Corso di Crittografia A.A. 2017-2018

Note sui residui quadratici

Leonardo Tamiano

July 5, 2018

Contents

1 Introduzione ai residui quadratici

All'inizio del corso abbiamo discusso la soluzione di congruenze *lineari*, ovvero congruenze della forma

$$ax + b \equiv \mod n$$

in cui a, b e n erano i dati in input e x era l'incognita da trovare.

Naturalmente ci possiamo porre lo stesso problema per congruenze il cui grado è maggiore di 1, ovvero per congruenze non lineari. Le congruenze non lineari più semplici sono quelle di grado 2, ovvero congruenze della forma

$$\alpha x^2 + \beta x + \gamma \equiv 0 \mod n$$

in cui α, β, γ e n sono i dati e x è l'incognita da trovare. Lo scopo di questa dispensa sarà dunque analizzare questo problema introducendo tutta una serie di concetti e risultati molto utili. Il risultato finale sarà la descrizione di un algoritmo in grado di risolvere queste equazioni all'interno in campi finiti (dunque in $\mathbb{Z}_p$ con p primo oppure nel campo finito più generale $\mathbb{F}_{p^f}$).

Come prima cosa supponiamo che il modulo con cui lavoriamo è sempre un primo p. Questo segue da tutta una serie di risultati che non riportiamo per brevità. Inoltre è possibile argomentare, cosa che non faremmo in questa sede, che la risoluzione di equazioni congruenziali di secondo grado generali può essere ridotta alla soluzione di particolari congruenze quadratiche, ovvero quelle aventi la seguente forma

$$x^2 \equiv a \mod p$$

dove a è un intero e p è un numero primo. Il nostro compito sarà dunque analizzare quest'ultimo tipo di congruenze quadratiche.

1.1 Definizione di residuo quadratico

Quando abbiamo congruenze del tipo $x^2 \equiv a \mod p$ siamo naturalmente interessati a caratterizare gli interi a per cui tale congruenza è risolubile. Riportiamo dunque la seguente definizione

Definizione 1.1. Sia p un primo. Diciamo che $a \in \mathbb{Z}$ è un *residuo quadratico modulo* p se esiste un $x \in \mathbb{Z}_p$ tale che

$$x^2 \equiv a \mod p$$

Quindi a è un residuo quadratico modulo p quando la congruenza $x^2 \equiv a \mod p$ ammette almeno una soluzione.

Molte volte si scriverà a è un $R.Q.$ modulo p per dire che a è un residuo quadratico modulo p.

1.2 Residui quadratici in $\mathbb{Z}_p$, con p primo

Ricordiamo che, essendo p primo, si ha che $\mathbb{Z}_p$ è un campo. In realtà, dato che $\mathbb{Z}_p$ è finito si ha che $\mathbb{Z}_p$ è un campo finito. Da questo segue che se $f(x)$ è un polinomio a coefficienti in $\mathbb{Z}_p$, ovvero se $f(x) \in \mathbb{Z}_p[X]$, allora il grado di $f(x)$ limita il numero di radici del polinomio. In particolare se $f(x) \in \mathbb{Z}_p[X]$ ha grado n, allora $f(x)$ può avere *al massimo* n radici distinte.

Ma allora, nel nostro caso particolare, fissata una congruenza del tipo

$$x^2 \equiv a \mod p$$

tale congruenza definisce il polinomio $f(x) = x^2 - a \in \mathbb{Z}_p[X]$ e, dal paragrafo precedente, segue che tale polinomio può avere al massimo 2 radici distinte. Questo vuol dire che possono esistere al massimo due distinti x che siano soluzioni della nostra congruenza quadratica, sempre supponendo che il modulo utilizzato sia un primo p.

Notiamo infine che, posta x soluzione di $x^2 \equiv a \mod p$, abbiamo che anche $-x$ è soluzione di $x^2 \equiv a \mod p$. Infatti,

$$(-x)^2 \equiv_p x^2 \equiv_p a$$

Ricapitolando, abbiamo la seguente situazione: Lavorando in $\mathbb{Z}_p$ l'equazione $x^2 \equiv a \mod p$ può avere o zero soluzioni oppure due soluzioni, e se ne ha due, allora le due soluzioni sono l'uno l'opposto dell'altro (sempre in $\mathbb{Z}_p$).

