

# Università di Pisa

Facoltà di Scienze Matematiche Fisiche e Naturali  
Corso di Laurea in Matematica

Anno Accademico 2007/2008

Elaborato finale

NOTE SUL PROBLEMA

$$n = a^2 + kb^2$$

Candidato  
**Jacopo D'Aurizio**

Relatore  
**Chiarissimo Prof.  
Giuseppe Puglisi**

# Indice

1	Introduzione al lavoro	3
2	Simboli e abbreviazioni utilizzate	4
3	Lemma di moltiplicatività	5
4	Lemma del residuo quadratico	5
5	Lemma di unicità	7
6	Metodo di discesa	8
7	Teorema di Bambah-Chowla	8
8	Radici quadrate in $(\mathbb{Z}/p\mathbb{Z})^*$	9
9	Prodotto triplo di Jacobi	10
10	Identità di Jacobi e Lorenz	11
11	Numero di rappresentazioni $r_k(n)$ sotto una differente ottica	14
12	Caso $k = 4$	15
13	Prime stranezze, caso $k = 5$	15
14	Forme quadratiche	15
15	Caso $k = 5$ , giunge chiarezza	19
16	Composizione e gruppo delle classi	20
17	Teoria dei generi	21
18	Formula delle classi	23
19	Caso $k = 7$ e affini	25
20	Numeri idonei	25
21	Crivello di Atkin	26
22	Ruolo delle leggi di reciprocità di ordine superiore	27
23	Campo delle classi di Hilbert	31
24	Moltiplicazione complessa	32
25	Ringraziamenti	35

# 1 Introduzione al lavoro

Il problema di quali interi siano o meno esprimibili come somma di due quadrati (o di un quadrato e un fissato multiplo di un quadrato) affonda le sue radici nell'antichità, basti pensare alle equazioni di Pell come generalizzazione delle equazioni diofantee o al metodo della retta secante per la risoluzione di problemi della forma

$$ax^2 + bxy + cy^2 = z^2 \quad a, b, c, x, y, z \in \mathbb{Z}$$

I contributi maggiori in materia sono stati forniti da Gauss, Lagrange, Legendre, Jacobi ed Eulero nel corso del diciottesimo e del diciannovesimo secolo, attraverso tecniche al confine tra algebra, geometria e teoria dei numeri vera e propria.

In queste pagine vorremmo indagare, con metodi elementari (fin dove possibile), il problema di quali interi  $n$  possano essere rappresentati dalla forma (*canonica*)  $a^2 + kb^2$  (con  $k > 0$ ) e in quanti possibili modi ( $r_k(n)$ ).

Attraverso la moltiplicatività della norma sugli anelli  $\mathbb{Z}[\sqrt{-k}]$  vedremo come il problema si riconduca quasi immediatamente allo studio di quali *primi* possano essere espressi in tale forma; presenteremo una dimostrazione della legge di reciprocità quadratica (che riveste un ruolo fondamentale nella trattazione) di natura puramente combinatorica, indipendente cioè dal *lemma di Gauss* o da considerazioni su campi finiti di caratteristica  $p$ , che pure si riveleranno utili come fondamenta di un algoritmo (*Algoritmo di Shank*) per l'estrazione di radice quadrata in  $(\mathbb{Z}/p\mathbb{Z})^*$ ; vedremo come dal *prodotto triplo di Jacobi*

$$\prod_{n \geq 1} (1 - q^{2n})(1 + uq^{2n-1})(1 + u^{-1}q^{2n-1}) = \sum_{n \geq 0} u^n q^{n^2}$$

discendano semplicemente identità per  $r_1(n)$  ed  $r_2(n)$  (le tecniche utilizzate, proprie del *calcolo umbrale*, sono affini a quelle utilizzate da Ramanujan per produrre le note identità sulla funzione delle partizioni); mostreremo come sia possibile, in alcuni casi fortunati, computare la rappresentazione canonica di un primo attraverso un algoritmo euclideo (fondato cioè su considerazioni concernenti anelli euclidei, ed a complessità logaritmica). Indagheremo sul fatto che la condizione

$$\exists a \in (\mathbb{Z}/p\mathbb{Z})^* : a^2 + k \equiv 0 \pmod{p}$$

nella quasi totalità dei casi non sia sufficiente a garantire la rappresentabilità in forma canonica di un primo  $p$ , sebbene la classificazione delle forme quadratiche binarie, intere e definite positive fornisca una naturale estensione del precedente algoritmo di riduzione. Osserveremo come neppure questa classificazione sia completamente risolutiva, introducendo perciò elementi di *teoria dei generi*; vedremo quale sia il ruolo dei *numeri idonei* di Eulero e come il *crivello di Atkin* sia una naturale applicazione della teoria stessa.

Al termine della trattazione illustreremo (riservandoci di omettere alcune dimostrazioni, ove queste esulino palesemente dagli scopi del presente lavoro) come tecniche algebriche più avanzate, in congiunzione con la teoria della moltiplicazione complessa, risolvano brillantemente il problema in analisi, fornendo un criterio esaustivo per decidere quando l'equazione

$$p = a^2 + kb^2$$

posseda o meno soluzioni intere, lasciando comunque spazio a congetture ed approfondimenti.

## 2 Simboli e abbreviazioni utilizzate

$\#A$	Cardinalità dell'insieme $A$
$\gcd(a, b)$	Massimo comun divisore tra $a$ e $b$
$a \pmod{p}$	Classe residua di $a$ in $(\mathbb{Z}/p\mathbb{Z})^*$
$\chi(m)$	Carattere di Dirichlet, omomorfismo tra un gruppo abeliano e $\mathbb{C}^*$
$L(a, p) = a^{(p-1)/2} \pmod{p}$	Simbolo di Legendre (reciprocità quadratica)
$J(m, n)$	Simbolo di Jacobi, estensione moltiplicativa del simbolo di Legendre
$K(m, n)$	Simbolo di Kronecker, estensione del simbolo di Jacobi
$L_3(a, \pi)$	Estensione del simbolo di Legendre per la reciprocità cubica
$L_4(a, \pi)$	Estensione del simbolo di Legendre per la reciprocità biquadratica
$L(s, \chi)$	Funzione $L$ di Dirichlet associata al carattere $\chi$
$GL(n, \mathbb{Z})$	Gruppo delle matrici $n \times n$ a coefficienti in $\mathbb{Z}$ e determinante $\pm 1$
$SL(n, \mathbb{Z})$	Gruppo delle matrici $n \times n$ a coefficienti in $\mathbb{Z}$ e determinante $+1$
$(f * g)(n) = \sum_{d n} f(d)g(n/d)$	Convoluzione moltiplicativa tra le funzioni aritmetiche $f$ e $g$
$d(n)$	Numero di divisori di $n$
$\omega(n)$	Numero di divisori primi di $n$
$\Omega(n)$	Numero di divisori primi di $n$ , contati con molteplicità
$\Omega_k(n)$	Numero di divisori primi di $n$ per cui $-k$ è residuo quadratico, contati con molteplicità

### 3 Lemma di moltiplicatività

**Teorema 3.1.** Per ogni intero positivo  $k$  l'insieme degli interi nella forma  $a^2 + kb^2$  è un monoide moltiplicativo

*Dimostrazione.* E' una semplice conseguenza della moltiplicatività dell'usuale norma su  $\mathbb{C}$ , posto infatti

$$z = a + b\sqrt{-k} \quad w = c + d\sqrt{-k}$$

si ha

$$\begin{aligned} z\bar{z} &= a^2 + kb^2 & w\bar{w} &= c^2 + kd^2 \\ z\bar{w} &= (ac + kbd) + (bc - ad)\sqrt{-k} \\ (a^2 + kb^2)(c^2 + kd^2) &= z\bar{w}z\bar{w} = (ac + kbd)^2 + k(bc - ad)^2 \end{aligned}$$

□

Da ciò non è difficile dedurre la correlazione del problema in analisi con la decomposizione

$$n = Q\bar{Q} = \prod_{i=1}^{\Omega_k(n)} q_i \bar{q}_i$$

ove i  $q_i$  sono irriducibili nell'anello  $\mathbb{Z}[\sqrt{-k}]$ .

### 4 Lemma del residuo quadratico

Denotando con  $L(-k, p)$  l'usuale simbolo di Legendre, pari a  $(-k)^{(p-1)/2} \pmod{p}$ , ovvero a +1 nel caso in cui  $-k$  sia un residuo quadratico in  $(\mathbb{Z}/p\mathbb{Z})^*$ , -1 altrimenti, si ha

**Teorema 4.1.** Se  $n = a^2 + kb^2$ , per ogni primo  $p$  che divide esattamente  $n$ , si ha  $L(-k, p) = +1$ .

*Dimostrazione.* Da  $a^2 + kb^2 \equiv 0 \pmod{p}$  segue  $(a \cdot b^{-1})^2 \equiv -k \pmod{p}$ . □

**Teorema 4.2.** Fissato un  $k$  dispari, il fatto che  $-k$  sia o meno residuo quadratico in  $\mathbb{Z}/p\mathbb{Z}$  dipende unicamente dalla classe residua di  $p$  modulo  $4k$ .

*Dimostrazione.* E' un risultato universalmente noto come *Lemma di Gauss*, sostanzialmente equivalente al teorema di reciprocità quadratica. In questo paragrafo porteremo avanti un approccio inusuale: seguendo quanto tracciato da un recente articolo di W.Castryck[5], dimostreremo il teorema di reciprocità per via combinatorica per poi dedurne il Lemma di Gauss come corollario.

Assegnato un primo dispari  $q$ , per ogni intero dispari  $m$  denotiamo con  $N_m$  il numero di soluzioni in  $(\mathbb{Z}/q\mathbb{Z})^m$  di

$$x_1^2 - x_2^2 + x_3^2 - \dots + x_m^2 = 1$$

Effettuando la sostituzione  $x_1 \leftarrow x_1 + x_2$  otteniamo

$$x_1^2 + x_3^2 - \dots + x_m^2 - 1 = -2x_1x_2$$

Per ogni valore non nullo di  $x_1$  e per qualunque valore di  $x_3, \dots, x_m$  esiste un unico valore di  $x_2$  che soddisfa l'identità. Se  $x_1 = 0$  il valore di  $x_2$  non ha alcuna rilevanza e l'equazione diviene  $x_3^2 - \dots + x_m^2 = 1$ .

In sintesi

$$N_m = q^{m-2}(q-1) + qN_{m-2} = q^{m-1} + q^{(m-1)/2}$$

e in particolare, per  $p$  primo dispari,

$$N_p \equiv 1 + L(q, p) \pmod{p}$$

In alternativa,  $N_p$  può essere calcolato come

$$\sum_{u_1+u_2+\dots+u_p=1} N(x_1^2 = u_1)N(x_2^2 = -u_2)N(x_3^2 = u_3) \dots N(x_p^2 = u_p)$$

ove  $N(\dots)$  indica il numero di soluzioni della corrispondente equazione univariata in  $\mathbb{Z}/q\mathbb{Z}$ . Segue

$$N_p = q^{p-1} + \sum_{u_1+u_2+\dots+u_p=1} \prod_{j=1}^p (1 + L(u_j, q))$$

che si semplifica in

$$N_p = q^{p-1} + L\left((-1)^{(p-1)/2}, q\right) \sum_{u_1+u_2+\dots+u_p=1} L(u_1 u_2 \dots u_p, q)$$

L'ultima somma svanisce quasi completamente modulo  $p$ , dato che le  $p$ -uple  $(u_1, \dots, u_p)$  che soddisfano  $\sum_{j=1}^p u_j = 1$  possono essere raccolte in gruppi di taglia  $p$  tramite shift; l'unica eccezione è sostituita dalla  $p$ -upla  $(p^{-1}, \dots, p^{-1})$ , per cui

$$N_p = 1 + (-1)^{(p-1)(q-1)/4} L(p^{-p}, q) = 1 + (-1)^{(p-1)(q-1)/4} L(p, q)$$

Il *double counting* effettuato produce dunque l'identità (*Reciprocità Quadratica*)

$$L(p, q) L(q, p) = (-1)^{(p-1)(q-1)/4}$$

Resta escluso il computo di  $L(2, p)$ : notiamo però che, se  $p = 8k + 1$ ,  $-1$  è residuo biquadratico (detto  $g$  un generatore di  $(\mathbb{Z}/p\mathbb{Z})^*$ , si ha  $g^{8k} = 1$ ,  $g^{4k} = -1$ ), e per l'identità

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

$2$  risulta residuo quadratico, come pure  $-1$  in virtù del fatto che  $p \equiv 1 \pmod{4}$ ; dalla moltiplicatività del simbolo di Legendre segue che  $-2$  è pure residuo quadratico. Se  $p \equiv 3 \pmod{8}$  si ha

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

$-2$  risulta dunque il quadrato di  $\pm 2^{(p+1)/4}$ , mentre  $-1$  non è residuo quadratico. Se  $p = 8k + 5$ ,  $L(-1, p) = 1$ , alché, per la moltiplicatività di  $L$  e l'identità

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

si ha che  $2$  non è residuo quadratico (se lo fosse  $-1$  dovrebbe essere residuo biquadratico, ma  $-1 = g^{4k+2}$  è una potenza non multipla di  $4$  di un generatore, da cui un assurdo). In ultima analisi, se  $p = 8k + 7$

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

onde per cui

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

In sintesi:

$$L(-1, p) = (-1)^{\frac{p-1}{2}}$$

$$L(2, p) = (-1)^{\frac{p^2-1}{8}}$$

$$L(-2, p) = (-1)^{\frac{(p-1)(p-3)}{8}}$$

Definendo il simbolo di Jacobi come estensione moltiplicativa del simbolo di Legendre

$$J(a, p) = L(a, p)$$

$$J(a, q_1 q_2) = L(a, q_1) L(a, q_2)$$

non è difficile provare che per due interi dispari  $n$  ed  $m$  si ha pure

$$J(n, m) J(m, n) = (-1)^{(n-1)(m-1)/4}$$

$$J(2, n) = (-1)^{(n^2-1)/8}$$

e la periodicità

$$J(n + km, m) = J(n, m)$$

è conservata. E' possibile estendere ulteriormente il simbolo di Jacobi rimuovendo la condizione sulla parità degli argomenti; ciò che si ottiene è il simbolo di Kronecker, per cui

$$K\left((-1)^{(p-1)/2}, 2\right) = K(2, p) = L(2, p)$$

□

**Lemma 4.3.**

$$1 = L(-k, p) = L(-1, p) \cdot L(k, p) \iff \begin{cases} p \equiv 1 \pmod{4} & L(p, k) = 1 \\ p \equiv 3 \pmod{4}, k \equiv 1 \pmod{4} & L(p, k) = 1 \end{cases}$$

*Dimostrazione.* Nel caso in cui  $k$  sia pari, si sostituisca  $k + p$  in sua vece. Tutto quel che segue è conseguenza della moltiplicatività del simbolo di Legendre e della legge di reciprocità quadratica. □

## 5 Lemma di unicità

**Teorema 5.1.** *Se un primo  $p$  è esprimibile nella forma  $a^2 + kb^2$  lo è in modo sostanzialmente univoco (a meno di cambiamenti di segno di  $a$  oppure  $b$ ).*

