XI Bienal de Matemática 2024
Universidade Federal de São Carlos - UFSCar
29 de julho a 02 de agosto de 2024

Aritmética em domínios quadráticos

Resolvendo equações Diofantinas não lineares via fatoração

Gondim, Rodrigo[1];

Resumo:

Nesse minicurso vamos apresentar um pouco da aritmética de alguns domínios de inteiros quadráticos, dando maior atenção aos que são domínios euclidianos. Lembramos que domínios euclidianos são domínios de ideais principais e portanto, domínios de fatoração única.

Como queremos trabalhar com fatoração, estaremos particularmente interessados em entender os elementos inversíveis e os elementos irredutíveis, para isso usamos a norma e o traço definidos em domínios quadráticos.

Nosso objetivo final é aplicar a aritmética em tais domínios para tratar certas equações Diofantinas não lineares. A ideia central é fatorar a equação em um domínio que seja de fatoração única e utilizar essa fatoração para resolver a equação, primeiramente no domínio e posteriormente nos inteiros.

Palavras-chave:*Equações Diofantinas, domínios quadráticos, fatoração única.*

[1]UFRPE

Sumário

1 INTRODUÇÃO

Uma equação Diofantina é, em sua versão mais clássica, uma equação polinomial com coeficientes inteiros, em pelo menos duas variáveis, para a qual buscamos encontrar soluções inteiras. As primeiras equações Diofantinas estudadas foram as lineares, que estavam presentes em textos ancestrais na Babilônia, China e Índia, aparecem no clássico *Arithmetica* de Diophantus e foram totalmente resolvidas por Euler. Estamos interessados em estudar certas classes de equações Diofantinas não lineares, utilizando fatoração em domínios quadráticos.

As equações Diofantinas não lineares são um objeto clássico de estudo em matemática, tendo sido um dos grandes motores para o desenvolvimento da álgebra. Vale lembrar que até mesmo para o último teorema de Fermat foi tentada uma abordagem via fatoração. O problema é que nem todos os anéis de inteiros ciclotômicos são de fatoração única. Gauss, no clássico *Disquisitiones Arithmeticae*, já estava interessado no problema de dicernir quando um domínio era fatorial, mas foi Dirichlet quem nos deu as maiores contribuições.

A proposta do minicurso é traçar um caminho geodésico, suave e elementar para apresentar classes de domínios quadráticos que são de fatoração única, a partir dos domínios euclidianos. Assim, seremos capazes de atacar duas classes de equações Diofantinas não lineares que possuem uma fatoração em tais domínios.

Dentre os problemas que estaremos interessados, destacamos alguns clássicos, como ternas pitagóricas e equações de Pell-Fermat, bem como vários problemas de competições matemáticas internacionais incluindo problemas da IMO.

Por completude, incluímos dois apêndices, um sobre a lei da reciprocidade quadrática e um outro sobre primos que podem ser escritos da forma $x^2 + ny^2$.

2 Aritmética em domínios

Esse primeiro capítulo é uma revisão de um curso básico de álgebra, uma boa referência seria [GARCIA].

2.1 Anéis, domínios e corpos

Um anel é uma estrutura algébrica que consiste em um conjunto não vazio e duas operações, assim, escrevemos $(A, +, .)$.

A operação $+$ é chamada de adição.

$$(+) : A \times A \to A \, (a, b) \mapsto a + b$$

A adição cumpre as seguintes condições:

- Associativa: $a + (b + c) = (a + b) + c$;
- Comutativa: $a + b = b + a$;
- Elemento Neutro: $0 + a = a + 0 = a$;
- Simétrico: $a + (-a) = (-a) + a = 0$;

A operação $.$ é chamada multiplicação.

$$(.) : A \times A \to A \, (a, b) \mapsto a.b$$

A multiplicação cumpre as seguintes condições:

- Associativa: $a. \, (b.c) = (a.b) \, .c$;
- Comutativa: $a.b = b.a$;
- Elemento Neutro: $a.1 = 1.a = a$;
- Distributiva: $a. \, (b + c) = a.b + a.c$.

Exemplo 2.1 *1.* $\mathbb{N}$ *não é anel uma vez que não existe simétrico;*

2. $\mathbb{Z}$ *é um anel especial, como vamos ver na próxima seção;*

3. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *são anéis muito especiais, como vamos ver na próxima seção;*

4. Os conjuntos $\mathbb{Z}_n$ *das classes de restos na divisão por* p *são anéis.*

2.2 Anéis especiais

Seja $(A, +, .)$ um anel.

Definição 2.1 Dizemos que $a \in A$, $a \neq 0$ é inversível se existir $b \in A$ tal que $a.b = 1$. Lembramos que o inverso, quando existe, é único e denotado $a^{-1} \in A$.

$$A^* = \{a \in A \mid \ a \text{ é inversível}\}.$$

Definição 2.2 Dizemos que $a \in A$, $a \neq 0$ é divisor de zero se existir $b \in A$, $b \neq 0$ tal que $a.b = 0$.

$$Z(A) = \{a \in A \mid \ a \text{ é divisor de zero}\}.$$

Definição 2.3 *Dizemos que $a \in A$, $a \neq 0$ é nilpotente se existir $n \in \mathbb{N}$ tal que $a^n = 0$.*

Finalmente estamos prontos para definir os anéis especiais que nos interessam.

Definição 2.4 Dizemos que o anel A é um corpo se todo $a \in A, a \neq 0$ é inversível, isto é, $A^* = A \setminus \{0\}$.

Definição 2.5 Dizemos que A é um domínio (de integridade) se $ab = 0$ implica $a = 0$ ou $b = 0$, isto é, $Z(A) = \emptyset$.

Exemplo 2.2

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são corpos.
2. $\mathbb{Z}$ é um domínio, mas não é corpo.
3. $\mathbb{Z}_n$ é um corpo se, e somente se, $n = p$ é primo.

Proposição 2.1 $Z(A) \cap A^* = \varnothing$.

Corolário 2.1 *Todo corpo é um domínio.*

Sejam A um anel e $B \subset A$, dizemos que B é um subanel de A se

(i) $0, 1 \in B$;

(ii) for fechado para adição e multiplicação, isto é, dados $a, b \in B$, tivermos $a + b \in B$ e $a.b \in B$;

(iii) for fechado para o simétrico, isto é, se $a \in B$, então $-a \in B$.

2.3 Anéis de Polinômios

Seja A um anel. Vamos definir $A[x]$, o anel dos polinômios com coeficientes em A em uma indeterminada x.

Definição 2.6 Um polinômio $f \in A[x]$ é uma expressão formal

$$f = a_0 + a_1 x + \ldots + a_n x^n = \sum_{\text{Soma Finita}} a_i x^i$$

Vamos definir a adição de polinômios: Sejam $f = \sum a_i x^i, g = \sum b_i x^i \in A[x]$.

$$f + g = \sum (a_i + b_i)\, x^i \tag{1}$$

A adição cumpre as seguintes condições:

- Associativa;
- Comutativa;
- 0 é o elemento neutro;
- $-f = \sum (-a_i)\, x^i$ é o simétrico de f .

Vamos definir a multiplicação de dois polinômios $f, g \in A[x]$ por $fg = \sum c_i x^i$ em que

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0.$$

Assim, temos

$$c_0 = a_0 b_0,$$

$$c_1 = a_0 b_1 + a_1 b_0.$$

A multiplicação de polinômios cumpre as seguintes condições:

- Associativa;
- Comutativa;
- 1 é o elemento neutro;
- A multiplicação distribui a adição .

Proposição 2.2 *$A[x]$ com a adição e a multiplicação assim definidas é um anel.*

Demonstração: Verifique. □

Vamos agora definir o grau de um polinômio não nulo.

Seja $f \in A[x], f \neq 0$. Denote $f = \sum a_i x^i$, o grau de f será denotado por

$$\text{gr}(f) = max\{n \mid a_n \neq 0\}.$$

Nestas condições, a_n é chamado coeficiente líder e $a_n x^n$ o termo líder.

As propriedades básicas do grau são as seguintes:

1. $\text{gr}(f+g) \leq \max\{\text{gr}(f), \text{gr}(g)\}$. Note que a desigualdade pode ser estrita.

$$f = x^2 + 1, g = -x^2 + x \Rightarrow f + g = x + 1.$$

Se $\text{gr}(f) > \text{gr}(g)$, então $\text{gr}(f+g) = \text{gr}(f)$.

2. $\text{gr}(fg) \leq \text{gr}(f) + \text{gr}(g)$. Note que a desigualdade pode ser estrita.

$$f = \overline{2}x + 1, g = \overline{2}x^3 \Rightarrow f.g = \overline{2}x^3 \in \mathbb{Z}_4[x].$$

Se D é um domínio, então $\text{gr}(f.g) = \text{gr}(f) + \text{gr}(g)$.

Proposição 2.3 *Seja D um domínio. Então os polinômios inversíveis em $D[x]$ são os polinômios constantes, que são inversíveis em D, isto é, $(D[x])^* = D^*$.*

Demonstração: Claro que se $f = c \in D[x]$, com $c \in D^*$, é um polinômio constante, então $f^{-1} = c^{-1}$ pois $f.f^{-1} = c.c^{-1} = 1$.

Reciprocamente, se $f \in D[x]$ é inversível, então existe $g \in D[x]$ tal que $f.g = 1$. Tomando grau, obtemos $\text{gr}(f.g) = \text{gr}(1) = 0$. Como D é um domínio, $\text{gr}(f) + \text{gr}(g) = 0$. Por outro lado, $\text{gr}(f) \geq 0$ e $\text{gr}(g) \geq 0$ logo $\text{gr}(f) = \text{gr}(g) = 0$.

Logo f e g são polinômios constantes, ou seja ,são elementos de D que são inversíveis: $f = c, g = c^{-1}$.

□

Exemplo 2.3 Em $\mathbb{Z}_4[x]$ o polinômio $f = \overline{2}x + \overline{1}$ é inversível uma vez que $f^2 = \overline{1}$.

Em geral temos o seguinte resultado que foge aos nossos objetivos.

Teorema 2.1 *Seja A um anel. Um polinômio $f \in A[x]$ da forma $f = a_n x^n + \ldots + a_1 x + a_0$ é inversível se, e somente se, a_0 é inversível e todo a_i com $i = 1, \ldots, n$ é nilpotente.*

Demonstração: Ver [ATIYAH]. □

Proposição 2.4 *Seja D um anel. $D[x]$ é um domínio se, e somente se, D é um domínio.*

Demonstração:

Inicialmente suponhamos que $D[x]$ é um domínio, vamos mostrar que D é um domínio. Por contrapositiva, suponhamos que D não seja um domínio, então existem $a, b \in D, ab \neq 0$ tais que $a.b = 0$. Considere os polinômios constantes $f = a, g = b \in D[x], f, g \neq 0$ mas $f.g = 0$, daí $D[x]$ não é domínio. Absurdo!

Reciprocamente, se D é um domínio, vamos mostrar que $D[x]$ é um domínio. Com efeito, sejam $f, g \in D[x]$ em que $f, g \neq 0$. Podemos reescrever assim:

$$f = \underbrace{a_n x^n}_{\text{Termo Líder}} + f', \text{com } \operatorname{gr}\left(f'\right) < n.$$

$$g = \underbrace{b_m x^m}_{\text{Termo Líder}} + g', \text{com } \operatorname{gr}\left(g'\right) < m.$$

Como D é um domínio e $a_n, b_m \neq 0$, temos $a_n b_m \neq 0$

$$fg = \underbrace{a_n b_m x^{n+m}}_{\text{Termo Líder}} + h' \Rightarrow fg \neq 0$$

□

2.4 Domínios Euclidianos

Inicialmente lembramos o Teorema da divisão euclidiana original, em $\mathbb{Z}$.

Teorema 2.2 (Divisão Euclidiana) *Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$, unicamente determinados por a, b e efetivamente calculáveis tais que:*

(i) $a = bq + r$;

(ii) $0 \leq r < |b|$.

Vamos entender os ingredientes utilizados na demonstração do teorema da divisão euclidiana.

1. $\mathbb{Z}$ é um domínio;
2. A função $|.| : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ "mede" o "tamanho" do resto;
3. O princípio da boa ordenação em $\mathbb{Z}_+$.

Definição 2.7 Sejam D um domínio e $\varphi : D \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ uma função. Dizemos que (D, φ) é um domínio euclidiano se: Dados $\alpha, \beta \in D$ com $b \neq 0$, existirem $\lambda, \rho \in D$ tais que

(i) $\alpha = \beta\lambda + \rho$;

(ii) $\rho = 0$ ou $\varphi(\rho) < \varphi(\beta)$.

Teorema 2.3 (Algoritmo da divisão de polinômios) *Sejam D um domínio e $f, g \in D[x]$ com $f = a_n x^n + \ldots + a_0$ e $g = b_m x^m + \ldots + b_0$. Se $b_m \in D^*$, então existem $q, r \in D[x]$ tais que:*

(i) $f = gq + r$;

(ii) $r = 0$ *ou* $\text{gr}(r) < \text{gr}(g)$.

Demonstração: Se $n < m$, tome $q = 0$ e $r = f$. Então:

$$f = g.0 + f \text{ e } \text{gr}(f) < \text{gr}(q).$$

Vamos supor agora que $n \geq m$ e apresentar um algoritmo para baixar o grau de f. Seja $f = a_n x^n + \ldots + a_0$ um polinômio de grau $n \geq m$ e defina $f' = f - g.a_n b_m^{-1} x^{n-m}$. É evidente que o coeficiente líder de $g.a_n b_m^{-1} x^{n-m}$ coincide com o coeficiente líder de f, portanto, $\text{gr}(f') < \text{gr}(f)$, isto é, o grau do polinomio baixou.

Por indução na segunda forma podemos assumir que f' cumpra as condições do teorema, assim $f' = f - g.a_n b_m^{-1} x^{n-m} = g.q' + r'$, isso implica em $r' = 0$ ou $\text{gr}\left(r'\right) < \text{gr}(g)$. Portanto, podemos escrever

$$f = g.q + r = g(a_n b_n^{-1} x^{n-m} + q') + r'.$$

Assim, $q = a_n b_n^{-1} x^{n-m} + q'$ e $r = r'$.

□

Corolário 2.2 *Se $\mathbb{K}$ é um corpo, então $\mathbb{K}[x]$ é um Domínio Euclidiano com $\varphi = \text{gr}$.*

2.4.1 Inteiros de Gauss

Os inteiros de Gauss são o seguinte domínio.

$$\mathbb{Z}[i] = \left\{a + bi \mid \ a, b \in \mathbb{Z} \text{ e } i^2 = -1\right\} \subset \mathbb{C} \tag{2}$$

Verifique que $\mathbb{Z}[i]$ é fechado para a adição, para o simétrico e para a multiplicação em $\mathbb{C}$, logo é um subanel de $\mathbb{C}$. Claro que $\mathbb{Z}[i]$ é um domínio uma vez que é um subanel de um corpo (que portanto é um domínio).

Dado $\alpha = a + bi \in \mathbb{Z}[i]$, definimos o conjugado de α por:

$$\overline{a + bi} = a - bi$$

Sejam agora $\alpha, \beta \in \mathbb{Z}[i]$. Verifique as seguintes expressões:

- $\overline{\overline{\alpha}} = \alpha$;
- $\overline{\alpha} = \alpha \Leftrightarrow \alpha \in \mathbb{Z}$;
- $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$;
- $\overline{\alpha\beta} = \overline{\alpha}.\overline{\beta}$.

Dado $\alpha = a + bi$ definimos a norma algébrica de α por:

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

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2 \geq 0$$

Assim sendo, a norma algébrica é uma função:

$$\begin{array}{rccc} N: & \mathbb{Z}[i] & \to & \mathbb{Z}_{\geq}0 \\ & a + bi & \mapsto & a^2 + b^2 \end{array}$$

A propriedade fundamental da norma algébrica é sua multiplicatividade, isto é:

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

Teorema 2.4 *Os inteiros de Gauss* $\mathbb{Z}[i]$ *são um domínio euclidiano com* $\varphi = N$.

Demonstração:

Dados $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$, considere $\alpha\beta^{-1} \in \mathbb{C}$. Denotemos $\alpha = a + bi$ e $\beta = c + di$. Como $\mathbb{C}$ é um corpo faz sentido calcular:

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i$$

Observe agora que $x = \frac{ac+bd}{c^2+d^2} \in \mathbb{Q}$ e $y = \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}$.

