La legge di reciprocità quadratica

Symétrie est ce qu'on voit d'une vue

Blaise Pascal

Rocco Chirivì *Dipartimento di Matematica e Fisica "Ennio De Giorgi" - Università del Salento*

La *legge di reciprocità quadratica* è stata congetturata da Eulero e Legendre e dimostrata in modo rigoroso da Gauss nella sua fondamentale opera *Disquisitiones Arithmeticae* (1798). Questo risultato, di cui Gauss ha dato ben otto diverse dimostrazioni e da lui chiamato "aureum theorema", permette, svelando una simmetria nascosta, di decidere quando un numero intero è un residuo quadratico modulo un numero primo.

Per illustrare l'importanza di tale problema consideriamo le equazioni di secondo grado nei numeri reali. La formula risolutiva di un'equazione quadratica $ax^2 + bx + c = 0$, nell'incognita x, era già nota, seppur solo per esempi e con limitazioni sul segno dei coefficienti a, b, c, ai matematici babilonesi intorno al 400 a.c. (vedi [1], anche per tutte le altre notizie storiche). Comunque, come consueto per l'antichità, le soluzioni negative venivano scartate. E, cosa più importante per ciò di cui vogliamo parlare qui, i problemi considerati avevano sempre soluzioni reali; cioè il discriminante $\Delta \doteq b^2 - 4ac$ delle equazioni quadratiche, era sempre un numero positivo.

Dobbiamo aspettare il XVI secolo per un primo uso consapevole dei numeri complessi; ad esempio Cardano nell'*Ars magna* (1545) suggerisce, pur ammettendo trattarsi di "torture mentali", che le soluzioni di $x^2 - 10x + 40 = 0$ siano $5 + \sqrt{-15}$ e $5 - \sqrt{-15}$. Solo con l'estensione del campo dei numeri reali al campo dei numeri complessi è possibile scrivere la formula risolutiva dell'equazione generica di secondo grado sopra riportata. Le due radici sono $(-b \pm \sqrt{\Delta})/2a$ e quindi, per valori di a, b, c che rendono negativo Δ, si tratta di numeri complessi *non* reali.

Quest'estensione è infatti necessaria visto che non tutti i numeri reali ammettono radice quadrata: un numero reale ammette radice quadrata reale se e solo se è non negativo. Possiamo esprimere quanto appena detto in maniera equivalente come: l'insieme $\mathbb{R}^{*2}$ dei numeri reali non nulli che sono quadrati di altri numeri reali coincide con l'insieme $\mathbb{R}_{>0}$ dei numeri positivi.

Possiamo anche studiare le equazioni di secondo grado sul campo dei numeri razionali: consideriamo, cioè, un'equazione $ax^2 + bx + c = 0$ con $a, b, c \in \mathbb{Q}$ e ci chiediamo quando abbia soluzioni razionali. Visto che $\mathbb{Q}$ è un sottocampo di $\mathbb{R}$, l'equazione deve avere soluzioni reali; quindi $\Delta > 0$. Ovviamente questo è necessario ma non

sufficiente in quanto se abbiamo, ad esempio, $\Delta = 2$ allora $\sqrt{2} \notin \mathbb{Q}$. Infatti, per avere soluzioni razionali, dobbiamo chiedere che Δ sia il quadrato di una frazione; devono esistere cioè $e, f \in \mathbb{N}$, con $f > 0$, per cui $\Delta = (e/f)^2$.

È invece ovvio che sul campo $\mathbb{C}$ dei numeri complessi non vi è alcun problema: ogni equazione di secondo grado ammette due radici se contate con molteplicità.

Oltre ai campi $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ considerati sopra, esistono anche campi con un numero finito di elementi. Tali campi sono completamente classificati: per ogni numero primo p e intero positivo n esiste, a meno di isomorfismo, un solo campo con p^n elementi, esso viene indicato con $\mathbb{F}_{p^n}$.