*Dimostrazione.* Posto  $z = a + b\sqrt{-k}$  si ha  $p = z\bar{z}$ . Ma  $z$  non può che essere irriducibile nell'anello  $\mathbb{Z}[\sqrt{-k}]$ , avendo per norma un primo di  $\mathbb{Z}$ , segue che non esistono altre possibili scritture  $p = w\bar{w}$  a indurre  $p = c^2 + kd^2$ . □

Si noti pure come quest'argomento sia intimamente connesso con la congettura “*esistono infiniti primi nella forma  $m^2 + 1$* ”. Un numero nella forma  $m^2 + 1$ , con  $m$  pari, ammette divisori primi solo e soltanto nella forma  $4k + 1$  ( $m^2 + 1 = kp$  con  $p \equiv 3 \pmod{4}$  implica  $L(-1, p) = 1$ , assurdo). Indicizzati con  $\{q_i\}_{i=1}^{+\infty}$  i primi in tale forma, e denotando con  $U_i$  e  $V_i$  ( $U_i < V_i = q_i - U_i$ ) i più piccoli interi positivi nelle stesse classi di equivalenza  $\pmod{q_i}$  delle due radici di  $-1$  in  $(\mathbb{Z}/q_i\mathbb{Z})^*$ , si ha

$$\exists! i : m \equiv \pm U_i \pmod{q_i} \iff (m^2 + 1) \text{ primo}$$

e la congettura che esistano infiniti primi nella forma  $m^2 + 1$  (con  $m$  pari) equivale al fatto che esistano infiniti interi pari  $2k$  per cui

$$\frac{d^{2k}}{dx^{2k}} \left( \sum_{n \geq 1} x^{2n} - \sum_{q_i} \frac{x^{U_i} + x^{V_i}}{1 - x^{q_i}} \right) \Big|_{x=0} = 0$$

Sventuratamente il naturale discorso sulla densità dei coefficienti nulli non è risolutivo, in quanto

$$\prod_{p=1(4)} \left( 1 - \frac{2}{p} \right) \leq \prod_{p=1(4)} \left( 1 - \frac{1}{p} \right) \leq c \cdot \left( \lim_{M \rightarrow +\infty} \sum_{n=1}^M \frac{1}{n} \right)^{-1} = 0$$

## 6 Metodo di discesa

Abbiamo visto che  $L(-k, p) = 1$  è condizione necessaria affinché un primo  $p$  sia esprimibile in forma canonica, ma è anche condizione sufficiente? In generale, purtroppo no, ma il metodo di discesa ci chiarirà le idee. Se  $-k$  è residuo quadratico in  $\mathbb{Z}/p\mathbb{Z}$  esistono tre interi  $a_1, b_1 = 1$  e  $c_1$  che soddisfano

$$a_1^2 + k b_1^2 = c_1 p \quad |a_1|, |b_1| < p/2, \quad c_1 < p$$

Reinterpretando quanto appena scritto modulo  $c_1$  otteniamo

$$a_2^2 + k b_2^2 = c_1 c_2$$

E per la moltiplicatività della norma sui complessi

$$\left( \frac{a_1 a_2 + k b_1 b_2}{c_1} \right)^2 + k \left( \frac{b_1 a_2 - a_1 b_2}{c_1} \right)^2 = c_2 p$$

Condizione sufficiente affinché si verifichi  $c_2 < c_1$  è che sia  $k \leq 3$ :

$$\begin{aligned} L(-1, p) = 1 &\Leftrightarrow p \equiv 1 \pmod{4} &\Leftrightarrow p = a^2 + b^2 \\ L(-2, p) = 1 &\Leftrightarrow p \equiv 1, 3 \pmod{8} &\Leftrightarrow p = a^2 + 2b^2 \\ L(-3, p) = 1 &\Leftrightarrow p \equiv 1 \pmod{3} &\Leftrightarrow p = a^2 + 3b^2 \end{aligned}$$

## 7 Teorema di Bambah-Chowla

**Teorema 7.1.** *Esiste una costante positiva  $C$  tale che, comunque scelto un numero naturale  $u$ , nell'intervallo  $[u, u + C u^{1/4}]$  è possibile rinvenire un intero che è somma di due quadrati.*

*Dimostrazione.* Senza perdita di generalità possiamo assumere che  $u$  non sia un quadrato: se lo fosse,  $u + 1$  sarebbe somma di due quadrati. Scegliamo dunque un intero  $m$  tale che

$$m < \sqrt{u} < m + 1$$

e un numero reale positivo  $\lambda$  che realizzi

$$m^2 + \lambda^2 = u$$

in modo che il punto  $(m, \lambda)$  appartenga alla circonferenza centrata nell'origine avente raggio  $\sqrt{u}$ . Preso successivamente un intero  $n$  tale che

$$n - 1 \leq \lambda < n$$

si ha

$$m^2 + n^2 \leq m^2 + (\lambda + 1)^2 = u + 2\lambda + 1$$

Ma  $\lambda$  verifica

$$\lambda^2 = u - m^2 < u - (\sqrt{u} - 1)^2 = 2\sqrt{u} - 1 < 2\sqrt{u}$$

perciò si ha  $\lambda < \sqrt{2} u^{1/4}$  e

$$2\lambda + 1 < 2^{3/2} u^{1/4} + 1 < 3 u^{1/4}$$

appena  $u \geq 1154$ , in tal caso

$$m^2 + n^2 < u + 3 u^{1/4}$$

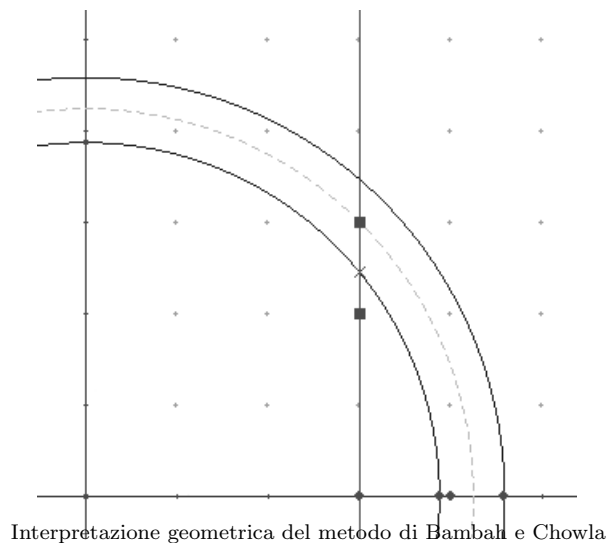
e quando  $u < 1154$  vale la disuguaglianza più debole

$$m^2 + n^2 < u + 4 u^{1/4}$$

□

Il metodo di Bambah e Chowla è di semplice interpretazione geometrica e di facile generalizzazione: non è difficile provare, ad esempio, che nell'intervallo  $[u, u + 5 u^{1/4}]$  vi è sempre un intero della forma  $a^2 + 2b^2$ , e che

$$\forall k \quad \exists C_k > 0 : \forall x \in \mathbb{N} \quad \exists (a, b) \in \mathbb{N}^2 : (a^2 + k b^2) \in [x, x + C_k x^{1/4}]$$



Interpretazione geometrica del metodo di Bambah e Chowla

Nonostante la natura elementare del metodo, al momento non sono note stime migliori (per una panoramica sul problema, anche attraverso metodi analitici, si veda Halberstam [10]).

## 8 Radici quadrate in $(\mathbb{Z}/p\mathbb{Z})^*$

L'estetica e l'utilità del metodo di discesa sono indubbie, ma come determinare la radice quadrata di un certo  $a \in (\mathbb{Z}/p\mathbb{Z})^*$  che realizzi  $L(a, p) = a^{(p-1)/2} = 1$ ? Per  $p \equiv 3 \pmod{4}$ , detto  $b = a^{(p+1)/4}$ , si ha

$$b^2 = a^{(p+1)/2} = a L(a, p) = a$$

e il gioco è fatto. Analogamente (o quasi) per  $p \equiv 5 \pmod{8}$  si consideri  $b = a^{(p+3)/8}$ :

$$b^4 = a^{(p+3)/2} = a^2 L(a, p) = a^2$$

dunque  $b = \pm\sqrt{a}$  oppure  $b = \pm\sqrt{-a}$ , e, a patto di disporre di una radice quadrata di  $-1$  in  $(\mathbb{Z}/p\mathbb{Z})^*$  (che esiste in quanto  $p \equiv 5 \pmod{8} \Rightarrow p \equiv 1 \pmod{4} \Rightarrow L(-1, p) = 1$ ), la questione è risolta anche in questo caso. D'altro canto per il teorema di Wilson

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

Negli altri casi, si prenda un  $b$  tale che  $L(b^2 - 4a, p) = -1$ , per cui  $q(x) = x^2 + bx + a$  risulti irriducibile su  $\mathbb{F}_p$  dando origine al campo finito

$$\mathbb{K} \simeq \mathbb{F}_{p^2} \simeq \mathbb{F}_p[x]/(q(x))$$

Sia ora  $\zeta$  una radice di  $q(x)$  in  $\mathbb{K}$ . Per l'automorfismo di Frobenius

$$\zeta^2 + b\zeta + a = 0 \iff (\zeta^2 + b\zeta + a)^p = 0 \iff \zeta^{2p} + b\zeta^p + a = 0$$

anche  $\zeta^p$  è radice, e per il teorema di Viète risulta

$$\zeta \cdot \zeta^p = \zeta^{p+1} = a \quad \sqrt{a} = \zeta^{(p+1)/2}$$

E' sufficiente dunque considerare come agisce la mappa di moltiplicazione per  $x$  nell'anello  $\mathbb{K}$

$$M_x = \begin{pmatrix} 0 & -a \\ 1 & -b \end{pmatrix}$$

per poter concludere

$$\sqrt{a} = e_1^T M_x^{(p+1)/2} e_1$$

Ove l'esponenziazione matriciale richiede al più  $8 \log_2(p)$  moltiplicazioni in  $(\mathbb{Z}/p\mathbb{Z})^*$ . Per dettagli ed approfondimenti si veda il Menezes-Oorschot-Vanstone[3].

## 9 Prodotto triplo di Jacobi

**Teorema 9.1.** *Per ogni numero complesso  $x$  di modulo strettamente minore di 1 e per qualunque numero complesso  $a$  non nullo si ha*

$$\prod_{n \geq 1} (1 - x^{2n})(1 + a x^{2n-1})(1 + a^{-1} x^{2n-1}) = \sum_{n \geq 0} a^n x^{n^2}$$

*Dimostrazione.* Consideriamo la funzione

$$F(a) = \prod_{n \geq 1} (1 + a^2 x^{2n-1})(1 + a^{-2} x^{2n-1})$$

per proprietà telescopica è evidente che  $\frac{F(a)}{F(ax)} = a^2 x$ , per cui, posto

$$G(a) = F(a) \prod_{n \geq 1} (1 - x^{2n})$$

si ha

$$G(a) = a^2 x G(ax)$$

Per definizione  $G$  risulta essere una funzione pari, preso dunque il suo sviluppo di Laurent

$$G(a) = \sum_{m=-\infty}^{+\infty} k_m a^{2m}$$

per l'equazione funzionale riportata deve verificarsi

$$k_m = k_{m-1} x^{2m-1}$$

ossia

$$a_m = k_0 x^{m^2} \quad G(a) = k_0 \sum_{m=-\infty}^{+\infty} x^{m^2} a^{2m}$$

L'unico problema è la determinazione di  $k_0$ : passando ai logaritmi e considerando le serie di Taylor in  $x$  si ha

$$\log(k_0) + \log \left( 1 + \sum_{n \geq 1} x^{n^2} (a^{2n} + a^{-2n}) \right) = - \sum_{m \geq 1} \sum_{n \geq 1} \frac{1}{m} (x^{2nm} + (-a^2 x^{2n-1})^m + (-a^{-2} x^{2n-1})^m)$$

Il membro destro della precedente difetta di termine noto, onde per cui dev'essere

$$\log(k_0) = 0 \implies k_0 = 1$$

□

Muniti di questo potente strumento possiamo dimostrare, senza eccessiva fatica, che

•

$$r_1(n) = 4(\chi_4 * 1)(n) = 4(d_{1,4}(n) - d_{3,4}(n))$$

•

$$r_2(n) = 2(\chi_8 * 1)(n) = 2(d_{1,8}(n) + d_{3,8}(n) - d_{5,8}(n) - d_{7,8}(n))$$

ove

$$r_k(n) = \# \{ (a, b) \in \mathbb{Z}^2 : n = a^2 + k b^2 \}$$

$$d_{c,d}(n) = \sum_{d|n, d \equiv c(d)} 1$$

$$\chi_4(n) = \begin{cases} 1 & \text{se } n \equiv 1(4) \\ -1 & \text{se } n \equiv -1(4) \\ 0 & \text{se } n \equiv 0(2) \end{cases}$$

$$\chi_8(n) = \begin{cases} 1 & \text{se } n \equiv 1, 3(8) \\ -1 & \text{se } n \equiv 5, 7(8) \\ 0 & \text{se } n \equiv 0(2) \end{cases}$$

## 10 Identità di Jacobi e Lorenz

Consideriamo l'identità provata nel paragrafo precedente:

$$\prod_{n \geq 1} (1 - x^{2n})(1 + ax^{2n-1})(1 + a^{-1}x^{2n-1}) = \sum_{n=-\infty}^{+\infty} a^n x^{n^2}$$

sostituendo  $-a^2x$  in vece di  $a$ ,  $x$  in vece di  $x^2$  e moltiplicando per  $a$  abbiamo

$$(a - a^{-1}) \prod_{n \geq 1} (1 - a^2 x^n)(1 - a^{-2} x^n)(1 - x^n) = \sum_{n=-\infty}^{+\infty} (-1)^n a^{2n+1} x^{(n^2+n)/2}$$

Separando coefficienti pari e dispari ed utilizzando nuovamente il prodotto triplo abbiamo

$$\begin{aligned} & \sum_{n=-\infty}^{+\infty} a^{4n+1} x^{2n^2+n} - \sum_{n=-\infty}^{+\infty} a^{4n-1} x^{2n^2-n} = \\ & = a \prod_{n \geq 1} (1 + a^4 x^{4n-1})(1 + a^{-4} x^{4n-3})(1 - x^{4n}) - a^{-1} \prod_{n \geq 1} (1 + a^{-4} x^{4n-1})(1 + a^4 x^{4n-3})(1 - x^{4n}) \end{aligned}$$

Differenziando rispetto ad  $a$ , ponendo  $a = 1$  e dividendo per 2 abbiamo

$$\prod_{n \geq 1} (1 - x^n)^3 = \left\{ 1 - 4 \sum_{n \geq 1} \frac{x^{4n-3}}{1 + x^{4n-3}} - \frac{x^{4n-1}}{1 + x^{4n-1}} \right\} \prod_{n \geq 1} (1 + x^{4n-1})(1 + x^{4n-3})(1 - x^{4n})$$