Ma allora i residui quadratici modulo p sono esattamente i seguenti elementi

$$0^2, 1^2, 2^2, ..., ((p-1)/2)^2$$

Notiamo infatti che, presi due elementi distinti $a, b \in \{0, 1, ..., (p-1)/2\}$, si ha che tali elementi definiscono residui quadratici diversi. Infatti, se non fosse così, ovvero se per assurdo $a^2 \equiv b^2 \mod p$, allora, dato che sono distinti, devono necessariamente essere l'uno l'opposto dell'altro. Ma questo è un assurdo in quanto sia l'inverso di a che l'inverso di b si trovano in $\{(p+1)/2, ..., p-1\}$

$$-1 \equiv_p p-1, \quad -2 \equiv_p p-2, \quad , ..., \quad -(p-1)/2 \equiv_p (p+1)/2$$

Concludendo, abbiamo visto che in $\mathbb{Z}_p$ ci sono esattamente $(p+1)/2$ residui quadratici, che escludendo lo 0 sono proprio la metà degli elementi di $\mathbb{Z}_p$. Questa semplice osservazione potrebbe essere già utilizzata per sviluppare un algoritmo che risolve equazioni del tipo $x^2 \equiv a \mod p$: prima ci si calcola tutti i residui quadratici $\{0^2, 1^2, ..., ((p-1)/2)^2\}$ e, se becchiamo a, abbiamo la nostra soluzione. Notiamo però che il costo di tale algoritmo è $O(p)$, e dunque risulta essere un algoritmo *esponenziale* rispetto alla lunghezza dell'input. L'algoritmo presentato alla fine risulta essere leggermente più complesso di questo, ma almeno riesce ad ottenere una complessità *polinomiale*.

1.2.1 Esempio: Residui quadratici in $\mathbb{Z}_p$

Andiamo adesso a vedere chi sono i residui quadrtici in $\mathbb{Z}_p$, per $p \in \{2, 3, 5, 7\}$

- In $\mathbb{Z}_2 = \{0, 1\}$ i *R.Q.* sono,

$$0^2 = 0, \quad 1^2 = 1$$

- In $\mathbb{Z}_3 = \{0, 1, 2\}$ i *R.Q.* sono,

$$0^2 = 0, \quad 1^2 = 1$$

- In $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ i *R.Q.* sono,

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4$$

- In $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ i *R.Q.* sono,

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 2$$

1.3 Se $\langle g \rangle = \mathbb{Z}_p$, allora g^j è R.Q. $\iff$ j è pari

- ($\Leftarrow$). Se j è pari allora $j = 2h$, con $h \in \mathbb{Z}$. Ma allora $g^j = g^{2h} = (g^h)^2$ in $\mathbb{Z}_p$, e quindi g^j è un *R.Q.* in $\mathbb{Z}_p$.

- ($\Rightarrow$). Viceversa, supponiamo che g^j è un *R.Q.*, ovvero supponiamo che esiste un $x \in \mathbb{Z}_p$ tale che $x^2 \equiv g^j \mod p$. Notiamo che g genera $\mathbb{Z}_p$ e quindi deve anche generare x, ovvero esiste un $h \in \mathbb{N}$ tale che $g^h = x$. Ma allora abbiamo che

$$x^2 \equiv_p (g^h)^2 \equiv_p g^j \iff g^{2h-j} \equiv_p 0$$

ma questo succede se e solo se (risultato basilare della teoria dei gruppi)

$$2h - j \equiv 0 \mod p - 1$$

Ora, notiamo che $p - 1$ è pari, dunque contiene un fattore 2. Per avere che $2h - j$ sia un multiplo di $p - 1$, dobbiamo necessariamente avere che anche $2h - j$ contenga un fattore 2, ovvero che anche $2h - j$ sia pari. Ma questo è vero solo se j è pari.

2 Simbolo di Legendre

Il simbolo di Legendre è uno strumento importante utilizzato per analizzare il numero di soluzioni di una congruenza quadratica della forma

$$x^2 \equiv a \mod p$$

con $a, p \in \mathbb{Z}$ e p primo.

2.1 Definizione di simbolo di Legendre

Sia $p \in \mathbb{Z}$ un numero primo e sia $a \in \mathbb{Z}$. Definiamo il *simbolo di Legendre*, denotato da $\left(\frac{a}{p}\right)$, nel seguente modo,

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & p \mid a \\ 1 & a \text{ è un } R.Q. \text{ modulo } p \\ -1 & a \text{ non è un } R.Q. \text{ modulo } p \end{cases}$$

Per fare qualche esempio abbiamo che

$$\left(\frac{2}{7}\right) = 1, \quad \left(\frac{3}{7}\right) = -1, \quad \left(\frac{14}{7}\right) = 0,$$

2.2 Come calcolare $\left(\frac{a}{p}\right)$

Riportiamo a seguire la prima proposizione che ci aiuterà nel calcolo del simbolo di Legendre.

Proposizione 2.1. Sia p primo e sia $a \in \mathbb{Z}$. Allora vale il seguente

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

Proof. Sia g un generatore di $\mathbb{Z}_p$ e assumiamo che $p \not| a$ (il caso $p \mid a$ è banale). Notiamo che g deve generare a, ovvero deve esistere un $h \in \mathbb{N}$ tale che $a = g^h$.