Sejam m, n os inteiros mais próximos de x, y respectivamente, isto é, $| x - m | \leq 1/2$ e $| y - n | \leq 1/2$. O inteiro de Gauss $\lambda = m + ni$ será nosso quociente na divisão euclidiana. Assim, definimos $\rho = \alpha - q\beta$ donde obtemos, $\alpha = \lambda\beta + \rho$. Falta mostrar que o resto $\rho \in D$ é "pequeno". Com efeito,

$$\frac{\rho}{\beta} = \frac{\alpha}{\beta} - \lambda = (x + iy) - (m + ni)$$

Reagrupando, obtemos:

$$\frac{\rho}{\beta} = (x - m) + (y - n)i \text{ ou ainda } \rho = \beta[(x - m) + (y - n)i]$$

Assim sendo,

$$N(\rho) = N(\beta)\left[|x-m|^2 + |y-n|^2\right]$$

Por outro lado, $|x-m|^2 \leq \frac{1}{4}$ e $|y-n|^2 \leq \frac{1}{4}$, portanto $N(r) < N(\beta)$ como queríamos demonstrar.

□

Observação 2.1 Observamos que em geral, não podemos garantir a unicidade do quociente e do resto uma vez que tivemos escolhas ambíguas na demonstração. O inteiro mais próximo de 1/2 poderia ser escolhido 0 ou 1, indistintamente.

Exemplo 2.4 Sejam $\alpha = 17 + 13i \in \mathbb{Z}[i]$ e $\beta = 3 + 4i \in \mathbb{Z}[i]$. Vamos fazer a divisão Euclidiana e determinar $\lambda, \rho \in \mathbb{Z}[i]$ tais que $\alpha = \lambda\beta + \rho$ e $N(\rho) < N(\beta)$. Primeiramente, fazemos $\alpha\beta^{-1} \in \mathbb{C}$.

$$\frac{\alpha}{\beta} = \frac{17+13i}{3+4i} = \frac{(17+13i)(3-4i)}{25} = \frac{103}{25} - \frac{29}{25}$$

Ou seja, $x = \frac{103}{25}$ que implica $m = 4$ e $y = -\frac{29}{25}$ que nos fornece $n = -1$ ou seja, $\lambda = 4 - i$. Por definição $\rho = \alpha - \lambda\beta = 17+13i-(3+4i)(4-i) = 17+13i-(16+13i) = 1$.

2.4.2 Inteiros de Eisenstein

Seja $\omega = e^{2\pi/3} \in \mathbb{C}$ uma raíz cúbica primitiva da unidade, isto é $\omega^2 + \omega + 1 = 0$. Note que $\omega^2 = \omega^{-1} = \overline{\omega}$.

Os inteiros de Eisenstein são o domínio:

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Analogamente aos inteiros de Gauss, os inteiros de Eisenstein possuem uma conjugação que consiste na restrição da conjugação em $\mathbb{C}$:

$$\overline{a + b\omega} = a + b\overline{\omega} = a + b\omega^2.$$

Continuando as semelhanças, definimos a norma algébrica em $\mathbb{Z}[\omega]$ por

$$N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = a^2 - ab + b^2 \in \mathbb{Z}_+.$$

Novamente a norma é multiplicativa. Além disso temos o seguinte resultado que será demonstrado na próxima seção.

Teorema 2.5 *Os inteiros de Eisenstein $\mathbb{Z}[\omega]$ são um domínio euclidiano com $\varphi = N$.*

Demonstração: Verifique agora ou espere a próxima seção. □

2.4.3 Domínios do tipo $\mathbb{Z}[\sqrt{d}]$

Seja d um inteiro livre de quadrados, queremos investigar as propriedades aritméticas dos domínios:

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Veremos nas próximas seções que nem sempre tais domínios são euclidianos, um dos nossos objetivos centrais é discutir quais são os possíveis d a fim que o domínio $\mathbb{Z}[\sqrt{d}]$ seja Euclidiano.

2.5 Divisibilidade em Domínios e mdc

Sejam D um domínio e $\alpha, \beta \in D$. Dizemos que β divide α, notação $\beta \mid \alpha$, se existir $\gamma \in D$ tal que $\alpha = \beta\gamma$. Caso contrário $\beta \nmid \alpha$.

Caso trivial: se $\alpha = 0$ ou $\beta = 0$, então a divisibilidade se trivializa. Com efeito, para todo $\beta \in \mathbb{Z}$, temos $\beta \mid 0$ pois $0 = 0.\beta$. Além disso não existe $\alpha \neq 0$ tal que $0 \mid \alpha$ pois, nesse caso, teríamos $\alpha = 0.\gamma = 0$.

A partir de agora vamos considerar $\alpha, \beta \neq 0$.

Propriedades

1. Se $u \in D^*$, então $u \mid \alpha$ para todo $\alpha \in D$, pois $\alpha = u\,(u^{-1}\alpha)$. Tal fatoração é dita fatoração trivial.

2. Se $\gamma \mid \beta$ e $\gamma \mid \alpha$ e $x, y \in D$, então $\gamma \mid \alpha x + \beta y$.

   De fato, $\alpha = \gamma\alpha'$ e $\beta = \gamma\beta' \Rightarrow \alpha x + \beta y = \gamma\alpha' x + \gamma\beta' y = \gamma\left(\alpha' x + \beta' y\right)$.

3. Se $\alpha, \beta \neq 0$ e $\alpha \mid \beta$ e $\beta \mid \alpha$, então $\alpha = u\beta\,(u \in D^*)$. Nesse caso α e β são ditos associados.

   Notação: $\alpha \sim \beta$. Essa é uma relação de equivalência. (Verifique!)

Definição 2.8 Sejam D um domínio e $\alpha, \beta \in D \setminus \{0\}$. Um elemento $\delta \in D$ é dito um mdc para α, β se:

1. $\delta \mid \alpha$ e $\delta \mid \beta$;

2. Se $\delta' \mid \alpha$ e $\delta' \mid \beta$ então $\delta' \mid \delta$.

Observação 2.2 O mdc nem sempre existe. Além disso, quando existe, só está definido a menos de associados. A classe dos domínios para os quais todo par de elementos possui mdc contém a classse dos domínios de fatoração única, como veremos mais adiante.

Lema 2.1 (Lema de Euclides) *Seja D um domínio e $\alpha, \beta \in D \setminus \{0\}$. Sejam ainda $\lambda, \rho \in D$ tais que $\alpha = \beta\lambda + \rho$. Se existir* $\mathrm{mdc}\,(\beta, \rho)$*, então existe* $\mathrm{mdc}\,(\alpha, \beta)$ *e além disso:* $\mathrm{mdc}\,(\alpha, \beta) \sim \mathrm{mdc}\,(\beta, \rho)$.

Demonstração: Vamos mostrar que o conjunto dos divisores comuns de α, β coincide com o conjunto dos divisores comuns de β, α e o resultado segue. De fato, se $\delta \mid \alpha$ e $\delta \mid \beta$, então $\delta \mid \rho = \alpha - \beta\lambda$. Reciprocamente, se $\delta \mid \beta$ e $\delta \mid \rho$, então $\delta \mid \alpha = \beta\lambda + \rho$. □

Teorema 2.6 *Seja (D, φ) um domínio euclidiano. O algoritmo das divisões sucessivas entre $\alpha, \beta \in D \setminus 0$, fornece um* mdc *para α, β.*

Demonstração: Considere $\alpha = \rho_{-1}$ e $\beta = \rho_0$, dividindo α por β, obtemos $\alpha = \beta\lambda + \rho$ e denotamos $\lambda_1 = \lambda$ e $\rho_1 = \rho$. Pelo lema de Euclides, $\text{mdc}(\rho_{-1}, \rho_0) = \text{mdc}(\rho_0, \rho_1)$. Se $\beta \mid \alpha$, então $\rho = 0$ e o algorítmo termina. Nesse caso, $\text{mdc}(\alpha, \beta) = \beta$. Caso contrário, fazendo divisões sucessivas, obtemos indutivamente ρ_{i+1} e λ_{i+1} a partir da fórmula

$$\rho_{i-1} = \rho_i\lambda_{i+1} + \rho_{i+1}.$$

Pelo Lema de Euclides, temos:

$$\text{mdc}\,(\alpha, \beta) \sim \text{mdc}\,(\rho_0, \rho_1) \sim \text{mdc}\,(\rho_1, \rho_2) \sim \cdots$$

Note que deve existir $k \in \mathbb{N}$ tal que $\rho_{k+1} = 0$.

Com efeito, caso não houvesse tal k, teríamos uma sequencia decrescente infinita de naturais:

$$\varphi\,(\rho_1) > \varphi\,(\rho_2) > \varphi\,(\rho_3) > \cdots$$

Isso é um absurdo.

Para tal k, temos $r_k \mid r_{k-1}$. Assim sendo, r_k é um $\text{mdc}(r_k, r_{k-1})$.

□

Exemplo 2.5 $\text{mdc}\,(x^4 - 1, x^3 + x^2 + x + 1) \in \mathbb{Q}\,[x]$.

$$\text{mdc}\left(x^4 - 1, x^3 + x^2 + x + 1\right) = x^3 + x^2 + x + 1.$$

Teorema 2.7 (Lema de Bézout) *Seja (D, φ) um domínio euclidiano e sejam $\alpha, \beta \in D$ e $\delta = \text{mdc}(\alpha, \beta)$, então existem $x, y \in D$ tais que:*

$$\alpha x + \beta y = \delta.$$

Além disso, tais x, y podem ser efetivamente calculados por divisões sucessivas.

Demonstração: [O algorítmo estendido de Euclides]

Novamente, denotemos $\rho_{-1} = \alpha$ e $\rho_0 = \beta$ Claramente, $\rho_{-1} = 1.a + 0.b$, assim definimos $x_{-1} = 1$ e $y_{-1} = 0$. Analogamente, $r_0 = 0.a + 1.b$, definimos $x_0 = 0$ e $y_0 = 1$.
Indutivamente, podemos definir ρ_{i+1} e λ_{i+1} a partir de divisões sucessivas:

$$\rho_{i-1} = \rho_i\lambda_{i+1} + \rho_{i+1}.$$

Agora, indutivamente, se conhecemos $\rho_{i-1} = \alpha x_{i-1} + \beta y_{i-1}$ e $\rho_i = \alpha x_i + \beta y_i$ obtemos

$$\rho_{i+1} = \rho_{i-1} - \rho_i \lambda_{i+1} = (\alpha x_{i-1} + \beta y_{i-1}) - \lambda_{i+1}(\alpha x_i + \beta y_i) = \alpha(x_{i-1} - \lambda_{i+1} x_i) + \beta(y_{i-1} - \lambda_{i+1} y_i).$$

Finalmente, definimos $x_{i+1} = x_{i-1} - \lambda_{i+1} x_i$ e $y_{i+1} = y_{i-1} - \lambda_{i+1} y_i$.
Sabemos que o algoritmo de Euclides para o mdc termina quando $r_{k+1} = 0$ sendo $r_k = \text{mdc}(\alpha, \beta)$. Assim, obtemos $x = x_k$ e $y = y_k$, uma solução da equação original.

□

2.6 Elementos primos e irredutíveis

Nessa seção gostaríamos de destacar dois conceitos muito importantes da aritmética em domínios, a saber: os conceitos de elemento primo e de elemento irredutível. Nos *Elementos*, Euclides já identificava essas duas propriedades para os interiros e entendia a relação entre elas, mas não foi além, lembramos que Euclides nunca se importou com a unicidade de fatoração tendo esta sido dada como certa por dois milênios sem uma adequada demonstração. Por outro lado, Gauss em seu *Disquisitiones arithmeticae* compreendeu profundamente o papel que cada um desses conceitos desempenhava naquela que é a primeira demonstração do assim chamado Teorema Fundamental da Aritmética (da existência e unicidade de fatoração nos inteiros). Como ele mesmo ressaltou, durante séculos as pessoas utilizavam a unicidade da fatoração em primos nos inteiros sem nunca ninguém tê-la demonstrado. Ele percebeu ainda que a unicidade da fatoração não é verdade em todos os domínios, como veremos no Exemplo 2.6.

Sejam D um domínio e $\alpha, \beta \in D$, $\alpha, \beta \neq 0$. Lembramos que β *divide* α, e escrevemos $\beta \mid \alpha$ se existir $\gamma \in D$ tal que $\alpha = \beta\gamma$; essa é chamada uma *fatoração* de α em D. Claramente, se $u \in D$ é um elemento invertível, então $u \mid \alpha$ para todo $\alpha \in D$, de modo que uma fatoração $\alpha = u(u^{-1}\alpha)$ é chamada fatoração trivial.

Definição 2.9 Um elemento $\pi \in D \setminus \{0\}$, não invertível, é chamado *irredutível* se só admitir fatoração trivial.

Definição 2.10 Um elemento $\pi \in D \setminus \{0\}$ é um *elemento primo* se π não for inversível e se $\pi \mid \alpha\beta$ implicar $\pi \mid \alpha$ ou $\pi \mid \beta$.

Em primeiro lugar vejamos como se relacionam tais conceitos:

Proposição 2.5 *Sejam D um domínio e $\pi \in D$. Se π é um elemento primo, então π é irredutível.*

Demonstração: Seja $\pi = \alpha\beta$ uma fatoração de π. Devemos mostrar que tal fatoração é trivial. Como $\pi \mid \alpha\beta$ e π é primo, então $\pi \mid \alpha$ ou $\pi \mid \beta$. Digamos que $\pi \mid \alpha$, sem perda de generalidade, ou seja, $\alpha = \pi\lambda$. Daí $\pi = \pi\lambda\beta$ e como $\pi \neq 0$ e D é um domínio, obtemos $\beta\lambda = 1$ que implica que β é invertível como queríamos demonstrar. □

Exemplo 2.6 Considere o domínio $D = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b, \in \mathbb{Z}\}$. Considere as seguintes fatorações de $4 = 4 + 0\sqrt{5}$.

$$(2 + 0\sqrt{5})(2 + 0\sqrt{5}) = 4 + 0\sqrt{5} = (1 + \sqrt{5})(-1 + \sqrt{5}).$$

É fácil verificar que $2 \in D$ é irredutível, por outro lado, $2 \nmid (1 + \sqrt{5})$ e $2 \nmid (-1 + \sqrt{5})$ que mostra que 2 não é primo em D.

Observação 2.3 Nos inteiros, a demonstração usual da equivalência entre os conceitos de irredutível e primo se utiliza do Lema de Bezout, que diz: dados $a, b \in \mathbb{Z}$ e $d = \text{mdc}(a, b)$, existem inteiros x, y tais que $ax + by = d$. Em domínios em que vale uma relação tipo Bézout temos a recíproca da proposição 2.5. Se o domínio D for euclidiano, então é possível fazer um algoritmo estendido de Euclides, que é uma relação de Bézout e concluir a equivalência entre os conceitos de primo e irredutível. Como vimos no Exemplo 2.6 anterior existe uma relação entre a não equivalência desses conceitos e a possibilidade de múltiplas fatorações não equivalentes para um mesmo elemento.

2.7 Ideais em um anel

Sejam A um anel e $I \subset A$ um subconjunto. Dizemos que I é um ideal de A se:

(i) $0 \in I$;

(ii) $x, y \in I \Rightarrow x + y \in I$;

(iii) $x \in I, \alpha \in A \Rightarrow \alpha x \in I$.

Exemplo 2.7 Seja A um anel, os seguintes ideais são chamados triviais.

1. $0 = \{0\} \subset A$ (Ideal Nulo);
2. $A \subset A$ (Ideal Total).

Um ideal não trivial $I \subset A$ satisfaz $0 \subsetneq I \subsetneq A$.

Proposição 2.6 *Sejam A um anel e $I \subset A$ um ideal. Se existir $u \in A^*$ (elemento inversível) tal que $u \in I$, então $I = A$.*

Demonstração: Por definição, $I \subset A$, falta mostrar que $A \subset I$. Seja $\alpha \in A$, escreva $\alpha = u(u^{-1}\alpha)$ como $u \in I$ obtemos $\alpha \in I$ e o resultado segue. □

Corolário 2.3 *Seja $\mathbb{K}$ um corpo. Os únicos ideais de $\mathbb{K}$ são os triviais.*

Demonstração: Seja $I \subset \mathbb{K}$ um ideal. Se $I \subset \mathbb{K}$ é um ideal não nulo. Existe $x \in I$, $x \neq 0$. Como $\mathbb{K}$ é um corpo, x é inversível, logo $I = \mathbb{K}$. □

Os corpos são desinteressantes do ponto de vista aritmético.

Quando o anel A não ee um corpo, sempre existem ideais não triviais. O primeiro tipo de tais ideais são os ditos ideais principais, gerados por um elemento não nulo e não inversível.

Definição 2.11 Sejam A um anel e $a \in A$, o conjunto $I = aA = (a) = \{ak \mid k \in A\}$ é um ideal de A chamado ideal principal gerado por a.

Claramente $(0) = 0$ e se $u \in A^*$ é um elemento inversível, então $(u) = A$.

Caso contrário, $a \neq 0$ e $a \notin A^*$, então $0 \subsetneq (a) \subsetneq A$.

Exemplo 2.8 Ideais não triviais em $\mathbb{Z}$.

