1 $N2^+$ - Appendice

1.1 Residui Quadratici $\pmod p$

In $\mathbb{F}_p$, fissato un generatore g, i residui quadratici sono tutti e soli gli elementi dell'insieme

$$Q = \{0\} \cup \left\{ g^{2k} \text{ t.c. } 1 \leq k \leq \frac{p-1}{2} \right\}$$

ossia le potenze pari di g. In particolare il prodotto di due non-residui quadratici è un residuo quadratico, ed a è un residuo quadratico se e solo se realizza

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

Per il teorema di Wilson è sempre vero che

$$(p-1)! \equiv -1 \pmod p$$

e possiamo riscrivere l'identità come

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

In particolare, se $p \equiv 1 \pmod 4$, -1 è un residuo quadratico che ha come 'radice quadrata' $\pm \left(\frac{p-1}{2}!\right)$. In caso contrario, $p \equiv 3 \pmod 4$, si ha

$$(-1)^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod p$$

che -1 non è un residuo quadratico. Da ciò discende che ogni primo $p \equiv 1 \pmod 4$ si scrive in modo sostanzialmente unico come somma di due quadrati. Chiamiamo infatti u_0 il più piccolo intero (in modulo) per cui si abbia $u_0^2 \equiv -1 \pmod p$: risulta

$$u_0^2 + 1 = k_0 p \quad \text{con} \quad k_0 \leq \frac{p}{4}$$

Prendiamo ora u_1 e v_1, di modulo più piccolo possibile, tali da verificare $u_1 \equiv u_0 \pmod{k_0}$,$v_1 \equiv 1 \pmod{k_0}$. Risulta:

$$u_1^2 + v_1^2 = k_1 k_0 \quad \text{con} \quad k_1 < k_0$$

D'altro canto l'insieme degli interi esprimibili come somma di due quadrati è chiuso per moltiplicazione, in quanto

$$(a+ib)(c-id) = (ac+bd)+i(bc-ad) \longrightarrow (a^2+b^2)(c^2+d^2) = (ac+bd)^2+(bc-ad)^2$$

Ora, posto $a = u_0, b = v_0 = 1, c = u_1, d = v_1$, si ha che k_0 divide sia $ac+bd$ che $bc-ad$; moltiplicando le identità precedentemente scritte si ha dunque

$$u_2^2 + v_2^2 = k_1 p \quad \text{con} \quad k_1 < k_0$$

e il processo di discesa prosegue fin quando non si ha $k_i = 1$, che produce la fattorizzazione negli interi di Gauss

$$p = (u_i + iv_i)(u_i - iv_i)$$

ove ambo i fattori sono primi in $\mathbb{Z}[i]$, avendo per norma un primo di $\mathbb{Z}$: segue l'unicità della scrittura

$$p = u_i^2 + v_i^2$$

a meno di cambiamenti di segno o trasposizione delle variabili. Incidentalmente, il numero di modi in cui è possibile esprimere un generico intero m come somma di due quadrati è in biezione con le possibili scomposizioni [1]

$$m = z \cdot \bar{z} \quad \text{con} \quad z \in \mathbb{Z}[i]$$

dunque con le medesime scomposizioni per i primi di $\mathbb{Z}$ che dividono m: in particolare, se un primo $p \equiv 3 \pmod 4$ divide esattamente m con molteplicità dispari, quest'ultimo non può essere espresso come somma di due quadrati; in caso contrario si ha

$$\#\left\{(a,b) \in \mathbb{Z}^2 \text{ t.c. } a^2+b^2 = m\right\} = 4\left(\sum_{\substack{d|n \\ d\equiv 1 \pmod 4}} 1 \quad - \sum_{\substack{d|n \\ d\equiv 3 \pmod 4}} 1\right)$$

(si noti che il membro destro è il quadruplo di una funzione moltiplicativa).
Un discorso moralmente analogo si ha con la somma di quattro quadrati:

$$\#\left\{(a,b,c,d) \in \mathbb{Z}^4 \text{ t.c. } a^2+b^2+c^2+d^2 = m\right\} = 4 \sum_{\substack{d|n \\ d\not\equiv 1 \pmod 4}} d$$

Per quanto riguarda la somma di tre quadrati: ogni intero che non sia della forma $4^u(8k+7)$ può essere espresso come somma di tre quadrati, ma il numero di rappresentazioni non si esprime attraverso funzioni aritmetiche elementari.
Tornando ai residui quadratici, consideriamo che l'identità

$$(1+i)^2 = 2i$$

implica che la condizione di residuosità quadratica per il 2 dipenda dalla condizione di residuosità quartica per -1, ovvero unicamente dalla classe residua $p \pmod 8$[2]. In particolare si ha

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

Consideriamo ora il prodotto

$$Z = a \cdot 2a \cdot \ldots \cdot \frac{p-1}{2}\, a = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}!\right)$$

definiamo una funzione modulo

$$\|x\| = \begin{cases} x & \text{se} \quad 1 \le x \le \frac{p-1}{2} \\ -x & \text{se} \quad \frac{p+1}{2} \le x \le (p-1) \end{cases}$$

[1] Un discorso completamente analogo prova che ogni primo p per cui -2 sia un residuo quadratico (ovvero ogni primo congruo a 1 o 3 modulo 8, come sarà chiaro successivamente) si può esprimere in modo sostanzialmente unico come $a^2 + 2b^2$.