Notiamo poi che dal Piccolo Teorema di Fermat segue che $a^{p-1} \equiv 1 \mod p$ e, dato che p è primo, l'equazione $x^2 \equiv 1 \mod p$ ha solo due soluzioni, $x \equiv \pm 1 \mod p$. Ma allora abbiamo che

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

Sostituendo a con g^h troviamo quindi

$$a^{(p-1)/2} \equiv (g^h)^{(p-1)/2} \equiv (g^{(p-1)/2})^h \equiv \pm 1 \mod p$$

Con un ragionamento analogo a quello di prima si trova che necessariamente $g^{(p-1)/2} \equiv \pm 1 \mod p$. Questa volta però, dato che g è un generatore di $\mathbb{Z}_p$, abbiamo che non può succedere il caso $g^{(p-1)/2} \equiv 1 \mod p$. Infatti, se per assurdo dovesse succedere, allora l'ordine di g sarebbe $\leq (p-1)/2$, il che è una assurdo in quanto l'ordine di g è proprio $p-1$. Ma allora $g^{(p-1)/2} \equiv -1 \mod p$.

Troviamo quindi la seguente situazione

$$(g^{(p-1)/2})^h \equiv (-1)^h \pm 1 \mod p$$

Utilizzando il risultato dimostrato precedentemente troviamo quindi che

$$a^{(p-1)/2} \equiv (g^{(p-1)/2})^h \equiv (-1)^h \equiv \begin{cases} 1 & h \text{ è pari } \implies g^h = a \text{ è } R.Q. \text{ modulo } p \\ -1 & h \text{ è dispari } \implies g^h = a \text{ non è } R.Q. \text{ modulo } p \end{cases}$$

□

2.3 Proprietà basilari del simbolo di Legendre

Andiamo a elencare una serie di proprietà elementari del simbolo di Legendre. Tali proprietà facilitano la vista nei calcoli e sono dunque molto importanti da tenere a mente.

Proposizione 2.2. Sia p primo e sia $a \in \mathbb{Z}$. Valgono le seguenti proprietà

1. Il simbolo $\left(\frac{a}{p}\right)$ dipende solo dalla classe di a modulo p, in formula:

$$\forall \alpha \in \mathbb{Z} : [\left(\frac{a}{p}\right) = \left(\frac{a+\alpha p}{p}\right)]$$

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $p \nmid b \implies \left(\frac{ab^2}{p}\right) = ap$
4. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$

Proof. Tutte le proprietà seguono direttamente dalla proposizione precedente, ovvero possono essere dimostrate utilizzando il fatto che $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$ □

2.4 Lemma di Gauss

Il Lemma di Gauss ci permette di calcolare il simbolo di Legendre in un modo diverso. Tale risultato viene principalmente utilizzato per calcolare in modo efficiente i simboli di Legendre della forma $\left(\frac{2}{p}\right)$, con p primo.

Proposizione 2.3 (Lemma di Gauss)**.** Sia p primo e sia $a \in \mathbb{Z}$ tale che $p \nmid a$, allora

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

dove $n(a,p) :=$ numero degli interi contenuti nell'insieme $\{a, 2a, ..., (\frac{p-1}{2})a\}$ il cui resto nella divisione per p è $> (p-1)/2$.

Proof. Osserviamo che l'insieme $A = \{a, 2a, ..., (\frac{p-1}{2})a\}$ ha esattamente $(p-1)/2$ elementi. Dato che a è invertibile modulo p si ha poi che questi elementi sono tutti distinti tra loro modulo p.

Sia A_1 l'insieme degli elementi di A il cui resto nella divisione per p è $\leq (p-1)/2$. Sia m la cardinalità di A_1 e indichiamo con $r_1, r_2, ..., r_m$ i resti modulo p degli elementi di A_1.

In modo analogo, sia $A_2 = A \setminus A_1$ l'insieme degli elementi di A il cui resto nella divisione per p è $> (p-1)/2$. Sia n la cardinalità di A_2 e indichiamo con $s_1, s_2, ..., s_n$ i resti modulo p degli elementi di A_2. Notiamo che $n = n(a,p)$.

Notiamo ora che per ogni $s_i \in A_2$ possiamo considerare l'elemento $p - s_i$ il cui resto nella divisione per p è $\leq (p-1)/2$. Infatti per ogni $i = 1, ..., n$ si ha

$$\begin{aligned} s_i \in A_2 &\iff s_i > p/2 \\ &\iff p - s_i < p - p/2 = p/2 \end{aligned}$$

dunque gli elementi della forma $p - s_i$ sono compresi tra 1 e $(p-1)/2$, che è lo stesso intervallo coperto dagli elementi di A_1.

Ma allora, se consideriamo l'insieme $A' = \{r_1, r_2, ..., r_m, p-s_1, ..., p-s_n\}$ notiamo subito che tale insieme è composto da $m+n = (p-1)/2$ elementi, ciascuno compreso tra 1 e $(p-1)/2$. L'idea adesso è quella di mostrare che gli elementi di A' sono tutti distinti, e quindi che A' è uguale all'insieme $\{1, 2, ..., (p-1)/2\}$.