1. O conjunto dos números pares é um ideal em $\mathbb{Z}$.
   - $0 \in I$ pois $0 = 2.0$;
   - $x, y \in I$, então $x = 2k$, $y = 2q$, logo $x + y = 2(k + q)$;
   - $x \in I, a \in \mathbb{Z}, x = 2k$ logo $ax = a(2x) = 2(ak) \in I$.
2. Em geral, dado $n \in \mathbb{Z}$, o conjunto $n\mathbb{Z} = (n) = \{nk \mid k \in \mathbb{Z}\}$ é um ideal principal de $\mathbb{Z}$ chamado ideal gerado por n.
   - $0 \in n\mathbb{Z}$ pois $0 = n.0$.
   - $x, y \in n\mathbb{Z}$, $x = nk$, $y = nq$, logo $x + y = n\,(k + q)$ em $\mathbb{Z}$.
   - $x \in n\mathbb{Z}$, $n \in \mathbb{Z}$, $x = nk$ logo $ax = a\,(nk) = (ak) \in n\mathbb{Z}$.

Além disso, todos os ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z}$, ou seja, são principais. Assim, $\mathbb{Z}$ é um Domínio de Ideais Principais (DIP)

2.8 Ideais Finitamente Gerados

Sejam A um anel e $\alpha_1, \alpha_2, ..., \alpha_n \in A$. O conjunto

$$(\alpha_1, \ldots, \alpha_n) = \{\alpha_1 x_1 + \ldots + \alpha_n x_n \mid x_i \in A\}$$

é um ideal de A. Dizemos que esse é o ideal gerado por $\{\alpha_1, \ldots, \alpha_n\}$.

Proposição 2.7 *$I = (\alpha_1, \ldots, \alpha_n) \subset A$ é um ideal de A.*

Demonstração: De fato,

(i) $0 \in I$.

(ii) Se $x, y \in I \Rightarrow x + y \in I$. Com efeito,

$$x = \alpha_1 x_1 + \ldots + \alpha_n x_n;$$

$$y = \beta_1 x_1 + \ldots + \beta_n x_n.$$

Portanto

$$x + y = (\alpha_1 + \beta_1)x_1 + \ldots + (\alpha_n + \beta_n)x_n \subset I.$$

(iii) Se $x \in I, \alpha \in A$, então $\alpha x \in I$.

$$\alpha x = (\alpha\alpha_1)x_1 + \ldots + (\alpha\alpha_n)x_n \in I.$$

□

Observação 2.4 Eventualmente um ideal que é dado por um conjunto de n elementos, poderia ser gerado por uma quantidade menor de elementos.

Caso Especial: Seja D um domínio e sejam $\alpha, \beta, \gamma \in D$. Suponhamos que o ideal gerado por α, β possa ser gerado por γ, apenas, isto é: $(\alpha, \beta) = (\gamma)$. Vamos interpretar essa igualdade.

Primeiramente, $\alpha, \beta \in (\gamma) \subset D \Leftrightarrow \gamma \mid \alpha$ e $\gamma \mid \beta$. Nesse caso $\gamma \mid \alpha x + \beta y$ quaisquer que sejam $x, y \in D$.

Por outro lado, $\gamma \in (\alpha, \beta) \subset D \Leftrightarrow \gamma = \alpha x + \beta y$, para alguns $x, y \in D$. Note que se $\gamma' \mid \alpha$ e $\gamma' \mid \beta$, então $\gamma' \mid \alpha x + \beta y = \gamma$.

Assim, concluímos que γ é um mdc para α e β.

Definição 2.12 *Um anel A é dito Noetheriano se todos os seus ideais são finitamente gerados.*

Teorema 2.8 *Seja A um anel. São equivalentes as seguintes condições:*

(i) *A é Noetheriano;*

(ii) *Toda cadeia ascendente de ideais em A*

$$I_1 \subset I_2 \subset \ldots$$

é estacionária, isto é, existe k tal que $I_k = I_{k+1} = \ldots$

Demonstração: Ver [ATIYAH]. □

2.9 Domínios de Ideais Principais

Um domínio D é dito domínio de ideais principais (DIP) se todo ideal em D for da forma $I = \alpha D$ para algum $\alpha \in D$.

Em um DIP, dados $\alpha, \beta \in D$, existe $\gamma \in D$ tal que $(\alpha, \beta) = (\gamma)$ logo $\gamma = \text{mdc}(\alpha, \beta$ e além disso, existem $x, y \in D$ tais que $\alpha x + \beta y = \gamma$. Ou seja um DIP é um ambinte no qual sempre vale uma relação tipo Bezout. Nesse caso, vamos ver que todo elemento irredutível num DIP é primo.

Teorema 2.9 (DE $\Rightarrow$ DIP) *Todo domínio euclidiano é um domínio de ideais principais.*

Demonstração:

Seja $\alpha \in I, \alpha \neq 0$ um elemento tal que $\varphi(\alpha) \in \mathbb{Z}_+$ é mínimo. Vamos mostrar que $I = \alpha D$). Por um lado, $\alpha \in I$ nos fornece $(\alpha) \subset I$. Falta mostrar que $I \subset (\alpha)$.

Seja $\beta \in I$, queremos mostrar que $\beta \in (\alpha)$, ou seja $\alpha \mid \beta$. Fazendo a divisão euclidiana de β por α, obtemos $\lambda, \rho \in D$ tais que $\varphi(\rho) < \varphi(\alpha)$ desde que $\rho \neq 0$. Por outro lado, $\rho = \beta - \alpha\lambda, \beta \in I$ e $\alpha \in I \Rightarrow \alpha\lambda \in I$ logo $\rho \in I$, pela minimalidade de $\varphi(\alpha)$, não podermos ter $\varphi(\rho) < \varphi(\alpha)$, portanto $\rho = 0$. Daí $I = (\alpha)$. □

Exemplo 2.9 Vamos ver na próxima seção que todo DIP é Domínio de fatoração única. Por outro lado, o Domínio $D = \mathbb{Z}[x]$ é de fatoração única mas não é um domínio de ideais principais.

Com efeito, sejam $f = 2, g = x \in \mathbb{Z}[x]$, sabemos que um $\text{mdc}(2, x) = 1$ (verifique).

Por outro lado, não existem $\tilde{f}, \tilde{g} \in \mathbb{Z}[x]$ tais que $2\tilde{f} + x\tilde{g} = 1$.

De fato, suponhamos, por absurdo, $\tilde{f} = a_0 + a_1 x + \cdots + a_n x^n$

$\tilde{g} = b_0 + b_1 x + \cdots + b_m x^n$ tal que

$2\tilde{f} + x\tilde{g} = 1$, faça $x = 0$

$$2\tilde{f}(0) + (0) = 1 \tag{3}$$

$2a_0 = 1$ que é um absurdo para $a_0 \in \mathbb{Z}$.

O ideal $(2, x)$ não é principal em $\mathbb{Z}[x]$.

Proposição 2.8 (DIP: Irredutível $\Leftrightarrow$ Primo) *Num DIP todo elemento irredutivel é primo, assim, os conceitos de primo e irredutível coincidem.*

Demonstração: Seja $\alpha \in D$ um elemento irredutível, digamos que $\alpha \mid \beta\gamma$ e $\alpha \nmid \beta$. Sendo α irredutível em D, temos $\text{mdc}(\alpha, \beta) = 1$. Como D é um DIP, temos a seguinte igualdade de ideais $(\alpha, \beta) = (1) = D$. Assim, existem $x, y \in D$ tais que $\alpha x + \beta y = 1$. Multiplicando por γ, obtemos $\alpha\gamma x + \beta\gamma y = \gamma$, daí, concluímos que $\alpha \mid \gamma$ uma vez que $\alpha \mid \beta\gamma$, por hipótese.

2.10 Domínios de Fatoração Única

Os domínios de fatoração única são o ambiente adequado para resolver equações Diofantinas via fatoração. A fim de evitar patologias indesejadas, vamos sempre supor que os domínios sejam Noetherianos.

Definição 2.13 *Dizemos que um domínio Noetheriano D é um domínio de fatoração única (DFU) se para todo $\alpha \in D$ com $\alpha \neq 0$ e $\alpha \notin D^*$, existirem elementos irredutíveis $\pi_1, \ldots, \pi_n \in D$ tais que $\alpha = \pi_1 \ldots \pi_n$, e além disso, tal fatoração seja essecialmente única, a menos de permutação e associados, isto é, se houver outra fatoração desse tipo, $\alpha = \tau_1 \ldots \tau_n$, então $m = n$ e a menos de permutação $\pi_i \sim \tau_i$ para todo $i = 1, \ldots, n$.*

Proposição 2.9 (Existência de fatoração) *Seja D um domínio Noetheriano. Então todo elemento não nulo de D que não é inversível pode ser escrito como um produto finito de elementos irredutíveis.*

Demonstração: Considere o seguinte conjunto:

$$S = \{0\} \cup D^* \cup \{\alpha \in D \mid \alpha \text{ é produto de um número finito de elementos irredutíveis}\}.$$

Suponhamos que $S \neq D$ e seja $\alpha \in D \setminus S$, como α não é zero nem inversível e nem irredutível, podemos escrever $\alpha = \beta\gamma$ em que β, γ não são nulos e nem inversíveis. Assim, $\beta, \gamma \mid \alpha$, mas nem β e nem γ são associados a α. Além disso, $\beta \in D \setminus S$ ou $\gamma \in D \setminus S$ pois caso contrário, se $\beta, \gamma \in S$, então $\alpha = \beta\gamma \in S$. Podemos então construir, por indução, uma sequência (α_n) tal que $\alpha_1 = \alpha$ e $\alpha_{n+1} \mid \alpha_n$ mas não são associados. Seja $I = \{\delta \in D \mid \alpha_n \mid \delta \text{ para algum } n\}$. Afirmo que I é um ideal de D e que o mesmo não é finitamente gerado (verifique). Isso é uma contradição pois A é Noetheriano. Daí concluímos que $S = D$ e o resultado segue. □

Proposição 2.10 (DFU: irredutível $\Leftrightarrow$ primo) *Seja D um domínio Noetheriano. Então são equivalentes as seguintes afirmações*

(i) *D é um domínio de fatoração única;*

(ii) *Todo elemento irredutível de D é primo.*

Demonstração: Sejam D um DFU e $\pi \in D$ um elemento irredutível. Vamos mostrar que π é primo. Suponha que $\pi \mid \beta\gamma$, então existe $\delta \in D$ tal que $\beta\gamma = \pi\delta$ escrevendo a fatoração em irredutíveis de β e γ e usando a unicidade da fatoração é fácil ver que $\pi \mid \beta$ ou $\pi \mid \gamma$ uma vez que π é um elemento irredutível que necessariamente pertence a união das fatorações.

Reciprocamente, suponha que todo elemento irredutível de D seja primo. Como cada elemento de D possui fatoração em irredutíveis, só nos resta mostrar que tal fatoração é única, a menos de ordem e de associados.

Suponha que $\alpha \in D$ possui duas fatorações em irredutívies.

$$\pi_1 \ldots \pi_n = \alpha = \tau_1 \ldots \tau_m.$$

Como em D todo irredutível é primo, π_1 é primo e como $\pi_1 \mid \tau_1 \dots \tau_m$, podemos supor, sem perda de generalidade que $\pi_1 \mid \tau_1$. Por hipótese τ_1 é irredutível, logo π_1 e τ_1 são associados.

Supondo $n \leq m$ e usando o argumento anterior para cada um dos irredutíveis $\pi_1, \dots, \pi_n$, obtemos $\pi_1 = \tau_1, \dots, \pi_n = \tau_n$. Queremos concluir que $m = n$. Se não for o caso, então $m > n$ e temos

$$\tau_{n+1} \dots \tau_m = u.$$

Nessa fatoração u é um invertível e isso implica que os τ_j são invertíveis para $j = n+1, \dots, m$ que é um absurdo. Logo concluímos que $m = n$ e a unicidade segue. □

Corolário 2.4 (DIP ⇒ DFU) *Todo domínio de ideais principais é domínio de fatoração única.*

Demonstração: Primeiramente, note que todo DIP é Noetheriano, assim, a existência de fatoração segue da Proposição 2.9. Nos resta mostrar a unicidade de fatoração. Pela Proposição 2.8, sabemos que num DIP os conceitos de primo e irredutível coincidem, portanto, pela Proposição 2.10, a unicidade segue.

Da mesma forma que se faz nos inteiros, podemos organizar a fatoração de um elemento $\alpha \in D$ da forma $\alpha = u\pi_1^{e_1} \dots \pi_n^{e_n}$ em que cada um dos π_i não são associados e $u \in D^*$. Além disso, dados $\alpha, \beta \in D$ podemos utilizar os mesmos irredutíveis em ambas fatorações. Para isso, consideramos expoentes nulos caso um irredutível divida apenas um dos dois.

Proposição 2.11 *Sejam $\alpha, \beta \in D \setminus 0$ com $\alpha, \beta \notin D^*$ fatorados como $\alpha = u\pi_1^{e_1} \dots \pi_n^{e_n}$ e $\beta = v\pi_1^{f_1} \dots \pi_n^{f_n}$ em que $u, v \in D^*$ e com $e_i, f_i \geq 0$. Então:*

1. *$\beta \mid \alpha$ se, e somente se, $f_i \leq e_i$ para todo $i = 1, \dots, n$;*
2. *Seja $M_i = \max\{e_i, f_i\}$ e $m_i = \min\{e_i, f_i\}$. Então*
   - *(a)* $\operatorname{mdc}(\alpha, \beta) \sim \pi_1^{m_1} \dots \pi_n^{m_n}$.
   - *(b)* $\operatorname{mmc}(\alpha, \beta) \sim \pi_1^{M_1} \dots \pi_n^{M_n}$.

   Em particular, $\alpha\beta \sim \operatorname{mdc}(\alpha, \beta) \operatorname{mmc}(alpha, \beta)$.

Demonstração: Verifique! □

Terminamos a seção enunciando o Teorema de Gauss.

Teorema 2.10 (Teorema de Gauss) *O domínio $\mathbb{Z}[X]$ é um Domínio de fatoração única.*

Demonstração: Ver [GARCIA] Página 48 Teorema II.3.1. □

2.11 Dois lemas úteis em um DFU

Em teoria dos números clássica o próximo resultado é conhecido como o Lema $ab = cd$, aqui seria algo como o lema $\alpha\beta = \gamma\delta$.

Lema 2.2 (Lema $ab = cd$) *Seja D um DFU e sejam $\alpha, \beta, \gamma, \delta \in D$ elementos não nulos tais que $\alpha\beta = \gamma\delta$. Então existem $x, y, z, w \in D$ tais que $\alpha = xy$, $\beta = zw$, $\gamma = xz$ e $\delta = yw$, além disso,* $\mathrm{mdc}(y, z) = 1$.

Demonstração: Seja K o corpo de frações de D. Como $\frac{\alpha}{\gamma} = \frac{\delta}{\beta}$ e D é um DFU, sabemos que existe uma representação irredutível da fração, digamos $\frac{\alpha}{\gamma} = \frac{\delta}{\beta} = \frac{y}{z}$ com $\mathrm{mdc}(y, z) = 1$. Agora temos $\alpha z = \gamma y$ que implica $z \mid \gamma$, logo $\gamma = xz$ para algum $x \in D$ e $\delta z = \beta y$ que nos fornece $z \mid \beta$, portanto $\beta = zw$ para algum $w \in D$. O resultado segue imediatamente. □

Exemplo 2.10 (IMO-SL-78) Prove que para quaisquer inteiros positivos x, y, z tais que $xy - z^2 = 1$ podemos encontrar inteiros não negativos a, b, c, d tais que $x = a^2 + b^2$, $y = c^2 + d^2$ e $z = ac + bd$.

Vamos escrever $xy = z^2 + 1$ e fatorar em $\mathbb{Z}[i]$, inteiros de Gauss, que sabemos ser um DFU. Temos $xy = (z + i)(z - i)$, assim, pelo Lema 2.2, existem inteiros Gaussianos $\alpha, \beta, \gamma, \delta$ tais que $x = \alpha\beta$, $y = \gamma\delta$, $z + i = \alpha\gamma$ e $z - i = \beta\delta$.

Vamos escrever $\alpha = a_1 + a_2 i$, $\beta = b_1 + b_2 i$, $\gamma = c_1 + c_2 i$ e $\delta = d_1 + d_2 i$. Primeiramente note que $\mathrm{mdc}(a_1, a_2) = \mathrm{mdc}(b_1, b_2) = \mathrm{mdc}(c_1, c_2) = \mathrm{mdc}(d_1, d_2) = 1$. Com efeito, se existisse $p \in \mathbb{Z}$ um primo tal que $p \mid \mathrm{mdc}(a_1, a_2)$, então $p \mid z + i \in \mathbb{Z}[i]$ que é um absurdo. As outras igualdades são similares.

