Università degli Studi di Milano
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Triennale in Matematica

Interi Algebrici di Campi Quadratici Complessi

Prof.ssa Vittoria ZAMBELLI

elaborato finale di
Martino BORELLO
Matr. 689541

ANNO ACCADEMICO 2007 - 2008

Indice

Introduzione

L'argomento di questo elaborato è l'anello degli **interi algebrici dei campi quadratici complessi**.

Consideriamo l'estensione $\mathbb{Q}[\sqrt{d}]$ del campo razionale mediante $\sqrt{d}$, dove d è un intero negativo privo di fattori quadratici. All'interno di questo campo andiamo a considerare degli elementi particolari, gli interi algebrici, ovvero le radici di polinomi monici a coefficienti in $\mathbb{Z}$. Indichiamo con A_d l'insieme degli interi algebrici, che vedremo essere un anello. Abbiamo il seguente diagramma

$$\begin{array}{ccc} A_d & \subset & \mathbb{Q}[\sqrt{d}] \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Sappiamo dai corsi di algebra che l'anello $\mathbb{Z}$ ha delle proprietà algebriche molto forti, ovvero che è un dominio a fattorizzazione unica, un dominio a ideali principali e anche un dominio euclideo (per nozioni algebriche di base diamo come riferimento il libro di Allenby, [All83], in cui sono citati anche i risultati principali approfonditi in questo elaborato).

Ricordiamo solo il seguente risultato, basilare per la comprensione della struttura stessa dell'elaborato: per ogni dominio d'integrità D, dotato di unità, valgono le seguenti implicazioni

$$D \text{ è euclideo} \Rightarrow D \text{ è un PID} \Rightarrow D \text{ è un UFD}$$

È naturale (anche se, in realtà, si tratta di una conquista relativamente

recente) chiedersi se l'anello A_d abbia anch'esso le citate proprietà di $\mathbb{Z}$. Giungeremo, innanzitutto, al seguente risultato: l'anello A_d appartiene a una famiglia molto particolare di anelli, i domini di Dedekind, per i quali le proprietà di essere UFD e di essere PID sono equivalenti. Vedremo come queste due proprietà siano equivalenti a loro volta al fatto che gli ideali dell'anello A_d appartengano tutti ad un'unica classe di una particolare relazione di equivalenza.

Ci occuperemo, dapprima, della proprietà di essere dominio euclideo e giungeremo al seguente risultato: A_d è un dominio euclideo se e solo se $d \in \{-1, -2, -3, -7, -11\}$. Questo risultato si ottiene in modo piuttosto semplice con un'elegante dimostrazione geometrica. Il riferimento principale per questa sezione è il testo di W. Bruns, [Bru00].

La seconda parte riguarderà la proprietà di fattorizzazione unica, questione ben più complessa (basti pensare che per valori positivi di d è tuttora un problema aperto). Ci riferiremo all'articolo del 1969 di H.M. Stark, [Sta69], che fu il primo a porre fine al problema per valori negativi di d, e al testo di I.N. Stewart, [Ste79]. Il risultato, piuttosto sorprendente, è che sono solo nove i campi quadratici complessi in cui A_d è un UFD, precisamente gli A_d con $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$.

Nell'appendice daremo, infine, degli esempi di possibili applicazioni delle proprietà dell'anello A_d alla risoluzione di equazioni diofantee. Vedremo, in particolare, alcuni casi delle cosiddette curve di Mordell e il teorema di Ramanujan-Nagell. Il riferimento per questa sezione sono i testi di L.J. Mordell, [Mor69], e di I.N. Stewart.

Capitolo 1

Generalità sui campi quadratici

1.1 Interi algebrici e campi quadratici

Definizione 1. *Un **campo di numeri** è un sottocampo di $\mathbb{C}$ di grado finito (cioè di dimensione finita come spazio vettoriale) su $\mathbb{Q}$.*

Una classe infinita di campi di numeri è quella dei campi

$$\mathbb{Q}[\sqrt{d}] = \{q_1 + q_2\sqrt{d} \mid q_1, q_2 \in \mathbb{Q}\}$$

con $d \in \mathbb{Z}$, privo di fattori quadratici. Chiaramente questi campi hanno grado 2 su $\mathbb{Q}$, avendo come base $\{1, \sqrt{d}\}$. Si può supporre d intero privo di fattori quadratici, in quanto se $d = m^2 d'$, con $m, d' \in \mathbb{Z}$ e d' privo di fattori quadratici, si ha $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d'}]$. I campi $\mathbb{Q}[\sqrt{d}]$, per d intero privo di fattori quadratici, sono tutti a due a due non isomorfi.

Definizione 2. *Chiamiamo $\mathbb{Q}[\sqrt{d}]$, con d intero privo di fattori quadratici, **campo quadratico**. In particolare, $\mathbb{Q}[\sqrt{d}]$ viene detto **campo quadratico reale** per $d > 0$ e **campo quadratico complesso** per $d < 0$.*

Introduciamo una nozione fondamentale per la nostra trattazione.

Definizione 3. *Un numero complesso è un **intero algebrico** se e solo se è una radice di un polinomio monico a coefficienti in $\mathbb{Z}$.*

Enunciamo senza dimostrazione (cfr.[Mar77], pag.14) il seguente semplice teorema.

Teorema 1. *Sia α un intero algebrico. Allora il polinomio monico irriducibile su $\mathbb{Q}$ che ha α come radice ha coefficienti in $\mathbb{Z}$.*

Per quanto riguarda la forma degli interi algebrici nei campi quadratici abbiamo il seguente risultato.

Teorema 2. *Sia d un intero privo di fattori quadratici. L'insieme degli interi algebrici nel campo quadratico $\mathbb{Q}[\sqrt{d}]$ è*

$$\begin{array}{ll} \left\{a+b\sqrt{d}:\ a,b\in\mathbb{Z}\right\} & se\ d\equiv 2,3 \pmod 4 \\ \left\{\frac{a+b\sqrt{d}}{2}:\ a,b\in\mathbb{Z},\ a\equiv b\ (mod\ 2)\right\} & se\ d\equiv 1 \pmod 4 \end{array}$$

Dimostrazione. Trattiamo, innanzitutto, il caso semplice $\alpha = a \in \mathbb{Q}$. Allora si ha a intero algebrico se e solo se $a \in \mathbb{Z}$.
Sia ora $\alpha = r + s\sqrt{d},\ r,s \in \mathbb{Q},\ s \neq 0$. Allora il polinomio monico irriducibile su $\mathbb{Q}$ avente α come radice è

$$x^2 - 2rx + r^2 - ds^2$$

Si ha quindi α intero algebrico se e solo se

$$\begin{cases} (a)\ \ 2r \in \mathbb{Z} \\ (b)\ \ r^2 - ds^2 \in \mathbb{Z} \end{cases}$$

Si ha $(a) \ \Leftrightarrow\ (a1)\ \ r \in \mathbb{Z} \ \vee\ (a2)\ \ r \in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$

Si ha $(a1) \wedge (b) \Leftrightarrow \begin{cases} (a1) \\ (b1)\ \ s \in \mathbb{Z} \end{cases}$, perché d è privo di fattori quadratici.

Esprimiamo $(a2)$ nel modo equivalente $r = \frac{2n+1}{2},\ n \in \mathbb{Z}$.

Si ricava con semplici passaggi $(a2) \wedge (b) \Leftrightarrow \begin{cases} (a2) \\ (b2)\ \ 4ds^2 \equiv 1 \pmod 4 \end{cases}$

Sia ora $d \equiv 1 \pmod 4$. Allora si ha $(b2) \Leftrightarrow s \in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$.
Se invece $d \equiv 2,3 \pmod 4$ è facile verificare con semplici calcoli che $(b2)$ non può verificarsi.
Concludiamo perciò che:
se $d \equiv 1 \pmod 4$ allora α è un intero algebrico se e solo se valgono $(a1) \wedge (b1)$ o $(a2) \wedge (b2)$;
se $d \equiv 2,3 \pmod 4$ allora α è un intero algebrico se e solo se valgono $(a1) \wedge (b1)$. □

Gli interi algebrici in $\mathbb{Q}[\sqrt{d}]$ costituiscono un anello, che denoteremo A_d. Un risultato analogo vale per ogni campo di numeri (cfr.[Mar77], pag.16) ed ha quindi senso la seguente definizione.

Definizione 4. *Chiamiamo* ***anello di numeri*** *corrispondente al campo di numeri K l'anello degli interi algebrici di K.*

Notiamo che il risultato del teorema può essere espresso nella forma più sintetica

$$A_d = \mathbb{Z}[\omega_d] \text{ con } \omega_d = \begin{cases} \sqrt{d} & \text{se } d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{se } d \equiv 1 \pmod 4 \end{cases}$$

Introduciamo ora i concetti fondamentali di traccia e di norma, che qui vedremo solo nel caso particolare dei campi quadratici.
Se $\alpha = a + b\sqrt{d}$, con $a, b \in \mathbb{Q}$ è il generico elemento di $\mathbb{Q}[\sqrt{d}]$, denoteremo con $\overline{\alpha}$ l'elemento $a - b\sqrt{d}$. Esso coincide con il coniugato complesso di α per $d < 0$.

Definizione 5. *Definiamo la* ***traccia*** *T e la* ***norma*** *N di α come*

$$T(\alpha) = \alpha + \overline{\alpha}$$

$$N(\alpha) = \alpha\overline{\alpha}$$

Raccogliamo nelle osservazioni che seguono alcuni risultati utili riguardanti traccia e norma.

Osservazione 1. Se $\alpha = a + b\sqrt{d},\ a, b \in \mathbb{Q}$, allora ovviamente

$$T(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$$

$$N(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

Nel caso $d < 0$ si nota che la norma è sempre non negativa.

Osservazione 2. Dalla Definizione 5 segue immediatamente

$$T(\alpha + \beta) = T(\alpha) + T(\beta)$$

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

per ogni $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$.

Osservazione 3. Dalla dimostrazione del Teorema 2 e dalla Definizione 5 si deduce che $\alpha \in \mathbb{Q}[\sqrt{d}]$ è un intero algebrico se e solo se $T(\alpha), N(\alpha) \in \mathbb{Z}$.

Introduciamo la nozione di discriminante, sempre nel caso particolare dei campi quadratici complessi.

Definizione 6. *Per ogni coppia di elementi $\alpha, \beta \in \mathbb{Q}[\sqrt{d}]$ definiamo il* ***discriminante*** *di α, β come*

$$disc(\alpha, \beta) = \left(\det \begin{pmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{pmatrix} \right)^2$$

Nel prossimo paragrafo estenderemo la nozione di discriminante di elementi al concetto di discriminante dell'anello A_d.

1.2 Ideali dell'anello A_d

Definizione 7. *Sia $\mathfrak{a}$ un ideale di un anello commutativo A dotato di unità. Diciamo che gli elementi $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}$* ***generano*** *$\mathfrak{a}$ se ogni elemento $\alpha \in \mathfrak{a}$ può essere scritto nella forma*

$$\alpha = \rho_1\alpha_1 + \ldots + \rho_n\alpha_n$$

con $\rho_i \in A,\ i = 1, \ldots, n$.

Definizione 8. *Sia $\mathfrak{a}$ un ideale di un anello commutativo A dotato di unità. Diciamo che gli elementi $\alpha_1, \ldots, \alpha_n \in \mathfrak{a}$ sono una $\mathbb{Z}$-**base** di $\mathfrak{a}$ se ogni elemento $\alpha \in \mathfrak{a}$ può essere scritto nella forma*

$$\alpha = r_1\alpha_1 + \ldots + r_n\alpha_n$$

con $r_i \in \mathbb{Z},\ i = 1, \ldots, n$.

Introdotto il concetto di base, si ha il seguente teorema.

Teorema 3. *Siano $\{\beta_1, \beta_2\}$ e $\{\gamma_1, \gamma_2\}$ due $\mathbb{Z}$-basi per A_d. Allora*

$$disc(\beta_1, \beta_2) = disc(\gamma_1, \gamma_2)$$

Dimostrazione. Basta notare che

$$\begin{cases} \gamma_1 = r_{11}\beta_1 + r_{12}\beta_2, \\ \gamma_2 = r_{21}\beta_1 + r_{22}\beta_2 \end{cases} \qquad \text{con } \det \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix} = \pm 1$$

Si ottiene

$$\mathrm{disc}(\gamma_1, \gamma_2) = (r_{11}r_{22} - r_{12}r_{21})^2 \mathrm{disc}(\beta_1, \beta_2) = \mathrm{disc}(\beta_1, \beta_2)$$

□

Osservazione 4. Il Teorema 3 ci garantisce che il discriminante di una $\mathbb{Z}$-base è un invariante per l'anello A_d, e possiamo quindi parlare di $\mathrm{disc}(A_d)$ o anche di $\mathrm{disc}(\mathbb{Q}[\sqrt{d}])$. Utilizzando la definizione di discriminante sulla $\mathbb{Z}$-base $\{1, \omega_d\}$ otteniamo che

$$\mathrm{disc}(A_d) = \begin{cases} d & \text{se } d \equiv 1 \pmod 4 \\ 4d & \text{se } d \equiv 2, 3 \pmod 4 \end{cases}$$

Diamo ora due teoremi che riguardano gli ideali dell'anello A_d.

Teorema 4. *Sia $\mathfrak{a}$ un ideale non nullo di A_d. Allora $\mathfrak{a}$ possiede una $\mathbb{Z}$-base α_1, α_2 con $\alpha_1 = a_1 \in \mathbb{Z}$, dove $\mathfrak{a} \cap \mathbb{Z} = \mathbb{Z}a_1$.*

Dimostrazione. Sia $\alpha \in \mathfrak{a},\ \alpha \neq 0$. Vale $\alpha\overline{\alpha} = N(\alpha) \in \mathbb{Z} \cap \mathfrak{a}$. Quindi $\mathbb{Z} \cap \mathfrak{a} \neq (0)$ e $\mathbb{Z} \cap \mathfrak{a}$ è un ideale di $\mathbb{Z}$, quindi $\exists a_1 \in \mathbb{Z},\ a_1 \neq 0$, tale che $\mathbb{Z} \cap \mathfrak{a} = \mathbb{Z}a_1$.
Scegliamo l'elemento $\alpha_2 = a_2 + b_2\omega_d \in \mathfrak{a}$, con $a_2, b_2 \in \mathbb{Z}$ tali che

$$|b_2| = \min\{|b| : a + b\omega_d \in \mathfrak{a}, b \neq 0\}$$

Osserviamo che b_2 è ben definito, in quanto ad esempio $a_1\omega_d \in \mathfrak{a}\backslash\mathbb{Z}$.