Supponiamo per assurdo che non sia così, ovvero supponiamo che esistono due elementi di A' che sono uguali tra loro. Questi numeri chiaramente devono essere uno della forma r_j e l'altro della forma $p - s_i$, per qualche j e i. Ma allora otteniamo

$$\begin{aligned} p - s_i = r_j &\implies r_j + s_i = p \\ &\implies r_j + s_i \equiv 0 \mod p \end{aligned}$$

ricordiamo però che, per come erano stati ottenuti r_j e s_i, abbiamo che esistono degli interi $h, k \in \{1, ..., (p-1)/2\}$ tali che

$$\begin{cases} r_j \equiv ah \mod p \\ s_i \equiv ak \mod p \end{cases}$$

mettendo tutto insieme troviamo

$$a(h+k) \equiv_p ah + ak \equiv_p r_j + s_i \equiv_p 0$$

e lavorando in un dominio di integrità possiamo concludere che $a \equiv 0 \mod p$ oppure $h + k \equiv 0 \mod p$, situazione assurda in quanto $p \not| a$ e $0 < h + k < p - 1$.

Ricapitolando abbiamo mostrato che $A' = \{r_1, r_2, ..., r_m p - s_1, ..., p - s_m\}$ è uguale all'insieme $\{1, 2, ..., (p-1)/2\}$. Ma allora possiamo moltiplicare tutti gli elementi di A' in entrambi le rappresentazioni per ottenere lo stesso numero.

$$1 \cdot 2 \cdot ... \cdot (p-1)/2 = r_1 \cdot r_2 \cdot ... \cdot r_m \cdot (p - s_1) \cdot ... \cdot (p - s_n)$$

Riducendo poi modulo p otteniamo

$$\begin{aligned} ((p-1)/2)! &\equiv r_1 \cdot r_2 \cdot ... \cdot r_m \cdot (-s_1) \cdot ... \cdot (-s_n) \mod p \\ &\equiv (-1)^n r_1 r_2 ... r_m s_1 s_2 ... s_n \mod p \\ &\equiv (-1)^n a^{(p-1)/2} ((p-1)/2)! \mod p \end{aligned}$$

Infine, basta notare che $((p-1)/2)!$ è invertibile modulo p, che $n = n(a, p)$, e che $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$ per ottenere quello che si voleva dimostrare, ovvero che

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

□

2.5 Calcolo di $(\frac{2}{p})$

Una importante applicazione del lemma di Gauss è quella utilizzata per calcolare i simboli di Legendre della forma $\left(\frac{2}{p}\right)$. In particolare vale il seguente

Proposizione 2.4. Sia p primo, allora

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$$

Proof. Dal Lemma di Gauss segue che $\left(\frac{2}{p}\right) = (-1)^{n(2,p)}$, dove $n(2,p)$ è il numero degli elementi di $A := \{2, 4, ..., p-1\}$ il cui resto nella divisione per p è $> (p-1)/2$.

Notiamo che, essendo gli elementi di tale insieme tutti strettamente minori di p, abbiamo che il loro valore è uguale al loro resto nella divisione di p. Ma allora per calcolare $n(2,p)$ ci basta calcolare il numero di elementi di $n(2,p)$ che sono $> (p-1)/2$, oppure, equivalentemente, possiamo contare il numero di elenenti che sono $\leq (p-1)/2$ e complementare il numero trovato con il numero totale di elementi.

Notiamo che gli elementi di A sono tutti della forma $2h$, con $h \in \{1, ..., \frac{(p-1)}{2}\}$. Inoltre si ha

$$2h \leq (p-1)/2 \iff h \leq (p-1)/4$$

dunque ci sono esattamente $\lfloor (p-1)/4 \rfloor$ elementi di A che sono $\leq (p-1)/2$. Complementando troviamo che il numero di elementi di A che sono $> (p-1)/2$, ovvero il valore di $n(2,p)$, è dato da

$$n(2,p) = (p-1)/2 - \lfloor (p-1)/4 \rfloor$$

Infine, è possibile far vedere che $n(2,p)$ e $(p^2-1)/8$ hanno la stessa parità. Questo lo si fa distinguendo vari casi, a seconda del resto di p modulo 8.