I campi finiti sono di fondamentale importanza per la teoria dei numeri, la geometria algebrica e le applicazioni alla crittografia ma anche, ad esempio, per certi settori della fisica. Noi saremo interessanti in particolare ai campi $\mathbb{F}_p$ (con p numero primo). È possibile realizzare $\mathbb{F}_p$ come l'insieme $\mathbb{Z}/p\mathbb{Z}$ delle classi di resto degli interi modulo p. In quello che segue, con un lieve abuso di notazione, indicheremo la classe di un intero a modulo il primo p con lo stesso simbolo a. Così, ad esempio, abbiamo $-19 = 2$ in $\mathbb{F}_7$ in quanto -19 e 2 hanno lo stesso resto quando divisi per 7. Osserviamo anche che le operazioni in $\mathbb{F}_p$ sono quelle dell'aritmetica modulare: la somma e il prodotto delle classi di a e b è, rispettivamente, la classe della somma e del prodotto di a e b.

Come abbiamo fatto per $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, è naturale ed, anzi, di grande importanza, studiare le equazioni di secondo grado nei campi finiti. Inoltre se il primo p non è 2 allora la formula risolutiva vista sopra continua ad essere valida e può essere dimostrata nello stesso modo che per $\mathbb{R}$.

Ad esempio, se consideriamo l'equazione $x^2 - x + 5 = 0$ nel campo $\mathbb{F}_7$, abbiamo $\Delta = -19 = 2$ e quindi, osservando che $3^2 = 9 = 2$ in $\mathbb{F}_7$, otteniamo che le soluzioni sono $(1 \pm \sqrt{2})/2 = (1 \pm 3)/2$, cioè 2 e -1. Si noti che il simbolo $\sqrt{2}$ significa "la classe di resto che ha per quadrato la classe di resto 2".

Consideriamo un ulteriore esempio sempre in $\mathbb{F}_7$: l'equazione $x^2 - x + 3 = 0$ non ha alcuna soluzione in quanto $\Delta = -11 = 3$ non ammette radice quadrata in $\mathbb{F}_7$. Infatti l'insieme $\mathbb{F}_7^{*2}$ dei residui quadratici non nulli di $\mathbb{F}_7$ è dato da $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4 = -3$ e $(\pm 3)^2 = 9 = 2$; in particolare 3 non è un quadrato modulo 7.

Come si vede subito da questi esempi, per studiare le equazioni di secondo grado sui campi finiti $\mathbb{F}_p$, è necessario essere in grado di decidere quali siano i residui quadratici: diciamo che un intero q è un *residuo quadratico* modulo un primo p se esiste un intero a per cui $q \equiv a^2 \pmod{p}$. È ovvio che q è un residuo quadratico non nullo modulo p se e solo se $q \in \mathbb{F}_p^{*2}$. Capire se un intero q è un residuo quadratico è un problema per niente ovvio: ad esempio la classe di 29 è o meno un quadrato modulo il primo 43? Una possibile risposta elementare si ha calcolando tutti i possibili quadrati $(\pm 1)^2, (\pm 2)^2, (\pm 3)^2, \ldots$ modulo 43 e verificando se 29 appare in tale lista.

In questo problema q e p hanno ruoli molto diversi: q è una classe di resto modulo p o, in altri termini, q è considerato come elemento del campo finito $\mathbb{F}_p$. Nostro obiettivo in questo articolo è mostrare che invece, grazie alla legge di reciprocità quadratica, esiste una simmetria: per decidere se q è un quadrato modulo p si può, in maniera equivalente, studiare se p è un quadrato modulo q. Inoltre, questa simmetria ci permette di trovare una risposta efficiente al problema di decidere se un intero è o meno un residuo quadratico.

Ci toccherà però costruire un piccolo tratto di teoria per poter anche solo enunciare la legge di reciprocità quadratica. Ma, come succede spesso in matematica, la fatica compiuta sarà ampiamente ripagata dalla scoperta di quella che abbiamo chiamato simmetria nascosta.