Nessas condições, como $\alpha\beta = x$, devemos ter $\beta = q\overline{\alpha}$ para algum $q \in \mathbb{Q}$, escrevendo $q = \frac{m}{n}$ obtemos $n\beta = m\overline{\alpha}$ daí $\mathrm{mdc}(nb_1, nb_2) = \mathrm{mdc}(ma_1, ma_2)$ e portanto $m = n$ logo $\beta = \overline{\alpha}$. Analogamente, $\gamma = \overline{\delta}$. Segue diretamente que $x = \alpha\beta = \alpha\overline{\alpha} = a_1^2 + a_2^2$, $y = d\overline{d} = d_1^2 + d_2^2$ e após algumas continhas encontramos $z = a_1 d_1 + a_2 d_2$.

O próximo lema é bastante elementar deixamos a demonstração ao leitor (usar a fatoração única).

Lema 2.3 *Seja D um DFU e sejam $\alpha, \beta, \gamma \in D \setminus 0$ com $\alpha, \beta, \gamma \notin D^*$. Se $\alpha\beta = \gamma^n$ para algum $n \in Z$ com $n \geq 2$, e $\mathrm{mdc}(\alpha, \beta) = 1$, então existem $\tau_1, \tau_2 \in D$ e $u \in D^*$ tais que $a = u\tau_1^n$, $b = u^{-1}\tau_2^n$ e $\gamma = \tau_1\tau_2$.*

Exemplo 2.11 (Ternas pitagóricas) Sejam $a, b, c \in \mathbb{Z}$ inteiros coprimos tais que $a^2 = b^2 + c^2$. Então b, c tem paridades distintas, digamos b é ímpar e c é par, além disso, existem inteiros coprimos $m < n$ tais que $a = n^2 + m^2$, $b = n^2 - m^2$ e $c = 2mn$

Primeiramente note que $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, c) = \mathrm{mdc}(c, b) = 1$ e que a primeira asserção é elementar.

Fatorando em $\mathbb{Z}[i]$, temos $a^2 = (b+ci)(b-ci)$. Vamos mostrar que $\mathrm{mdc}(b+ci, b-ci) = 1$ para utilizar o lema. De fato, seja $\delta = \mathrm{mdc}(b + ci, b - ci)$, pelas propriedades do mdc,

temos $\delta \mid 2b$ *e* $\delta \mid 2c$ *em* $\mathbb{Z}[i]$. *Como* $\text{mdc}(b,c) = 1$ *em* $\mathbb{Z}$, *é facil ver que* $\text{mdc}(b,c) = 1$ *em* $\mathbb{Z}[i]$. *Daí segue que* $\delta \mid 2$, *mas sabsmo que* $\delta = 2$ *é impossível uma vez que* b *e* c *tem paridades distaintas. Vamos mostrar que* $\delta = 1$. *De fato, suponhamos que* $\delta \neq 1$, *então* $\delta \sim 1+i$, *donde concluímos que* $1+i \mid b+ci$, *que implica* $2 \mid b^2+c^2$, *absurdo.*

Logo, $b+ci, b-ci$ *são coprimos em* $\mathbb{Z}[i]$, *e portanto, existem* $m, n \in \mathbb{Z}$ *tais que* $b+ci = u(n+mi)^2$. *Como* $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ *(verifique), podemos supor, a menos de uma reordenação que* $b+ci = (n+mi)^2 = n^2 - m^2 + 2mni$ *e o resultado segue.*

2.12 Exercícios

1. Mostre que $\mathbb{Z}/n\mathbb{Z}$ é um corpo se, e somente se $n = p$ é um número primo.

2. Mostre que todo domínio finito é um corpo. Sugestão: Se D é um domínio com um número finito de elementos, seja $a \in D \setminus \{0\}$. Defina $\mu : D \to D$ $\mu(x) = ax$. Mostre que a função μ é injetiva e conclua que a mesma é sobrejetiva. Conclua que a é inversível e portanto, D é um corpo.

3. Em cada um dos itens abaixo, determinar o quociente e o resto da divisão de f por g, em que $f, g \in \mathbb{K}[X]$. Em seguida prossiga com o processo de divisões sucessivas de modo a obter um polinômio $d = \text{mdc}(f,g)$ (Algoritmo de Euclides). Encontrar polinômios $a = a(X)$ e $b = b(X)$ tais que $af + bg = d$.

   (a) $f = X^3 + 1$, $g = X^2 - 1$, $\mathbb{K} = \mathbb{Q}$;
   (b) $f = X^3 - 2X^2 + 1$, $g = X^2 - 3$, $\mathbb{K} = \mathbb{Q}$;
   (c) $f = X^4 + X^2 + 1$, $g = X^2 - 1$, $\mathbb{K} = \mathbb{Z}_3$;
   (d) $f = X^5 - 2$, $g = x^2 - \sqrt[5]{4}$, $\mathbb{K} = \mathbb{R}$;
   (e) $f = X^4 - X^2 + 1$, $g = X + i$, $\mathbb{K} = \mathbb{C}$.

4. Em cada um dos itens abaixo, determinar o quociente e o resto da divisão de α por β, em que $\alpha, \beta \in D$, com D domínio euclidiano. Em seguida prossiga com o processo de divisões sucessivas de modo a obter $\delta = \text{mdc}(\alpha, \beta)$ (Algoritmo de Euclides). Encontrar $x, y \in D$ tais que $\alpha x + \beta y = \delta$.

   (a) $D = \mathbb{Z}[i]$, $\alpha = 14 - 3i$ e $\beta = 4 + 5i$;
   (b) $D = \mathbb{Z}[i]$, $\alpha = 4 + 3i$ e $\beta = -2 + 11i$;
   (c) $D = \mathbb{Z}[\omega]$, $\alpha = 23 + 6\omega$ e $\beta = 2 + 3\omega$.

5. Seja $\mathbb{K}$ um corpo e $\mathbb{K}[X]$ o anel de polinômios sobre $\mathbb{K}$. Mostre os seguintes resultados:

   (i) Dados $\alpha \in \mathbb{K}$ e $f \in \mathbb{K}[x]$, então $f(\alpha) = 0 \Leftrightarrow (x - \alpha) \mid f$ em $\mathbb{K}[x]$, isto é, $f = (x - \alpha).q$, com $q \in \mathbb{K}[x]$.
   (ii) Um polinômio de grau n, $f \in \mathbb{K}[x]$, admite, no máximo, n raízes em $\mathbb{K}$.
   (iii) Seja $\mathbb{K}$ um corpo infinito e $f \in \mathbb{K}[x]$ um polinômio tal que $f(a) = 0$ para todo $a \in \mathbb{K}$. Mostrar que $f = 0$ é o polinômio nulo. Dar exemplo, em um corpo finito, de um polinômio não nulo que satisfaz a propriedade requerida.

(i v) Se $\alpha \in \mathbb{K}$ é raiz de um polinômio $f \in \mathbb{K}[x]$, e se $(x-\alpha)^m \mid f$ e $(x-\alpha)^{m+1} \nmid f$, dizemos que α é uma raiz de f com multiplicidade m. Mostre que se α_1, ..., α_k são todas as raízes de f em $\mathbb{K}$, com respectivas multiplicidades m_1, ..., m_k. Então $f = (x-\alpha_1)^{m_1}...(x-\alpha_k)^{m_k} g$ em que $g \in \mathbb{K}[x]$ e $g(a) \neq 0$ para todo $a \in \mathbb{K}$.

6. Mostre que

   (a) $\mathbb{Z}$ não admite subanéis próprios.

   (b) Existem subanéis próprios de $\mathbb{Q}$ distintos de $\mathbb{Z}$. Todo subanel de $\mathbb{Q}$ contém $\mathbb{Z}$.

7. Seja $\alpha \in \mathbb{C}$, dizemos que α é algébrico se existir um polinômio com coeficientes racionais tal que $f(\alpha) = 0$. O polinômio mínimo de α é o polinômio mônico de menor grau tal que $f(\alpha) = 0$. Quando o polinômio mínimo tem coeficientes inteiros dizemos que o número é um inteiro algébrico. Encontrar, se existir, o polinômio mínimo de cada um dos números abaixo:
   (a) $\sqrt{2}$ (b) $\sqrt{3}$ (c) $\sqrt{2}+1$ (d) $\sqrt[3]{2}$ (e) $\frac{\sqrt{5}-1}{2}$ (f) π (g) $i-\sqrt{2}$

8. Defina o produto de dois ideais e compare com a interseção mostrando a relação entre os mesmos e um exemplo em que não coincidam.

9. Seja A um anel e $I, J \subset A$ dois ideais de A.

   (a) Mostre que $I \cap J$ é um ideal de A;

   (b) Mostre que se A é um DIP e $I = (a)$ e $J = (b)$. Então

   $$I \cap J = \{0\} \Leftrightarrow \text{mdc}(a,b) = 1.$$

10. Seja D um domínio. Imite a construção dos racionais a partir dos inteiros para construir o corpo de frações de D, um conjunto de classes de equivalências de pares de elementos em D:

    $$\mathbb{K} = \{\frac{\alpha}{\beta} \mid \alpha, \beta \in D, \beta \neq 0\}$$

    Com a relação $\frac{\alpha}{\beta} = \frac{\gamma}{\delta}$ se, e somente se, $\alpha\delta = \beta\gamma$. Defina a soma e o produto em $\mathbb{K}$ e mostre que $\mathbb{K}$ é um corpo que possui uma cópia de D como subanel.

3 Domínios de inteiros quadráticos

3.1 Corpos quadráticos e seus anéis de inteiros

Um corpo $\mathbb{K}$, de característica zero, ou seja, $\mathbb{Q} \subset \mathbb{K}$, é dito um corpo quadrático se $\dim_{\mathbb{Q}} \mathbb{K} = 2$. Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados. Todo corpo quadrático pode ser identificado com um corpo do tipo

$$\mathbb{K} = \mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}.$$

Em um corpo quadrático $\mathbb{Q}(\sqrt{d})$ vamos considerar o automorfismo de conjugação.

$$\overline{()} : \mathbb{K} \to \mathbb{K}$$

Dado $\alpha = x + y\sqrt{d} \in \mathbb{K}$, definimos $\overline{\alpha} = x - y\sqrt{d}$. Segue, naturalmente da definição, as seguintes propriedades da conjugação.

(i) $\alpha \in \mathbb{Q} \iff \overline{\alpha} = \alpha$;

(ii) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$,

(iii) $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.

Definimos a norma de $\alpha \in \mathbb{K}$ por $N(\alpha) = \alpha\overline{\alpha}$. Naturalmente a norma satisfaz $N(\alpha\beta) = N(\alpha)N(\beta)$.

O traço de $\alpha \in \mathbb{K}$ é definido por $T(\alpha) = \alpha + \overline{\alpha}$. Note que $N(\alpha), T(\alpha) \in \mathbb{Q}$.

Definição 3.1 *Seja $\alpha \in \mathbb{Q}(\sqrt{d})$, dizemos que α é um inteiro quadrático de $\mathbb{Q}(\sqrt{d})$ se existirem inteiros $a, b \in \mathbb{Z}$ tais que $\alpha^2 + a\alpha + b = 0$.*

Observação 3.1 *Note nessa definição que todo inteiro $a \in \mathbb{Z}$ é um inteiro quadrático e que um racional $q \in \mathbb{Q}$ é inteiro quadrático em $\mathbb{K}$ se, e somente se, $q \in \mathbb{Z}$.*

Proposição 3.1 *Seja $\alpha \in \mathbb{Q}(\sqrt{d})$, então temos $\alpha^2 - T(\alpha)\alpha + N(\alpha) = 0$. Além disso, α é um inteiro quadrático se, e somente se, $N(\alpha), T(\alpha) \in \mathbb{Z}$.*

Demonstração: Qualquer que seja $\alpha \in \mathbb{K}$, temos $\overline{\alpha} = T(\alpha) - \alpha$ portanto $N(\alpha) = \alpha(T(\alpha) - \alpha)$ que resulta na expressão $\alpha^2 - T(\alpha)\alpha + N(\alpha) = 0$. Assim, se $T(\alpha), N(\alpha) \in \mathbb{Z}$, então α é um inteiro quadrático. Reciprocamente, se α é um inteiro quadrático então existem inteiros a, b tais que $\alpha^2 + a\alpha + b = 0$, é facil verificar que $T(\alpha) = -a$ e $N(\alpha) = b$. □

Observação 3.2 *É fácil verificar que todo elemento da forma $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ é um inteiro quadrático. Com efeito, $N(\alpha) = a^2 - db^2$ e $T(\alpha) = 2a$. Por outro lado, em alguns casos existem outros inteiros quadrátios em $\mathbb{K}$ como mostraremos no próximo exemplo.*

Exemplo 3.1 *Seja* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *e* $\alpha = \frac{1+\sqrt{5}}{2}$*, como* $T(\alpha) = 1$ *e* $N(\alpha) = -1$*, então* α *é um inteiro quadrático em* $\mathbb{K}$*.*

Definição 3.2 *Definimos o domínio de inteiros quadráticos de* $\mathbb{Q}(\sqrt{d})$ *por*

$$\mathcal{O}(\sqrt{d}) = \{\alpha \in \mathbb{Q}(\sqrt{d}) \mid \ \alpha \text{ é inteiro quadrático}\}.$$

Verifique que realmente $\mathcal{O}(\sqrt{d})$ é fechado para a adição, para o simétrico e para a multiplicação, sendo realmente um domínio. Como havíamos comentado anteriormente, temos as seguintes inclusões

$$\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{d}).$$

Em geral, anéis de inteiros de um corpo de números (não necessariamente quadráticos) são ditos integralmente fechados. Em particular, quando vale a igualdade $\mathcal{O}(\sqrt{d}) = \mathbb{Z}[\sqrt{d}]$, dizemos que $\mathbb{Z}[\sqrt{d}]$ é integralmente fechado (IF).

Observação 3.3 *Temos as seguintes implicações:*

$$DE \Rightarrow DIP \Rightarrow DFU \Rightarrow IF.$$

Nenhuma das recíprocas é verdadeira em geral.

Exemplo 3.2 $\mathcal{O}(\sqrt{5}) = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \subset \mathbb{Q}(\sqrt{5})$*. De fato, a inclusão* $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] \subset \mathcal{O}(\sqrt{5})$ *segue diretamente do fato que* $\frac{1+\sqrt{5}}{2} \in \mathcal{O}(\sqrt{5})$*. Para mostrar a inclusão reversa, seja* $\alpha = p + q\sqrt{5} \in \mathcal{O}(\sqrt{5})$ *com* $p, q \in \mathbb{Q}$*. Pela Proposição 3.1,* $T(\alpha) = 2p \in \mathbb{Z}$ *e* $N(\alpha) = p^2 - 5q^2 \in \mathbb{Z}$*, logo* $p = \frac{a}{2}$ *com* $a \in \mathbb{Z}$ *e portanto* $2q \in \mathbb{Z}$ *que nos dá* $q = \frac{b}{2}$ *com* $b \in \mathbb{Z}$ *e o resultado segue.*

Note, em particular, que $\mathbb{Z}[\sqrt{5}]$ *não é um domínio de fatoração única. De fato, nós já sabíamos disso.*

$$2.2 = 4 = (\sqrt{5} - 1)(\sqrt{5} + 1).$$

O elemento 2 *é irredutível em* $\mathbb{Z}[\sqrt{5}]$ *mas não é primo.*

Em geral temos o seguinte lema.

Lema 3.1 *Se* $\alpha = p + q\sqrt{d} \in \mathcal{O}(\sqrt{d})$*, com* $p, q \in \mathbb{Q}$ *e* d *livre de quadrados, então* $2p, 2q \in \mathbb{Z}$*.*

Demonstração: De fato, pela Proposição 3.1, temos $T(\alpha) = 2p \in \mathbb{Z}$ e $N(\alpha) = p^2 - dq^2 \in \mathbb{Z}$. Assim, temos $4N(\alpha) = (2p)^2 - d(2q)^2 \in \mathbb{Z}$ que implica $d(2q)^2 \in \mathbb{Z}$. Suponha, por absurdo, que $2q \notin \mathbb{Z}$, então $2q = m/n$ com $m, n \in \mathbb{Z}$ coprimos. Temos, portanto $d(2q)^2 = d(\frac{m}{n})^2 = d\frac{m^2}{n^2} \in \mathbb{Z}$. Como m, n são coprimos, $n^2 \mid d$ que é um absurdo uma vez que d é livre de quadrados. □

Estamos agora em condições de enunciar o teorema principal da seção.

Teorema 3.1 *Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados. Então:*

(i) *Se $d \equiv 2, 3 \pmod 4$, então $\mathcal{O}(\sqrt{d}) = \mathbb{Z}[\sqrt{d}]$;*

(ii) *Se $d \equiv 1 \pmod 4$, então $\mathcal{O}(\sqrt{d}) = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.*

Demonstração:

(i) Como já observamos, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}(\sqrt{d})$. Seja agora $\alpha = a + b\sqrt{d} \in \mathcal{O}(\sqrt{d})$ e suponha que $a \notin \mathbb{Z}$. Pelo Lema 3.1, $2a \in \mathbb{Z}$ é ímpar. Ainda pelo Lema 3.1, $N(\alpha) \in \mathbb{Z}$ que implica $4N(\alpha) = (2a)^2 - d(2b)^2$ é múltiplo de 4, daí $d(2b)^2 \equiv 1 \pmod 4$ que implica $2b$ ímpar e portanto $d \equiv 1 \pmod 4$ que não é o caso. Resta provar que b é inteiro (verifique).

