Licenciatura em Matemática
Departamento de Matemática
Universidade do Minho

Apontamentos de teoria de números

Assis Azevedo

Ano lectivo 2008/2009

Conteúdo

0. Exercícios de Revisão

Neste capítulo apresento alguns exercícios elementares (no sentido em que usam poucos conhecimentos para a sua resolução) mas que podem ser de resolução não trivial.

Começamos com duas igualdades que nos dão um método de factorizar somas ou diferenças de potências com o mesmo expoente.

$$\forall a,b \in \mathbb{R} \quad \begin{cases} a^n - b^n &= (a-b)\left(\displaystyle\sum_{i=0}^{n-1} a^{n-1-i}b^i\right) \\ a^n + b^n &= (a+b)\left(\displaystyle\sum_{i=0}^{n-1} (-1)^i a^{n-1-i}b^i\right) \quad \text{se } n \text{ é ímpar.} \end{cases}$$

Note-se que se $n = 2$ a primeira igualdade reduz-se a um dos chamados casos notáveis: $a^2 - b^2 = (a-b)(a+b)$.

A demonstração da primeira das igualdades (por exemplo) pode ser feita facilmente usando os seguintes passos,

$$\begin{aligned} (a-b)\left(\sum_{i=0}^{n-1} a^{n-1-i}b^i\right) &= a\left(\sum_{i=0}^{n-1} a^{n-1-i}b^i\right) - b\left(\sum_{i=0}^{n-1} a^{n-1-i}b^i\right) \\ &= \left(\sum_{i=0}^{n-1} a^{n-i}b^i\right) - \left(\sum_{i=0}^{n-1} a^{n-1-i}b^{i+1}\right) \\ &= \left(\sum_{i=0}^{n-1} a^{n-i}b^i\right) - \left(\sum_{i=1}^{n} a^{n-i}b^i\right) \;=\; a^n - b^n. \end{aligned}$$

Os seguintes exercícios podem ser resolvidos aplicando estas igualdades.

---

1. *Mostre que, se* $a, b \in \mathbb{Z}$, *então* $a^4 - b^4$ *não é um número primo.*

2. *Encontre um divisor primo de:* $2^{30} + 1$; $2^{40} + 1$; $2^{36} + 1$.

3. *Factorize os números:* $10^6 - 1$; $2^{24} - 1$; $10^8 - 1$; ; $2^{15} - 1$.

4. *Sejam* $a, b, n, m \in \mathbb{N}$. *Mostre que*

   a) *se* $a > 1$ *e* $a^n + 1$ *é primo então* n *é uma potência de* 2;

   b) *se* $a^n - 1$ *é primo então* $a = 2$ *e* n *é primo;*

   c) *se* $a^n + b^m$ *é primo então* (n, m) *é uma potência de* 2.

5. *Mostre que* $2^{2^m} - 1$ *tem pelo menos* m *factores primos distintos.*

O exercício 4. leva-nos à apresentação dos números de Fermat e de Mersenne.

- Um número da forma $2^n + 1$, com $n \in \mathbb{N}$, diz-se um **número de Fermat** (sec. XVII). Do exercício 4.a) podemos concluir que se um número de Fermat é primo então é necessariamente da forma $2^{2^m} + 1$ para algum $m \in \mathbb{N}$. Fermat conjecturou que os números desta forma são todos primos. Euler em 1732 mostrou que os factores de $F_m = 2^{2^m} + 1$, com $m > 2$ são necessariamente da forma $k2^{m+2} + 1$. Depois disto bastou-lhe fazer duas tentativas para encontrar um divisor próprio de F_5, a saber, 641.

  O teste mais conhecido para testar a primalidade de um número de Fermat é o chamado teste de Pepin: F_m é primo se e só se $3^{\frac{F_m - 1}{2}} \equiv -1 \pmod{F_m}$.

  Não se conhece nenhum número primo de Fermat para $m > 4$. O maior número de Fermat que se sabe ser composto é o correspondente a $m = 11\,602\,478\,782$. A pagina **http://www.prothsearch.net/fermat.html** tem informação actualizada sobre os números de Fermat.

- Um número primo diz-se um **primo de Mersenne** se for da forma $2^n - 1$. Do exercício 4. b) podemos concluir que n tem de ser primo. Os 4 maiores primos

conhecidos são primos de Mersenne, tendo o maior deles, $2^{25964951}-1$, 7816230 dígitos. Não se sabe também se existe uma infinidade primos de Mersenne. A pagina **http://www.mersenne.org/** tem informação actualizada sobre estes números.

De seguida vejamos alguns resultados simples sobre a distribuição dos números primos. Os dois primeiros resultados podem entrar como primeiros passos na pesquisa de divisores de um dado número. Vamos denotar por $\mathbb{P}$ o conjunto dos números primos.

---

1. *Mostre que, se o menor factor primo do inteiro positivo n é maior que $\sqrt{n}$, então n é primo ou 1.*

2. *Mostre que, se o menor factor primo p do inteiro positivo n é maior que $\sqrt[3]{n}$, então n/p é primo ou 1.*

3. *Mostre que, se $p \in \mathbb{N}$ e p, $p+2$ e $p+4$ são primos, então $p = 3$.*

   Nota: *Não se sabe se existe uma infinidade de pares $(p, p+2)$ tais que p e $p+2$ são números primos. Estes pares de primos dizem-se* **primos gémeos**. *Como exemplos temos: $(3,5)$, $(5,7)$, $(5,7)$, $(11,13)$ e $(17,19)$. Sabe-se que, tirando o par $(3,5)$ todos os outros pares de primos gémeos são da forma $(6n-1, 6n+1)$. Apesar de não se saber se existe uma infinidade de pares de primos gémeos sabe-se que*

   $$\sum_{(p,p+2)\in\mathbb{P}^2} \frac{1}{p} \qquad \textit{é convergente.}$$

   Compare este resultado com alínea c) do exercício 7,

4. *Mostre que os termos de uma progressão aritmética de razão positiva não podem ser todos primos.*

   Nota: *O chamado teorema de Dirichlet diz que numa progressão aritmética se o primeiro termo (ou outro qualquer) e a razão forem números inteiros primos entre si então nessa progressão aritmética existe uma infinidade de números primos.*

5. *Seja $n > 2$ e p um divisor primo de $n! - 1$. Mostre que $p \geq n$. Conclua que existe uma infinidade de números primos.*

   Nota: *Este é essencialmente o raciocínio de Euclides (século IV e III antes de Cristo).*

6. *Seja $n \in \mathbb{N}$. Mostre $(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$ são n inteiros compostos consecutivos.*

   Nota: *Daqui resulta que dois números primos consecutivos podem estar tão distante um do outro quanto se queira.*

7. *Mostre que:*

   a) $x \geq -\frac{1}{2}\log(1-x)$ *se* $x \in]0, \frac{1}{2}]$;

   b) $$\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p}} = \prod_{p\in\mathbb{P}} \left(\sum_{i=0}^{\infty} \frac{1}{p^i} \right) = \sum_{n=1}^{\infty} \frac{1}{n};$$

   c) $\displaystyle\sum_{p\in\mathbb{P}}^{\infty} \frac{1}{p}$ *é uma série divergente. (use a), para* $x = \frac{1}{p}$, *e b)).*

   Nota: *Este resultado contrabalança o resultado anterior, dizendo que no global os números primos não estão muito separados uns dos outros. Este resultado, como muitos em teoria elementar dos números, foi demonstrado por Leonhard* **Euler** *que viveu de* 15 *de Abril de* 1707 *a* 18 *de Setembro de* 1783.

Os próximos exercícios usam apenas alguma manipulação algébrica. Em alguns procuramos factorizar algumas expressões. No exercício 5 (por exemplo) podemos analisar os diversos casos consoante o resto da divisão dos inteiros em questão por 6. Nos exercícios 6, 7, 8 e 9 podemos usar um raciocínio semelhante.

---

1. *Prove que $n^4 + 4$ não é primo se $n > 1$.*

2. *Para que inteiros n positivos é $n^4 + 4^n$ primo?*

3. *Mostre que, se m é uma soma de dois quadrados, então $2m$ é também uma soma de dois quadrados.*

4. *Se $n \in \mathbb{N}$, $10^{2n+1} - 10^{2n} - 10^{n+1} + 4 \cdot 10^n + 1$ é um quadrado perfeito?*

5. *Mostre que, se 6 divide a soma de três inteiros então também divide a soma dos cubos desses inteiros.*

6. *Mostre que, $a, b, c \in \mathbb{N}$ e 9 divide $a^3 + b^3 + c^3$ então a, b ou c é múltiplo de 3.*

7. *Sejam $a, b, c \in \mathbb{N}$ tais que c é ímpar e $a^2 + 2b^2 = 2c$. Mostre que a é par e b é ímpar.*

8. *Mostre que se um número é soma de 2 quadrados inteiros então o resto da sua divisão por 4 não é 3.*

9. *Mostre que se um número é soma de 3 quadrados inteiros então o resto da sua divisão por 8 não é 7.*

   Nota: *Qualquer número inteiro é a soma de 4 quadrados.*

10. *Para que valores de $a, b, c \in \mathbb{R}$ se tem a igualdade $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = \frac{1}{a+b+c}$?*

11. *Determine todos os pares $(a, b) \in \mathbb{R}^2$ tais que*

$$a, b, ab, a^2 + b$$

    estejam em progressão aritmética.

12. *Calcule todos os ternos $(a, b, c) \in \mathbb{R}^3$ tais que a, b, c estão em sucessão aritmética e $a - 1, b - 1, c + 1$ em progressão geométrica.*

13. *Quais os valores de $a, x, y \in \mathbb{N}$, para os quais $x^2 + y^2 = axy$?*

14. *Mostre que, se $a, b \in \mathbb{N}$, então $a!b!$ divide $(a + b)!$.*

15. *Mostre que, se p é um número primo e $1 \leq k < p$ então $\binom{p}{k}$ é múltiplo de p.*

16. *Sejam m, n inteiros primos entre si e maiores que 1. Mostre que*

$$\sum_{k=1}^{n-1} \left[\frac{mk}{n}\right] = \frac{(m-1)(n-1)}{2}.$$

Sugestão: *Calcule $\left[\frac{mk}{n}\right] + \left[\frac{m(n-k)}{n}\right]$, para $k \in \{1, \ldots, n-1\}$.*

17. *Para que valores de $n \in \mathbb{N}$,*

$$\sum_{j=1}^{n} j \quad \textit{divide} \quad \prod_{j=1}^{n} j.$$

Os dois próximos exercícios são relativos à chamada série harmónica. O primeiro mostra que a sucessão $(S_n)_{n\in\mathbb{N}}$ das somas parciais da série só é um número inteiro se $n = 1$. E o segundo refere-se às chamadas **fracções egípcias**, que são as somas de elementos diferentes da série harmónica. O exercício 2 fornece um algoritmo para escrever um número racional como fracção egípcia.

---

1. *Sejam $n \in \mathbb{N}$ e k a maior potência de 2 menor ou igual a n.*

   a) *Mostre que não existe $a \in \mathbb{N}$ tal que $a < n$, $a \neq 2^k$ e $2^k | a$.*

   b) *Conclua que $1 + \frac{1}{2} + \cdots + \frac{1}{n}$ não é um inteiro.*

2. a) *Mostre que, se $n \in \mathbb{N}$ então $\frac{1}{n} = \frac{1}{n+1} + \frac{1}{n(n+1)}$.*

   b) *Mostre que todo o número racional positivo é soma de um número finito de termos (não necessariamente seguidos) da série harmónica.*

   Nota: *Usando o algoritmo referido acima*

$$\frac{2}{3} \;=\; \frac{1}{3} + \frac{1}{3} \;=\; \frac{1}{3} + \frac{1}{4} + \frac{1}{12}.$$

   Mas existe uma decomposição "mais simples": $\frac{2}{3} = \frac{1}{2} + \frac{1}{6}$.

Os próximos exercícios podem ser resolvidos procurando uma fórmula de recorrência.

1. *Considere n rectas no plano tais que: duas quaisquer delas são concorrentes; não existem três delas que se intersectem num mesmo ponto.*

   Em quantas regiões "fica o plano dividido"?

2. *Seja D a região aberta delimitada por duas rectas paralelas. Considere m pontos, $A_1, \ldots, A_m$, numa das rectas e n pontos, $B_1, \ldots, B_n$ na outra. Para $i \in \{1, 2, \ldots, m\}$ e $j \in \{1, 2, \ldots, n\}$ considere a recta $r_{i,j}$, definida pelos pontos A_i e B_j. Suponha ainda que destas (nm) rectas, não existem três que se intersectem num mesmo ponto de D.*

   Quantos são os pontos de intersecção das rectas acima definidas que pertencem a D?

Vejamos exemplos que podem ter algum cariz computacional. O primeiro desses exemplos é relativa à chamada conjectura de Collatz.

Há muita literatura sobre esta conjectura e generalizações. Dois exemplos:

- na página http://www.numbertheory.org/php/collatz.html pode fazer algumas experiências.
- na página http://math.scranton.edu/monks/software/Collatz/Collatz.html pode encontrar rotinas para o Maple para o estudo desta conjectura.

1. *Considere a função T definida por* $T : \mathbb{Z} \longrightarrow \mathbb{Z}$.

$$n \mapsto \begin{cases} \frac{n}{2} & \text{se } n \text{ é par} \\ \frac{3n+1}{2} & \text{se } n \text{ é ímpar} \end{cases}$$

   Para cada $k \in \mathbb{Z}$, podemos criar a sucessão $(T^n(k))_{n \in \mathbb{N}_0}$ em que $T^0(k) = k$ e $T^m(k) = T(T^{m-1}(k))$ se $m \in \mathbb{N}$.