- Se $p \equiv 1 \mod 8$, allora $p = 8h+1$ e quindi

$$\frac{p^2-1}{8} = \frac{64h^2+16h+1-1}{8} = 8h^2 + 2h \text{ (pari)}$$

$$\frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor = 4h - 2h \text{ (pari)}$$

- Se $p \equiv -1 \mod 8$, allora $p = 8h-1$ e quindi

$$\frac{p^2-1}{8} = \frac{64h^2-16h+1-1}{8} = 8h^2 - 2h \text{ (pari)}$$

$$\frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor = (4h-1) - (2h-1) = 2h \text{ (pari)}$$

- Se $p \equiv 3 \mod 8$, allora $p = 8h + 3$ e quindi

$$\frac{p^2-1}{8} = \frac{64h^2+48h+9-1}{8} = 8h^2 + 6h + 1 \text{ (dispari)}$$

$$\frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor = (4h+1) - 2h = 2h + 1 \text{ (dispari)}$$

- Se $p \equiv -3 \mod 8$, allora $p = 8h - 3$ e quindi

$$\frac{p^2-1}{8} = \frac{64h^2-48h+9-1}{8} = 8h^2 - 6h + 1 \text{ (dispari)}$$

$$\frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor = (4h-2) - (2h-1) = 2h - 1 \text{ (dispari)}$$

□

2.6 Modo alternativo per calcolare $\left(\frac{a}{p}\right)$

A seguire presentiamo un nuovo modo per calcolare il simbolo di Legendre $\left(\frac{a}{p}\right)$. Ricordiamo che abbiamo già presentato due modi per calcolare il simbolo di Legendre: uno utilizzando l'esponenziazione modulare e l'altro utilizzando il Lemma di Gauss. Potrebbe dunque nascere qualche dubbio sul perché stiamo presentando svariati metodi per calcolare lo stesso oggetto. Notiamo solamente che questo nuovo modo verrà utilizzato nella dimostrazione di un risultato fondamentale nel calcolo del simbolo di Legendre, la Legge di reciprocità quadratica.

Proposizione 2.5. Sia p primo e sia $a \in \mathbb{Z}$ dispari e tale che $MCD(a,p) = 1$. Allora

$$\left(\frac{a}{p}\right) = (-1)^{\tau(a,p)}$$

dove

$$\mu(a,p) = \sum_{i=0}^{(p-1)/2} [\frac{ai}{p}]$$

Proof. Notiamo che, per il Lemam di Gauss, ci basta dimostrare che $\tau(a,p) \equiv_2 n(a,p)$.

Ora, per ogni $i = 1, ..., (p-1)/2$ possiamo dividere ia per p e ottenere un quoziente e un resto. In formula, $\forall i = 1, ..., (p-1)/2$ abbiamo che

$$ia = p \cdot \lfloor \frac{ia}{p} \rfloor + S_i, \quad 0 \leq S_i \leq p-1$$

Utilizzando la stessa notazione che abbiamo presentato nella dimostrazione del Lemma di Gauss troviamo che

$$\{S_1, S_2, ..., S_{(p-1)/2}\} = \{r_1, r_2, ..., r_m, s_1, s_2, ..., s_n\}$$

e dunque, sommando su tutti gli i, troviamo

$$\begin{aligned}\sum_{i=1}^{(p-1)/2} ia &= p\sum_{i=0}^{(p-1)/2} \lfloor \frac{ia}{p} \rfloor + \sum_{i=1}^{(p-1)/2} S_i \\ &= p\cdot\tau(a,p) + \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_i\end{aligned}$$

Ricordiamo poi che nella dimostrazione del Lemma di Gauss avevamo dimostrato che $\{r_1, r_2, ..., r_m, p-s_1, ..., p-s_n\} = \{1, 2, ..., (p-1)/2\}$. Ma allora otteniamo la seguente uguaglianza

$$\begin{aligned}\sum_{i=1}^{(p-1)/2} i &= \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} p - s_j \\ &= \sum_{i=1}^{m} r_i - \sum_{j=1}^{n} s_j + p\cdot n\end{aligned}$$

il che equivale a dire che

$$\sum_{i=1}^{m} r_i = \sum_{i=1}^{(p-1)/2} i + \sum_{j=1}^{n} s_j - p\cdot n$$

Sostituendo quest'ultima equazione in quella più generale di prima troviamo

$$\begin{aligned}\sum_{i=1}^{(p-1)/2} ia &= p\cdot\tau(a,p) + \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_i \\ &= p\cdot\tau(a,p) + (\sum_{i=1}^{(p-1)/2} i + \sum_{j=1}^{n} s_j - p\cdot n) + \sum_{j=1}^{n} s_i\end{aligned}$$

che nuovamente equivale a dire

$$(a-1)\sum_{i=1}^{(p-1)/2} = p\cdot\tau(a,p) - p\cdot n + 2\sum_{j=1}^{n} s_j$$

Per finire notiamo che per le ipotesi fatte su a si ha che $a-1$ è pari mentre p è dispari. Riducendo modulo 2 otteniamo dunque

$$0 \equiv_2 (a-1)\sum_{i=1}^{(p-1)/2} \equiv_2 p\cdot\tau(a,p) - p\cdot n + 2\sum_{j=1}^{n} s_j \equiv_2 \tau(a,p) - n$$

il che vale se e solo se

$$\tau(a,p) \equiv n(a,p) \mod 2$$

in quanto $n = n(a,p)$. □

2.7 Legge di reciprocità quadratica

La legge di reciprocità quadratica è uno dei risultati fondamentali nel calcolo dei simboli di Legendre. Andiamo prima a presentare l'enunciato, poi una dimostrazione geometrica del risultato e infine alcune osservazioni di tipo pratico su come viene effettivamente utilizzato per calcolare i simboli di Legendre.