Anche se posposte per facilità di lettura, abbiamo deciso di includere le dimostrazioni dei risultati che vedremo. È infatti solo studiando con grande attenzione le dimostrazioni che si può apprezzare la matematica. Quelle qui riportate sono poco più che traduzioni di ciò che può essere letto in "A course in arithmetic" di Jean-Pierre Serre [2].

Cominciamo definendo il *simbolo di Legendre*: dato un intero a definiamo

$$\left(\frac{a}{p}\right) \doteq \begin{cases} 0 & \text{se } a \text{ è divisibile per } p \\ 1 & \text{se } a \text{ è un residuo quadratico} \\ & \text{non nullo modulo } p \\ -1 & \text{se } a \text{ non è un residuo quadratico} \\ & \text{modulo } p. \end{cases}$$

Questo è equivalente a dire che $\left(\frac{a}{p}\right) = 1$ se e solo se $a \in \mathbb{F}_p^{*2}$. Ad esempio: per quanto abbiamo visto su 2 e 3 in $\mathbb{F}_7$, si ha

$$\left(\frac{2}{7}\right) = 1 \quad \text{e} \quad \left(\frac{3}{7}\right) = -1.$$

La nostra prima osservazione è la seguente

Proposizione 1 (Criterio di Eulero)**.** *L'insieme $\mathbb{F}_p^{*2}$ dei residui quadratici non nulli è il nucleo dell'omomorfismo*

$$\mathbb{F}_p^* \ni x \longmapsto x^{(p-1)/2} \in \{\pm 1\}$$

ed ha indice 2 in $\mathbb{F}_p^*$. In particolare

$$\left(\frac{x}{p}\right) = x^{(p-1)/2}$$

per ogni $x \in \mathbb{F}_p^*$.

Il criterio di Eulero ci dice che in $\mathbb{F}_p^*$ ci sono tanti residui quadratici quanti non residui quadratici visto che $\mathbb{F}_p^{*2}$ ha indice 2 in $\mathbb{F}_p^*$.

Grazie al criterio di Eulero possiamo calcolare $\left(\frac{x}{p}\right)$ eseguendo la potenza $x^{\frac{p-1}{2}}$ in $\mathbb{F}_p$. Ad esempio

$$\left(\frac{2}{7}\right) = 2^{\frac{7-1}{2}} = 2^3 = 8 = 1$$

e

$$\left(\frac{3}{7}\right) = 3^{\frac{7-1}{2}} = 3^3 = 27 = -1$$

in $\mathbb{F}_7$; e questo concorda con quanto avevamo già visto. Ma il criterio di Eulero non è ancora abbastanza, ad esempio abbiamo

$$\left(\frac{29}{43}\right) = 29^{\frac{43-1}{2}} = 29^{21}$$

e questo è un calcolo non immediato.

Tale metodo, però, può essere applicato per decidere se -1 è un quadrato modulo p. Infatti abbiamo subito

Corollario 2. *Per il simbolo di Legendre in -1 si ha*

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

e quindi -1 è un residuo quadratico modulo p se e solo se p è congruo ad 1 modulo 4.

Ad esempio, il primo 7 non è congruo ad 1 modulo 4 e quindi -1 non è un quadrato modulo 7, infatti -1 non compare nella lista dei quadrati visti sopra. Come altro esempio consideriamo il primo 13; visto che esso è congruo ad 1 modulo 4 sappiamo che -1 è un quadrato in $\mathbb{F}_{13}$, ed infatti abbiamo $5^2 = 25 = -1$. Come conseguenza l'equazione $x^2 + 1 = 0$ non ha alcuna soluzione in $\mathbb{F}_7$ mentre ha le due soluzioni ± 5 in $\mathbb{F}_{13}$.

Il criterio di Eulero può esser usato per dimostrare il seguente risultato che ci dice quando 2 è un residuo quadratico modulo p.

