Formas Quadráticas e Fracções Contínuas

Luís Diogo, Carlos Florentino e Diogo Veloso

8 de Novembro de 2006

Resumo

Este artigo é baseado no curso "Quadratic Forms and Continued Fractions", de R. Takloo-Bighash, integrado na Escola Diagonal que decorreu em Setembro de 2005, no Instituto Superior Técnico.

1 Introdução

A teoria dos números é uma das disciplinas mais antigas da matemática. Pode dizer-se que um dos seus objectivos é encontrar soluções inteiras ou racionais de equações polinomiais a várias variáveis, por exemplo

$$45x^7y^9 + 8zy^3 - 23w^4 + 1 = 0.$$

Claro que à partida não é fácil arranjar soluções de uma equação deste género, ou provar que não existem soluções. Como fazê-lo, então? Existe algum método? De um modo geral não. Mesmo provar que não existem soluções não triviais[1] de

$$x^3 + y^3 = z^3$$

é já complicado.

As equações polinomiais com coeficientes inteiros e para as quais se procuram soluções inteiras são chamadas equações diofantinas, em homenagem a Diofanto, um matemático do século III, de Alexandria.

Então que tipo de equações vamos estudar? De um modo geral, vamos estudar problemas relacionados com polinómios do tipo

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

onde $a, b, c \in \mathbb{Z}$, designados por formas quadráticas. Neste caso, sim, existem várias teorias para responder aos diferentes problemas que iremos colocar.

Vamos primeiro abordar a equação de Pell

$$x^2 - Dy^2 = 1$$

onde D é um inteiro positivo não quadrado[2]. Esta é uma equação antiga, tendo já sido estudada por vários matemáticos indianos antes de chegar à Europa. De facto, Brahmagupta estudou-a no século VII e Bhaskara no século XII. Na Europa, o primeiro matemático a encontrar uma solução geral foi Brouncker, no século XVII. Mais tarde Euler confundiu Brouncker com Pell, outro matemático

[1] isto é, com um dos inteiros x, y, z igual a zero.
[2] ou seja, D não é um quadrado perfeito.

Artigo © 2006 . A cópia privada é permitida.

da época, e chamou-lhe equação de Pell. Vamos resolver esta equação através de fracções contínuas.

Em seguida veremos como achar todas as soluções inteiras de

$$x^2 + y^2 = z^2,$$

os chamados triplos pitagóricos.

Na parte final vamos estudar que números podem ser representados por formas quadráticas definidas positivas, isto é

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

com $a > 0$ e $4ac - b^2 > 0$. Por exemplo, que números se podem escrever na forma $x^2 + y^2$ ou $x^2 + ny^2$?

Para estudar o problema acima vamos relacioná-lo com uma determinada acção do grupo de matrizes 2 por 2 com coeficientes inteiros e determinante 1 no plano hiperbólico. Esta teoria vai permitir dizer que números se podem escrever da forma $x^2 + ny^2$, para alguns n. Este assunto está bastante relacionado com o estudo dos inteiros num corpo quadrático.

Apesar da longa história e de constituirem os primeiros casos não triviais de equações diofantinas, a investigação da aritmética das equações quadráticas está longe de ter terminado. No fim deste artigo apresentamos alguns resultados recentes sobre este "velho" assunto da teoria dos números.

O objectivo destas notas foi dar uma ideia mais prática do que teórica de como arranjar soluções de determinados problemas. Ao longo do texto há bastantes exercícios, de vários graus de dificuldade, que formam parte integrante deste artigo. Encorajamos o leitor a tentar fazer a maior parte. Para quem estiver também interessado nas vertentes mais teóricas destes assuntos, ou na teoria dos números em geral, sugerimos os livros [IR, K, MT, ST].

Exercício 1. Encontre uma solução não trivial de $x^2 - 13y^2 = 1$.

Agradecimentos. Gostaríamos de agradecer à organização da Escola Diagonal e ao Professor Ramin Takloo-Bighash, às Professoras Sílvia Anjos e Esmeralda Dias, e ao Gonçalo Tabuada pela ajuda nas sessões de problemas.

2 Noções Básicas de Aritmética

Antes de abordar os problemas referidos, vamos começar por rever alguns conceitos básicos. Uma referência para esta secção é, por exemplo, [K]. O nosso primeiro problema é encontrar as soluções $x, y \in \mathbb{Z}$ de

$$ax + by = c$$

onde a, b, c são inteiros dados.

Definição 1. Se $a, b \in \mathbb{Z}$, dizemos que a *divide* b, ou que b é *divisível* por a, ou ainda que a é um *divisor* de b se existe $n \in \mathbb{Z}$ tal que $b = an$. Nesse caso escrevemos $a|b$.

Note-se que $1|b$ para qualquer inteiro b, e que pelo contrário, 0 só é divisor de si próprio. Note-se também que excepto para ± 1, nenhum inteiro divide 1.

Proposição 2. *i) Se $a|b$ e $b|c$ então $a|c$;*
ii) Se $a|b$ e $a|c$ então $a|(b \pm c)$;
iii) Se r é inteiro e $a|b$ então $a|br$.

Definição 3. Dizemos que $g > 0$ é o máximo divisor comum de a e b, $g = \gcd(a, b)$,[3] se para qualquer d tal que $d|a$ e $d|b$ se tem $d|g$.

Exercício 2. Sejam a e b inteiros. Prove que $\gcd(\lambda a, \lambda b) = \lambda \gcd(a, b)$.

Teorema 1. *[Algoritmo da divisão] Sejam $a, b \in \mathbb{N}$. Então existe um único $q \in \mathbb{N}$ e um único $r \in \{0, ..., b-1\}$ tal que $a = bq + r$.*

Demonstração. Primeiro provamos a existência. Seja q a parte inteira de a/b, isto é $q = \lfloor a/b \rfloor$ é o único inteiro tal que $q \leq a/b < q + 1$. Então

$$0 \leq a - bq = b(a/b - q) < b.$$

Assim, definindo r como $a - bq$ temos $0 \leq r \leq b - 1$. Deixamos a prova da unicidade ao leitor. □

Apresentamos agora um algoritmo que fornece o $\gcd(a, b)$ de quaisquer inteiros positivos a e b.
Suponhamos, sem perda de generalidade, que $a > b$. Pondo $a_1 = a, b_1 = b$, temos, pelo algoritmo da divisão, que existem $q_1, r_1 \in \mathbb{Z}$ com $0 \leq r_1 \leq b_1 - 1$ tais que:

$$a_1 = b_1 q_1 + r_1.$$

Se $r_1 = 0$ então o algorítmo termina e $\gcd(a, b) = b$. Se $r_1 > 0$, pomos $a_2 = b_1, b_2 = r_1$ e existem, como antes, $q_2, r_2 \in \mathbb{N}_0$ com $0 \leq r_2 \leq b_2 - 1 = r_1 - 1$. Logo $r_2 < r_1$. Se $r_2 > 0$, pomos de novo $a_{k+1} = b_k, b_{k+1} = r_k$ e temos, indutivamente que, $r_{k+1} < r_k$, logo r_k é decrescente e acabará por ser zero. Representando estas divisões sucessivas, obtemos:

$$\begin{aligned} a_1 &= b_1 q_1 + r_1 \\ a_2 &= b_2 q_2 + r_2 \\ &\vdots \\ a_{k-2} &= b_{k-2} q_{k-2} + r_{k-2} \\ a_{k-1} &= b_{k-1} q_{k-1} + r_{k-1} \\ a_k &= b_k q_k. \end{aligned}$$

Finalmente, b_k será o $\gcd(a, b)$. De facto b_k divide $a_k = b_{k-1}$ e $b_k = r_{k-1}$ e assim $b_k | a_{k-1} (= b_{k-2})$. De novo b_k divide $r_{k-2} = b_{k-1} = a_k$ logo divide a_{k-2}, e assim sucessivamente. Temos então que b_k divide b_1 e a_1.
Por outro lado, se $d|a = a_1$, e $d|b (= b_1 = a_2)$ então d divide $r_1 = b_2 = a_3$, logo $d|r_2 (= b_3)$. Do mesmo modo $d|r_3$ e assim sucessivamente, até obtermos que d é divisor de $r_{k-1} = b_k$. Logo b_k é o $\gcd(a, b)$. Assim, temos

Teorema 2. *[Algoritmo de Euclides] Sejam $a, b \in \mathbb{N}$. Então o algoritmo descrito acima fornece o $\gcd(a, b)$ num número finito de passos.*

[3] Do inglês *greatest common divisor*

Exemplo 1. Se $a = 84, b = 60$, o algoritmo de Euclides diz-nos que

$$84 = 60 \times 1 + 24$$

$$60 = 24 \times 2 + 12$$

$$24 = 12 \times 2.$$

Assim $\gcd(84, 60) = 12$.

Exercício 3. Calcule o gcd dos seguintes números:

- 627 e 308;
- 1260 e 692.

Estamos agora em condições de resolver o problema proposto acima: encontrar soluções $x, y \in \mathbb{Z}$ de

$$ax + by = c$$

onde a, b, c são inteiros dados.

Em primeiro lugar, para que a equação tenha solução é necessário que $\gcd(a, b)|c$. De facto, o $\gcd(a, b)$ divide a e divide b logo tem que dividir c. Acontece que esta condição é também suficiente. Se $g = \gcd(a, b)$ então existem infinitos $x, y \in \mathbb{Z}$ tais que $ax + by = g$. Apesar de não o provarmos aqui, o próximo exemplo contém detalhes suficientes para permitir ao leitor completar a prova por si.

Exemplo 2. Para encontrar uma solução de $68x + 255y = 340$, primeiro calculamos o $\gcd(68, 255)$

$$255 = 68 \times 3 + 51$$

$$68 = 51 \times 1 + 17$$

$$51 = 17 \times 3.$$

Logo $\gcd(68, 255) = 17$. Como 17 divide 340 então o problema acima tem solução. Através dos cálculos acima conseguimos arranjar a, b tais que $68a + 255b = 17$. De facto

$$17 = 68 - 51 = 68 - (255 - 68 \times 3) = 68 \times 4 - 255 = 68 \times 4 + 255 \times (-1).$$

Assim temos $a = 4$ e $b = -1$. Para arranjar uma solução de $68x + 255y = 340 = 17 \times 20$ só temos que multiplicar as soluções acima por 20. O resultado é $x = 80$ e $y = -20$. Mas será este resultado único? Não. De facto, pondo $x = 80 - 15k$ e $y = -20 + 4k$, com k inteiro, obtemos todas as soluções do problema. Consegue explicar porquê?

