Lezione 27

Prerequisiti: Congruenze modulo un intero.

La legge di reciprocità quadratica.

Dedichiamo quest'ultimo capitolo allo studio della risolubilità delle congruenze quadratiche del tipo

$$x^2 \equiv a \pmod{p}, \qquad (*)$$

dove a è un qualsiasi intero e p è un numero primo.

Definizione 27.1 Sia p un numero primo, sia a un intero. Allora a si dice un *residuo quadratico modulo p* se la congruenza (*) ha soluzione.

Esempio 27.2
a) 2 non è un residuo quadratico modulo 3.
b) 2 e 3 non sono residui quadratici modulo 5, mentre lo sono 1 e 4.

Sarà utile la seguente notazione:

Definizione 27.3 Per ogni primo dispari p ed ogni intero a si dice *simbolo di Legendre* "a su p" il numero

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se} \quad p \mid a \\ 1 & \text{se} \quad p \nmid a \text{ e } a \text{ è un residuo quadratico modulo } p \\ -1 & \text{altrimenti} \end{cases}$$

Osservazione 27.4 Per ogni intero a, se b è un intero tale che $a \equiv b \pmod{p}$, allora, evidentemente, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. In particolare, detto r il resto della divisione di a per p, evidentemente si ha che $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$. Quindi, nel calcolo del simbolo di Legendre, potremo sempre ricondurci ai numeri $0,1,...,p-1$. Ciò si rivela utile già nell'applicazione del prossimo risultato, che dà una formula esplicita per calcolare il valore di $\left(\frac{a}{p}\right)$.

Proposizione 27.5 (*Criterio di Eulero*) Per ogni primo dispari p ed ogni intero a si ha

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

Dimostrazione: Se p divide a, la tesi è banale. Supponiamo allora che p non divida a. Sia $g \in \{1,2,...,p-1\}$ tale che $\mathbf{Z}_p^{\,*} = \langle [g]_p \rangle$ (ricordiamo che il gruppo moltiplicativo di un campo finito

è sempre ciclico, vedi Algebra 2, Proposizione 24.8). Sia $i \in \mathbb{N}$ tale che $[a]_p = [g^i]_p$, cioè $a \equiv g^i \pmod{p}$. Allora, in base all'Osservazione 27.4, si ha

$$\left(\frac{a}{p}\right) = \left(\frac{g^i}{p}\right) \tag{1}$$

Essendo per ipotesi p dispari, $\frac{p-1}{2}$ è intero. Quindi possiamo considerare $h = g^{\frac{p-1}{2}}$. Si ha, allora,

$$[h]_p{}^2 = [g]_p{}^{p-1} = [1]_p, \quad \text{cioè} \quad p \mid (h+1)(h-1).$$

Ora, essendo $[h]_p = \left[g^{\frac{p-1}{2}}\right]_p \neq [1]_p$, segue che $p \nmid h-1$. Allora, essendo p primo, si ha che $p \mid h+1$, cioè $h \equiv -1 \pmod{p}$. Pertanto

$$a^{\frac{p-1}{2}} \equiv \left(g^i\right)^{\frac{p-1}{2}} = h^i \equiv (-1)^i \pmod{p} \tag{2}$$

Stanti le uguaglianze (1) e (2), la tesi segue una volta provato che

$$\left(\frac{g^i}{p}\right) \equiv (-1)^i \pmod{p} \tag{3}$$

Poiché $p \nmid g$, ciò equivale ad affermare che g^i è un residuo quadratico modulo p se e solo se i è pari. Se i è pari, la congruenza $x^2 \equiv g^i \pmod{p}$ ha soluzione $x = g^{\frac{i}{2}}$. Viceversa, se tale congruenza ha una soluzione x, possiamo supporre che sia $x = g^j$ per qualche numero naturale j. Allora $g^{2j} \equiv g^i \pmod{p}$, che implica $p-1 \mid 2j-i$. Essendo $p-1$ pari, se ne deriva che i è pari. Ciò prova (3) e conclude la dimostrazione. □