Dividendo ambo i membri per

$$\begin{aligned} \prod_{n \geq 1} (1 + x^n)^2 (1 - x^n) &= \prod_{n \geq 1} (1 + x^n)(1 - x^{2n}) = \prod_{n \geq 1} (1 + x^{2n})(1 - x^{2n})(1 + x^{2n-1}) = \\ &= \prod_{n \geq 1} (1 + x^{4n-1})(1 + x^{4n-3})(1 - x^{4n}) \end{aligned}$$

si ottiene

$$\prod_{n \geq 1} \left( \frac{1 - x^n}{1 + x^n} \right)^2 = 1 - 4 \sum_{n \geq 1} \frac{x^{4n-3}}{1 + x^{4n-3}} - \frac{x^{4n-1}}{1 + x^{4n-1}}$$

ma

$$\prod_{n \geq 1} \frac{1 - x^n}{1 + x^n} = \prod_{n \geq 1} \frac{(1 - x^{2n})(1 - x^{2n-1})}{1 + x^n} = \prod_{n \geq 1} (1 - x^n)(1 - x^{2n-1}) = \prod_{n \geq 1} (1 - x^{2n})(1 - x^{2n-1})^2 = \sum_{n=-\infty}^{+\infty} (-1)^n x^{n^2}$$

Cambiando di segno la  $x$  otteniamo dunque

$$\left( \sum_{n=-\infty}^{+\infty} x^{n^2} \right)^2 = 1 + 4 \sum_{n \geq 1} \frac{x^{4n-3}}{1 - x^{4n-3}} - \frac{x^{4n-1}}{1 - x^{4n-1}}$$

la cui interpretazione combinatorica è

$$r_1(n) = 4(d_{1,4}(n) - d_{3,4}(n))$$

Fattorizzando  $n$  come  $n = \prod p_i^{\alpha_i} \prod q_j^{\beta_j}$ , ove  $p_i = 1(4)$  e  $q_j = 3(4)$ , non è difficile convincersi del fatto che  $r_1/4$  sia una funzione moltiplicativa. L'identità  $d_{1,4}(n) - d_{3,4}(n) = (\chi_4 * 1)(n)$  va dunque testata solo sulle potenze dei primi, dove è banale. Incidentalmente, si noti come

$$\prod_{n \geq 1} (1 + x^n)^2 (1 - x^n) = \prod_{n \geq 1} (1 + x^{4n-1})(1 + x^{4n-3})(1 - x^{4n}) = \frac{1}{2} \sum_{n \in \mathbb{Z}} x^{(n^2+n)/2}$$

sia la  $q$ -serie associata ai numeri triangolari (è sufficiente sostituire  $x$  ad  $a$  e  $x$  ad  $x^2$  nell'usuale prodotto triplo); definito  $t(n)$  come

$$t(n) = \# \left\{ a \geq b \geq 1 : n = \frac{a^2 + a}{2} + \frac{b^2 + b}{2} \right\}$$

si ha

$$t(n) = d_{1,4}(4n+1) - d_{3,4}(4n+1) = (\chi_4 * 1)(4n+1)$$

in quanto

$$n = \frac{a^2 + a}{2} + \frac{b^2 + b}{2} \iff 4n + 1 = (a + b + 1)^2 + (a - b)^2$$

Occupiamoci ora del caso  $k = 2$ . Seguendo quanto proposto da Varouchas [14], poniamo

$$\begin{aligned} \Psi(x|q) &= \sum_{n \geq 0} x^n q^{n^2} = \prod_{n \geq 1} (1 - q^{2n})(1 + x q^{2n-1})(1 + x^{-1} q^{2n-1}) \\ \Phi(x) &= \Phi(x|q) = \sum_{m, n \in \mathbb{Z}} x^{2m+2n+1} q^{4m^2+4n^2+m+3n} \end{aligned}$$

Abbiamo immediatamente

$$\begin{aligned} \Phi(x) &= x \Psi(x^2 q | q^4) \Psi(x^2 q^3 | q^4) \\ \Phi(x) &= x \prod_{n \geq 1} (1 + x^2 q^{8n-3})(1 + x^{-2} q^{8n-5})(1 + x^2 q^{8n-1})(1 + x^{-2} q^{8n-7})(1 - q^{8n})^2 \\ \Phi(1) &= \prod_{n \geq 1} (1 + q^{2n-1})(1 - q^{8n})^2 \end{aligned}$$

Passando alla derivata logaritmica

$$\Theta(q) = \frac{\Phi'(1)}{\Phi(1)} = 1 - 2 \sum_{n \geq 0} (-1)^{n(n-1)/2} \frac{q^{2n+1}}{1 + q^{2n+1}}$$

Ponendo  $r = m + n$  e  $s = m - n$  nella prima definizione della  $\Phi$  si ha

$$\begin{aligned} \Phi(x) &= \sum_{r=s(2)} x^{2r+1} q^{2r^2+2s^2+2r+s} \\ \Phi(x^{-1}) &= \sum_{r=s(2)} x^{-2r-1} q^{2r^2+2s^2+2r+s} \end{aligned}$$

e sostituendo  $r$  in vece di  $-r - 1$

$$\begin{aligned} \Phi(x^{-1}) &= \sum_{r \neq s(2)} x^{2r+1} q^{2r^2+2s^2+2r+s} \\ \Phi(x) - \Phi(x^{-1}) &= \sum_{r, s \in \mathbb{Z}} (-1)^{r+s} x^{2r+1} q^{2r^2+2s^2+2r+s} = x \Psi(-x^2 q^2 | q^2) \Psi(-q | q^2) \\ \Phi(x) - \Phi(x^{-1}) &= x \prod_{n \geq 1} (1 - x^2 q^{4n})(1 - x^{-2} q^{4n-4})(1 - q^{4n-1})(1 - q^{4n-3})(1 - q^{4n})^2 \\ \Phi(x) - \Phi(x^{-1}) &= (x - x^{-1}) \prod_{n \geq 1} (1 - x^2 q^{4n})(1 - x^{-2} q^{4n})(1 - q^{2n-1})(1 - q^{4n})^2 \end{aligned}$$

Ora

$$\begin{aligned} \left. \frac{\Phi(x) - \Phi(x^{-1})}{x - x^{-1}} \right|_{x=1} &= \Phi'(1) = \prod_{n \geq 1} (1 - q^{4n})^4 (1 - q^{2n-1}) \\ \prod_{n \geq 1} (1 - q^{4n})^4 (1 - q^{2n-1}) &= \frac{\Psi'(1)}{\Psi(1)} \Psi(1) = \Theta(q) \prod_{n \geq 1} (1 + q^{2n-1})(1 - q^{8n})^2 \end{aligned}$$

per cui

$$\Theta(q) = \prod_{n \geq 1} \frac{(1 - q^{4n})^4 (1 - q^{2n-1})}{(1 - q^{8n})^2 (1 + q^{2n-1})} = \prod_{n \geq 1} \frac{(1 + q^{2n})^2 (1 - q^{2n})^2 (1 - q^{2n-1})}{(1 + q^{4n})^2 (1 + q^{2n-1})}$$

$$\Theta(q) = \prod_{n \geq 1} \frac{(1 + q^{4n-2})^2 (1 + q^n)^2 (1 - q^n)^2 (1 - q^{2n-1})}{(1 + q^{2n-1})} = \prod_{n \geq 1} (1 + q^{4n-2})^2 (1 + q^{2n}) (1 + q^n) (1 - q^n)^2 (1 - q^{2n-1})$$

$$\Theta(q) = \prod_{n \geq 1} (1 + q^{4n-2})^2 (1 + q^{2n}) (1 - q^{2n}) (1 - q^n) (1 - q^{2n-1}) = \prod_{n \geq 1} (1 + q^{4n-2})^2 (1 + q^{2n}) (1 - q^{2n})^2 (1 - q^{2n-1})^2$$

A seguito di queste riduzioni risulta

$$\Theta(-q) = \Psi(1|q)\Psi(1|q^2) = \sum_{m \in \mathbb{Z}} q^{m^2} \sum_{n \in \mathbb{Z}} q^{2n^2}$$

$$\sum_{m, n \in \mathbb{Z}} q^{m^2 + 2n^2} = 1 + 2 \sum_{u \geq 0} (-1)^{u(u-1)/2} \frac{q^{2u+1}}{1 - q^{2u+1}}$$

e finalmente, considerando le classi residue modulo 8 degli esponenti che compaiono nel membro destro:

$$r_2(n) = 2(d_{1,8} + d_{3,8} - d_{5,8} - d_{7,8})(n)$$

Nuovamente, fattorizzando  $n$  come  $n = \prod p_i^{\alpha_i} \prod q_j^{\beta_j} \prod P_k^{\gamma_k} \prod Q_l^{\delta_l}$ , ove  $p_i = 1(8), q_j = 3(8), P_k = 5(8), Q_l = 7(8)$ , non è difficile provare la moltiplicatività della funzione aritmetica  $r_2/2$  (ricordiamo che per il teorema di struttura dei gruppi abeliani gli elementi di  $(\mathbb{Z}/8\mathbb{Z})^*$  si possono esprimere come  $\pm 5^t$  con  $t = 0, 1$ ), onde per cui l'identità

$$(d_{1,8} + d_{3,8} - d_{5,8} - d_{7,8}) = (\chi_8 * 1)$$

va verificata solo sulle potenze dei primi, per cui è banale. Con metodi del tutto analoghi (facciamo riferimento agli articoli di Ewell[2] e Hirschhorn[7]) è possibile provare anche

$$\left( \sum_{n \in \mathbb{Z}} q^{n^2} \right)^4 = 1 + 8 \sum_{n \geq 1, n \neq 0(4)} \frac{n q^n}{1 - q^n} \iff \# \{ (a, b, c, d) \in \mathbb{Z}^4 : n = a^2 + b^2 + c^2 + d^2 \} = 8 \sum_{d|n, d \neq 0(4)} d$$

$$\left( \sum_{m \in \mathbb{Z}} q^{m^2} \right) \left( \sum_{n \in \mathbb{Z}} q^{3n^2} \right) = 1 + 2 \sum_{n \geq 1} \left( \frac{q^{3n-1}}{1 - q^{3n-1}} - \frac{q^{3n-2}}{1 - q^{3n-2}} \right) \iff r_3(n) = 2(d_{1,3}(n) - d_{2,3}(n)) = 2(\chi_3 * 1)(n)$$

## 11 Numero di rappresentazioni $r_k(n)$ sotto una differente ottica

Abbiamo visto come il prodotto triplo di Jacobi sia un potente strumento per il calcolo del numero di rappresentazioni da parte di semplici forme quadratiche; tuttavia simili metodi di calcolo sono difficilmente generalizzabili, è per questo necessario soffermarci su un'interpretazione meramente algebrica del problema. Supponiamo di avere la fattorizzazione (in  $\mathbb{Z}$ )

$$n = \prod P_i^{\alpha_i} \prod Q_j^{\beta_j}$$

ove i  $P_i$  ammettano decomposizione  $P_i = p_i \bar{p}_i$  nell'anello  $\mathbb{Z}[\sqrt{-k}]$ , mentre i  $Q_i$  non l'ammettano. Poiché le rappresentazioni di  $n$  come

$$n = a^2 + k b^2$$

sono in biezione con le decomposizioni

$$n = (a + b\sqrt{-k})(a - b\sqrt{-k}) = u\bar{u} \quad u \in \mathbb{Z}[\sqrt{-k}]$$

è evidente che, se  $n$  è esprimibile in forma canonica, dev'essere,  $\forall j, \beta_j \equiv 0 \pmod{2}$ .

Nei casi  $k = 1, 2, 3$  abbiamo visto come

$$L(-k, p) = 1 \implies p = a^2 + kb^2$$

$$L(-k, p) = -1 \implies p \neq a^2 + kb^2$$

per cui, vista la sostanziale univocità della rappresentazione  $p = a^2 + kb^2$  nel primo caso riportato, si ha

$$r_k(n) = \#\mathcal{U}_{\mathbb{Z}[\sqrt{-k}]} \cdot d\left(\prod P_i^{\alpha_i}\right) = \#\mathcal{U}_{\mathbb{Z}[\sqrt{-k}]} \cdot \prod(1 + \alpha_i)$$

dove il primo fattore del membro destro è la cardinalità del gruppo delle unità dell'anello in pedice. Il computo delle rappresentazioni è dunque ricondotto allo studio di quali primi di  $\mathbb{Z}$  siano o meno esprimibili in forma canonica; questo anche nel caso in cui  $\mathbb{Z}[\sqrt{-k}]$  non sia a fattorizzazione unica (*UFD*).

## 12 Caso $k = 4$

$$r_4(n) = 2(d_{1,4}(n) - d_{3,4}(n)) = 2(\chi_4 * 1)(n)$$

In quanto per ogni intero dispari  $n$  che verifichi

$$n = x^2 + z^2$$

si ha  $x \not\equiv z \pmod{2}$ ; per ogni intero  $n$  congruo a 2 modulo 4 non vi sono possibili rappresentazioni; per ogni intero nella forma  $n = 4k$  è sufficiente ricondursi alle rappresentazioni di  $k$  come  $a^2 + b^2$ .

## 13 Prime stranezze, caso $k = 5$

Per  $k = 5$  la condizione  $L(-5, p) = 1$  non è più sufficiente a garantire  $p = a^2 + 5b^2$ . Ciò non ci stupisce, infatti  $p = a^2 + 5b^2$  implica  $p \equiv a^2 + b^2 \equiv 1 \pmod{4}$ , a sua volta equivalente a  $L(-1, p) = +1$ . Una prima stranezza fa la sua comparsa all'interno della teoria: ogni primo congruo a 3 oppure a 7 modulo 20, sebbene ammetta  $-5$  come residuo quadratico, non è esprimibile in forma canonica. Per far luce sull'argomento è necessario lo studio di certe forme quadratiche.

## 14 Forme quadratiche

Una forma quadratica

$$f(x, y) = ax^2 + bxy + cy^2$$

viene detta *primitiva* se  $\gcd(a, b, c) = 1$ . Un intero  $m$  è *rappresentato* da tale forma quadratica se l'equazione

$$m = f(x, y)$$

ammette una soluzione intera in  $x$  e  $y$ ;  $m$  è inoltre detto *propriamente rappresentato* se  $x$  ed  $y$  risultano liberi da fattori comuni. Diciamo inoltre che due forme  $f(x, y)$  e  $g(x, y)$  sono equivalenti se esistono 4 interi  $p, q, r, s$  tali che

$$f(x, y) = g(px + qy, rx + sy) \quad ps - qr = \pm 1$$

Abbiamo  $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{GL}(2, \mathbb{Z})$ , da cui segue che l'equivalenza a meno di omotetie tra forme quadratiche è a tutti gli effetti una relazione di equivalenza, che diciamo *impropria* nel caso in cui  $ps - qr = -1$ . Una forma  $f(x, y)$  rappresenta propriamente un intero  $m$  se e solo se risulta propriamente equivalente ad una forma

$$mx^2 + bxy + cy^2$$

per una qualche coppia di interi  $b$  e  $c$ .

Supponiamo infatti che sia  $f(p, q) = m$  con  $\text{gcd}(p, q) = 1$ . Possiamo allora determinare  $r$  ed  $s$  in modo tale che si abbia  $ps - qr = 1$ , e a questo punto

$$f(px + ry, qx + sy) = f(p, q)x^2 + (f(p, s) + f(r, q))xy + f(r, s)y^2 = mx^2 + bxy + cy^2$$

Viceversa, presa  $f(x, y) = mx^2 + bxy + cy^2$ , si ha banalmente  $f(1, 0) = m$ .