Corollario 3. *Per il simbolo di Legendre in 2 si ha*

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

e quindi 2 è un residuo quadratico modulo p se e solo se p è congruo ad 1 o a -1 modulo 8.

Come esempio consideriamo il primo 17. Visto che 17 è congruo ad 1 modulo 8, 2 è un quadrato modulo 17; ed infatti $6^2 = 36 = 2$ modulo 17.

Nei due casi di -1 e 2 analizzati, il simbolo di Legendre dipende dall'appartenenza di p a certe classi modulo un altro intero $N_{-1} \doteq 4$ per -1 e $N_2 \doteq 8$ per 2. Questo è vero in generale, non solo per -1 e 2, ed è una conseguenza di quanto vedremo in seguito. Appare già qui un primo fenomeno di simmetria: il primo p da modulo diventa una classe modulo un altro intero per decidere se -1 e 2 sono residui quadratici.

Come altra conseguenza del criterio di Eulero, abbiamo che il simbolo di Legendre è moltiplicativo, cioè

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right),$$

visto che la mappa $x \longmapsto x^{(p-1)/2}$ è un omomorfismo.

Si noti che, mentre è chiaro che il prodotto di due residui quadratici è ancora un residuo quadratico e che il prodotto di un residuo quadratico e un non residuo quadratico è un non residuo quadratico, non è ovvio che il prodotto di due non quadrati sia un quadrato. Questo però segue da quanto provato: se x e y sono non residui quadratici allora

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = (-1)\cdot(-1) = 1,$$

cioè xy *è* un quadrato modulo p.

Dalla moltiplicatività di $x \longmapsto \left(\frac{x}{p}\right)$ segue che, per calcolare $\left(\frac{n}{p}\right)$, con n intero qualsiasi, basta fattorizzare n in primi, usando anche il fattore -1 se n è negativo. Avendo già descritto come calcolare il simbolo di Legendre per -1 e 2, in problema del calcolo di $\left(\frac{n}{p}\right)$ viene così ricondotto al calcolo di $\left(\frac{q}{p}\right)$ con p e q primi dispari distinti.

Possiamo ora enunciare la legge di reciprocità quadratica; in particolare vediamo che il simbolo di Legendre ha una semplicissima, e inattesa, simmetria per lo scambio $p \longleftrightarrow q$.

Teorema 4 (Legge di reciprocità quadratica)**.** *Se p e q sono primi dispari distinti allora*

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

Cioè

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

tranne nel caso in cui p e q sono entrambi congrui a -1 modulo 4 in cui

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

Ricaviamo che i due problemi:

- q è o meno un quadrato modulo p
- p è o meno un quadrato modulo q

hanno la stessa risposta tranne nel caso in cui p e q hanno entrambi resto -1 per 4 in cui hanno risposta opposta. La legge di reciprocità è quindi un risultato altamente non banale che svela un elegante e sorprendente legame tra i due problemi.

Vediamo un esempio. Abbiamo già osservato che $\left(\frac{3}{7}\right) = -1$, cioè 3 non è un quadrato in $\mathbb{F}_7$; inoltre $\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$. Quindi $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right)$ e infatti 3 e 7 sono entrambi congrui a -1 modulo 4.

Un altro esempio. Per $q = 7$ e $p = 5$ si ha $\left(\frac{5}{7}\right) = -1$ in quanto $5 = -2$ non è in $\mathbb{F}_7^{*2}$ e anche $\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$ in quanto in $\mathbb{F}_5^*$ solo ± 1 sono quadrati. Quindi in questo secondo esempio i due simboli di Legendre $\left(\frac{5}{7}\right)$ e $\left(\frac{7}{5}\right)$ sono uguali ed infatti 5 non è congruo a -1 modulo 4.

La legge di reciprocità quadratica e il calcolo del simbolo di Legendre in 2 ci permettono di risolvere subito il problema che ci eravamo posti: 29 è un residuo quadratico modulo 43? Calcolando le classi di resto modulo 4 dei primi convolti abbiamo

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = \\ = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$$

e quindi 29 non è un quadrato modulo 43.