   Por exemplo, para $k = 7$, definimos a sucessão:

$$7,\ 11,\ 17,\ 26,\ 13,\ 20,\ 10,\ 5,\ 8,\ 4,\ 2,\ 1,\ 2,\ 1,\ 2,\ \ldots$$

A conjectura de Collatz afirma que, se $k \in \mathbb{Z}$ então a sucessão $(T^n(k))_{n\in\mathbb{N}}$, obtida por aplicação sucessiva de T a k atinge o número 1, se $k > 0$, um dos números -1, -5 ou -17, se $k < 0$, entrando depois em ciclo.

a) *Encontre a sucessão obtida a partir de $n = 29$.*

b) *Mostre que a sucessão obtida para $n = (2^k - 1)/3$, onde k é um inteiro positivo par, atinge o inteiro 1.*

2. *Uma expansão de Cantor de um inteiro positivo n é*

$$n = a_m m! + a_{m-1}(m-1)! + \cdots + a_2 2! + a_1 1!$$

onde a_j é um inteiro com $0 \leq a_j \leq j$.

a) *Determine uma expansão de Cantor de 14, 56 e 384.*

b) *Mostre que, dado $n \in \mathbb{N}$ existe uma e uma só expansão de Cantor para n.*

3. *Seja $S \subseteq \{1, 2, \ldots, 2n\}$ tal que*

$$\forall a, b \in S \quad [\ a|b \Rightarrow a = b\ ].$$

a) *Faça $n = 6$ e encontre os subconjuntos de $\{1, 2, \ldots, 12\}$ que satisfazem a condição acima.*

b) *Para $n \in \mathbb{N}$, qual o maior número possível de elementos que S pode ter?*

4. *Seja $n \in \mathbb{N}$ e considere n inteiros (não necessariamente distintos). Mostre que existe uma escolha de alguns deles cuja soma é múltipla de n.*

De seguida vamos aplicar alguns (poucos) conhecimentos de análise diferencial para o cálculo de algumas somas finitas. Estamos a pensar em somas do tipo

$$\sum_{k=1}^{n} p(k)\, x^k$$

em que $p(k)$ é um polinómio.

A ideia é muito simples. Começamos por escrever $p(k)$ como combinação linear de polinómios da forma k, $k(k-1)$, $k(k-1)(k-2)$ etc..

Suponhamos que $p(k) = A_1\,k + A_2\,k(k-1) + \cdots$. Deste modo

$$\begin{aligned}
\sum_{k=1}^{n} p(k)\,x^k &= \sum_{k=1}^{n} \left[A_1\,k + A_2\,k(k-1) + \cdots\right] x^k \\
&= \sum_{k=1}^{n} A_1\,k\,x^k + \sum_{k=1}^{n} A_2\,k(k-1)\,x^k + \cdots \\
&= A_1\,x \sum_{k=1}^{n} k\,x^{k-1} + A_2\,x^2 \sum_{k=1}^{n} k(k-1)\,x^{k-2} + \cdots \\
&= A_1\,x \sum_{k=1}^{n} k\,x^{k-1} + A_2\,x^2 \sum_{k=2}^{n} k(k-1)\,x^{k-2} + \cdots
\end{aligned}$$

Resta-nos então saber calcular expressões "fechadas" para as somas

$$\sum_{k=1}^{n} k\,x^k, \qquad \sum_{k=2}^{n} k(k-1)\,x^{k-1}, \qquad \sum_{k=3}^{n} k(k-1)(k-2)\,x^{k-2}, \cdots$$

ou seja, para as somas (com a notação usual para as derivadas)

$$\left(\sum_{k=0}^{n} x^k\right)', \qquad \left(\sum_{k=0}^{n} x^k\right)'', \qquad \left(\sum_{k=0}^{n} x^k\right)''', \cdots$$

Uma vez que, se $x \neq 1$, $\displaystyle\sum_{k=0}^{n} x^k = \frac{x^{n+1}-1}{x-1}$, podemos concluir que, para $x \neq 1$,

$$\begin{aligned}
\sum_{k=1}^{n} k x^{k-1} &= \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2} \\
\sum_{k=2}^{n} k(k-1)x^{k-2} &= \frac{(n-n^2)x^{n+1} + 2(n^2-1)x^n - (n^2+n)x^{n-1} + 2}{(x-1)^3} \\
&\vdots
\end{aligned}$$

Note-se ainda que se $x = 1$ podemos aplicar limites.

Como exemplo vamos calcular $\sum_{k=1}^{n+2} \frac{5k}{4^k}$.

Note-se que esta soma é é igual a $f(\frac{1}{4})$ em que $f: \mathbb{R} \longrightarrow \mathbb{R}.$

$$x \mapsto \sum_{k=1}^{n} 5k\, x^k$$

Deste modo, se $x \neq 1$,

$$f(x) = 5x \sum_{k=1}^{n} k\, x^{k-1} = 5x\, \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2} \quad \text{pelo que vimos acima.}$$

Em particular

$$f(\frac{1}{4}) = \frac{5}{4}\, \frac{\frac{n}{4^{n+1}} - \frac{n+1}{4^n} + 1}{\frac{3^2}{4^2}} = \frac{5(4^{n+1} - 3\,n - 4)}{9 \cdot 4^{n+1}}$$

---

1. *Calcule, usando eventualmente os métodos referidos acima,*

   a) $\sum_{k=1}^{n} k10^{k-1}$; b) $\sum_{k=1}^{n+2} \frac{5k+3}{4^k}$;

   c) $\sum_{k=1}^{n} \frac{2k^2 - 3k}{4^k}$; d) $\sum_{k=1}^{n} \frac{2k + 3^{k-1}}{5^k}$;

   e) $\sum_{k=1}^{n} \frac{k^2 3^k}{5^{k+1}}$; f) $\sum_{k=0}^{n} \frac{\binom{n}{k}}{(k+1)2^{k+1}}$.

1. Preliminares

Neste capítulo vamos recordar a definição dos anéis $< \mathbb{Z}_n, +_n, \cdot_n >$, com $n \in \mathbb{N}$. Como curiosidade falaremos dos critérios de divisibilidade por 9 e por 11 e do chamado calendário gregoriano. Serão também recordadas algumas propriedades do máximo divisor comum e do mínimo múltiplo comum de inteiros.

Finalizaremos com alguns resultados relacionados com a noções de ordem de um elemento de um grupo abstracto.

No que segue, m, n, k, m_1, n_1, etc. representam inteiros positivos e $a, b, c, l, r, s, x_k, y_k$, etc. representam números inteiros.

1.1 Anel dos inteiros módulo n

Vamos "recordar" duas apresentações do anel dos inteiros módulo n, que representaremos por $\mathbb{Z}_n$.

Primeira definição:
Consideremos, sobre o anel $< \mathbb{Z}, +, \cdot >$, a relação binária $\equiv_n$ definida por:

$$a \equiv_n b \iff n | a - b. \qquad \text{(lê-se "}a \text{ congruente com } b \text{ módulo } n\text{")}$$

Verifique que se trata de facto de uma congruência e que o anel quociente $\mathbb{Z}/\equiv_n$ tem n elementos: $[0]_n, [1]_n, \ldots, [n-1]_n$ (em que $[i]_n$ representa a classe de equivalência de i).

Escreveremos também $a \equiv b \pmod{n}$ em vez de $a \equiv_n b$

Segunda definição:

Consideremos sobre o conjunto $\{0, 1, \ldots, n-1\}$ as operações $+_n$ e $\cdot_n$ definidas por:

$$a +_n b = \text{resto da divisão de } a + b \text{ por } n;$$

$$a \cdot_n b = \text{resto da divisão de } a \cdot b \text{ por } n.$$

Verifique que $< \{0, 1, \ldots, n-1\}, +_n, \cdot_n >$ é um anel.

Proposição 1.1 *Se $n \in \mathbb{N}$ então o anel $< \{0, 1, \ldots, n-1\}, +_n, \cdot_n >$ é isomorfo ao anel $< \mathbb{Z}, +, \cdot > / \equiv_n$.*

Demonstração: Note-se que a função $\Phi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & < \{0, 1, \ldots, n-1 > \\ m & \mapsto & \text{resto da divisão de } m \text{ por } n \end{array}$ é um homomorfismo de anel (verifique!), sobrejectivo e tal que

$$\forall a, b \in \mathbb{N} : \ [\ \Phi(a) = \Phi(b) \iff a \equiv_n b\,].$$

A conclusão segue do teorema fundamental do homomorfismo para anéis. ■

Atendendo a este resultado usaremos indistintamente as duas definições para o anel dos inteiros módulo n.

1.1.1 Critério de divisibilidade por 2, 3, 4, 5, 8, 9 e por 11

Consideremos um número inteiro $n = (a_k \cdots a_1 a_0)_{10}$ escrito na base 10. Isto significa que

$$n \ = \ a_0 + a_1 \times 10 + \cdots + a_k \times 10^k.$$

Observe-se que

$$10 \ \equiv \ \begin{cases} 0 \pmod 2 \\ 0 \pmod 5 \\ 1 \pmod 3 \\ 1 \pmod 9 \\ -1 \pmod{11} \end{cases}$$

Uma vez que estamos na presença de congruências, podemos concluir que, se $k \in \mathbb{N}$,

$$10^k \equiv \begin{cases} 0 \ (\mathrm{mod}\ 2) \\ 0 \ (\mathrm{mod}\ 5) \\ 1 \ (\mathrm{mod}\ 3) \\ 1 \ (\mathrm{mod}\ 9) \\ 1 \ (\mathrm{mod}\ 11) \text{ se } k \text{ é par} \\ -1 \ (\mathrm{mod}\ 11) \text{ se } k \text{ é ímpar.} \end{cases}$$

Por outro lado, $10^k \equiv 0 \pmod{2^k}$, se $k \geq 2$. Deste modo,

$$n = a_0 + a_1 \times 10 + \cdots + a_k \times 10^k \equiv \begin{cases} a_0 & (\mathrm{mod}\ 2) \\ a_0 & (\mathrm{mod}\ 5) \\ a_0 + a_1 & (\mathrm{mod}\ 4) \\ a_0 + a_1 + a_2 & (\mathrm{mod}\ 8) \\ a_0 + a_1 + \cdots + a_k & (\mathrm{mod}\ 3) \\ a_0 + a_1 + \cdots + a_k & (\mathrm{mod}\ 9) \\ a_0 - a_1 + \cdots + (-1)^k a_k & (\mathrm{mod}\ 11). \end{cases}$$

Em particular o resto da divisão de n por 9 ou por 3 é igual ao resto da divisão de $a_0 + a_1 + \cdots + a_k$ por 9 ou por 3, o que justifica a chamada "prova dos nove".

Podemos generalizar este resultado na parte que diz respeito ao 9 e ao 11.

Proposição 1.2 *Seja $b \in \mathbb{N} \setminus \{1\}$. Seja $n = (a_k \cdots a_1 a_0)_b$ um número inteiro escrito na base b. Então*

$$\begin{aligned} n &\equiv a_0 + a_1 + \cdots + a_k \ (\mathrm{mod}\ b-1), \\ n &\equiv a_0 - a_1 + \cdots + (-1)^k a_k \ (\mathrm{mod}\ b+1). \end{aligned}$$

■

1.1.2 Calendário gregoriano

Um ano terrestre é o tempo que a Terra demora a fazer uma órbita completa em torno do Sol. Sabe-se hoje que um ano é aproximadamente igual a $365,2422$ dias.

No calendário actual convencionou-se que o ano x seria um ano comum (isto é, com 365 dias) se

$$4 \nmid x \text{ ou } (100 \mid x \text{ e } 400 \nmid x).$$

Os outros anos seriam os anos bissextos (com 366 dias). O dia "extra" é sempre o dia 29 de Fevereiro.

Assim, os anos 1900, 1998, 1999, 2001 e 2100 não são bissextos, mas os anos 1904, 1996, 2000 e 2400 são bissextos.

Deste modo, em cada 400 anos consecutivos existem 97 anos bissextos o que implica que esses 400 anos têm 146097 ($= 365 \times 400 + 97$) dias, ou seja uma média de $365,2425$ dias/ano. Deste modo, em cada 10 000 anos o calendário (como definido actualmente) tem um erro de aproximadamente 3 dias em relação ao calendário real.

Daqui se reconhece que de algum modo: o ano deveria começar a 01 de Março (o que até não seria original); o ciclo dos 400 anos deveria começar a 01 de Março de algum ano que fosse múltiplo de 400.

Questão: Que dia de semana serão os dias: 02 de Outubro de 2006 e 13 de Janeiro de 3321?

Se hoje, 02 de Outubro de 2005, é domingo, então o dia 02 de Outubro de 2006 será uma segunda-feira, porque terão passado 365 dias e $365 = 52 \times 7 + 1$, isto é 52 semanas mais 1 dia.

Pelas razões invocadas atrás, para calcularmos os dias de semana de dias do futuro ou do passado é bom saber que o dia 1 de Março de 2000 foi uma quarta-feira.

Usemos a seguinte notação: o dia x do mês y do ano z será denotado por dia $x/(y-2)/z$, se $y \geq 3$, por $x/(y+10)/z-1$ se $y < 3$. Por exemplo, o dia 7 de Julho de 7777 denota-se por 7/5/7777 e o dia 13 de Janeiro de 3321 denota-se por 13/10/3320. Estamos a usar o dia 1 de Março como o primeiro dia do ano.

Com esta notação, o número de dias que vai de 1 de Março de 2000 (dia 1/1/2000) até 1 de Março de 3321 (dia 1/1/3321) é:

$$365 \times 1321 + \underbrace{\left[\frac{1321}{4}\right] - \left[\frac{1321}{100}\right] + \left[\frac{1321}{400}\right]}_{\text{número de dias 29 de Fevereiro}} .$$

Por outro lado, o número de dias que vai de 1 de Março de 3321 até 13 de Janeiro de 3321 é:

$$31 + 30 + 31 + 30 + 31 + 31 + 30 + 31 + 30 + 31 + 12.$$

Assim, se n é o número de dias que vai de 1 de Março de 2000 até o dia 13 de Janeiro de 3321, então

$$\begin{aligned} n &= 365 \times 1321 + 330 - 13 + 3 \\ &\quad +31 + 30 + 31 + 30 + 31 + 31 + 30 + 31 + 30 + 31 + 12 \\ &\equiv 1 \times 5 + 1 - 6 + 3 + 3 + 2 + 3 + 2 + 3 + 3 + 2 + 3 + 2 + 3 + 5 \ (\mod 7) \\ &\equiv 6 \ (\mod 7). \end{aligned}$$

(note-se que não interessa fazer as contas dos dias que passaram, mas sim fazer as contas módulo 7.)

Conclusão, uma vez que o dia 1 de Março de 2000 foi uma quarta-feira, o dia 13 de Janeiro de 3321 será uma terça-feira.