(ii) Primeiramente vamos mostrar que $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subset \mathcal{O}(\sqrt{d})$. De fato, se $\alpha \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, então $\alpha = a + b\frac{1+\sqrt{d}}{2} = \frac{2a+b+b\sqrt{d}}{2} = \frac{p+q\sqrt{d}}{2}$ com $p, q \in \mathbb{Z}$ e $p \equiv q \pmod 2$.

Seja agora $\alpha = a + b\sqrt{d} \in \mathcal{O}(\sqrt{d})$ e suponha que $a \notin \mathbb{Z}$. Pelo Lema 3.1, $2a, 2b \in \mathbb{Z}$. Assim $\alpha = \frac{p+q\sqrt{d}}{2}$, nesse caso, p, q seriam ímpares e $N(\alpha) \in \mathbb{Z}$ logo $\alpha \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Reciprocamente, se $\alpha = a + b\sqrt{d} \in \mathcal{O}(\sqrt{d})$ e $a \notin \mathbb{Z}$, pelo Lema 3.1, $2a \in \mathbb{Z}$ é ímpar e $N(\alpha) \in \mathbb{Z}$ que implica $4N(\alpha) = (2a)^2 - d(2b)^2$ é múltiplo de 4, daí $d(2b)^2 \equiv 1 \pmod 4$ que implica $2b$ ímpar. Escrevendo $2a = 2p + 1$ e $2b = 2q + 1$ com $p, q \in \mathbb{Z}$, obtemos $a + b\sqrt{d} = p + q\sqrt{d} + \frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ e o resultado segue.

□

3.2 Domínios Quadráticos Euclidianos

Inicialmente considere o seguinte Lema.

Lema 3.2 *Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados. Suponha que o domínio de inteiros quadráticos $\mathcal{O}(\sqrt{d})$ satisfaz a seguinte condição: dado $\gamma \in \mathbb{Q}(\sqrt{d})$ existe $\delta \in \mathcal{O}(\sqrt{d})$ tal que $\mid N(\gamma - \delta) \mid < 1$. Então $\mathcal{O}(\sqrt{d})$ é um domínio euclidiano com respeito a $\varphi = \mid N() \mid$.*

Demonstração: Suponha que $\mathcal{O}(\sqrt{d})$ goza da propriedade supracitada, então vamos mostra que é um domínio euclidiano. Com efeito, Sejam $\alpha, \beta \in \mathcal{O}(\sqrt{d})$ com $\beta \neq 0$. Em $\mathbb{Q}(\sqrt{d})$, temos $\gamma = \alpha\beta^{-1}$ logo existe $\delta \in \mathcal{O}(\sqrt{d})$ tal que $N(\alpha\beta^{-1} - \delta) < 1$. Vamos tomar δ como quociente e definir $\rho = \alpha - \beta\delta \in \mathcal{O}(\sqrt{d})$ como resto. Claramente, $\alpha = \beta\delta + \rho$ e $N(\rho) = N(\alpha - \beta\delta) = N(\beta)N(\alpha\beta^{-1} - \delta) < N(\beta)$. □

Agora estamos em condições de demonstrar o seguinte teorema, que caracteriza os valores negativos de d para os quais $\mathcal{O}(\sqrt{d})$ é DE e encontra vários valores positivos cumprindo tal condição. Esses valores positivos não são todos.

Teorema 3.2 *Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados. O domínio de inteiros quadráticos $\mathcal{O}(\sqrt{d})$ é um domínio euclidiano com respeito à norma para*

$$d \in \{-11, , -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13\}.$$

Demonstração: Nossa demonstração não funciona para $d = 6, 7, 11$. Deixamos ao leitor a verificação desses casos especiais. A demonstração se faz separadamente, em casos. Vamos considerar o primeiro caso, suponha $d \not\equiv 1 \pmod 4$, nesse caso, $d \in \{-1, -2, 2, 3\}$ e $\mathcal{O}(\sqrt{d}) = \mathbb{Z}[\sqrt{d}]$. Dado $\gamma = x+y\sqrt{d}$ com $x, y, \in \mathbb{Q}$, existem $r, s \in \mathbb{Z}$ tais que $\mid x-r \mid \leq 1/2$ e $\mid y - s \mid \leq 1/2$. Seja $\delta = r + s\sqrt{d}$, então

$$\mid N(\gamma - \delta) \mid \leq (x - r)^2 + \mid d \mid (y - s)^2 \leq \frac{1 + \mid d \mid}{4} < 1.$$

No segundo caso, suponha $d \leq 13$ e $d \equiv 1 \pmod 4$, nesse caso, $d \in \{-3, -7, -11, 5, 13\}$ e $\mathcal{O}(\sqrt{d}) = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Seja $\gamma = x + y\sqrt{d}$ com $x, y, \in \mathbb{Q}$, existem $r, s \in \mathbb{Z}$ tais que $\mid 2x - r \mid \leq 1/2$ e $\mid 2y - s \mid \leq 1/2$. Defina $\delta = \frac{r}{2} + \frac{s}{2}\sqrt{d} \in \mathcal{O}(\sqrt{d})$. Temos assim

$$\mid N(\gamma - \delta) \mid \leq (x - r/2)^2 + \mid d \mid (y - s/2)^2 \leq \frac{1 + \mid d \mid}{16} < 1.$$

□

Além disso temos o seguinte resultado cuja demonstração foge aos interesses desse curso.

Teorema 3.3 *Seja $d < 0$ um inteiro livre de quadrados, então $\mathcal{O}(\sqrt{d})$ é domínio euclidiano se, e somente se:*

$$d \in \{-1, -2, -3, -7, -11\}.$$

Demonstração: Ver [STEWART].

Existem domínios quadráticos euclidianos com respeito a outras funções e existem domínios quadráticos que são de fatoração única sem ser euclidianos.

Os dois seguintes teoremas fogem aos objetivos do curso, os deixo enunciados por completude. As demonstrações de tais resultados podem ser encontrados em [STEWART].

Teorema 3.4 *Seja $\mathcal{O}(\sqrt{d})$ um domínio de inteiros quadrático. Então $\mathcal{O}(\sqrt{d})$ é um DFU se, e somente se, $\mathcal{O}(\sqrt{d})$ é um DIP.*

Teorema 3.5 *Seja $d < 0$ um inteiro livre de quadrados. Então o anel de inteiros quadráticos $\mathcal{O}(\sqrt{d})$ é um DFU se, e somente se:*

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

3.3 Elementos inversíveis e equações de Pell-Fermat

Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados. Um elemento $u \in \mathcal{O}(\sqrt{d})$ é inversível se existir $u^{-1} \in \mathcal{O}(\sqrt{d})$ tal que $uu^{-1} = 1$.

Lema 3.3 *$u \in \mathcal{O}(\sqrt{d})$ é inversível se, e somente se, $\mid N(u) \mid = 1$.*

Demonstração: Se $N(u) = \pm 1$, então $u(\pm\overline{u}) = 1$, logo u é inversível. Reciprocamente, se u é inversível, então existe v tal que $uv = 1$, tomando normas, temos $N(u)N(v) = 1$ e o resultado segue uma vez que $N(u), N(v) \in \mathbb{Z}$. □

Teorema 3.6 *Seja $d < 0$ um inteiro livre de quadrados. Então*

1. $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$;
2. $\mathbb{Z}[\omega]^* = \{\pm 1, \pm\omega, \pm\omega^2\}$;
3. $\mathcal{O}(\sqrt{d})^* = \{\pm 1\}$ *se* $d \neq -1, -3$

Demonstração: Os casos 1 e 2 são clássicos, note que $\mathbb{Z}[i] = \mathcal{O}(\sqrt{-1})$ e $\mathbb{Z}[\omega] = \mathcal{O}(\sqrt{-3})$. Deixamos a verificação desse caso ao cargo do leitor. A demonstração do caso 3 deve ser separada em duas partes, vamos considerar apenas o caso em que $d \not\equiv 1 \pmod 4$. Nesse caso, considerando $c = -d > 0$ obtemos $x^2 + cy^2 = 1$ cuja única solução interira é a trivial $x = \pm 1$.

□

Observação 3.4 No caso em que $d > 0$ e $d \not\equiv 1 \pmod 4$ a condição $N(z) = \pm 1$ é equivalente à equação Diofantina de Pell-Fermat $x^2 - dy^2 = \pm 1$.

Exemplo 3.3 Considere a equação

$$x^2 - 2y^2 = 1$$

uma solução não trivial é $(3, 2)$ que corresponde ao elemento inversível $\alpha = 3 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ que é maior que 1 e minimal. Suas potências são: $\alpha^2 = 17 + 12\sqrt{2}$, $\alpha^3 = 99 + 70\sqrt{2}$, $\alpha^4 = 577 + 408\sqrt{2}$, ...
que dão origem às seguintes soluções da equação de Pell-Fermat: $(17, 12)$, $(99, 70)$, $(577, 408)$, ...
Note que que $(x - y\sqrt{2})(x + y\sqrt{2}) = 1$ nos fornece

$$\frac{x}{y} - \sqrt{2} = \frac{1}{y(x + y\sqrt{2})} < \frac{1}{y^2}.$$

Assims sendo, quando $x, y, \to \infty$, o racional $\frac{x}{y}$ vai ser uma boa aproximação de $\sqrt{2}$. Esse fato foi usado em antigos textos sagrados do Hinduismo para aproximar $\sqrt{2}$ a fim de construir templos. Surpreendentemente, a aproximação utilizada era

$$\sqrt{2} \approx \frac{577}{408} = 1.41421568627\ldots$$

Em notação decimal encontramos 5 casas decimais corretas nessa aproximação.

Teorema 3.7 (Dirichlet) *Seja $\alpha \in \mathbb{R}$ um número irracional. Então existem infinitos inteiros x, y, $y > 0$ tais que $\frac{x}{y}$ é uma fração irredutível e*

$$\left| \frac{x}{y} - \alpha \right| < \frac{1}{y^2}.$$

Uma demonstração simples do teorema de Dirichlet está sugerida nos problemas. No caso quadrático mostraremos que o teorema de Dirichlet é equivalente ao teorema de Euler sobre as soluções das equações de Pell-Fermat.

Proposição 3.2 *Seja $d > 0$ um inteiro que não é quadrado. Então são equivalentes:*

(i) *Existem infinitos inteiros positivos x, y tais que $x^2 - dy^2 = 1$;*

(ii) *Existem infinitos inteiros positivos x, y tais que $\mid \frac{x}{y} - \sqrt{d} \mid < \frac{1}{y^2}$;*

(iii) *Existe $m > 0$ para o qual existem infinitos inteiros positivos x, y satisfazendo $x^2 - dy^2 = m$*

Demonstração: A primeira implicação, $(i) \Rightarrow (ii)$ é clara pois, para cada solução em inteiros positivos de $x^2 - dy^2 = 1$ obtemos:

$$\mid \frac{x}{y} - \sqrt{d} \mid = \frac{1}{y(x + \sqrt{d}y)} < \frac{1}{y^2}.$$

Assim, o resultado segue.
A segunda implicação, $(ii) \Rightarrow (iii)$ será demonstrada por redução ao absurdo. Suponhamos, por absurdo, que não exista natural m tal que $x^2 - dy^2 = m$ possua uma infinidade de soluções em inteiros positivos. Para nós é suficiente considerar x, y para os quais $\mid \frac{x}{y} - \sqrt{d} \mid y^2 < 1$ que implica $\frac{x}{y} < 2\sqrt{d} + 1$ (por hipótese há uma infinidade de tais x, y). Observe que existe, apenas uma quantidade finita de naturais n para os quais $\mid \frac{x}{y} - \sqrt{d} \mid = \frac{n}{y(x+\sqrt{d}y)} < \frac{1}{y^2}$. De fato, nesse caso $n < \frac{x+y\sqrt{d}}{y} = \frac{x}{y} + \sqrt{d} < 1 + 3\sqrt{d}$. Supondo a existência de um número finito de soluções em inteiros positivos de $x^2 - dy^2 = n$ para cada n, como há somente um número finito de valores de n que nos interessam, chegamos em uma contradição.
Vamos mostrar agora a terceira implicação, isto é, $(iii) \Rightarrow (i)$. Dado que existem infinitos $x, y \in \mathbb{Z}$ tais que $x^2 - dy^2 = m$, existe uma infinidade deles satisfazendo $x \equiv x' \pmod{m}$ e $y \equiv y' \pmod{m}$. Sejam $\alpha = x + y\sqrt{d}$ e $\alpha' = x' + y'\sqrt{d}$, como ambos possuem a mesma norma $N(\alpha) = N(\alpha') = m$, então $\alpha/\alpha' \in \mathbb{Q}(\sqrt{d})$ tem norma unitária. Falta mostrar que $\alpha/\alpha' \in \mathbb{Z}(\sqrt{d})$, de fato,

$$\frac{\alpha}{\alpha'} = \frac{x + y\sqrt{d}}{x' + y'\sqrt{d}} = \frac{(x + y\sqrt{d})(x' - y'\sqrt{d})}{N(\alpha')} = \frac{(xx' - dyy') + (x'y - xy')\sqrt{d}}{m}.$$

Por hipótese $x \equiv x' \pmod{m}$ e $y \equiv y' \pmod{m}$, portanto $xx' - dyy' \equiv x^2 - dy^2 \equiv 0 \pmod{m}$ e $x'y - xy' \equiv xy - xy = 0 \pmod{m}$ logo $m \mid xx' - dyy'$ e $m \mid x'y - xy'$ e o resultado segue.

□

Teorema 3.8 *Seja $d \in \mathbb{Z}$ um inteiro positivo livre de quadrados e considere a equação Diofantina $x^2 - dy^2 = 1$. Existe uma única solução minimal $(a, b) \in \mathbb{Z}_+^2$ derivada da unidade fundamental minimal $u_0 = a + b\sqrt{d} \in \mathcal{O}(\sqrt{d})$, $\alpha_0 > 1$. Então toda solução positiva da equação de Pell-Fermat é da forma $u_n = u_0^n$ com $n \in \mathbb{Z}$.*

Observação 3.5 *A equação generalizada de Pell-Fermat $x^2 - dy^2 = m$ ou não possui solução em inteiros ou caso exista uma solução em inteiros positivos $(x_0, y_0) \in \mathbb{Z}_+^2$, então haverá infinitas. Além disso, existe um conjunto finito de soluções minimais não associadas $\alpha_i \in \mathcal{O}(\sqrt{d})$, com $i = \{1, \ldots, s\}$, então todas as outras soluções são associadas a $\alpha_{n,i} = \alpha_i u_0^n$. Para maiores detalhes, ver [NAGELL].*

Exemplo 3.4 A equação $x^2 - 2y^2 = 119$ possui como soluções minimais os pontos determinados pelos inteiros de $\mathbb{Z}[\sqrt{2}]$, não associadas $\alpha_1 = 11 + \sqrt{2}$ e $\alpha_2 = 13 + 5\sqrt{2}$.

3.4 Elementos primos e elementos irredutíveis

Lembramos que, em geral, todo elemento primo é irredutível, mas a recíproca só é válida em DFU.

Proposição 3.3 *Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados.*

1. *Se $\alpha \in \mathcal{O}(\sqrt{d})$ possui como norma $p = N(\alpha) \in \mathbb{Z}$ um número primo, então α é um elemento irredutível.*
2. *Seja $p \in \mathbb{Z}$ um primo.*
   (a) *Se existe $\alpha \in \mathcal{O}(\sqrt{d})$ tal que $N(\alpha) = p$, então $p = \alpha\overline{\alpha}$ é uma fatoração em irredutíveis de $p \in \mathcal{O}(\sqrt{d})$.*
   (b) *Caso contrário, p é irredutível em $\mathcal{O}(\sqrt{d})$.*

Demonstração:

1. Caso α não fosse irredutível em $\mathcal{O}(\sqrt{d})$, deveriam existir $\alpha_1, \alpha_2 \in \mathcal{O}(\sqrt{d})$ com norma $N(\alpha_i) > 1$ tais que $\alpha = \alpha_1\alpha_2$. Tomando normas, obtemos $N(\alpha) = N(\alpha_1)N(\alpha_2) = p$ que é um absurdo.
2. (a) Como $N(\alpha) = p$ o resultado segue pelo item anterior.
   (b) Trivial.

□

Vimos assim, que para entender os elementos inversíveis em um domínio de inteiros quadráticos temos que encontrar os elementos cuja norma é um primo inteiro. O próximo resultado, conhecido como Lema de Thue será bastante útil para esse fim.