Agora relembramos a definição de número primo:

Definição 4. Um número $p > 1$ diz-se *primo* se os únicos divisores positivos de p são 1 e p.

Uma propriedade muito útil dos números primos, e que pode facilmente ser verificada, é a seguinte.

Proposição 5. *Um número $p > 1$ é primo se e só se para todo $a, b \in \mathbb{Z}$, $p|ab$ implica $p|a$ ou $p|b$.*

Por causa da sua importância costuma-se chamar *teorema fundamental da aritmética* ao seguinte resultado.

Teorema 3. *Seja $n \in \mathbb{Z}$. Então existem primos $p_1, ..., p_m$ e inteiros positivos $\alpha_1, ..., \alpha_m$, tais que*

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}.$$

Esta representação é única a menos de permutação.

Exemplo 3. $234235 = 5 \times 79 \times 543$;

- $7112 = 2^3 \times 7 \times 127$.

Corolário 1. *Existem infinitos números primos.*

Demonstração. Suponhamos que existia apenas um número finito de primos, $p_1, ..., p_n$ digamos. Consideremos então o número $N = 1 + p_1 \cdots p_n$. Pelo teorema acima, N tem que ser produto de números primos. Suponhamos que p_i é um desses primos. Assim $p_i | N (= 1 + p_1 \cdots p_n)$. Mas $p_i | p_1 \cdots p_n$, e portanto tem que dividir 1, o que é absurdo. □

Exercício 4. Dado um inteiro n, encontre n inteiros consecutivos, nenhum dos quais é primo.

Agora definimos um conceito que nos vai ser útil.

Definição 6. [Relação de congruência] Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, escrevemos $a \equiv b \mod n$ se $n | (b - a)$.

Exercício 5. Prove que $\equiv$ define uma relação de equivalência, i.e, para todo o $m \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$, temos.

- $a \equiv a \mod m$;
- $a \equiv b \mod m \Rightarrow b \equiv a \mod m$;
- $a \equiv b \mod m$, e $b \equiv c \mod m \Rightarrow a \equiv c \mod m$.

A classe de equivalência de $a \in \mathbb{Z}$ é o conjunto $\{a + mk : k \in \mathbb{Z}\}$. Representamo-lo por $a + m\mathbb{Z}$. O conjunto das classes de equivalência $\{a + m\mathbb{Z} : a \in \mathbb{Z}\}$ é representado por $\mathbb{Z}/m\mathbb{Z}$.

Proposição 7. *As seguintes operações estão bem definidas nas classes de equivalência* $\mod m$

- $(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}$
- $(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = (a \cdot b) + m\mathbb{Z}$

Demonstração. Só provamos o primeiro ponto, deixando o segundo para o leitor. Sejam $A \in a + m\mathbb{Z}, B \in b + m\mathbb{Z}$, i.e. $A = a + mr$ para algum $r \in \mathbb{Z}$, e $B = b + ms$ para algum $s \in \mathbb{Z}$. Temos então que:

$$A + B = a + mr + b + ms = a + b + m(r + s)$$

e logo $A + B \in (a + b) + m\mathbb{Z}$. □

Exercício 6. Prove que se p é um número primo, então $(a+p\mathbb{Z})\cdot(b+p\mathbb{Z}) = p\mathbb{Z}$ implica $a+p\mathbb{Z} = p\mathbb{Z}$ ou $b+p\mathbb{Z} = p\mathbb{Z}$.

É fácil ver que, para quaisquer $a, b \in \mathbb{Z}$ as equações $a+m\mathbb{Z} = b+m\mathbb{Z}$ e $a \equiv b \mod m$ são equivalentes. Assim, a Proposição anterior fornece as seguintes regras de cálculo que são muito usadas na prática.

Proposição 8. *Sejam $a, a', b, b' \in \mathbb{Z}$ e $m \in \mathbb{N}$, verificando $a \equiv a' \mod m$ e $b \equiv b' \mod m$. Então*

$$\begin{aligned} a+b &\equiv a'+b' \mod m \\ a\cdot b &\equiv a'\cdot b' \mod m. \end{aligned}$$

Exercício 7. Sejam a, b primos entre si, i.e. tais que $\gcd(a,b) = 1$. Sejam também $x_1, x_2 \in \mathbb{Z}$. Prove que existe uma única solução de:

$$\begin{cases} x \equiv x_1 \mod a \\ x \equiv x_2 \mod b \end{cases}$$

com $0 \leq x < a\cdot b$. Assim esta é a única solução $\mod a\cdot b$. Isto é, se y for outra solução, então $x \equiv y \mod a\cdot b$.

Agora vamos enunciar um teorema que já era conhecido por matemáticos chineses do século III. Como já fizemos noutro caso não o vamos provar, mas deixamos ao leitor detalhes suficientes para que o possa fazer por si.

Teorema 4. *[Teorema Chinês dos Restos] Sejam $m_1, m_2, \ldots, m_k \in \mathbb{Z}$, tais que $\gcd(m_i, m_j) = 1$ para todos os índices $i, j = 1, ..., k$ distintos. Então para todo o $a_1, \ldots, a_k \in \mathbb{Z}$, o sistema:*

$$\begin{cases} x \equiv a_1 \mod m_1 \\ \vdots \\ x \equiv a_k \mod m_k \end{cases}$$

tem sempre uma solução $x \in \mathbb{Z}$.

Exemplo 4. Queremos encontrar $x \in \mathbb{Z}$ tal que

$$\begin{cases} x \equiv 3 \mod 7 \\ x \equiv 8 \mod 11 \\ x \equiv 1 \mod 13 \end{cases}.$$

Assim $x = 7a+3$ para algum $a \in \mathbb{Z}$, $x = 11b+8$ para algum $b \in \mathbb{Z}$, e ainda $x = 13c+1$ para algum $c \in \mathbb{Z}$. Donde sai, em particular, que $7a+3 = 11b+8$.
Logo

$$7a + 11(-b) = 5.$$

Apliquemos o algoritmo de Euclides a 7 e 11.

$$\begin{aligned} 11 &= 7\times 1 + 4 \\ 7 &= 4\times 1 + 3 \\ 4 &= 3\times 1 + 1 \end{aligned}$$

Assim temos que

$$1 = 4 - 3 = 4 - (7 - 4) = (11 - 7) - (7 - (11 - 7)) = 7 \times (-3) + 11 \times 2.$$

Portanto $a = -15$ e $b = -10$ verificam $7(-15) + 11(-10) = -105 + 110 = 5$. Pelo exercício anterior $x \equiv 7(-15) + 3 \equiv -102 \equiv 52 \mod 7 \times 11$.

Assim reduzimos o problema acima a encontrar soluções de

$$\begin{cases} x \equiv 52 \mod 77 \\ x \equiv 1 \mod 13 \end{cases}$$

Como no início, temos $x = 77d + 52$ para algum $d \in \mathbb{Z}$ e $x = 13e + 1$ para algum $e \in \mathbb{Z}$. Logo $13b - 77a = 51$. Aplicando o algoritmo de Euclides a $(77, 13)$,

$$\begin{aligned} 77 &= 13 \times 5 + 12 \\ 13 &= 12 \times 1 + 1. \end{aligned}$$

Assim temos que

$$1 = 13 - 12 = 13 - (77 - 13 \times 5) = 13 \times 6 - 77.$$

Portanto $a = 51$ e $b = 51 \times 6 = 306$. Logo uma solução $\mod 77 \times 13 = 1001$ é dada, por exemplo, por: $13 \times 306 + 1 = 3979 \equiv 976 \mod 1001$. De facto $976 = 7 \times 139 + 3 = 11 \times 88 + 8 = 13 \times 75 + 1$.

Exercício 8. Resolva o sistema

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 1 \mod 3 \\ x \equiv 1 \mod 5 \end{cases}$$

Exercício 9. Demonstre o Teorema chinês dos restos.

Definimos agora, com o único objectivo de familiarizar o leitor, os conceitos de anel e corpo.

Definição 9. Dizemos que um conjunto A com duas operações associativas $+$ e $\cdot$ é um *anel* se para quaisquer $a, b, c \in A$ se tem

- Existem elementos $0 \in A$ tal que $a + 0 = a$, e $1 \in A$ tal que $a \cdot 1 = a$
- Existe $a' \in A$ tal que $a + a' = 0$
- $a + b = b + a$ e $a \cdot b = b \cdot a$
- $a \cdot (b + c) = a \cdot b + a \cdot c$.

Ao elemento a' da segunda propriedade acima, é usual denotar por $-a$.

Assim um anel tem, num certo sentido, as mesmas propriedades que $\mathbb{Z}$. A Proposição 7 diz-nos que $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ é um anel. Deste modo podemos simplificar expressões com variáveis em $\mathbb{Z}/m\mathbb{Z}$ usando as regras que estamos habituados a usar em $\mathbb{Z}$. Note-se contudo que não existe divisão definida. De facto em $\mathbb{Z}/4\mathbb{Z}$ o elemento $2 + 4\mathbb{Z}$ não tem inverso pois $2 \times 2 \equiv 0 \mod 4$. Um anel $(A, +, \cdot)$ diz-se um corpo se verificar a seguinte propriedade adicional

- Para $a \neq 0$ existe $a'' \in A$ tal que $a \cdot a'' = 1$.

Como acima, é usual denotar o elemento a'' por a^{-1} ou por $1/a$.

Notemos que se p é primo, $\mathbb{Z}/p\mathbb{Z}$ é um corpo. Logo temos a divisão definida. Deste modo qualquer equação da forma $ax \equiv b \mod p$ com $a, b \in \mathbb{Z}$ e $p \nmid a$ tem solução $x \in \mathbb{Z}$.

O que se segue ser-nos-á útil mais adiante, quando tratarmos da equação de Pell.

Definição 10. Dado um inteiro não quadrado D, definimos $\mathbb{Z}[\sqrt{D}] := \{z = x + y\sqrt{D} : x, y \in \mathbb{Z}\}$.

$\mathbb{Z}[\sqrt{D}]$ é um anel com a soma e a multiplicação naturais. A $\mathbb{Z}[\sqrt{-1}]$ chamamos o anel dos inteiros Gaussianos.

Definição 11. O *conjugado* de $z = x + y\sqrt{D}$ é $\bar{z} = x - y\sqrt{D}$. A *norma* de $z \in \mathbb{Z}[\sqrt{D}]$ é $N(z) = z\bar{z}$.