Con quanto visto è possibile discutere un'equazione di secondo grado $ax^2 + bx + c = 0$ in un campo finito $\mathbb{F}_p$. Calcoliamo $\Delta = b^2 - 4ac$ e, con la legge di reciprocità quadratica, come fatto sopra per 29 e 43, calcoliamo il simbolo di Legendre $\left(\frac{\Delta}{p}\right)$. Se otteniamo -1, cioè se Δ non è un residuo quadratico modulo p, allora l'equazione non ha alcuna soluzione. Se invece otteniamo 1, cioè se Δ è un residuo quadratico, allora l'equazione può essere risolta. Si noti però che la legge di reciprocità non ci permette di *calcolare* la radice quadrata di Δ in $\mathbb{F}_p$, possiamo solo decidere se essa esiste o meno.

Come esempio di applicazione della legge di reciprocità quadratica possiamo risolvere un esercizio posto da Goro Shimura in [3]. Consideriamo il polinomio $f(x) \doteq x^2 - 3$ e calcoliamone i valori in $0, 1, 2, 3, \ldots$ Fattorizzandoli otteniamo

$$-3,\ -2,\ 1,\ 6 = 2 \cdot 3,\ 13,\ 22 = 2 \cdot 11, \\ 33 = 3 \cdot 11,\ 46 = 2 \cdot 23,\ 61, \ldots$$

Escludendo 2 e 3, i primi che appaiono in queste fattorizzazioni sono $11,\ 13,\ 23,\ 61, \ldots$. È possibile caratterizzare tali primi? E continuando a calcolare il polinomio $f(x)$ e a fattorizzare i risultati, quali altri primi troveremo?

Osserviamo che un primo p diverso da 3 appare come fattore di $f(n)$ con $n \in \mathbb{N}$ se e solo se $n^2 - 3 = f(n) \equiv 0 \pmod{p}$; questo è come dire che 3 è un quadrato modulo p. Allora $p \neq 3$ appare nella lista dei primi che stiamo

considerando se e solo se $\left(\frac{3}{p}\right) = 1$. Ma la legge di reciprocità ci dice che, per un primo p dispari, si ha $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ se $p \equiv 1 \pmod 4$, mentre $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ se $p \equiv -1 \pmod 4$. Inoltre, visto che $p \neq 3$, abbiamo $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$ se $p \equiv 1 \pmod 3$ mentre $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$ se $p \equiv -1 \pmod 3$. Mettendo insieme abbiamo

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod{12} \\ -1 & \text{se } p \equiv \pm 5 \pmod{12} \end{cases}$$

Questo ci permette di concludere che i primi che compaiono nella lista sono tutti e soli quelli congrui a 1 o -1 modulo 12.

Osserviamo, inoltre, che il calcolo del simbolo di Legendre in 3 ci dice che per decidere se 3 è un residuo quadratico modulo p basta controllare in che classe modulo $N_3 \doteq 12$ sia il primo p. Proponiamo al lettore di dimostrare, usando quanto visto, che, analogamente ai casi 2 e 3, si può porre $N_q \doteq 4q$ per ogni primo q.

Oltre alla legge di reciprocità quadratica qui presentata, esistono anche leggi di reciprocità superiore. Lo stesso Gauss, sempre in *Disquisitiones Arithmeticae*, ha enunciato la legge di reciprocità quartica mentre la legge di reciprocità cubica è dovuta al suo studente Eisenstein. Queste leggi sono poi confluite nella *teoria del corpo di classe*, in particolare nella *legge di reciprocità di Artin*, che tratta le estensioni dei numeri razionali con gruppo di Galois abeliano. Ancora oltre, lo studio del caso non abeliano è oggi al centro della ricerca in matematica con una rete di congetture e risultati parziali che formano il *programma di Langlands*.