Se quisermos andar para trás no tempo e quisermos saber, por exemplo, em que dia de semana foi o dia 8 de Janeiro de 1935 (data de nascimento de Elvis Presley) podemos proceder de modo análogo: de 8 de Janeiro de 1935 até 1 de Março do mesmo ano passaram $52 = 31 + 21 \equiv 3 \pmod 7$ dias; o número de dias que vai de 1 de Março de 1935 até 1 de Março de 2000 é $65 \times 365 + 17 \equiv 2 \times 1 + 3 \equiv 5 \pmod 7$; assim do dia em que o Elvis nasceu até o dia 1 de Março de 2000 passou um número de dias congruente com 1 módulo 7. Conclusão: o Elvis nasceu numa terça-feira.

1.2 Um pouco de teoria elementar de grupos

Se $< G, \cdot >$ (ou simplesmente G) é um grupo finito e $a \in G$, denotamos por $ord\, a$ o menor inteiro positivo k tal que a^k é o elemento neutro de G (que denotaremos por e). Representemos por $< a >$ o subgrupo de G gerado por a. Os seguintes resultados são bem conhecidos:

- $< a >= \{e, a, \ldots, a^{ord\, a\ -1}\}$;

- $a^s = e$ se e só se $ord\, a$ divide s;
- $ord\, a^s = \frac{ord\, a}{(ord\, a, s)}$;
- $< a >=< a^s >$ se e só se $(s, ord\, a) = 1$ (é uma consequência da observação anterior). Em particular, se $ord\, a$ é um número primo, cada um dos elementos $a, a^2, \ldots, a^{n-1}$ gera $< a >$;
- [**Teorema de Lagrange**] Se G é um grupo finito então $a^{|G|} = e$ (ou seja, a ordem de a divide a ordem de G).

1.3 Máximo divisor comum

Definição 1.3 *Sejam a, b inteiros não ambos nulos. Define-se* **máximo divisor comum** *de a e b e denota-se por (a, b) ou por $mdc(a, b)$ como sendo o maior inteiro que divide a e b.*

Se $(a, b) = 1$ diz-se que a e b são primos entre si.

Escreverei mdc para simplificar máximo divisor comum.

Note-se que, qualquer inteiro é um divisor de 0. Esta é a razão porque na definição de mdc, foi colocada a restrição de a e b não serem ambos nulos.

A seguinte proposição, agrupa algumas das consequências mais simples sobre a noção de máximo divisor comum.

Proposição 1.4 *Se a e b são inteiros não ambos nulos, então:*

a) *a definição acima tem sentido;*

b) $(a, b) = (b, a) = (-a, b) = (a, -b) = (-a, -b)$;

c) $(a, b) \geq 1$;

d) $(a, 1) = 1$;

e) $(a, a) = (a, 0) = |a|$ *se* $a \neq 0$;

f) *se* $a = bq + r$, *com* $q, r \in \mathbb{Z}$ *então* $(a, b) = (r, b)$;

g) *se* $d \in \mathbb{N}$ *então* $(da, db) = d(a, b)$;

h) *se* $d = (a, b)$ *então* $(\frac{a}{d}, \frac{b}{d}) = 1$. ■

Como aplicação destes resultados podemos calcular o máximo divisor comum de dois quaisquer inteiros. Para isso basta aplicar algumas vezes o algoritmo da divisão e a alínea f) da proposição anterior. Por exemplo, para calcular $(218, 486)$ obtemos,

$$\begin{aligned}
(218, 486) &= (218, 50) && \text{porque } 486 = 2 \times 218 + 50 \\
&= (50, 18) && \text{porque } 218 = 4 \times 50 + 18 \\
&= (18, 14) && \text{porque } 50 = 2 \times 18 + 14 \\
&= (14, 4) && \text{porque } 18 = 1 \times 14 + 4 \\
&= (4, 2) && \text{porque } 14 = 3 \times 4 + 2 \\
&= (2, 0) && \text{porque } 4 = 2 \times 2 + 0 \\
&= 2 && \text{pela Proposição 1.4, alínea e)}
\end{aligned}$$

Note-se que, se calcularmos o máximo divisor de a e b aplicando este método, a sucessão dos restos que surge é estritamente decrescente até tomar o valor 0. Nesse momento podemos concluir que $(a, b) = (r, 0) = r$ em que r é o último resto diferente de 0 que apareceu nas nossas contas.

É claro que na prática não necessitamos de fazer estas contas até ao fim. Por exemplo, no caso anterior é obvio que $(14, 4) = 2$, pois os divisores positivos de 4 são 1, 2 e 4 e o 4 não divide 14.

Vejamos outro exemplo,

$$\begin{aligned}
(71\,877, 24\,947) &= (24\,947, 21\,983) && \text{porque } 71\,877 = 2 \times 24\,947 + 21\,983 \\
&= (21\,983, 2\,964) && \text{porque } 24\,947 = 21\,983 + 2\,964 \\
&= (2\,964, 1\,235) && \text{porque } 21\,964 = 7 \times 2\,964 + 1\,235 \\
&= (1\,235, 496) && \text{porque } 2\,964 = 2 \times 1\,235 + 494 \\
&= (494, 247) && \text{porque } 1\,235 = 2 \times 494 + 247 \\
&= (247, 0) && \text{porque } 494 = 2 \times 247 \\
&= 247.
\end{aligned}$$

Note-se também que cada um dos restos que aparecem se pode escrever como combinação linear (com coeficientes inteiros) dos restos anteriores e de a e b. Deste modo, o máximo divisor comum de a e b escreve-se como combinação linear (com coeficientes inteiros) de a e b. Formalmente temos o seguinte teorema.

Teorema 1.5 *Se a e b são inteiros, não ambos nulos e $d = (a, b)$ então existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$.*

Demonstração: Vamos mostrar, por hipótese de indução sobre a que, se $b \geq a \geq 0$ então existem $x, y \in \mathbb{Z}$ tais que $(a, b) = ax + by$ (os outros casos são uma consequência imediata deste caso).

Se $a = 0$ então pela Proposição 1.4, $(a, b) = b$ e, portanto, $(a, b) = 1 \times a + 1 \times b$.

Se $a \geq 1$ consideremos q e r tais que $b = aq + r$ com $0 \leq r < a$. Como $d = (a, b) = (a, r)$ e $a > r \geq 0$ sabemos, por hipótese de indução, que existem $x, y \in \mathbb{Z}$ tais que $ax + ry = d$. Daqui resulta que $a(x - qy) + by = d$. ■

Na prática o que se faz é usar o algoritmo que foi usado para o cálculo do máximo divisor comum, mas agora, de baixo para cima. Costuma-se chamar **algoritmo de Euclides** a este método para encontrar o máximo divisor comum de dois inteiros.

Uma consequência deste resultado é a seguinte.

Proposição 1.6 *Se $a, b, c \in \mathbb{Z}$ são tais que $a \mid bc$ e $(a, b) = 1$ então $a \mid c$.*

Demonstração: Sejam, usando a proposição anterior, $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Desta igualdade obtemos, multiplicando por c, $acx + bcy = c$. Como $a \mid acx$ e $a \mid bcy$ (porque $a \mid bc$) então $a \mid acx + bcy = c$. ■

Corolário 1.7 *Se p é um número primo e $b, c \in \mathbb{Z}$ então $p \mid bc$ se e só se $p \mid b$ ou $p \mid c$.* ■

Definição 1.8 *Sejam a e b inteiros não nulos. Define-se* **mínimo múltiplo comum** *de a e b e denota-se por $[a, b]$ ou $mmc(a, b)$ como sendo o menor inteiro positivo que é simultaneamente múltiplo de a e de b.*

Escreverei mmc para simplificar mínimo múltiplo comum.

Exercício 1.9 *Qual a razão da restrição feita na definição de mmc? Porque é que a existência do menor múltiplo comum está garantida (nas condições referidas na definição)?*

Sejam a e b inteiros não nulos. Seja $\{p_1, \ldots, p_k\}$ o conjunto dos números primos que dividem a ou b. Então podemos escrever:

$$a = p_1^{n_1} \cdots p_k^{n_k}, \qquad b = p_1^{m_1} \cdots p_k^{m_k} \qquad \text{em que } n_1, \ldots, n_k, m_1, \ldots, m_k \in \mathbb{N}_0.$$

Um inteiro positivo c divide a (respectivamente b) se e só se pode ser escrito na forma $p_1^{s_1} \cdots p_k^{s_k}$ com $0 \leq s_i \leq n_i$ (respectivamente $0 \leq s_i \leq m_i$), para $1 \leq i \leq k$. Assim, c divide a e divide b se e só se c for da forma $p_1^{s_1} \cdots p_k^{s_k}$ com $0 \leq s_i \leq \min\{n_i, m_i\}$, para $1 \leq i \leq k$.

De modo análogo se mostra que, um inteiro positivo c é múltiplo de a e de b se e só se pode ser escrito na forma $p_1^{s_1} \cdots p_k^{s_k} y$ em que $s_i \geq \max\{n_i, m_i\}$, para $1 \leq i \leq k$.

Como conclusão obtemos:

- $(a, b) = p_1^{\min\{n_1, m_1\}} \cdots p_k^{\min\{n_k, m_k\}}$;
- $[a, b] = p_1^{\max\{n_1, m_1\}} \cdots p_k^{\max\{n_k, m_k\}}$;
- $[a, b] = \frac{ab}{(a,b)}$;
- (a, b) (respectivamente $[a, b]$) é múltiplo (respectivamente divisor) de todos os divisores (respectivamente múltiplos) comuns a a e a b.

Esta última observação pode ser reescrita do seguinte modo.

Proposição 1.10 *Sejam a, b inteiros não nulos e d, D inteiros positivos. Então:*

a) $d = (a, b) \Leftrightarrow \begin{cases} d \mid a, \ d \mid b; \\ \\ d' \mid a, \ d' \mid b \Rightarrow d' \mid d. \end{cases}$

b) $D = [a,b] \Leftrightarrow \begin{cases} a \mid D,\ b \mid D; \\ \\ a \mid D',\ b \mid D' \Rightarrow D \mid D'. \end{cases}$ ■

O que é dito nesta proposição, com a excepção referente à positividade de d e de D, costuma ser usado para definir mdc e de mmc num anel qualquer.

Note-se que, para um anel qualquer, não está garantida a existência de mdc nem de mmc. Além disso, se d (resp. D) é um mdc (resp. mmc) de a e b, e ε é um elemento invertível no anel, então εd (resp. εD) é um mdc (resp. mmc). Se usássemos estas definições para mdc e mmc no anel dos inteiros e se (por exemplo) d fosse um mdc de a e b, então $-d$ também seria um mdc de a e b. Para garantirmos a unicidade de mdc e de mmc obrigámos o mmc e o mdc a serem positivos.

É claro que poderíamos definir mdc e mmc de um conjunto finito $\{a_1, a_2, \ldots, a_n\}$ de inteiros, não todos nulos no caso do mdc, e não nulos no caso do mmc. A notação usada é $(a_1, a_2, \ldots, a_n)$ ou $mdc(a_1, a_2, \ldots, a_n)$ para o mdc e $[a_1, a_2, \ldots, a_n]$ ou $mmc(a_1, a_2, \ldots, a_n)$ para o mmc.

Como consequências das definições temos os seguintes resultados cuja demonstração é deixada como exercício.

Proposição 1.11 *Se $a, b, c, k, s, n_1, \ldots, n_s \in \mathbb{N}$ então:*

a) $[a,b] \mid k \Leftrightarrow a \mid k$ *e* $b \mid k$;

b) $k \mid (a,b) \Leftrightarrow k \mid a$ *e* $k \mid b$;

c) $[[n_1, n_2], \ldots, n_s] = [n_1, n_2, \ldots, n_s]$; $\qquad ((n_1, n_2), \ldots, n_s) = (n_1, n_2, \ldots, n_s)$;

d) $(c, [a,b]) = [(c,a), (c,b)]$.

Exercícios

1.1. Mostre que em cada ano civil o número de sexta-feiras, dia 13 é no mínimo 1 e no máximo 3.

1.2. Quais das seguintes afirmações são verdadeiras?

a) Se a^n divide b^n, então a divide b;

b) Se n^n divide m^m então n divide m;

c) Se a^n divide $2b^n$, então a divide b;

1.3. Mostre que $3^{10} \equiv 1 \pmod{11^2}$.

1.4. Resolva a congruência $x^4 + y^4 = 1 \pmod 5$.

1.5. Mostre que a congruência $x^3 + y^3 + z^3 = 4 \pmod 9$ não tem solução.

1.6. Mostre que o produto de dois inteiros da forma $6k + 5$ é da forma $6k + 1$.

1.7. Mostre que o produto de três inteiros consecutivos é divisível por 6.

1.8. Mostre que o quadrado de todo o inteiro ímpar é da forma $8k + 1$.

1.9. Mostre que a quarta potência de todo o inteiro ímpar é da forma $16k + 1$.

1.10. Mostre que, se n é ímpar e 3 não divide n, então $n^2 - 1$ é múltiplo de 24.

1.11. Mostre que se um número primo ímpar é uma soma de dois quadrados então é congruente com 1 módulo 4.

1.12. Seja n um número inteiro cuja soma dos seus algarismos é 375. Mostre que n não é um quadrado.

1.13. Mostre que, se $x^5 + y^5 = z^5$ então $x + y - z$ é um múltiplo de 5.

1.14. Mostre que, se $n \in \mathbb{N}$, 30 divide $n^5 - n$ e 252 divide $n^9 - n^3$.

1.15. Mostre que, se n, m são inteiros ímpares então 8 divide $n^4 + m^4 - 2$.

1.16. Mostre que não existe $n \in \mathbb{N}$ tal que $4n^2 - 3$ seja múltiplo de 7.

1.17. Mostre que, se p, q são primos maiores do que 3 então $p^2 - q^2$ é múltiplo de 24.

1.18. Sejam p, q e r números primos tais que $p^2 + q^2 + r^2$ é um número primo. Mostre que p, q ou r é igual a 3.

1.19. Resolva a congruência $x^2 \equiv x \pmod{n}$, para $n \in \{2, 4, 6, 8\}$.

1.20. Mostre que, se p é primo e $x \in \mathbb{Z}$ é tal que $x^2 \equiv x \pmod{p}$ então $x \equiv 0 \pmod{p}$ ou $x \equiv 1 \pmod{p}$.