Observe que temos $x^2 - Dy^2 = (x + y\sqrt{D})(x - y\sqrt{D}) = z\bar{z}$.

Notamos que no caso $D = -1$, estas noções correspondem precisamente às noções de conjugado e de norma nos números complexos.

Exercício 10. Prove que $N(zw) = N(z)N(w)$.

- Prove que uma solução da equação de Pell é o mesmo que um elemento $z \in \mathbb{Z}[\sqrt{D}]$ tal que $N(z) = 1$.

Assim, se z for tal que $N(z) = 1$ então $N(z^k) = 1$ para qualquer $k \in \mathbb{N}$. No caso $D > 0$ isto significa que se houver uma solução não trivial da equação de Pell então há infinitas soluções.[4] Na próxima secção, provaremos que qualquer equação $x^2 - Dy^2 = 1$ tem sempre soluções.

Exemplo 5. Para $D = 3$ temos

$$N(2 + \sqrt{3}) = 1.$$

Logo, como $(2 + \sqrt{3})^2 = 7 + 4\sqrt{3}$, temos também que

$$N(7 + 4\sqrt{3}) = 1.$$

Vemos assim que os pares $(2, 1)$ e $(7, 4)$ são soluções da equação $x^2 - 3y^2 = 1$.

Exercício 11. Considere $D = -1$. Prove, usando as propriedades da norma, que se $X^2 + Y^2 = A$ e $Z^2 + W^2 = B$, então existe uma solução de $x^2 + y^2 = AB$.

Prove também que se $\gcd(X, Y) = \gcd(Z, W) = 1$, então a solução que se obtém acima tem também $\gcd = 1$.

Observação 1. Por analogia com os inteiros, os primos no anel $\mathbb{Z}[\sqrt{D}]$ são definidos como os números $z = x + y\sqrt{D}$ tais que para toda a decomposição de z como $a \cdot b$, onde $a, b \in \mathbb{Z}[\sqrt{D}]$, temos $z|a$ ou $z|b$. Contudo a factorização única em números primos não se verifica na maior parte destes anéis. Perceber este caso mais geral foi um passo importante na história da Álgebra e da Teoria dos números.

[4] Isto acontece porque, quando $D > 0$, $\mathbb{Z}[\sqrt{D}]$ não tem raízes da unidade para além de ± 1.

3 Fracções Contínuas e a Equação de Pell

Desde tempos remotos que sábios procuraram o valor exacto de alguns números, por exemplo π, $\sqrt{2}$, etc. Por exemplo o valor dado a $\sqrt{2}$ na Babilónia era $17/12$. Arquimedes no séc.III ac provou que $223/71 < \pi < 22/7$. O indiano Aryabatha usava $\pi = 3,1416$ no séc.V, e no séc.VI o chinês Zu Chongzie usava já $\pi = 355/113$, que como veremos é uma aproximação muito boa.

Estamos assim, interessados em encontrar a melhor aproximação racional a um dado número. Para isso utilizaremos fracções contínuas. Mais tarde veremos que, surpreendentemente, tudo isto está relacionado com a equação de Pell.

Começamos então por definir fracção contínua.

Definição 12. Uma *fracção contínua* é uma expressão da forma

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

onde $a_k \in \mathbb{Z}$ e $a_1, a_2, ... > 0$. Representamo-la por $[a_0, a_1, a_2, \ldots]$.

Chamamos a

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} = [a_0, ..., a_n]$$

o *n-ésimo convergente* da fracção contínua. Note que $[a_0, ..., a_n] = \frac{p_n}{q_n}$ para determinados $p_n, q_n \in \mathbb{N}$, que tomaremos como sendo primos entre si.

Exercício 12. Prove que

- $p_0 = a_0$, $q_0 = 1$;
- $p_1 = a_0 a_1 + 1$, $q_1 = a_1$;
- $p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$.

Exercício 13. Usando indução, prove que:

- $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$;
- $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$.

Podemos levantar algumas questões sobre fracções contínuas:

- O que se quer dizer com um processo de soma e divisão infinitos?
- Que números podem ser representados por fracções contínuas?
- Essa representação é única?

Pode-se provar que para cada fracção contínua, a sucessão definida pelos convergentes $\frac{p_n}{q_n}$ tem um limite. Este é o significado da fracção contínua $[a_0, ..., a_n, ...]$. Também se pode mostrar que todo número real se pode escrever como fracção contínua. Por exemplo para π, temos

$$\pi = 3 + \pi - 3.$$

Escolhemos 3 porque é o único inteiro tal que $0 \leq \pi - 3 < 1$. Mas queremos escrever

$$\pi = 3 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}.$$

Logo, a_1 tem que verificar

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}} = \frac{1}{\pi - 3} = 7.0625...$$

Assim, $a_1 = 7$ e podemos continuar até termos encontrado a_n.

Existe, de facto, alguma ambiguidade mas *só em fracções contínuas finitas*! Por exemplo, $a_0 = (a_0 - 1) + \frac{1}{1}$, logo $[a_0] = [a_0 - 1, 1]$, ou mais geralmente $[a_0, ..., a_n] = [a_0, ..., a_n - 1, 1]$.

É claro que qualquer fracção contínua finita representa um número racional. O que já não é tão claro é que qualquer número racional é representado por uma fracção contínua finita. Seja $\frac{a}{b}$ um número racional. Dividindo a por b temos que, $a = q_1 b + r_1$, para algum $0 \leq r_1 \leq b - 1$. Logo:

$$\frac{a}{b} = \frac{q_1 b + r_1}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}}.$$

Agora dividimos b por r_1. De novo, $b = q_2 r_1 + r_2$ para algum $0 \leq r_2 \leq r_1 - 1$. Assim:

$$\frac{a}{b} = q_1 + \frac{1}{\frac{q_2 r_1 + r_2}{r_1}} = q_1 + \cfrac{1}{q_2 + \cfrac{r_2}{r_1}}.$$

Se o leitor prestar atenção verificará que o que se tem estado a fazer é exactamente o mesmo que no *Algoritmo de Euclides*. Assim, o processo tem que parar e a fracção contínua será finita.

Exemplo 6. Vamos desenvolver em fracção contínua $\frac{255}{68}$:

$$\frac{255}{68} = \frac{3 \times 68 + 51}{68} = 3 + \frac{1}{\frac{68}{51}} =$$

$$3 + \cfrac{1}{1 + \cfrac{17}{51}} = 3 + \cfrac{1}{1 + \cfrac{1}{3}}.$$

Exemplo 7. Dos seguintes cálculos pode-se ver facilmente que $\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, ...]$

$$\begin{aligned}
\sqrt{7} &= 2 + \sqrt{7} - 2 \\
\frac{1}{\sqrt{7}-2} &= \frac{\sqrt{7}+2}{3} = 1 + \frac{\sqrt{7}-1}{3} \\
\frac{3}{\sqrt{7}-1} &= \frac{3(\sqrt{7}+1)}{6} = \frac{\sqrt{7}+1}{2} = 1 + \frac{\sqrt{7}-1}{2} \\
\frac{2}{\sqrt{7}-1} &= \frac{\sqrt{7}+1}{3} = 1 + \frac{\sqrt{7}-2}{3} \\
\frac{3}{\sqrt{7}-2} &= \sqrt{7}+2 = 4 + \sqrt{7} - 2
\end{aligned}$$

Observação 2. Para fracções contínuas periódicas vamos colocar uma barra sobre a parte periódica. Assim por exemplo a fracção contínua de $\sqrt{7}$ é escrita como $\left[2, \overline{1, 1, 1, 4}\right]$. A equação de Pell está relacionada com este tipo de fracções contínuas.

Os dois teoremas que enunciamos em seguida relacionam a fracção contínua com as aproximações racionais de um dado número. Estas dizem que um número racional é uma boa aproximação de ξ, se e só se for um convergente da fracção contínua de ξ. Assim as melhores aproximações são convergentes da fracção contínua e vice-versa.

Teorema 5. *Seja* $\xi = [a_0, a_1, \ldots]$. *Se* $\frac{a}{b}$ *verifica*

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2},$$

então

$$\frac{a}{b} = \frac{p_n}{q_n},$$

para algum n. *Além disso, se* $\gcd(a, b) = 1$, *então* $a = p_n$ *e* $b = q_n$.

Por outro lado também temos o seguinte.

Teorema 6. *Seja* $\xi = [a_0, a_1, \ldots]$. *Então*

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$$

para qualquer n.

O recíproco deste último teorema não é verdadeiro.

Exercício 14. Seja $\xi \in \mathbb{R}$. Encontre números p e q que verificam $\left|\xi - \frac{p}{q}\right| < \frac{1}{q^2}$ e tais que $\frac{p}{q}$ não é um convergente de ξ.

Exemplo 8. Temos que $\frac{24}{5}$ é uma boa aproximação $\sqrt{23}$. De facto

$$\left|\sqrt{23} - \frac{24}{5}\right| < 0.0042 < \frac{1}{2 \times 25} = 0.02.$$

Logo $\frac{24}{5}$ tem que ser igual a um convergente da fracção contínua de $\sqrt{23}$. De facto $\frac{24}{5} = [4, 1, 3, 1]$, e $\sqrt{23} = \left[4, \overline{1, 3, 1, 8}\right]$.

Agora poderíamos perguntar porque é que obtivemos de novo uma fracção contínua periódica da raiz quadrada de um inteiro não quadrado. Mais abaixo veremos que não é um acaso.

Entretanto damos um exemplo histórico.

Exemplo 9. Com uma calculadora podem-se obter os primeiros "dígitos" da fracção contínua de π

$$\pi = [3, 7, 15, 1, 292, 1, 1, ...]$$

n	a_n	p_n	q_n
0	3	3	1
1	7	$22 = 3 \times 7 + 1$	$7 = 7 \times 1 + 0$
2	15	$333 = 22 \times 15 + 3$	$106 = 7 \times 15 + 1$
3	1	$355 = 333 \times 1 + 22$	$113 = 106 \times 1 + 7$
4	292	$103993 = 355 \times 292 + 333$	$33102 = 106 \times 292 + 106$

Assim, $\frac{355}{113}$ é uma boa aproximação de π, e $\frac{103993}{33102}$ uma excelente.

Respondemos agora à questão proposta mais acima.

