Congruenze quadratiche

Definizione di residuo quadratico

Sia p un primo dispari e sia a un intero tale che $(a,p)=1$. Se la congruenza

$$1)\quad x^2 \equiv a \pmod{p}$$

ha soluzione si dice che a è un residuo quadratico modulo p, se non ha soluzione si dice che a è un non residuo.

Esempio

Sia $p=11$ e sia $a=5$: ci domandiamo se la congruenza

$$2)\quad x^2 \equiv \bar{5} \pmod{11}$$

ha soluzione. Procediamo per tentativi e calcoliamo i quadrati di $x=1,2,3,\dots,10$, ridu cendo mod 11. Si ha (le congruenze sono mod 11)

$$\begin{array}{|c|c|c|c|c|} 1^2\equiv 1\equiv 1 & 2^2=4\equiv 4 & 3^2=9\equiv 9 & 4^2=16\equiv 5 & 5^2=25\equiv 3 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 10^2=100\equiv 1 & 9^2\equiv 81\equiv 4 & 8^2=64\equiv 9 & 7^2=49\equiv 5 & 6^2=36\equiv 3 \end{array}$$

Dalla tabella precedente vediamo che la congruenza 2) ha due soluzioni, incongrue mod 11, precisamente $x\equiv 4 \pmod{11}$ e $x\equiv 7 \pmod{11}$.

Ne concludiamo che 5 è residuo quadratico mod 11, e la congruenza 2) ha due soluzioni.

Dalla tabella si vede anche che i residui quadratici mod 11 sono

1, 3, 4, 5, 9 (residui quadratici mod 11)

e gli altri elementi del sistema ridotto di resti, cioè

2, 6, 7, 8, 10 (non residui quadratici mod 11)

sono non residui.

I residui quadratici mod 11 sono in numero di $5 = \frac{11-1}{2}$, e lo stesso i non residui.

Il precedente esempio illustra un fatto generale, come dimostra il seguente

Teorema 1

Sia p un primo dispari: allora ogni sistema ridotto di resti modulo p contiene esattamente $\frac{p-1}{2}$ residui quadratici ed esattamente $\frac{p-1}{2}$ non residui quadratici modulo p. I residui quadratici sono congrui mod p ai numeri

3) $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$

Inoltre la congruenza quadratica

$$x^2 \equiv a \pmod{p}$$

ha esattamente due soluzioni (incongrue mod p) se a è residuo quadratico, nessuna soluzione se a è un non residuo mod p.

Dimostrazione

Come prima cosa dimostriamo che i numeri $1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$, sono incongrui mod p. Supponiamo infatti che $x^2 \equiv y^2 \pmod p$, con $1 \le x, y \le \frac{p-1}{2}$. Si ha $x^2 - y^2 = (x-y)(x+y) \equiv 0 \pmod p$ e quindi $p \mid (x-y)$, oppure $p \mid (x+y)$. La seconda eventualità si scarta, infatti $2 \le x+y \le \frac{p-1}{2} + \frac{p-1}{2} = p-1$ e quindi $p \nmid (x+y)$. Non resta che ammettere che $p \mid (x-y)$ che implica $x = y$ (infatti $|x-y| < \frac{p-1}{2}$). Ciò prova che i numeri in 3) sono incongrui mod p. Inoltre se $r = 1, 2, 3, \dots, \frac{p-1}{2}$ da $(p-r)^2 = p^2 + r^2 - 2pr \equiv r^2 \pmod p$ segue

$$1^2 \equiv (p-1)^2 \pmod p$$
$$2^2 \equiv (p-2)^2 \pmod p$$
$$3^2 \equiv (p-3)^2 \pmod p$$

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

e quindi, nel sistema ridotto di resti

$$x = \underbrace{1, 2, 3 \dots, \frac{p-1}{2}}, \underbrace{\left(p - \frac{p-1}{2}\right), \dots, (p-1)}$$

facendo il prodotto dei numeri x con $\frac{p-1}{2} < x \le p-1$ non si ottiene nulla di nuovo.