1.21. Mostre que, se p é um número primo, $a, b \in \mathbb{Z}$ e $k \in \mathbb{N}$ são tais que $a \equiv b \pmod{p^k}$ então $a^p \equiv b^p \pmod{p^{k+1}}$.

1.22. Seja p um número primo e $n \in \mathbb{N}$. Mostre que se $n \geq p$ então $\binom{n}{p} \equiv \left[\frac{n}{p}\right] \pmod{p}$.

1.23. Existe algum inteiro n cujo cubo"termine" em 63?

1.24. Qual o menor inteiro n cujo cubo "termina" em 92?

1.25. Determine todos os inteiros da forma $66\cdots6$ que são múltiplos de 7.

1.26. Mostre que os número $99\cdots9$ e $10\cdots01$, em que o número de algarismos é par, são múltiplos de 11.

1.27. Encontre $n > 100$ tal que $11\cdots1$ (n algarismos) é múltiplo de 7.

1.28. Mostre que, se $11\cdots1$ (n algarismos) é primo, então n é primo.

1.29. Mostre que existe uma infinidade de primos da forma $4n + 3$. **Sugestão:** Suponha que $\{p_1, \ldots, p_k\}$ é o conjunto formado por todos os primos da forma $4n + 3$ excluindo o 3 e considere $N = 4p_1p_2\cdots p_k + 3$.

1.30. Mostre que existe uma infinidade de primos da forma $6n + 5$.

1.31. Seja m um inteiro que não é múltiplo de 3.

a) Mostre que $4m^2 + 3$ é congruente com 4 ou com 7 módulo 12.

b) Mostre que existe um número primo congruente com 7 módulo 12 que divide $4m^2 + 3$.

c) Conclua que existe um número infinito de primos da forma $12k + 7$, com $k \in \mathbb{N}$.

1.32. Seja a um inteiro maior que 1. Mostre que, se p e q são primos ímpares tais que $q \mid a^p - 1$, então:

a) $q|\, a-1$ ou q é congruente com 1 módulo $2p$;

b) Mostre que existe uma infinidade de números primos na sucessão $(2pn+1)_{n\in\mathbb{N}}$;

c) Conclua que existe um número infinito de primos da forma $6n+1$.

1.33. Em quantos zeros termina 1000! ?

1.34. Qual o maior inteiro n tal que 7^n divide $\begin{pmatrix} 5000 \\ 2000 \end{pmatrix}$?

1.35. Determine todos os inteiros n tais que $n!$ termina exactamente em 75 zeros.

1.36. Mostre se n é um inteiro positivo é impossível $n!$ terminar exactamente em 153, 154 ou 155 zeros.

1.37. Quais são os dois últimos algarismos de 9^{9^9}? E de $7^{9^{9^9}}$?

1.38. Mostre que, se $n \in \mathbb{N}$, 19 divide $2^{2^{6n+2}}+3$.

1.39. Mostre que, se a é um inteiro ímpar e $n \geq 3$ então $a^{2^{n-2}} \equiv 1 \pmod{2^n}$.

1.40. Mostre que, se $k \in \mathbb{N}$, 3^{k+1} divide $2^{3^k}+1$.

1.41. Mostre que, se a, b e c são inteiros tal que $c|\, ab$, então $c|\, (a,c)(b,c)$.

1.42. Mostre que, se a, b e c são inteiros positivos tais que $(a,b)=1$ e $ab=c^n$, então existe um inteiro positivo d e e tal que $a=d^n$ e $b=e^n$.

1.43. Mostre que, se $a,b,d \in \mathbb{N}$ são tais que $(a,b)=d$, então $(\frac{a}{d},b)$ divide d. Dê um exemplo em que $(\frac{a}{d},b)=1$ e outro em que $(\frac{a}{d},b)\neq 1$.

1.44. Mostre que, se $(a,b)=1$ então $(a+b, a^2-ab+b^2) \in \{1,3\}$.

1.45. Sejam $a,b \in \mathbb{Z}$ tais que $(a,b)=2$. Mostre que $(a+b, a^2-ab+b^2)$ divide 12.

1.46. Mostre que, se $n \in \mathbb{N}$, $(n!+1,(n+1)!+1)=1$.

1.47. Para que valores de $n \in \mathbb{N}$, $(2n^2+3n+8, n^2+n+9)=1$?

1.48. Para a e b inteiros primos entre si, determine $(a^2+b^2, a+b)$.

1.49. Sejam $a, b, c, d \in \mathbb{N}$ tais que $|ad - bc| = 1$. Mostre que, se $c + d \neq 0$, então $(a + b, c + d) = 1$.

1.50. Sejam $m, n \in \mathbb{N}$ com m ímpar. Mostre que $(2^m - 1, 2^n + 1) = 1$.

1.51. Mostre que, se $a, m, n \in \mathbb{N}$ e $m \neq n$ então $(a^{2^m} + 1, a^{2^n} + 1) \in \{1, 2\}$.

1.52. Mostre que, se $n.m \in \mathbb{N}$ e $a > 1$ então $(a^m - 1, a^n - 1) = a^{(n,m)} - 1$.

1.53. Mostre que, se $x \in \mathbb{Q}$, $a, b \in \mathbb{N}$ são tais que $(a, b) = 1$, $ax, bx \in \mathbb{N}$, então $x \in \mathbb{N}$.

1.54. Sejam a, b inteiros diferentes. Mostre que existe uma infinidade de inteiros n tais que $(a + n, b + n) = 1$.

1.55. Mostre que, se a e b são inteiros positivos, então $(a, b) = (a + b, [a, b])$.

1.56. Determine dois inteiros positivos a e b tais que $a + b = 798$ e $[a, b] = 10780$.

1.57. Determine todos os pares $(a, b) \in \mathbb{N}^2$ tais que $8[a, b] = 105(a, b) + 30$.

1.58. Mostre que, se a, b e c são inteiros positivos, então $[a, b, c] = \dfrac{abc(a, b, c)}{(a, b)(a, c)(b, c)}$.

1.59. Para um inteiro positivo n. Quantos pares de inteiros positivos satisfazem $[a, b] = n$.

1.60. Sejam a, b inteiros diferentes e primos entre si e $m \in \mathbb{N}$.

Mostre que,

$$\left(\frac{a^m - b^m}{a - b}, a - b\right) = (a - b, m).$$

2. Equações lineares

2.1 Equações diofantinas

Comecemos com um exemplo.

Exemplo 2.1 *Suponhamos que só existiam moedas de* 15 *e de* 7 *escudos e que eu queria pagar (em dinheiro) uma certa quantia em escudos. Será que é sempre possível? E se só existissem moedas de* 12 *e de* 30 *escudos?*

No primeiro caso, se conseguirmos pagar 1 escudo então também sabemos pagar qualquer quantia: basta repetir o pagamento de 1 escudos as vezes que forem necessárias. Para pagar 1 escudo podemos usar uma moeda de 15 e receber de troco duas moedas de 7. Deste modo, se quisermos pagar 23 escudos podemos usar 23 moedas de 15 e receber de troco 46 moedas de 7. É claro que seria mais simples pagar com 2 moedas de 15 e receber 1 moeda de 7 de troco. No fundo estamos a encontrar soluções inteiras da equação $7x + 15y = 1$.

No segundo caso é claro que qualquer quantia que se consiga pagar é necessariamente múltipla de 6, porque 12 e 30 são múltiplos de 6. Por outro lado podemos pagar 6 escudos usando uma moeda de 30 e recebendo de troco duas moedas de 12. Deste modo podemos fazer o pagamento de qualquer quantia que seja múltipla de 6.

Chegamos assim à seguinte definição.

Definição 2.2 *Uma equação nas variáveis inteiras* x, y *do tipo*

$$ax + by = c, \quad \text{com } a, b, c \in \mathbb{Z}$$

diz-se uma **equação diofantina**.

A palavra diofantina "vem" de Diophantus da Alexandria, matemático grego do século III.

É claro que se $a = 0$ ou $b = 0$ a equação tem resolução imediata. Por exemplo, se $a = 0$ e $b \neq 0$ então existe solução se b divide c e, nesse caso a solução geral é dada por x qualquer e $y = \frac{c}{b}$. Para os casos "não triviais" temos o seguinte teorema.

Teorema 2.3 *Sejam a, b inteiros não ambos nulos, $c \in \mathbb{Z}$ e $d = (a, b)$. A equação*

$$ax + by = c \qquad \textit{(nas incógnitas inteiras } x, y\textit{)}$$

tem solução se e só se d divide c.

Além disso, se x_0, y_0 são tais que $ax_0 + by_0 = c$ então a solução geral da equação $ax + by = c$ é

$$\begin{cases} x &= x_0 + \frac{b}{d}\, t \\ y &= y_0 - \frac{a}{d}\, t, \quad \textit{com } t \in \mathbb{Z}. \end{cases}$$

Demonstração: Se a ou b é igual a 0 o resultado é imediato. Vejamos o caso em que $a \neq 0 \neq b$.

Para a primeira parte do teorema.

$\Rightarrow$

Suponhamos que a equação tem solução e sejam $x, y \in \mathbb{Z}$ tais que $ax+by = c$. Então $d \mid ax$ (porque $d \mid a$), $d \mid by$ (porque $d \mid b$) e, portanto $d \mid ax + by = c$.

$\Leftarrow$

Suponhamos que $d \mid c$ e seja k tal que $kd = c$. Usando o Teorema 1.5, sejam $\alpha, \beta \in \mathbb{Z}$ tais que $a\alpha + b\beta = d$. Multiplicando esta última igualdade por k obtemos $a(\alpha k) + b(\beta k) = dk = c$, o que mostra que $x = \alpha k$, $y = \beta k$ é solução da equação $ax + by = c$.

Para a segunda parte do teorema.

Sejam x_0, y_0 tais que $ax_0 + by_0 = c$. Então, se $t \in \mathbb{Z}$,

$$a(x_0 + \frac{b}{d}\, t) + b(y_0 - \frac{a}{d}\, t) = ax_0 + \frac{ab}{d}\, t + by_0 - \frac{ab}{d}\, t = ax_0 + by_0 = c,$$

o que mostra que $x = x_0 + \frac{b}{d}\, t$, $y = y_0 - \frac{b}{d}\, t$ é solução da equação.

Inversamente, para mostrar que, se $x, y \in \mathbb{Z}$ são tais que $ax + by = c$, então x, y são da forma pretendida basta notar que,

$$\begin{array}{rcl} \left\{ \begin{array}{lcl} ax + by & = & c \\ ax_0 + by_0 & = & c \end{array} \right. & \iff & \left\{ \begin{array}{lcl} \frac{a}{d}\, x + \frac{b}{d}\, y & = & \frac{c}{d} \\ \frac{a}{d}\, x_0 + \frac{b}{d}\, y_0 & = & \frac{c}{d} \end{array} \right. \\ & \implies & \frac{a}{d}\,(x - x_0) + \frac{b}{d}\,(y - y_0) = 0 \\ & \iff & \frac{a}{d}\,(x - x_0) = -\frac{b}{d}\,(y - y_0). \end{array}$$

Deste modo $\frac{b}{d}$ divide $\frac{a}{d}\,(x - x_0)$. Usando a alínea h) da Proposição 1.4 e a Proposição 1.6 podemos concluir que $\frac{b}{d}$ divide $(x - x_0)$ e, portanto existe $t \in \mathbb{Z}$ tal que $x - x_0 = \frac{b}{d}\, t$. Substituindo na igualdade $\frac{a}{d}\,(x - x_0) = -\frac{b}{d}\,(y - y_0)$ obtemos $\frac{a}{d}\frac{b}{d}\, t = -\frac{b}{d}\,(y - y_0)$ ou seja $y - y_0 = -\frac{a}{d}\, t$. Conclusão, existe $t \in \mathbb{Z}$ tal que $x = x_0 + \frac{b}{d}\, t$ e $y = y_0 - \frac{a}{d}\, t$. ■

Voltemos ao Exemplo 2.1. Uma vez que a equação $15x + 7y = 17$ tem como solução $x = 3$, $y = -4$ (por exemplo), para pagar 17 escudos, basta pagar com 3 moedas de 15 escudos e receber de troco 4 moedas de 7 escudos. Outra hipótese seria pagar com 11 moedas de 7 escudos e receber de troco 4 moedas de 15 escudos. É claro que o teorema anterior dá-nos um método de encontrar todas as soluções possíveis.

Nota 2.4 *Note-se que, se encontrarmos por algum meio (tentativas, observação, algum meio sistemático), uma solução de uma equação do tipo $ax + by = c$ então podemos sempre encontrar* **todas** *as soluções dessa equação.*

Vamos agora mostrar, com um exemplo, outro meio de encontrar uma solução (quando existe) de uma equação diofantina.

Começo por notar que se a equação $ax + by = c$ for tal que $(a, b) \mid c$, então esta equação é equivalente a uma equação do tipo $Ax + By = C$ em que $(A, B) = 1$ (basta considerar $A = \frac{a}{(a,b)}$, $B = \frac{b}{(a,b)}$ e $C = \frac{c}{(a,b)}$).

Exemplo 2.5 *Consideremos a equação $15x + 41y = 27$. Recordo que basta encontrar uma solução.*

Começamos por isolar a variável cujo coeficiente tem menor valor absoluto. Obtemos

$$x = \frac{27 - 41y}{15}.$$

Utilizando o algoritmo da divisão ($27 = 1 \times 15 + 12$ e $41 = 2 \times 15 + 11$) obtemos

$$x = 1 - 2y + \frac{12 - 11y}{15}.$$

Daqui podemos concluir que y tem de ser tal que $\frac{12-11y}{15} \in \mathbb{Z}$. Ou encontramos um valor de y nestas condições e depois tiramos o valor de x correspondente, ou procuramos $z \in \mathbb{Z}$ tal que $\frac{12-11y}{15} = z$, ou seja, tal que $11y+15z = 12$ (obtemos assim uma equação do mesmo tipo da anterior).