Proposição 13. *Um número real ξ tem fracção contínua periódica se e só se ξ é uma solução de um polinómio de grau dois com coeficientes inteiros.*

Demonstração. Só vamos fazer a prova numa direcção e apenas no caso das fracções contínuas completamente periódicas. Então tomemos um número real α com fracção contínua periódica.

$$\alpha = \left[\overline{b_1, b_2, \ldots, b_m}\right] = b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots \cfrac{1}{b_m + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \ddots}}}}} = b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ddots \cfrac{1}{b_m + \cfrac{1}{\alpha}}}}$$

Começamos por observar que

$$b_{m-1} + \cfrac{1}{b_m + \cfrac{1}{\alpha}} = b_{m-1} + \frac{\alpha}{b_m\alpha + 1} = \frac{(b_m\alpha + 1)b_{m-1} + \alpha}{b_m\alpha + 1} = \frac{A\alpha + B}{C\alpha + D}$$

onde $A, B, C, D \in \mathbb{Z}$. Analogamente,

$$b_{m-2} + \cfrac{1}{b_{m-1} + \cfrac{1}{b_m + \cfrac{1}{\alpha}}} = b_{m-2} + \cfrac{1}{\cfrac{A\alpha + B}{C\alpha + D}} = \ldots = \frac{A'\alpha + B'}{C'\alpha + D'}$$

$$\vdots$$

e obtemos por fim que

$$\alpha = \frac{a\alpha + b}{c\alpha + d}$$

para determinados $a, b, c, d \in \mathbb{Z}$. Logo,

$$c\alpha^2 + \alpha d = a\alpha + b \quad \Rightarrow \quad c\alpha^2 + (d-a)\alpha - b = 0.$$

assim, α é a solução de uma equação quadrática com coeficientes inteiros. Para a demonstração do recíproco, consulte-se [MT]. □

Agora, e finalmente, relacionamos fracções contínuas com soluções da equação de Pell.

Exercício 15. Prove que se $(x, y) \in \mathbb{Z}^2$ é solução de $x^2 - Dy^2 = 1$, então $\frac{x}{y}$ é um convergente da fracção contínua de $\sqrt{D}$.

Deste modo estamos a relacionar soluções da equação de Pell com convergentes da fracção contínua de $\sqrt{D}$. De facto temos:

Teorema 7. *Se* $\sqrt{D} = [a_0, \overline{a_1, ..., a_n}]$ *então* $p_{n-1}^2 - Dq_{n-1}^2 = \pm 1$, *onde* $\frac{p_{n-1}}{q_{n-1}} = [a_0, a_1, ..., a_{n-1}]$.

Agora convém ao leitor ter bem presente a definição e propriedades da norma que foram apresentadas na parte final da segunda secção.

Exemplo 10. Como encontrar uma solução de $x^2 - 17y^2 = 1$? Primeiro temos que saber qual é a fracção contínua de $\sqrt{17} = \left[4, \overline{8}\right]$ Como $[4] = \frac{4}{1}$ obtemos que $4^2 - 17 \times 1^2 = -1$. E daqui como é que conseguimos arranjar uma solução da equação de Pell? Note que $4^2 - 17 \times 1^2 = -1$ é equivalente a dizer que $N(4 + \sqrt{17}) = -1$. Mas a norma é multiplicativa, assim $1 = N(4 + \sqrt{17})N(4 + \sqrt{17}) = N((4 + \sqrt{17})(4 + \sqrt{17})) = N(33 + 8\sqrt{17})$. Então $(33, 8)$ deve ser uma solução da equação de Pell. De facto $33^2 - 17 \times 8^2 = 1089 - 1088 = 1$.

Corolário 2. *Seja D um inteiro positivo não quadrado. Então a equação de Pell $x^2 - Dy^2 = 1$ tem sempre infinitas soluções.*

Demonstração. O resultado decorre do teorema 7. Quando $p_{n-1}^2 - Dq_{n-1}^2 = -1$, usamos a norma para obter uma solução como no exemplo acima. Com esta solução de norma 1 podemos obter uma infinidade de soluções usando a propriedade multiplicativa da norma (ver o método descrito a seguir ao Exercício 10). □

Esta demonstração do Teorema 7 e o consequente método de resolução da equação de Pell são devidos a Lagrange, por volta de 1766. No entanto, existe um outro método, tão antigo como engenhoso, para resolover esta equação que foi desenvolvido por Brahmagupta no século VII e Bhaskara no século XII, que foi chamado o método cíclico ou *chakravala*. O leitor interessado poderá encontrar os detalhes desta história no endereço http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Pell.html.

Exemplo 11. Encontremos uma solução de $x^2 - 19y^2 = 1$. Temos que

$$\sqrt{19} = \left[4, \overline{2, 1, 3, 1, 2, 8}\right]$$

Para calcular $[4, 2, 1, 3, 1, 2]$ fazemos a seguinte tabela:

n	a_n	p_n	q_n
0	4	4	1
1	2	$9 = 4 \times 2 + 1$	$2 = 1 \times 2 + 0$
2	1	$13 = 9 \times 1 + 4$	$3 = 2 \times 1 + 1$
3	3	$48 = 13 \times 3 + 9$	$11 = 3 \times 3 + 2$
4	1	$61 = 48 \times 1 + 13$	$14 = 11 \times 1 + 3$
5	2	$170 = 61 \times 2 + 48$	$39 = 14 \times 2 + 11$

Logo $170^2 - 19 \times 39^2$ tem que ser ± 1. De facto $170^2 = 28900$ e $19 \times 39^2 = 28899$.

Exercício 16. Encontre soluções não triviais da equação de Pell com:

- $D = 51$;
- $D = 78$.

Observação 3. A estrutura das fracções contínuas de $\sqrt{D}$ onde D é um inteiro positivo não quadrado, é bastante particular. De facto, ainda que não haja um modo fácil de as calcular, pode-se mostrar que tais fracções contínuas são sempre periódicas da forma:

$$\left[a_0, \overline{a_1, a_2, ..., a_2, a_1, 2a_0}\right].$$

Assim por exemplo nem $\left[1, \overline{2, 3, 4}\right]$ nem $\left[2, \overline{3, 4, 3}\right]$ podem ser as fracções contínuas de $\sqrt{D}$ para algum $D \in \mathbb{Z}$.

4 Teorema de Fermat e Reciprocidade Quadrática

Neste capítulo vamos enunciar o teorema da reciprocidade quadrática e dar algumas aplicações. Depois provaremos o teorema, devido a Fermat, segundo o qual todos os primos da forma $4k + 1$ são a soma de dois quadrados.

Comecemos então por preparar o terreno para a reciprocidade quadrática. Dizemos que $a \in \mathbb{Z}$ é um *resíduo quadrático módulo* m (m um número natural) se a equação

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

tem uma solução inteira, isto é se existe uma raiz quadrada de $a \mod m$.

Definimos agora o símbolo de Legendre.

Definição 14. Dado um número primo p e um inteiro a, definimos a função

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{se } p \mid a \\ 1, & \text{se } p \nmid a \text{ e } a \text{ é um resíduo quadrático módulo } p \\ -1, & \text{se } p \nmid a \text{ e } a \text{ não é um resíduo quadrático módulo } p \end{cases}$$

à qual chamamos *símbolo de Legendre*.

Exemplo 12. Dado que as equações $x^2 \equiv 1 \mod 7$, e $x^2 \equiv 2 \mod 7$, têm 1 e 3 como soluções em $\mathbb{Z}/7\mathbb{Z}$, respectivamente, os números 1 e 2 são resíduos quadráticos módulo 7 e por isso, $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = 1$. Do mesmo modo, podemos obter os outros valores do símbolo de Legendre $\mod 7$:

$$\left(\frac{0}{7}\right) = 0 \qquad \left(\frac{3}{7}\right) = -1 \qquad \left(\frac{4}{7}\right) = 1 \qquad \left(\frac{5}{7}\right) = -1 \qquad \left(\frac{6}{7}\right) = -1.$$

Naturalmente, qualquer símbolo $\left(\frac{a}{7}\right)$, com $a \in \mathbb{Z}$, é determinado pelos valores acima pois $\left(\frac{a}{7}\right) = \left(\frac{b}{7}\right)$ sempre que $a \equiv b \mod 7$.

Exercício 17. Prove que para qualquer primo ímpar p se tem:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, a, b inteiros
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \mod 4 \\ -1 & \text{se } p \equiv 3 \mod 4, \end{cases}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

O teorema da reciprocidade quadrática estabelece uma relação entre as equações $x^2 \equiv q \mod p$ e $x^2 \equiv p \mod q$. Podemos enunciá-lo da seguinte forma.

Teorema 8. *Se p e q são primos ímpares distintos, então*

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

Exemplo 13. Não existe solução da equação $x^2 \equiv 3 \mod 257$ porque

$$\left(\frac{3}{257}\right) = (-1)^{\frac{(3-1)(257-1)}{4}} \cdot \left(\frac{257}{3}\right) = (-1)^{2\cdot\frac{256}{4}} \cdot \left(\frac{2}{3}\right) = -1.$$

Do mesmo modo, $x^2 \equiv 7 \mod 257$ não tem solução, dado que

$$\left(\frac{7}{257}\right) = (-1)^{\frac{(7-1)(257-1)}{4}} \cdot \left(\frac{257}{7}\right) = \left(\frac{5}{7}\right) = -1.$$

Exercício 18. Decida se existem soluções de:

- $x^2 \equiv 13 \mod 211$
- $x^2 \equiv 247 \mod 1201$
- $x^2 + 5x + 4 \equiv 47 \mod 509$.

Para ver a eficácia da reciprocidade quadrática, tente encontrar as soluções, nos casos de resposta afirmativa às questões acima.

A primeira demonstração completa da reciprocidade quadrática é devida a Gauss por volta de 1796. Uma das demonstrações mais simples foi obtida por Eisenstein, e pode ser consultada em [MT] ou em [IR].

Vamos agora considerar o seguinte problema.

Problema 1. Que números naturais podem ser escritos da forma $x^2 + y^2$, com $\gcd(x, y) = 1$?

Uma resposta não tão incompleta é dada pelo seguinte teorema de Fermat.

Teorema 9. *Seja $p > 2$ um número primo. Então,*

$$p = x^2 + y^2 \quad \Leftrightarrow \quad p \equiv 1 \mod 4.$$

Em breve veremos como se pode utilizar este resultado para dar uma resposta completa ao problema acima. Vamos apresentar duas demonstrações do teorema de Fermat; uma, nesta secção, usando aproximação por fracções contínuas e a outra, na secção 7, usando a teoria das formas quadráticas definidas positivas.