Teorema 2.1 (Legge di reciprocità quadratica)**.** Siano p, q numeri primi con p dispari e $q < p$. Allora

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) & p \equiv q \equiv 3 \mod 4 \\ \left(\frac{p}{q}\right) & \text{altrimenti} \end{cases}$$

Proof. Consideriamo il rettangolo aperto R del piano xy di vertici $(0,0), (p/2,0), (0,q/2), (p/2,q/2)$. Notiamo che tale rettangolo ha esattamente $(p-1)(q-1)/4$ punti interi. L'idea della dimostrazione è quella di contare questi il numero di questi punti interi.

Sia D la diagonale del rettangolo descritta dalla retta di equazione

$$y = \frac{q}{p}x \iff py = qx$$

Notiamo che, dato che $MCD(p,q) = 1$, allora nessuno dei punti a coordinate intere di R giace su D. Infatti, se così non fosse, ovvero se per assurdo esiste un punto di R a coordinate intere (x^*, y^*) che giace su D, allora si ha $py^* = qx^*$, e quindi, dato che $MCD(p,q) = 1$, si ha che $p \mid x^*$ e $q \mid y^*$. Questo è un assurdo, in quanto sappiamo che x^* si trova nell'intervallo $[1, (p-1)/2]$, e dunque non può essere un multiplo di p.

Indichiamo con R_1 la porzione di R posta sotto D e con R_2 la porzione di R posta sopra D. I punti di R_1 le cui coordinate sono intere sono tutti e soli i punti del tipo (i,j) con $1 \le i \le (p-1)/2$ e $1 \le j \le \lfloor \frac{qi}{p} \rfloor$. Sommandoli tutti otteniamo quindi

$$\sum_{i=1}^{(p-1)/2} \lfloor \frac{qi}{p} \rfloor = \tau(q,p)$$

Analogamente, i punti di R_2 le cui coordinate sono intere sono tutti e soli i punti del tipo (i,j) con $1 \le j \le (q-1)/2$ e $1 \le i \le \lfloor \frac{pj}{q} \rfloor$. Sommandoli tutti otteniamo

$$\sum_{j=1}^{(q-1)/2} \lfloor \frac{pj}{q} \rfloor = \tau(p,q)$$

Otteniamo dunque la seguente uguaglianza

$$\tau(q,p) + \tau(p,q) = (p-1)(q-1)/4$$

e, dalla proposizione precedente, segue che

$$\begin{aligned} \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) &= (-1)^{\tau(p,q)}(-1)^{\tau(q,p)} \\ &= (-1)^{\tau(p,q)+\tau(q,p)} \\ &= (-1)^{\frac{(p-1)(q-1)}{4}} \end{aligned}$$

Infine, notando che $\left(\frac{p}{q}\right)^{-1} = \left(\frac{p}{q}\right)$ otteniamo il risultato voluto, ovvero che

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

□

Osserviamo che la legge di reciprocità quadratica lega tra loro le seguenti due congruenze, relative a moduli diversi, che sono $x^2 \equiv q \mod p$ e $x^2 \equiv p \mod q$. Tale legge, se utilizzata insieme alle altre proprietà del simbolo di Legendre, facilita enormemente il calcolo del simbolo. Ad esempio se dobbiamo calcolare il simbolo di legendre $\left(\frac{7}{73}\right)$ ci basta verificare che sia 73 e 7 sono primi e notare che $7 \equiv 3 \mod 4$ mentre $73 \equiv 1 \mod 4$ e, utilizzando la legge di reciprocità quadratica, possiamo inferire che

$$\left(\frac{7}{73}\right) = -\left(\frac{73}{7}\right)$$

ora ci basta ridurre 73 modulo 7 per ottenere 3, e dalle proprietà del simbolo troviamo che

$$-\left(\frac{73}{7}\right) = -\left(\frac{3}{7}\right)$$

Nuovamente, possiamo utilizzare la legge di reciprocità quadratica e le proprietà generali del simbolo per ottenere

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

dunque concludiamo che $\left(\frac{7}{73}\right) = -1$, ovvero la congruenza di secondo grado $x^2 \equiv 7 \mod 73$ non ha soluzioni in $\mathbb{Z}_{73}$.