Fazendo a esta equação o mesmo que foi feito para a anterior obtemos

$$y = 1 - z + \frac{1 - 4z}{11}.$$

Procuramos agora $z \in \mathbb{Z}$ tal que $\frac{1-4z}{11}$ seja um número inteiro, por exemplo $z = 3$ (que implica $y = -3$ e $x = 10$) ou $z = -8$ (que implica $y = 12$ e $x = -31$).

Se não conseguíssemos encontrar um valor de z tal que $\frac{1-4z}{11} \in \mathbb{Z}$, repetíamos o processo, isto é, escreveríamos $\frac{1-4z}{11} = w$ e tentaríamos resolver esta nova equação. Teríamos assim: $11w + 4z = 1$ e portanto $z = -2w + \frac{1-3w}{4}$, etc..

O que é que nos garante que este processo termina sempre? O facto da sucessão dos menores dos módulos das coordenadas das equações encontradas decrescer até 0, obtendo nessa altura uma equação de resolução trivial.

Uma pequena observação: voltando ao início, quando tínhamos a igualdade $x = \frac{27-41y}{15}$, poderíamos ter optado por escrever $x = 2 - 3y + \frac{-3+4y}{15}$, o que, em princípio, iria simplificar as contas.

2.2 Congruências do tipo $ax \equiv b \pmod{n}$

Comecemos por uma definição.

Definição 2.6 *Seja $n \in \mathbb{N}$ e A um subconjunto de $\mathbb{Z}$. Dizemos que:*

- *A é um* **sistema completo de resíduos** *(abreviadamente* **scr***)* **módulo** *n se todo o inteiro for congruente módulo n com um e um só elemento de A;*

- *A é um* **sistema reduzido de resíduos** *(abreviadamente* **srr***)* **módulo** *n se for formado por inteiros primos com n e se todo o inteiro primo com n for congruente módulo n com um e um só elemento de A.*

Se usarmos a notação: $[i]_n$ para representarmos a classe de equivalência de i relativamente à congruência $\equiv_n$ (e recordando que, se $[a]_n = [b]_n$, então $(a, n) = (b, n)$) podemos reformular as definições de **scr** e de **srr** módulo n do seguinte modo:

- A é um **scr** módulo n se e só se para todo $i \in \mathbb{Z}$, $A \cap [i]_n$ é um conjunto singular;
- A é um **srr** módulo n se e só se para todo $i \in \mathbb{Z}$,

$$A \cap [i]_n \quad = \quad \begin{cases} \text{um conjunto singular} & \text{se } (i, n) = 1 \\ \text{o conjunto vazio} & \text{se } (i, n) \neq 1. \end{cases}$$

As seguintes observações decorrem facilmente das definições. Dado $n \in \mathbb{N}$:

- $\{0, 1, \ldots, n-1\}$ é um **scr** módulo n;
- $\{0, 1, \ldots, \frac{n-1}{2}\} \cup \{, -1, \ldots, -\frac{n-1}{2}\}$ se n é ímpar e $\{0, 1, \ldots, \frac{n}{2}\} \cup \{-1, \ldots, -\frac{n}{2} - 1\}$ se n é par;
- $\{a \in \{0, 1, \ldots, n-1\} : (a, n) = 1\}$ é um **srr** módulo n;
- se A é um **scr** módulo n então $\{a \in A : (a, n) = 1\}$ é um **srr** módulo n;
- se A é um **scr** (ou um **srr**) módulo n e se substituirmos um elemento de A por um inteiro que seja congruente com ele módulo n obtemos um **scr** (ou um **srr**) modulo n. De facto todos os **scr** (ou **srr**) são obtidos deste modo.

Proposição 2.7 *Seja $n \in \mathbb{N}$ e $A \subseteq \mathbb{Z}$.*

a) *Se A tem n elementos então A é um* **scr** *módulo n se e só se os seus elementos são incongruentes dois a dois módulo n.*

b) *Se A tem tantos elementos como um dado* **srr** *módulo n então A é um* **srr** *módulo n se e só se os seus elementos são primos com n e incongruentes dois a dois módulo n.*

Demonstração: Que um scr e um srr satisfazem as condições referidas decorre das próprias definições.

Suponhamos agora que os elementos de A são incongruentes módulo n e seja B um scr módulo n, para a alínea a) ou um srr módulo n, para a alínea b). Para concluir basta notar que a função $f : A \to B$ que a cada $a \in A$ associa o único elemento de B que é congruente com a módulo n é bijectiva pois é injectiva e A e B têm o mesmo número de elementos. ■

Nesta secção pretendemos resolver equações do tipo

$$ax \equiv b \ (\mod n), \qquad \text{em que } a, b \in \mathbb{Z} \text{ e } n \in \mathbb{N}.$$

Uma vez que, se x_0 é solução da equação, então $x_0 + nt$ (com $t \in \mathbb{Z}$) também é, só precisamos de encontrar as soluções no conjunto $\{0, 1, \ldots, n-1\}$ ou em qualquer outro sistema completo de resíduos de n. Assim, qualquer congruência deste tipo, ou não tem solução ou tem uma infinidade de soluções. É claro que esta congruência pode ser entendida como uma equação em $\mathbb{Z}_n$ e neste caso tem no máximo n soluções.

Por abuso de notação quando dissermos que a congruência tem k soluções, estaremos a subentender, que essas soluções são incongruentes módulo n.

Por exemplo, a equação $4x \equiv 0 \pmod 8$ tem duas soluções (incongruentes módulo 8): $x = 0$ e $x = 2$.

Vamos então ver que estas congruências podem ser resolvidas usando o que sabemos sobre equações diofantinas.

Se $a \equiv 0 \pmod n$ a congruência é de resolução trivial, tendo n ou 0 soluções consoante b é ou não congruente com 0 módulo n.

Teorema 2.8 *Sejam $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ tais que $a \not\equiv 0 \pmod n$. Se $d = (a, n)$ então a congruência $ax \equiv b \pmod n$ tem solução se e só se $d \mid b$.*

Além disso, se $d \mid n$ e x_0 é uma solução da congruência então a solução geral é dada por:

$$x = x_0 + \frac{n}{d}\, t \quad \textit{com } t \in \mathbb{Z}.$$

Em particular, existem d soluções (incongruentes módulo n), por exemplo:

$$\left\{ x_0 + \frac{n}{d}\, t : \quad t \in \{0, 1, \ldots, d-1\} \right\}.$$

Demonstração: Para a primeira parte basta notar que,

$$\begin{aligned} \exists x \in \mathbb{Z}: \quad ax \equiv b \ (\bmod n) &\Leftrightarrow \exists x \in \mathbb{Z}: \quad n \mid ax - b \\ &\Leftrightarrow \exists x \in \mathbb{Z}\ \exists y \in \mathbb{Z}: ax - b = ny \\ &\Leftrightarrow \exists x, y \in \mathbb{Z}: ax - ny = b \\ &\Leftrightarrow d \mid b, \text{ pelo Teorema 2.3.} \end{aligned}$$

A segunda parte do teorema é uma consequência imediata do Teorema 2.3. ■

Corolário 2.9 *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então:*

a) *se $(a, n) = 1$ então existe $c \in \mathbb{Z}$ tal que $ac \equiv 1 \pmod{n}$;*

b) *(lei do corte) se $(a, n) = 1$, $c \in \mathbb{Z}$ e $ac \equiv ab \pmod{n}$ então $b \equiv c \pmod{n}$.*

Demonstração: Para a alínea a) basta aplicar o teorema anterior à congruência $ax \equiv 1 \ (\bmod n)$. Para a alínea b) basta "multiplicar a igualdade $ac \equiv ab \pmod{n}$ por c" em que c é tal que $ac \equiv 1 \pmod{n}$. ■

Por razões óbvias se $ac \equiv 1 \pmod{n}$ dizemos que c é um inverso módulo de n de a.

Chama-se a atenção para o facto de que a lei do corte funciona apenas nas condições referidas no corolário anterior. Isto é verdade pois se $(a, n) \neq 1$ então se considerarmos $b = n$ e $c = \frac{n}{(a,n)}$ (por exemplo) temos

$$ab \equiv ac \ (\bmod n) \text{ e } b \not\equiv c \ (\bmod n).$$

Como no caso das equações diofantinas, todas as congruências lineares que tiverem solução são equivalentes a congruências da forma $ax \equiv b \pmod{n}$ em que $(a, b) = 1$. Antes de começarmos a tentar resolver este tipo de equação devemos tentar ver se existe algum factor comum a a e a b. Esse factor é necessariamente primo com n e, portanto a congruência pode ser simplificada usando a lei do corte. A partir daqui talvez valha a pena ver se à fácil encontrar um inteiro que multiplicado por a dê 1 (ou outro número que possa de certo modo simplificar a congruência.

A lei do corte pode ser usada para mostrar que certo tipo de conjunto é um scr ou um srr módulo um inteiro positivo n.

Proposição 2.10 *Seja $n \in \mathbb{N}$.*

a) *Se $m, r \in \mathbb{Z}$ e $(n, m) = 1$ então $\{r, m + r, 2m + r, \ldots, (n-1)m + r\}$ é um* **scr** *modulo n.*

b) *Se A é um* **srr** *(ou* **scr***) módulo n e $a \in \mathbb{Z}$ é primo com n então $\{ak : k \in A\}$ é um* **srr** *(ou* **srr***) módulo n.*

Demonstração: Para a alínea a) basta mostrar, usando a Proposição 2.7, que $im + r$ e $jm + r$ não são congruentes módulo n para todo $i, j \in \{0, 1, \ldots, n-1\}$ se $i \neq j$. Mas

$$\begin{aligned} im + r \equiv jm + r \ (\mathrm{mod}\ n) &\Leftrightarrow im \equiv jm \ (\mathrm{mod}\ n) \\ &\Leftrightarrow i \equiv j \ (\mathrm{mod}\ n) \qquad \text{pela lei do corte} \\ &\Leftrightarrow i = j \qquad \text{porque } 0 \leq i, j \leq n-1. \end{aligned}$$

Para a alínea b) o raciocínio é semelhante ao usado na alínea a) notando ainda que o produto de dois números primos com n é ainda primo com n. ■

Observações:

- se n for um número "pequeno", o método das tentativas é, por vezes, o método mais rápido para resolver a congruência $ax \equiv b \ (\mathrm{mod}\ n)$;
- se $n = p_1^{n_1} \cdots p_k^{n_k}$ e $A, B \in \mathbb{Z}$, então

$$A \equiv B \ (\mathrm{mod}\ n) \Leftrightarrow \forall i \in \{1, \ldots, k\} \quad A \equiv B \ (\mathrm{mod}\ p_i^{n_i});$$

- como consequência da observação anterior, a resolução da congruência $ax \equiv b \ (\mathrm{mod}\ n)$ é equivalente à resolução do sistema

$$\begin{cases} ax \equiv b \ (\mathrm{mod}\ p_1^{n_1}) \\ \quad \ddots \\ ax \equiv b \ (\mathrm{mod}\ p_k^{n_k}). \end{cases}$$

Deste modo, por exemplo, para resolvermos a congruência $3x \equiv 4 \ (\mathrm{mod}\ 2020)$ podemos usar vários métodos:

- por tentativas verificar cada um dos inteiros de $\{0, 1, \ldots, 2019\}$ ou de outro qualquer sistema completo de resíduos módulo 2020. Note-se que esta congruência admite uma solução módulo 2020. Deste modo se encontrarmos uma solução não precisamos de continuar a procurar;
- multiplicar pelo inverso de 3 módulo 2020;
- "passar" esta congruência para uma equação diofantina e resolvê-la pelos métodos já descritos anteriormente;
- notar que $2020 = 4 \times 5 \times 101$ e resolver o sistema

$$\begin{cases} 3x & \equiv & 4 \ (\mod 4) \\ 3x & \equiv & 4 \ (\mod 5) \\ 3x & \equiv & 4 \ (\mod 101). \end{cases}$$

Note que cada uma das congruências deste sistema pode ser resolvida usando os métodos anteriores. Em princípio o método das tentativa é o mais fácil para resolver as duas primeiras congruências. Em relação à terceira talvez o mais fácil seja notar que $3 \times 34 = 102 \equiv 1 \pmod{101}$ e, portanto, a congruência é equivalente a $x \equiv 136 \equiv 35 \pmod{101}$. É claro que aquilo que se pede é a resolução do sistema e não (apenas) a resolução de cada uma das congruências.

2.2.1 Teorema chinês dos restos

O chamado Teorema Chinês dos Restos (Sec V) dá um método sistemático de resolução de sistemas de congruências do tipo $ax \equiv b \pmod{n}$. Aparentemente a ideia surgiu com a necessidade de contar o número de soldados numa parada. Suponhamos que sabemos que o número de soldados é no máximo 1000. Mandamos ordenar os soldados em filas de 7 e depois em filas de 11 e depois em filas de 13 (o que é mais simples do que contar os soldados) e contamos o número de soldados que sobraram em cada um dos casos. Suponhamos que esses números foram 6, 5 e 3. Estamos assim perante

o sistema,

$$\begin{cases} x & \equiv & 6 \ (\mod 7) \\ x & \equiv & 5 \ (\mod 11) \\ x & \equiv & 3 \ (\mod 13) \end{cases}$$

cuja solução é $x \equiv 874 \pmod{1001}$ (note-se que $7 \times 11 \times 13 = 1001$). Deste modo existe $k \in \mathbb{Z}$ tal que o número de soldados é $874 + 1001\,k$. Como o número pretendido é no máximo 1000 podemos concluir que existem 874 soldados na parada.

Recorda-se que uma congruência do tipo $ax \equiv b \pmod{n}$ é impossível se (a, n) não divide b ou é equivalente a uma congruência do tipo $x \equiv c \pmod{m}$ (em que $m = \frac{n}{(a,n)}$) caso contrário. Resta-nos assim considerar sistemas em que todas as congruências são da forma

$$\begin{cases} x & \equiv & a_1 \ (\mod n_1) \\ & \ddots & \\ x & \equiv & a_k \ (\mod n_k) \end{cases}$$

É claro que, se D for um múltiplo comum a $n_1, \ldots, n_2$ e se x_0 for uma solução, então $x = x_0 + Dt$ com $t \in \mathbb{Z}$ é também uma solução do sistema. Assim basta-nos procurar soluções no conjunto $\{0, 1, \ldots, D-1\}$ ou em qualquer outro sistema completo de resíduos módulo D. Evidentemente que o mais natural será considerar D o mais pequeno possível, isto é D o mínimo múltiplo comum dos inteiros $n_1, \ldots, n_k$.