Para provar o teorema precisamos primeiro do resultado seguinte, que deixamos como exercício.

Exercício 19. Se $x \in \mathbb{R}$ e $n \in \mathbb{N}$, então existe uma fracção $\frac{a}{b}$, com $\gcd(a,b) = 1$, tal que $0 < b \leq n$ e

$$\left| x - \frac{a}{b} \right| \leq \frac{1}{b(n+1)}.$$

Sugestão: Use uma aproximação de x por fracção contínua.

Demonstração. [Teorema de Fermat] e $p = x^2 + y^2$, é trivial verificar que $p \equiv 1 \mod 4$. Reciprocamente, $p \equiv 1 \mod 4$ implica que $\left(\frac{-1}{p}\right) = 1$, pelo exercício 17. Então, por definição do símbolo de Legendre, temos

$$\exists r > 0 : \qquad r^2 \equiv -1 \mod p.$$

Seja $n = \lfloor \sqrt{p} \rfloor$ (onde $\lfloor \cdot \rfloor$ denota a função parte inteira). Usando o exercício acima, existem inteiros a e b tais que $0 < b \leq n$ e

$$\left| -\frac{r}{p} - \frac{a}{b} \right| \leq \frac{1}{b(n+1)} < \frac{1}{b\sqrt{p}}.$$

Seja $c = rb + pa$. Então, $c > b$, e

$$\left| \frac{rb + pa}{pb} \right| < \frac{1}{b\sqrt{p}} \Rightarrow |rb + pa| < \frac{pb}{b\sqrt{p}} = \sqrt{p} \Rightarrow |c| < \sqrt{p}.$$

Portanto, $0 < b^2 + c^2 < 2p$.

$$b^2 + c^2 \equiv b^2 + r^2 b^2 \equiv b^2(1 + r^2) \equiv b^2(1 - 1) \equiv 0 \mod p$$

Logo, podemos concluir que $b^2 + c^2 = p$. □

Podemos agora dar uma resposta completa ao problema 1.

Teorema 10. *Um número natural pode ser expresso como x^2+y^2, com $\gcd(x,y) = 1$ se e só se não tem factores primos da forma $4k+3$.*

Demonstração. Usando o exercício 11, não é difícil provar que qualquer número sem factores primos da forma $4k+3$ pode ser escrito como $x^2 + y^2$ para algum x, y com $\gcd(x,y) = 1$. Basta usar as propriedades da norma e notar que um tal número tem apenas 2, e primos da forma $4k+1$, na sua factorização. Reciprocamente, suponha-se que existe um n com um factor primo p, da forma $4k+3$, tal que $n = x^2 + y^2$, para algum $x, y \in \mathbb{Z}$ com $\gcd(x,y) = 1$. Então temos

$$x^2 + y^2 \equiv 0 \mod p \qquad \text{logo} \qquad x^2 \equiv -y^2 \mod p. \tag{1}$$

Se $x \equiv y \equiv 0 \mod p$ temos um absurdo, porque então $p|x$ e $p|y$. Caso contrário a equação (1) implica que -1 é um resíduo quadrático módulo p, pois $\mathbb{Z}/p\mathbb{Z}$ é um corpo. Mas pelo exercício 17, se $p \equiv 3 \mod 4$ então $\left(\frac{-1}{p}\right) = -1$. Logo temos uma contradição. □

5 Triplos Pitagóricos

Vamos agora estudar um outro problema clássico relativo a equações quadráticas. Queremos encontrar todas as soluções inteiras de

$$X^2 + Y^2 = Z^2.$$

A uma tal solução (X, Y, Z) chamamos triplo pitagórico. Começamos por notar que isto é equivalente a encontrar todas as soluções racionais de $x^2 + y^2 = 1$, através da transformação

$$x = \frac{X}{Z}, \qquad y = \frac{Y}{Z}.$$

Suponhamos que x, y são de facto soluções da equação. Então (x, y) é um ponto da circunferência (ver figura 1). A inclinação da recta que passa por (x, y) e $(1, 0)$

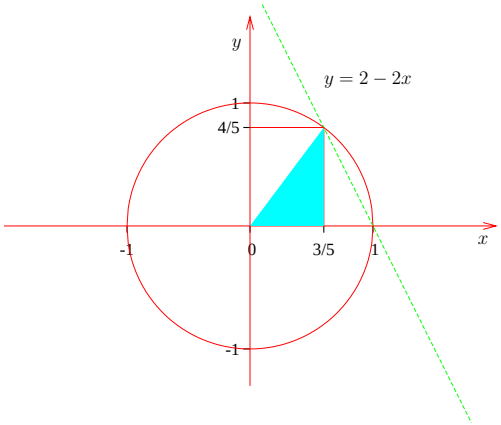

Figura 1: Triplos pitagóricos pelo método dos declives

$$m = \frac{y - 0}{x - 1} = \frac{y}{x - 1}.$$

Vamos agora ver a recíproca: suponhamos que $m \in \mathbb{Q}$ é a inclinação de uma recta que passa por $(1, 0)$ e outra solução (x, y). Então, temos

$$\begin{aligned} x^2 + y^2 &= 1 \\ y &= mx - m. \end{aligned}$$

Substituindo, obtemos:

$$x^2 + m^2(x - 1)^2 = 1 \Rightarrow (1 + m^2)x^2 - 2m^2x + (m^2 - 1) = 0.$$

É um facto bem conhecido que o quociente do termo de ordem mais baixa pelo termo de ordem mais alta de um polinómio é o produto das suas raízes (prove-o!). Assim, o produto das duas raízes do polinómio acima é $\frac{m^2-1}{m^2+1}$. Como sabemos que uma das soluções é 1 a outra tem que ser

$$x_0 = \frac{m^2 - 1}{m^2 + 1},$$

o que dá

$$y_0 = m(x_0 - 1) = m\left(\frac{m^2-1}{m^2+1} - 1\right) = -\frac{2m}{m^2+1}.$$

Assim, fazendo $m = -a/b$, com $a, b \in \mathbb{Z}$, podemos classificar *todas* as soluções racionais de $x^2 + y^2 = 1$ como pares da forma:

$$(x_0, y_0) = \left(\frac{m^2-1}{m^2+1}, -\frac{2m}{m^2+1}\right) = \left(\frac{a^2-b^2}{a^2+b^2}, \frac{2ab}{a^2+b^2}\right).$$

Voltando agora aos triplos pitagóricos, temos que se $Z^2 = X^2 + Y^2$ com $\gcd(X, Y, Z) = 1$ então

$$\frac{X}{Z} = \frac{a^2-b^2}{a^2+b^2} \qquad \text{e} \qquad \frac{Y}{Z} = \frac{2ab}{a^2+b^2}$$

para certos $a, b \in \mathbb{Z}$ primos entre si. Provámos então o seguinte resultado.

Proposição 15. *Qualquer triplo pitagórico* (X, Y, Z) *com* $\gcd(X, Y, Z) = 1$ *é da forma*

$$X = \frac{a^2-b^2}{\delta(a,b)}, \qquad Y = \frac{2ab}{\delta(a,b)} \qquad e \qquad Z = \frac{a^2+b^2}{\delta(a,b)},$$

onde $a, b \in \mathbb{N}$ *e*

$$\delta(a,b) = \begin{cases} 2 & \textit{se } a \textit{ e } b \textit{ ímpar} \\ 1 & \textit{caso contrário.} \end{cases}$$

Exemplo 14. Se tomarmos $a = 2$ e $b = 1$, então $\delta(a, b) = 1$ e obtemos o triplo da figura 1, $(X, Y, Z) = (3, 4, 5)$. Menos trivial é o caso $a = 7$, $b = 4$, que dá

$$X = 33, \qquad Y = 56, \qquad Z = 65.$$

Observação 4. Usando este método das rectas com declive racional podemos encontrar todas as soluções de equações da forma:

$$ax^2 + bxy + cy^2 = A$$

desde que, como acima, saibamos pelo menos uma solução.

Depois de termos determinado todos os triplos pitagóricos, e de saber os números que podem ser escritos na forma $x^2 + y^2$, podemos generalizar o Problema 1, e perguntar quais os inteiros podem ser escritos da forma $x^2 + ny^2$, onde n é um inteiro positivo fixado. Por exemplo, para $n = 2$ e $n = 3$, temos os seguintes resultados, que foram enunciados por Fermat e demonstrados por Euler (veja-se o Exemplo 20 e o Exercício 33):

$$p = x^2 + 2y^2 \quad \Leftrightarrow \quad p \equiv 1 \text{ ou } 3 \mod 8.$$

$$p = x^2 + 3y^2 \quad \Leftrightarrow \quad p = 3 \text{ ou } p \equiv 1 \mod 3.$$

Para estudar estas questões, vamos agora introduzir alguns conceitos geométricos que serão relacionados, mais tarde, com formas quadráticas definidas positivas.

6 O plano Hiperbólico e a acção de $SL_2(\mathbb{Z})$

Ao conjunto dos números complexos com parte imaginária positiva

$$\mathbb{H} = \{z = x + iy \in \mathbb{C} : y > 0\},$$

chamamos plano hiperbólico.

Observação 5. A razão para dar a este espaço o nome hiperbólico prende-se com o facto de ser um modelo natural para a geometria hiperbólica (que é um tipo de geometria não euclidiana). Mais concretamente, equipando $\mathbb{H}$ com a métrica Riemanniana

$$ds^2 = \frac{dx \otimes dy}{y^2},$$

obtemos uma superfície de curvatura seccional -1. Isto implica, por exemplo, que a soma dos ângulos internos de um triângulo feito com segmentos geodésicos é a diferença entre π e a área desse triângulo (necessariamente menor que π). Para uma introdução à geometria do plano hiperbólico e suas aplicações, que está fora do âmbito destas notas consulte-se, por exemplo, o livro [R].

Consideremos agora os seguintes grupos de matrizes.

- $GL_2(\mathbb{Z})$ é o grupo das matrizes 2×2 invertíveis com entradas inteiras e cuja inversa tem também entradas inteiras. Como se pode facilmente verificar, uma matriz 2×2 de entradas inteiras está em $GL_2(\mathbb{Z})$ se e só se tem determinante 1 ou -1.
- $SL_2(\mathbb{Z})$ é o subgrupo de $GL_2(\mathbb{Z})$ cujos elementos têm determinante igual a 1.