[2] Se $p \equiv 3, 7 \pmod 8$, il set dei quadrati coincide con quello delle quarte potenze. Se $p \equiv 1, 5 \pmod 8$, il set delle quarte potenze è costituito da tutti gli elementi nella forma g^{4k}, con $1 \le k \le \frac{p-1}{4}$, ed a è un residuo quartico se e solo verifica $a^{\frac{p-1}{4}} \equiv 1 \pmod p$.

e denotiamo con n il numero di interi della forma ka che giacciono nel secondo intervallo. Possiamo scrivere

$$Z = (-1)^n \prod_{j=1}^{\frac{p-1}{2}} \|ja\|$$

e notare che i termini del prodotto sono tutti distinti in quanto

$$\|ja\| = \|ka\| \longrightarrow j = \pm k$$

ma non può verificarsi $p|(j+k)$, poichè il membro destro è maggiorato da p. Segue:

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

donde l'incredibile *Lemma di Eisenstein*

$$a^{\frac{p-1}{2}} = (-1)^n \quad \text{con} \quad n = \sum_{\substack{0<u<p \\ u \equiv 0 \,(\mathrm{mod}\ 2)}} \left\lfloor \frac{ua}{p} \right\rfloor$$

Che già di per sè garantisce il fatto che la residuosità quadratica (o la mancata tale) di a modulo p dipenda unicamente dalla classe residua di $p \pmod{4a}$. Inoltre, per double counting sui punti a coordinate intere contenuti in un rettangolo $(p-1)\times(q-1)$, rispettivamente al di sopra e al di sotto della diagonale, si ha pure che ogni coppia (p,q) di primi dispari realizza

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

Se dunque p è residuo quadratico modulo q, q è residuo quadratico modulo p, a meno che p e q non siano entrambi della forma $4k+3$, e in tal caso si verifica l'opposto. Quanto enunciato è il *Teorema di Reciprocità Quadratica.*

Definito il *Simbolo di Jacobi* per un intero a e un intero dispari m come estensione moltiplicativa del simbolo di Legendre, attraverso

$$\left(\frac{a}{m}\right) = \prod_{p_i^{\alpha_i}||m} \left(a^{\frac{p_i-1}{2}} \pmod{p_1}\right)^{\alpha_i}$$

risultano vere le seguenti identità:

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{4}} \qquad \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} \qquad \left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$$

che permettono di conoscere molto rapidamente se un intero è o meno un residuo quadratico modulo p:

$$\left(\frac{153}{1009}\right) = \left(\frac{91}{153}\right) = \left(\frac{62}{91}\right) = -\left(\frac{31}{91}\right) = -\left(\frac{-2}{31}\right) = \left(\frac{2}{31}\right) = 1$$

(la complessità è la stessa del calcolo di un massimo comun divisore; analoga situazione per l'estrazione della radice quadrata di un residuo: si consiglia di

sfogliare la bibliografia in merito all'algoritmo di Shanks e a quello di Cipolla e Lehmer.) Si osservi come il simbolo di Jacobi non denoti la condizione di residuosità per un modulo composito, si ha infatti

$$\left(\frac{2}{15}\right) = 1$$

sebbene (e qui l'avversativa è da leggersi come causale) 2 non sia residuo quadratico $\pmod 3$ o $\pmod 5$. E' vero tuttavia che il numero delle soluzioni dell'equazione

$$x^2 + bx + c \equiv 0 \pmod{p_1^{\alpha_1} \dots p_k^{\alpha^k}} \quad \text{con} \quad p_i > 2$$

sia pari a

$$\prod_{j=1}^{k} \left(1 + \left(\frac{b^2 - 4c}{p_j}\right)\right) \quad \text{assumendo} \quad \left(\frac{mp_j}{p_j}\right) = 0$$

per il Teorema Cinese del Resto e il Teorema di Struttura dei gruppi $(\mathbb{Z}/p^k\mathbb{Z})^*$. Viene naturale chiedersi: ammesso che il discriminante D sia un residuo quadratico, come si passa dalle soluzioni di $Q(x) = x^2 - D \equiv 0 \pmod{p^k}$ a quelle di $Q(x) \equiv 0 \pmod{p^{k+1}}$? Attraverso il *Lemma di Hensel*. Supponiamo che $d_1^2 \equiv D \pmod{p^k}$ e cerchiamo h tale che

$$(d_1 + hp^k)^2 \equiv D \pmod{p^{k+1}} \quad \text{con} \quad 0 \leq h \leq (p-1)$$

Una scelta funzionante è

$$h = \frac{d_1^2 - D}{p^k} \cdot \left((-2d_1)^{-1} \pmod p\right)$$

Si noti come tale procedimento di shift sia algebricamente analogo all'iterazione di Newton e funzioni per polinomi di ogni grado (dimostrando di fatto il teorema di struttura per i gruppi $(\mathbb{Z}/p^k\mathbb{Z})^*$).