3 Simbolo di Jacobi

Arrivati a questo punto sappiamo calcolare il simbolo di Legendre in vari casi. Notiamo però che se dobbiamo calcolare $\left(\frac{a}{p}\right)$ e ci troviamo nel caso in cui a è un numero dispari $< p$ e non primo, allora per calcolare il simbolo dobbiamo necessariamente fattorizzare a, cosa che potrebbe essere molto costosa. L'idea adesso è quella di introdurre un nuovo simbolo, il simbolo di Jacobi, in modo tale da eliminare quei pochi intoppi che ci rimangono nel calcolo dei simboli di Legendre. Una cosa molto importante da tenere a mente è che questo nuovo simbolo, a differenza del simbolo di Legendre, non sarà collegato in alcun modo all'esistenza di soluzioni di congruenze della forma $x^2 \equiv a \mod p$, come lo era il simbolo di Legendre. Bisogna quindi vedere il simbolo di Jacobi semplicemente come uno strumento formale, senza significato, che ci aiuterà a calcolare i simbolo di Legendre.

3.1 Definizione di simbolo di Jacobi

Sia $a \in \mathbb{Z}$ e sia n un intero positivo dispari. Consideriamo poi la fattorizzazione di $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$. Definiamo il *simbolo di Jacobi* nel seguente modo

$$\underbrace{\left(\frac{a}{n}\right)}_{\text{simbolo di Jacobi}} = \underbrace{\left(\frac{a}{p_1}\right)^{\alpha_1} ... \left(\frac{a}{p_r}\right)^{\alpha_r}}_{\text{simboli di legendre}}$$

Dunque il simbolo $\left(\frac{a}{n}\right)$ è di Legendre se il denominatore è primo ed è di Jacobi se il denominatore non è primo.

3.2 Proprietà del simbolo di Jacobi

Anche il simbolo di Jacobi possiede tutta una serie di proprietà, analoghe a quelle del simbolo di Legendre e molto utili per semplificare i calcoli. Andiamo quindi a elencare le proprietà più importanti.

1. Se $a \equiv b \mod n$, allora $\left(\frac{a}{n}\right) = bn$
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
3. $\left(\frac{a}{n}\right) = 1$, $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
4. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$
5. Se m, n sono interi dispari, allora

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}$$

4 Algoritmo 1: Calcolo simbolo di Legendre/Jacobi

A seguire riportiamo un programma scritto in python che calcola il simbolo $\left(\frac{a}{n}\right)$. Ricordiamo che il valore assunto dal simbolo quando n non è primo non ci dice nulla sull'esistenza o meno di soluzioni alla congruenza $x^2 \equiv a \mod n$. Invece, se n è primo, allora il valore del simbolo ci permette di stablire se esiste o no una soluzione a tale congruenza.

Il codice riportato essenzialmente utilizza in modo iterativo tutte le proprietà del simbolo di Legendre (e di Jacobi) viste fino ad ora per cercare di semplificare il calcolo.

```
def legendre(a, p):
  # does a divides p ?
  if a % p == 0:
      return 0

  # is a equal to 1?
  if a == 1:
      return 1

  # is a greater than p?
  if a > p:
      return legendre(a % p, p)

  # are a and p both odd?
  if a % 2 == 1 and p % 2 == 1:
      # are a and p both congruent to 3 mod 4?
      if a % 4 == 3 and p % 4 == 3:
          return -legendre(p, a)
      else:
          return legendre(p, a)

  # is a even?
  if a % 2 == 0:
      # is (p^2 - 1)/8 even or odd?
      if ((p ** 2 - 1) / 8) % 2 == 0:
          return legendre(int(a / 2), p)
      else:
          return -legendre(int(a / 2), p)
```

5 Algoritmo 2: Calcolo radici quadrate in $\mathbb{Z}_p$

Fino ad adesso abbiamo studiato un metodo, il calcolo del simbolo di Legendre, per stabilire se, dati $a, p \in \mathbb{Z}$ con p primo, la congruenza

$$x^2 \equiv a \mod p$$

ha una soluzione oppure no. Lo scopo di questa sezione sarà quello di descrivere un algoritmo per il calcolo effettivo della radice quadrata di un elemento $a \in \mathbb{Z}_p$, assumendo ovviamente che $\left(\frac{a}{p}\right) = 1$.

L'algoritmo, per funzionare, necessita di un intero $n < p$ che non sia un residuo quadratico modulo p, ovvero tale che $\left(\frac{n}{p}\right) = -1$. Andiamo subito a vedere il perché di questa richiesta.

Scomponiamo $p - 1 = 2^r s$, con $r \in \mathbb{N}^+$, s dispari e defniamo

$$\xi := n^s \mod p$$

allora vale il seguente lemma

Lemma 5.1. Il numero ξ è una radice 2^r-esima primitiva dell'unità in $\mathbb{Z}_p$.

Proof. Ricordiamo che ξ è una radice 2^r-esima primitiva dell'unità in $\mathbb{Z}_p$ se ξ è una radice 2^r-esima dell'unità, ovvero $\xi^{2^r} \equiv 1 \mod p$, e tutte e sole le radici 2^r-esime dell'unità in $\mathbb{Z}_p$ sono potenze di ξ.