Vale perciò $\alpha_1 = a_1 \in \mathbb{Q}\backslash\{0\}, \alpha_2 \notin \mathbb{Q}$. Gli elementi α_1, α_2 costituiscono quindi una base di $\mathbb{Q}[\sqrt{d}]$, visto come $\mathbb{Q}$-spazio vettoriale, in quanto linearmente indipendenti in uno spazio vettoriale di dimensione 2. Per ogni elemento $\alpha \in \mathbb{Q}[\sqrt{d}]$, in particolare per ogni $\alpha \in \mathfrak{a}$, esisteranno opportuni $q_1, q_2 \in \mathbb{Q}$ tali che

$$\alpha = q_1\alpha_1 + q_2\alpha_2.$$

Dobbiamo quindi mostrare che, se $\alpha \in \mathfrak{a}$, allora $q_1, q_2 \in \mathbb{Z}$. Sia $\alpha = a + b\omega_d$; posto $b = t_2b_2 + u_2$, con $t_2, u_2 \in \mathbb{Z},\ 0 \leq u_2 < |b_2|$, si ha

$$(a - t_2a_2) + u_2\omega_d = \alpha - t_2\alpha_2 \in \mathfrak{a}.$$

Per la minimalità di b_2 deve essere $u_2 = 0$, quindi $\alpha - t_2\alpha_2 = a - t_2a_2 \in \mathbb{Z} \cap \mathfrak{a}$ e quindi $a - t_2a_2 = t_1a_1 = t_1\alpha_1$ con $t_1 \in \mathbb{Z}$. Concludiamo perciò

$$\alpha = t_1\alpha_1 + t_2\alpha_2.$$

□

Teorema 5. *Sia $\mathfrak{a}$ un ideale non nullo di A_d. Allora l'anello quoziente $A_d/\mathfrak{a}$ possiede un numero finito di elementi. Più precisamente:*
se consideriamo per $\mathfrak{a}$ una $\mathbb{Z}$-base α_1, α_2 con $\alpha_1 = a_1 \in \mathbb{Z}$ e $\alpha_2 = a_2 + b_2\omega_d$, allora l'anello quoziente $A_d/\mathfrak{a}$ possiede esattamente $|a_1||b_2|$ elementi, rappresentati da

$$a + b\omega_d, \qquad 0 \leq a < |a_1|, \qquad 0 \leq b < |b_2| \tag{1.1}$$

Dimostrazione. Sia $\gamma = c + f\omega_d \in A_d$. Mediante la divisione con resto in $\mathbb{Z}$ scegliamo $g \in \mathbb{Z}$ tale che

$$f = gb_2 + t, \qquad 0 \leq t < |b_2|$$

e poniamo

$$\gamma' = \gamma - g\alpha_2 = c + (gb_2 + t)\omega_d - g(a_2 + b_2\omega_d) = (c - ga_2) + t\omega_d = c' + t\omega_d$$

Scegliamo ancora tramite la divisione con resto un $h \in \mathbb{Z}$ tale che

$$c' = ha_1 + e \qquad 0 \leq e < |a_1|$$

Allora vale

$$\gamma = g\alpha_2 + c' + t\omega_d = (g\alpha_2 + h\alpha_1) + (e + t\omega_d)$$

Siccome il primo addendo appartiene ad $\mathfrak{a}$ e il secondo è scritto nella forma (1.1), rimane solo da mostrare che gli elementi in (1.1) individuano laterali distinti. Da

$$(a + b\omega_d) - (a' + b'\omega_d) \in \mathfrak{a}$$

segue che $b - b'$ è multiplo di b_2. Da $0 \leq b, b' < |b_2|$ è possibile solo $b = b'$. Inoltre

$$a - a' \in \mathbb{Z} \cap \mathfrak{a} = \mathbb{Z}a_1$$

che implica, da $0 \leq a, a' < |a_1|$, che $a = a'$. □

Definizione 9. *Chiamiamo* ***indice*** *dell'ideale* $\mathfrak{a}$ *in* A_d *il numero di elementi di* $A_d/\mathfrak{a}$ *e lo indichiamo con* $[A_d : \mathfrak{a}]$.

Mostriamo che l'indice $[A_d : \mathfrak{a}]$ si può calcolare mediante una qualsiasi $\mathbb{Z}$-base. Se consideriamo una $\mathbb{Z}$-base $\beta_i = c_i + f_i\omega_d$ di $\mathfrak{a}$, vale

$$[A_d : \mathfrak{a}] = \left| det \begin{pmatrix} c_1 & f_1 \\ c_2 & f_2 \end{pmatrix} \right|$$

Infatti esiste una matrice M con $|det(M)| = 1$ tale che

$$\begin{pmatrix} a_1 & 0 \\ a_2 & b_2 \end{pmatrix} = M \begin{pmatrix} c_1 & f_1 \\ c_2 & f_2 \end{pmatrix}$$

e quindi si ottiene

$$\left| det \begin{pmatrix} c_1 & f_1 \\ c_2 & f_2 \end{pmatrix} \right| = |a_1||b_2|$$

che è effettivamente l'indice $[A_d : \mathfrak{a}]$, come stabilito nel Teorema 5.
La definizione di indice appena introdotta è legata fortemente alla definizione di norma di un elemento, come mostra il seguente teorema.

Teorema 6. *Sia* $\alpha \in A_d$ *e* $\mathfrak{a} = (\alpha)$ *l'ideale generato da* α. *Allora vale*

$$[A_d : \mathfrak{a}] = |N(\alpha)|$$

Dimostrazione. Gli elementi $\alpha, \alpha\omega_d$ costituiscono una $\mathbb{Z}$-base per $\mathfrak{a}$.
Se $\alpha = a + b\omega_d$ si ha

$$\alpha\omega_d = b\frac{d-1}{4} + (a+b)\omega_d, \qquad [A_d : \mathfrak{a}] = \left| det \begin{pmatrix} a & b \\ b\frac{d-1}{4} & a+b \end{pmatrix} \right| = |N(\alpha)|$$

per $d \equiv 1 \pmod 4$, e

$$\alpha\omega_d = bd + a\omega_d \qquad [A_d : \mathfrak{a}] = \left| det \begin{pmatrix} a & b \\ bd & a \end{pmatrix} \right| = |N(\alpha)|$$

per $d \equiv 2, 3 \pmod 4$ □

1.3 Proprietà di A_d come dominio di Dedekind

Definizione 10. *Sia D un anello commutativo. Un ideale $\mathfrak{a}$ diverso da D si dice* ***primo*** *se e solo se da $a, b \in D$ e $ab \in \mathfrak{a}$ segue $a \in \mathfrak{a}$ o $b \in \mathfrak{a}$.*

Definizione 11. *Un* ***dominio di Dedekind*** *è un dominio di integrità D tale che*

1. *ogni ideale è finitamente generato;*
2. *ogni ideale primo non nullo è massimale;*
3. *D è integralmente chiuso nel suo campo dei quozienti K.*

L'ultima condizione significa che se $\alpha/\beta \in K$ è radice di un polinomio monico a coefficienti in D, allora $\alpha/\beta \in D$.

Teorema 7. *Ogni insieme I non vuoto di ideali propri di un dominio di Dedekind D possiede un elemento massimale, ovvero esiste un $\mathfrak{m} \in I$ tale che da $\mathfrak{m} \subseteq \mathfrak{i} \in I$ segue $\mathfrak{m} = \mathfrak{i}$.*

Dimostrazione. Dimostriamo, innanzitutto, che ogni catena di ideali di D del tipo

$$\mathfrak{i}_1 \subseteq \mathfrak{i}_2 \subseteq \mathfrak{i}_3 \subseteq \dots$$

è stazionaria. Consideriamo infatti l'ideale $\mathfrak{i} = \bigcup \mathfrak{i}_n$ (il fatto che sia un ideale si dimostra facilmente: $\forall \alpha, \beta \in \mathfrak{i},\ \exists\ \overline{n}$ tale che $\alpha, \beta \in \mathfrak{i}_{\overline{n}}$; pertanto $\alpha - \beta \in \mathfrak{i}_{\overline{n}} \subseteq \mathfrak{i}$, e $\forall \delta \in D,\ \delta\alpha \in \mathfrak{i}_{\overline{n}} \subseteq \mathfrak{i}$). Esso è finitamente generato. Allora deve esistere un ideale $\mathfrak{i}_{\overline{n}}$ della catena che contiene tutti i generatori di $\mathfrak{i}$, pertanto $\mathfrak{i}_{\overline{n}} = \mathfrak{i}$ e così tutti gli ideali successivi.
A questo punto consideriamo il nostro insieme I. Se per assurdo non esistesse in esso un ideale massimale, vorrebbe dire che $\forall \mathfrak{i} \in I,\ \exists \mathfrak{j} \in I$ tale che $\mathfrak{i} \subset \mathfrak{j}$ propriamente e sarebbe quindi possibile costruire una catena ascendente non stazionaria. Assurdo. □

Valgono i seguenti teoremi, di cui omettiamo la dimostrazione (cfr.[Mar77], pagg.56-60).

Teorema 8. *Sia* $\mathfrak{a}$ *un ideale non nullo nel dominio di Dedekind* D*. Allora esiste un ideale* $\mathfrak{b}$ *tale che* $\mathfrak{ab}$ *è principale.*

Teorema 9. *Ogni ideale proprio in un dominio di Dedekind* D *si può rappresentare in modo unico come prodotto di ideali primi.*

Con questi risultati possiamo provare il teorema fondamentale per la nostra trattazione.

Teorema 10. *Un dominio di Dedekind* D *è un UFD se e solo se è un PID.*

Dimostrazione. Come ben sappiamo un PID è sempre un UFD. Per quanto riguarda i domini di Dedekind, questa proprietà si può anche facilmente ricavare dal Teorema 9.
Proviamo ora l'altra implicazione. Per assurdo, assumiamo che D non sia un PID. Sia $\mathfrak{p}$ un ideale proprio primo non principale (che deve esistere in virtù del Teorema 9, altrimenti tutti gli ideali sarebbero principali). Consideriamo l'insieme degli ideali $\mathfrak{i}$ tali che $\mathfrak{pi}$ è principale (il Teorema 8 ci garantisce che questo insieme non è vuoto). Fissiamo un suo elemento massimale $\mathfrak{m}$ (la cui esistenza è garantita dal Teorema 7). Poniamo $\mathfrak{pm} = (\alpha)$. Si ha che α è irriducibile, dal momento che se $\alpha = \beta\gamma$, allora, sempre per il Teorema 9, o (β) o (γ) sono della forma $\mathfrak{pj}$, per qualche $\mathfrak{j}$ che divide $\mathfrak{m}$. La massimalità di $\mathfrak{m}$ implica $\mathfrak{j} = \mathfrak{m}$, perciò uno tra β e γ deve essere unitario.
D'altra parte, fissiamo un $\delta \in \mathfrak{p}\backslash(\alpha)$ e un $\varepsilon \in \mathfrak{m}\backslash(\alpha)$ (che esistono rispettivamente in quanto $\mathfrak{p}$ non è principale e in quanto $\mathfrak{p} \neq D$) e notiamo che $\delta\varepsilon \in (\alpha)$. Perciò $\alpha|\delta\varepsilon$, ma α non divide né δ né ε. Abbiamo perciò che α è un irriducibile che non è primo, assurdo perché D è un UFD. □

Quanto detto si può applicare all'anello A_d, che è un dominio di Dedekind. Sussiste infatti un teorema più generale, di cui omettiamo la dimostrazione (cfr.[Mar77], pagg.56-60).

Teorema 11. *Ogni anello di numeri è un dominio di Dedekind.*

Ricapitoliamo perciò i risultati che ci interesseranno per il seguito:

1. A_d è un UFD se e solo se A_d è un PID;
2. in A_d ogni ideale proprio è rappresentabile in modo unico come prodotto di ideali primi.

1.4 Cenni sulle forme quadratiche

Definizione 12. *Una* ***forma quadratica binaria*** *su $\mathbb{Z}$ è un'espressione*

$$ax^2 + bxy + cy^2$$

omogenea, di secondo grado nelle variabili, con coefficienti $a, b, c \in \mathbb{Z}$.

Nel contesto delle forme quadratiche è fondamentale il concetto di equivalenza che ora andremo ad illustrare.

Si riconosce facilmente che due forme quali $2x^2+3y^2$ e $3x^2+2y^2$ in realtà coincidono, essendo l'una ottenuta dall'altra mediante un semplice cambio di variabili. Non è altrettanto evidente che la forma $2x^2 + 4xy + 5y^2$ sia essenzialmente la stessa delle due appena menzionate. Tuttavia essa può essere scritta come

$$2(x + y)^2 + 3y^2$$

e quando le variabili x e y assumono tutti i valori interi, lo stesso accade per le variabili $x + y$ e y, e viceversa. La prima forma e la terza sono collegate da una sostituzione molto semplice: se poniamo $x = X + Y$ e $y = Y$, allora

$$2x^2 + 3y^2 = 2X^2 + 4XY + 5Y^2$$

La domanda che ci poniamo è la seguente: quali sostituzioni del tipo

$$x = pX + qY, \qquad y = rX + sY \tag{1.2}$$

hanno la proprietà di stabilire una corrispondenza biunivoca fra tutte le coppie di interi x, y e tutte le coppie di interi X, Y. Procediamo nel seguente modo: moltiplichiamo la prima equazione per s, la seconda per q e sottraiamo, ottendendo

$$sx - qy = (ps - qr)X$$

e in modo analogo otteniamo

$$-rx + py = (ps - qr)Y$$

Il numero $ps - qr$ non può essere zero, poiché in tal caso $sx - qy$ e $-rx + py$ sarebbero sempre nulli e le variabili x e y non sarebbero indipendenti. Ponendo $\Delta = ps - qr$ e dividendo per Δ, le equazioni che esprimono X e Y in termini di x e y sono

$$X = \frac{s}{\Delta}x - \frac{q}{\Delta}y, \qquad Y = -\frac{r}{\Delta}x + \frac{p}{\Delta}y \tag{1.3}$$

I quattro coefficienti devono essere interi e ciò è sicuramente vero se $\Delta = \pm 1$. Viceversa, se i coefficienti sono interi, lo è anche

$$\frac{p}{\Delta}\frac{s}{\Delta} - \frac{q}{\Delta}\frac{r}{\Delta} = \frac{1}{\Delta}$$

che è intero solo se $\Delta = \pm 1$.

La sostituzione ha, quindi, la proprietà desiderata di far corrispondere tutte le coppie di interi x, y con tutte le coppie di interi X, Y e viceversa se e solo se i coefficienti p, q, r, s della sostituzione sono interi e $ps - qr = \pm 1$.

Definizione 13. *Definiamo $ps - qr$* ***determinante*** *della sostituzione. Una sostituzione della forma* (1.2) *con coefficienti interi e determinante 1 viene detta* ***sostituzione unimodulare****.*

Per evitare complicazioni nel seguito non considereremo sostituzioni con determinante -1. Possiamo finalmente introdurre la seguente definizione.

Definizione 14. *Due forme collegate da una sostituzione unimodulare sono dette* ***equivalenti****.*

Sarà conveniente denotare una forma quadratica $ax^2 + bxy + cy^2$ con i suoi coefficienti interi (a, b, c). Introduciamo ora la nozione di discriminante di una forma.

Definizione 15. *Il **discriminante** di una forma quadratica (a, b, c) è definito come il numero $b^2 - 4ac$.*

Si verifica in modo diretto che forme equivalenti hanno lo stesso discriminante (non vale in generale il viceversa).

Consideriamo ora le forme con discriminante negativo.
Moltiplichiamo la forma per $4a$ ed effettuiamo la procedura di completare il quadrato, come segue:

$$4a(ax^2 + bxy + cy^2) = 4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 + (4ac - b^2)y^2$$

Poiché in questo caso $4ac - b^2 > 0$, l'ultima espressione è sempre positiva tranne che per $x = y = 0$, in cui è uguale a zero. Ne segue che tutti i valori assunti dalla forma hanno lo stesso segno, che è lo stesso di a. Chiameremo una tale forma **definita positiva** se $a > 0$, **definita negativa** se $a < 0$.
È sempre possibile passare da una forma definita negativa ad una forma definita positiva, semplicemente cambiando segno a tutti i coefficienti. Pertanto nel trattare le forme definite è sufficiente considerare solo quelle definite positive.

Tutte le infinite forme di dato discriminante d possono essere ridistribuite in classi, mettendo nella stessa classe qualsiasi coppia di forme equivalenti. Mediante un numero finito di passaggi (cfr.[Dav], pagg.125-126) possiamo mostrare che ogni forma positiva è equivalente ad una i cui coefficienti soddisfano una delle condizioni seguenti:

$$\begin{cases} c > a \quad \text{e} \quad -a < b \leq a \\ c = a \quad \text{e} \quad 0 \leq b \leq a \end{cases} \tag{1.4}$$

Chiameremo **ridotta** una forma con tali condizioni. È notevole ed importante il teorema (di cui non daremo la dimostrazione) per cui esiste una e

una sola forma ridotta equivalente a una forma data. Alla luce di tale teorema il problema se due date forme siano o meno equivalenti può essere risolto riducendo ognuna di esse. Se le due forme ridotte coincidono, allora quelle assegnate sono equivalenti, altrimenti no.

Dalle condizioni (1.4) segue facilmente che esistono solo un numero finito di forme di discriminante d assegnato. Poniamo $d = -D$, cosicchè D è positivo e

$$4ac - b^2 = D$$

Poiché $b^2 \leq a^2 \leq ac$, per la (1.4), si ha $3ac \leq D$. Esistono solo un numero finito di interi positivi a e c che soddisfano tale condizione e, per ogni scelta di a e c, esistono al più due possibilità per b. Il numero delle forme ridotte è naturalmente uguale al numero di classi di equivalenza di forme, poiché vi è precisamente una forma ridotta in ciascuna classe. Questo numero è denominato **numero di classi di discriminante** d.

1.5 Ideali frazionari e numero di classi di ideali

Si ricordi che un ideale di A_d può essere descritto come un A_d-sottomodulo di A_d. Andiamo allora a considerare gli A_d-sottomoduli di $\mathbb{Q}[\sqrt{d}]$ e diamo la seguente definizione.