Esercizio 27.6 Determiniamo, in base alla Proposizione 27.5,

a) $\left(\frac{3}{29}\right) \equiv 3^{14} = (3^3)^4 3^2 \equiv (-2)^4 9 = 16 \cdot 9 = 144 = 5 \cdot 29 - 1 \equiv -1 \pmod{29}$. Quindi si ha che $\left(\frac{3}{29}\right) = -1$, e 3 non è residuo quadratico modulo 29.

b) $\left(\frac{5}{29}\right) \equiv 5^{14} = (5^2)^7 \equiv (-4)^7 = (-64)^2(-4) \equiv 6^2(-4) \equiv -28 \equiv 1 \pmod{29}$. Pertanto si ha che $\left(\frac{5}{29}\right) = 1$. Quindi 5 è residuo quadratico modulo 29. Una soluzione della congruenza $x^2 \equiv 5$ è $x = 11$. (Infatti $11^2 - 5 = 4 \cdot 29$).

Dalla Proposizione 27.5 si deduce immediatamente che il simbolo di Legendre gode della proprietà moltiplicativa:

Corollario 27.7 Se p è un numero primo dispari, per ogni $a, b \in \mathbf{Z}$ si ha

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

Questa proprietà è particolarmente utile quando i numeri a e p sono troppo grandi per poter applicare direttamente la Proposizione 27.5.

Esempio 27.8

a) $\left(\frac{13}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{-13}{17}\right) = \left(\frac{16}{17}\right)\left(\frac{4}{17}\right) = 1$. Nella prima uguaglianza abbiamo utilizzato il Corollario 27.7, nella seconda l'Osservazione 27.4, nell'ultima il fatto che 16 e 4 sono quadrati, e quindi certamente residui quadratici modulo qualunque numero primo.

b) $\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1$. Qui si giunge immediatamente alla conclusione applicando l'Osservazione 27.4. Tieniamo comunque presente questo risultato: come vedremo, non è un caso se invertendo i ruoli di 13 e 17 il simbolo di Legendre resta invariato.

Esempio 27.9 Sia p un primo dispari. Allora, in virtù della Proposizione 27.5, si ha

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

quindi

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

In base alla Proposizione 22.8, segue che il numero intero p è primo in $\mathbf{Z}[i]$ se e solo se $p \equiv 3 \pmod 4$. In particolare, 5 non è primo in $\mathbf{Z}[i]$. D'altronde, esso ammette la decomposizione $5 = (1+2i)(1-2i)$. Ricordiamo, inoltre, che 2 non è primo, in quanto $2 = (1+i)(1-i)$. Ecco un modo alternativo di svolgere l'Esercizio 22.9.

La classificazione di $\left(\frac{-1}{p}\right)$ che abbiamo appena effettuato ammette anche un'altra interessante applicazione:

Corollario 27.10 Esistono infiniti numeri primi congrui a 1 modulo 4.

Dimostrazione: Supponiamo per assurdo che i numeri primi congrui a 1 modulo 4 siano in numero finito, siano essi $p_1, \ldots, p_k$. Sia $m = (2p_1 \cdots p_k)^2 + 1$. Allora m è dispari, quindi possiede un divisore primo dispari p. Segue che $(2p_1 \cdots p_k)^2 \equiv -1 \pmod p$ (*). Quindi $\left(\frac{-1}{p}\right) = 1$, cioè, in

base all'Esempio 27.9, si ha che $p \equiv 1 \pmod 4$. Ma allora $p = p_i$ per qualche i, e ciò contraddice (*). □

Nota storica La dimostrazione del Corollario 27.10 riproduce, nei tratti essenziali, quella data da Euclide (IV sec. a. C.) per l'infinità dei numeri primi (vedi *Gli Elementi,* Libro IX, Proposizione 20). L'enunciato del corollario è, per contro, un caso particolare del teorema di P.G. Lejeune-Dirichlet (1805-1859) secondo cui ogni progressione aritmetica in cui il termine iniziale e la ragione sono coprimi contiene infiniti numeri primi.