Exemplo 15.

$$\begin{pmatrix} 2 & 9 \\ 1 & 5 \end{pmatrix} \in SL_2(\mathbb{Z})$$

com inversa dada por

$$\begin{pmatrix} 5 & -9 \\ -1 & 2 \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Exercício 20. Prove que $SL_2(\mathbb{Z})$ é o grupo gerado pelas matrizes

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{e} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

isto é, que qualquer matriz em $SL_2(\mathbb{Z})$ pode ser escrita como um produto de um número finito destas matrizes e suas inversas.

Uma noção matemática muito importante é a de uma acção de grupo num conjunto.

Definição 16.

- Dizemos que um grupo G *actua* num conjunto M se existe uma aplicação $\phi : G \times M \to M$ tal que $\phi(g_1, \phi(g_2, m)) = \phi(g_1 g_2, m)$ e $\phi(e, m) = m$, para todo $g_1, g_2 \in G$ e $m \in M$, onde $e \in G$ designa a identidade de G.

- Ao conjunto $G \cdot x = \{\phi(g,x) : g \in G\}$ chama-se a *órbita* de x pela acção de G. O espaço quociente $M/G = \{G \cdot x : x \in M\}$ é designado o *espaço das órbitas*.

Observação 6. Quando a aplicação ϕ está subentendida, escrevemos normalmente $g \cdot x$ em vez de $\phi(g,x)$. Observe-se que, se M é um espaço topológico, o espaço das órbitas adquire também uma topologia natural (chamada topologia quociente).

Muitas vezes, é útil considerar a relação de equivalência definida por uma acção. Esta é a relação definida por $x \sim y$, $x, y \in M$, se e só se x e y estão na mesma órbita.

Exercício 21. Prove que a aplicação $\phi(n,x) = x + 2\pi n$ define uma acção de $\mathbb{Z}$ em $\mathbb{R}$. Neste caso $\mathbb{Z} \cdot x = x + 2\pi\mathbb{Z}$ e o espaço das órbitas $\mathbb{R}/\mathbb{Z}$ pode ser identificado com a circunferência S^1.

Definição 17. Definimos a seguinte acção de $SL_2(\mathbb{Z})$ em $\mathbb{H}$:

$$\gamma \cdot z := \frac{pz+q}{rz+s}. \qquad \gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbb{Z}), \quad z \in \mathbb{H}$$

Mais precisamente, esta operação é definida pela aplicação $F : SL_2(\mathbb{Z}) \times \mathbb{H} \to \mathbb{H}$ dada por $F(\gamma, z) = \frac{pz+q}{rz+s}$, onde γ é como acima.

Exercício 22. Prove que F está bem definida, i.e., se $z \in \mathbb{H}$ e $\gamma \in SL_2(\mathbb{Z})$ então $F(\gamma, z) \in \mathbb{H}$. Prove, também, que é uma acção no sentido da Definição 16.

Esta acção de $SL_2(\mathbb{Z})$ pode ser representada graficamente como na Figura 2. Nela, fazemos uma divisão do plano hiperbólico por um conjunto infinito de regiões conexas, limitadas por segmentos de recta e arcos de circunferência. Vamos mostrar que cada elemento de $SL_2(\mathbb{Z})$ envia uma destas regiões noutra, e que a órbita de qualquer ponto intersecta qualquer uma destas regiões. As letras representam o elemento $\gamma \in SL_2(\mathbb{Z})$ usado para obter uma dada região a partir da região K que está sombreada na Figura. Por exemplo, qualquer ponto na região TS é da forma $TS \cdot x$ com $x \in K$. Vejamos como actuam as matrizes S e T (Exercício 20) e que geram $SL_2(\mathbb{Z})$.

Exercício 23. Sendo (x,y) um ponto de $\mathbb{H}$, mostre que $T \cdot (x,y) = (x+1, y)$ e que $S \cdot (x,y) = \frac{1}{x^2+y^2}(-x, y)$.

A proposição seguinte mostra então que cada uma das regiões na Figura 2 é transformada em qualquer outra por acção de algum elemento de $SL_2(\mathbb{Z})$.

Proposição 18. *Qualquer $\tau \in \mathbb{H}$ está na órbita de um ponto contido na região*

$$K = \{z = x + iy \in \mathbb{H} : x \in [-\frac{1}{2}, \frac{1}{2}], \quad |z| \geq 1\}.$$

Demonstração. Qualquer ponto $z = x + iy \in \mathbb{H}$ cuja parte imaginária y é superior a 1 está na órbita de um ponto de K, pois basta que actuemos sucessivamente com a transformação T para que a sua parte real x fique em $[-\frac{1}{2}, \frac{1}{2}]$ (dado que T preserva y). Como S transforma $z \in \mathbb{H}$ em $z' = x' + iy' = -1/z$, deduzimos que $y' = y/|z|^2$ (pelo Exercício 23) o que implica que $y' \leq 1/y$ (pois

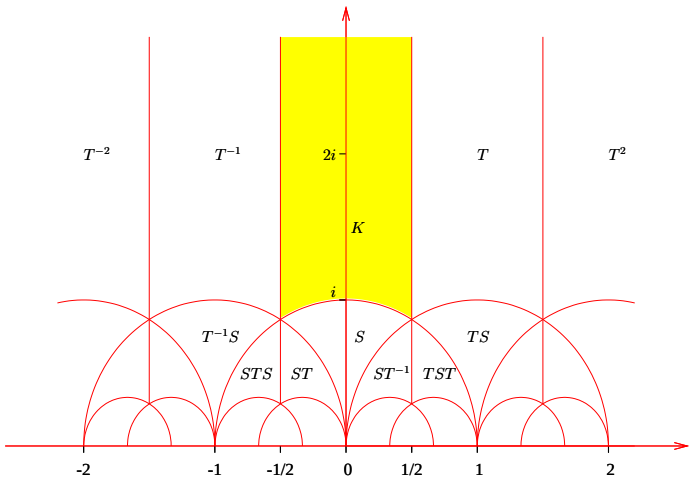

Figura 2: Subdivisão do plano hiperbólico de acordo com a acção de $SL_2(\mathbb{Z})$

$|z| \geq y$). Concluímos assim que os valores de y em qualquer órbita são limitados superiormente. A proposição segue então do facto que S envia o interior da circunferência unitária no seu exterior (Exercício 23), e por isso (quando $|z| < 1$) faz sempre aumentar o valor de y. □

Para descrevermos o espaço das órbitas desta acção, basta então estudar a acção de $SL_2(\mathbb{Z})$ na região K. Aqui ficam algumas questões que serão relevantes mais tarde.

Exercício 24. Mostre que:

i) Quaisquer dois pontos distintos no interior de K não estão na mesma órbita;

ii) Na fronteira de K qualquer ponto é equivalente (i.e, está na mesma órbita) a outro distinto, excepto o ponto $z = i$;

iii) O espaço quociente $\mathbb{H}/SL_2(\mathbb{Z})$ pode ser identificado com um disco fechado.

7 Representação de inteiros por formas quadráticas

Já sabemos, através do teorema de Fermat (Teorema 9) que números podem ser escritos na forma $x^2 + y^2$ para $x, y \in \mathbb{Z}$. Agora vamos generalizar esse resultado. Por exemplo

Problema 2. Que números podem ser escritos na forma

$$458x^2 + 214xy + 25y^2?$$

O estudo deste tipo de problemas foi iniciado por Lagrange em 1773-1775, que introduziu as noções de discriminante, equivalência e formas reduzidas que definiremos em seguida.

Designaremos por

$$f(x, y) = ax^2 + bxy + cy^2, \qquad a, b, c \in \mathbb{Z}$$

uma forma quadrática genérica de coeficientes inteiros. Note-se que esta forma quadrática pode ser também vista como uma função $\mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ definida por uma matriz 2×2 simétrica. De facto, a forma acima é definida pela multiplicação matricial

$$f(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Observação 7. De forma sintética, representaremos a forma quadrática $f = ax^2 + bxy + cy^2$ por (a,b,c) e a correspondente matriz 2×2 acima por M_f. Muitas vezes assume-se que b é par porque neste caso, M_f tem entradas inteiras.

Definição 19. Dizemos que f é *primitiva* se $\gcd(a,b,c) = 1$. Diz-se que f *representa* $m \in \mathbb{Z}$ se a equação $f(x,y) = m$ tem soluções inteiras x e y. Se além disso x e y forem primos entre si, então dizemos que m é *representado propriamente* por f.

Como consequência do teorema de Fermat, temos:

Exemplo 16. O inteiro m é representado propriamente por $x^2 + y^2$ se e só se m não tem factores primos da forma $4k + 3$.

Existe uma útil noção de equivalência entre formas quadráticas.

Definição 20. Duas formas quadráticas $f(x,y)$ e $g(x,y)$ são ditas *equivalentes* se existe

$$\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL_2(\mathbb{Z})$$

tal que $f(x,y) = g(px + qy, rx + sy)$, para todo $x, y \in \mathbb{Z}$. Se pudermos tomar $\gamma \in SL_2(\mathbb{Z})$, então dizemos que f e g são *propriamente equivalentes*.

Exercício 25. Verifique que f e g são equivalentes se e só se as matrizes correspondentes verificam $M_g = \gamma^t M_f \gamma$ para certa matriz $\gamma \in GL_2(\mathbb{Z})$. Neste caso escrevemos $\gamma(f) = g$. Assumindo $f = (a,b,c)$ determine $\gamma(f)$ em termos de (a,b,c) e das entradas de γ. (Sugestão: calcule a inversa da matriz γ).

Observação 8. Uma vez que γ é invertível, é fácil ver que formas equivalentes representam exactamente os mesmos números inteiros.

Exemplo 17. As formas $x^2+(x+y)^2 = 2x^2+2xy+y^2$ e x^2+y^2 são propriamente equivalentes pois a primeira obtém-se da segunda pela mudança de variáveis $(x,y) \mapsto (x, x+y)$, representada por uma matriz de determinante 1. Logo, representam precisamente os mesmos inteiros.

Exercício 26. Prove que $\phi(\gamma, f) := \gamma(f)$ define uma acção de $GL_2(\mathbb{Z})$ (e de $SL_2(\mathbb{Z})$) no conjunto das formas quadráticas.
Prove que a acção preserva formas primitivas, i.e se f é primitiva então $\gamma(f)$ é primitiva para qualquer γ em $SL_2(\mathbb{Z})$.

Definimos agora um importante invariante de uma forma quadrática.

Definição 21. Dada uma forma quadrática $f(x,y) = ax^2 + bxy + cy^2$, chamamos ao número $D = b^2 - 4ac$, o *discriminante* de f.