Definizione 16. *Un A_d-sottomodulo $\mathfrak{A}$ di $\mathbb{Q}[\sqrt{d}]$ si dice **ideale frazionario** di A_d se esiste un $\gamma \in A_d$, $\gamma \neq 0$, tale che $\gamma\mathfrak{A} \subseteq A_d$.*

Osservazione 5. L'insieme $\mathfrak{b} = \gamma\mathfrak{A}$ è un ideale di A_d e $\mathfrak{A} = \gamma^{-1}\mathfrak{b}$. Perciò gli ideali frazionari di A_d sono i sottoinsiemi di $\mathbb{Q}[\sqrt{d}]$ della forma $\gamma^{-1}\mathfrak{b}$, dove $\mathfrak{b}$ è un ideale di A_d e γ è un elemento di A_d non nullo.

Osservazione 6. Un ideale di A_d è chiaramente un ideale frazionario e viceversa un ideale frazionario è un ideale se e solo se è contenuto in A_d.

Il prodotto di ideali frazionari è ancora un ideale frazionario. Infatti, se $\mathfrak{A}_1 = \gamma_1^{-1}\mathfrak{b}_1, \mathfrak{A}_2 = \gamma_2^{-1}\mathfrak{b}_2$, dove $\mathfrak{b}_1, \mathfrak{b}_2$ sono ideali e γ_1, γ_2 sono elementi non nulli di A_d, allora $\mathfrak{A}_1\mathfrak{A}_2 = (\gamma_1\gamma_2)^{-1}\mathfrak{b}_1\mathfrak{b}_2$. In più vale il seguente teorema.

Teorema 12. *Gli ideali frazionari non nulli di A_d formano un gruppo abeliano, che denotiamo $\mathcal{F}$, con l'operazione moltiplicazione.*

Traccia della dimostrazione. La proprietà associativa e la proprietà commutativa seguono dalle stesse proprietà in $\mathbb{Q}[\sqrt{d}]$. A_d è l'unità del gruppo. Per ogni ideale $\mathfrak{b}$ di A_d definiamo

$$\mathfrak{b}^{-1} = \{\alpha \in \mathbb{Q}[\sqrt{d}] \mid \alpha\mathfrak{b} \subseteq A_d\}$$

Chiaramente $\mathfrak{b}^{-1}$ è un A_d-sottomodulo e, se $\mathfrak{b} \neq (0)$ allora $\forall \gamma \in \mathfrak{b}, \gamma \neq 0$, abbiamo $\gamma\mathfrak{b}^{-1} \subseteq A_d$, quindi $\mathfrak{b}^{-1}$ è un ideale frazionario. Dalla definizione segue

$$\mathfrak{b}\mathfrak{b}^{-1} = \mathfrak{b}^{-1}\mathfrak{b} \subseteq A_d$$

Si può dimostrare che vale l'uguaglianza (cfr.[Ste79], pag.112-116).
Perciò, dato un ideale frazionario non nullo $\mathfrak{A} = \gamma^{-1}\mathfrak{b}$, il suo inverso è $\mathfrak{A}^{-1} = \gamma\mathfrak{b}^{-1}$. □

Definizione 17. *Diciamo che un ideale frazionario è **principale** se è della forma $\gamma^{-1}(\beta)$, dove (β) è un ideale principale di A_d.*

È facile rendersi conto che l'insieme degli ideali principali frazionari è un sottogruppo di $\mathcal{F}$, ed è un sottogruppo normale, in quanto $\mathcal{F}$ abeliano. Chiamiamo $\mathcal{P}$ tale sottogruppo.

Definizione 18. *Diciamo $\mathcal{H} = \mathcal{F}/\mathcal{P}$ **gruppo di classi di ideali**. Definiamo inoltre **numero di classi di ideali** l'ordine di tale gruppo e lo indichiamo con $h(d)$.*

Osservazione 7. Si noti che il simbolo $h(d)$ sottolinea la dipendenza di tale numero dall'anello A_d che si considera: $h(d)$ è il numero di classi di ideali dell'anello A_d. Con abuso di notazione si dice spesso che $h(d)$ è il numero di classi di ideali del campo $\mathbb{Q}[\sqrt{d}]$, intendendo in realtà il numero di classi di ideali dell'anello di numeri corrispondente.

Due ideali frazionari $\mathfrak{A}, \mathfrak{B}$ sono equivalenti se appartengono allo stesso laterale di $\mathcal{P}$ in $\mathcal{F}$. Indichiamo con $[\mathfrak{A}]$ la classe di equivalenza contenente $\mathfrak{A}$. Sappiamo che $\mathfrak{A} = \gamma^{-1}\mathfrak{b}$, quindi $\mathfrak{b} = \gamma\mathfrak{A} = (\gamma)\mathfrak{A}$ da cui segue che $\mathfrak{b} \in [\mathfrak{A}]$. Abbiamo dunque che ogni classe di equivalenza contiene un ideale.

Siano ora $\mathfrak{i}$ e $\mathfrak{j}$ ideali equivalenti. Allora $\mathfrak{i} = \mathfrak{A}\mathfrak{j}$ dove $\mathfrak{A}$ è un ideale frazionario principale, ovvero $\mathfrak{A} = \gamma^{-1}(\beta)$, con (β) ideale principale. Quindi $\mathfrak{i}(\gamma) = \mathfrak{j}(\beta)$. Viceversa se $\mathfrak{i}(\gamma) = \mathfrak{j}(\beta)$ con $(\gamma), (\beta)$ ideali principali, allora $\mathfrak{i}$ e $\mathfrak{j}$ appartengono alla stessa classe.

Questo ci permette di descrivere $\mathcal{H}$ come segue: consideriamo l'insieme $\mathcal{I}$ degli ideali di A_d e definiamo su di esso la relazione $\sim$, dove

$$\mathfrak{i} \sim \mathfrak{j} \quad \Leftrightarrow \quad \exists \beta, \gamma \ \text{ tali che } \ \mathfrak{i}(\gamma) = \mathfrak{j}(\beta)$$

Allora $\mathcal{H}$ è l'insieme delle classi di equivalenza $[\mathfrak{i}]$ con l'operazione di gruppo definita da

$$[\mathfrak{i}][\mathfrak{j}] = [\mathfrak{ij}]$$

Questa è la ragione per cui $\mathcal{H}$ si chiama gruppo di classi di ideali.

Abbiamo ora il teorema fondamentale

Teorema 13. *A_d è un UFD se e solo se $h(d) = 1$.*

Dimostrazione. A_d è UFD se e solo se A_d è un PID (Teorema 10). Dalla definizione di ideale frazionario e di ideale frazionario principale segue che A_d è un PID se e solo se ogni ideale frazionario è principale, che è equivalente a chiedere $\mathcal{F} = \mathcal{P}$, ovvero a $|\mathcal{H}| = h(d) = 1$ □

Concludiamo questo primo capitolo con la seguente osservazione.

Osservazione 8. Esiste un corrispondenza 1-1 tra l'insieme delle forme quadratiche binarie ridotte con discriminante negativo d, $d \equiv 1 \pmod 4$, e l'insieme delle classi di ideali del campo quadratico d. Sia (a, b, c) una forma quadratica binaria, definita positiva, ridotta, con discriminante d, $d \equiv 1 \pmod 4$, e si consideri la funzione che manda la forma (a, b, c) nella classe di ideali contenente $(a, \frac{-b+\sqrt{d}}{2})$. Questa funzione è iniettiva e surietti-va (cfr.[Par]), quindi il numero di forme ridotte è uguale al numero di classi di ideali, per $d \equiv 1 \pmod 4$.

Capitolo 2

Campi quadratici complessi in cui A_d è euclideo

2.1 Preliminari sui domini euclidei

La teoria dei numeri in $\mathbb{Z}$ si basa sull'algoritmo delle divisioni, che garantisce l'esistenza e l'unicità della fattorizzazione in primi e del massimo comune divisore. Possiamo svolgere considerazioni analoghe in anelli che ammettono divisione con resto, ovvero gli anelli euclidei, di cui richiamiamo la definizione.

Definizione 19. *Un dominio di integrità D dotato di unità è un* ***dominio euclideo*** *se si può definire un'applicazione $\varphi : D\backslash\{0\} \to \mathbb{N}_0$ tale che*

1. *se $\alpha, \beta \in D\backslash\{0\}$ e $\alpha|\beta$, allora $\varphi(\alpha) \leq \varphi(\beta)$,*
2. *per ogni $\alpha, \beta \in D$ con $\beta \neq 0$ esistono $\gamma, \rho \in D$ tali che $\alpha = \beta\gamma + \rho$ con $\rho = 0$ o $\rho \neq 0$ e $\varphi(\rho) < \varphi(\beta)$.*

Consideriamo ora A_d con la norma N della Definizione 5.

Definizione 20. *A_d o (con meno precisione) $\mathbb{Q}[\sqrt{d}]$ si chiama* ***N-euclideo*** *se A_d è un dominio euclideo con la funzione $\varphi : \alpha \mapsto |N(\alpha)|$.*

Osservazione 9. Dall'Osservazione 2 ($N(\alpha\beta) = N(\alpha)N(\beta)$) si deduce facilmente che la prima condizione della Definizione 19 è sempre verificata in A_d. Pertanto per verificare se A_d è $N-$euclideo basterà controllare se vale la seconda condizione.

Osservazione 10. Per $d < 0$ si ha $N : A_d\backslash\{0\} \to \mathbb{N}_0$. In tal caso si può omettere il valore assoluto e si ha quindi che φ coincide con N.

Stabiliamo ora un teorema fondamentale per gli sviluppi successivi, premettendo ad esso un lemma utile per la dimostrazione.

Lemma 1. *$\mathbb{Q}[\sqrt{d}]$ è il campo dei quozienti di A_d.*

Dimostrazione. Chiamiamo K il campo dei quozienti di A_d in $\mathbb{Q}[\sqrt{d}]$. Poiché $\mathbb{Z} \subseteq A_d$, si ha che $\mathbb{Q} \subset K$. Dato $A_d = \mathbb{Z}[\omega_d]$, si ha che $\omega_d \in K$ e quindi $\mathbb{Q}[\sqrt{d}] \subseteq K$. Poiché $\mathbb{Q}[\sqrt{d}]$ è campo, vale l'uguaglianza. □

Teorema 14. *A_d è N-euclideo se e solo se per ogni $\eta \in Q[\sqrt{d}]$ esiste un $\gamma \in A_d$ con $|N(\eta - \gamma)| < 1$.*

Dimostrazione. Proviamo le due implicazioni:
$\Rightarrow$) Sia $\eta \in Q[\sqrt{d}]$. Per il Lemma 1, si ha che $\eta = \alpha/\beta$, con $\alpha, \beta \in A_d,\ \beta \neq 0$. Per ipotesi, esistono $\gamma, \rho \in A_d$, con $\rho = 0$ o $|N(\rho)| < |N(\beta)|$, tali che $\alpha = \gamma\beta + \rho$. Abbiamo quindi che

$$1 > \frac{|N(\rho)|}{|N(\beta)|} = \left|N\left(\frac{\rho}{\beta}\right)\right| = \left|N\left(\frac{\alpha}{\beta} - \gamma\right)\right| = |N(\eta - \gamma)|$$

$\Leftarrow$) Siano $\alpha, \beta \in A_d$, $\beta \neq 0$. Per ipotesi si ha che esiste $\gamma \in A_d$ tale che

$$\left|N\left(\frac{\alpha}{\beta} - \gamma\right)\right| = \left|N\left(\frac{\alpha - \gamma\beta}{\beta}\right)\right| < 1$$

Chiamiamo $\rho = \alpha - \gamma\beta$ (ρ può anche essere nullo). Si ha in ogni caso $|N(\rho)| < |N(\beta)|$, da cui la tesi. □

2.2 Determinazione degli A_d euclidei

Cominciamo dimostrando un semplice lemma.

Lemma 2. *Sia $d < 0$. Allora si ha che l'insieme degli unitari in A_d è costituito dai seguenti elementi:*

$$\begin{cases} \{1, \sqrt{-1}, -1, -\sqrt{-1}\} & \text{se } d = -1 \\ \left\{\pm 1, \pm\left(\frac{-1+\sqrt{-3}}{2}\right), \pm\left(\frac{1+\sqrt{-3}}{2}\right)\right\} & \text{se } d = -3 \\ \{1, -1\} & \text{altrimenti} \end{cases}$$

Dimostrazione. Dalla Definizione 5 e dalle Osservazioni 2 e 3 si deduce facilmente che in A_d, $d < 0$, un elemento α è unitario se e solo se la sua norma è 1.

Ricordando la forma degli elementi di A_d si deduce che trovare elementi di norma 1 corrisponde a trovare le soluzioni intere di

$$x^2 + |d|y^2 = 1 \qquad \text{se } d \equiv 2, 3 \pmod 4$$

$$\begin{cases} x^2 + |d|y^2 = 4 \\ x \equiv y \pmod 2 \end{cases} \qquad \text{se } d \equiv 1 \pmod 4$$

Da cui la tesi. □

Teorema 15. *Per $d<0$ sono equivalenti:*

1. *$d \in \{-1, -2, -3, -7, -11\}$;*
2. *A_d è N-euclideo;*
3. *A_d è euclideo.*

Dimostrazione. 1) $\Leftrightarrow$ 2) Consideriamo il caso $d \equiv 2, 3 \pmod 4$.

Ricordando che $A_d = \mathbb{Z}[\sqrt{d}]$, si ha che gli elementi di A_d formano una griglia nel piano complesso, come si vede in Figura 1.

I punti con la più grande distanza minima dai punti della griglia sono proprio i punti centrali delle maglie fondamentali. La condizione del Teorema 14

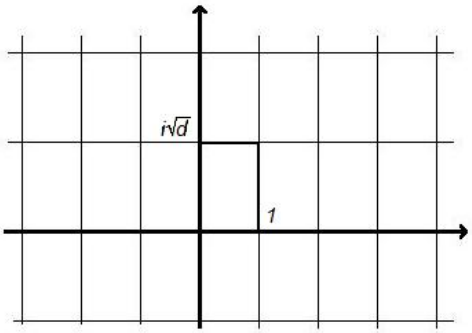

Figura 1

è verificata se e solo se la diagonale della maglia fondamentale ha una lunghezza < 2, cioè quando

$$\sqrt{1+|d|} < 2$$

Questo si verifica se e solo se $d = -1, -2$.

Consideriamo ora il caso $d \equiv 1 \pmod 4$.
Si ha $A_d = Z\left[\frac{1+i\sqrt{|d|}}{2}\right]$ e la situazione è un po' più complicata. I punti di A_d formano una griglia come nella Figura 2.

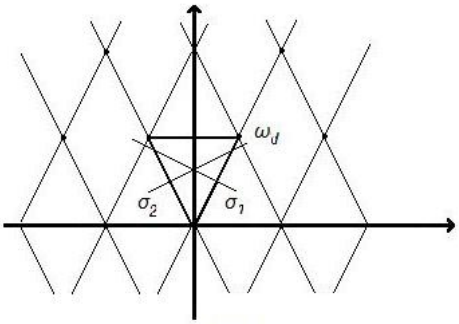

Figura 2

Qui la maglia fondamentale è un rombo. Per trovare i punti con la più grande distanza minima dai punti della griglia, consideriamo mezzo rombo: un triangolo isoscele con base 1 e lato

$$\frac{1}{2}\sqrt{1+|d|}$$

Il punto che stiamo cercando è il centro della circonferenza inscritta in questo triangolo, cioè l'intersezione degli assi dei lati del triangolo. L'equazione dell'asse σ_1 è, in coordinate cartesiane,

$$y - \frac{1}{4}\sqrt{|d|} = -\frac{1}{\sqrt{|d|}}\left(x - \frac{1}{4}\right)$$

Quindi

$$y = \frac{1}{\sqrt{|d|}}\left(x - \frac{1}{4}(|d|) + 1\right)$$

L'intersezione con l'asse immaginario è $\left(0, \frac{1}{4}\left(\sqrt{|d|} + \frac{1}{\sqrt{|d|}}\right)\right)$, e il raggio della circonferenza è

$$\frac{1}{4}\left(\sqrt{|d|} + \frac{1}{\sqrt{|d|}}\right)$$

Vale

$$\frac{1}{4}\left(\sqrt{|d|} + \frac{1}{\sqrt{|d|}}\right) < 1 \Leftrightarrow \frac{1}{16}\left(|d| + 2 + \frac{1}{|d|}\right) < 1 \Leftrightarrow |d| < 13$$

(per $d \in \mathbb{Z}$). Da cui otteniamo l'equivalenza (1) $\Leftrightarrow$ (2) del teorema.

