p + 1$) per il Criterio di Euler, essendo $2p + 1 \equiv 7 \pmod{8}$. **(a, $\Leftarrow$)**. Poniamo $n := 2p + 1$. Se $2^p \equiv 1 \pmod{n}$, allora necessariamente $p = \text{ord}_n(2)$ e quindi $p \mid \varphi(n)$. Se $n = p_1^{e_1} \cdots p_r^{e_r}$ allora $p \mid \left(\prod_{i=1}^r p_i^{e_i - 1} \cdot (p_i - 1)\right)$. Poiché si vede subito che $p \nmid p_i$, per ogni i, allora $p \mid (p_i - 1)$, per qualche i. D'altro lato $2p + 1 = p_i \cdot n'$ dove $n' := \frac{n}{p_i}$. Se $n' > 1$, allora è subito visto che deve essere $n' > 2$, e quindi si avrebbe che $p \nmid (p_i - 1)$, poiché avremmo che $p > p_i - 1$, e ciò è assurdo. Pertanto $n' = 1$, cioè $2p + 1 = p_i$ è un primo. **(b)**. È una semplice conseguenza di (a).]

6.16. Sia p un primo dispari. Mostrare che $X^4 \equiv -4 \pmod{p}$ è risolubile se e soltanto se $p \equiv 1 \pmod{4}$.
[Suggerimento. Si noti che $X^4 + 4 = ((X+1)^2 + 1)((X-1)^2 + 1)$. Pertanto $X^4 \equiv -4 \pmod{p}$ è risolubile se e soltanto se almeno una delle congruenze $((X+1)^2 + 1) \equiv 0 \pmod{p}$ oppure $((X-1)^2 + 1) \equiv 0 \pmod{p}$ è risolubile. È subito che entrambe sono risolubili se e soltanto se $(\frac{-1}{p}) = 1$.]

6.17. Calcolare i seguenti simboli di Jacobi:

$$\textbf{(a)}\ \left(\frac{713}{1009}\right); \qquad \textbf{(b)}\ \left(\frac{111}{991}\right); \qquad \textbf{(c)}\ \left(\frac{313}{367}\right).$$

[Soluzione. **(a)** Si noti che $1009 \equiv 1 \pmod 4$ ed è primo e che $713 = 23 \cdot 31$.

$$\begin{aligned}\left(\frac{23}{1009}\right) &= \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \\ &= \left(\frac{4}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1, \\ \left(\frac{31}{1009}\right) &= \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \\ &= \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = \\ &= -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1\end{aligned}$$

quindi $(\frac{713}{1009}) = 1$. **(b)**: -1. **(c)**: 1.]

6.18. Determinare il numero delle soluzioni della congruenza

$$X^2 \equiv 4 \pmod{105}.$$

[Soluzione. Poiché $105 = 3 \cdot 5 \cdot 7$ e ciascuna delle congruenze $X^2 \equiv 4 \pmod 3, X^2 \equiv 4 \pmod 5, X^2 \equiv 4 \pmod 7$ ha due soluzioni, allora la congruenza data ha 2^3 soluzioni (mod 105): $2, 23, 37, 47, 58, 68, 82, 103$.]

6.19. (Gauss). Sia p un primo dispari. Siano $n, n+1$ due interi consecutivi nel sistema ridotto di residui $S^* := \{1, 2, \ldots, p-1\}$. Denotiamo con (RR) (rispettivamente: (RN); (NR); (NN)) il numero delle coppie di interi consecutivi $(n, n+1)$ di S^* tali che $(\frac{n}{p}) = 1$ e $(\frac{n+1}{p}) = 1$ (rispettivamente: $(\frac{n}{p}) = 1$ e $(\frac{n+1}{p}) = -1$; $(\frac{n}{p}) = -1$ e $(\frac{n+1}{p}) = 1$; $(\frac{n}{p}) = -1$ e $(\frac{n+1}{p}) = -1$). I seguenti enunciati mostrano che la distribuzione dei residui e dei non residui quadratici è essenzialmente casuale, in quanto ciascuna delle quattro possibilità si presenta con una frequenza pressoché uguale (cioè, frequenza uguale a circa $\left[\frac{1}{4}(p-1)\right]$).
Poniamo $\varepsilon := (-1)^{\frac{p-1}{2}} = (\frac{-1}{p}) = (\frac{p-1}{p})$. Mostrare che:

(1) (RR) + (RN) $= \frac{1}{2}(p - 2 - \varepsilon)$;

(2) (NR) + (NN) $= \frac{1}{2}(p - 2 + \varepsilon)$;

(3) (RR) + (NR) $= \frac{1}{2}(p-1) - 1 = \frac{1}{2}(p-3)$;

(4) (RN) + (NN) $= \frac{1}{2}(p-1)$;

(5) $\sum_{n=1}^{p-2}(\frac{n(n+1)}{p}) = -1$;

(6) (RR) + (NN) - (RN) - (NR) $= -1$;

(7) (RR) + (NN) $= \frac{1}{2}(p-3)$;

(8) (RR) - (NN) $= -\frac{1}{2}(1+\varepsilon)$;

(9) (RR) $= \frac{1}{4}(p-4-\varepsilon)$;

(10) (NN) $= \frac{1}{4}(p-2+\varepsilon)$;

(11) (RN) + (NR) $= \frac{1}{2}(p-1)$;

(12) (RN) - (NR) $= 1-\frac{1}{2}(1+\varepsilon) = \frac{1}{2}(1-\varepsilon)$;

(13) (RN) $= \frac{1}{4}(p-\varepsilon)$;

(14) (NR) $= \frac{1}{4}(p-2+\varepsilon)$.

[Suggerimento. **(1)** Il numero (RR) + (RN) è il numero delle coppie $(n, n+1)$ per cui n è un residuo quadratico, dove n varia tra 1 e $p-2$. Quindi tale numero dipende dal valore di

$$\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = \varepsilon.$$

Se $p-1$ è un non residuo quadratico, cioè se $\varepsilon = -1$, allora i residui quadratici sono tutti tra gli interi $\{1, 2, \ldots, p-2\}$ e quindi (RR) + (RN) $= \frac{1}{2}(p-1)$. Se $p-1$ è un residuo quadratico, cioè $\varepsilon = 1$, allora i residui quadratici tra gli interi $\{1, 2, \ldots, p-2\}$ sono $\frac{1}{2}(p-1)-1 = \frac{1}{2}(p-3)$.
Similmente si dimostrano **(2)**, **(3)** e **(4)**.
(5) Se n^* è un inverso aritmentico di n allora:

$$n(n+1) = n^2 + n \equiv n^2(1+n^*) \pmod{p}$$

e quindi

$$\sum_{n=1}^{p-2}\left(\frac{n(n+1)}{p}\right) = \sum_{n=1}^{p-2}\left(\frac{1+n^*}{p}\right) = \sum_{n=2}^{p-1}\left(\frac{n}{p}\right).$$

Poichè

$$\sum_{n=1}^{p-1}\left(\frac{n}{p}\right) = 0,$$

allora

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

(6) segue da (5).
(7) e **(8)** sono semplici conseguenze di (6), (1), e (2).
(9) e **(10)** seguono da (7) e (8).
(11) e **(12)** seguono da (3) e (4) e dal fatto che (RN) - (NR) + (NN) - (RR) =1.
(13) e **(14)** seguono immediatamente da (11) e (12).]