Per quanto riguarda la congruenza

$$x^2 \equiv a \pmod{p^k}$$

se a è residuo quadratico, cioè se $a \equiv r^2 \pmod p$ per un valore r con $1 \le r \le \frac{p-1}{2}$, ci sono primi due soluzioni, precisamente $x = r$ e $x = p - r$.
Se, viceversa, a è non residuo, la congruenza non ha nessuna soluzione. Ciò prova completamente il teo$_2$ rema 1.

Osservazione 1

Le precedenti questioni si possono affrontare anche ricordando che, se p è un primo dispari, esistono radici primitive mod p. Infatti, se g è una radice primitiva mod p, la congruenza

$$4) \quad x^2 \equiv a \pmod p$$

è privale, posto $x \equiv g^{r(x)} \pmod p$ e $a \equiv g^{r(a)} \pmod p$, a

$$5) \quad x^2 \equiv (g^{r(x)})^2 \equiv g^{r(a)} \pmod p$$

che a sua volta equivale alla congruenza li$_2$ neare

$$6) \quad 2r(x) \equiv r(a) \pmod{(p-1)}$$

Dato che la 6) ha soluzione se e solo se $(2, p-1) = 2 \mid r(a)$, possiamo dire (che) la 4) ha soluzio$_2$ ne se e solo se a è una potenza pari di g, cioè $a \equiv g^{2k} \pmod p$ e non ha nessuna so$_2$

luzione se a è una potenza dispari di g.
Ne segue che i residui quadratici sono congrui alle potenze pari di g

$$g^2, g^4, \ldots .$$

e i non residui alle potenze dispari

$$g^1, g^3, \ldots .$$

Dato che i numeri $g^r \pmod p$, con l'esponente $r = 1, 2, \ldots, p-1$ rappresentano l'intero sistema ridotto di resti mod p, ci sono evidentemente $\frac{p-1}{2}$ valori pari di r (cui corrispondono i residui quadratici) e $\frac{p-1}{2}$ valori dispari, cui corrispondono i non residui. Inoltre la congruenza lineare 6), se ha soluzione, ne ha due incongrue mod $(p-1)$, cui corrispondono le due soluzioni di 4). Ritroviamo quindi tutti i risultati precedenti.

Due problemi importanti

Consideriamo i due problemi seguenti:

i) data la congruenza $x^2 \equiv a \pmod p$, c'è un modo "veloce" per sapere se ha soluzione? (cioè se a è un residuo o un non residuo quadratico?)

ii) una volta chiarito che a è un residuo quadratico mod p, c'è un modo "veloce" per calcolare le soluzioni di $x^2 \equiv a \pmod p$?

Vedremo ora come si può rispondere ai due quesiti.

Rispondiamo al primo quesito i).

Il criterio di Eulero

Dato un primo p dispari ed un valore a, con $(a,p)=1$, si ha quanto segue:

- a è residuo quadratico mod p, se e solo se

$$7) \quad a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

- a è non residuo quadratico mod p se e solo se

$$8) \quad a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Dimostrazione

Supponiamo che a sia un residuo quadratico: allora, indicando con g una radice primitiva mod p, si ha $a \equiv g^{2k} \pmod p$, da cui segue

$$9) \quad a^{(p-1)/2} \equiv (g^{2k})^{(p-1)/2} \equiv (g^{p-1})^k \equiv 1^k \equiv 1 \pmod p.$$

Supponiamo ora che a sia un non residuo quadratico mod p : si ha allora $a \equiv g^{2k+1} \pmod p$, da cui segue

$$10)\quad a^{(p-1)/2} \equiv \left(g^{2k+1}\right)^{(p-1)/2} \equiv \left(g^{(p-1)/2}\right)^{2k+1} \equiv$$
$$\equiv (-1)^{2k+1} \equiv -1 \pmod p$$

Viceversa, se vale la 7), a è certamente un residuo quadratico mod p : infatti se fosse un non residuo dovrebbe valere la 8). Alla stessa maniera, se vale la 8) a è certamente un non residuo quadratico mod p, infatti se fosse un residuo dovrebbe valere la 7).