Il *discriminante* della forma  $ax^2 + bxy + cy^2$  è definito come  $D = b^2 - 4ac$ ; è semplice provare che forme equivalenti hanno il medesimo discriminante. Si noti inoltre che

$$4af(x, y) = (2ax + by)^2 - Dy^2$$

e che

$$\begin{aligned} b = 0(2) &\Leftrightarrow D = 0(4) \\ b = 1(2) &\Leftrightarrow D = 1(4) \end{aligned}$$

**Teorema 14.1.** *Sia  $D$  un intero congruo a 0 o 1 modulo 4, ed  $m$  un intero dispari primo con  $D$ .  $m$  è propriamente rappresentato da una forma primitiva di discriminante  $D$  se e solo se  $D$  è un residuo quadratico modulo  $m$ .*

*Dimostrazione.* Se  $f(x, y)$  rappresenta propriamente  $m$  possiamo assumere  $f(x, y) = mx^2 + bxy + cy^2$ , alché  $D = b^2 - 4mc$  e  $D \equiv b^2 \pmod{m}$ . Viceversa, supponiamo  $D \equiv b^2 \pmod{m}$ . Poiché  $m$  è dispari, a meno di rimpiazzare  $b$  con  $b + m$  possiamo supporre che  $D$  e  $b$  abbiano la stessa parità, in modo tale che  $D \equiv 0, 1 \pmod{4}$  implichi  $D \equiv b^2 \pmod{4m}$ . Ciò significa  $D = b^2 - 4mc$  per un qualche  $c$ , dunque  $mx^2 + bxy + cy^2$  rappresenta propriamente  $m$  ed ha discriminante  $D$ , inoltre i coefficienti sono primi tra loro in quanto  $m$  è primo con  $D$ .  $\square$

Questo teorema ha un corollario di fondamentale importanza nella nostra trattazione:

**Teorema 14.2.** *Sia  $n$  un intero e  $p$  un primo dispari che non divide  $n$ . Allora  $L(-n, p) = 1$  se e soltanto se  $p$  è propriamente rappresentato da una forma primitiva con discriminante  $-4n$ .*

*Dimostrazione.* Segue banalmente dal teorema precedente, in quanto  $-4n$  è un residuo quadratico modulo  $p$  se e soltanto se lo è  $-n$ .  $\square$

Una forma primitiva definita positiva ( $D < 0$ , *ellittica*) è detta *ridotta* se

$$|b| \leq a \leq c$$

e

$$b \geq 0$$

se si verifica  $|b| = a$  oppure  $a = c$ .

Un possibile algoritmo di riduzione di una forma quadratica  $ax^2 + bxy + cy^2$  non deve far nient'altro che limitare quanto più possibile il valore assoluto del coefficiente centrale tramite trasformazioni in  $\text{SL}(2, \mathbb{Z})$ :

- se  $c < a$ , si rimpiazzano  $(a, b, c)$  con  $(c, -b, a)$  tramite  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

- se  $b > a$ , si rimpiazzano  $(a, b, c)$  con la forma equivalente  $(a, b_1, c_1)$  tramite  $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ ,  
dove  $b_1 = b + 2at$ ,  $t$  sia scelto in modo tale che si abbia  $b_1 < a$ ,  $c_1$  verifichi  $D = b_1^2 - 4ac_1$

L'algoritmo di riduzione appena esposto ha una gradevole interpretazione geometrica (per le connessioni tra questa interpretazione e l'aritmetica delle forme modulari si veda Karumbidza [12]): detti  $\zeta$  e  $\bar{\zeta}$  i numeri complessi che soddisfano

$$ax^2 + bxy + cy^2 = a(x - \zeta y)(x - \bar{\zeta} y) \quad \Im(\zeta) \geq 0$$

la condizione  $|b| \leq a \leq c$  (e  $b \geq 0$  se si verifica  $|b| = a$  oppure  $a = c$ ) è equivalente a  $\zeta \in \mathcal{F}$ , ove

$$\mathcal{F} = \left\{ \zeta \in \mathbb{C} : \Re(\zeta) \in \left[-\frac{1}{2}, \frac{1}{2}\right), |\zeta| > 1 \text{ oppure } |\zeta| = 1 \text{ e } \Re(\zeta) \leq 0 \right\}$$

Gli elementi di  $SL(2, \mathbb{Z})$  nella forma

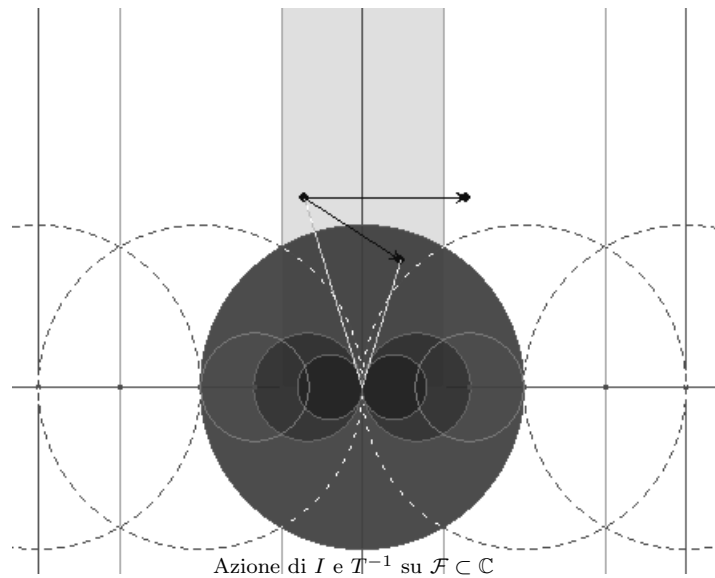
$$T^k = \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix}$$

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

agiscono sui coefficienti di una forma quadratica come riportato nel paragrafo precedente, e sulle radici associate come segue:

$$\begin{aligned} T^k &: \zeta \longrightarrow \zeta - k \\ I &: \zeta \longrightarrow -\zeta^{-1} \end{aligned}$$

Supponiamo che sia  $\zeta$  non sia in  $\mathcal{F}$ : l'immagine di  $\zeta$  secondo un'opportuna traslazione  $T^k$  avrà parte reale compresa tra  $-1/2$  e  $1/2$ . Nel caso in cui questo nuovo  $\zeta$  abbia modulo inferiore ad 1 sarà possibile applicare l'inversione  $I$  per poi, eventualmente, applicare una nuova traslazione e così via. Il processo avrà necessariamente termine per la stretta decrescita del valore assoluto del coefficiente centrale  $|b| = 2a|\Re(\zeta)|$ , comunque intero.



Ecco un esempio di riduzione di una forma quadratica  $ax^2 + bxy + cy^2$  con  $(a, b, c) = (458, 214, 25)$ :

$$(458, 214, 25) \xrightarrow{I} (25, -214, 458) \xrightarrow{T^4} (25, -14, 2) \xrightarrow{I} (2, 14, 25) \xrightarrow{T^{-3}} (2, 2, 1) \xrightarrow{I} (1, -2, 2) \xrightarrow{T} (1, 0, 1)$$

L'algoritmo, in analogia con il computo del massimo comun divisore, ha complessità nell'ordine del logaritmo del più grande coefficiente della forma quadratica.

**Teorema 14.3.** *Ogni forma primitiva definita positiva è propriamente equivalente ad un'unica forma ridotta.*

*Dimostrazione.* Per prima cosa mostriamo che ogni data forma è propriamente equivalente ad una che soddisfi  $|b| \leq a \leq c$ . Tra tutte le forme propriamente equivalenti a quella assegnata, si consideri  $f(x, y) = ax^2 + bxy + cy^2$  tale che il modulo di  $b$  sia il più piccolo possibile. Se  $a < |b|$ , allora

$$g(x, y) = f(x + my, y) = ax^2 + (2am + b)xy + c'y^2$$

è propriamente equivalente ad  $f(x, y)$ . Poiché  $a < |b|$ , possiamo scegliere  $m \in \mathbb{Z}$  tale che  $|2am + b| < |b|$ , che contraddice la minimalità di  $f(x, y)$ . Abbiamo dunque  $a \geq |b|$ , e similmente  $c \geq |b|$ . Se  $a > c$  è necessario scambiare i coefficienti più esterni, trasformazione possibile grazie all'equivalenza propria  $(x, y) \rightarrow (-y, x)$ . La forma risultante soddisfa  $|b| \leq a \leq c$ . Il passo successivo è mostrare che una forma siffatta è propriamente equivalente ad una forma ridotta, ma la forma è già ridotta a meno che non sia  $b < 0$  e  $a = -b$  oppure  $a = c$ . In questi casi eccezionali la forma  $ax^2 - bxy + cy^2$  è ridotta, così dobbiamo solo mostrare che le due forme  $ax^2 \pm bxy + cy^2$  sono propriamente equivalenti:

$$\begin{array}{ll} a = -b & : (x, y) \rightarrow (x + y, y) \quad \text{porta} \quad ax^2 - axy + cy^2 \quad \text{in} \quad ax^2 + axy + cy^2 \\ a = c & : (x, y) \rightarrow (-y, x) \quad \text{porta} \quad ax^2 + bxy + ay^2 \quad \text{in} \quad ax^2 - bxy + ay^2 \end{array}$$

Il passo conclusivo è provare che due differenti forme ridotte non possono essere propriamente equivalenti: se  $f(x, y) = ax^2 + bxy + c^2$  soddisfa  $|b| \leq a \leq c$ , non è difficile provare che

$$f(x, y) \geq (a - |b| + c) \min(x^2, y^2)$$

Segue  $f(x, y) \geq (a - |b| + c)$  a meno che non sia  $xy = 0$ ;  $a$  è dunque il più piccolo intero positivo rappresentato da  $f(x, y)$ , e se  $c > a$ ,  $c$  è il secondo intero positivo più piccolo rappresentato da  $f(x, y)$ . Assumiamo che  $f(x, y) = ax^2 + bxy + cy^2$  sia una forma ridotta che soddisfi la disuguaglianza stretta  $|b| < a < c$ . Si ha che

$$a < c < a - |b| + c$$

sono i tre più piccoli interi positivi rappresentati dalla forma in questione, e da qui non è difficile provare che, supposta  $g(x, y)$  forma ridotta equivalente a  $f(x, y)$ , deve valere

$$g(x, y) = ax^2 \pm bxy + cy^2$$

e condizioni analoghe valgono anche nei casi  $a = |b|$  o  $a = c$ . □

Supponiamo ora che  $ax^2 + bxy + cy^2$  sia una forma quadratica ridotta e definita positiva. Deve aversi

$$\begin{aligned} -D = 4ac - b^2 &\geq 4a^2 - a^2 = 3a^2 \\ a &\leq \sqrt{-D/3} \end{aligned}$$

Esistono dunque un numero finito di coppie  $(a, b)$ , e poiché  $c = (b^2 - D)/(4a)$ , anche un numero finito di scelte per  $c$ . Seguendo la nomenclatura inizialmente fornita da Gauss, diciamo che due forme sono nella stessa *classe* se propriamente equivalenti. Denotando con  $h(D)$  il numero delle classi di forme primitive definite positive di discriminante  $D$  (il numero delle forme ridotte), abbiamo:

**Teorema 14.4.** *Sia  $n$  un intero positivo e  $p$  un intero dispari che non divide  $n$ .  $L(-n, p) = 1$  se e solo se  $p$  è rappresentato da una delle  $h(-4n)$  forme ridotte di discriminante  $-4n$ .*

Un esempio farà luce sulla questione: poniamo  $p = 23$  ed  $n = 7$ . Si ha  $L(-7, 23) = L(23, 7) = L(2, 7) = 1$ , inoltre

$$\sqrt{-7} \equiv \pm 7^6 \equiv \pm 3^3 \equiv \pm 27 \equiv \pm 4 \pmod{23}$$

onde per cui esiste un intero  $u$  che verifica

$$-(4 \cdot 7) = (2 \cdot 4)^2 - 4 \cdot 23 \cdot u$$

Si ha banalmente  $u = 1$ , segue che la forma

$$23x^2 + 8xy + y^2$$

ha discriminante  $-28$  e rappresenta il primo  $23$  per  $(x, y) = (1, 0)$ . Il calcolo della forma ridotta produce

$$(23, 8, 1) \xrightarrow{I} (1, -8, 23) \xrightarrow{T^4} (1, 0, 7)$$

da cui risulta che per  $k = 7$  la forma quadratica canonica  $x^2 + 7y^2$  rappresenta il primo  $23$  quando  $(x, y) = (\pm 4, \pm 1)$ . In sostanza l'algoritmo di riduzione delle forme quadratiche rimpiazza e generalizza il metodo di discesa presentato ad inizio articolo. Notiamo pure che se  $h(-4n) = 1$ , la condizione di reciprocità quadratica coimplica la rappresentabilità di un primo in forma canonica. Sventuratamente, l'identità  $h(-4n) = 1$  è realizzata in uno sparuto numero di casi:

**Teorema 14.5** (Landau).

$$h(-4n) = 1 \iff n = 1, 2, 3, 4, 7$$

*Dimostrazione.* Dapprima supponiamo che  $n$  non sia potenza di un primo. Allora  $n = ac$  con  $\gcd(a, c) = 1$  e  $ax^2 + cy^2$  è una forma ridotta di discriminante  $-4n$ . Se  $n = 2^r$  con  $r \geq 4$ , la forma

$$4x^2 + 4xy + (2^{r-2} + 1)y^2$$

ha coefficienti relativamente primi, è ridotta (in quanto  $4 \leq 2^{r-2} + 1$ ) ed ha discriminante  $-4n$ . In ultima istanza, supponiamo  $n = p^r$  con  $p$  primo dispari. Se  $n + 1$  può essere espresso nella forma  $n + 1 = ac$ , con  $2 \leq a < c$  e  $\gcd(a, c) = 1$ , la forma

$$ax^2 + 2xy + cy^2$$

è ridotta di discriminante  $-4n$ . L'unico caso rimasto in sospeso è quello in cui  $n = p^r$  e  $n + 1 = 2^s$ . Se  $s \geq 6$ , la forma

$$8x^2 + 6xy + (2^{s-3} + 1)y^2$$

ha coefficienti relativamente primi ed è ridotta in quanto  $8 \leq 2^{s-3} + 1$ . Inoltre, se  $s = 4$  notiamo che  $15$  non è potenza di un primo, e per  $s = 5$  un'ispezione diretta comunica che  $h(-4 \cdot 31) = 3$ .  $\square$

## 15 Caso $k = 5$ , giunge chiarezza

Esistono solo due forme quadratiche ridotte di discriminante  $-20$ , per l'esattezza

$$\begin{array}{ll} x^2 + 5y^2 & \text{rappresenta } 1, 9 \in (\mathbb{Z}/20\mathbb{Z})^* \\ 2x^2 + 2xy + 3y^2 & \text{rappresenta } 3, 7 \in (\mathbb{Z}/20\mathbb{Z})^* \end{array}$$

Di conseguenza, per quanto visto sui primi rappresentati da forme quadratiche:

$$\begin{array}{ll} p = x^2 + 5y^2 & \iff p \equiv 1, 9 \pmod{20} \\ p = 2x^2 + 2xy + 3y^2 & \iff p \equiv 3, 7 \pmod{20} \end{array}$$

Inoltre

$$\begin{aligned} \text{(Fermat)} \quad p, q &\equiv 3, 7 \pmod{20} \implies pq = x^2 + 5y^2 \\ \text{(Eulero)} \quad p &\equiv 3, 7 \pmod{20} \implies 2p = x^2 + 5y^2 \end{aligned}$$

Non c'è da stupirsi: posto infatti, per  $z \in \mathbb{C}$ ,  $N(z) = z\bar{z}$ , si ha

$$2x^2 + 2x + 3 = 2N\left(x - \frac{-1 + \sqrt{-5}}{2}\right)$$

$$(2x^2 + 2x + 3)(2z^2 + 2z + 3) = 4N\left(x - \frac{-1 + \sqrt{-5}}{2}\right)N\left(z - \frac{-1 - \sqrt{-5}}{2}\right)$$

$$(2x^2 + 2x + 3)(2z^2 + 2z + 3) = 4N\left(\frac{2xz + x + z + 3}{2} + \sqrt{-5}\frac{x - z}{2}\right) = N((2xz + x + z + 3) + \sqrt{-5}(x - z))$$

$$(2x^2 + 2x + 3)(2z^2 + 2z + 3) = (2xz + x + z + 3)^2 + 5(x - z)^2$$

$$(2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2) = (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2$$

Da ciò non è difficile concludere che, data la fattorizzazione in  $\mathbb{Z}$

$$n = \prod p_i^{\alpha_i} \prod q_j^{\beta_j} \prod R_k^{\gamma_k}$$

dove  $p_i \equiv 1, 9 \pmod{20}$ ,  $q_j = 2$  oppure  $q_j \equiv 3, 7 \pmod{20}$ ,  $L(-5, R_k) = -1$ , a patto che si abbia

$$\forall k \quad R_k \equiv 0 \pmod{2}$$

$$\sum \beta_i \equiv 0 \pmod{2}$$

risulta

$$r_5(n) = 2d_{\{1,9\},20}(n) = 2(\chi_{20} * 1)(n)$$

mentre negli altri casi si verifica banalmente

$$r_5(n) = 0$$

E' a questo punto opportuno, facendo riferimento al Cox[1], introdurre alcuni elementi circa la teoria della composizione di forme e il gruppo delle classi.