2) $\Rightarrow$ 3) è ovvio.

3) $\Rightarrow$ 1) Sia A_d euclideo relativamente ad una funzione φ. Scegliamo tra tutti gli elementi non unitari diversi da 0 un elemento $\zeta \in A_d$ con $\varphi(\zeta)$ minimo. Sia $\eta \in A_d$. Allora si ha

$$\eta = \gamma\zeta + \rho \tag{2.1}$$

con $\rho = 0$ o $\varphi(\rho) < \varphi(\zeta)$. Dalla scelta di ζ segue $\rho = 0$ o ρ unitario. Sia $\mathfrak{a} = A_d\zeta$ l'ideale generato da ζ in A_d e $\pi : A_d \to A_d/\mathfrak{a}$ l'epimorfismo naturale. La (2.1) implica che $\pi(\eta) = \pi(\rho)$ con ρ unitario o $\rho = 0$. Supponiamo, per assurdo, che d non sia nessuno dei numeri di 1). Per il Lemma 2 gli unitari in A_d sono solo $+1$ e -1. Quindi

$$\pi(\eta) \in \{\pi(0), \pi(1), \pi(-1)\}$$

per ogni $\eta \in A_d$ e quindi $|A_d/\mathfrak{a}| \leq 3$. Abbiamo dimostrato (Teorema 6) che vale

$$|A_d/\mathfrak{a}| = N(\zeta)$$

da cui segue $N(\zeta) \leq 3$.

Nel caso $d \equiv 2, 3 \pmod 4, |d| > 3$, si ha

$$N(\zeta) = N(a + b\sqrt{d}) = a^2 + b^2|d| \leq 3 \Leftrightarrow |a| = 1, b = 0$$

poiché $\zeta \neq 0$.

Nel caso $d \equiv 1 \pmod 4$, $d > 12$, si ha

$$N(\zeta) = N\left(\frac{a + b\sqrt{d}}{2}\right) = \frac{a^2 + b^2|d|}{4} \leq 3 \Leftrightarrow |a| = 2, b = 0$$

sempre perché $\zeta \neq 0$ e perché $a \equiv b \pmod 2$.

In ogni caso si ha $\zeta = \pm 1$, in contraddizione con la scelta di ζ. □

Capitolo 3

Fattorizzazione in A_d per $-200 \leq d \leq -1$

3.1 Preliminari sulla fattorizzazione in A_d

In questo capitolo ci occuperemo di stabilire quali tra gli anelli di numeri A_d, con $-200 \leq d \leq -1$, siano UFD. I risultati che otterremo si possono facilmente estendere a intervalli più grandi, ma l'intervallo $-200 \leq d \leq -1$ è quello di ampiezza minima per ciò che dimostreremo nel capitolo successivo.

Innanzitutto, sappiamo che ogni anello euclideo è un UFD. Pertanto il Teorema 15 ci garantisce che per $d \in \{-1, -2, -3, -7, -11\}$ si ha che A_d è un UFD.

Dimostriamo ora un semplice teorema.

Teorema 16. *Sia $d \neq -1, -2$. Allora $\mathbb{Z}[\sqrt{d}]$ non è un UFD.*

Dimostrazione. Andiamo a considerare l'elemento 2 in $\mathbb{Z}[\sqrt{d}]$.
Abbiamo $N(2) = 4$, quindi gli eventuali divisori propri di 2 hanno norma 2. È facile osservare che per $d \neq -1, -2$ non esistono elementi in $\mathbb{Z}[\sqrt{d}]$ di norma 2, pertanto si ha che 2 è irriducibile per $d \neq -1, -2$.
Dimostriamo ora che per $d < 0$ l'elemento 2 non è mai primo.

Nel caso di d dispari si ha che

$$2|(d+1) = (1 + i\sqrt{|d|})(1 - i\sqrt{|d|})$$

ma ovviamente 2 non divide nessuno dei due fattori.
Nel caso di d pari si ha che

$$2|d = (i\sqrt{|d|})(-i\sqrt{|d|})$$

ma ancora 2 non divide nessuno dei due fattori.
Concludiamo, quindi, che 2 è irriducibile ma non primo per $d \neq -1, -2$, pertanto $\mathbb{Z}[\sqrt{d}]$ non è un UFD. □

Osservazione 11. Dai teoremi 15 e 16, ricordando la forma degli anelli A_d (Teorema 2), si ha che, per $d \equiv 2, 3 \pmod 4$, gli unici valori di d per cui A_d è un UFD sono -1 e -2.

Andiamo ora a dimostrare vari risultati che ci permetteranno di trattare il caso $d \equiv 1 \pmod 4$.

3.2 Fattorizzazione in ideali primi degli ideali principali (p)

Lemma 3. *Siano $\mathfrak{a}, \mathfrak{b}_1, \mathfrak{b}_2$ ideali di un anello commutativo dotato di unità. Si ha*

$$(\mathfrak{a} + \mathfrak{b}_1)(\mathfrak{a} + \mathfrak{b}_2) \subseteq \mathfrak{a} + \mathfrak{b}_1\mathfrak{b}_2$$

Dimostrazione. Siano $\alpha \in \mathfrak{a},\ \beta_1 \in \mathfrak{b}_1,\ \beta_2 \in \mathfrak{b}_2$. Allora

$$\begin{aligned}(\alpha + \beta_1)(\alpha + \beta_2) &= \alpha^2 + \alpha\beta_1 + \alpha\beta_2 + \beta_1\beta_2 \\ &= (\alpha + \beta_1 + \beta_2)\alpha + \beta_1\beta_2 \quad \in \mathfrak{a} + \mathfrak{b}_1\mathfrak{b}_2\end{aligned}$$

□

Lemma 4. *Sia D un anello di numeri. Allora se $\mathfrak{a}$ e $\mathfrak{b}$ sono ideali non nulli di D si ha*

$$[D : \mathfrak{ab}] = [D : \mathfrak{a}][D : \mathfrak{b}]$$

Dimostrazione. Si veda [Ste79], pagg.122-123. □

Teorema 17. *Sia K un campo di numeri di grado n con anello di numeri $D = \mathbb{Z}[\omega]$, con $\omega \in D$. Dato un primo $p \in \mathbb{Z}$, supponiamo che il polinomio minimo f di ω su $\mathbb{Q}$ abbia la seguente fattorizzazione in irriducibili su $\mathbb{Z}_p[t]$:*

$$\overline{f} = \overline{f}_1^{e_1} \dots \overline{f}_r^{e_r}$$

dove la barra denota l'omomorfismo naturale di anelli $\mathbb{Z}[t] \to \mathbb{Z}_p[t]$. Allora, se $f_i \in \mathbb{Z}[t]$ è una qualsiasi controimmagine di $\overline{f}_i$, l'ideale

$$\mathfrak{p}_i = (p) + (f_i(\omega))$$

è primo e la fattorizzazione in ideali primi dell'ideale (p) in D è

$$(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

Dimostrazione. Sia θ_i una radice di $\overline{f}_i$ in $\mathbb{Z}_p[\theta_i] \cong \mathbb{Z}_p[t]/(\overline{f}_i)$. C'è un omomorfismo naturale suriettivo $\nu_i : \mathbb{Z}[\omega] \to \mathbb{Z}_p[\theta_i]$ dato da

$$\nu_i(p(\omega)) = \overline{p}(\theta_i)$$

L'immagine di ν_i è $\mathbb{Z}_p[\theta_i]$ che è un campo, poiché $\overline{f}_i$ è irriducibile. Si ha, quindi, che $\ker \nu_i$ è un ideale massimale (e dunque primo) di $\mathbb{Z}[\omega] = D$. Chiaramente

$$(p) + (f_i(\omega)) \subseteq \ker \nu_i$$

Mostriamo l'altra inclusione. Sia $g(\omega) \in \ker \nu_i$, allora $\overline{g}(\theta_i) = 0$ e quindi $\overline{g} = \overline{f}_i \overline{h}$ per qualche $\overline{h} \in \mathbb{Z}_p[t]$. Ciò significa che il polinomio $g - f_i h \in \mathbb{Z}[t]$ ha coefficienti divisibili per p. Allora

$$g(\omega) = (g(\omega) - f_i(\omega)h(\omega)) + f_i(\omega)h(\omega) \in (p) + (f_i(\omega))$$

Pertanto si ha l'uguaglianza

$$\mathfrak{p}_i := \ker \nu_i = (p) + (f_i(\omega))$$

Ricapitolando, per ogni $\overline{f}_i$ abbiamo che l'ideale $\mathfrak{p}_i$ è primo e soddisfa $(p) \subseteq \mathfrak{p}_i$, ovvero $\exists \mathfrak{q}_i$ tale che $(p) = \mathfrak{p}_i\mathfrak{q}_i$. Per il Lemma 3, per induzione su r, abbiamo

$$\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \subseteq (p) + (f_1(\omega)^{e_1} \dots f_r(\omega)^{e_r}) \subseteq (p) + (f(\omega)) = (p)$$

Allora $(p)|\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ e quindi (ricordando che $\mathfrak{p}_i|(p)$ per ogni i) tutti e soli i fattori primi di (p) sono $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, con

$$(p) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \tag{3.1}$$

dove

$$0 < k_i \leq e_i \qquad (1 \leq i \leq r) \tag{3.2}$$

Sfruttando l'isomorfismo $D/\mathfrak{p}_i = \mathbb{Z}[\omega]/\mathfrak{p}_i \cong \mathbb{Z}_p[\theta_i]$ otteniamo

$$[D : \mathfrak{p}_i] = p^{d_i}$$

con $d_i = \deg \overline{f} = \deg f$. Abbiamo

$$[D : (p)] = |\mathbb{Z}[\omega]/(p)| = p^n$$

Da (3.1), utilizzando il Lemma 4 induttivamente, otteniamo

$$p^n = [D : (p)] = [D : \mathfrak{p}_1]^{k_1} \dots [D : \mathfrak{p}_r]^{k_r} = p^{d_1k_1 + \dots + d_rk_r}$$

che implica

$$d_1k_1 + \dots + d_rk_r = n = d_1e_1 + \dots + d_rk_r$$

Infine, da (3.2), deduciamo che $k_i = e_i$ $(1 \leq i \leq r)$, il che completa la dimostrazione. □

Osservazione 12. Il Teorema 17 ha un'applicazione molto significativa ai campi quadratici $\mathbb{Q}[\sqrt{d}]$. In essi, infatti, l'anello dei numeri A_d è, come abbiamo visto nel Teorema 2, della forma $\mathbb{Z}[\omega_d]$. Abbiamo che il polinomio minimo f di ω_d ha grado 2.

Pertanto considerando $\overline{f}$ in $\mathbb{Z}_p[t]$ possono verificarsi solo i seguenti tre casi:

1. $\overline{f}$ irriducibile,
2. $\overline{f} = \overline{f}_1^2$ con $\overline{f}_1$ di grado 1,
3. $\overline{f} = \overline{f}_1\overline{f}_2$ con $\overline{f}_1, \overline{f}_2$ distinti di grado 1.

A questi casi corrispondono i seguenti:

1. (p) primo,
2. $(p) = \mathfrak{p}_1^2$ con $\mathfrak{p}_1 = (p) + (f_1(\omega_d))$ primo,
3. $(p) = \mathfrak{p}_1\mathfrak{p}_2$ con $\mathfrak{p}_1 = (p) + (f_1(\omega_d))$ e $\mathfrak{p}_2 = (p) + (f_2(\omega_d))$ primi distinti.

3.3 Determinazione dei nove campi per cui A_d è un UFD

Enunciamo ora un teorema che ci assicura, in un anello di numeri D, l'esistenza, in ogni ideale non nullo, di un elemento con norma limitata da una funzione lineare dell'indice dell'ideale stesso. Diamo l'enunciato solo nel caso dei campi quadratici.

Teorema 18. *Se $\mathfrak{a}$ è un ideale non nullo di A_d allora $\mathfrak{a}$ contiene un elemento α con*

$$|N(\alpha)| \leq \frac{2}{\pi}\sqrt{|disc(A_d)|}[A_d : \mathfrak{a}]$$

Omettiamo la dimostrazione del Teorema (cfr.[Ste79], pagg.184,185). Essa fa uso del teorema di Minkowski (cfr.[Ste79], pagg.146,147) e di proprietà derivate da rappresentazioni geometriche degli interi algebrici (cfr.[Ste79], pagg.152-157) analoghe a quelle utilizzate nel Teorema 15. Dal Teorema 18 si può ricavare il seguente risultato.

Teorema 19. *Ogni classe di ideali frazionari di A_d contiene un ideale $\mathfrak{a}$ tale che*

$$[A_d : \mathfrak{a}] \leq \frac{2}{\pi}\sqrt{|disc(A_d)|}$$

Dimostrazione. La classe degli ideali frazionari equivalenti a $\mathfrak{a}^{-1}$ contiene un ideale $\mathfrak{c}$ tale che $\mathfrak{ac} \sim A_d$. Per il Teorema 18 esiste un $\gamma \in \mathfrak{c}$ tale che

$$|N(\gamma)| \leq \frac{2}{\pi}\sqrt{|\mathrm{disc}(A_d)|}[A_d : \mathfrak{c}]$$

Poiché $\mathfrak{c}|(\gamma)$ (in quanto $(\gamma) \subseteq \mathfrak{c}$) abbiamo

$$(\gamma) = \mathfrak{bc}$$

per un certo ideale $\mathfrak{b}$. Dal Lemma 4 abbiamo

$$[A_d : \mathfrak{b}][A_d : \mathfrak{c}] = [A_d : \mathfrak{bc}] = [A_d : (\gamma)] = |N(\gamma)|$$

Pertanto

$$[A_d : \mathfrak{b}] \leq \frac{2}{\pi}\sqrt{|\mathrm{disc}(A_d)|}$$

Ora basta mostrare $\mathfrak{b} \sim \mathfrak{a}$. Ma questo è chiaro dal momento che $\mathfrak{c} \sim \mathfrak{a}^{-1}$ e $\mathfrak{b} \sim \mathfrak{c}^{-1}$. □

Possiamo a questo punto presentare il teorema fondamentale, che è un'estensione del Teorema 13, a cui premettiamo un semplice lemma.

Lemma 5. *Sia $\mathfrak{a}$ un ideale non nullo di A_d. Allora $[A_d : \mathfrak{a}] \in \mathbb{N}$ è un elemento di $\mathfrak{a}$.*

Dimostrazione. Poiché $[A_d : \mathfrak{a}] = |A_d/\mathfrak{a}|$, per ogni $\alpha \in A_d$ si ha $[A_d : \mathfrak{a}]\alpha \in \mathfrak{a}$. Ponendo $\alpha = 1$ si ha la tesi. □

Teorema 20. *Supponiamo che per ogni primo $p \in \mathbb{N}$ con*

$$p \leq \frac{2}{\pi}\sqrt{|disc(A_d)|}$$

ogni ideale primo che divide (p) sia principale. Allora A_d ha numero di classi di ideali $h(d) = 1$.

Dimostrazione. Ogni classe di ideali frazionari contiene un ideale $\mathfrak{a}$ con $[A_d : \mathfrak{a}] \leq \frac{2}{\pi}\sqrt{|\text{disc}(A_d)|}$. Si ha

$$[A_d : \mathfrak{a}] = p_1 \dots p_k$$

dove $p_1 \dots p_k \in \mathbb{N}$ e $p_i \leq \frac{2}{\pi}\sqrt{|\text{disc}(A_d)|}$. Per il Lemma 5, $\mathfrak{a}|[A_d : \mathfrak{a}]$, perciò $\mathfrak{a}$ è prodotto di ideali primi ciascuno dei quali divide qualche (p_i). Per ipotesi tali ideali primi sono principali, pertanto $\mathfrak{a}$ è principale. Quindi ogni classe di ideali frazionari è uguale a $[A_d]$ e $h(d) = 1$. □

Consideriamo ora gli anelli A_d con $d \equiv 1 \pmod 4$, $-199 \leq d \leq -15$. Vale il seguente teorema.