Ciò prova completamente il criterio di Eulero.

Osservazione 2

Per dimostrare la 10) abbiamo usato il fatto che, se g è radice primitiva, si ha

$$11)\quad g^{(p-1)/2} \equiv -1 \pmod p$$

La 11) è certamente vera, poiché, si ha

$$12)\quad g^{(p-1)} - 1 = \left(g^{(p-1)/2} - 1\right)\left(g^{(p-1)/2} + 1\right) \equiv 0 \pmod p$$

per il piccolo teorema di Fermat, e quindi

$p \mid (g^{(p-1)/2} - 1)$ oppure $p \mid (g^{(p-1)/2} + 1)$. La prima eventualità non può essere vera, perché equivale a dire

$$13) \quad g^{(p-1)/2} \equiv 1 \pmod{p}$$

e quindi g non sarebbe radice primitiva. Vale quindi la seconda eventualità, cioè la 11).

Notiamo che il criterio di Eulero risponde positivamente al primo quesito i) di pag 5).

Infatti per sapere se la congruenza

$$14) \quad x^2 \equiv a \pmod{p}$$

ha soluzione o no basta calcolare $(a^{(p-1)/2} \bmod p)$.

La risposta al secondo quesito, cioè ii), è un po' più articolata. Si può infatti dimostrare che se a è un residuo quadratico mod p, con $p \equiv 3$ (modulo 4), allora la congruenza 14) ha come soluzione

$$15) \quad x \equiv a^{(p+1)/4} \pmod{p} \quad \left(\begin{array}{l}\text{ovviamente}\\ \text{anche } -x \pmod p\\ \text{è soluzione}\end{array}\right)$$

Infatti da 15) segue

$$16) \quad x^2 \equiv \left(a^{(p+1)/4}\right)^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} \cdot a \equiv a \pmod{p}$$

poiché, essendo a, per ipotesi, un residuo quadratico mod p, si ha

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

per il criterio di Eulero.

Nel caso in cui sia $p \equiv 1 \pmod 4$, non c'è un metodo così veloce per calcolare le soluzioni della 14) (c'è un procedimento un pò più lento).

In questa maniera abbiamo risposto ai due quesiti i) ed ii) delle pagg. 5) e 6).

L'estrazione della radice quadrata mod n (dove $n = pq$, con p e q primi dispari)

Sia $n = pq$, con p e q primi dispari.

La congruenza (con $(a,n)=1$) equivale a

$$17) \quad x^2 \equiv a \pmod n \iff \begin{cases} x^2 \equiv a \pmod p \\ x^2 \equiv a \pmod q \end{cases}$$

Se a è residuo quadratico sia mod p che mod q la congruenza $x^2 \equiv a \pmod p$ ha due radici (diciamo x_1 ed x_2) e la congruenza $x^2 \equiv a \pmod q$

ha altre due radici (diciamo y_1 ed y_2). Quindi, ricordando l'equivalenza 1), la congruenza

18) $x^2 \equiv a \pmod{n}$

ha quattro soluzioni (incongrue mod n) che si calcolano mediante il teorema cinese del resto, cioè risolvendo i sistemi

19) $\begin{cases} x \equiv x_i \pmod{p}, & i = 1,2 \\ x \equiv y_j \pmod{q}, & j = 1,2 \end{cases}$

Per quanto precedentemente dimostrato, il calcolo di $x_1, x_2 \pmod{p}$ e $y_1, y_2 \pmod{q}$ è particolarmente semplice e veloce se $p \equiv 3 \pmod 4$ ed anche $q \equiv 3 \pmod 4$.

Questo fatto è stato sfruttato per creare un importante crittosistema, il crittosistema di Rabin, che verrà esposto nelle pagine seguenti.

Crittosistema di Rabin

A. si vuol dotare di un crittosistema di Rabin e procede nel modo seguente,

- sceglie due primi p, q entrambi $\equiv 3 \pmod 4$ (questo per comodità di decifratura)
- rende noto il loro prodotto $n = pq$, mantenendo segreti p e q (il numero n è la chiave pubblica, i due primi sono la chiave privata).