## 16 Composizione e gruppo delle classi

Siano  $f(x, y)$  e  $g(x, y)$  due forme primitive definite positive di discriminante  $D$ , allora  $F$ , dello stesso tipo, è detta loro *composizione* se

$$f(x, y)g(x, y) = F(B_1(x, y; z, w), B_2(x, y; z, w))$$

con

$$B_i(x, y; z, w) = a_i xz + b_i xw + c_i yz + d_i yw$$

forme bilineari intere. Con la notazione appena introdotta, si ha

$$a_1 b_2 - a_2 b_1 = \pm f(1, 0)$$

$$a_1 c_2 - a_2 c_1 = \pm g(1, 0)$$

e la composizione si dice *diretta* quando ambedue i segni sono positivi.

**Lemma 16.1.** *Nell'ipotesi che  $f(x, y) = ax^2 + bxy + cy^2$  e  $g(x, y) = a'x^2 + b'xy + c'y^2$  abbiano discriminante  $D$  e soddisfino  $\gcd(a, a', (b + b')/2) = 1$  esiste un unico intero  $B$  modulo  $2aa'$  tale che*

$$B \equiv b \pmod{2a}$$

$$B \equiv b' \pmod{2a'}$$

$$B^2 \equiv D \pmod{4aa'}$$

Con la notazione introdotta, la *composizione di Dirichlet* di  $f(x, y)$  e  $g(x, y)$  è la forma

$$F(x, y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2$$

che risulta diretta, primitiva, definita positiva di discriminante  $D$ .

**Lemma 16.2.** *Sia  $D \equiv 0, 1 \pmod{4}$  un intero negativo, e  $C(D)$  l'insieme delle classi delle forme primitive definite positive di discriminante  $D$ . La composizione di Dirichlet induce un'operazione binaria ben definita su  $C(D)$ , che rende  $C(D)$  un gruppo abeliano finito il cui ordine è il numero di classi  $h(D)$ . Inoltre l'identità in  $C(D)$  è la classe contenente la forma principale*

$$\begin{aligned} x^2 - \frac{D}{4}y^2 & \text{ se } D \equiv 0 \pmod{4} \\ x^2 + xy - \frac{D-1}{4}y^2 & \text{ se } D \equiv 1 \pmod{4} \end{aligned}$$

e l'inversa della classe contenente  $ax^2 + bxy + cy^2$  è la classe contenente  $ax^2 - bxy + cy^2$ .

**Lemma 16.3.** *Una forma ridotta di discriminante  $D$  ha ordine  $\leq 2$  in  $C(D)$  se e solo se  $b = 0$ ,  $a = b$  o  $a = c$ .*

Un piccolo saggio delle conseguenze: un computo diretto mostra che  $C(-164)$  consta di 8 classi, di cui solo una ( $2x^2 + 2xy + 21y^2$ ) di ordine 2. Ciò prova che il gruppo delle classi  $C(-164)$  è  $\mathbb{Z}/8\mathbb{Z}$ .

**Lemma 16.4.** *Sia  $D \equiv 0, 1 \pmod{4}$  un intero negativo, ed  $r$  il numero di primi dispari istinti che dividono  $D$ . Si definisca inoltre  $\mu$  come segue: se  $D \equiv 1 \pmod{4}$ ,  $\mu = r$ , altrimenti, posto  $D = -4n$ ,*

$$\begin{aligned} n & \equiv 3 \pmod{4} & \mu & = r \\ n & \equiv 1, 2 \pmod{4} & \mu & = r + 1 \\ n & \equiv 4 \pmod{8} & \mu & = r + 1 \\ n & \equiv 0 \pmod{8} & \mu & = r + 2 \end{aligned}$$

Il gruppo delle classi  $C(D)$  risulta avere esattamente  $2^{\mu-1}$  elementi di ordine  $\leq 2$ .

## 17 Teoria dei generi

Consideriamo il sottogruppo  $H \subset \ker(\chi) \subset (\mathbb{Z}/D\mathbb{Z})^*$  dove  $H$  è l'insieme di tutti i valori rappresentati dalla forma principale, e  $\chi : (\mathbb{Z}/D\mathbb{Z})^* \rightarrow \pm 1$  è il carattere definito da  $\chi([p]) = L(D, p)$  per  $p \nmid D$  primo.

**Lemma 17.1.** *I valori rappresentati da una data forma  $f(x, y)$  in  $(\mathbb{Z}/D\mathbb{Z})^*$  sono un laterale di  $H$  in  $\ker(\chi)$*

*Dimostrazione.* Semplice conseguenza del fatto che, se  $f(x, y) = ax^2 + 2bxy + cy^2$  è una forma di discriminante  $-4n$  ed  $a$  è primo con  $4n$ , allora

$$af(x, y) = (ax + by)^2 + ny^2$$

implica che i valori di  $f(x, y)$  in  $(\mathbb{Z}/4n\mathbb{Z})^*$  giacciono nel laterale  $[a]^{-1}H$ . □

Il laterale appena definito determina il *genere* cui  $f(x, y)$  appartiene. Poiché tutte le forme in una data classe rappresentano i medesimi interi, assegnare ad ogni classe il laterale di  $H$  rappresentato definisce una mappa

$$\Phi : C(D) \longrightarrow \ker(\chi)/H$$

Un'osservazione cruciale è che  $\Phi$  è un omomorfismo di gruppi: siano  $f(x, y)$  e  $g(x, y)$  due forme di discriminante  $D$  a valori nei laterali  $H'$  ed  $H''$  rispettivamente. Possiamo assumere la loro composizione di Dirichlet  $F(x, y)$  sia definita, cosicché il prodotto di valori rappresentati da  $f(x, y)$  e  $g(x, y)$  risulta rappresentato da  $F(x, y)$ .  $H'H''$  è dunque il laterale rappresentato dalla composizione di  $f(x, y)$  e  $g(x, y)$  e questo prova che  $\Phi$  sia un omomorfismo. Ora, assumendo usualmente  $D \equiv 0, 1 \pmod{4}$ ,

**Lemma 17.2.** *Ogni genere di forme di discriminante  $D$  consta dello stesso numero di classi.*

*Dimostrazione.* Conseguenza del fatto che le fibre di un omomorfismo hanno lo stesso numero di elementi. Inoltre, poiché il sottogruppo  $H$  contiene tutti i quadrati in  $(\mathbb{Z}/D\mathbb{Z})^*$ , ogni elemento in  $\ker(\chi)/H$  ha ordine  $\leq 2$ : ciò implica, per il teorema di struttura dei gruppi abeliani finiti, che sia  $\ker(\chi)/H \simeq \{\pm 1\}^m$ , e che l'immagine di  $\Phi$  sia un sottogruppo di  $\ker(\chi)/H$  di ordine  $2^u$ .  $\square$

Segue che :

**Lemma 17.3.** *Il numero di generi di forme di discriminante  $D$  è una potenza di 2.*

E' vero inoltre che

**Lemma 17.4.** *Esistono  $2^\mu$  generi di forme con discriminante  $D$ , e il genere principale (ossia quello contenente la forma principale) consista delle classi in  $C(D)^2$ , il sottogruppo dei quadrati nel gruppo delle classi. Segue che ogni forma nel genere principale ha luogo per duplicazione.*

Siano  $p_1, \dots, p_r$  i primi dispari che dividono  $D$ . Si considerino i caratteri:

$$\chi_i(a) = L(a, p_i) \quad \text{per tutti gli } a \text{ primi con } p_i$$

$$\delta(a) = (-1)^{(a-1)/2} \quad \text{per tutti gli } a \text{ dispari}$$

$$\epsilon(a) = (-1)^{(a^2-1)/8} \quad \text{per tutti gli } a \text{ dispari}$$

Quando  $D \equiv 1 \pmod{4}$  diciamo che  $\chi_1, \dots, \chi_r$  sono i *caratteri assegnati*; se invece  $D = -4n$  assegnamo i caratteri secondo lo schema a seguire:

$$\begin{array}{ll} n \equiv 3 \pmod{4} & \chi_1 \dots, \chi_r \\ n \equiv 1 \pmod{4} & \chi_1 \dots, \chi_r, \delta \\ n \equiv 2 \pmod{8} & \chi_1 \dots, \chi_r, \delta\epsilon \\ n \equiv 6 \pmod{8} & \chi_1 \dots, \chi_r, \epsilon \\ n \equiv 4 \pmod{8} & \chi_1 \dots, \chi_r, \delta \\ n \equiv 0 \pmod{8} & \chi_1 \dots, \chi_r, \delta, \epsilon \end{array}$$

(si noti che il numero di caratteri assegnati è pari a  $\mu$ ) E' facile constatare come i caratteri assegnati forniscano un omomorfismo:

$$\Psi : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}^\mu$$

**Lemma 17.5.**  $\Psi$  è suriettivo e il suo nucleo consiste nel sottogruppo  $H$  dei valori rappresentati dalla forma principale.  $\Psi$  induce un isomorfismo

$$(\mathbb{Z}/D\mathbb{Z})^*/H \xrightarrow{\sim} \{\pm 1\}^\mu$$

*Dimostrazione.* Nel caso in cui  $D \equiv 1 \pmod{4}$  la dimostrazione è semplice: se  $p$  è un primo dispari, il simbolo di Legendre  $L(a, p)$  induce un omomorfismo suriettivo

$$L(\cdot, p) : (\mathbb{Z}/p^m\mathbb{Z})^* \longrightarrow \{\pm 1\}$$

il cui nucleo è il sottogruppo dei residui quadratici in  $(\mathbb{Z}/p^m\mathbb{Z})^*$  (per sollevamento Henseliano). Il teorema cinese del resto completa la dimostrazione:

$$(\mathbb{Z}/D\mathbb{Z})^* \xrightarrow{\sim} \prod_{j=1}^{\mu} (\mathbb{Z}/p_j^{m_j}\mathbb{Z})^*$$

Il caso  $D \equiv 0 \pmod{4}$  è problematico in quanto il sottogruppo  $H$  rappresentato da  $x^2 + ny^2$  può essere poco più grande del sottogruppo dei quadrati. In ogni caso è possibile invocare il teorema cinese del resto previa applicazione del teorema di struttura dei gruppi nella forma

$$(\mathbb{Z}/2^u\mathbb{Z})^*$$

per concludere in maniera analoga al caso precedente. Notiamo ora che  $\ker(\chi)$  ha indice 2 in  $(\mathbb{Z}/D\mathbb{Z})^*$ , per cui  $\ker(\chi)/H$  risulta avere ordine  $2^{\mu-1}$ . Sappiamo che il numero di generi è l'ordine di  $\Phi(C(D)) \subset \ker(\chi)/H$ , e poiché  $\Phi$  manda ogni classe nel set di valori da essa rappresentati, abbiamo bisogno di provare che ogni classe di congruenza in  $\ker(\chi)$  contiene un numero rappresentato da una forma di discriminante  $D$ : il teorema di Dirichlet sui primi nelle progressioni aritmetiche banalizza la questione. Consideriamo dunque la mappa

$$C/C^2 \longrightarrow \{\pm 1\}^{\mu-1}$$

indotta dall'omomorfismo

$$\Phi : C \longrightarrow \ker(\chi)/H \simeq \{\pm 1\}^{\mu-1}$$

La mappa di quadratura da  $C$  in sé produce la successione esatta corta

$$0 \longrightarrow C_0 \longrightarrow C \longrightarrow C^2 \longrightarrow 0$$

dove  $C_0$  è il sottogruppo degli elementi di ordine inferiore o pari a 2. Segue che l'indice  $[C : C^2]$  è pari all'ordine di  $C_0$ , ovvero a  $2^{\mu-1}$ , e che dominio e codominio della mappa  $C/C^2 \longrightarrow \{\pm 1\}^{\mu-1}$  hanno la stessa cardinalità, producendo un isomorfismo. Per queste ragioni  $C^2$  risulta essere nucleo della mappa  $\Phi$ , nonché insieme delle classi nel genere principale, da cui la tesi.  $\square$

## 18 Formula delle classi

Denotiamo con  $R(n)$  il numero di rappresentazioni di  $n$  tramite forme quadratiche (definite positive, ridotte) di discriminante  $D < -4$ . Per ogni  $n$  positivo primo con  $D$  si ha

$$R(n) = 2 \sum_{m|n} K(D, m)$$

in quanto è sufficiente considerare il numero di soluzioni della congruenza  $z^2 \equiv D \pmod{4n}$ . Semplici stime di natura analitica (si veda Davenport[6]) mostrano che

$$\lim_{n \rightarrow +\infty} \frac{1}{N} \sum_{\substack{n=1 \\ \gcd(n, D) = 1}}^n R(n) = 2 \frac{\phi(|D|)}{|D|} \sum_{m=1}^{+\infty} \frac{K(D, m)}{m}$$

Sia ora  $R(n, f)$  il numero di rappresentazioni di  $n$  secondo una particolare forma quadratica ridotta. Si ha che

$$\sum_{\substack{n=1 \\ \gcd(n, D)=1}}^N R(n, f)$$

è il numero di punti a coordinate intere  $(x, y)$  che verificano

$$0 < ax^2 + bxy + cy^2 \leq N \quad \gcd(ax^2 + bxy + cy^2, D) = 1$$

La seconda condizione vincola  $x$  ed  $y$  a giacere in certe coppie di classi residue modulo  $|D|$ , il cui numero è pari a  $|D| \phi(|D|)$  (si veda Landau, Vorlesungen[8]); è sufficiente per questo considerare le coppie di interi  $(x, y)$  che realizzano

$$ax^2 + bxy + cy^2 \leq N \quad x \equiv x_0, y \equiv y_0 \pmod{|D|}$$

L'area dell'ellisse  $ax^2 + bxy + cy^2 = N$  è chiaramente pari a

$$\frac{2\pi N}{\sqrt{4ac - b^2}} = \frac{2\pi}{\sqrt{|D|}} N$$

da cui

$$\lim_{N \rightarrow +\infty} \frac{1}{N} \sum_{\substack{n=1 \\ \gcd(n, D)=1}}^N R(n, f) = \frac{2\pi \phi(|D|)}{\sqrt{|D|^3}}$$

$$h(D) = \frac{\sqrt{|D|}}{\pi} L(1, \chi)$$

ove  $L(1, \chi)$  è la funzione  $L$  di Dirichlet associata al simbolo di Kronecker per  $D$ .