Proposição 3.4 (Lema de Thue) *Sejam $a, b, n \in \mathbb{Z}$ com $n > 1$. Se $\text{mdc}(a, n) = 1$, então existem inteiros x, y com $0 <| x |, | y |< \sqrt{n}$ tais que*

$$x \equiv ay \pmod{n}.$$

Demonstração: Seja $r = \lfloor \sqrt{n} \rfloor$, então r é o único inteiro tal que

$$r \leq n < (r+1)^2$$

Assim sendo, o número de pares (x, y) tais que $0 \leq x, y \leq r$ é $(r+1)^2$ que, como vimos, é maior que n. Pelo princípio das gavetas de Dirichlet, existem dois pares (x_1, y_1) e (x_2, y_2) tais que

$$x_1 - ay_1 \equiv x_2 - ay_2 \pmod{n}$$

Isso se dá uma vez que a é inversível $\pmod{n}$. Logo

$$x_1 - x_2 \equiv a(y_1 - y_2) \pmod{n}$$

Sejam agora $x = x_1 - x_2$ e $y = y_1 - y_2$, então $x \equiv ay \pmod{n}$. Nos resta mostrar que $0 <\mid x \mid, \mid y \mid< \sqrt{n}$. Vamos mostrar que $x, y \neq 0$ pois sabemos que $0 \leq \mid x \mid, \mid y \mid< r$. Com efeito, se um dentre x, y for nulo, então o outro também será, desse caso, os dois pontos seriam o mesmo, que não é o caso. □

Teorema 3.9 (Fermat-Euler) *Se $p \in \mathbb{Z}_+$ é tal que $p \equiv 1 \pmod{4}$, então existem $a, b \in \mathbb{Z}$ tais que $a^2 + b^2 = p$.*

Demonstração: Sabemos que para tais primos existe $v \in \mathbb{Z}$ tal que $v^2 \equiv -1 \pmod{p}$ (ver Apêndice I). Considere agora a congruência

$$x \equiv vy \pmod{p}$$

Pelo Lema de Thue, Proposição 3.4, existem $x, y \in \mathbb{Z}$ com $0 <\mid x \mid, \mid y \mid< \sqrt{p}$ satisfazendo tal congruência. Note que $0 < x^2 + y^2 < 2p$ e $x^2 + y^2 \equiv 0 \pmod{p}$, portanto $x^2 + y^2 = p$. □

Corolário 3.1 *Os elementos primos de $\mathbb{Z}[i]$ são, a menos de associados:*

(i) $1 + i$;

(ii) $p \in \mathbb{Z}$ *primo tal que* $p \equiv 3 \pmod{4}$;

(iii) $a + bi$ *com* $a^2 + b^2 = p$ *primo* $p \equiv 1 \pmod{4}$.

Demonstração: Primeiramente, é facil ver que os elementos da forma (i) e (iii), quando existem, são primos, pela Proposição 3.3. Com relação aos elementos da forma (ii), devemos mostrar que dado p um primo ímpar $p \equiv 3 \pmod{4}$, então não existem $a, b \in \mathbb{Z}$ tais que $a^2 + b^2 = p$ e isso é evidente uma vez que o quadrado de um inteiro só pode ser 0 ou 1 $\pmod{4}$.

Reciprocamente, seja $\alpha = a + bi \in \mathbb{Z}$ um primo. Suponhamos que $N(\alpha) \in \mathbb{Z}$ tenha ao menos dois fatores primos, digamos $p, q \in \mathbb{Z}$. Então α não é primo em $\mathbb{Z}[i]$. Com efeito, se p ou q for congruente a 1 $\pmod{4}$, então se fatora em $\mathbb{Z}[i]$ e um dos fatores divide α, caso contrário seu produto se fatora em $\mathbb{Z}[i]$. Assim, $N(\alpha) = p^n$ é uma potência de primo. Se $n \geq 3$ chegamos em uma contradição. Se $n = 1$, então, pela Proposição anterior, existem $x, y \in \mathbb{Z}$ tais que $N(x + yi) = p$ no caso em que $p \equiv 1 \pmod{4}$. Caso $n = 2$ devemos ter $p \equiv 3 \pmod{4}$ e o resultado segue.

□

Teorema 3.10 (Eisenstein) *Seja $p \in \mathbb{Z}_+$ um primo $p \neq 3$. a condição necessária e suficiente a fim de que existam $a, b \in \mathbb{Z}$ tais que*

$$a^2 - ab + b^2 = p$$

é que $p \equiv 1 \pmod 3$.

Demonstração: Multiplicando por 4 e completando quadrados, obtemos:

$$(2a - b)^2 + 3b^2 = 4p.$$

Fazendo congruência módulo 3 percebemos que p é um quadrado não nulo $\pmod 3$, assim, $p \equiv 1 \pmod 3$.
Reciprocamente, se $p \equiv 1 \pmod 3$, sabemos que existe $v \in \mathbb{Z}$ tal que $v^2 \equiv -3 \pmod p$ (ver Apêndice I). Pelo Lema de Thue, Proposição 3.4, existem $x, y \in \mathbb{Z}$ tais que

$$x \equiv yv \pmod p$$

com $0 <| x |, | y |< \sqrt{p}$. Note que $x^2 + 3y^2 \equiv 0 \pmod p$ e $x^2 + 3y^2 < 4p$. Verifique que $x^2 + 3y^2 \neq 2p, 3p$ portanto $x^2 + 3y^2 = p$. Multiplicando ambos os membros da equação por 4, o resultado segue fazendo $b = 2y$ e $a = x + y$. □

Corolário 3.2 *Os elementos primos de $\mathbb{Z}[\omega]$ são, a menos de associados:*

1. $1 - \omega$;
2. $p \in \mathbb{Z}$ *primo tal que* $p \equiv 2 \pmod 3$;
3. $a + b\omega$ *e* $a + b\omega^2$ *com* $a^2 - ab + b^2 = p$ *primo* $p \equiv 1 \pmod 3$.

3.5 Problemas

1. Encontre todas as soluções para a equação de Pell-Fermat $x^2 - dy^2 = 1$ nos casos em que $d = 3, 5, 6, 7, 8, 10$.
2. Mostre que se $d = c^2$, com $c \in \mathbb{Z}$, ou seja, d é um quadrado perfeito. Então a equação $x^2 - dy^2 = m$ possui, sempre um número finito de soluções. A solução trivial é $x = \pm c$ e $y = 0$. Encontre valores de d e de m para os quais a equação $x^2 - dy^2 = m$ possui soluções não triviais. Se $m = 1$ as únicas soluções são as triviais $(\pm 1, 0)$.
3. Mostre que as soluções inteiras positivas da equação $x^2 - 2y^2 = 1$ satisfazem a seguinte relação de recorrência: $(x_1, y_1) = (3, 2)$ e $x_{n+1} = 3x_n + 4y_n$, $y_{n+1} = 2x_n + 3y_n$.
4. Mostre que existem valores de d, não quadrados, para os quais a equação

   $$x^2 - dy^2 = -1$$

   possui solução e outros valores para os quais a mesma não admite solução.

5. Mostre que se (x_1, y_1) é a menor solução em inteiros positivos da equação $x^2 - dy^2 = -1$, então (x_2, y_2) definidos por $(x_2 + \sqrt{d}y_2) = (x_1 + \sqrt{d}y_1)^2$ é a menor solução em inteiros positivos de $x^2 - dy^2 = 1$.

6. Resolver nos inteiros a equação $x^2 - 5y^2 = 5$.

7. Resolver nos inteiros a equação $x^2 - 13y^2 = 3$.

8. Resolver nos inteiros a equação $x^2 - 3y^2 = -3$.

9. Prove o teorema de Dirichlet, 3.7.
   Seja $\alpha \in \mathbb{R}$ um número irracional. Então existem infinitos inteiros x, y, $y > 0$ tais que $\frac{x}{y}$ é uma fração irredutível e

$$| \frac{x}{y} - \alpha | < \frac{1}{y^2}.$$

   (a) Defina $\lfloor x \rfloor$, e $\{x\} = x - \lfloor x \rfloor$

   (b) Considere, para cada natural N os distintos (verifique que são distintos) elementos do intervalo [0,1]:

$$\{0\}, \{\alpha\}, \{2\alpha\}, ..., \{N\alpha\}$$

   (c) Divida o intervalo $[0, 1]$ em N partes iguais e conclua utilizando o princípio das gavetas de Dirichlet.

4 Aplicações em duas classes de equações Diofantinas

4.1 Equações do tipo $ab = c^n$

Estamos interessados em equações do tipo $ab = c^n$ como introduzidas no Lema 2.3. O caso mais comum de equações desse tipo pode ser reduzia a forma $x^2 - dy^2 = z^n$. Vamos considerar o caso em que $d \in \mathbb{Z}$ é livre de quadrados. Essa equação pode ser fatorada em $\mathcal{O}(\sqrt{d})$ em $N(\beta) = \alpha^n$ em que $\beta = x + y\sqrt{d}$. Supondo que $\mathcal{O}(\sqrt{d})$ seja um DFU, pelo Lema 2.3 temos $\beta = u\beta_1^n$ e $\overline{\beta} = \overline{u}\overline{\beta}_1^n$ com $N(u) = 1$ e $z = N(\beta_1)$. Note que o problema das ternas pitagóricas é exatamente $N(\beta) = z^2 \in \mathbb{Z}[i]$. Nosso próximo exemplo é uma variação de tal problema.

Exemplo 4.1 Encontre todos os triângulos com lados inteiros e coprimos, tendo um ângulo de 60^o. Equivalentemente, encontre todas as soluções em inteiros coprimos da equação

$$b^2 - bc + c^2 = a^2.$$

Solução:

Seja $\beta = b + c\omega \in \mathbb{Z}[\omega] = \mathcal{O}(-3)$. Nossa equação pode ser reescrita como $N(\beta) = a^2 \in \mathbb{Z}[\omega]$, e como $\mathbb{Z}[\omega]$ é um DFU, podemos usar o Lema 2.3. Vamos calcular $d = \text{mdc}(\beta, \overline{\beta}) \in \mathbb{Z}[\omega]$. Como $d \mid 2b$ e $d \mid 2c$, $d \mid 2$, como 2 não é norma de nenhum elemento em $\mathbb{Z}[\omega]$, pois a equação $x^2 - xy + y^2 = 2$ não possui solução inteira (verifique!), 2 é primo em $\mathbb{Z}[\omega]$. Portanto, se β e $\overline{\beta}$ não são coprimos em $\mathbb{Z}[\omega]$, então $2 \mid b + c\omega$ que implica $2 \mid b$ e $2 \mid c$ e portanto $2 \mid a$ que é um absurdo pois estamos supondo a, b, c coprimos. Logo $\text{mdc}(\beta, \overline{\beta}) = 1$ e portanto existem $u \in \mathbb{Z}[\omega]^*$ com $N(u) = 1$ e $\alpha \in \mathbb{Z}[\omega]$ tais que $\beta = u\alpha^2$. Escrevendo $\alpha = m + n\omega$, temos $\alpha^2 = (m^2 - n^2) + (2mn - n^2)\omega$. Obtemos assim uma família de soluções para $u = 1$, que é $b = m^2 - n^2$, $c = 2mn - n^2$ e $a = m^2 - mn + n^2$. Pode-se verificar que escolhendo outros inversíveis ainda estamos nessa classe de soluções.

Uma outra possível variação seria a seguinte equação Diofantina.

Exemplo 4.2 Encontrar todas as soluções em inteiros positivos da equação

$$x^2 + 1 = y^3.$$

Solução:

Seja $\alpha = x + i \in \mathbb{Z}[i]$, a equação pode ser reescrita como $N(\alpha) = y^3$. Seja $d = \text{mdc}(x + i, x - i) \in \mathbb{Z}[i]$, claramente $d \mid 2$ e $d \neq 2$ pois $2 \nmid x + i$. A fim de mostrar que α e $\overline{\alpha}$ são coprimos, como $2 = (1 + i)(1 - i)$ que são associados, resta mostrar que $d \neq 1 + i$. Suponha, por absurdo que $d = 1 + i$, então tomando norma, como $1 + i \mid x + i$ deveríamos ter $N(1 + i) \mid N(x + i)$ ou seja, $2 \mid x^2 + 1$ implicando $x = 2k + 1$ ímpar e $y = 2s$ par. Substituindo na equação original encontramos $4k^2 + 4k + 2 = 8s^3$ que é um absurdo (basta dividir por 2).

Agora que sabemos que $\text{mdc}(x+i, x-i) = 1$, podemos concluir que $x+i = (a+bi)^3$ (note que todos os elementos inversíveis em $\mathbb{Z}[i]$ são cubos perfeitos), logo $x = a^3 - 3ab^3$ e $1 = 3a^2b - b^3$, donde tiramos $b = \pm 1$. Caso $b = 1$ temos um absurdo, logo $b = -1$ que implica $a = 0$. Isso nos fornece $x = 0$ e $y = 1$ como única solução.

4.2 Equações do tipo $ab = cd$

Um dos casos mais recorrentes desse tipo de equação em domínios quadráticos pode ser reduzido à uma equação do tipo $N(\alpha) = N(\beta) \in \mathcal{O}(\sqrt{d})$. Supondo que $\mathcal{O}(\sqrt{d})$ seja um DFU, podemos usar o Lema 2.2. Nossa equação ficou $\alpha\overline{\alpha} = \beta\overline{\beta}$, assim, $\alpha = xy$, $\overline{\alpha} = ts$, $\beta = xt$, $\overline{\beta} = ys$ com $\text{mdc}(y,t) = 1$. Podemos escrever $\frac{\alpha}{\beta} = \frac{y}{t}$ e $\frac{\overline{\alpha}}{\overline{\beta}} = \frac{t}{y} = \frac{\overline{y}}{\overline{t}}$, e como $\text{mdc}(y,t) = 1$, temos $t = \overline{y}$ (desde que $\alpha \neq \beta$) que nos dá $s = \overline{x}$. Assim, $\alpha = xy$ e $\beta = x\overline{y}$ e portanto $\overline{\alpha} = \overline{xy}$ e $\overline{\beta} = \overline{x}y$.

Exemplo 4.3 (IMO-01) Sejam $a > b > c > d$ inteiros positivos e suponha que

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove que $ab + cd$ não é primo.

Solução:

Podemos reescrever a condição do enunciado da forma

$$a^2 - ac + c^2 = b^2 + bd + d^2.$$

Seja $\mathbb{Z}[\omega] = \mathcal{O}(-3)$ o domínio dos inteiros de Eisenstein, que sabemos ser um DE (portanto DFU). As normas de $\alpha = a + c\omega$ e $\beta = b - d\omega$ são $N(\alpha) = a^2 - ac + c^2$ e $N(\beta) = b^2 + bd + d^2$. Assim, a equação pode ser reduzida à

$$N(\alpha) = N(\beta) \in \mathcal{O}(-3).$$

O primeiro caso a considerar seria $\alpha = \beta$ que é um absurdo pelas condições do problema. Pelo Lema 2.2 e pelas discussões acima, existem $x, y \in \mathcal{O}(-3)$ tais que

$$a + c\omega = xy,\ a + c\overline{\omega} = \overline{xy},\ b - d\omega = x\overline{y},\ b - d\overline{\omega} = \overline{x}y.$$

Isolando a, b, c, d, obtemos

$$a = \frac{\overline{xy}\omega - xy\overline{\omega}}{\sqrt{3}i},\ b = \frac{\overline{x}y\omega - x\overline{y}\overline{\omega}}{\sqrt{3}i},\ c = \frac{xy - \overline{xy}}{\sqrt{3}i},\ d = \frac{\overline{x}y - x\overline{y}}{\sqrt{3}i}.$$

Calculando agora $ab + cd$, obtemos

$$ab + cd = -\frac{1}{3}[(\overline{xy}\omega - xy\overline{\omega})(\overline{x}y\omega - x\overline{y}\overline{\omega}) + (xy - \overline{xy})(\overline{x}y - x\overline{y})].$$

Simplificando, obtemos

$$ab + cd = N(y)v, \text{ escrevendo } x^2\overline{\omega}^2 = \frac{u + v\omega}{2} \in \mathcal{O}(-3).$$

Falta mostrar que $N(y) > 1$ e $v > 1$ e o resultado segue. Deixamos essa verificação para o leitor.