Vediamo ora, come promesso, le dimostrazioni dei risultati proposti.

Ricordiamo alcuni fatti elementari di teoria dei campi. Per prima cosa ogni campo $\mathbb{K}$ ammette una *chiusura algebrica*, cioè esiste un altro campo $\overline{\mathbb{K}}$ che contiene $\mathbb{K}$ e tale che ogni polinomio $f(x)$ a coefficienti in $\overline{\mathbb{K}}$ ha una radice, cioè una soluzione di $f(x) = 0$, in $\overline{\mathbb{K}}$. Ad esempio la chiusura algebrica dei numeri reali è il campo dei numeri complessi. Indicheremo la chiusura algebrica di $\mathbb{F}_p$ con $\overline{\mathbb{F}}_p$.

L'insieme $\mathbb{F}_p^*$ delle classi di resto diverse da 0 è un gruppo di ordine $p-1$; quindi, in particolare, $x^{p-1} = 1$ per ogni $x \in \mathbb{F}_p^*$. Non solo, come sottoinsieme di $\overline{\mathbb{F}}_p$, $\mathbb{F}_p^*$ è esattamente l'insieme degli x per cui $x^{p-1} = 1$.

Cominciamo dal criterio di Eulero.

Dimostrazione della Proposizione 1. Essendo $\mathbb{F}_p^*$ un gruppo abeliano è chiaro che la mappa $\varphi : x \longmapsto x^{(p-1)/2}$ è un omomorfismo di $\mathbb{F}_p^*$ in sé. Inoltre si ha $(x^{(p-1)/2})^2 = x^{p-1} = 1$ in quanto $\mathbb{F}_p^*$ ha ordine $p-1$; quindi $x^{(p-1)/2}$ è una soluzione dell'equazione $t^2 - 1 = 0$ nell'indeterminata t. Tale equazione ha per soluzioni ± 1 in ogni campo, quindi anche in $\mathbb{F}_p$. Questo prova che l'immagine di φ è contenuta in $\{\pm 1\}$.

Sia ora $y \in \overline{\mathbb{F}}_p$ una radice quadrata di x. Allora $x^{(p-1)/2} = y^{p-1}$ e, inoltre, $y^{p-1} = 1$ se e solo se $y \in \mathbb{F}_p$, cioè se e solo se x ha una radice quadrata in $\mathbb{F}_p$. E questo è equivalente a $x \in \mathbb{F}_p^{*2}$. Abbiamo così provato che $\mathbb{F}_p^{*2} = \operatorname{Ker}\varphi$ e che $\left(\frac{x}{p}\right) = x^{(p-1)/2}$.

Osserviamo ora che l'omomorfismo $\mathbb{F}_p^* \ni x \longmapsto x^2 \in \mathbb{F}_p^*$ non è iniettivo in quanto $(-1)^2 = 1$ e quindi esso non è neanche suriettivo. Visto che l'immagine di questo omomorfismo è $\mathbb{F}_p^{*2}$ abbiamo provato che $\operatorname{Ker}\varphi = \mathbb{F}_p^{*2}$ è propriamente contenuto in $\mathbb{F}_p^*$. Allora φ è una mappa suriettiva (cioè -1 viene raggiunto). Segue quindi che $\operatorname{Ker}\varphi$ ha indice 2 in $\mathbb{F}_p^*$, cioè metà elementi sono quadrati e metà non lo sono. □

Vediamo ora come il calcolo del simbolo di Legendre in 2 si ottenga dal criterio di Eulero.