Considerando la somma di Gauss (omettiamo di dimostrare l'identità, legata alle proprietà delle funzioni nello spazio di Schwarz, e in particolare allo sviluppo in serie di Fourier della funzione  $\Theta$  di Jacobi; da segnalare l'elegante ed elementare approccio del Bellman [13])

$$\sum_{m=1}^{|D|} K(D, m) e^{\frac{imn}{|D|}} = i\sqrt{|D|} K(D, n)$$

non è difficile concludere

$$L(1, \chi) = -\frac{\pi}{\sqrt{|D|}} \sum_{m=1}^{|D|} m \cdot K(D, m)$$

che implica, per  $k$  intero positivo maggiore di 1,

$$h(-4k) = -\frac{1}{4k} \sum_{j=1}^{4k} j \cdot K(-4k, j)$$

Si noti che, quando  $k = p$  è un primo congruo a 1 modulo 4, si ha semplicemente

$$h(-4k) = 2 \sum_{0 < j < k/4} L(j, p)$$

Negli altri casi il computo del numero delle classi può essere intrapreso attraverso una semplice integrazione numerica (formule di Newton-Cotes): consideriamo ad esempio il caso  $D = -15$ . Si ha

$$L(1, \chi) = \sum_{j=0}^{+\infty} \left( \frac{1}{15j+1} + \frac{1}{15j+2} + \frac{1}{15j+4} - \frac{1}{15j+7} + \frac{1}{15j+8} - \frac{1}{15j+11} - \frac{1}{15j+13} - \frac{1}{15j+14} \right)$$

e posto

$$f_{15}(x) = \frac{1 + x + x^3 - x^6 + x^7 - x^{10} - x^{12} - x^{13}}{1 - x^{15}}$$

risulta

$$h(-15) = \frac{\sqrt{15}}{\pi} L(1, \chi) = \int_0^1 f_{15}(x) dx$$

ove

$$\lim_{x \rightarrow 0} f_{15}(x) = 0 \quad \lim_{x \rightarrow 1} f_{15}(x) = -\frac{1}{15} \sum_{j=1}^{15} j \cdot K(j, 15) = h(-15) = 2$$

## 19 Caso $k = 7$ e affini

Proviamo ora a computare esplicitamente quali siano le forme quadratiche ridotte  $ax^2 + bxy + cy^2$  con discriminante  $-28$ . Abbiamo  $b \equiv D \equiv 0 \pmod{2}$ , nonché  $|b| \leq \sqrt{28/3}$ : le uniche possibilità sono dunque  $b = 0$ , con forma ridotta associata  $x^2 + 7y^2$ , e  $|b| = 2$ , ma in tal caso le relazioni  $ac = \frac{b^2 - D}{4} = 8$ ,  $|b| \leq a \leq c$  e  $\gcd(a, b, c) = 1$  risultano incompatibili. Segue che il gruppo delle classi  $C(-28)$  è banale, e che l'identità  $L(-7, p) = 1$  coimplica l'esistenza di una coppia  $(x, y) \in \mathbb{Z}^2$  (unica a meno dei segni) per cui  $p = x^2 + 7y^2$ .

L'intero  $k = 7$  non è l'unico a godere di questa ragguardevole proprietà (nel genere principale è inclusa un'unica classe): già Lagrange riportava nelle sue tavole le seguenti corrispondenze:

$$\begin{array}{lll} p = x^2 + 6y^2 & \iff & p \equiv 1, 7 \pmod{12} & \iff & L(-6, p) = L(2, p) = 1 \\ p = x^2 + 10y^2 & \iff & p \equiv 1, 9, 11, 19 \pmod{40} & \iff & L(-10, p) = L(-2, p) = 1 \\ p = x^2 + 13y^2 & \iff & p \equiv 1, 9, 17, 25, 29, 49 \pmod{52} & \iff & L(-13, p) = L(-1, p) = 1 \\ p = x^2 + 15y^2 & \iff & p \equiv 1, 19, 31, 49 \pmod{60} & \iff & L(-15, p) = 1 \\ p = x^2 + 21y^2 & \iff & p \equiv 1, 25, 37 \pmod{84} & \iff & L(-21, p) = L(-1, p) = 1 \\ p = x^2 + 22y^2 & \iff & p \equiv 1, 9, 15, 23, 25, 31, 47, 49, 71, 81 \pmod{88} & \iff & L(-22, p) = L(2, p) = 1 \\ p = x^2 + 30y^2 & \iff & p \equiv 1, 31, 49, 79 \pmod{120} & \iff & L(-30, p) = L(2, p) = 1 \end{array}$$

## 20 Numeri idonei

**Lemma 20.1.** *Se  $C(-4k)$  è tale da possedere una sola classe per genere ed  $n$  è un intero dispari primo con  $k$ , esprimibile in forma canonica in modo sostanzialmente univoco,  $n$  è primo.*

*Dimostrazione.* Il numero di modi in cui  $n$  può essere rappresentato propriamente da una forma ridotta di discriminante  $-4k$ , con  $k > 1$ , è pari a

$$2 \prod_{p|n} (1 + L(-n, p))$$

Inoltre, posto in tali ipotesi che  $f(x, y)$  rappresenti propriamente  $n$ , quest'ultimo è rappresentato propriamente in esattamente  $2^{\omega(n)+1}$  modi da una forma ridotta nel genere di  $f(x, y)$ .  $\square$

Al termine della quinta sezione delle sue *Disquisitiones* [9], Gauss ha elencato 65 discriminanti nella forma  $-4k$  per cui il numero delle classi eguaglia quello dei generi (*numeri idonei*):

$h(-4n)$	$n$
1	1, 2, 3, 4, 7
2	5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 38
4	21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253
8	105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760
16	840, 1320, 1365, 1848

Grazie al lemma d'inizio paragrafo Gauss è riuscito a provare la primalità di

$$18518809 = 197^2 + 1848 \cdot 100^2$$

un risultato piuttosto sorprendente per i tempi.

Nel 1934 Chowla ha provato che il numeri di discriminanti *idonei* nella forma  $-4k$  è finito; nel 1973 Weinberger ha provato che esiste al più un altro numero *idoneo* fatta eccezione per quelli già elencati da Gauss.

## 21 Crivello di Atkin

**Lemma 21.1.** *Sia  $n$  un intero positivo libero da quadrati e congruo a 1 modulo 4;  $n$  è primo se e solo se  $\#\{(x, y) : x > 0, y > 0, 4x^2 + y^2 = n\}$  è dispari.*

*Dimostrazione.* Sia  $S = \{(x, y) : y > 0, x^2 + 4y^2 = n\}$  e  $T$  l'insieme degli ideali di  $\mathbb{Z}[\sqrt{-1}]$  a norma  $n$ . Per ogni  $(x, y) \in S$  sia  $f(x, y) \in T$  l'ideale generato da  $y + 2xi$ .  $f$  è iniettiva, in quanto gli altri generatori di  $f(x, y)$  sono  $-y - 2xi, -2x + yi, 2x - yi$ , nessuno dei quali è nella forma  $y' + 2x'i$  per  $y' > 0$ . Si prenda ora un  $I \in T$ , generato da  $a + bi$ , con  $a^2 + b^2 = n$  e  $b \neq 0$  poiché  $n$  è libero da quadrati. Se  $a$  è pari e  $b > 0$  allora  $I = f(-a/2, b)$ ; se  $a$  è pari e  $b < 0$  allora  $I = f(a/2, -b)$ ; se  $a$  è dispari e  $a > 0$  allora  $I = f(b/2, a)$ ; se  $a$  è dispari e  $a < 0$  allora  $I = f(-b/2, -a)$ :  $f$  è surgettiva. A questo punto, se  $n$  è primo si ha  $\#T = 2$ , da cui  $\#\{(x, y) : x > 0, y > 0, 4x^2 + y^2 = n\} = \#S/2 = \#T/2 = 1$ ; il fatto che  $\{x^2 + y^2 : (x, y) \in \mathbb{Z}^2\}$  sia un monoide moltiplicativo completa la dimostrazione.  $\square$

**Lemma 21.2.** *Sia  $n$  un intero positivo libero da quadrati e congruo a 1 modulo 6;  $n$  è primo se e solo se  $\#\{(x, y) : x > 0, y > 0, 3x^2 + y^2 = n\}$  è dispari.*

*Dimostrazione.* Posto  $\omega = \frac{-1+\sqrt{3}}{2}$ , l'anello  $\mathbb{Z}[\omega]$  è a ideali principali ed ha come gruppo delle unità l'insieme  $\{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$ . Definito  $S$  come l'insieme  $\{(x, y) : y > 0, 3x^2 + y^2 = n\}$ ,  $T$  come l'insieme degli ideali di  $\mathbb{Z}[\omega]$  a norma  $n$ ,  $f(x, y)$  come l'ideale generato da  $x + y + 2\omega x$ , considerazioni analoghe a quelle esposte nel paragrafo precedente portano a concludere  $\#S = \#T$ .  $\square$

**Lemma 21.3.** *Sia  $n$  un intero positivo libero da quadrati e congruo a 11 modulo 12;  $n$  è primo se e solo se  $\#\{(x, y) : x > 0, y > 0, 3x^2 - y^2 = n\}$  è dispari.*

*Dimostrazione.* Il gruppo delle unità di  $\mathbb{Z}[\sqrt{3}]$  è l'insieme  $\{\pm(2 + \sqrt{3})^j : j \in \mathbb{Z}\}$ .

Poniamo  $S = \{(x, y) : |x| > y > 0, 3x^2 - y^2 = n\}$  chiamiamo  $T$  l'insieme degli ideali a norma  $n$  in  $\mathbb{Z}[\sqrt{3}]$ , e per ogni  $(x, y) \in S$  definiamo  $f(x, y)$  come l'ideale generato da  $y + \sqrt{3}x$ . In analogia a quanto già esposto, sappiamo che per provare la tesi è sufficiente mostrare che  $S$  e  $T$  sono in biezione. Detto  $L = \log(2 + \sqrt{3})$ , definiamo un omomorfismo  $\text{Log} : \mathbb{Q}[\sqrt{3}]^* \rightarrow \mathbb{R}^2$  tramite  $\text{Log}(a + b\sqrt{3}) = (\log|a + b\sqrt{3}|, \log|a - b\sqrt{3}|)$ , per cui  $\text{Log} \mathbb{Z}[\sqrt{3}]^* = (L, -L)\mathbb{Z}$ . Si noti che, se  $|b| > a > 0$  allora  $|u - v| < L$  dove  $(u, v) = \text{Log}(a + b\sqrt{3})$ , e che  $|u - v| \leq L$  implica che sia  $|a| < |b|$  oppure  $|a| \geq 3|b|$ . Iniettività: siano  $(x, y)$  e  $(x', y')$  elementi distinti di  $S$ ,  $(u, v) = \text{Log}(y + \sqrt{3}x)$ ,  $(u', v') = \text{Log}(y' + \sqrt{3}x')$ . Si ha  $|u - v| < L$  e  $|u' - v'| < L$ , per cui  $|u - u' - v + v'| < 2L$ . Se fosse  $f(x, y) = f(x', y')$  si avrebbe  $(u, v) - (u', v') \in (L, -L)\mathbb{Z}$ , ovvero (per disuguaglianza triangolare)  $(u, v) = (u', v')$ . Si avrebbe dunque  $(x', y') \in \{(x, y), (-x, -y)\}$ , ovvero  $(x', y') = (x, y)$  per positività delle seconde componenti, assurdo. Suriettività: dato un ideale  $I$  di  $\mathbb{Z}[\sqrt{3}]$  a norma  $n$ , se ne consideri un generatore  $(a + b\sqrt{3})$  e si ponga  $(u, v) = \text{Log}(a + b\sqrt{3})$ . Si scelga ora un intero  $j$  che disti al più  $\frac{1}{2}$  da  $\frac{v-u}{2L}$  e si ponga  $y + x\sqrt{3} = (a + b\sqrt{3})(2 + \sqrt{3})^j$ . Segue:

$$\text{Log}(y + x\sqrt{3}) = (u + jL, v - jL)$$

$$|(u + jL) - (v - jL)| \leq L$$

$$|y| \leq |x| \quad \text{oppure} \quad |y| \geq 3|x|$$

Tuttavia  $n = \pm(3x^2 - y^2)$ , e  $n \equiv 11 \pmod{12}$  implica  $n = 3x^2 - y^2$ , per cui  $|y| \leq |x|$ ; inoltre  $y \neq 0$  e  $|y| \neq |x|$  poiché  $n$  è libero da quadrati. Se  $y > 0$  si ha  $I = f(x, y)$ , se  $y < 0$  si ha  $I = f(-x, -y)$ , e la biezione è provata.  $\square$

I tre lemmi provati costituiscono le basi per un algoritmo di crivello con molti punti di contatto con quello di Eratostene: sia  $A$  la lista  $[6, 7, \dots, M]$ , cui ad ogni elemento è associata una marca in  $\{0, 1\}$ , inizialmente pari a 0 (a indicare non-primalità); sia  $P$  la lista  $[2, 3, 5]$ .

- Per ogni elemento  $m$  di  $A$ 
  - Se  $m$  è congruo a 1, 13, 17, 29, 37, 41, 49, 53 (mod 60) se ne cambi di parità la marca associata tante volte quante le soluzioni di  $4x^2 + y^2 = m$
  - Se  $m$  è congruo a 7, 19, 31, 43 (mod 60) se ne cambi di parità la marca associata tante volte quante le soluzioni di  $3x^2 + y^2 = m$
  - Se  $m$  è congruo a 11, 23, 47, 60 (mod 60) se ne cambi di parità la marca associata tante volte quante le soluzioni di  $3x^2 - y^2 = m$ , con  $x > y$
  - Se  $m$  è in una qualche altra classe di resto modulo 60, lo si ignori
- Si cominci con il considerare il più piccolo elemento di  $A$
- Si prenda il primo elemento a seguire con marca 1 e lo si includa in  $P$
- Si prenda il quadrato dell'ultimo elemento considerato e si applichi la marca 0 a tutti i suoi multipli in  $A$
- Si ripetano i passi di crivello fino ad esaurimento di  $A$

Un'implementazione efficiente di questo algoritmo (*crivello di Atkin*) permette di computare i primi fino ad  $M$  con  $O(M/\log \log M)$  operazioni e  $M^{1/2+o(1)}$  bit di memoria, mentre il crivello di Eratostene, nell'implementazione più efficiente conosciuta, richiede  $O(M)$  operazioni e  $O(M^{1/2}(\log \log M)/\log M)$  bit di memoria. Per i dettagli implementativi si faccia riferimento all'articolo originale di Atkin e Bernstein [4].