Chi vuol mandare un messaggio M (con $1 < M < n$) ad A. lo cifra calcolando

$$20) \quad C \equiv M^2 \pmod n$$

A. riceve il cifrato C e lo decifra estraendo le quattro radici quadrate di $C \pmod n$, nel modo seguente

- A. calcola a e b tali che

$$21) \quad ap + bq = 1 \quad \text{(identità di Bézout)}$$

(cioè A. calcola $(p,q) = 1$ mediante l'algoritmo euclideo e poi ne ricava le 5), identità di Bezout).

Calcolo poi

22) $C^{\frac{p+1}{4}} \equiv r \pmod p$, $C^{\frac{q+1}{4}} \equiv s \pmod q$

Ne segue che, ponendo

23) $x \equiv aps + bqr \pmod n$

24) $y = aps - bqr \pmod n$

le quattro radici quadrate di $C \bmod n$, saranno $\pm x$ e $\pm y$. Una di queste è il messaggio M.

—

Esercizio

Dimostrate che le formule 23) e 24) si ottengono seguendo il procedimento indicato a pag 10), per il calcolo delle quattro radici quadrate di $C \pmod n$.

Bob è titolare del cifrosistema di Rabin (1)

con $n = 77$ chiave pubblica

$p = 11$, $q = 7$ chiave privata

Chiunque può cifrare per Bob un messaggio M con $1 < M < 77$ calcolando

(1) $C = M^2 \pmod n$

Bob decifra calcolando

$$(p \equiv 3 \,(4),\ q \equiv 3 \,(4))$$

(2) $x \equiv aps + bqr \pmod n$

$y \equiv aps - bqr \pmod n$

dove $ap + bq = 1$, $r \equiv C^{(p+1)/4} \pmod p$

$s \equiv C^{(p+1)/4} \pmod q$

A questo punto le quattro radici quadrate di $C \bmod n$ sono $\pm x$ e $\pm y$.

Bob precalcola ap e bq con l'algoritmo euclideo (cioè calcola $(p, q) = 1$ e lo esprime come combinazione lineare di p e q (identità di Bézout).

Nel nostro caso si ha:

$11 = 7 \cdot 1 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

$3 = 1 \cdot 3 + 0$

$\Rightarrow \quad 1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 =$

$= 2(11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7$

e quindi, per noi,

$a = 2$ e $b = -3$ $\quad (ap+bq=1 \;,\; 2\cdot 11 - 3\cdot 7 = 1)$

Perciò le ② diventano

$$③ \begin{cases} x \equiv 2\cdot 11\cdot s + (-3)(7)r \pmod{77} \\ y = 2\cdot 11\cdot s - (-3)(7)r \pmod{77} \end{cases}$$

cioè

$$④ \begin{cases} x = 22\cdot s - 21\cdot r \pmod{77} \\ y = 22\cdot s + 21 r \pmod{77} \end{cases}$$

I due numeri r ed s non possono essere pre calcolati, in quanto dipendono dal cifrato, precisamente

$$\begin{cases} r \equiv C^{\frac{p+1}{4}} \pmod{p} \\ s = C^{\frac{p+1}{4}} \pmod{q} \end{cases}$$

Alice manda a Bob il cifrato C del messaggio $M = 25$, cioè $C \equiv (25)^2 \pmod{77}$

per noi se $C \equiv M^2 \equiv (25)^2 \equiv 625 \equiv 9 \pmod{77}$

si ha

$$r \equiv 9^{\frac{11+1}{4}} \equiv 9^3 \pmod{11} \quad \text{e} \quad s \equiv 9^{\frac{7+1}{4}} \equiv 9^2 \pmod{7}$$