Por exemplo, o discriminante de $x^2 + ny^2$ é $-4n$.

Exercício 27. Mostre que formas equivalentes têm o mesmo discriminante. Assim, o discriminante é de facto invariante pela acção de $SL_2(\mathbb{Z})$.

Exercício 28. Mostre que $D = 0$ se e só se f é da forma $\lambda(ax + by)^2$, onde $\lambda, a, b \in \mathbb{Z}$.

Notando que

$$af(x,y) = a^2x^2 + abxy + acy^2 = \left(ax + \frac{by}{2}\right)^2 + acy^2 - \frac{b^2}{4}y^2 =$$
$$= \left(ax + \frac{by}{2}\right)^2 - \frac{1}{4}y^2 D,$$

vemos que:

1. se $D > 0$, então f representa tanto números positivos como negativos.
2. se $D < 0$, então
   i) $a > 0 \Rightarrow f$ é sempre positivo.
   ii) $a < 0 \Rightarrow f$ é sempre negativo.

Quando $D < 0$ e $a > 0$ dizemos que f é *definida positiva*. Isto ocorre precisamente quando a correspondente matriz M_f é definida positiva, uma vez que $D = -4 \det M_f$.

Exercício 29. Prove que se f é definida positiva, então $\gamma(f)$ é definida positiva para qualquer $\gamma \in SL_2(\mathbb{Z})$.

Assim, podemos dizer que $SL_2(\mathbb{Z})$ actua no conjunto, que designaremos por $\mathcal{P}$, das formas quadráticas definidas positivas.

De aqui em diante, iremos considerar *apenas* formas f definidas positivas. Por isso, D será doravante um inteiro negativo e seguiremos a convenção usual segundo a qual $\sqrt{D}$ denota a raiz quadrada de D com parte imaginária positiva.

Definição 22. Uma forma quadrática $f(x,y) = ax^2 + bxy + cy^2 \in \mathcal{P}$ é chamada *reduzida* se for primitiva e se

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

O nosso objectivo agora é mostrar que qualquer forma definida positiva é propriamente equivalente a uma única forma reduzida. A estratégia é mostrar que as acções de $SL_2(\mathbb{Z})$ em $\mathcal{P}$ e no plano hiperbólico são, num certo sentido, a mesma. Para isso, começamos por associar um número complexo τ no plano hiperbólico a uma forma quadrática definida positiva.

Definição 23. Seja $f(x,y) = ax^2 + bxy + cy^2 \in \mathcal{P}$. Definimos a seguinte correspondência

$$\tau : \mathcal{P} \longrightarrow \mathbb{H} : \qquad f \mapsto \tau_f = \frac{-b + \sqrt{D}}{2a}.$$

Dado que $\operatorname{Im} \tau_f = \frac{1}{i}\frac{\sqrt{D}}{2a} > 0$, τ_f está no plano hiperbólico $\mathbb{H}$. Note-se que $\tau_f = \tau_g$ se e só se f e g são ambas múltiplos inteiros da mesma forma primitiva.

Temos então o seguinte resultado.

Teorema 11. *A acção $\phi : SL_2(\mathbb{Z}) \times \mathcal{P} \to \mathcal{P}$ corresponde através da aplicação $\tau : \mathcal{P} \to \mathbb{H}$ à acção $F : SL_2(\mathbb{Z}) \times \mathbb{H} \to \mathbb{H}$. Isto significa que $F(\gamma, \tau_f) = \tau(\phi(\gamma, f)) = \tau_{\gamma(f)}$.*

Outra forma de enunciar este resultado é dizendo que o diagrama

$$\begin{tikzcd} \mathcal{P} \arrow[r, "\tau"] \arrow[d, "\gamma"'] & \mathbb{H} \arrow[d, "\gamma"] \\ \mathcal{P} \arrow[r, "\tau"'] & \mathbb{H} \end{tikzcd}$$

é comutativo para qualquer $\gamma \in SL_2(\mathbb{Z})$.

Demonstração. Deixamos a demonstração para o leitor, notando que basta prová-lo para os dois geradores S e T de $SL_2(\mathbb{Z})$, uma vez que F e ϕ são acções. □

Teorema 12. *Qualquer forma primitiva definida positiva é propriamente equivalente a uma e somente uma forma reduzida.*

Demonstração. Temos que mostrar que a órbita, por $SL_2(\mathbb{Z})$, de qualquer forma primitiva contém uma e uma só forma reduzida. A ideia da demonstração é verificar que a imagem, pela aplicação τ, de uma forma quadrática reduzida é a região $\mathcal{F}$ indicada na figura 3 (as linhas cheias pertencem ao conjunto, mas as tracejadas não).

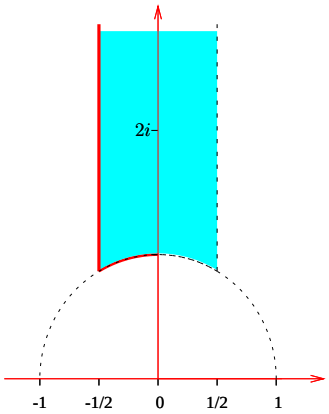

Figura 3: Região em $\mathbb{H}$ correspondente a formas reduzidas

Como a acção em $\mathcal{P}$ é equivalente à acção em $\mathbb{H}$ pelo teorema anterior, e a região $\mathcal{F}$ contém um e apenas um elemento de qualquer órbita de $SL_2(\mathbb{Z})$ em $\mathbb{H}$ (ver a Proposição 18 e o Exercício 24) o teorema ficará demonstrado. Consideremos então uma forma reduzida $f = (a, b, c)$ verificando $|b| < a < c$. A parte real de τ_f é $-\frac{b}{2a}$ e por isso, pertence a $]-\frac{1}{2}, \frac{1}{2}[$. Por outro lado, temos, $|\tau_f|^2 = \frac{b^2+(4ac-b^2)}{4a^2} = \frac{c}{a} > 1$ e portanto, τ_f está no interior de $\mathcal{F}$. Deixamos para o leitor a verificação de que os casos limite $b = -a$ e $c = a$, também têm $\tau_f \in \mathcal{F}$. □

Dada uma forma primitiva, a seguinte receita permite-nos obter a única forma reduzida que é propriamente equivalente a ela. Este resultado dá uma demonstração alternativa do teorema anterior.

PROPOSIÇÃO 24. *Se f é primitiva, obtém-se uma forma reduzida pela aplicação sucessiva (de um finito número) dos seguintes passos:*

1. *Se $c < a$ ou se ($a = c$ e $b < 0$), mudamos (a, b, c) para $(c, -b, a)$. Isto corresponde a actuar com a matriz* $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
2. *Se $|b| > a$, mudamos (a, b, c) para (a, b', c') onde $b' = b + 2ak$ e $c' = c + bk + ak^2$, para algum k tal que $|b'| \leq a$. Isto corresponde a actuar com a matriz* $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$.
3. *Se $b = -a$, mudamos (a, b, c) para (a, a, c). Isto corresponde a actuar com a matriz* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Exercício 30. Prove que este algoritmo termina e que dá sempre origem a uma forma reduzida.

Exemplo 18. Seja $f(x, y) = 458x^2 + 214xy + 25y^2$ que tem *discriminante* $D = -4$. A receita da proposição acima pode ser descrita pela seguinte tabela.

(a, b, c)	passo	novos valores	matriz
$(458, 214, 25)$	1	$(25, -214, 458)$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
$(25, -214, 458)$	2, com $k = 4$	$(25, -14, 2)$	$\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$
$(25, -14, 2)$	1	$(2, 14, 25)$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
$(2, 14, 25)$	2, com $k = -3$	$(2, 2, 1)$	$\begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}$
$(2, 2, 1)$	1	$(1, -2, 2)$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
$(1, -2, 2)$	2, com $k = 1$	$(1, 0, 1)$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Dado que $x^2 + y^2$ é representada por $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ e f por $\begin{pmatrix} 458 & 107 \\ 107 & 25 \end{pmatrix}$, de acordo com a tabela,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \gamma^t \begin{pmatrix} 458 & 107 \\ 107 & 25 \end{pmatrix} \gamma$$

onde γ é dado pela multiplicação das matrizes usadas antes:

$$\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 3 & 4 \\ -13 & -17 \end{pmatrix}.$$

Logo os números representados por f e por $x^2 + y^2$ são os mesmos!

Exercício 31. Determine as formas reduzidas equivalentes nos casos:

- $f = (5, 11, 7)$;
- $f = (5, -13, 9)$.

Vamos agora provar que para um dado valor D existe somente um número finito de formas reduzidas de discriminante D.

Definição 25. Denotamos o conjunto de classes de equivalência de formas reduzidas de discriminante D por $\mathcal{C}(D)$, e chamamos ao número $h(D) = \#\,\mathcal{C}(D)$, o número de classe de D.

Teorema 13. *Para qualquer inteiro $D < 0$, existe um número finito de formas reduzidas de discriminante D.*

Demonstração. Seja $ax^2 + bxy + cy^2$ uma forma reduzida de discriminante $D = b^2 - 4ac$. Logo $|b| \leq a \leq c$, e

$$-D = 4ac - b^2 \geq 4b^2 - b^2 = 3b^2 \geq 0. \tag{2}$$

Isto implica que $\sqrt{-\frac{D}{3}} \geq |b|$, e dado que $D + 4ac = b^2$, para D fixo, existe somente um número finito de possibilidades (a, b, c) para que $f = (a, b, c)$ seja uma forma reduzida de discriminante D. □

Podemos, por exemplo, calcular todas as formas reduzidas com $D = -4$.

Exemplo 19. Se $D = -4$ então por (2) temos $4 \geq 3a^2$. Portanto $a = 1$ ou $a = 0$. Como $a = 0$ não representa uma forma definida positiva, temos $a = 1$, $|b| \leq 1$ e $-4 = b^2 - 4c$, o que apenas tem $b = 0$ e $c = 1$ como solução. Concluímos então que $x^2 + y^2$ é a única forma reduzida de discriminante -4.

Exercício 32. Calcule todas as formas reduzidas com os seguintes discriminantes: $D = -3, -7, -8, -11, -12, -15, -16, -28$.

Esboçamos a prova do seguinte teorema. Seja n inteiro.

Teorema 14. *$h(-4n) = 1$ se e só se $n = 1, 2, 3, 4, 7$.*

Demonstração. [Landau] Para qualquer n a forma $x^2 + ny^2$ é reduzida. Para $n = 1, 2, 3, 4, 7$ o leitor pode verificar como no exemplo acima que esta é a única forma reduzida com discriminante $-4n$. Para provar que $h(-4n) > 1$ para outros n, indicaremos uma forma reduzida de discriminante $-4n$ que não é equivalente à apresentada acima.