## 22 Ruolo delle leggi di reciprocità di ordine superiore

**Lemma 22.1.** Sia  $\omega = e^{\frac{2\pi i}{3}} = \frac{1+\sqrt{-3}}{2}$ . L'anello  $\mathbb{Z}[\omega]$  risulta euclideo secondo la norma  $N(a + b\omega) = a^2 - ab + b^2$ ;  $\mathbb{Z}[\omega]$  è dunque un anello a ideali principali (PID) e a fattorizzazione unica (UFD), avente gruppo delle unità  $\mathbb{Z}[\omega]^* = \{\pm 1, \pm \omega, \pm \omega^2\}$ . Inoltre, se  $p$  è un primo di  $\mathbb{Z}$ , si verifica:

- Se  $p = 3$  allora  $1 - \omega$  è primo in  $\mathbb{Z}[\omega]$  e  $3 = -\omega^2(1 - \omega)^2$
- Se  $p \equiv 1 \pmod{3}$  allora esiste un primo  $\pi \in \mathbb{Z}[\omega]$  tale che  $p = \pi\bar{\pi}$
- Se  $p \equiv 2 \pmod{3}$  allora  $p$  resta primo in  $\mathbb{Z}[\omega]$

**Lemma 22.2.** Se  $\pi$  è un primo di  $\mathbb{Z}[\omega]$  il quoziente  $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$  è un campo finito di  $N(\pi)$  elementi. Inoltre

- Se  $p = 3$  o  $p \equiv 1 \pmod{3}$  allora  $N(\pi) = p$  e  $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$
- Se  $p \equiv 2 \pmod{3}$  allora  $N(\pi) = p^2$  e  $\mathbb{Z}/p\mathbb{Z}$  è l'unico sottocampo di ordine  $p$  del campo  $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$  con  $p^2$  elementi

**Lemma 22.3** (Piccolo Teorema di Fermat). *Sia  $\pi$  un primo di  $\mathbb{Z}[\omega]$  che non divide  $\alpha \in \mathbb{Z}[\omega]$ . Si ha*

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$$

*Dimostrazione.*  $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$  è un gruppo finito di ordine  $N(\pi) - 1$ . □

Sia ora  $\pi$  un primo di  $\mathbb{Z}[\omega]$  che non divide 3 (ovvero non associato a  $1 - \omega$ ) e  $\alpha$  un elemento di  $\mathbb{Z}[\omega]$  non divisibile per  $\pi$ . E' chiaro che  $3 \mid N(\pi) - 1$ , dunque  $x = \alpha^{(N(\pi)-1)/3}$  è una radice terza dell'unità (mod  $\pi$ ). Poiché

$$x^3 - 1 = (x - 1)(x - \omega)(x - \omega^2) \pmod{\pi}$$

si ha

$$\alpha^{(N(\pi)-1)/3} \equiv 1, \omega, \omega^2 \pmod{\pi}$$

E' dunque possibile definire un'estensione del simbolo di Legendre  $L_3(\alpha, \pi)$  come l'unica radice cubica dell'unità che realizza

$$\alpha^{(N(\pi)-1)/3} = L_3(\alpha, \pi)$$

ed è immediata la moltiplicatività

$$L_3(\alpha\beta, \pi) = L_3(\alpha, \pi) \cdot L_3(\beta, \pi)$$

e il fatto che il simbolo definisca un omomorfismo da  $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$  in  $\mathbb{C}^*$ . Ricordiamo che il gruppo moltiplicativo di un campo finito è ciclico, onde per cui

$$L_3(\alpha, \pi) = 1 \iff \alpha^{(N(\pi)-1)/3} \equiv 1 \pmod{\pi} \iff x^3 \equiv \alpha \pmod{\pi} \text{ ha soluzione in } \mathbb{Z}[\omega]$$

Definiamo ora come *primario* ogni primo  $\pi \in \mathbb{Z}[\omega]$  che realizzi  $\pi \equiv \pm 1 \pmod{3}$ . Per ogni primo  $\pi \in \mathbb{Z}[\omega]$  che non divide 3, esattamente due dei sei associati  $\pm\pi, \pm\omega\pi, \pm\omega^2\pi$  risultano *primari*.

**Teorema 22.4** (Reciprocità cubica). *Se  $\pi$  e  $\vartheta$  sono primi primari di  $\mathbb{Z}[\omega]$  non aventi la medesima norma si ha:*

$$L_3(\pi, \vartheta) = L_3(\vartheta, \pi)$$

*Dimostrazione.* Per questo teorema e il lemma seguente si veda Ireland and Rosen [11]. □

**Lemma 22.5.** *Sia  $\pi \in \mathbb{Z}[\omega]$  un primo primario non associato a  $1 - \omega$  nella forma  $\pi = -1 + 3m + 3n\omega$ . Si ha*

- $L_3(-1, \pi) = 1$
- $L_3(\omega, \pi) = \omega^{m+n}$
- $L_3(1 - \omega, \pi) = \omega^{2m}$

**Teorema 22.6.** *Sia  $p \in \mathbb{Z}$  un primo.  $p = x^2 + 27y^2$  se e solo se  $p \equiv 1 \pmod{3}$  e 2 è un residuo cubico modulo  $p$ .*

*Dimostrazione.* Se  $p = x^2 + 27y^2$  chiaramente  $p \equiv 1 \pmod{3}$ . Sia  $\pi = x + \sqrt{-3}y$  in modo tale che si abbia  $p = \pi\bar{\pi}$ . 2 è residuo cubico modulo  $p$  se e solo se  $L_3(2, \pi) = 1$ , ma sia 2 che  $\pi$  sono primi primari in  $\mathbb{Z}[\omega]$ , dunque per reciprocità

$$L_3(2, \pi) = L_3(\pi, 2) = \pi \pmod{2}$$

Dato che  $\pi = x + 3y + 6y\omega$ ,  $\pi \equiv x + y \pmod{2}$ , ed  $x$  ed  $y$  devono avere parità opposte per realizzare  $p = x^2 + 27y^2$ . Viceversa, si supponga  $p \equiv 1 \pmod{3}$  e 2 residuo cubico modulo  $p$ . Possiamo scrivere

$p = \pi\bar{\pi}$  e assumere che  $\pi$  sia un primo primario in  $\mathbb{Z}[\omega]$ . Ciò significa  $\pi = a + 3b\omega$  per una qualche coppia di interi  $a$  e  $b$ . Si ha

$$4p = 4\pi\bar{\pi} = 4(a^2 - 3ab + 9b^2) = (2a - 3b)^2 + 27b^2$$

Provare che  $b$  sia pari equivale dunque a dimostrare  $p = x^2 + 27y^2$ . D'altro canto, sempre per reciprocità,

$$1 = L_3(2, \pi) = L_3(\pi, 2) \iff a + 3b\omega \equiv 1 \pmod{2}$$

risulta che  $a$  è dispari e  $b$  pari, da cui la tesi. □

**Lemma 22.7.** *L'anello  $\mathbb{Z}[i]$  risulta euclideo secondo la norma  $N(a + ib) = a^2 + b^2$ ;  $\mathbb{Z}[i]$  è dunque un anello a ideali principali (PID) e a fattorizzazione unica (UFD), avente gruppo delle unità  $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ . Inoltre, se  $p$  è un primo di  $\mathbb{Z}$ , si verifica:*

- Se  $p = 2$  allora  $1 + i$  è primo in  $\mathbb{Z}[i]$  e  $2 = -i^3(1 + i)^2$
- Se  $p \equiv 1 \pmod{4}$  allora esiste un primo  $\pi \in \mathbb{Z}[i]$  tale che  $p = \pi\bar{\pi}$
- Se  $p \equiv 3 \pmod{4}$  allora  $p$  resta primo in  $\mathbb{Z}[i]$

**Lemma 22.8** (Piccolo Teorema di Fermat). *Sia  $\pi$  un primo di  $\mathbb{Z}[i]$  che non divide  $\alpha \in \mathbb{Z}[i]$ . Si ha*

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$$

Sia ora  $\pi$  un primo di  $\mathbb{Z}[i]$  non associato a  $1 + i$  e  $\alpha$  un elemento di  $\mathbb{Z}[i]$  non divisibile per  $\pi$ . E' chiaro che  $4|N(\pi) - 1$ , dunque  $x = \alpha^{(N(\pi)-1)/4}$  è una radice quarta dell'unità  $\pmod{\pi}$ . Poiché

$$x^4 - 1 = (x - 1)(x + 1)(x - i)(x + i) \pmod{\pi}$$

si ha

$$\alpha^{(N(\pi)-1)/4} \equiv \pm 1, \pm i \pmod{\pi}$$

E' dunque possibile definire un'estensione del simbolo di Legendre  $L_4(\alpha, \pi)$  come l'unica radice quarta dell'unità che realizza

$$\alpha^{(N(\pi)-1)/4} = L_4(\alpha, \pi)$$

Nuovamente il simbolo definisce un omomorfismo da  $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^*$  in  $\mathbb{C}^*$ , e si ha

$$L_4(\alpha, \pi) = 1 \iff x^4 \equiv \alpha \pmod{\pi} \text{ ha soluzione in } \mathbb{Z}[i]$$

Tra gli interi di Gauss sono detti *primari* i primi  $\pi = a + bi$  ove  $b$  è pari ed  $a$  è congruo a  $b + 1$  modulo 4; ogni primo non associato a  $1 + i$  ammette tra i suoi associati  $\pm\pi, \pm i\pi$  un unico rappresentante primario.

**Teorema 22.9** (Reciprocità biquadratica). *Se  $\pi$  e  $\vartheta$  sono primi distinti primari di  $\mathbb{Z}[i]$  si ha:*

$$L_4(\pi, \vartheta) \cdot L_4(\vartheta, \pi) = (-1)^{(N(\pi)-1)(N(\vartheta)-1)/16}$$

Per questo teorema e il lemma seguente si veda Ireland and Rosen [11].

**Lemma 22.10.** *Sia  $\pi \in \mathbb{Z}[\omega]$  un primo primario non associato a  $1 - \omega$  nella forma  $\pi = a + ib$ . Si ha*

- $L_4(-1, \pi) = 1$
- $L_4(i, \pi) = i^{-(a-1)/2}$
- $L_4(1 + i, \pi) = i^{(a-b-1-b^2)/4}$

- $L_4(2, \pi) = i^{ab/2}$

*Dimostrazione.* Si noti come l'ultima identità possa essere provata per via elementare:  $p \equiv 1 \pmod{4}$  implica  $p = a^2 + b^2$ , con  $a$  dispari e  $b$  pari. Si ha

$$L(a, p) = L(p, a) = L(b^2, a) = 1$$

e da  $2p = (a + b)^2 + (a - b)^2$  segue in maniera analoga

$$L(a + b, p) = J(p, a + b) = J(2, a + b) = (-1)^{(a+b)^2-1)/8}$$

Posto  $\pi = a + ib$ , applicando la definizione  $L_4(\alpha, \pi) = \alpha^{(N(\pi)-1)/4}$  si ha

$$L(a + b, p) = i^{(a^2+b^2-1)/4} \cdot i^{ab/2} = L_4(i, \pi) \cdot i^{ab/2}$$

d'altro canto

$$(a + b)^2 \equiv 2ab \pmod{p} \implies (a + b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4} \pmod{p} \implies L(a + b, p) = L_4(2ab, \pi)$$

Inoltre

$$-2ai(a + bi) \equiv -2a^2i + 2ab \equiv 0 \pmod{\pi} \implies 2ab \equiv 2a^2i \pmod{\pi}$$

Abbiamo dunque una lunga catena di identità

$$L_4(i, \pi) \cdot i^{ab/2} = L(a + b, p) = L_4(2ab, \pi) = L_4(2a^2i, \pi) = L_4(2i, \pi) \cdot L(a, p) = L_4(2i, \pi)$$

ove è sufficiente raffrontare gli estremi per giungere al risultato desiderato.  $\square$

**Teorema 22.11.** *Sia  $p \in \mathbb{Z}$  un primo.  $p = x^2 + 64y^2$  se e solo se  $p \equiv 1 \pmod{4}$  e 2 è un residuo biquadratico modulo  $p$ .*

*Dimostrazione.*  $p = x^2 + 64y^2$  implica chiaramente  $p \equiv 1 \pmod{4}$ , e da

$$p = (x + 8iy)(x - 8iy) = \pi\bar{\pi}$$

segue  $L_4(2, \pi) = i^4 = 1$ , da cui discende la risolubilità dell'equazione  $x^4 \equiv 2 \pmod{p}$ .

Viceversa,  $p \equiv 1 \pmod{4}$  implica l'esistenza di una coppia di interi  $(a, b)$  che realizza  $p = a^2 + b^2$ , ove siamo liberi di supporre  $a$  dispari e  $b$  pari. In queste ipotesi  $\pi = a + ib$  è un primo primario in  $\mathbb{Z}[i]$ , e per reciprocità biquadratica

$$L_4(2, \pi) = i^{ab/2} = 1 \implies ab/2 \equiv 0 \pmod{4} \implies b \equiv 0 \pmod{8}$$

si ha  $b = 8c$ , da cui discende  $p = a^2 + 64c^2$ .  $\square$

## 23 Campo delle classi di Hilbert

Abbiamo visto come lo studio del nostro problema a livello di *interi* (in  $\mathbb{Z}$  o in una sua estensione complessa di grado 2) diventi difficoltoso una volta persa la proprietà di fattorizzazione unica, posseduta da  $\mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\omega]$ . La trattazione generale del problema si svolge a livello di ideali, in quanto

**Teorema 23.1.** *Sia  $K$  un campo di numeri (sottocampo di  $\mathbb{C}$  avente grado finito su  $\mathbb{Q}$ ), e  $\mathcal{O}_K$  il suo anello degli interi.  $\mathcal{O}_K$  è un dominio di Dedekind, dunque*

- $\mathcal{O}_K$  è integralmente chiuso in  $K$ : ogni elemento di  $K$ , radice di un polinomio monico a coefficienti in  $\mathcal{O}_K$ , appartiene ad  $\mathcal{O}_K$
- $\mathcal{O}_K$  è un anello noetheriano: data una catena di ideali  $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$  esiste un intero  $n$  per cui  $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \dots$
- Ogni ideale primo non nullo di  $\mathcal{O}_K$  è massimale
- Ogni ideale non nullo  $\mathfrak{a}$  in  $\mathcal{O}_K$  può essere espresso come prodotto  $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$  di ideali primi, e la decomposizione è unica a meno dell'ordine. Inoltre i  $\mathfrak{p}_i$  sono esattamente gli ideali primi di  $\mathcal{O}_K$  contenenti  $\mathfrak{a}$

L'ultima proprietà si configura come ideale condizione di lavoro; non stupisce che nel gruppo di Galois di una particolare estensione di  $K$  esista un automorfismo (*simbolo di Artin*) che generalizzi le leggi di reciprocità viste per gli interi, gli interi di Gauss e gli interi di Eisenstein. Per tutta la teoria che andremo a esporre (omettendo le dimostrazioni) si faccia riferimento al Cox[1].