4.3 Problemas

1. Resolver nos inteiros $y^3 = x^2 + 1$.
2. (a) Mostre que para cada inteiro n o número de soluções da equação $x^2 - xy + y^2 = n$ é finito e divisível por 6.
   (b) Determine todas as soluções inteiras de $x^2 - xy + y^2 = n$.
3. Seja $p = 4m - 1$ um primo e sejam x, y inteiros coprimos tais que
$$x^2 + y^2 = z^{2m}$$
4. Resolver nos inteiros $13^x + 3 = y^2$.
5. Resolver nos inteiros $x^2 + 8 = y^3$.
6. Resolver nos inteiros a equação $x^2 + 11 = 3^n$ quando n é um inteiro maior que 1.
7. Resolver nos inteiros $x^2 + x + 2 = y^3$.
8. Resolver nos inteiros $x^2 + y^2 = z^5$ com x, y coprimos.
9. Mostre que a equação Diofantina $4y^2 = x^3 - 3$ não possui solução inteira.
10. Mostre que a equação Diofantina $x^3 + y^3 + z^3 = 0$ só possui solução trivial, isto é, tais que $xyz = 0$.
11. Resolver nos inteiros a equação $x^3 = y^2 - 2$.
12. Resolver nos inteiros a equação $x^3 + 6 = y^2$.
13. Resolver nos inteiros a equação $x^3 + 7 = y^2$.
14. Resolver nos inteiros a equação $x^3 + 11 = y^2$.
15. Resolver nos inteiros a equação $x^3 = y^2 + 2$.

5 Apêndice I: A lei da reciprocidade quadrática

Neste apêndice vamos recordar ideias contidas em [IRELAND].

5.1 O símbolo de Legendre

Seja $p \in \mathbb{Z}_+$ um primo ímpar, o símbolo de Legandre $\left(\frac{a}{p}\right) = 0$ se $a \equiv 0 \pmod{p}$, $\left(\frac{a}{p}\right) = 1$ se $a \not\equiv 0 \pmod{p}$ e existe $v \in \mathbb{Z}$ tal que $v^2 \equiv a \pmod{p}$ e $\left(\frac{a}{p}\right) = -1$ caso contrário. O caso $p = 2$ é trivial uma vez que toda classe é resíduo quadrático em $\mathbb{Z}_2$.

Primeiramente observamos que elevando cada $a \in \mathbb{Z}_p$ ao quadrado determinamos assim todos os resíduos quadráticos de $\mathbb{Z}_p$.

Exemplo 5.1 Os resíduos quadráticos de $\mathbb{Z}_7$ são $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Note que excetuando o zero obtivemos $6/2 = 3$ resíduos quadráticos. Isso não é uma coincidência, pois se $a, b \neq 0 \in \mathbb{Z}_p$ e $a^2 = b^2 \in \mathbb{Z}_p$, então $a = \pm b \in \mathbb{Z}_p$. Ou seja, quando $p > 2$ é um primmo ímpar, então metado dos resíduos não nulos são quadrados e a outra metade não o são.

Proposição 5.1 (Lema de Euler) *Sejam $a, p \in \mathbb{Z}$ com $p > 0$ um primo ímpar. Então:*

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

Demonstração: Claro que se $a \equiv 0 \pmod{p}$, o resultado é veradeiro. Vamos supor que $a \not\equiv 0 \pmod{p}$. Pelo pequeno Teorema de Fermat, temos $a^{p-1} \equiv 1 \pmod{p}$, daí

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} - 1) \equiv 0 \pmod{p}.$$

Considere agora o polinômio $f = x^{(p-1)/2} - 1 \in \mathbb{Z}_p[x]$ sabemos que se $a \equiv b^2 \pmod{p}$ é um resíduo quadrático, então $f(a) = b^{p-1} - 1 = 0 \in \mathbb{Z}_p$. O poliômio f tem grau $(p-1)/2$ e exatamente $(p-1)/2$ raízes em $\mathbb{Z}_p^*$ correspondendo aos resíduos quadráticos. Assim, se $\left(\frac{a}{p}\right) = 1$ o resultado vale. Por outro lado, o polinômio $g = x^{(p-1)/2} + 1 \in \mathbb{Z}_p[x]$ também deverá ter $(p-1)/2$ raízes em $\mathbb{Z}_p$ uma vez que

$$fg = x^{p-1} - 1 \in \mathbb{Z}_p.$$

Pelo pequeno Teorema de Fermat, fg possui $p-1$ raízes em $\mathbb{Z}_p$, portanto se $\left(\frac{a}{p}\right) = -1$, ou seja, a nã é um resíduo quadrático em $\mathbb{Z}_p$, então a deverá ser raíz de g e portanto $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. E o resultado segue.

□

Corolário 5.1 (O símbolo de Legendre de -1.) *Seja $p > 2$ um primo ímpar. Então*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Ou seja, -1 é um resíduo quadrático em $\mathbb{Z}_p$ se, e somente se, $p \equiv 1 \pmod 4$.

Demonstração: Verifique. □

Corolário 5.2 (Propriedades básicas do símbolo de Legendre) *Seja $p \in \mathbb{Z}$ um primo, então o símbolo de Legendre cumpre as seguintes condições:*

1. *Se $a \equiv b \pmod p$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*
3. *Se $\text{mdc}(a, p) = 1$, então $\left(\frac{a^2}{p}\right) = 1$ e $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.*

Demonstração: Verifique. □

5.2 Números algébricos e inteiros algébricos

Um número complexo $\alpha \in \mathbb{C}$ é dito um número algébrico se existir um polinômio não nulo $f \in \mathbb{Q}[x]$ tal que $f(\alpha) = 0$. Um número algébrico é dito um inteiro algébrico se existir um polinômio mônico $f \in \mathbb{Z}[x]$ tal que $f(\alpha) = 0$. Claramente todo inteiro algébrico é também um número algébrico, por definição. A recíproca obviamente não é verdadeira.

Proposição 5.2 *Seja $q \in \mathbb{Q}$ um número racional. O número q é um inteiro algébrico se, e somente se, $q \in \mathbb{Z}$ é um inteiro.*

Teorema 5.1 *O conjunto dos números algébricos, $\overline{Q} \subset \mathbb{C}$ é um corpo.*

Teorema 5.2 *O conjunto $\Omega \subset \mathbb{C}$ dos inteiros algébricos é um domínio.*

Proposição 5.3 *Seja $p \in \mathbb{Z}$ um primo e sejam $\alpha, \beta \in \Omega$. Então*

$$(\alpha + \beta)^p \equiv \alpha^p + \beta^p \pmod p \in \Omega.$$

5.3 O símbolo de Legandre de 2

Nessa seção vamos demonstrar que para todo primo ímpar $p \in \mathbb{Z}_+$ temos

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Para isso, seja $\zeta = cis(2\pi/8)$ uma raíz primitiva da unidade, é facil ver que $\zeta^2 = i$ e que $\zeta^2 = -i$, portanto:

$$\zeta^2 + \zeta^{-2} = 2.$$

Seja $\tau = \zeta + \zeta^{-1}$, sendo $p \in \mathbb{Z}$ um primo ímpar, sabemos que:

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

Ou seja:

$$\tau^p = \tau \left(\frac{2}{p}\right) \pmod{p}.$$

Pela Proposição 5.3, sabemos que

$$\tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \pmod{p}.$$

Dado que $\zeta^8 = 1$, sabemos que $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ quando $p \equiv \pm 1 \pmod 8$. Por outro lado, se $p \equiv \pm 3 \pmod 8$, temos $\zeta^3 = -\zeta^{-1}$ que nos fornece $\zeta^p + \zeta^{-p} = -(\zeta + \zeta^{-1})$ quando $p \equiv \pm 3 \pmod 8$. Assim, faz sentido considerar $\epsilon = \frac{p^2-1}{8}$. Daí,

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

Multiplicando por τ, obtemos:

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

Pensando como congruência em $\mathbb{Z}$, dado que p é um primo ímpar, obtemos:

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

5.4 Somas de Gauss e a Lei da reciprocidade quadrática

Vamos utilizar as somas (quadráticas) de Gauss a fim de demonstrar o princípio da Reciprocidade quadrática, o teorema preferido de Gasuss. Nessa seção $p \in \mathbb{Z}_+$ é um primo ímpar e $\zeta = e^{2\pi/p}$.

Lema 5.1

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p & se \quad a \equiv 0 \pmod{p} \\ 0 & se \quad a \not\equiv 0 \pmod{p} \end{cases}$$

Demonstração: Se $a \equiv o \pmod p$, então $\zeta^a = 1$ e o primeiro resultado segue pois é uma soma soma constante com p somandos. Caso contrário podemos usar a fórmula da soma da PG, isto é:

$$\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = 0.$$

□

Defina $\delta(x, y) = 1$ se $x \equiv y \pmod p$ e $\delta(x, y) = 0$ se $x \not\equiv o \pmod p$.

Corolário 5.3

$$\sum_{t=0}^{p-1} \zeta^{t(x-y)} = p\delta(x,y)$$

Demonstração: Imediato. □

Lema 5.2

$$\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0.$$

Demonstração: Excetuando $0 \in \mathbb{Z}_p$, existem tantos quadrados quanto não quadrados em $\mathbb{Z}_p$ e assim o símbolos de Legendre se cancelam. □

Definição 5.1 A soma (quadrática) de Gauss é definida por

$$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}.$$

Proposição 5.4 *Seja* $g = g_1$, *então* $g_a = \left(\frac{a}{p}\right) g$.

Demonstração: Primeiramente vamos considerar o caso em que $a \equiv 0 \pmod{p}$. Nesse caso, $\zeta^{at} = 1$ para todo t e $g_a = 0$ pelo Lema 5.2 e o resultado segue.

Suponhamos agora que $a \not\equiv 0 \pmod{p}$, então:

$$\left(\frac{a}{p}\right) g_a = \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \sum_{s=0}^{p-1} \left(\frac{s}{p}\right) \zeta^{s} = g.$$

Na igualdade delicada em que trocamos a variável do somatório de t para s, o fizemos pois a aplicação $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ dada por $f(t) = at$ é uma bijeção.

Lembrando que nesse caso $\left(\frac{a}{p}\right)^2 = 1$, o resultado segue. □

Proposição 5.5

$$g^2 = (-1)^{(p-1)/2} p =: p^*.$$

Demonstração: A estratégia para demonstrar esse resultado consiste em calcular de duas maneiras diferentes o seguinte somatório:

$$\sum_{a=1}^{p-1} g_a g_{-a}.$$

Por um lado, sabemos que para todo $a \not\equiv 0 \pmod{p}$, temos

$$g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2.$$

Portanto,

$$\sum_{a=1}^{p-1} g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1)g^2.$$

Por outro lado, podemos escrever $g_a = \sum_x \left(\frac{x}{p}\right)\zeta^{ax}$ e $g_{-a} = \sum_y \left(\frac{y}{p}\right)\zeta^{-ay}$ que nos dá:

$$\sum_{a=1}^{p-1} g_a g_{-a} = \sum_{x,y}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)} = \sum_{x,y}\left(\frac{xy}{p}\right)\delta(x,y)p = \sum_x \left(\frac{x}{p}\right)^2 p = (p-1)p.$$

Na segunda igualdade utilizamos o Corolário 5.3. □ Comparando as duas expressões e fazendo $p^* = (-1)^{(p-1)/2}$, obtemos:

$$g^2 = p^*.$$

Teorema 5.3 (Gauss - Lei da Reciprocidade quadrática) *Sejam $p, q \in \mathbb{Z}_+$ primos ímpares distintos, então:*

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

Demonstração: Vamos trabalhar com congruências $\pmod q$ no anel Ω, o anel dos inteiros algébricos. Seja g como nas proposições anteriores.

$$g^{q-1} = (g^2)^{(q-1)/2} = (p^*)^{(q-1)/2} \equiv \left(\frac{p^*}{q}\right) \pmod q.$$

Portanto, temos:

$$g^q \equiv \left(\frac{p^*}{q}\right) g \pmod q.$$

Pela Proposição 5.3, temos:

$$g^q = (\sum_{t=0}^{q-1}\left(\frac{t}{p}\right)\zeta^t)^q \equiv \sum_{t=0}^{q-1}\left(\frac{t}{q}\right)^q \zeta^{qt} \equiv \sum_{t=0}^{q-1}\left(\frac{t}{q}\right)\zeta^{qt} \equiv g_q \pmod q.$$

Aqui usamos o fato que $\left(\frac{t}{q}\right) = \pm 1$ e q é ímpar. Da congruência $g^q \equiv g_q \pmod q$, obtemos a igualdade $g^q = g_q$. Portanto:

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod q.$$

Podemos agora multiplicar por g e usar o fato que $g^2 = p^*$ para obter uma congruência em $\mathbb{Z}$:

$$\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \pmod q.$$

Cancelando p^* obtemos:

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod q.$$

E o resultado segue. □

5.5 Usando a lei da reprocidade quadrática

Para nossas aplicações será muio útil o seguinte resultado:

Proposição 5.6 *Sejam $a, p \in \mathbb{Z} \setminus 0$ com p um primo ímpar. Então são equivalentes as seguintes afirmações:*

(i) *Existem $x, y \in \mathbb{Z}$ coprimos tais que*

$$x^2 + ny^2 \equiv 0 \pmod{p}.$$

(ii) *O símbolo de Legendre* $\left(\frac{-n}{p}\right) = 1$.

Demonstração: Suponhamos, inicialmente, que $\left(\frac{-n}{p}\right) = 1$, então existe $v \in \mathbb{Z}_p$ tal que $v^2 \equiv -n \pmod{p}$. Tomando $x = v$ e $y = 1$ obtemos uma solução para a equação $x^2 + ny^2 \equiv 0 \pmod{p}$.

Reciprocamente, suponhamos que existam $x, y \in \mathbb{Z}$ coprimos tais que

$$x^2 + ny^2 \equiv 0 \pmod{p}.$$

Como $y \neq 0 \pmod{p}$ e $\mathbb{Z}_p$ é um corpo, temos

$$(xy^{-1}) \equiv -n \pmod{p}.$$

Assim, $\left(\frac{-n}{p}\right) = 1$ e o resultado segue. □

Essa Proposição está intimamente ligada ao problema de encontrar quais primos podem ser escritos da forma $x^2 + ny^2$, como veremos no próximo apêndice.

Proposição 5.7 *Seja $p \in \mathbb{Z}_+$ um inteiro ímpar. Então são equivalentes as asserções seguintes:*

(i) $p \equiv 1, 3 \pmod{8}$*;*

(ii) *O símbolo de Legendre* $\left(\frac{-2}{p}\right) = 1$*;*

(iii) *Existem $x, y \in \mathbb{Z}$ coprimos tais que*

$$x^2 + 2y^2 \equiv 0 \pmod{p}.$$

Demonstração: Os ítens (ii) e (iii) são equivalentes pela Proposição 5.6. Sabemos que os símbolos de Legendre $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ e $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. O resultado segue de uma verificação usual.

□

Um resultado que utilizamos para determinar os elementos primos nos inteiros de Eisenstein foi o seguinte:

Proposição 5.8 *Seja $p > 3$ um primo ímpar. Então são equivalentes:*

(i) $p \equiv 1 \pmod 3$*;*

(ii) $\left(\frac{-3}{p}\right) = 1$*;*

(iii) *Existem $x, y \in \mathbb{Z}$ coprimos tais que*

$$x^2 + 3y^2 \equiv 0 \pmod p.$$

Demonstração:

Primeiramente, suponhamos que $p \equiv 1 \pmod 3$: Vamos calcular o símbolo de Legendre $\left(\frac{-3}{p}\right)$. Para isso, note que $-3 = 3^*$, assim, pela Lei da reciprocidade quadrática:

$$\left(\frac{-3}{p}\right) = \left(\frac{3^*}{p}\right) = \left(\frac{p}{3}\right) = 1.$$

Suponhamos agora que $\left(\frac{-3}{p}\right) = 1$, então, pela Proposição 5.6, obtemos uma solução para a equação $x^2 + 3y^2 \equiv 0 \pmod p$.

Finalmente, suponhamos que existam $x, y \in \mathbb{Z}$ não nulos $\pmod p$ tais que

$$x^2 + 3y^2 \equiv 0 \pmod p.$$

Ainda pela Proposição 5.6, $\left(\frac{-3}{p}\right) = 1$ e portanto $p \equiv 1 \pmod 3$.

□

5.6 Problemas

1. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que $\left(\frac{-5}{p}\right) = 1$ se, e somente se,

$$p \equiv 1, 3, 7, 9 \pmod{20}.$$

2. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que $\left(\frac{-7}{p}\right) = 1$ se, e somente se,

$$p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}.$$

3. Sejam $n \in \mathbb{Z}_+$ e $p = 2^{2^n} + 1$ um primo. Mostre que 3 não é um quadrado módulo p.

4. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que existe $x \in \mathbb{Z}$ tal que $p \mid x^2 - x + 3$ se, e somente se, $p \mid y^2 - y + 25$.

5. (IMO) Sejam a, b inteiros positivos tais que $15a + 16b$ e $16a - 15b$ sejam quadrados perfeitos. Encontrar o menor valor que pode tomar o menor deles.