Teorema 21. *Sia $d \equiv 1 \pmod 4$, $d \leq -15$, e sia $p \in \mathbb{N}$ primo, $p < \frac{2}{\pi}\sqrt{|d|}$. Allora ogni ideale $\mathfrak{a}$ tale che $[A_d : \mathfrak{a}] = p$ non è principale.*

Dimostrazione. Supponiamo per assurdo $\mathfrak{a} = (\alpha)$ con $\alpha = \frac{a+b\sqrt{d}}{2} \in A_d$. Allora per il Teorema 6 si ha

$$N(\alpha) = \frac{a^2 + |d|b^2}{4} = p = [A_d : \mathfrak{a}]$$

Pertanto abbiamo

$$a^2 + |d|b^2 = 4p \tag{3.3}$$

Abbiamo

$$p < \frac{2}{\pi}\sqrt{|d|} \Leftrightarrow 4p < \frac{8}{\pi}\sqrt{|d|}$$

e

$$\frac{8}{\pi}\sqrt{|d|} < |d| \Leftrightarrow |d| > \left(\frac{8}{\pi}\right)^2$$

Pertanto se $d \leq -15$, si ha

$$4p < \frac{8}{\pi}\sqrt{|d|} < |d| \tag{3.4}$$

Ma da (3.3) e (3.4) segue $b = 0$, pertanto abbiamo

$$a^2 = 4p$$

da cui $a \notin \mathbb{Z}$. Assurdo. □

Abbiamo tutti gli strumenti per determinare i valori di d, con $d \equiv 1 \pmod 4$, $-199 \leq d \leq -15$, per cui A_d è un UFD. Per tali valori si ha $A_d = \mathbb{Z}[\omega_d]$, con $\omega_d = \frac{1+\sqrt{d}}{2}$, $\mathrm{disc}(A_d) = d$ e il polinomio minimo per ω_d è

$$f(t) = t^2 - t + \frac{1-d}{4}$$

La tabella seguente riporta nell'ordine d e vettori

$$[f(0), f(1), \ldots, f(p-1)] \in (\mathbb{Z}_p)^p$$

per ogni $p < \frac{2}{\pi}\sqrt{|d|}$. Per esempio, per $d = -111$ abbiamo

$$\underset{\pmod 2}{[f(0), f(1)]}, \quad \underset{\pmod 3}{[f(0), f(1), f(2)]}, \quad \underset{\pmod 5}{[f(0), f(1), f(2), f(3), f(4)]}$$

dove $f(t) = t^2 - t + 28$.

−15, [0, 0]	−111, [0, 0], [1, 1, 0], [3, 3, 0, 4, 0]
−19, [1, 1]	−115, [1, 1], [2, 2, 1], [4, 4, 1, 0, 1]
−23, [0, 0], [0, 0, 2]	−119, [0, 0], [0, 0, 2], [0, 0, 2, 1, 2]
−31, [0, 0], [2, 2, 1]	−123, [1, 1], [1, 1, 0], [1, 1, 3, 2, 3], [3, 3, 5, 2, 1, 2, 5]
−35, [1, 1], [0, 0, 2]	−127, [0, 0], [2, 2, 1], [2, 2, 4, 3, 4], [4, 4, 6, 3, 2, 3, 6]
−39, [0, 0], [1, 1, 0]	−131, [1, 1], [0, 0, 2], [3, 3, 0, 4, 0], [5, 5, 0, 4, 3, 4, 0]
−43, [1, 1], [2, 2, 1]	−135, [0, 0], [1, 1, 0], [4, 4, 1, 0, 1], [6, 6, 1, 5, 4, 5, 1]
−47, [0, 0], [0, 0, 2]	−139, [1, 1], [2, 2, 1], [0, 0, 2, 1, 2], [0, 0, 2, 6, 5, 6, 2]
−51, [1, 1], [1, 1, 0]	−143, [0, 0], [0, 0, 2], [1, 1, 3, 2, 3], [1, 1, 3, 0, 6, 0, 3]
−55, [0, 0], [2, 2, 1]	−151, [0, 0], [2, 2, 1], [3, 3, 0, 4, 0], [3, 3, 5, 2, 1, 2, 5]
−59, [1, 1], [0, 0, 2]	−155, [1, 1], [0, 0, 2], [4, 4, 1, 0, 1], [4, 4, 6, 3, 2, 3, 6]
−67, [1, 1], [2, 2, 1], [2, 2, 4, 3, 4]	−159, [0, 0], [1, 1, 0], [0, 0, 2, 1, 2], [5, 5, 0, 4, 3, 4, 0]
−71, [0, 0], [0, 0, 2], [3, 3, 0, 4, 0]	−163, [1, 1], [2, 2, 1], [1, 1, 3, 2, 3], [6, 6, 1, 5, 4, 5, 1]
−79, [0, 0], [2, 2, 1], [0, 0, 2, 1, 2]	−167, [0, 0], [0, 0, 2], [2, 2, 4, 3, 4], [0, 0, 2, 6, 5, 6, 2]
−83, [1, 1], [0, 0, 2], [1, 1, 3, 2, 3]	−179, [1, 1], [0, 0, 2], [0, 0, 2, 1, 2], [3, 3, 5, 2, 1, 2, 5]
−87, [0, 0], [1, 1, 0], [2, 2, 4, 3, 4]	−183, [0, 0], [1, 1, 0], [1, 1, 3, 2, 3], [4, 4, 6, 3, 2, 3, 6]
−91, [1, 1], [2, 2, 1], [3, 3, 0, 4, 0]	−187, [1, 1], [2, 2, 1], [2, 2, 4, 3, 4], [5, 5, 0, 4, 3, 4, 0]
−95, [0, 0], [0, 0, 2], [4, 4, 1, 0, 1]	−191, [0, 0], [0, 0, 2], [3, 3, 0, 4, 0], [6, 6, 1, 5, 4, 5, 1]
−103, [0, 0], [2, 2, 1], [1, 1, 3, 2, 3]	−195, [1, 1], [1, 1, 0], [4, 4, 1, 0, 1], [0, 0, 2, 6, 5, 6, 2]
−107, [1, 1], [0, 0, 2], [2, 2, 4, 3, 4]	−199, [0, 0], [2, 2, 1], [0, 0, 2, 1, 2], [1, 1, 3, 0, 6, 0, 3]

Per $d \neq -19, -43, -67, -163$, si ha che $\overline{f}$ è riducibile per almeno qualche $p < \frac{2}{\pi}\sqrt{|d|}$. Pertanto per tali primi p si ha

$$(p) = \langle \begin{matrix} \mathfrak{p}_1^2 \\ \mathfrak{p}_1\mathfrak{p}_2 \end{matrix} \tag{3.5}$$

Consideriamo l'ideale primo $\mathfrak{p}_1$. Da (3.5), per il Lemma 4 si ha

$$[A_d : \mathfrak{p}_1] = p$$

Per il Teorema 21, si ha dunque che $\mathfrak{p}_1$ non è principale.
Consideriamo ora i casi $d \in \{-19, -43, -67, -163\}$. Per tali valori si ha che il polinomio $\overline{f}$ è irriducibile in $\mathbb{Z}_p[t]$ per ogni $p < \frac{2}{\pi}\sqrt{|d|}$ (dalla tabella si nota infatti che non ha radici ed essendo di secondo grado è irriducibile). Dall'Osservazione 12 si ha allora che (p) è primo per ogni $p < \frac{2}{\pi}\sqrt{|d|}$. Siamo nelle ipotesi del Teorema 20 e quindi $h(d) = 1$.

Osservazione 13. Notiamo che i teoremi 20 e 21 forniscono un algoritmo per verificare in modo semplice, come, in effetti, abbiamo fatto per $-199 \leq d \leq -15$, se A_d è un UFD per $d \equiv 1 \pmod 4$, $d \leq -15$. Basta, infatti, considerare il polinomio minimo di ω_d e verificare se è irriducibile in $\mathbb{Z}_p[t]$ per ogni $p < \frac{2}{\pi}\sqrt{|d|}$. Se ciò avviene, allora A_d è un UFD, altrimenti no. Questo algoritmo è facilmente implementabile con un calcolatore e permette di ampliare a piacere l'intervallo in cui andiamo a verificare se A_d è un UFD. Come mostreremo nel capitolo successivo, $-200 \leq d \leq -1$ è l'intervallo di minima ampiezza che dobbiamo considerare.

Ricapitoliamo tutti i risultati del capitolo in un teorema.

Teorema 22. *Per $-200 \leq d \leq -1$ sono equivalenti:*

1. *A_d è un UFD (h(d)=1),*

2. *$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$.*

Capitolo 4

Fattorizzazione in A_d per $d < -200$

4.1 Il teorema di Stark

Abbiamo dimostrato nel capitolo precedente che, per $-200 \leq d \leq -1$, ci sono solo nove campi quadrati complessi $\mathbb{Q}[\sqrt{d}]$ il cui anello degli interi algebrici A_d è un UFD. In questo capitolo mostreremo che questi nove campi sono gli unici campi quadratici complessi per cui A_d è un UFD o, equivalentemente, per cui $h(d) = 1$. Dimostreremo infatti il seguente teorema, che chiameremo **teorema di Stark**.

Teorema 23. *Per ogni $d < -200$, $d \in \mathbb{Z}$ privo di fattori quadratici, si ha $h(d) \neq 1$.*

Osservazione 14. Ricordando i risultati del Teorema 16, dobbiamo dimostrare soltanto che per $d \equiv 1 \pmod 4$, $d < -200$, si ha $h(d) \neq 1$. Pertanto da qui in poi considereremo solo tali valori per d.

Osservazione 15. Tenendo conto delle osservazioni 8 e 14, il Teorema 23 assume la forma, legata alle forme quadratiche, su cui già Gauss aveva proposto una congettura (cfr. [Gau66], pagg.361-363), osservando tabelle simili

a quella riportata nel capitolo precedente: Gauss aveva congetturato che $h(d) \to \infty$ quando $d \to -\infty$. La dimostrazione del Teorema 23 ha però richiesto molto tempo e solo Harold M. Stark vi pose soluzione, nel 1969. In questo capitolo faremo riferimento costante al suo articolo [Sta69], pertanto non riporteremo ogni volta il riferimento, sottointendendolo.

Prima di dare la dimostrazione del Teorema 23, daremo una serie di risultati che non dimostreremo.
Si può mostrare (cfr.[Dic11]), sfruttando le proprietà delle forme quadratiche e la definizione di forma quadratica ridotta, che se $d < -8$ e $h(d) = 1$, allora sia $|d|$ che $\frac{|d|+1}{4}$ sono primi. Questo risultato aiutò Dickson a dedurre che se $d < -11$ e $h(d) = 1$ allora

$$|d| \equiv 19 \pmod{24} \tag{4.1}$$

4.2 Le funzioni fondamentali

Definizione 21. *Un **carattere complesso (mod** m**)** è un omomorfismo*

$$\chi : (\mathbb{Z}_m^*, \cdot) \to (\mathbb{C}, \cdot)$$

*Per ogni carattere mod m possiamo definire un **carattere numerico** $\chi(n)$, per $n \in \mathbb{Z}$: se $(n, m) = 1$ allora poniamo $\chi(n) = \chi([n]_m)$, altrimenti poniamo $\chi(n) = 0$.*
*Se consideriamo come spazio di arrivo $(\mathbb{R}, \cdot)$ parleremo di **caratteri reali**.*

Introduciamo delle funzioni fondamentali per la trattazione successiva: la funzione zeta di Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} \tag{4.2}$$

e le L-funzioni di Dirichlet

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} \tag{4.3}$$

dove χ è un carattere numerico. Qui avremo bisogno di considerare solo caratteri primitivi reali (cfr.[Mar77], pag.198), e questi sono in una corrispondenza 1-1 con i campi quadratici: sia k il discriminante di un campo quadratico. Si definisca χ_k come

$$\chi_k(j) = \left(\frac{k}{j}\right) = \begin{cases} 1 & \text{se } k \text{ è quadrato in } \mathbb{Z}_j^* \\ -1 & \text{se } k \text{ non è quadrato in } \mathbb{Z}_j^* \end{cases} \tag{4.4}$$

Allora χ_k è un carattere reale primitivo (mod $|k|$) e

$$\zeta(s)L(s,\chi_k) = \zeta_k(s) \tag{4.5}$$

dove $\zeta_k(s)$ è la funzione zeta di Dedekind per $\mathbb{Q}(\sqrt{k})$ definita da

$$\zeta_k(s) = \sum_{\mathfrak{a}} ([A_d : \mathfrak{a}])^{-s} \tag{4.6}$$

dove $\mathfrak{a}$ varia tra gli ideali di A_d.

Da questo punto in poi, k **e** d **denoteranno discriminanti di campi quadratici e** d **sarà sempre negativo**.

È noto che $\zeta_d(s)$ può sempre essere espressa nei termini di funzioni zeta di Epstein, quando $d < -4$

$$\zeta_d(s) = \sum_{Q} \zeta(s,Q) \tag{4.7}$$

dove Q varia su un insieme completo di forme quadratiche binarie, definite positive, non equivalenti, a coefficienti interi e discriminante d e

$$\zeta(s,Q) = \frac{1}{2} \sum_{x,y\neq 0,0} Q(x,y)^{-s} \tag{4.8}$$

La funzione zeta di Epstein può essere anche generalizzata dall'inserimento di un carattere,

$$L(s,\chi,Q) = \frac{1}{2} \sum_{x,y\neq 0,0} \chi(Q(x,y))Q(x,y)^{-s} \tag{4.9}$$

e così abbiamo la generalizzazione di (4.5) e (4.7), quando $d < -4$

$$L(s,\chi_k)L(s,\chi_{kd}) = \sum_{Q} L(s,\chi_k,Q) \tag{4.10}$$

Storicamente, il primo ad usare ciascuna di queste funzioni fu Dirichlet, che mostrò che

$$L(1,\chi_k) = \begin{cases} \frac{\pi h(k)}{\sqrt{|k|}} & k < -4 \\ \frac{2h(k)\log\epsilon_0}{\sqrt{k}} & k > 0 \end{cases} \tag{4.11}$$

dove, se $k > 0$, ϵ_0 denota l'unità fondamentale (cfr.[Mar77], pag.141) di $\mathbb{Q}[\sqrt{k}]$. Dirichlet mostrò anche che, per $k < -4$

$$h(k) = \frac{1}{[2 - \chi_k(2)]} \sum_{1 \le j \le \frac{|k|}{2}} \chi_k(j) \tag{4.12}$$

L'equazione (4.12) aiuta ad arrivare al seguente risultato: se $|d|$ è primo e $|d| \equiv 19 \pmod{24}$ allora possiamo riordinare i termini di (4.12) per mostrare

$$h(8d) \equiv 2 \pmod 4, \qquad h(12d) \equiv 4 \pmod 8 \tag{4.13}$$

Useremo questi risultati in seguito.

4.3 Primi sviluppi della congettura di Gauss

C'è uno sviluppo di $\zeta(s,Q)$ molto utile, che è pertinente al nostro problema. Sia

$$Q(x,y) = ax^2 + bxy + cy^2, \qquad d = b^2 - 4ac, \qquad a > 0 \tag{4.14}$$

Allora

$$a^s\zeta(s,Q) = \zeta(2s) + \left(\frac{\sqrt{|d|}}{2a}\right)^{1-2s} \frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)}\zeta(2s-1) + \frac{1}{\Gamma(s)}\left(\frac{\sqrt{|d|}}{2a\pi}\right)^{-s} h(s) \tag{4.15}$$

dove

$$h(s) = 4\left(\frac{\sqrt{|d|}}{2a}\right)^{\frac{1}{2}} \sum_{n=1}^{\infty} K_{s-\frac{1}{2}}\left(\frac{\pi n\sqrt{|d|}}{a}\right)\cos\left(\frac{n\pi b}{a}\right) n^{s-\frac{1}{2}} \sum_{y|n} y^{1-2s} \tag{4.16}$$

Qui Γ denota la funzione gamma e K_s è una funzione di Bessel modificata del secondo tipo, data da

$$K_s(x) = \int_0^{\infty} e^{-x\cosh t}\cosh(st)dt \qquad (x > 0, s \text{ complesso}) \tag{4.17}$$

o alternativamente,

$$\int_{-\infty}^{\infty} \frac{e^{ixu}du}{(u^2+1)^s} = \frac{2\sqrt{\pi}}{\Gamma(s)} \left(\frac{|x|}{2}\right)^{s-1/2} K_{s-1/2}(|x|) \quad \left(x \text{ reale} \neq 0, Re(s) > \frac{1}{2}\right) \tag{4.18}$$

$K_{s-1/2}$ entra in (4.16) tramite l'integrale in (4.18), l'equazione (4.17) serve per dare l'estensione di $K_{s-1/2}$ all'intero piano s e mostra che $K_{s-1/2}$ è invariante a sinistra quando s è sostituito da $1-s$.