- Se n não é um número primo, então $n = ac$, com $\gcd(a, c) = 1$ e $a < c$, logo nós podemos tomar
$$f(x, y) = ax^2 + cy^2 \text{ e } D = -4n.$$
- Se $n = 8$, tomamos
$$3x^2 + 2xy + 3y^2.$$
- Se $n = 2^r$ $r \geq 4$, tomamos
$$4x^2 + 4xy + (2^{r-2} + 1)y^2.$$

- Se $n = p^r$, com p ímpar dividimos os casos em:
  - se $n+1$ pode ser escrito como ac, com $\gcd(a,c) = 1$, tomamos
  $$ax^2 + 2xy + cy^2;$$
  - se $n+1 = 2^s$ com $s \geq 6$, tomamos
  $$8x^2 + 6xy + (2^{s-3}+1)y^2;$$
  - considerar os casos restantes $p = 3, 7, 31$ e $r = 1$.

□

Estamos a aproximar-nos de um dos nossos objectivos iniciais: saber quais os números representados por uma dada forma quadrática. Infelizmente, só o conseguiremos completar nos casos $h(D) = 1$, onde D é o discriminante da forma.

Lema 26. *Uma forma $f(x,y)$ representa propriamente m se e só se f é propriamente equivalente a*

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

para certos inteiros b e c.

Demonstração. Se f é propriamente equivalente a g como acima, g representa m propriamente, pois basta tomar $(x,y) = (1,0)$; então f também representa m propriamente (note que se $\gamma(f) = g$, com $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, vem $f(p,r) = m$). Reciprocamente, seja $f(p,q) = m$ com $\gcd(p,q) = 1$. Então existem $r, s \in \mathbb{Z}$ tais que $ps - rq = 1$, logo $\det \begin{pmatrix} p & q \\ r & s \end{pmatrix} = 1$. Um cálculo mostra que

$$f(px+ry, qx+sy) = f(p,q)x^2 + (2apr + bps + brq + 2cqs)xy + f(r,s)y^2,$$

o que implica que f é propriamente equivalente a g da forma pretendida. □

Note-se que temos sempre $D = b^2 - 4ac \equiv 0, 1 \mod 4$, dado que $b^2 \equiv 0, 1 \mod 4$.

Lema 27. *Seja $D \equiv 0, 1 \mod 4$, e $m > 2$ um número primo. Então m é propriamente representável por uma forma primitiva de discriminante D se e só se D é um resíduo quadrático módulo m.*

Demonstração. Se m é propriamente representável por f, então, pelo lema anterior, podemos assumir que é da forma $f(x,y) = mx^2 + bxy + cy^2$, e vem $D = b^2 - 4mc \equiv b^2 \mod m$. Logo D é um resíduo quadrático módulo m. Reciprocamente, se D é um resíduo quadrático módulo m, então $D \equiv d^2 \mod m$ para um certo d. Isto implica que $D \equiv b^2 \mod 4m$, onde $b = d$ se $D \equiv d^2 \mod 4$, ou $b = d + m$ caso contrário. Portanto, $D = b^2 - 4mc$ para algum $c \in \mathbb{Z}$. Assim, a forma $mx^2 + bxy + cy^2$ é primitiva pois m é primo, tem discriminante D e representa m propriamente. □

As seguintes são consequências imediatas dos lemas acima.

Corolário 3. *Seja n um inteiro e p um primo ímpar que não divide n. Então $\left(\frac{-4n}{p}\right) = 1$ se e só se p é representado por uma forma primitiva de discriminante $-4n$.*

Como consequência, obtemos uma nova prova do teorema de Fermat.

Corolário 4. *Se p é um primo ímpar, $p = x^2 + y^2$ se e só se $p \equiv 1 \mod 4$.*

Demonstração. Se $p \equiv 1 \mod 4$ então temos, pelo Exercício 17, que $\left(\frac{-1}{p}\right) = 1$. Como 4 é um quadrado, temos também $\left(\frac{-4}{p}\right) = 1$. O corolário anterior diz-nos então que p é representado por uma forma primitiva de discriminante -4. Mas a única forma reduzida de discriminante -4 é $x^2 + y^2$ (ver Exemplo 19). □

Corolário 5. *Seja $h(-4n) = 1$ e $p \nmid n$. Então $\left(\frac{-n}{p}\right) = 1$ se e só se $p = x^2 + ny^2$.*

Exemplo 20. Pelo corolário acima $x^2 + 2y^2 = p$, para um primo $p \neq 2$, se e só se $\left(\frac{-8}{p}\right) = 1$. Mas, pelo Exercício 17, isto é equivalente a

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

Logo $\frac{p-1}{2} + \frac{p^2-1}{8}$ tem que ser par, o que significa que 16 divide $4(p-1) + (p^2 - 1) = (p-1)(4+p+1)$. Qualquer primo ímpar é de uma das seguintes formas $8k+1, 8k+3, 8k+5, 8k+7$. Agora é fácil verificar que

$$p = x^2 + 2y^2 \quad \Leftrightarrow \quad p \equiv 1 \text{ ou } 3 \mod 8.$$

Exercício 33. Faça o mesmo para $x^2 + Dy^2$, onde $D = 3, 4, 7$.

Exemplo 21. Vejamos para que primos p se tem $\left(\frac{-20}{p}\right) = 1$. Usando a reciprocidade quadrática e o Exercício 17

$$\left(\frac{-20}{p}\right) = \left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right).$$

Para que $(-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right)$ tome o valor 1 necessitamos que seja $p \equiv 1 \mod 4$ e $\left(\frac{p}{5}\right) = 1$ ou $p \equiv 3 \mod 4$ e $\left(\frac{p}{5}\right) = -1$.

Podemos facilmente verificar que os resíduos quadráticos módulo 5 são apenas $0, 1, 4 (\mod 5)$, e logo os resíduos não-quadráticos são dados por $2, 3 (\mod 5)$. Assim estamos à procura dos números que verificam uma das condições:

- $p \equiv 1 \mod 4$ e $p \equiv 0, 1, 4 \mod 5$;
- $p \equiv 3 \mod 4$ e $p \equiv 2, 3 \mod 5$.

O leitor pode facilmente verificar, usando o teorema chinês dos restos (Teorema 4), que fora $p = 5$, estes primos são exactamente aqueles para os quais $p \equiv 1, 3, 7, 9 \mod 20$.

Podemos também mostrar que $h(-20) = 2$ e que as duas formas reduzidas primitivas com discriminante -20 são

$$x^2 + 5y^2 \qquad \text{e} \qquad 2x^2 + 2xy + 3y^2.$$

É fácil verificar que só a forma $x^2 + 5y^2$ pode representar os números congruentes com $1, 9 \mod 20$ e que só a forma $2x^2 + 2xy + 3y^2$ pode representar os números congruentes com $3, 7 \mod 20$. Portanto, temos o seguinte:

- $p = x^2 + 5y^2 \Leftrightarrow p \equiv 1, 9 \mod 20$.
- $p = 2x^2 + 2xy + 3y^2 \Leftrightarrow p \equiv 3, 7 \mod 20$.

Contudo as congruências não permitem resolver o problema da representabilidade em todos os casos. Além disso, existem formas que representam exactamente os mesmos inteiros e que não são equivalentes.

Exercício 34. Prove que as formas $2x^2+xy+3y^2$ e $2x^2-xy+3y^2$ representam os mesmos números, mas não são equivalentes.

Aqui ficam os últimos exercícios.

Exercício 35. Quais os $n \in \mathbb{N}$ que verificam $x^2 + 5y^2 = n$, com x, y inteiros?

Exercício 36. Encontre os primos p que podem ser escritos como $x^2 + 8y^2$. E que naturais n podem ser escritos da mesma forma?

A teoria da representabilidade de formas quadráticas está ainda activa e recentemente conduziu a alguns resultados notáveis. Por exemplo, J. H. Conway e W. Schneeberger provaram em 1993 que, para uma forma quadrática definida positiva (com qualquer número de variáveis) dada por uma matriz com entradas inteiras (como observado acima, no caso de formas a duas variáveis $ax^2 + bxy + cy^2$, isto significa que b é par) representar qualquer inteiro positivo, é suficiente que ela represente qualquer inteiro de 1 a 15. Este é o chamado *teorema-15* (consulte, por exemplo, [C2]). Em 1999, M. Bhargava descobriu uma demonstração mais simples deste resultado [B]. Em 2005, ele foi mais longe e provou, em conjunto com J. Hanke, o *teorema-290*. Este resultado diz que uma forma quadrática definida positiva com coeficientes inteiros representa qualquer inteiro positivo se representar qualquer inteiro de 1 a 290 (de facto, basta que represente somente determinados 29 destes números).

Como estas notas estão agora a chegar ao fim, deixaremos o leitor com alguns problemas para pensar.

Problema 3. Prove que não existem formas quadráticas em duas variáveis que representam todos os inteiros positivos. O mesmo é verdade para três variáveis.

Problema 4. Existe alguma solução para $x^2 - 3y^2 = 10$? Mais geralmente, em que hipóteses se pode resolver $x^2 - Dy^2 = n$?

Problema 5. Consegue descobrir os números n tais que $x^3 + y^3 = n$?

Divirtam-se!...

Referências

[B] M. Bhargava, *On Conway-Schneeberger fifteen theorem*, in Quadratic Forms and their Applications (Dublin, 1999), 27–37, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000.

[C1] J. H. Conway, *The sensual quadratic form*, Carus Mathematical Monographs, The Mathematical Association of America, 1997.

[C2] J. H. Conway, *Universal quadratic forms and the fifteen theorem*, in Quadratic Forms and their Applications (Dublin, 1999), 23–26, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000.

[IR] K. Ireland e M. Rosen, A Classical Introduction to Modern Number Theory, Second Edition, Springer Verlag, 1990.

[K] Hua Loo Keng, Introduction to Number Theory, Springer Verlag, 1982.

[MT] S. J. Miller, R. Takloo-Bighash, An Invitation to Modern Number Theory, Princeton U. P., 2006.

[R] J. G. Ratcliffe, Foundations of Hyperbolic Manifolds, Springer Verlag GTM 149, 1994.

[ST] I. Stewart and D. Tall, Algebraic Number Theory, Chapman & Hall, 1987.