Il prossimo lemma è un risultato preliminare al principale teorema di questa lezione: entrambi sono dovuti a Carl Friedrich Gauss (1777-1855), che ha dedicato alle congruenze quadratiche gran parte della sua opera *Disquisitiones Arithmeticae.*

Introduciamo la seguente notazione: per ogni primo dispari p indicheremo

$$P = \left\{ [1]_p, \ldots, \left[\frac{p-1}{2} \right]_p \right\}, \quad Q = \left\{ -[1]_p, \ldots, -\left[\frac{p-1}{2} \right]_p \right\}$$

è chiaro che $\mathbf{Z}_p^*$ è l'unione disgiunta di P e Q, che hanno entrambi $\frac{p-1}{2}$ elementi.

Lemma 27.11 (*Lemma di Gauss*) Per ogni primo dispari p ed ogni intero a non multiplo di p si ha

$$\left(\frac{a}{p} \right) = (-1)^{|aP \cap Q|}.$$

Dimostrazione: Siano $x, y \in P$ distinti. Allora si ha che $x \neq -y$, perché $-y \in Q$. Poiché p non divide a segue che ($ax \neq ay$ e) $ax \neq -ay$. Quindi aP ha esattamente $\frac{p-1}{2}$ elementi e nessuno dei seguenti $\frac{p-1}{2}$ insiemi contiene due elementi di aP:

$$\{[1]_p, -[1]_p\}, \ldots, \left\{ \left[\frac{p-1}{2} \right]_p, -\left[\frac{p-1}{2} \right]_p \right\}.$$

Pertanto ognuno di questi insiemi contiene esattamente un elemento di aP, per cui

$$aP = \left\{ e_i [i]_p \,\middle|\, e_i = 1 \text{ oppure } e_i = -1, 1 \leq i \leq \frac{p-1}{2} \right\}.$$

Il prodotto di tutti gli elementi di aP è uguale a

$$[a]_p^{\frac{p-1}{2}} \left[\frac{p-1}{2}! \right]_p,$$

ma è anche uguale a

$$\prod_{i=1}^{\frac{p-1}{2}} e_i \left[\frac{p-1}{2}! \right]_p = (-1)^{|aP \cap Q|} \left[\frac{p-1}{2}! \right]_p .$$

Dunque, essendo $\left[\frac{p-1}{2}! \right]_p$ non nullo, segue che

$$a^{\frac{p-1}{2}} \equiv (-1)^{|aP \cap Q|} \pmod{p}.$$

La tesi segue allora dalla Proposizione 27.5. □

Siamo ora in grado di dimostrare il seguente

Teorema 27.12 (*Legge di reciprocità quadratica*) Siano *p*,*q* numeri primi dispari distinti. Allora

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

Nota L'enunciato, posto in questa forma, evidenzia che il simbolo di Legendre relativo a due numeri primi dispari distinti, in quasi tutti i casi, non cambia se si invertono i due numeri. Esiste un'altra formulazione più ermetica, ma più semplice, in cui l'enunciato è compattato in una formula:

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

Si noti che l'esponente è dispari se e solo se $\frac{p-1}{2}, \frac{q-1}{2}$ sono entrambi dispari, ossia $p \equiv q \equiv 3 \pmod 4$.