La migliore prova della (4.15) è quella di Mordell che procedette tramite la formula della somma di Poisson ma che mantenne l'integrale in (4.18) invece di introdurre $K_{s-1/2}$. Se uno vuole una stima di $h(s)$, si può anche derivare (4.15) per mezzo della formula della somma di Eulero-Maclaurin, come fece Deuring. Per i nostri propositi, abbiamo solo bisogno di stimare in modo grossolano che, per s fissato,

$$h(s) \to 0 \qquad \text{quando } \frac{\sqrt{|d|}}{a} \to \infty \tag{4.19}$$

Il primo progresso rispetto all'originale congettura di Gauss fu fatto nel 1918 da Hecke che trovò una connessione con l'ipotesi di Riemann per $\zeta_d(s)$. Hecke mostrò, usando il suo sviluppo della funzione zeta di Dedekind, che se $\zeta_d(s) \neq 0$ per x reale nell'intervallo $1 - 1/\log|d| < s < 1$, allora

$$h(d) > c\frac{\sqrt{|d|}}{\log|d|}$$

dove c è una costante positiva. Mahler, successivamente, mostrò che lo stesso risultato si può basare su (4.15). Illustriamo il suo metodo quando $h(d) = 1$.

Notiamo che c'è sempre una forma con discriminante d data da

$$Q(x,y) = \begin{cases} x^2 + |d|y^2/4, & d \text{ pari} \\ x^2 + xy + (|d|+1)y^2/4, & d \text{ dispari} \end{cases} \tag{4.20}$$

Se $h(d) = 1$, allora

$$\zeta(s)L(s,\chi_d) = \zeta_d(s) = \zeta(s,Q) \tag{4.21}$$

dove Q è dato da (4.20). Ma quando applichiamo (4.15) con $a = 1$ notiamo che per $s = 1 - 1/\log|d|$, $\zeta(s, Q) > 0$ per $|d|$ abbastanza grande. Questo perché per $s = 1 - 1/\log|d|$

$$\begin{aligned} &\zeta(2s) > \zeta(2) = \pi^2/6 && (|d| \geq 8) \\ &\zeta(2s-1) \sim -\tfrac{1}{2}\log|d| && \text{se } d \to -\infty \end{aligned} \tag{4.22}$$

cosicché

$$\left(\frac{\sqrt{|d|}}{2}\right)^{1-2s} \zeta(2s-1)\frac{\sqrt{\pi}\Gamma(s-1/2)}{\Gamma(s)} \to 0 \qquad \text{se } d \to -\infty \tag{4.23}$$

Da (4.15), (4.19), (4.21), (4.22) e (4.23) segue che, se $|d|$ è sufficientemente grande e $h(d) = 1$, allora

$$\zeta_d\left(1 - \frac{1}{\log|d|}\right) > 0$$

Ma $\zeta_d(s)$ ha un polo del primo ordine in $s = 1$ con residuo > 0 e quindi $\zeta_d(s) \to -\infty$ quando $s \to 1^-$. Quindi, per $|d|$ abbastanza grande con $h(d) = 1$, $\zeta_d(s)$ ha uno zero reale tra $1 - 1/\log|d|$ e 1. Dal momento che $\zeta(s)$ non ha zeri reali tra 0 e 1, vediamo da (4.5) che quanto detto implica che $L(s, \chi_d)$ ha uno zero reale nello stesso intervallo di s.

Poco prima del lavoro di Mahler, Deuring aveva mostrato nel 1933, con lo stesso metodo, che se $h(d) = 1$ per infiniti numeri negativi d allora l'ipotesi di Riemann è vera per $\zeta(s)$. Supponiamo che s sia un numero complesso fissato con $\mathrm{Re}s > \frac{1}{2}$ tale che $\zeta(s) = 0$. Da (4.15) e (4.19) segue che

$$\lim_{d \to -\infty} \zeta(s, Q) = \zeta(2s) \neq 0$$

dove Q è data da (4.20). Ma se $h(d) = 1$ per infiniti d da (4.21) segue che $\zeta(s, Q) = 0$ per infiniti d. Questa è una contraddizione e il risultato di Deuring è quindi raggiunto.

4.4 I risultati di Heilbronn e Linfoot

I risultati di Deuring ispirarono anche Heilbronn, che nel 1934 stabilì che l'originale congettura di Gauss era vera. È negli scritti di Heilbronn che

vediamo per la prima volta la funzione $L(s,\chi,Q)$ e la relazione (4.10). Infatti, $L(s,\chi,Q)$ ha uno sviluppo molto simile a (4.15). Se k e d sono discriminanti di campi quadratici, $d<0$, $(k,d)=1$, e $Q(x,y)$ data da (4.14), allora

$$\begin{aligned} a^s L(s,\chi_k,Q) = \quad & \chi_k(a)\zeta(2s)\textstyle\prod_{p|k,p \text{ primo}}(1-p^{-2s}) + \chi_k(a)\left(\frac{|k|\sqrt{|d|}}{2a}\right)^{1-2s}\cdot \\ & \cdot\frac{\sqrt{\pi}\Gamma(s-1/2)}{\Gamma(s)}\zeta(2s-1)\textstyle\prod_{p|k,p \text{ primo}}(1-p)^{2s-2}+ \\ & +\frac{1}{\Gamma(s)}\left(\frac{|k|\sqrt{|d|}}{2a\pi}\right)^{-s} H(s) \end{aligned} \tag{4.24}$$

dove

$$\begin{aligned} H(s) = \quad & 4\left(\frac{\sqrt{d}}{2a|k|}\right)^{1/2}\textstyle\sum_{n=1}^{\infty} K_{s-1/2}\left(\frac{\pi n\sqrt{d}}{a|k|}\right) n^{s-1/2}\sum_{y|n} y^{1-2s} \\ & \cdot\mathrm{Re}\left[\textstyle\sum_{j=1}^{|k|}\chi_k(Q(j,y))\exp\left(\frac{2\pi ijn}{|k|y}+\frac{\pi ibn}{a|k|}\right)\right] \end{aligned} \tag{4.25}$$

è una funzione intera e se $a=1$ la quantità nelle [ ] è già un numero reale. Tale risultato è dovuto a Stark. Si noti che se poniamo $k=1$, la (4.24) e la (4.25) si riducono a (4.15) e (4.16). Uno sviluppo simile è anche possibile per caratteri complessi (mod $|k|$). Lavorando con la formula della somma di Eulero-Maclaurin, come fece Heilbronn, si può ottenere solo una stima di $H(s)$, ma noi abbiamo bisogno soltanto del semplice risultato che, per s fissato,

$$H(s)\to 0 \qquad \text{se } \sqrt{|d|}/a|k|\to\infty \tag{4.26}$$

Ora possiamo procedere come negli scritti di Deuring: si suppongano k e s fissati, con $\mathrm{Re}[s]>\frac{1}{2}$. Se Q è dato da (4.20), allora

$$\lim_{d\to-\infty,|d| \text{ primo}} L(s,\chi_k,Q) = \zeta(2s)\prod_{p|k,p \text{ primo}}(1-p^{-2s})\neq 0 \tag{4.27}$$

La condizione che $|d|$ sia primo è stata inclusa affinché si possa usare lo sviluppo di (4.24), che ha la restrizione $(k,d)=1$. Tale restrizione non ci crea problema, perché se $h(d)=1$ e $d<-8$, allora $|d|$ è primo. Da (4.10) e (4.24), osserviamo che se $h(d)=1$ per infiniti d, allora l'ipotesi di Riemann per $L(s,\chi_k)$ è vera. Ma qui k è arbitrario e questo contraddice il teorema

di Hecke che afferma che, se $k < 0$, $|k|$ è sufficientemente grande e $h(k) = 1$, allora $L(s, \chi_k) = 0$ per qualche s nell'intervallo $1 - 1/\log|k| < s < 1$. Allora c'è solo un numero finito di campi quadratici complessi con numero di classi di ideali uguale a 1. Heilbronn e Linfoot precisarono tale analisi e mostrarono che ci sono al massimo dieci campi quadratici complessi con numero di classi di ideali uguale a 1, con il decimo campo (se esiste) che fornisce un controesempio all'ipotesi di Riemann generalizzata.

4.5 Dimostrazione del teorema di Stark

Abbiamo tutte le premesse per dare la dimostrazione del Teorema 23.

Dimostrazione. Articoleremo la dimostrazione in tre passi.

Primo passo: il processo di elevazione a potenza

Iniziamo dall'apparentemente irrilevante osservazione che

$$e^{\pi\sqrt{163}/5} + \sqrt{5} = 3048.996... \approx 3049 = 5F_{15} - 1 \tag{4.28}$$

dove $F_{15} = 610$ è il quindicesimo numero di Fibonacci. Il membro sinistro di (4.28) si può ricavare da (4.24) ponendo $d = -163$, $k = 5$, $s = 1$. Vediamo come si ottiene questo risultato da (4.24) quando $s = 1$.

Da questo punto in poi supponiamo $h(d) = 1$ con $d < -4$ e $k > 0$. Prendiamo Q data da (4.20). Allora, da (4.10) e (4.11), moltiplicando entrambi i membri della (4.24), con $s = 1$, per $k\sqrt{|d|}/2\pi$, otteniamo

$$\begin{aligned} h(kd)h(k)\log\epsilon_0 = \; & \tfrac{\pi k\sqrt{|d|}}{12}\textstyle\prod_{p|k}(1-p^{-2}) + \\ & + \begin{cases} 0 & \text{se } k \text{ ha due fattori primi distinti} \\ -\log p & \text{se } k \text{ è una potenza di } p \end{cases} + \\ & + 2\textstyle\sum_{n=1}^{\infty} e^{-\pi n\sqrt{|d|}/k} \sum_{y|n} \frac{1}{n} \sum_{j=1}^{k} \chi_k(Q(j,y)) \cdot \\ & \cdot \exp\left(\tfrac{2\pi i n j}{ky} + \tfrac{\pi i n}{k}\right) \end{aligned} \tag{4.29}$$

dove ϵ_0 è l'unità fondamentale di $\mathbb{Q}(\sqrt{k})$. Dal momento che abbiamo assunto che k sia un discriminante positivo, se k è una potenza di un primo p allora

$k = 8$ o $k = p \equiv 1 \pmod 4$.

Dal momento che

$$h(-815) = 30, \qquad h(5) = 1,$$

se poniamo $d = -163$ e $k = 5$ in (4.29), otteniamo

$$30 \log\left(\frac{1+\sqrt{5}}{2}\right) = \frac{2\pi\sqrt{163}}{5} - \log 5 + 2(1+\sqrt{5})e^{-\pi\sqrt{163}/5} + ... \qquad (4.30)$$

dove abbiamo omesso i termini dopo il primo nelle serie infinite. Dividendo (4.30) per 2 e portando $\log 5$ a sinistra abbiamo

$$\log\left[5\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{15}\right] = \frac{\pi\sqrt{163}}{5} + (1+\sqrt{5})e^{-\pi\sqrt{163}/5} + ...$$

ed, elevando tutto a potenza, otteniamo

$$\begin{aligned} 5\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{15} &= e^{\pi\sqrt{163}/5}\exp[(1+\sqrt{5})e^{-\pi\sqrt{163}/5} + ...] \\ &= e^{\pi\sqrt{163}/5} + (1+\sqrt{5}) + ... \end{aligned} \qquad (4.31)$$

Dal momento che

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

si vede come si può ottenere (4.28) da (4.31). Infatti, se invertiamo (4.31), moltiplichiamo per 5 e aggiungiamo il risultato a (4.31), otteniamo una serie infinita per $5F_{15}$ che inizia

$$5F_{15} = e^{\pi\sqrt{163}/5} + (1+\sqrt{5}) + ...$$

Questo mostra il metodo semplice con cui si può operare su entrambi i membri di (4.29) per ottenere un intero razionale nei termini di una serie di potenze infinita di $e^{-\pi\sqrt{|d|}/k}$ e legarlo alle soluzioni di equazioni lineari per ricorrenza del secondo ordine. Aggiungiamo il fatto che se $h(-815)$ fosse stata per esempio 31, allora avremmo avuto a che fare con $F_{15\frac{1}{2}}$. Pertanto abbiamo bisogno di sapere che $h(-815)$ sia pari per ottenere davvero un numero di Fibonacci. Allo stesso modo, quando usiamo $k = 8$ e 12, abbiamo

bisogno di (4.13) per assicurarci di avere realmente a che fare con interi razionali. Poniamo la (4.13) nella seguente forma (se $d < -11$ e $h(d) = 1$):

$$h(8d) = 4N + 2, \qquad h(12d) = 8M + 4 \tag{4.32}$$

Secondo passo: ricerca di equazioni diofantee

Ci rimane da capire come usare il processo di elevazione a potenza. In questo caso usiamo l'idea di Heegner: forse possiamo trovare un'equazione diofantea che leghi gli interi che otteniamo tramite il processo da due diversi valori di k e forse sappiamo risolvere questa equazione. In effetti ciò accade con $k = 8$ e 12.

Vediamo che sorgono immediatamente complicazioni, in quanto noi stiamo usando

$$Q(x, y) = x^2 + xy + \frac{|d| + 1}{4} y^2$$

e nel calcolare i coefficienti di $H(1)$ abbiamo bisogno di conoscere $\frac{|d|+1}{4} \pmod k$. Da (4.1) tutto ciò che sappiamo è

$$\frac{|d| + 1}{4} \equiv 5 \pmod 6 \tag{4.33}$$

Allora ci sono due casi quando $k = 12$ e ognuno di essi si sviluppa in ulteriori due casi quando $k = 8$. Uno dei quattro casi illustra il metodo in modo sufficiente. Scegliamo arbitrariamente il caso

$$\frac{|d| + 1}{4} \equiv 1 \pmod 8 \tag{4.34}$$

che insieme a (4.33) dà

$$\frac{|d| + 1}{4} \equiv 17 \pmod{24} \tag{4.35}$$

Questo caso include i due campi con $d = -67$ e $d = -163$.

Per semplificare le cose, poniamo

$$q = \frac{1}{64} e^{\pi\sqrt{|d|}} \tag{4.36}$$

dove il fattore 1/64 è incluso per cancellare le potenze di 2 che altrimenti comparirebbero.