Dimostrazione del Corollario 3. Sia α una radice ottava primitiva dell'unità in $\overline{\mathbb{F}}_p$ (cioè α è una soluzione di $t^8 - 1 = 0$ ma non è soluzione di $t^4 - 1$, in altre parole α è soluzione di $t^4 + 1$) e sia $y \doteq \alpha + \alpha^{-1}$. Abbiamo

$$y^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + 2 + \alpha^{-2} = 2,$$

dove abbiamo usato

$$\alpha^2 + \alpha^{-2} = \alpha^{-2}(\alpha^4 + 1) = 0.$$

Cioè y è una radice di 2 in $\overline{\mathbb{F}}_p$. Allora

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

Osserviamo ora che, avendo $\mathbb{F}_p$ caratteristica p risulta,

$$y^p = (\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p}.$$

Quindi, se $p \equiv \pm 1 \pmod 8$, abbiamo

$$y^p = \alpha^p + \alpha^{-p} = \alpha + \alpha^{-1} = y,$$

da cui

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

Se, invece, $p \equiv \pm 3 \pmod 8$ abbiamo

$$y^p = \alpha^p + \alpha^{-p} = \alpha^3 + \alpha^{-3} = -(\alpha + \alpha^{-1}) = -y$$

dove abbiamo usato di nuovo $\alpha^4 = -1$. Concludiamo che

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

□

Nella dimostrazione della legge di reciprocità quadratica useremo due lemmi. Fissiamo p e q primi dispari distinti e sia ω una radice primitiva q–esima dell'unità in $\overline{\mathbb{F}}_p$. Osserviamo che se $x \in \mathbb{F}_q \simeq \mathbb{Z}/q\mathbb{Z}$ allora ω^x è ben definito; possiamo così considerare quella che si chiama *somma di Gauss*

$$y = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right)\omega^x.$$

Ad esempio, visto che $\mathbb{F}_7^{*2} = \{1, 2, -3 = 4\}$, per $q = 7$ si ha

$$y = \omega + \omega^2 - \omega^3 + \omega^4 - \omega^5 - \omega^6$$

dove $\omega \in \overline{\mathbb{F}}_p$ è una radice settima primitiva dell'unità.

Nel seguente lemma vediamo che questa somma ci fornisce, a meno del segno, una radice quadrata di q in $\overline{\mathbb{F}}_p$.

Lemma 5 (Lemma di Gauss)**.** *Si ha* $y^2 = (-1)^{(q-1)/2}q$ *in* $\overline{\mathbb{F}}_p$.

Dimostrazione. Abbiamo

$$\begin{aligned} y^2 &= \textstyle\sum_{x,z \in \mathbb{F}_q} \left(\frac{xz}{q}\right)\omega^{x+z} \\ &= \textstyle\sum_{u \in \mathbb{F}_q} \omega^u \left(\sum_{t \in \mathbb{F}_q} \left(\frac{t(u-t)}{q}\right)\right) \end{aligned}$$

Ora, se $t \neq 0$, allora

$$\begin{aligned} \left(\frac{t(u-t)}{q}\right) &= \left(\frac{-t^2}{q}\right)\left(\frac{1-ut^{-1}}{q}\right) \\ &= (-1)^{(q-1)/2}\left(\frac{1-ut^{-1}}{q}\right) \end{aligned}$$

dove abbiamo usato che

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

Mentre, se $t = 0$, allora chiaramente

$$\left(\frac{t(u-t)}{q}\right) = 0.$$

Quindi abbiamo

$$y^2 = (-1)^{(q-1)/2} \sum_{u \in \mathbb{F}_q} A_u \omega^u$$

con

$$A_u = \sum_{t \in \mathbb{F}_q^*} \left(\frac{1-ut^{-1}}{q}\right).$$

Osserviamo ora che

$$A_0 = \sum_{t \in \mathbb{F}_q^*} \left(\frac{1}{q}\right) = q - 1$$

in quanto $\left(\frac{1}{q}\right) = 1$. Se invece $u \neq 0$ allora, al variare di t in $\mathbb{F}_q^*$, l'elemento $1 - ut^{-1}$ assume una ed una sola volta tutti i valori in $\mathbb{F}_q \setminus \{1\}$. Quindi, per $u \neq 0$, si ha