**Teorema 23.2.** *Dato un campo di numeri  $K$  esiste un'estensione galoisiana  $L$  di  $K$ , detta campo delle classi di Hilbert, tale che*

- $L$  è un'estensione abeliana non ramificata di  $K$ , galoisiana su  $\mathbb{Q}$
- Ogni estensione abeliana non ramificata di  $K$  giace in  $L$

**Teorema 23.3.** *Sia  $L$  campo delle classi di Hilbert di  $K$ , e  $\mathfrak{p}$  un ideale primo di  $K$ .  $\mathfrak{p}$  si spezza completamente in  $L$  se e solo  $\mathfrak{p}$  è un ideale principale.*

**Teorema 23.4.** *Sia  $K = \mathbb{Q}(\sqrt{-k})$*

$$p = x^2 + ky^2 \iff p \text{ si spezza completamente in } L \iff \begin{cases} L(-k, p) = 1 \\ f_k(x) \equiv 0 \pmod{p} \text{ ha soluzione intera} \end{cases}$$

dove  $L = K(\alpha)$  ed  $f_k$  è polinomio minimo di  $\alpha$  su  $K$ , avente grado

$$[L : K] = |\text{Gal}(L/K)| = |C(\mathcal{O}_K)|$$

**Teorema 23.5.** *Sia  $K$  un corpo quadratico immaginario di discriminante  $d_K < 0$ , ed  $f(x, y) = ax^2 + bxy + cy^2$  una forma quadratica primitiva con discriminante  $d_K$ .*

$$a[1, \tau] = [a, a\tau] = [a, (-b + \sqrt{d_K})/2] = \{ma + n(-b + \sqrt{d_K})/2 : m, n \in \mathbb{Z}\}$$

è un ideale di  $\mathcal{O}_K$ , e la mappa che manda  $f(x, y)$  in  $[a, (-b + \sqrt{d_K})/2]$  induce un isomorfismo tra il gruppo delle classi di forme quadratiche  $C(d_K)$  e il gruppo delle classi di ideali  $C(\mathcal{O}_K)$ , definito come quoziente tra  $I_K$ , gruppo degli ideali frazionari di  $\mathcal{O}_K$ , e  $P_K$ , gruppo degli ideali principali di  $\mathcal{O}_K$ .

## 24 Moltiplicazione complessa

La trattazione generale si evolve successivamente attraverso morfismi tra ideali e reticoli, e tra reticoli e funzioni ellittiche. Al termine del paragrafo vedremo come le funzioni  $\theta$  di Jacobi, il cui ruolo è stato centrale nella determinazione di espressioni chiuse per  $r_1(n)$  ed  $r_2(n)$ , tornino alla ribalta nella costruzione di un algoritmo (dovuto a Kalfoten e Yui) per decidere quali primi posseggano espressione canonica.

Diciamo che  $L$  è un *reticolo* se è un sottogruppo additivo di  $\mathbb{C}$  generato da due numeri complessi  $\omega_1$  ed  $\omega_2$  linearmente indipendenti su  $\mathbb{R}$ . Una *funzione ellittica* su  $L$  è un funzione meromorfa  $f(z)$  definita su tutto  $\mathbb{C}$  (salvo singolarità isolate) e doppiamente periodica:

$$\forall z \in \mathbb{C} \quad f(z + \omega_1) = f(z + \omega_2) = f(z)$$

Una celebre funzione ellittica è la  $\wp$  di Weierstrass, definita come

$$\wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} \left( \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)$$

avente poli di molteplicità 2 nei nodi del reticolo. Questa funzione soddisfa le identità

$$\wp'(z)^2 = 4\wp(z)^2 - g_2(L)\wp(z) - g_3(L)$$

$$\wp(\lambda z; \lambda L) = \lambda^{-2} \wp(z; L)$$

dove

$$g_2(L) = 60 \sum_{\omega \in L - \{0\}} \omega^{-4} \quad g_3(L) = 140 \sum_{\omega \in L - \{0\}} \omega^{-6}$$

Si è soliti denotare con  $e_1, e_2, e_3$  le radici della cubica  $4z^2 - g_2(L)z - g_3(L)$ , con  $\Delta(L)$  il discriminante

$$\Delta(L) = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2$$

e con  $j(L)$  la quantità

$$j(L) = 1728 \frac{g_2(L)^3}{\Delta(L)}$$

che risulta invariante per omotetie del reticolo  $L$ . Dato un numero complesso  $\tau$  con parte immaginaria positiva, le proprietà analitiche della funzione modulare  $j(\tau) = j([1, \tau])$  rivestono un ruolo di primaria importanza all'interno della teoria della moltiplicazione complessa, in quanto

**Lemma 24.1.** *Ogni funzione ellittica pari definita su un reticolo  $L$  è una funzione razionale in  $\wp(z; L)$ .*

**Lemma 24.2.** *Diciamo che un reticolo  $L$  possiede un ordine  $R$  come anello di moltiplicazione complessa quando il gruppo degli endomorfismi della curva ellittica  $y^2 = 4x^2 - g_2(L)x - g_3(L)$  è isomorfo, come anello, ad  $R$ .*

*Se  $\mathcal{O}$  è un ordine in un corpo quadratico immaginario esiste una corrispondenza biunivoca tra il gruppo delle classi di ideali  $C(\mathcal{O})$  e le classi di omotetia di reticoli che hanno  $\mathcal{O}$  come anello di moltiplicazione complessa.*

**Lemma 24.3.** *Due ideali frazionari sono omotetici come reticoli se e solo se giacciono nella stessa classe all'interno del gruppo delle classi di ideali  $C(\mathcal{O})$ .*

**Teorema 24.4.** *Se  $\mathcal{O}$  è un ordine in un corpo quadratico immaginario  $K$  ed  $\mathfrak{a}$  è un ideale frazionario proprio di  $\mathcal{O}$ , l'invariante  $j(\mathfrak{a})$  è un numero algebrico reale e  $K(j(\mathfrak{a}))$  è campo delle classi per l'ordine  $\mathcal{O}$ .*

*Dimostrazione.* Per provare  $L = K(j(\mathbf{a}))$  è sufficiente considerare come gli interi primi si decompongono in  $L$  e in  $K(j(\mathbf{a}))$ : entrano in gioco le proprietà della funzione modulare, che definiremo tra poco.  $\square$

**Lemma 24.5.** *Per un fissato ordine  $\mathcal{O}$  tutti gli invarianti  $j(\mathbf{a})$  sono coniugati, configurandosi dunque come le radici del medesimo polinomio irriducibile su  $\mathbb{Q}$ .*

**Lemma 24.6.** *Se  $g_2$  e  $g_3$  sono due numeri complessi tali per cui  $g_2^3 - 27g_3^2 \neq 0$  esiste un reticolo  $L$  che realizza  $g_2 = g_2(L), g_3 = g_3(L)$*

**Lemma 24.7.** *L'invariante  $j(\tau)$  è una funzione olomorfa in  $q = q(\tau) = e^{2\pi i\tau}$  e si ha*

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{+\infty} c_n q^n$$

ove i coefficienti  $c_n$  risultano tutti interi.

**Teorema 24.8.** *Sia  $\Gamma_0(m)$  il sottogruppo di  $SL(2, \mathbb{Z})$  delle matrici  $M$  per cui  $M_{21} \equiv 0 \pmod{m}$ .  $j(\tau)$  è una funzione modulare su  $SL(2, \mathbb{Z})$ , ed ogni funzione modulare su  $SL(2, \mathbb{Z})$  è una funzione razionale in  $j(\tau)$ ;  $j(\tau)$  e  $j(m\tau)$  sono funzioni modulari su  $\Gamma_0(m)$ , ed ogni funzione modulare su  $\Gamma_0(m)$  è funzione razionale in  $j(\tau)$  e  $j(m\tau)$ .*

**Lemma 24.9.** *Se definiamo*

$$C(m) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = m, a > 0, 0 \leq b < d, \gcd(a, b, d) = 1 \right\}$$

Per ogni  $\sigma \in C(m)$  l'insieme

$$\left( \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}^{-1} SL(2, \mathbb{Z}) \sigma \right) \cap SL(2, \mathbb{Z})$$

è un laterale destro di  $\Gamma_0(m)$  in  $SL(2, \mathbb{Z})$ . Risulta

$$|C(m)| = m \prod_{p|m} \left( 1 + \frac{1}{p} \right)$$

e

$$\Phi_m(X, j(\tau)) = \prod_{\sigma \in C(m)} (X - j(\sigma\tau))$$

è detta equazione modulare.

**Teorema 24.10.** *L'equazione modulare gode delle seguenti proprietà:*

- $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$
- $\Phi_m(X, Y)$  è irriducibile come polinomio in  $X$
- $\Phi_m(X, Y) = \Phi_m(Y, X)$
- Se  $m$  non è un quadrato  $\Phi_m(X, X)$  è un polinomio di grado maggiore di 1 il cui coefficiente di testa è  $\pm 1$
- Per ogni primo  $p$  si ha  $\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod{p\mathbb{Z}[X, Y]}$

**Teorema 24.11.** *Se  $K$  è un corpo quadratico immaginario,  $K(j(\mathcal{O}_K))$  è il suo campo della classi di Hilbert (ovvero estensione galoisiana entro cui è ben definito un simbolo di reciprocità); facendo riferimento al **Teorema 23.3** si ha inoltre*

$$f_k(x) = \prod_{j=1}^{h(-4k)} (x - j(\mathbf{a}_i))$$

Consideriamo ad esempio il caso  $k = 21$ : l'ordine  $\mathbb{Z}[\sqrt{-21}]$  è massimale in  $K = \mathbb{Q}(\sqrt{-21})$  e si ha  $h(-84) = 4$ . Per computo diretto delle forme quadratiche ridotte di discriminante  $-84$  si ha che il gruppo delle classi di ideali di  $K$  è isomorfo al gruppo di Klein. In particolare

$$C(\mathcal{O}_K) = \{[\mathcal{O}_K], [P_2], [P_3], [P_5]\}$$

dove

$$\begin{aligned} P_2 &= (2, \sqrt{-21} - 1) & P_3 &= (3, \sqrt{-21}) & P_5 &= (5, \sqrt{-21} - 3) \\ [P_2]^2 &= [\mathcal{O}_K] & [P_3]^2 &= [\mathcal{O}_K] & [P_5] &= [P_2] \cdot [P_3] \end{aligned}$$

Eccoci dunque al cuore dell'algoritmo di Kalfoten e Yui: attraverso le funzioni  $\vartheta$  di Jacobi è possibile calcolare l'invariante  $j$  per ognuno dei quattro reticoli con un buon grado di precisione; nel nostro caso si ha

$$\begin{aligned} j(\sqrt{-21}) &= 3196802718613.9132928032899986\dots \\ j((\sqrt{-21} - 1)/2) &= -1787216.6012476570198674\dots \\ j((\sqrt{-21})/3) &= 15488.6808931242445923\dots \\ j((\sqrt{-21} - 3)/5) &= 58.0070617294852765\dots \end{aligned}$$

previo ricorso all'identità

$$j(\tau) = 32 \frac{(\vartheta(0; \tau)^8 + \vartheta(1/2; \tau)^8 + e^{2\pi i \tau} \vartheta(\tau/2; \tau)^8)^3}{e^{2\pi i \tau} (\vartheta(0; \tau) \vartheta(1/2; \tau) \vartheta(\tau/2; \tau))^8}$$

ove

$$\vartheta(z; \tau) = 1 + 2 \sum_{n=1}^{+\infty} e^{n^2 \pi i \tau} \cos(2\pi n z)$$

A questo punto il polinomio minimo per  $j(\mathcal{O}_K)$  risulta essere

$$\begin{aligned} f_{21}(x) &= x^4 - 3196800946944 x^3 - 5663679223085309952 x^2 + \\ &\quad + 88821246589810089394176 x - 5133201653210986057826304 \end{aligned}$$

e, preso un primo  $p$ , le condizioni

$$L(-21, p) = 1 \quad \exists a \in \mathbb{F}_p : f_{21}(a) = 0$$

equivalgono a

$$\exists (x, y) \in \mathbb{Z}^2 : p = x^2 + 21 y^2$$

## 25 Ringraziamenti

Ringrazio il Professor Giuseppe Puglisi per l'instancabile lavoro di revisione, i preziosi suggerimenti e il clima cordiale instaurato; il Professor Roberto Dvornicich e il Professor Umberto Zannier per i testi forniti; il Professor Traverso e Fabrizio Caruso per la fiducia riposta in me, che mi auguro abbia trovato degno coronamento. Ringrazio la Maestra Beatrice, il Professor Augusto, il Professor Moretta e il Professor Rossetti per avermi educato e stimolato con devozione assoluta, lungo un percorso che spero si rivelerà fruttuoso e affine ai miei ideali. Ringrazio la Professoressa Lalli e la Professoressa De Fanis per avermi aperto gli occhi su realtà ben distanti dalla matematica, e non per questo meno ricche. Ringrazio i ragazzi del Carducci, e gli altri miei colleghi più cari, per l'allegria, l'affetto, le serate trascorse assieme, i consigli, i litigi, tutto quello che degnamente ci rende giovani. Ringrazio gli amici lontani, confidando che la storia e i ricordi comuni non affievoliscano ma cementifichino quello che è stato, e che sarà; ringrazio mio padre, mia nonna, la mia famiglia piccola, per essere stata presente nei momenti felici, e non avermi abbandonato in tempi che felici non sono stati affatto; ringrazio l'incredibile Alessandra, mia splendida ragazza, per la tenacia dimostrata nel tollerare i miei difetti, il suo sapermi guidare, la sua sincerità.

E ringrazio mia madre, che spero abbia vegliato su di me in tutti questi anni, se è vero che esiste un aldilà.

## Riferimenti bibliografici

- [1] David A.Cox. *Primes Of The Form  $x^2 + ny^2$* . John Wiley And Sons, Amherst, Massachussetts, USA, 1980.
- [2] John A.Ewell. A Simple Derivation of Jacobi's Four-Square Formula. *The American Mathematical Monthly*, 85(3):323, 1982.
- [3] P.C. van Oorschot A.J. Menezes and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, New York, USA, 2001.
- [4] A. Atkin and D. Bernstein. Prime sieves using binary quadratic forms, 1999.
- [5] Wouter Castryck. A shortened classical proof of the quadratic reciprocity law. *The American Mathematical Monthly*, 71(5):289, 2006.
- [6] Harold Davenport. *Multiplicative Number Theory*. Springer-Verlag, Berlin, Germany, 1980.
- [7] Micheal D.Hirschhorn. A Simple Proof of Jacobi Two-Square Theorem. *The American Mathematical Monthly*, 92(8):597, 1985.
- [8] E.Landau. *Vorlesungen über Zahlentheorie*. Leipzig, Germany, 1927.
- [9] C. F. Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, New York, USA, 1986.
- [10] Heini Halberstam. Gaps in Integer Sequences. *Mathematics Magazine*, 56(3):131, 1983.
- [11] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, New York, USA, 1998.
- [12] Archiebold Karumbidza. *Class Numbers of Binary Forms and Imaginary Quadratic Fields*. PhD thesis, African Institute for Mathematical Sciences, Cape Town, South Africa, June 2004.
- [13] R.Bellman. *A Brief Introduction to Theta Functions*. Holt, Rinehart and Winston (Athena series), New York, USA, 1961.
- [14] Jean Varouchas. Démonstration Élémentaire d'une Identité de Lorenz. *The Ramanujan Journal*, 2(4):495, 1998.