Sia $k = 12$. L'unità fondamentale di $\mathbb{Q}(\sqrt{12})$ è $2+\sqrt{3}$ e $h(12) = 1$. Allora dividendo entrambi i membri di (4.29) per 8 e usando (4.32) e (4.35) si ha

$$\left(M + \frac{1}{2}\right)\log(2+\sqrt{3}) = \frac{\pi\sqrt{|d|}}{12} - q^{-1/12} - \frac{1}{3}q^{-1/4} + O(q^{-1/3}) \qquad (4.37)$$

dove O si riferisce qui e anche più tardi a $d \to -\infty$. Quando eleviamo a potenza entrambi i lati di (4.37) e dividiamo per $\sqrt{2}$, otteniamo

$$\begin{aligned}\left(\tfrac{1+\sqrt{3}}{2}\right)(2+\sqrt{3})^M &= \tfrac{1}{\sqrt{2}}(2+\sqrt{3})^{M+1/2} \\ &= q^{1/12}[1 - q^{-1/12} + \tfrac{1}{2}q^{-1/6} - \tfrac{1}{2}q^{-1/4} + O(q^{-1/3})]\end{aligned} \qquad (4.38)$$

Se invertiamo entrambi i lati di (4.38) e moltiplichiamo per $-\frac{1}{2}$, otteniamo

$$\left(\frac{1-\sqrt{3}}{2}\right)(2-\sqrt{3})^M = -\frac{1}{2}q^{-1/12}[1 - q^{-1/12} + O(q^{-1/6})] \qquad (4.39)$$

e quando sommiamo (4.38) e (4.39) otteniamo

$$W_M = q^{1/12}[1 - q^{-1/12} - q^{-1/4} + O(q^{-1/3})] \qquad (4.40)$$

dove

$$W_n = \left(\frac{1+\sqrt{3}}{2}\right)(2+\sqrt{3})^n + \left(\frac{1-\sqrt{3}}{2}\right)(2-\sqrt{3})^n \qquad (4.41)$$

è la soluzione dell'equazione per ricorrenza del secondo ordine

$$W_{n+2} = 4W_{n+1} - W_n, \quad W_0 = 1, \quad W_1 = 5 \qquad (4.42)$$

Poniamo

$$f = W_M + 1 \qquad (4.43)$$

cosicché f sia un intero positivo. Da (4.40) segue che

$$f^3 + 3 = q^{1/4} + O(q^{-1/12}) \qquad (4.44)$$

Sia ora $k = 8$. L'unità fondamentale di $\mathbb{Q}(\sqrt{8})$ è $1 + \sqrt{2}$ e $h(8) = 1$. Poniamo

$$R_1 = 1 + \sqrt{2}, \qquad R_2 = 1 - \sqrt{2} \tag{4.45}$$

Se dividiamo entrambi i membri di (4.29) per 4 e usiamo la (4.32) e la (4.35), otteniamo

$$\left(N + \frac{1}{2}\right) \log R_1 + \frac{1}{4} \log 2 = \frac{\pi\sqrt{|d|}}{8} + R_1^{-1/2} q^{-1/8} + O(q^{-3/8}) \tag{4.46}$$

Elevando a potenza entrambi i membri di (4.46) e dividendo poi per $2^{(3/4)}$, otteniamo

$$\frac{1}{\sqrt{2}} R_1^{N+1/2} = q^{1/8} \left[1 + R_1^{-1/2} q^{-1/8} + \frac{1}{2} R_1^{-1} q^{-1/4} + O(q^{-3/8})\right] \tag{4.47}$$

che elevata al quadrato dà

$$\begin{aligned} \tfrac{1}{2} R_1^{2N+1} &= q^{1/4}[1 + 2R_1^{-1/2} q^{-1/8} + 2R_1^{-1} q^{-1/4} + O(q^{-3/8}] \\ &= q^{1/4} + 2R_1^{-1/2} q^{1/8}[1 + R_1^{-1/2} q^{-1/8} + O(q^{-1/4})] \end{aligned} \tag{4.48}$$

Combiniamo (4.47) e (4.48) per ottenere

$$\frac{1}{2} R_1^{2N+1} - \sqrt{2} R_1^N = q^{1/4} + O(q^{-1/8}) \tag{4.49}$$

ma dal momento che $R_2 = -1/R_1$, vediamo da (4.47) e (4.48) che

$$R_2^N = O(q^{-1/8}), \qquad R_1^{2N+1} = O(q^{-1/4})$$

e quindi possiamo scrivere (4.49) nella forma

$$Z_{2N+1} - 4Y_N = q^{1/4} + O(q^{-1/8}) \tag{4.50}$$

Qui

$$Y_n = \frac{1}{2\sqrt{2}}(R_1^n - R_2^n), \tag{4.51}$$

$$Z_n = \frac{1}{2}(R_1^n + R_2^n) \tag{4.52}$$

sono entrambe soluzioni dell'equazione per ricorrenza del secondo ordine

$$X_{n+2} = 2X_{n+1} + X_n \tag{4.53}$$

con le condizioni iniziali

$$Y_0 = 0, \qquad Y_1 = 1; \qquad Z_0 = 1, \qquad Z_1 = 1 \tag{4.54}$$

Allora, se $|d|$ è sufficientemente grande e $(|d|+1)/4 \equiv 1 \pmod 8$, i membri di sinistra di (4.44) e (4.50) saranno differenti per meno di 1, e, essendo interi, devono essere per forza uguali. Tale risultato ci fornisce l'equazione diofantea desiderata. Lo stesso accade, analogamente, negli altri tre casi. Siamo ora in grado di mostrare che, se $|d|$ è sufficientemente grande (e $h(d) = 1$), allora

$$Y_{2N+1} - 4Y_N = f^3 + 3 \qquad [(|d|+1)/4 \equiv 1 \pmod 8] \tag{4.55}$$

$$Y_{2N+1} - 4Y_N = f^3 + 3 \qquad [(|d|+1)/4 \equiv 5 \pmod 8] \tag{4.56}$$

$$Y_{2N+1} - 4Y_{N+1} = f^3 - 3 \qquad [(|d|+1)/4 \equiv 3 \pmod 8] \tag{4.57}$$

$$Y_{2N+1} - 4Y_{N+1} = f^3 - 3 \qquad [(|d|+1)/4 \equiv 7 \pmod 8] \tag{4.58}$$

dove

$$f = \begin{cases} W_M + 1 & \text{in (4.55) e (4.56),} \\ W_M - 1 & \text{in (4.57) e (4.58).} \end{cases} \tag{4.59}$$

I termini di errore possono essere analizzati per dare un significato più preciso all'espressione sufficientemente grande. Ciò richiede semplici, ma noiosi, calcoli e stime del valore assoluto, che qui omettiamo (cfr.[Sta67]). Il risultato è che, se $|d| \geq 200$, allora devono valere le (4.55) – (4.58). Troviamo anche che le (4.55) – (4.58) valgono per $d \in \{-19, -43, -67, -163\}$. I numeri

che riguardano questi casi sono:

$$\begin{array}{llllll} d=-19, & h(12d)=4, & h(8d)=6, & & & \\ & M=0, & N=1, & f=2, & Z_3=7, & Y_1=1. \\ d=-43, & h(12d)=12, & h(8d)=10, & & & \\ & M=1, & N=2, & f=4, & Z_3=41, & Y_3=5. \\ d=-67, & h(12d)=12, & h(8d)=14, & & & \\ & M=1, & N=3, & f=6, & Z_3=239, & Y_3=5. \\ d=-163, & h(12d)=20, & h(8d)=22, & & & \\ & M=2, & N=5, & f=20, & Z_{11}=8119, & Y_5=29. \end{array}$$

Notiamo infine che le stime che abbiamo omesso sono abbastanza precise. Per esempio, se $d=-163$, entrambi i membri di (4.55) valgono 8003, mentre

$$q^{1/4}=\frac{1}{2\sqrt{2}}e^{\pi\sqrt{163}/4}=8002,9998...$$

Terzo passo: risoluzione delle equazioni diofantee trovate

Dobbiamo, infine, risolvere le equazioni (4.55)-(4.58) e questo è fortunatamente possibile. Illustriamo il metodo di risoluzione, considerando l'equazione (4.55). Le seguenti relazioni tra Z_n e Y_n si provano facilmente: per ogni n,

$$Z_{2n+1}=4Y_nY_{n+1}+(-1)^n \tag{4.60}$$

$$Y_{2n}=2Y_nZ_n \tag{4.61}$$

$$Y_{2n-1}=4Y_n^2-2Y_nZ_n+(-1)^n=2Z_n^2-2Y_nZ_n-(-1)^n \tag{4.62}$$

$$Z_n^2=2Y_n^2+(-1)^n \tag{4.63}$$

$$Y_{n-1}=Z_n-Y_n \tag{4.64}$$

$$Z_{n-1} = 2Y_n - Z_n \tag{4.65}$$

Supponiamo ora che valga (4.55). Da (4.60), questa può essere scritta come

$$4Y_N(Y_{N+1} - 1) = f^3 + 3 - (-1)^N \tag{4.66}$$

Perciò f è pari,

$$f = 2g \tag{4.67}$$

e quindi N è dispari,

$$N = 2N' - 1 \tag{4.68}$$

con $N' > 0$, dal momento che $N \geq 0$. L'equazione (4.66) diviene

$$Y_{2N'-1}(Y_{2N'} - 1) = 2g^3 + 1$$

e, insieme a (4.61) e (4.62), si ha

$$(4Y_{N'}^2 - 2Y_{N'}Z_{N'} + (-1)^{N'})(2Y_{N'}Z_{N'} - 1) = 2g^3 + 1 \tag{4.69}$$

o equivalentemente

$$(2Z_{N'}^2 - 2Y_{N'}Z_{N'} - (-1)^{N'})(2Y_{N'}Z_{N'} - 1) = 2g^3 + 1 \tag{4.70}$$

Usiamo una tra la (4.69) e la (4.70) che ci consente di cancellare gli 1. Se N' è dispari allora vediamo da (4.69), con l'aiuto di (4.63) e (4.64), che

$$\begin{aligned} g^3 &= 4Y_{N'}^3 Z_{N'} - 2Y_{N'}^2 Z_{N'}^2 - 2Y_{N'}^2 = \\ &= 4Y_{N'}^3 Z_{N'} - 2Y_{N'}^2 (Z_{N'}^2 - (-1)^{N'}) = \\ &= 4Y_{N'}^3 (Z_{N'} - Y_{N'}) = \\ &= 4Y_{N'}^3 Y_{N'-1} \qquad (N' \text{ dispari}) \end{aligned} \tag{4.71}$$

mentre se N' è pari, allora (4.70), (4.63) e (4.65) danno

$$\begin{aligned} g^3 &= 2Y_{N'}Z_{N'}^3 - 2Y_{N'}^2 Z_{N'}^2 - Z_{N'}^2 = \\ &= 2Y_{N'}Z_{N'}^3 - Z_{N'}^2 (2Y_{N'}^2 + (-1)^{N'}) = \\ &= Z_{N'}^3 (2Y_{N'} - Z_{N'}) = \\ &= Z_{N'}^3 Z_{N'-1} \qquad (N' \text{ pari}) \end{aligned} \tag{4.72}$$

L'equazione (4.71) ci porta a risolvere un'equazione del tipo

$$Y_n = 2h^3 \tag{4.73}$$

mentre la (4.72) ci porta a

$$Z_n = h^3 \tag{4.74}$$

dove $n = N' - 1$ nelle (4.73) e (4.74) per il caso che stiamo considerando. L'equazione (4.63) trasforma le (4.73) e (4.74) in

$$Z_n^2 = 8h^6 + (-1)^n \tag{4.75}$$

e

$$2Y_n^2 = h^6 - (-1)^n \tag{4.76}$$

rispettivamente.

Allora ci riduciamo a risolvere due equazioni diofantee

$$8x^6 \pm 1 = y^2$$

e

$$x^6 \pm 1 = 2y^2$$

Si tratta di un semplice esercizio (cfr.[Sta67], Lemma 5). Quelle ottenute sono esattamente le stesse equazioni che Heegner doveva risolvere usando il suo metodo. Dopo aver risolto tali equazioni, scopriamo che le uniche soluzioni di (4.73) e (4.74) con $n \geq 0$ sono

$$Y_0 = 2(0)^3, \quad Y_1 = 2(1)^3 \tag{4.77}$$

per (4.73) e

$$Z_0 = (1)^3, \quad Z_1 = (1)^3 \tag{4.78}$$

per (4.74). Usando le condizioni di parità o disparità di N', troviamo allora che le uniche soluzioni di (4.55) sono

$$N = 1, f = 0; \qquad N = 3, f = 6; \qquad N = 5, f = 20.$$

In tal modo possiamo risolvere (refe56)-(4.58). Esse si riducono ultimamente alle equazioni (4.73) e (4.74), a volte con le condizioni di parità invertite. L'equazione (4.74) segue sempre da (4.72) perché Z_n non è mai 0; comunque, dal momento che $Y_0 = 0$, l'equazione (4.73) segue da (4.71) solo se $N' \neq 0$ e quindi se abbiamo N' pari in (4.71), dobbiamo includere $N' = 0$ nella lista di soluzioni alla fine. Il risultato finale è che l'unica soluzione di (4.56) è

$$N = 1, f = 2;$$

le uniche soluzioni di (4.57) sono

$$N = 0, f = 2; \qquad N = 2, f = 4;$$

e l'unica soluzione di (4.58) è

$$N = 0, f = 0.$$

Quindi non esiste in nessun caso una soluzione a (4.56)-(4.58) con $f > 20$. Ritornando ora a f, abbiamo in tutti i casi

$$f = q^{1/12} + O(q^{-1/6}) \tag{4.79}$$

(si vedano (4.40) e (4.43) per l'unico caso qui considerato) dove ricordiamo che

$$q^{1/12} = \sqrt{2}e^{\pi\sqrt{|d|}/12}.$$

La nostra stima dei termini di errore nella (4.79) è tale da garantire che se $|d| \geq 200$, allora $f > 20$. Quindi, se $h(d) = 1$, allora $|d| < -200$. Ciò conclude la dimostrazione. □

Appendice A

Applicazioni alle equazioni diofantee

A.1 Cenni storici

I Pitagorici studiarono molte proprietà dei numeri naturali e il famoso teorema di Pitagora, anche se geometrico, ha un notevole contenuto aritmetico. Gli antichi Babilonesi avevano notato empiricamente molte cosiddette **terne pitagoriche**, come 3, 4, 5 e 5, 12, 13. Una tavola, risalente circa al 1500 a.C., includeva la terna 4961, 6480, 8161, che dimostra le sofisticate tecniche dei Babilonesi. Gli antichi Greci, pur concentrandosi sulla geometria, continuarono ad avere un interesse nelle proprietà aritmetiche dei numeri. Nel 250 d.C. circa Diofanto di Alessandria scrisse un significativo trattato sulle equazioni polinomiali di cui studiava le soluzioni in frazioni. Casi particolari di queste equazioni con soluzioni intere sono tuttora chiamate equazioni diofantee.

Uno dei più grandi teorici dei numeri del XVII secolo fu Pierre de Fermat (1601-1665). La sua fama rimane per la sua corrispondenza con altri matematici, poiché pubblicò molto poco. Alla sua morte lasciò molti teoremi la cui prova era conosciuta, se completa, solo da lui stesso. Il più famoso

di questi fu una nota ai margini della sua copia personale del trattato di Diofanto, scritta in latino, che tradotta dice:

Risolvere un cubo nella somma di due cubi, una potenza quarta nella somma di due potenze quarte, o in generale ogni potenza più alta della seconda in due dello stesso tipo, è impossibile; del qual fatto io ho trovato una notevole dimostrazione. Il margine è troppo piccolo per contenerla...

Più precisamente, Fermat affermò che, al contrario del caso delle terne pitagoriche, l'equazione

$$x^n + y^n = z^n$$

non ha soluzioni intere x, y, z (a parte quelle banali in cui uno o più degli x, y, z sono uguali a zero). Questa affermazione, così semplice da enunciare, è conosciuta come **Ultimo Teorema di Fermat** ed è rimasta una congettura fino al 1994, anno in cui Andrew Wiles ha dato una dimostrazione completa del teorema. Nei 350 anni intercorsi tra l'enunciazione del teorema e la sua dimostrazione, molti matematici si cimentarono con tale problema. Uno degli errori più frequenti fu quello di attribuire erroneamente ad alcuni anelli di numeri la proprietà di essere UFD. Nel seguito della trattazione, forniremo degli esempi di come, invece, la proprietà di essere UFD per gli anelli di numeri nei nove campi quadratici complessi indicati nei precedenti capitoli possa essere sfruttata per risolvere alcune equazioni diofantee particolari.

A.2 Le curve di Mordell

Incominciamo chiarendo le definizioni e i termini di questo tipo di problemi. Consideriamo un polinomio $f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$.
Definiamo **equazione diofantea** l'equazione

$$f(x_1, x_2, \ldots, x_n) = 0 \tag{A.1}$$

di cui cerchiamo **soluzioni intere** (ovvero $x_1, x_2, \ldots, x_n \in \mathbb{Z}$) non banali. Una soluzione di (A.1) con $x_1, x_2, \ldots, x_n \in \mathbb{Q}$ è detta **soluzione razionale**.

Chiaramente, nel caso omogeneo il problema di trovare soluzioni razionali è equivalente a quello di trovare soluzioni intere.

Dimostriamo ora un lemma molto semplice che sta alla base della risoluzione di molte equazioni diofantee.

Lemma 6. *Sia D un UFD. Siano $\alpha, \beta, \gamma \in D$ tali che $\alpha\beta = \gamma^n$ (con $n \in \mathbb{N}$). Se α e β sono coprimi allora esistono $\overline{\alpha}, \overline{\beta} \in D$ e due elementi unitari $\overline{\varepsilon}_1, \overline{\varepsilon}_2 \in D$ tali che $\alpha = \overline{\varepsilon}_1\overline{\alpha}^n$ e $\beta = \overline{\varepsilon}_2\overline{\beta}^n$ e $\overline{\alpha}, \overline{\beta}$ dividono γ.*

Dimostrazione. Sia $\alpha = \pi_1^{m_1} \dots \pi_r^{m_r}$ e $\beta = \pi_{r+1}^{m_{r+1}} \dots \pi_s^{m_s}$ con i π_i $(1 \leq i \leq s)$ fattori irriducibili distinti (per ipotesi). Sia poi $\gamma = \eta_1^{q_1} \dots \eta_t^{q_t}$, con i η_i $(1 \leq i \leq t)$ fattori irriducibili distinti. Per l'unicità di fattorizzazione si ha $t = s$ e a meno di riordinare i fattori di γ, $\pi_i = \varepsilon_i\eta_i$, con ε_i unitari di D. Inoltre si ha $nq_i = m_i$ per $1 \leq i \leq t$. Allora basta porre $\overline{\alpha} = \eta_1^{q_i} \dots \eta_r^{q_r}$ e $\overline{\beta} = \eta_{r+1}^{q_{r+1}} \dots \eta_s^{q_s}$, $\overline{\varepsilon}_1 = \varepsilon_1 \dots \varepsilon_r$ e $\overline{\varepsilon}_2 = \varepsilon_{r+1} \dots \varepsilon_s$, per ottenere la tesi. □

Sfruttiamo questo risultato per dimostrare due teoremi.