Dimostrazione: Per il Lemma 27.11, posto $\mu = |qP \cap Q|$, si ha

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

Determiniamo il valore di μ. Questo numero conta i numeri del tipo *qx,* con $1 \le x \le \frac{p-1}{2}$ che differiscono per un multiplo di *p* (cioè un numero *py*) da uno dei numeri $-\frac{p-1}{2}, \ldots, -1$, ossia sono tali che, per qualche intero *y*,

$$-\frac{p}{2} < qx - py < 0.$$

Chiaramente, per ogni valore di x esiste al più un valore di y siffatto, e per ognuno di questi y si ha

$$0 < \frac{qx}{p} < y < \frac{qx}{p} + \frac{1}{2} \le \frac{q(p-1)}{2p} + \frac{1}{2} < \frac{q+1}{2},$$

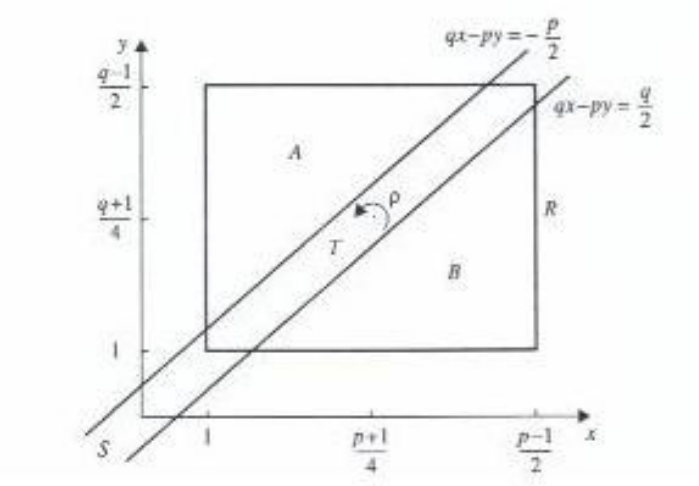
per cui

$$1 \le y \le \frac{q-1}{2}.$$

Quindi $\mu = \left| \left\{ (x,y) \middle| 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}, -\frac{p}{2} < qx - py < 0 \right\} \right|$. Analogamente, $\left(\frac{p}{q}\right) = (-1)^{\nu}$, ove $\nu = \left| \left\{ (x,y) \middle| 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}, 0 < qx - py < \frac{q}{2} \right\} \right|$, per cui

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu+\nu}. \tag{5}$$

Qui $\mu + \nu$ è il numero dei punti a coordinate intere del piano cartesiano che appartengono al rettangolo raffigurato e sono tali che $-\frac{p}{2} < qx - py < 0$ oppure $0 < qx - py < \frac{q}{2}$, ossia, equivalentemente, $-\frac{p}{2} < qx - py < \frac{q}{2}$: essendo p,q coprimi, $qx - py$ non è infatti mai nullo. Quindi i punti cercati sono i punti a coordinate intere compresi nella striscia e nel rettangolo raffigurati:



Il numero dei punti a coordinate intere compresi nel rettangolo è $\frac{(p-1)(q-1)}{4}$. Detto α il numero dei punti a coordinate intere compresi nel triangolo A, e β il numero di quelli compresi nel triangolo B, si ha quindi

$$\mu + \nu = \frac{(p-1)(q-1)}{4} - (\alpha + \beta).$$

Alla luce della (5), per concludere la dimostrazione basta provare che $\alpha + \beta$ è pari. Ma ciò è vero, perché, data la simmetria della figura, $\alpha = \beta$. □

Osservazione 27.13 Nell'Esempio 27.8, il risultato in a) si può dunque dedurre immediatamente da quello in b), che era stato ricavato banalmente.
È chiaro che Il Teorema 27.12 è particolarmente indicato quando uno dei due primi è piccolo, e l'altro è grande.

Esempio 27.14 La congruenza $x^2 \equiv 5 \pmod{1499}$ ha soluzione se e solo ha soluzione la congruenza $x^2 \equiv 1499 \pmod{5}$. Questa equivale alla congruenza $x^2 \equiv 4 \pmod{5}$, che ha soluzione (ad esempio, $x = 2$). Quindi anche la prima congruenza ha soluzione: la più piccola (tra quelle positive) è $x = 417$.