$$\begin{aligned} A_u &= \textstyle\sum_{t \in \mathbb{F}_q^*} \left(\frac{1-ut^{-1}}{q}\right) \\ &= \textstyle\sum_{s \in \mathbb{F}_q \setminus \{1\}} \left(\frac{s}{q}\right) \\ &= \textstyle\sum_{s \in \mathbb{F}_q} \left(\frac{s}{q}\right) - \left(\frac{1}{q}\right) \\ &= -1 \end{aligned}$$

dove nell'ultima uguaglianza abbiamo usato che la somma indicata vale 0 in quanto $\mathbb{F}_p^{*2}$ ha indice 2 in $\mathbb{F}_p^*$, cioè ci sono tanti quadrati quanti non quadrati.

Possiamo ora concludere la dimostrazione del lemma mettendo insieme quanto visto e notando che, essendo ω una radice q–esima dell'unità, si

ha $\sum_{u\in\mathbb{F}_q^*}\omega^u = \omega+\omega^2+\cdots+\omega^{q-1} = -1$

$$\begin{aligned} y^2 &= (-1)^{(q-1)/2}\textstyle\sum_{u\in\mathbb{F}_q} A_u\omega^u \\ &= (-1)^{(q-1)/2}(q-1-\textstyle\sum_{u\in\mathbb{F}_q^*}\omega^u) \\ &= (-1)^{(q-1)/2}q. \end{aligned}$$

□

L'altro lemma di cui avremo bisogno è il seguente

Lemma 6. *Si ha* $y^{p-1} = \left(\frac{p}{q}\right)$.

Dimostrazione. Nei calcoli che seguono, basta osservare che $\overline{\mathbb{F}}_p$ è un campo a caratteristica p e che p^{-1} è un quadrato modulo q se e solo se lo è p. Abbiamo

$$\begin{aligned} y^p &= (\textstyle\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\omega^x)^p \\ &= \textstyle\sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\omega^{px} \\ &= \textstyle\sum_{z\in\mathbb{F}_q}\left(\frac{zp^{-1}}{q}\right)\omega^z \\ &= \left(\frac{p}{q}\right)\textstyle\sum_{z\in\mathbb{F}_q}\left(\frac{z}{q}\right)\omega^z \\ &= \left(\frac{p}{q}\right)y \end{aligned}$$

da cui la tesi visto che, per il lemma precedente, y è diverso da 0. □

Infine, possiamo ora vedere la dimostrazione della legge di reciprocità.

Dimostrazione del Teorema 4. Sia

$$y = \sum_{x\in\mathbb{F}_q}\left(\frac{x}{q}\right)\omega^x \in \overline{\mathbb{F}}_q$$

la somma di Gauss considerata sopra. Dal primo lemma sappiamo che

$$y^2 = (-1)^{(q-1)/2}q$$

e quindi

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

usando il secondo lemma. Per concludere basta ora osservare che

$$\begin{aligned} \left(\frac{(-1)^{(q-1)/2}}{p}\right) &= \left(\frac{-1}{p}\right)^{(q-1)/2} \\ &= ((-1)^{(p-1)/2})^{(q-1)/2} \\ &= (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \end{aligned}$$

per l'espressione data del simbolo di Legendre in -1. □

[1] Morris Kline: *Storia del pensiero matematico*, Einaudi, Volumi 1 & 2 (1999).

[2] Jean–Pierre Serre: *A course in arithmetic*, Springer–Verlag (1973).

[3] Goro Shimura: *The map of my life*, Springer–Verlag (2008).

Rocco Chirivì: Laureato in matematica all'università di Pisa e alla Scuola Normale Superiore. Ha conseguito il dottorato di ricerca presso la Scuola Normale Superiore. È stato ricercatore in Algebra alla Sapienza di Roma e all'università di Pisa. Da maggio 2012 è ricercatore presso il dipartimento di Matematica e Fisica dell'Università del Salento. Si occupa di teoria delle rappresentazioni di algebre e gruppi di Lie.