Teorema 24. *L'equazione*

$$x^2 + 4 = y^3 \tag{A.2}$$

ha come uniche soluzioni intere $(\pm 11, 5)$ *e* $(\pm 2, 2)$.

Dimostrazione. Sia (x, y) una soluzione intera.
Per prima cosa supponiamo x dispari (e quindi y dispari) e lavoriamo nell'anello $\mathbb{Z}[i]$, che è un UFD. Allora (A.2) si fattorizza nel modo seguente

$$(2 + ix)(2 - ix) = y^3$$

Un fattore comune (proprio) $h + ik$ di $2 + ix$ e $2 - ix$ è anche un fattore della loro somma 4. Considerando le norme si ha

$$(h^2 + k^2) | (x^2 + 4) \qquad (h^2 + k^2) | 16$$

che implicano (x dispari)

$$h^2 + k^2 = 1$$

cioè $h + ik$ unitario. Pertanto $2 + ix$ e $2 - ix$ sono coprimi. Dalla fattorizzazione unica di $\mathbb{Z}[i]$ e dal Lemma 6 segue che uno è $\varepsilon_1\alpha^3$ e l'altro $\varepsilon_2\beta^3$, dove ε_1 e ε_2 sono unitari di $\mathbb{Z}[i]$ e $\alpha, \beta \in \mathbb{Z}[i]$. Ma gli unitari in $\mathbb{Z}[i]$ sono $\pm 1, \pm i$, che sono tutti cubi, pertanto

$$2 + ix = (a + ib)^3$$

per qualche $a, b \in \mathbb{Z}$. Passando ai coniugati, troviamo

$$2 - ix = (a - ib)^3$$

Sommando le due equazioni,

$$4 = 2a(a^2 - 3b^2)$$

cosicché

$$a(a^2 - 3b^2) = 2$$

Si ha perciò che a divide 2, quindi $a \in \{\pm 1, \pm 2\}$ e la scelta di a determina b. È facile vedere che le uniche soluzioni (a, b) sono $(-1, \pm 1)$ e $(2, \pm 1)$. Allora

$$y^3 = ((a + ib)(a - ib))^3 = (a^2 + b^2)^3$$

così (y dispari) $y = a^2 + b^2 = 5$. Allora $x^2 + 4 = 125$, da cui $x = \pm 11$.

Ora supponiamo x pari; poniamo $x = 2X$. Allora y è pari anch'esso; poniamo $y = 2Y$. Abbiamo

$$X^2 + 1 = 2Y^3$$

Quindi X deve essere dispari; poniamo $X = 2k + 1$. Il massimo comune divisore di $(X + i)$ e $(X - i)$ divide la differenza $2i = (1 + i)^2$. Ora, $(1 + i)$ divide $(X + i)$ e $(X - i)$, ma $(1 + i)^2$ no, pertanto il massimo comune divisore di $(X + i)$ e $(X - i)$ è $1 + i$. Ora

$$(1 + iX)(1 - iX)) = 2Y^3$$

e il fattore $1+i$ compare due volte nel membro di sinistra (ricordando che $1+iX = i(X-i)$ e $1-iX = -i(X+i)$).
Quindi dev'esserci una fattorizzazione

$$1+iX = (1+i)(a+ib)^3$$

da cui, ragionando come nel caso precedente (x dispari), si ottiene

$$1 = (a+b)(a^2-4ab+b^2)$$

cosicché $a = \pm 1$ e $b = 0$ o $a = 0$ e $b = \pm 1$. Questo implica $x = \pm 2$ e quindi $y = 2$. □

Teorema 25. *L'equazione*

$$x^2 + 2 = y^3 \tag{A.3}$$

ha come uniche soluzioni intere $(\pm 5, 3)$.

Dimostrazione. Sia (x, y) una soluzione intera. Innanzitutto x è dispari. Altrimenti $2|y$, da cui $4|(x^2+2)$ e quindi $x^2 \equiv 2 \pmod 4$, ma 2 non è un quadrato mod 4.
Lavoriamo nell'anello $\mathbb{Z}[\sqrt{-2}]$, che è un UFD. (A.3) si fattorizza nel modo seguente

$$(x+\sqrt{-2})(x-\sqrt{-2}) = y^3$$

Un fattore proprio $h+\sqrt{-2}k$ di $x+\sqrt{-2}$ e $x-\sqrt{-2}$ deve dividere la loro differenza $2\sqrt{-2}$. Considerando le norme

$$(h^2+2k^2)|8 \qquad (h^2+2k^2)|(x^2+2)$$

che implicano (x dispari)

$$h^2 + 2k^2 = 1$$

cioè $h+\sqrt{-2}k$ unitario. Pertanto $x+\sqrt{-2}$ e $x-\sqrt{-2}$ sono coprimi. Dal Lemma 6 e dal Lemma 2 (unito al fatto che $1^3 = 1$ e $(-1)^3 = -1$) segue che

$$x+\sqrt{-2} = (a+\sqrt{-2}b)^3$$

per qualche $a, b \in \mathbb{Z}$. Prendendo il coniugato, troviamo

$$x - \sqrt{-2} = (a - \sqrt{-2}b)^3$$

Sottraendo le due equazioni,

$$2\sqrt{-2} = 2\sqrt{-2}b(3a^2 - 2b^2)$$

da cui

$$b(3a^2 - 2b^2) = 1$$

che ha come soluzioni intere $a = \pm 1$ e $b = 1$. Da

$$y^3 = ((a + \sqrt{-2}b)(a - \sqrt{-2}b))^3 = (a^2 + 2b^2)^3$$

abbiamo $y = a^2 + 2b^2 = 3$ e $x^2 + 2 = 27$, da cui $x = \pm 5$. □

Questi due teoremi sono esempi di una teoria più vasta che riguarda una famiglia di curve ellittiche studiate in particolare da Mordell.

Definizione 22. *Chiamiamo* ***curva di Mordell*** *una curva di equazione*

$$x^2 + k = y^3 \tag{A.4}$$

con $k \in \mathbb{Z}$.

Si può dimostrare che l'equazione (A.4) ha un numero finito di soluzioni intere per ogni $k \neq 0$ (cfr. [Usp39], pagg.397-401, e [Mor69]).
Eulero scoprì che le uniche soluzioni intere per il caso in cui $k = -1$,

$$x^2 - y^3 = 1 \tag{A.5}$$

sono $(x, y) = (-1, 0),\ (0, \pm 1),\ (2, \pm 3)$. Questo può essere provato in vari modi; in [Usp39] è lasciato come esercizio (pag.413) mentre in [Mor69] è dimostrato (pag.126). Si può notare che l'equazione (A.5) non è altro che un caso particolare della cosiddetta **congettura di Catalan** (1844) secondo la

quale 8 e 9 (2^3 e 3^2) sono le uniche potenze successive (escludendo 0 e 1). In altre parole che

$$x^p - y^q = 1$$

ha come unica soluzione intera non banale $(x, p, y, q) = (3, 2, 2, 3)$.
Questo problema era già stato posto da Levi ben Gerson (1288-1344) ben cinquecento anni prima di Catalan, ma fu risolto solo nel 2002 da Mihăilescu ([Mih04]), che verificò la congettura.

A.3 Il teorema di Ramanujan-Nagell

Diamo un ultimo esempio più complesso e significativo di come la proprietà di fattorizzazione unica degli anelli di numeri possa essere usata per provare teoremi sulle equazioni diofantee. Sfruttando il fatto che A_{-7} è un UFD Nagell verificò la congettura di Ramanujan:

Teorema 26. *Le uniche soluzioni della equazione*

$$x^2 + 7 = 2^n$$

con x, n interi sono

$$\begin{array}{rccccc} \pm x = & 1 & 3 & 5 & 11 & 181 \\ n = & 3 & 4 & 5 & 7 & 15 \end{array}$$

Dimostrazione. x è chiaramente dispari. Supponiamo x positivo.
Caso n pari. Abbiamo la fattorizzazione

$$(2^{n/2} + x)(2^{n/2} - x) = 7$$

cosicché

$$2^{n/2} + x = 7 \qquad 2^{n/2} - x = 1$$

quindi

$$2^{1+n/2} = 8$$

da cui $n = 4$ e $x = 3$.

Caso n dispari. Supponiamo $n > 3$ (si vede facilmente che $n = 3$, insieme a $x = 1$, è l'unica soluzione con $n \leq 3$). Abbiamo che

$$2 = \left(\frac{1+\sqrt{-7}}{2}\right)\left(\frac{1-\sqrt{-7}}{2}\right)$$

è la fattorizzazione di 2 in irriducibili (ricordiamo che A_{-7} è un UFD). x è dispari; poniamo $x = 2k + 1$, così che $x^2 + 7 = 4k^2 + 4k + 8$ è divisibile per 4. Ponendo $m = n - 2$ possiamo riscrivere l'equazione iniziale come

$$\frac{x^2+7}{4} = 2^m$$

così che

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) = \left(\frac{1+\sqrt{-7}}{2}\right)^m \left(\frac{1-\sqrt{-7}}{2}\right)^m$$

e il membro di destra è una fattorizzazione in irriducibili. Nè $\left(\frac{1+\sqrt{-7}}{2}\right)$ nè $\left(\frac{1-\sqrt{-7}}{2}\right)$ sono fattori comuni dei termini a sinistra, perché un fattore comune dovrebbe dividere la loro differenza, $\sqrt{-7}$, che non è possibile (lo si vede passando alle norme). Per la fattorizzazione unica e per il Lemma 2 abbiamo perciò che

$$\left(\frac{x\pm\sqrt{-7}}{2}\right) = \pm\left(\frac{1\pm\sqrt{-7}}{2}\right)^m$$

da cui si ricava che

$$\left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m \in \{\pm\sqrt{-7}\} \tag{A.6}$$

Mostriamo che non si può verificare il caso $+\sqrt{-7}$. Altrimenti, ponendo $a = \left(\frac{1+\sqrt{-7}}{2}\right)$ e $b = \left(\frac{1-\sqrt{-7}}{2}\right)$ (ricordando $ab = 2$, $a + b = 1$ e $a - b = \sqrt{-7}$) avremmo

$$+\sqrt{-7} = a - b = a^m - b^m$$

Poiché

$$a^2 = (1-b)^2 = 1 - 2b + b^2 = 1 - ab^2 + b^2 \equiv 1 \pmod{b^2}$$

e quindi

$$a^m \equiv a(a^2)^{(m-1)/2} \equiv a \qquad (\text{mod } b^2)$$

da cui

$$a \equiv a - b \qquad (\text{mod } b^2)$$

che è assurdo (non esiste $n \in \mathbb{Z}$ tale che $\left(\frac{1+\sqrt{-7}}{2}\right) + n\left(\frac{1+\sqrt{-7}}{2}\right)^2 = \sqrt{-7}$). Quindi il segno deve essere negativo. Ricordando che m è dispari e

$$(x+y)^m = \sum_{k=0}^{m} \binom{m}{k} x^{m-k} y^k$$

$$(x-y)^m = \sum_{k=0}^{m} (-1)^k \binom{m}{k} x^{m-k} y^k$$

da (A.6) con $-\sqrt{-7}$ si ottiene

$$-2^{m-1} = \binom{m}{1} - \binom{m}{3}7 + \binom{m}{5}7^2 - \ldots \pm \binom{m}{m}7^{(m-1)/2}$$

da cui

$$-2^{m-1} \equiv m \qquad (\text{mod } 7) \tag{A.7}$$

Si ha $2^6 \equiv 1 \pmod 7$ e quindi, moltiplicando (A.7) per 6 e scrivendo $m = 42k + l$ otteniamo

$$-3 \cdot 2^l \equiv 6l \qquad (\text{mod } 42)$$

e si ricava facilmente che le uniche soluzioni (m dispari) sono

$$m \equiv 3,\ 5,\ 13 \qquad (\text{mod } 42)$$

Si ha che $n = 5,\ 7,\ 15$ (ricordiamo $n = m + 2$) sono effettivamente soluzioni (con $x = 5,\ 11,\ 181$ rispettivamente). Mostriamo che $m = 3,\ 5,\ 13$ sono gli unici valori che sono validi. Basta mostrare che non possiamo avere due soluzioni dell'equazione originale che siano congruenti mod 42.
Siano m, m_1 due soluzioni congruenti mod 42 e sia 7^l la massima potenza di 7 che divide $m - m_1$. Allora

$$a^{m_1} = a^m a^{m_1-m} = a^m \left(\frac{1}{2}\right)^{m_1-m} (1+\sqrt{-7})^{m_1-m} \tag{A.8}$$

Ora, si ricava (utilizzando gli sviluppi del binomio con conti piuttosto lunghi che omettiamo)

$$\left(\frac{1}{2}\right)^{m_1-m} = \left[\left(\frac{1}{2}\right)^6\right]^{(m_1-m)/6} \equiv 1 \qquad (\text{mod } 7^{l+1})$$

e

$$(1+\sqrt{-7})^{m_1-m} \equiv 1 + (m_1-m)\sqrt{-7} \qquad (\text{mod } 7^{l+1})$$

Dal momento che

$$a^m \equiv \frac{1+m\sqrt{-7}}{2^m} \qquad (\text{mod } 7)$$

sostituendo in (A.8) si ha

$$a^{m_1} \equiv a^m + \frac{m_1-m}{2^m}\sqrt{-7} \qquad (\text{mod } 7^{l+1})$$

e (si ricava allo stesso modo)

$$b^{m_1} \equiv b^m - \frac{m_1-m}{2^m}\sqrt{-7} \qquad (\text{mod } 7^{l+1})$$

ma

$$a^m - b^m = a^{m_1} - b^{m_1}$$

quindi

$$(m-m_1)\sqrt{-7} \equiv 0 \qquad (\text{mod } 7^{l+1})$$

Poiché m e m_1 sono interi, deve essere

$$(m-m_1) \equiv 0 \qquad (\text{mod } 7^{l+1})$$

che contraddice la scelta di l. □

Bibliografia

[All83] R.B.J.T. Allenby. *Rings, fields and groups: an introduction to abstract algebra.* London Arnold, 1983.

[Bor66] Z.I. Borevich, I.R. Shafarevich. *Number theory.* Academic press, 1966.

[Bru00] W. Bruns. *Zahlentheorie.* Fachbereich Mathematik/Informatik, Universität Osnabrück, 2000.

[Dav] H. Davemport. *Aritmetica superiore: un'introduzione alla teoria dei numeri.* Bologna Nicola Zanichelli Editore.

[Dic11] L.E. Dickson. On the negative discriminants for which there is a single class of positive primitive binary quadratic forms. *Bull.Amer.Math.Soc. 17*, pages 534–537, 1911.

[Gau66] C.F. Gauss. *Disquisitiones arithmeticae.* Yale Univ. Press, New Haven, english edition, 1966.

[Hil98] D. Hilbert. *The Theory of Algebraic Number Fields.* Springer, 1998.

[Ire72] K. Ireland, M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer, 1972.

[Mar77] D.A. Marcus. *Number Fields.* Springer, 1977.

[Mih04] P. Mihailescu. Primary cyclotomic units and a proof of catalan's conjecture. *J. reine angew. Math. 572*, pages 167–195, 2004.

[Mor69] L.J. Mordell. *Diophantine equations*. London Academic Press, Inc., 1969.

[Par] Kapil Hari Paranjape. Some lectures on number theory, elliptic curves and cryptology. *www.imsc.res.in/∼kapil*.

[Sta67] H.M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J. 14*, pages 1–27, 1967.

[Sta69] H.M. Stark. On the problem of unique factorization in complex quadratic fields. *Proc. of Symposia in Pure Mathematics, XII, American Math. Soc.*, pages 41–56, 1969.

[Ste79] I.N. Stewart. *Algebraic Number Theory*. Chapman and Hall, 1979.

[Usp39] J.V. Uspensky, M.A. Heaslet. *Elementary number theory*. McGraw-Hill Book Company, 1939.