Um modo de resolver este sistema é usar o seguinte raciocínio:

$$\begin{cases} x & \equiv & a_1 \ (\mod n_1) \\ x & \equiv & a_2 \ (\mod n_2) \\ & \ddots & \\ x & \equiv & a_k \ (\mod n_k) \end{cases} \Leftrightarrow \begin{cases} x & = & a_1 + n_1\,t \ \text{ para algum } t \in \mathbb{Z} \\ a_1 + n_1\,t & \equiv & a_2 \ (\mod n_2) \\ & \ddots & \\ x & \equiv & a_k \ (\mod n_k) \end{cases}$$

$$\Leftrightarrow \begin{cases} x & = & a_1 + n_1\,t \ \text{ para algum } t \in \mathbb{Z} \\ n_1\,t & \equiv & a_2 - a_1 \ (\mod n_2) \\ & \ddots & \\ x & \equiv & a_k \ (\mod n_k) \end{cases}$$

Note-se que a congruência $n_1\, t \equiv a_2 - a_1 \pmod{n_2}$ tem solução se e só se (n_1, n_2) divide $a_2 - a_1$. Se esta congruência tiver solução encontramos a sua solução, que será da forma $t = t_0 + \frac{n_2}{(n_1,n_2)}\, s$ e substituímos no sistemas obtendo (note-se que $\frac{n_1\, n_2}{(n_1,n_2)} = [n_1, n_2]$)

$$\begin{cases} x &= a_1 + n_1 t_0 + [n_1, n_2]\, s \\ t &= t_0 + \frac{n_2}{(n_1,n_2)}\, s \ \text{ para algum } k \in \mathbb{Z} \\ & \ddots \\ x &\equiv a_k \pmod{n_k} \end{cases}$$

Se no início existissem apenas duas congruências então a solução do sistema estava encontrada. Caso contrário substituímos $x = a_1 + n_1 t_0 + [n_1, n_2]\, s$ na terceira congruência e continuamos o processo.

É claro que há situações em que a descoberta de uma solução do sistema ou de parte dele é trivial. Nestes casos a resolução completa do sistema fica muito simplificada uma vez que, como veremos, se encontrarmos uma solução então saberemos quais são todas as soluções.

Vejamos um exemplo. Quais os números inteiros positivos que divididos por $2, 3, 4, 5, 6$ dão resto $1, 2, 3, 4, 5$ (respectivamente). A resolução deste problema conduz-nos (provavelmente) à resolução do sistema, com $x \in \mathbb{N}$,

$$\begin{cases} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 5 \pmod{6} \end{cases}$$

Sabemos já que nos basta encontrar soluções no conjunto $\{0, 1, \ldots, 59\}$ ou em qualquer outro sistema completo de resíduos módulo 60.

Se olharmos para este sistema de outro modo, por exemplo,

$$\begin{cases} x & \equiv & -1 \ (\mod 2) \\ x & \equiv & -1 \ (\mod 3) \\ x & \equiv & -1 \ (\mod 4) \\ x & \equiv & -1 \ (\mod 5) \\ x & \equiv & -1 \ (\mod 6) \end{cases}$$

vemos facilmente que $x = 1$ é uma solução deste sistema com a incógnita em $\mathbb{Z}$. Pelo que foi dito atrás, se somarmos a -1 um múltiplo de 60 obtemos soluções do sistema que estão naturalmente em $\mathbb{N}$.

O teorema chinês dos restos diz-nos que, se conseguirmos encontrar (por algum método) uma solução do sistema então passaremos a conhecer todas as suas soluções.

Teorema 2.11 (Teorema Chinês dos Restos) *Se $k \in \mathbb{N} \setminus \{1\}$, $a_1, \ldots, a_k \in \mathbb{Z}$ e $n_1, \ldots, n_k \in \mathbb{N}$ então o sistema,*

$$\begin{cases} x & \equiv & a_1 \ (\mod n_1) \\ & \ddots & \\ x & \equiv & a_k \ (\mod n_k) \end{cases}$$

tem solução se e só se, para todo $i, j \in \{1, \ldots, k\}$, $(n_i, n_j) \mid a_j - a_i$.

Além disso, se x_0 for uma solução do sistema, então a solução geral é dada por

$$x = x_0 + [n_1, \ldots, n_k]t, \ t \in \mathbb{Z}.$$

Em particular, se o sistema tiver solução, ele admite uma só solução módulo $[n_1, \ldots, n_k]$.

Demonstração: (por indução sobre k) O caso em que $k = 2$ já foi analisado atrás.

Caso geral: Se o sistema tem solução e $i, j \in \{1, \ldots, k\}$ então o sistema

$$\begin{cases} x & \equiv & a_i \ (\mod n_i) \\ x & \equiv & a_j \ (\mod n_j) \end{cases}$$

tem solução (pois é um subsistema do sistema original). Pelo que foi feito para o caso $k = 2$, podemos concluir que $(n_i, n_j) \mid a_j - a_i$.

Inversamente, suponhamos que se para todo $i, j \in \{1, \ldots, k\}$, $(n_i, n_j) \mid a_j - a_i$. Vejamos, por indução sobre k, que o sistema admite uma e uma só solução módulo $[n_1, \ldots, n_k]$.

O caso $k = 2$ já foi visto.

Passo de indução: Suponhamos que $k > 2$.

Seja b uma solução das duas últimas congruências. Pelo que foi feito para o caso $k = 2$, o sistema original é equivalente ao sistema (com $k - 1$ congruências)

$$\begin{cases} x \equiv a_1 & (\bmod\ n_1) \\ \quad \ddots & \\ x \equiv a_{k-2} & (\bmod\ n_{k-2}) \\ x \equiv b & (\bmod\ [n_{k-1}, n_k]) \end{cases}$$

Para concluir a demonstração basta então usar a hipótese de indução e mostrar que:

- para todo o $i \leq k - 2$, $(n_i, [n_{k-1}, n_k]) \mid b - a_i$. Note-se que pela Proposição 1.11:
  - $(n_i, [n_{k-1}, n_k]) = [(n_i, n_{k-1}), (n_i, n_k)]$;
  - $[(n_i, n_{k-1}), (n_i, n_k)] \mid b - a_i$ se e só se $(n_i, n_{k-1}) \mid b - a_i$ e $(n_i, n_k) \mid b - a_i$.
- $[n_1, \cdots, n_{k-2}, [n_{k-1}, n_k]] = [n_1, \ldots, n_k]$ (Proposição 1.11). ■

Usando este teorema e o que já fizemos atrás, podemos concluir que os números inteiros positivos que divididos por $2, 3, 4, 5, 6$ dão resto $1, 2, 3, 4, 5$ (respectivamente) são os números da forma $-1 + 60\,t$ com $t \in \mathbb{N}$.

2.3 Sistemas

Nesta secção os anéis considerados têm elemento um (e) e são comutativos. Na prática estaremos a pensar em $\mathbb{Z}$ e nos anéis do tipo $\mathbb{Z}_n$.

Seja $< A, +, \cdot >$ um anel e consideremos as equações

$$2x + 4y = 0, \qquad x + 2y = 0 \quad \text{com } x, y \in A.$$

Note-se que:

- toda a solução da segunda equação é solução da primeira pois podemos obter a primeira equação multiplicando a segunda por 2;
- se $A = \mathbb{Z}_8$ as equações não são equivalentes pois $x = 4$ e $y = 0$ é solução da primeira equação e não da segunda;
- se $A = \mathbb{Z}_n$, com n ímpar então as equações são equivalentes, uma vez que podemos obter a segunda equação multiplicando a primeira pelo inverso de 2 módulo n;
- se $A = \mathbb{Z}$ as equações são equivalentes apesar de 2 não ser invertível em $\mathbb{Z}$. De facto estas equações são equivalentes num corpo do qual $\mathbb{Z}$ é um subanel.

Consideremos agora um sistema do tipo

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,m}x_m &= b_1 \\ & \ddots \\ a_{k,1}x_1 + \cdots + a_{k,m}x_m &= b_k \end{cases} \quad \text{em } A.$$

Para resolvermos este sistema podemos aplicar as regras que utilizaríamos se estivéssemos a trabalhar com um corpo ($\mathbb{R}$ ou $\mathbb{C}$, por exemplo) desde que tenhamos o cuidado de só utilizarmos passos que sejam reversíveis. Por exemplo:

- substituir a equação i por (s vezes a equação i)+ (r vezes a equação j) se $se = \underbrace{e + e + \cdots + e}_{s \text{ vezes}}$ for invertível.

A chamada **Regra de Cramer** (e suas consequências) também pode ser usada, no caso de o nosso anel ser comutativo e com elemento um, em vez de $\mathbb{R}$ ou $\mathbb{C}$. O único cuidado a ter é na exigência de que a matriz dos coeficientes tenha determinante invertível.

Consideremos então $M \in M_{m\times m}(A)$. Tem sentido falar na matriz $(M^{adj})^t$ (a transposta da matriz adjunta de M). É ainda verdade que, se $\det(M)$ representa o determinante da matriz M e I_m representa a matriz identidade $m \times m$ então

$$M(M^{adj})^t = \det(A)I_m$$

Daqui se conclui que A é uma matriz invertível se e só se $\det(M)$ é invertível, e nesse caso $M^{-1} = (\det(M))^{-1}(M^{adj})^t$.

Note-se que: se o anel for $\mathbb{Z}$ esta condição é equivalente a dizer que $\det(M) = \pm 1$; se o anel for $\mathbb{Z}_n$ esta condição é equivalente a dizer que $(\det(M), n) = 1$.

Consideremos agora um sistema do tipo

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,m}x_m &= b_1 \\ & \ddots \\ a_{m,1}x_m + \cdots + a_{m,m}x_m &= b_m \end{cases} \quad \text{em } A.$$

Este sistema pode ser escrito na forma $MX = B$, em que

$$M = \begin{pmatrix} a_{1,1} & \cdots & a_{1m} \\ & \ddots & \\ a_{m,1} & \cdots & a_{m,m} \end{pmatrix}, \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Se $\det(M)$ for invertível, então

$$MX = B \;\Leftrightarrow\; M^{-1}MX = M^{-1}B \;\Leftrightarrow\; X = M^{-1}B,$$

donde se conclui que o sistema tem uma só solução.

2.4 Exercícios

2.1. Resolva as equações (com $x, y \in \mathbb{Z}$):

a) $3x + y = 13$;

b) $3x - 12y = 13$;

c) $11x + 7y = 200$;

d) $153x + 27y = 13$;

e) $3x - 201y = 133$.

2.2. No exercício anterior quais das equações admitem soluções com $x, y \in \mathbb{N}$?

2.3. Temos duas balanças: uma que marca pesos múltiplos de 10 e outra que marca pesos múltiplos de 13. Como é que com essas balanças podemos pesar 107 gramas?

2.4. Apenas com a utilização de dois relógios que só dão intervalos de tempo de 5 e de 11 minutos como podemos cozer um ovo durante 3 minutos?

2.5. Mostre que duas progressões aritméticas $a, a + d, a + 2d, \ldots$ e $b, b + c, b + 2c, \ldots$ (com $a, b, c, d \in \mathbb{Z}$) têm termos em comum se e só se (d, c) divide $a - b$.

2.6. Resolva as congruências:

a) $23x \equiv 7 \pmod{19}$;

b) $6x \equiv -2 \pmod{28}$;

c) $25x \equiv 15 \pmod{120}$;

d) $15x \equiv 9 \pmod{25}$.

2.7. Para que valores de $x, y \in \mathbb{Z}$:

a) $372x + 420y = 36$;

b) $234x - 151y = 44$ e $5x + 6y$ é múltiplo de 7;

c) $120x + 63y = 12$ e $3x + 6y$ é múltiplo de 11.

2.8. Resolva as equações:

a) $15x + 21y + 35z = 0$;

b) $15x + 21y + 35z = 1$.

2.9. Seja k um inteiro positivo. Considere a equação

$$(k + 2)x + 6y = 3, \qquad x, y \in \mathbb{Z}.$$

a) Para que valores de $k \in \mathbb{Z}$, a equação admite solução?

b) Escolha $k > 10$ nas condições da alínea (a) e encontre uma solução da equação tal que $x > 1000$ e $y < -1000$.

c) Fixado k, mostre que, se x_0, y_0 é uma solução da equação $(k+2)x + 6y = 3$ então (x_0, y_0) divide 3.

2.10. Para que valores de $x, y \in \mathbb{Z} \setminus \{0\}$ se tem $\dfrac{x+y}{xy} \in \mathbb{Z}$?

2.11. Resolva a equação

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{13}, \quad x, y \in \mathbb{Z} \setminus \{0\}.$$

2.12. Sejam $a, b, c, d, x, y, m, n \in \mathbb{Z}$ tais que $m = ax + by$, $n = cx + dy$ e $|ad - bc| = 1$. Mostre que $(m, n) = (x, y)$.

2.13. Resolva a equação $(6x + 15y)(8x + 7y) = 129, \quad x, y \in \mathbb{Z}$.

2.14. Estude a congruência $(a^2+a+1)x \equiv 2a+1 \pmod{a+2}$. Escolha o menor inteiro positivo a para o qual a congruência tenha mais que uma solução. Em seguida resolva a equação.

2.15. Para que valores de $a, b \in \mathbb{Z}$ a congruência

$$(6a^2 - a - 5)x \equiv 3a + b \ (\bmod\ 2a + 3)$$

tem mais que uma solução módulo $2a + 3$?

Escolha $a, b \in \mathbb{Z}$ tais que a congruência tenha mais do que uma solução, com $a \geq 20$, e resolva a congruência.