Ma

$9 \equiv -2 \pmod{11}$ quindi $9^3 \equiv (-2)^3 \equiv -8 \equiv 3 \pmod{11}$

$9 \equiv -2 \pmod{7}$ e quindi $9^2 \equiv 4 \pmod{7}$

Perciò otteniamo

$$\boxed{r = 3} \quad \text{e} \quad \boxed{s = 4}$$

Quindi la 4) diviene

$$x \equiv 22 \cdot 4 - 21 \cdot 3 \equiv 88 - 63 \equiv 25 \pmod{77}$$

$$y = 22 \cdot 4 + 21 \cdot 3 = 88 + 63 \equiv 11 + 63 \equiv 74 \pmod{77}$$

Le quattro radici quadrate di 9 mod 77 sono quindi

$$\pm 25, \pm 74 \pmod{77}$$

cioè, siccome $-25 + 77 = 52$ e $-74 + 77 = 3$,

(5) $3, 25, 52, 74$

Una di queste è il messaggio, precisamente è

$M = 25$.

Se supponiamo di avere un ipotetico algoritmo che estrae le radici quadrate mod n, si può fattorizzare n. Infatti se

x_1, x_2, x_3, x_4 con $x_i^2 \equiv c \pmod{n}$ per $i = 1, 2, 3, 4$ sono le quattro radici quadrate (dic) mod n, con

$$1 \leq x_1 < x_2 < n - x_2 < n - x_1 < n$$

(x_3 sotto $n - x_2$, x_4 sotto $n - x_1$)

scegliendone due si ottiene $x_i^2 \equiv c \equiv x_j^2 \pmod{n}$

da cui segue $x_i^2 - x_j^2 \equiv (x_i - x_j)(x_i + x_j) \equiv 0 \pmod{n}$

Se si scelgono x_i ed x_j tali che $x_i + x_j = n$

dall'ultima congruenza non si ottiene nulla (infatti è ovviamente verificata), mentre se si sceglie una coppia con $x_i + x_j \neq n$, dalla congruenza $(x_i - x_j)(x_i + x_j) \equiv 0 \pmod n$ segue che uno dei due fattori è multiplo di p e l'altro di q (infatti $x_i + x_j < 2n$, $x_i + x_j \not\equiv 0 \pmod n$), dunque calcolando $(x_i - x_j, n)$ oppure $(x_i + x_j, n)$ si fattorizza.

Esempio con $n = 77$

Come abbiamo visto i numeri

3, 25, 52, 74 sono le quattro radici quadrate di $c = 9 \pmod{77}$. Se scegliamo 3 e 74, oppure 25 e 52 non otteniamo nulla: vediamo gli altri casi:

- 25, 74 ci dà $(74-25)(74+25) = (49)(99) \equiv 0 \pmod{77}$ e $(49, 77) = 7$, $(99, 77) = 11$
- 3, 25 ci dà $(25-3)(25+3) \equiv (22)\cdot(28) \equiv 0 \pmod{77}$ e $(22, 77) = 11$, $(28, 77) = 7$.
- 3, 52 ci dà $(52-3)(52+3) = (49)\cdot(55) \equiv 0 \pmod{77}$ e $(49, 77) = 7$ e $(55, 77) = 11$.
- 52, 74 ci dà $(74-52)(74+52) = (22)(126) \equiv 0 \pmod{77}$ e $(22, 77) = 11$, $(126, 77) = 7$

Dunque, se l'ipotetico algoritmo che calcola le radici quadrate di $c \bmod n$ è veloce ("polynomial-time"), anche fattorizzare n è veloce (p.t.)
Infatti basta applicare alle somme (Calle di Hermite) di due prodotti (scelte bene) l'alg. euclideo e rifattorizzare n. (Esempio di riduzione di Turing, "Turing reduction").

- Osserviamo che

$$x \equiv apS + bqr \equiv bqr \equiv r \pmod{p}$$

(infatti $bq \equiv 1 \pmod{p}$ perché $ap + bq = 1$)

e $r^2 \equiv c \pmod{p}$

$$x \equiv apS + bqr \equiv ap S \equiv S \pmod{q}$$

(infatti $ap \equiv 1 \pmod{q}$ perché $ap + bq = 1$)

e $S^2 \equiv c \pmod{q}$

Quindi $\begin{cases} x \equiv r \pmod{p} \\ x \equiv S \pmod{q} \end{cases}$