Iniziamo notando che ξ è chiaramente una radice 2^r-esima dell'unità. Infatti per come è stata definita abbiamo che

$$\xi^{2^r} \equiv_p (n^s)^{2^r} \equiv_p n^{2^r s} \equiv_p n^{p-1} \equiv_p 1$$

Rimane da dimostrare che ξ è una radice 2^r-esima *primitiva* dell'unità. Supponiamo per assurdo che non lo sia. Dato che $2^r \mid p-1$, sappiamo, da risultati già dimostrati (vedere lezione 11 del 12/04/2018), che esiste una radice 2^r-esima primitiva dell'unità. Sia μ tale radice primitiva. Allora deve esistere un h tale che

$$\xi = \mu^h$$

Dato che ξ non è una radice 2^r-esima primitiva dell'unità, dobbiamo avere che $MCD(h, 2^r) \neq 1$. Dunque h deve almeno avere un fattore 2. Notiamo però che possiamo assumere senza perdità di generalità che h non ha nessun fattore dispari, ovvero che h è della forma 2^j, con $1 \leq j \leq r-1$. Infatti, se così non fosse, ovvero se $h = 2^j k$, con k dispari, allora possiamo considerare $\mu' := \mu^k$ e notare che anche μ' è una radice 2^r-esima primitiva dell'unità in quanto $MCD(2^r, k) = 1$ e dunque $\langle \mu^k \rangle = \langle \mu \rangle$.

Dunque sappiamo che esiste un μ tale che $\xi = \mu^{2^j}$, con $1 \leq j \leq r-1$. Da questo segue che

$$\xi = \mu^{2^j} = (\mu^{2^{j-1}})^2 \implies \left(\frac{\xi}{p}\right) = 1$$

ma noi sapevamo che $\xi \equiv n^s \mod p$, e che $\left(\frac{n}{p}\right) = -1$, e quindi

$$\left(\frac{\xi}{p}\right) = \left(\frac{n^s}{p}\right) = \left(\frac{n}{p}\right)^s = (-1)^s = -1$$

il che ci porta ad un assurdo. Concludiamo che ξ è una radice 2^r-esima primitiva dell'unità. □

Riflettiamo su quello che abbiamo dimostrato: sappiamo che $\xi = (n^s \mod p)$ è una radice 2^r-esima primitiva dell'unità in $\mathbb{Z}_p$. Sappiamo inoltre che $\xi \in \mathbb{Z}_p$. Questo vuol dire che $\mathbb{Z}_p$ contiene ξ e contiene anche tutte le sue potenze. In altre parole, se scomponiamo $p-1 = 2^r s$, con s dispari, allora sappiamo che $\mathbb{Z}_p$ contiene tutte le radici 2^h-esime dell'unità, per $h = 1, ..., r$.

5.1 Impostazione algoritmo

Notiamo i seguenti fatti

1. a^s è una radice 2^r-esima dell'unità, ed è quindi esprimibile come potenza di ξ. Infatti,

$$\left(\frac{a}{p}\right) = 1 \iff a^{(p-1)/2} \equiv 1 \mod p \iff (a^s)^{2^{r-1}} \equiv_p 1$$
$$\implies (a^s)^{2^r} \equiv 1 \mod p$$

   Inoltre, se a^s è una radice 2^r-esima dell'unità, anche a^{-s} lo è per il semplice fatto che

$$(a^{-s})^{2^r} \equiv_p ((a^s)^{2^r})^{-1} \equiv_p (1)^{-1} \equiv_p 1$$

   ma allora possiamo esprimere a^{-s} come potenza di ξ, ovvero esiste un $t \in \mathbb{N}$ con $0 < t < 2^{r-1}$ tale che

$$a^{-s} \equiv \xi^t \mod p$$

2. ξ non è una radice $2^{r-1}-$esima dell'unità. Infatti,

$$\left(\frac{n}{p}\right) = -1 \iff n^{(p-1)/2} \equiv_p -1 \iff n^{2^{r-1}s} \equiv_p -1$$
$$\iff (\xi)^{2^{r-1}} \equiv_p -1$$

5.2 Codice

```
def mod_square_root(a, p):
    if legendre(a, p) == -1:
        return None

    r, s = decompose(p - 1)
    n = find_non_quadratic_residue(p)
    xi = mod_exp(n, s, p)
    ro = mod_exp(a, int((s + 1) / 2), p)

    if mod_exp(a, s, p) == 1:
        return ro
    else:
        v = 0
        a_inv = (mod_inverse(a, p) + p) % p
        for h in range(0, r - 1):
            temp = ro
            temp = temp * mod_exp(xi, v, p)
            temp = mod_exp(temp, 2, p)
            temp = a_inv * temp % p
            temp = mod_exp(temp, 2 ** (r - h - 2), p)

            if temp == p-1:
                v += 2 ** h

    return ro * mod_exp(xi, v, p) % p
```