2.16. Determine as soluções de:

a) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \end{cases}$

b) $\begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 4 \pmod{17} \\ x \equiv 10 \pmod{25} \end{cases}$

c) $\begin{cases} x \equiv 1 \pmod m \\ x \equiv 1 \pmod n \\ x \equiv 1 \pmod k \\ x \in \mathbb{Z} \setminus \{1\}. \end{cases}$

d) $\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 1 \pmod{13} \\ x \equiv 1 \pmod 6 \\ x \in [34\,000, 34\,300] \end{cases}$

2.17. Quais os dois menores inteiros positivos que divididos por 3, 5 e 7 dão restos 2, 3 e 2 respectivamente?

2.18. Resolva os seguintes sistemas:

a) $\begin{cases} 4x+7y \equiv 6 \\ 5x+4y \equiv 2 \end{cases}$ em $\mathbb{Z}_{12}$;

b) $\begin{cases} 2x+6y \equiv 6 \\ 3x+2y \equiv 2 \end{cases}$ em $\mathbb{Z}_{12}$;

c) $\begin{cases} 3x+5y+z \equiv 11 \\ 2x+3y+2z \equiv 4 \\ 5x+y+3z \equiv 5 \end{cases}$ em $\mathbb{Z}_{12}$;

d) $\begin{cases} 2x+y+4z \equiv 7 \\ 3x-2y+5z \equiv 2 \\ 2x+4y-3z \equiv 6 \end{cases}$ em $\mathbb{Z}_9$;

e) $\begin{cases} 6x+y+5z \equiv 7 \\ 3x+3y+10z \equiv 8 \\ 2x+5y+3z \equiv 1 \end{cases}$ em $\mathbb{Z}_{12}$;

f) $\begin{cases} 2x+3y+5z \equiv 36 \\ 12x+9y+20z \equiv 8 \\ 3x+4y+15z \equiv 33 \end{cases}$ em $\mathbb{Z}_{60}$.

2.19. a) Quantas soluções em inteiros positivos têm as equações diofantinas $8x+9y = 277$ e $8x+9y = 43$?

b) Sejam $a, b, c \in \mathbb{Z}$ tais que $(a, b) = 1$ e considere a equação diofantina $ax+by = c$. Verifique que uma condição suficiente para que a equação tenha n soluções positivas é $c > nab$. Verifique, usando a alínea anterior que esta condição não é necessária.

2.20. Sejam a e b inteiros positivos primos entre si e n um inteiro positivo. Uma solução x, y da equação diofantina $ax+by = n$ diz-se não negativa, se x e y não são negativos. Mostre que:

a) se $n > ab-a-b$, então existe uma solução não negativa para a equação.

b) se $n = ab-a-b$, então não existe solução não negativa.

3. Teorema de Euler e Teorema de Wilson

3.1 Teorema de Euler

Sejam $n \in \mathbb{N}$ e $\mathbb{Z}_n^* = \{a \in \mathbb{N} : 1 \leq a \leq n,\ (a,n) = 1\}$.

Usando o facto de o produto de dois números primos com n ser ainda um número primo com n e o Corolário 2.9, mostramos que $(\mathbb{Z}_n^*, \cdot_n)$ é um grupo, o grupo dos elementos invertíveis do anel $< \mathbb{Z}_n, +_n, *_n >$.

É claro que, $(\mathbb{Z}_1^*, \cdot_1)$ e $(\mathbb{Z}_2^*, \cdot_2)$ são o grupo trivial, pois $\mathbb{Z}_1^* = \mathbb{Z}_2^* = \{1\}$.

Por outro lado, é fácil de ver que o grupo $(\mathbb{Z}_n^*, \cdot_n)$ tem 4 elementos se e só se $n \in \{5, 8, 10, 12\}$. As seguintes são as tabelas destes quatro grupos.

$\cdot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

tabela de $(\mathbb{Z}_{10}^*, \cdot_{10})$

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

tabela de $(\mathbb{Z}_5^*, \cdot_{10})$

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

tabela de $(\mathbb{Z}_8^*, \cdot_{10})$

$\cdot_5$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

tabela de $(\mathbb{Z}_{12}^*, \cdot_{10})$

Note-se que os dois primeiros grupos são cíclicos e os dois seguintes são isomorfos ao chamado grupo de Klein.

De facto, um resultado que veremos e que não é trivial mostra que, dado $n \in \mathbb{N}$, o grupo $(\mathbb{Z}_n^*, \cdot_n)$ é cíclico se e só se n é igual a 1, 2, 4, é uma potência de um número primo ímpar ou é o dobro da potência de um número primo ímpar.

Definição 3.1 *À função de* $\mathbb{N}$ *em* $\mathbb{Z}$ *que associa a cada inteiro* n *o cardinal de* $\mathbb{Z}_n^*$*, chamamos* **função de Euler** *e denotamos por* φ*.*

Por exemplo,

- $\varphi(1) = \varphi(2) = 1$;
- $\varphi(5) = \varphi(8) = \varphi(10) = \varphi(12) = 4$;
- $\varphi(p) = p - 1$, se p é primo, porque $\mathbb{Z}_p^* = \{a \in \mathbb{N} : 1 \leq a \leq p - 1\}$;
- se p é um número primo, $\varphi(p) = p - 1$;
- se $n \geq 2$ e n não é primo, então $\varphi(n) < n - 1$, porque se p é um divisor primo de n, $\mathbb{Z}_n^* \subseteq \{a \in \mathbb{N} : 1 \leq a \leq n - 1,\ a \neq p\}$.

Nota 3.2 *Se* $n \in \mathbb{N}$*, então:*

- *se* A *é um* **scr** *então* $\varphi(n)$ *é o cardinal do conjunto* $\{a \in A : (a, n) = 1\}$*;*
- $\varphi(n)$ *é o cardinal de um qualquer* **srr** *de* n*.*

O chamado Teorema de Euler permite-nos calcular potências módulo n de dado número a, primo com n, utilizando apenas potências menores do que $\varphi(n)$.

Teorema 3.3 (Teorema de Euler) *Se* $a \in \mathbb{Z}$ *e* $n \in \mathbb{N}$*, então*

$$(a, n) = 1 \quad \Rightarrow \quad a^{\varphi(n)} \equiv 1 \ (\text{ mod } n).$$

Demonstração: Seja $\{a_1, \ldots, a_{\varphi(n)}\}$ um **srr** de n e suponhamos que $(a, n) = 1$. Pela Proposição 2.10, $\{aa_1, \ldots, aa_{\varphi(n)}\}$ é um **srr** de n. Em particular, para todo $i \leq \varphi(n)$ existe um e um só j tal que $a_i \equiv aa_j \pmod{n}$. Assim

$$\prod_{i \leq \varphi(n)} a_i \ \equiv \prod_{i \leq \varphi(n)} aa_i \ (\text{ mod } n) = a^{\varphi(n)} \prod_{i \leq \varphi(n)} a_i \ (\text{ mod } n)$$

Usando a lei do corte (Corolário 2.9 ii)) concluímos que $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Este resultado pode também ser visto como um corolário do teorema de Lagrange para grupos. De facto se r é o resto da divisão de a por n então $(r, n) = (a, n) = 1$ e portanto $r \in \mathbb{Z}_n^*$. Usando o teorema de Lagrange, $r^{\varphi(n)}$ é igual (no grupo $\mathbb{Z}_n^*$) a 1 (elemento neutro do grupo). Por outras palavras $r^{\varphi(n)} \equiv 1 \pmod{n}$. Assim

$$\begin{aligned} a^{\varphi(n)} &\equiv r^{\varphi(n)} \ (\bmod n), \quad \text{porque } a \equiv r \ (\bmod n) \\ &\equiv 1 \ (\bmod n) \qquad \text{pelo que vimos acima.} \end{aligned}$$

■

Vejamos algumas consequências imediatas.

Corolário 3.4 (Pequeno Teorema de Fermat) *Se a é um número inteiro e p é um número primo que não divide a, então $a^{p-1} \equiv 1 \pmod{p}$.* ■

Corolário 3.5 *Se a é um número inteiro e p é um número primo então $a^p \equiv a \pmod{p}$.*

Demonstração: Se $p \mid a$ então $a \equiv 0 \pmod{p}$ e portanto $a^k \equiv 0 \pmod{p}$ qualquer que seja $k \in \mathbb{N}$. Em particular $a^p \equiv a \pmod{p}$.

Se p não divide a então $(a, p) = 1$ e, pelo corolário anterior $a^{p-1} \equiv 1 \pmod{p}$. Multiplicando por a obtemos o resultado pretendido. ■

Corolário 3.6 *Se $n \in \mathbb{N}$, $m, k \in \mathbb{N}_0$ e $a \in \mathbb{Z}$ são tais que $m \equiv k \pmod{\varphi(n)}$ e $(a, n) = 1$ então, $a^m \equiv a^k \pmod{n}$.*

Demonstração: Basta considerar o caso em que $m > k$.

Como $m \equiv k \pmod{\varphi(n)}$ existe $q \in \mathbb{N}$ tal que $m - k = q\,\varphi(n)$ e, portanto,

$$a^m = a^{k+q\,\varphi(n)} = a^k \left(a^{\varphi(n)}\right)^q \equiv a^k \ (\bmod n),$$

pelo Teorema de Euler. ■

Podemos agora resolver questões do tipo: qual o resto da divisão de a^m por n? A dificuldade existe se os números envolvidos forem grandes. Começamos por calcular o resto da divisão de a por n. Se r for esse resto então

$$a^m \equiv r^m \pmod{n}.$$

Já reduzimos a base da potência e agora vamos reduzir o expoente, se $(a, n) = 1$. Usando o corolário anterior, se s for o resto da divisão de m por $\varphi(n)$ então

$$a^m \equiv r^m \equiv r^s \pmod{n}.$$

Por exemplo, usando o facto de que $(2351, 18) = 1$ e $\varphi(18) = 6$ temos

$$2351^{1000} \equiv 11^4 \pmod{18}$$

uma vez que $2351 \equiv 11 \pmod{18}$ e $1000 \equiv 4 \pmod{6}$.

Para continuarmos "temos" de fazer os cálculos!! Obtemos $2351^{1000} \equiv 7 \pmod{18}$.

3.1.1 Números de Carmichael

Existem inteiros positivos n, que não são primos e que verificam a conclusão do Pequeno Teorema de Fermat.

Exemplo 3.7 *Sejam $n = 561$ $(= 3 \times 11 \times 17)$ e a um inteiro qualquer primo com 561. Como $\varphi(3)$, $\varphi(11)$ e $\varphi(17)$ dividem 560 podemos concluir, usando o Corolário 3.6, que a^{560} é congruente com 1, módulo 3, 11 e 17, ou seja, que $a^{560} \equiv 1 \pmod{561}$.*

Chegamos assim à seguinte definição.

Definição 3.8 *Um inteiro composto n diz-se um* **número de Carmichael**, *ou* **pseudoprimo**, *se:*

$$\forall a \in \mathbb{N} \ \left[(a, n) = 1 \ \Rightarrow \ a^{n-1} \equiv 1 \pmod{n}\right].$$

Os números de Carmichael são raros:

- menores que 100 000 são apenas: 561, 1 105, 1 729, 2 465, 2 821, 6 601, 8 911, 10 585, 15 841, 29 341, 41 041, 46 657, 52 633, 62 745, 63 973 e 75 361;

- existem apenas 2 163 que são menores que 25 000 000 000;
- existem apenas 246 683 que são menores que 10 000 000 000 000 000.

Apenas em 1994 foi demonstrado que existe um número infinito de números de Carmichael. Referência:W. R. Alford, A. Granville and C. Pomerance, "There are infinitely many Carmichael numbers," Ann. of Math., 140 (1994) 703-722.

Para mais resultados sobre números de Carmichael ver, por exemplo, http://www.utm.edu/research/primes/glossary/CarmichaelNumber.html

O seguinte resultado pode ser mostrado com um argumento análogo ao usado no Exemplo 3.7.

Proposição 3.9 *Seja $n = p_1 \cdots p_k$ com $k \geq 2$ e $p_1, \ldots, p_k$ números primos distintos, tais que*

$$\forall i \leq k \quad (p_i - 1) | (n - 1)$$

então n é um pseudoprimo. ■

Veremos mais tarde que todo o número de Carmichael é da forma referida na proposição anterior.

Exemplos 3.10 *A título de curiosidade, os menores números de Carmichael com k factores primos distintos são:*

- $561 = 3 \times 11 \times 17$, *se* $k = 3$;
- $41\,041 = 7 \times 11 \times 13 \times 41$, *se* $k = 4$;
- $825\,265 = 5 \times 7 \times 17 \times 19 \times 73$, *se* $k = 5$;
- $321\,197\,185 = 5 \times 19 \times 23 \times 29 \times 37 \times 137$, *se* $k = 6$;
- $5\,394\,826\,801 = 7 \times 13 \times 17 \times 23 \times 31 \times 67 \times 73$, *se* $k = 7$;
- $232\,250\,619\,601 = 7 \times 11 \times 13 \times 17 \times 31 \times 37 \times 73 \times 163$, *se* $k = 8$;

- $9\,746\,347\,772\,161 = 7 \times 11 \times 13 \times 17 \times 19 \times 31 \times 37 \times 41 \times 641$, *se* $k = 9$;
- $1\,436\,697\,831\,295\,441 = 11 \times 13 \times 19 \times 29 \times 31 \times 37 \times 41 \times 43 \times 71 \times 127$, *se* $k = 10$;
- $60\,977\,817\,398\,996\,785 = 5 \times 7 \times 17 \times 19 \times 23 \times 37 \times 53 \times 73 \times 79 \times 89 \times 233$, *se* $k = 11$;
- $7\,156\,857\,700\,403\,137\,441 = 11 \times 13 \times 17 \times 19 \times 29 \times 37 \times 41 \times 43 \times 61 \times 97 \times 109 \times 127$, *se* $k = 12$;
- $1\,791\,562\,810\,662\,585\,767\,521 = 11 \times 13 \times 17 \times 19 \times 31 \times 37 \times 43 \times 71 \times 73 \times 97 \times 109 \times 113 \times 127$, *se* $k = 13$;
- $87\,674\,969\,936\,234\,821\,377\,601 = 7 \times 13 \times 17 \times 19 \times 23 \times 31 \times 37 \times 41 \times 61 \times 67 \times 89 \times 163 \times 193 \times 241$, *se* $k = 14$;
- $6\,553\,130\,926\,752\,006\,031\,481\,761 = 11 \times 13 \times 17 \times 19 \times 29 \times 31 \times 41 \times 43 \times 61 \times 71 \times 73 \times 109 \times 113 \times 127 \times 181$, *se* $k = 15$;
- $1\,590\,231\,231\,043\,178\,376\,951\,698\,401 = 17 \times 19 \times 23 \times 29 \times 31 \times 37 \times 41 \times 43 \times 61 \times 67 \times 71 \times 73 \times 79 \times 97 \times 113 \times 199$, *se* $k = 16$.