6. Seja p um primo. Mostre que o número de soluções de $ax^2 + bx + c \equiv 0 \pmod p$ é $1 + \frac{b^2 - 4ac}{p}$.

7. Sejam $a, p \in \mathbb{Z}$ com p primo. Mostre que se $p \nmid a$, então:

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p} \right) = -1.$$

Se $p \mid a$, então

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p} \right) = p - 1.$$

6 Apêndice II: Primos da forma $x^2 + ny^2$

Como vimos em seções anteriores, para determinar os primos em um domínio de inteiros quadráticos $\mathbb{Z}[\sqrt{n}]$ precisamos entender quais são os primos $p \in \mathbb{Z}_+$ que podem ser escritos da forma $p = x^2 + ny^2$. Esse é um problema que foi extensivamente estudado por Euler e resolvido parcialmente por Gauss e Lagrange em mais de 100 anos de pesquisa. A solução geral do problema agrega ferramentas que fogem completamente ao escopo dessas notas, veja [COX], mas nesse apêndice vamos sumarizar resutados importantes contidos no primeiro capítulo do livro supracitado.

6.1 Introdução histórica

O problema de determinar quais são os primos que podem ser escritos da forma $p = x^2+ny^2$ com $x, y \in \mathbb{Z}$ remonta a uma série de conjecturas de Fermat, que durante mais de 40 anos motivaram vários artigos de Euler em busca da lei da Reciprocidade quadrática, enfim demonstrada por Gauss. Inicialmente destacamos as segunites conjecturas de Fermat demonstradas por Euler.

Teorema 6.1 (Euler) *Seja $p \in \mathbb{Z}_+$ um primo. Então:*

1. *$p = x^2 + y^2$ com $x, y \in \mathbb{Z}$ se, e somente se, $p = 2$ ou $p \equiv 1 \pmod 4$;*
2. *$p = x^2 + 2y^2$ com $x, y \in \mathbb{Z}$ se, e somente se, $p = 2$ ou $p \equiv 1, 3 \pmod 8$;*
3. *$p = x^2 + 3y^2$ com $x, y \in \mathbb{Z}$ se, e somente se, $p = 3$ ou $p \equiv 1 \pmod 3$.*

A estratégia de Euler, inspirado em Fermat, consistia em dividir o problema em dois passos:

1. O passo da reciprocidade;
2. O passo da descida.

6.2 O passo da reciprocidade

O passo da reciprocidade corresponde à Proposição 5.6 juntamente à busca por uma coleção de congruências do tipo:

$$p \equiv \alpha_1, \ldots, \alpha_n \pmod{4n},$$

que implique $x^2 + ny^2 \equiv \pmod p$.

Observação 6.1 Infelizmente nem sempre isso é possível, mas vamos conseguir algo do tipo no caso em que n é relativamente pequeno e livre de quadrados. Euler estava em busca da lei da reciprocidade quadrática. Com as ferramentas modernas a primeira parte desse passo é uma consequência natural da Lei da Reciprocidade quadrática.

6.3 O passo da descida

O chamado passo da descida, está associado às ideias iniciais de Fermat, que chamamos descida infinita de Fermat, bem como outros resultados que nos fornecem cotas superiores para as soluções, como o Lema de Thue e o princípio de Mikowski ou ainda o estudo de formas quadráticas definidas em $\mathbb{Z}$.

A título de ilustração vamos atacar uma das conjecturas de Fermat utlizando o Lema de Thue como passo da descida.

Teorema 6.2 (Euler) *Seja $p \in \mathbb{Z}_+$um primo. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + 2y^2$ se, e somente se, $p = 2$ ou $p \equiv 1, 3 \pmod 8$.*

Demonstração: O caso $p = 2$ é trivial. Vamos supor que $p \geq 3$ seja um primo ímpar. Sabemos, pela Proposição 5.7, que $p \equiv 1, 3 \pmod 8$ se, e somente se, o símbolo de Legendre $\left(\frac{-2}{p}\right) = 1$. Seja $v \in \mathbb{Z}$ tal que $v^2 \equiv -2 \pmod p$. Considere agora a congruência $x \equiv vy \pmod p$ que sabemos, pelo Lema de Thue, Proposição 3.4, possui solução $x, y \in \mathbb{Z}$ satisfazendo $0 <\mid x \mid, \mid y \mid< \sqrt{p}$. Então, por um lado:

$$x^2 + 2y^2 \equiv v^2y^2 + 2y^2 \equiv 0 \pmod p.$$

Por outro lado, temos:

$$0 < x^2 + 2y^2 < (\sqrt{p})^2 + 2(\sqrt{p})^2 = 3p.$$

Há agora, dois casos a serem considerados:

1. No primero caso, temos $x^2 + 2y^2 = p$ e o resultado segue.
2. No segundo caso, temos $x^2 + 2y^2 = 2p$. Nesse caso, $x = 2k$ com $k \in \mathbb{Z}$ é par, logo $4k^2 + 2y^2 = 2p$ que implica $y^2 + 2k^2 = p$ e o resultado segue.

□

6.4 Formas quadrática sobre $\mathbb{Z}$

Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados $d = 1 + 4k$. A norma algébrica em $\mathcal{O}(\sqrt{d}) = \mathbb{Z}[\alpha]$, com $\alpha = \frac{1+\sqrt{d}}{2}$ se escreve como

$$N(x + y\alpha) = x^2 + 2xy + ky^2.$$

Assim, faz sentido considerar formas quadráticas mais gerais e entender quando um primo p pode ser ser escrito como $p = f(x, y)$ em que $f(x, y)$ é uma forma quadrática definida sobre os inteiros.

Definição 6.1 Uma forma quadrática sobre $\mathbb{Z}$ é um polinômio homogêneo de grau dois com coeficientes inteiros:

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

Uma tal forma é dita primitiva se $\text{mdc}(a, b, c) = 1$.

Nessas condições dizemos que a forma é positiva definida, negativa definida ou indefinida se a forma real associada assim o for. Dada uma forma quadrática f sobre $\mathbb{Z}$, dizemos que um inteiro é representado por f se existirem inteiros x, y tais que $f(x, y) = m$. Nessas condições, dizemos que m é propriamente representado se $\text{mdc}(x, y) = 1$.

Definição 6.2 Dizemos que duas formas f, g são equivalentes se existirem inteiros a, b, c, d taos que:

$$f(x, y) = g(ax + by, cx + dy),$$

com $ad - bc \neq 0$.

Definição 6.3 Definimos o discriminante de uma forma quadrática

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

por $\Delta_f = b^2 - 4ac$.

É facil ver que formas equivalentes tem o mesmo discriminante. Além disso, formas do tipo $f(x, y) = x^2 + ny^2$ com $n > 0$ possuem discriminante $\Delta = -4n < 0$.

Lema 6.1 *Uma forma $f(x, y)$ definida sobre $\mathbb{Z}$ representa propriamente um inteiro m se, e somente se, a forma f é equivalente a uma forma do tipo $mx^2 + bxy + cy^2$.*

Proposição 6.1 *Sejam $\Delta \equiv 0, 1 \pmod 4$ um inteiro e m um inteiro ímpar coprimo com Δ. Então m é propriamente representado por uma forma primitiva com discriminante Δ se, e somente se, Δ é um resíduo quadrático $\pmod m$.*

Demonstração: Se $f(x, y)$ representa propriamente o inteiro m, então, pelo Lema 6.1, podemos escrever

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

Assim, $\Delta = b^2 - 4mc \equiv b^2 \pmod m$.
Reciprocamente, suponhamos que $\Delta \equiv b^2 \pmod m$. Como m é ímpar, podemos supor que D e b possuem a mesma paridade, caso contrário podemos trocar b por $b + m$ sem alterar a congruência. Pela hipótese $D \equiv 0, 1 \pmod 4$ isso implica que $D \equiv b^2 \pmod{4m}$ daí $D = b^2 - 4mc$ para algum $c \in \mathbb{Z}$ e desta feita m será propriamente representado por $f(x, y) = mx^2 + bxy + cy^2$ e o resultado segue. □

Corolário 6.1 *Sejam $m, p \in \mathbb{Z}_+$ com p primo $p \nmid n$. Então $\left(\frac{-n}{p}\right) = 1$ se, e somente se, p pode ser representado por uma forma de discriminante $-4n$,*

Demonstração: Segue diretamente da proposição anterioruma vez que $-4n$ é um resíduo quadrático módulo p se, e somente se,

$$\left(\frac{-4}{p}\right) = \left(\frac{-n}{p}\right) = 1.$$

□

Definição 6.4 Uma forma primitiva positiva definida $f(x,y) = ax^2 + bxy + cy^2$ é dita reduzida se

$$| b | \leq a \leq c, \text{ e } b \geq 0, \text{ se } | b | = a \text{ ou } a = c.$$

Observação 6.2 Primeiramente, note que sendo $f(x,y)$ positiva definida, a e c são positivos. Em segundo lugar note que fixado $\Delta < 0$ existe um número finito de formas reduzidas tendo Δ como discriminante.

O próximo resultado exige longos cálculos e sua demonstração será omitida.

Teorema 6.3 *Cada forma positiva definida $f(x,y)$ em $\mathbb{Z}$ é equivalente a uma única forma reduzida.*

Vamos denotar por $h(\Delta)$ o número de classes de formas primitivas positivo definidas com discriminante Δ. Pelo teorema anterior $h(\Delta)$ coincide com o número de formas reduzidas tendo discriminante Δ e esse número é finito uma vez que $\Delta < 0$. Obtemos assim o seguinte resultado.

Corolário 6.2 *Seja $\Delta < 0$ um inteiro fixado. O número $h(\Delta)$ de classes de formas primitivas com discriminante Δ é finito e coincide com o número de formas reduzidas com discriminante Δ.*

Exemplo 6.1 Formas quadráticas reduzidas com $h(\Delta) = 1$, $\Delta \equiv 0 \pmod 4$.

1. Para $\Delta = -4$ temos $f(x,y) = x^2 + y^2$.
2. Para $\Delta = -8$ temos $f(x,y) = x^2 + 2y^2$.
3. Para $\Delta = -12$ temos $f(x,y) = x^2 + 3y^2$.
4. Para $\Delta = -16$ temos $f(x,y) = x^2 + 4y^2$.
5. Para $\Delta = -28$ temos $f(x,y) = x^2 + 7y^2$.

De fato essas são as únicas.

Exemplo 6.2 Formas quadráticas reduzidas com $h(\Delta) = 1$, $\Delta \equiv 1 \pmod 4$.

1. Para $\Delta = -3$ temos $f(x,y) = x^2 + y^2$.
2. Para $\Delta = -7$ temos $f(x,y) = x^2 + xy + 2y^2$.
3. Para $\Delta = -11$ temos $f(x,y) = x^2 + xy + 3y^2$.
4. Para $\Delta = -19$ temos $f(x,y) = x^2 + xy + 5y^2$.
5. Para $\Delta = -27$ temos $f(x,y) = x^2 + xy + 7y^2$.

6. Para $\Delta = -43$ temos $f(x, y) = x^2 + xy + 11y^2$.
7. Para $\Delta = -67$ temos $f(x, y) = x^2 + xy + 17y^2$.
8. Para $\Delta = -163$ temos $f(x, y) = x^2 + xy + 41y^2$.

De fato essas são as únicas.

Exemplo 6.3 Formas quadráticas reduzidas com $h(\Delta) > 1$, $\Delta \equiv 0 \pmod 4$.

1. Para $\Delta = -20$ temos $f(x, y) = x^2 + 5y^2$ e $f = 2x^2 + 2xy + 3y^2$.
2. Para $\Delta = -24$ temos $f(x, y) = x^2 + 6y^2$ e $2x^2 + 3y^2$.

Seja $n \in \mathbb{Z}_+$. Dizemos que a forma

$$q_n(x, y) = x^2 + ny^2$$

é a única forma principal com $\Delta = -4n$ se não existir outra forma reduzida com discriminante Δ representando os mesmos restos que q_n em $(\mathbb{Z}_{4n})^*$.

A próxima proposição é o melhor que conseguimos com métodos elementares. Isso era exatamente o que Euler estava tentando encontrar. A demonstração fica trivial após toda a teoria das formas quadráticas e das hipóteses corretas. O caso geral é extremamente mais complexo. O livro [COX] é uma obra monumental e fonte de muitas inspirações, leia o livro! Ou pelo menos uma parte dele.

Teorema 6.4 *Sejam $n \in \mathbb{Z}_+$ e suponha que a forma $q_n(x^2 + ny^2)$ seja a única forma reduzida principal com discriminante $\Delta = -4n$. Seja $p \in \mathbb{Z}_+$ um primo $p \nmid n$. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + ny^2$ se, e somente se,*

$$p \equiv \beta^2, \beta^2 + n \pmod{4n}$$

para algum $\beta \in \mathbb{Z}_{4n}$.

Demonstração: Se y for par, então

$$p = x^2 + ny^2 \equiv x^2 \pmod{4n}.$$

Se y for ímpar, então

$$p = x^2 + ny^2 \equiv x^2 + n \pmod{4n}.$$

□

6.5 Problemas

1. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + 5y^2$ se, e somente se, $p \equiv 1, 9 \pmod{20}$.

2. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que existem $x, y \in \mathbb{Z}$ tais que $2p = x^2 + 5y^2$ se, e somente se, $p \equiv 3, 7 \pmod{20}$.

3. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que existem $x, y \in \mathbb{Z}$ tais que $p = 2x^2 + 2xy + 3y^2$ se, e somente se, $p \equiv 3, 7 \pmod{20}$.

4. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + 6y^2$ se, e somente se, $p \equiv 1, 7 \pmod{24}$.

5. (Iranian Olympiad) Seja $p \in \mathbb{Z}_+$ um primo. Mostre que existem $x, y \in \mathbb{Z}$ tais que $p = 2x^2 + 3y^2$ se, e somente se, $p \equiv 5, 11 \pmod{24}$.

6. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + 7y^2$ se, e somente se,
$$p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}.$$

7. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + 10y^2$ se, e somente se,
$$p \equiv 1, 9, 11, 19 \pmod{40}.$$

8. Seja $p \in \mathbb{Z}_+$ um primo. Mostre que existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + 14y^2$ ou $p = 2x^2 + 7y^2$ se, e somente se,
$$p \equiv 1, 9, 15, 23, 25, 29 \pmod{56}.$$

9. (Komal) Mostre que a equação $x^3 - x + 9 = 5y^2$ não possui solução em $\mathbb{Z}$.

Agradecimentos

Em primeiro lugar agradeço à minha companheira, Ailma Andrade, pelo carinho, amor, companherismo e muita paciência que teve, principalmente no mês em que escrevi, muito apressadamente, essas notas.

Não poderia seguir sem agradecer a meu irmão Rafael Nonato, por tudo.

Gostaria de agradecer profundamente a Bruno Heberton e Ysleide Thays que foram meus alunos num curso de Introdução à Teoria dos Anéis no curso de licenciatura em Matemática da UFRPE, onde leciono, e anotaram toda as minhas aulas e me entregaram o material, uma parte dele a base do primeiro capítulo dessas notas. Vale salientar que a parte final se formatou a partir de uma aula para uma Semana Olímpica.

Agradeço ainda, muitíssimo, aos amigos Alan Muniz, Aline Vilela, Aron Simis, Bárbara Costa, Charles Almeida, Davi Nilson, Francesco Russo, Gabriel Bastos, Gabriel Guedes, João Lemos, Kezia Mestre, Lenin Bezerra, Marcos Miguel, Rafael Holanda, Ricardo Conceição, Thiago Dias, Vinícius Portella e Viviana Ferrer que leram uma versão preliminar dessas maltraçadas linhas, fizeram comentários e correções, a fim de deixar o texto mais aprazível.

Ao leitor, advirto; todos os erros e imprecisões são de minha exclusiva responsabilidade, não recaindo de forma alguma sobre os amigos supracitados nenhuma fagulha de negligência, que tomo para mim.

Bibliografia

[ANDREESCU] ANDREESCU, Titu et al. An introduction to Diophantine equations: A problem-based approach. New York: Birkhäuser, 2010.

[ATIYAH] ATIYAH, Michael. Introduction to commutative algebra. CRC Press, 2018.

[COX] COX, David A. Primes of the Form x2+ ny2: Fermat, Class Field Theory, and Complex Multiplication. with Solutions. American Mathematical Soc., 2022.

[DJUKIĆ] DJUKIĆ, Dušan et al. The IMO Compendium: A Collection of Problems Suggested for the International Mathematical Olympiads: 1959-2009 Second Edition. Springer New York, 2011.

[DUMMIT] DUMMIT, Evan. Number theory, course notes

[FUJIWARA] FUJIWARA, Guilherme Camarinha. Inteiros de Gauss e Inteiros de Eisenstein. Eureka, v. 14, p. 23-31, 2002.

[GARCIA] GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de álgebra. Instituto de Matemática Pura e Aplicada, 2006.

[IRELAND] IRELAND, Kenneth; ROSEN, Michael Ireland. A classical introduction to modern number theory. Springer Science and Business Media, 1990.

[NAGELL] NAGELL, Trygve. Introduction to number theory. Wiley, 1951.

[STEWART] STEWART, Ian; TALL, David Orme. Algebraic number theory. London: Chapman and Hall, 1979.