Exercício 3.11 *Mostre que, se* $k \in \mathbb{N}$ *é tal que* $6k+1$, $12k+1$, $18k+1$ *são números primos, então* $(6k+1)(12k+1)(18k+1)$ *é um número de Carmichael.*

Apenas a título de curiosidade, um número composto n diz-se um **pseudoprimo de base** a se $a^{n-1} \equiv 1 \pmod{n}$. Assim, um inteiro n é um pseudoprimo se for pseudoprimo de base a, para todo a, primo com n.

Exemplos 3.12 *Vejamos alguns exemplos de pseudoprimos nas bases* 2 *e* 3*;*

- *na base* 2*:* 341, 561, 645, 1105, 1387, 1729, 1905, 915981, 916327, 934021, 950797, 976873, 983401, 997633*;*
- *na base* 3*:* 954577, 962809, 966301, 973241, 992251, 994507, 997633

Contrariamente ao que acontece para os números de Carmichael, é muito fácil (comparativamente) mostrar que existe uma infinidade de pseudoprimos de base a (com $a \in \mathbb{N}$). Vou fazer a demonstração no caso $a = 2$.

Proposição 3.13 *Se n é um pseudoprimo ímpar de base 2, então $2^n - 1$ é também um pseudoprimo ímpar de base 2.*

Demonstração: Sejam d, k tais que $n = dk$ e $1 < d, k < n$, e seja $m = 2^n - 1$. Então m é um número composto pois é divisível por $2^d - 1$.

Por hipótese $2^{n-1} \equiv 1 \pmod{n}$ e portanto, existe $k \in \mathbb{N}$ tal que $2^{n-1} - 1 = kn$. Assim,

$$2^{m-1} - 1 = 2^{2^n - 2} - 1 = 2^{2(2^{n-1}-1)} - 1 = 2^{2kn} - 1.$$

Em particular, $2^{m-1} - 1$ é um múltiplo de $m = 2^n - 1$, ou seja $2^m - 1 \equiv \pmod{m}$.

Concluímos assim que m é um pseudoprimo de base 2. ■

Corolário 3.14 *Existe uma infinidade de pseudoprimos de base 2,*

Demonstração: Basta notar que 341 é um pseudoprimo ímpar de base 2 e aplicar sucessivamente a proposição anterior. ■

A demonstração da existência de uma infinidade de pseudoprimos numa base qualquer a pode também ser feita de modo elementar (ver exercício seguinte).

Exercício 3.15 *Seja $a \in \mathbb{N}$, p um número primo que não divide $a^2 - 1$ e $m = \frac{a^{2p}-1}{a^2-1}$. Mostre que:*

a) *p divide $(m-1)(a^2-1)$;*

b) *p divide $m - 1$;*

c) *$2p$ divide $m - 1$;*

d) *$a^{2p} = 1 + m(a^2 - 1)$. Em particular $a^{2p} = 1 \pmod{m}$;*

e) *m é pseudoprimo de base a;*

f) *existe uma infinidade de pseudoprimos de base a.*

Note-se que o facto de existir uma infinidade de pseudoprimos em qualquer base não implica a existência de uma infinidade de pseudoprimos.

Nota 3.16 *Em termos computacionais é muito difícil verificar que um dado inteiro n é primo, mas é fácil ver se ele satisfaz uma condição do género $a^{n-1} \equiv 1 \pmod{n}$(com a fixo). Em particular, esta condição pode ser a primeira a ser testada para a verificação de que um dado inteiro é um número primo. Note-se que, apesar de existir um número infinito de números de Carmichael, assimptoticamente existem poucos quando comparados com os números primos. Por exemplo, no intervalo $[1,\ 25 \times 10^9]$, existem $2\,163$ números de Carmichael, $21\,853$ pseudoprimos na base 2 e $1\,091\,987\,405$ primos.*

Deste modo, se tivermos a lista de todos os pseudoprimos de base 2 até 25×10^9 podemos "facilmente" ver se um dado número n menor do que 25×10^9 é ou não primo, verificando simplesmente se ele não pertence à lista e se $2^n \equiv 1 \pmod{n}$.

3.2 Teorema de Wilson

O teorema, dito Teorema de Wilson (século $XVIII$) foi demonstrado pela primeira vez por Lagrange (um ano depois de ter sido enunciado por Wilson).

Comecemos por um resultado preliminar.

Lema 3.17 *Sejam p um número primo e $a \in \mathbb{N}$ então*

$$a^2 \equiv 1 \pmod{p} \iff [a \equiv 1 \pmod{p} \text{ ou } a \equiv -1 \pmod{p}].$$

Demonstração: Basta notar que:

$$\begin{aligned} a^2 \equiv 1 \pmod{p} &\Leftrightarrow p|(a^2-1) \\ &\Leftrightarrow p|(a-1)(a+1) \\ &\Leftrightarrow p|a-1 \text{ ou } p|a+1 \quad \text{pelo Corolário 1.7} \\ &\Leftrightarrow a \equiv 1 \pmod{p} \text{ ou } a \equiv -1 \pmod{p}. \end{aligned}$$

■

Teorema 3.18 (Teorema de Wilson) *Se p é um número primo, então*

$$(p-1)! \equiv -1 \ (\mod p).$$

Demonstração: Para cada $a \in \mathbb{Z}_p^* \setminus \{1, p-1\}$ seja $a' \in \mathbb{Z}_p^*$ tal que $aa' \equiv 1 \pmod{p}$ (recorde-se que $\mathbb{Z}_p^*$ é um grupo). Note-se que:

- se $a \in \mathbb{Z}_p^* \setminus \{1, p-1\}$, então $a \neq a'$ (pelo lema anterior);
- se $a, b \in \mathbb{Z}_p^* \setminus \{1, p-1\}$ então $\{a, a'\} = \{b, b'\}$ ou $\{a, a'\} \cap \{b, b'\} = \emptyset$.

Daqui se conclui que $\mathbb{Z}_p^* \setminus \{1, p-1\}$ é uma união disjunta de conjuntos da forma $\{a, a'\}$ de tal modo que $a \neq a'$ e $aa' = 1$. Assim $\prod_{x \in \mathbb{Z}_p^* \setminus \{1, p-1\}} x = 1$ e portanto

$$\begin{aligned} (p-1)! &= 1 \times (p-1) \times \prod_{x \in \mathbb{Z}_p^* \setminus \{1, p-1\}} x \\ &\equiv 1 \times (p-1) \times 1 \ (\mod p) \\ &\equiv -1 \ (\mod p). \end{aligned}$$

■

Para ilustrar a demonstração do Teorema de Wilson vamos considerar $p = 13$. Assim

$$\begin{aligned} 12! &= 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12 \\ &= 1 \times 12 \times (2 \times 7) \times (3 \times 9) \times (4 \times 10) \times (5 \times 8) \times (6 \times 11) \\ &\equiv -1 \ (\mod 13). \end{aligned}$$

Contrariamente ao que acontece com o Teorema de Euler, a propriedade enunciada no Teorema de Wilson caracteriza os números primos.

Proposição 3.19 *Seja $n > 1$. Então, se n não é primo,*

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

Demonstração: Se $n = 4$ então $(n-1)! = 6 \equiv 2 \pmod 4$.

Se $n > 4$, sejam $r, s \in \mathbb{N}$ tais que $1 < s \leq r < n$ e $n = rs$. Temos dois casos a considerar

- se $s < r$ então

$$\begin{aligned}(n-1)! &= s \times r \times \prod_{a \in \{1,\ldots,n-1\}\setminus\{s,r\}} a = n \times \prod_{a \in \{1,\ldots,n-1\}\setminus\{s,r\}} a \\ &\equiv 0 \ (\bmod n);\end{aligned}$$

- se $s = r$, então $2 < r$ pois caso contrário n seria igual a 4. Assim, $n = r^2 > 2r$ e

$$\begin{aligned}(n-1)! &= r \times 2r \times \prod_{a \in \{1,\ldots,n-1\}\setminus\{r,2r\}} a = 2n \times \prod_{a \in \{1,\ldots,n-1\}\setminus\{r,2r\}} a \\ &\equiv 0 \ (\bmod n).\end{aligned}$$

■

Corolário 3.20 *Se $n > 1$ então*

$$[n \text{ é um número primo } \Leftrightarrow (n-1)! \equiv -1 \ (\bmod n)]\,.$$

■

Apesar de este resultado dar uma caracterização dos números primos, na prática ela não ajuda muito, pois o cálculo de $k!$ (para k "grande") é computacionalmente impraticável.

O teorema de Wilson pode ser generalizado de duas maneiras (ver folhas de exercícios):

- se p é primo e $p > n \geq 1$ então

$$(n-1)!(p-n)! \equiv (-1)^n \ (\bmod p);$$

- se p é primo e $n \geq 1$ então

$$[(p-1)!]^{p^{n-1}} \equiv -1 \ (\bmod p^n).$$

3.3 A função de Euler

Veremos nesta secção que a função de Euler φ satisfaz a condição:

$$\forall m, n \in \mathbb{N}\ [(n, m) = 1\ \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)]$$

o que nos levará a encontrar uma formula para $\varphi(n)$ dada uma factorização de n como produto de potências de primos (ou se conhecermos todos os números primos que dividem n).

Note-se que em geral, se $n, m \in \mathbb{N}$, não se tem a igualdade $\varphi(nm) = \varphi(n)\varphi(m)$ (basta considerar $n = m = 2$). De facto (ver Exercício 37) $\varphi(nm) = \varphi(n)\varphi(m)$ se e só se $(n, m) = 1$.

Vamos começar por calcular $\varphi(p^k)$ para qualquer primo p e inteiro positivo k.

Lema 3.21 *Se p é um número primo e $k \in \mathbb{N}$,*

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1).$$

Demonstração: Os números inteiros que são não são primos com p^k são os múltiplos de p. Como existem p^{k-1} múltiplos de p entre 1 e p^k concluímos que $\varphi(p^k) = p^k - p^{k-1}$. ■

Como exemplo: $\varphi(121) = 11 \times 10 = 110$.

Teorema 3.22 *A função de Euler satisfaz a condição*

$$\forall m, n \in \mathbb{N}\ [(n, m) = 1\ \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)].$$

Demonstração: Sejam $m, n \in \mathbb{N}$ com $(m, n) = 1$. Vamos mostrar que no conjunto $\{1, 2, \ldots, mn\}$ existem $\varphi(n)\varphi(m)$ elementos primos com mn.

Plano da demonstração:

- note-se que um número é primo com nm se e só se for primo com n e com m;
- dispomos os números $1, 2, \ldots, mn$ numa tabela de m linhas e n colunas;

- mostramos que os elementos que são primos com m são exactamente os que estão em $\varphi(m)$ dessas linhas;
- veremos depois que, em cada uma dessas linhas existem $\varphi(n)$ elementos que são primos com n;
- concluímos assim que existem $\varphi(n)\varphi(m)$ elementos primos com mn.

Consideremos a tabela

linha 1	1	m+1	2m+1	$\cdots$	(n-1)m+1
linha 2	2	m+2	2m+2	$\cdots$	(n-1)m+2
linha 3	3	m+3	2m+3	$\cdots$	(n-1)m+3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
linha m	m	2m	3m	$\cdots$	nm

Seja $r \in \{1, 2, \ldots, m\}$. Notando que os elementos da linha r são da forma $im + r$ e que $(im + r, m) = (r, m)$, podemos concluir que:

- se $(r, m) = 1$, todos os elementos da linha r são primos com m;
- se $(r, m) \neq 1$, nenhum elemento da linha r é primo com m;
- por definição de $\varphi(m)$, existem $\varphi(m)$ linhas nas condições acima;
- usando o Proposição 2.7, cada linha constitui um **scr** de n;
- pela Nota 3.2, cada linha tem $\varphi(n)$ elementos primos com n;
- existem $\varphi(n)\varphi(m)$ elementos primos com m e com n. ■

Como corolário deste teorema e do Lema 3.21, temos uma fórmula para o cálculo de $\varphi(n)$, se $n \in \mathbb{N}$.

Corolário 3.23 *Se $n = p_1^{n_1} \cdots p_k^{n_k}$, em que $p_1, \ldots, p_k$ são números primos distintos, e $n_1, \ldots, n_k \in \mathbb{N}$ então,*

$$\begin{aligned} \varphi(n) &= (p_1^{n_1} - p_1^{n_1-1}) \cdots (p_k^{n_k} - p_k^{n_k-1}) \\ &= p_1^{n_1-1} \cdots p_k^{n_k-1}(p_1 - 1) \cdots (p_k - 1) \\ &= n \prod_{p \in \mathbb{P},\, p|n} (1 - \frac{1}{p}). \end{aligned}$$

■

Exemplos 3.24 $\varphi(253) = \varphi(11 \times 23) = 10 \times 22 = 220$, $\varphi(100) = \varphi(2^2 \times 5^2) = 2 \times 5 \times 4 = 40$.

Nota 3.25 *As funções $f : \mathbb{N} \to \mathbb{N}$, que satisfazem a condição,*

$$\forall m, n \in \mathbb{N}\ [(n, m) = 1\ \Rightarrow f(nm) = f(n)f(m)]$$

dizem-se funções multiplicativas.

Deste modo, se f é multiplicativa e $n = p_1^{n_1} \cdots p_k^{n_k}$, em que $p_1, \ldots, p_k$ são primos distintos e $n_1, \ldots, n_k \in \mathbb{N}$ então

$$f(n) = f(p_1^{n_1}) \cdots f(p_k^{n_k}).$$

Exercício 3.26 *As funções:*

$$\begin{aligned} \tau : \ \mathbb{N} &\longrightarrow \mathbb{N}; \\ n &\mapsto \text{número de divisores positivos de } n \\ \sigma : \ \mathbb{N} &\longrightarrow \mathbb{N}. \\ n &\mapsto \text{soma dos divisores positivos de } n \end{aligned}$$

são multiplicativas.

Como consequência da Nota 3.25 o seguinte corolário dá-nos uma expressão para $\tau(n)$ e $\sigma(n)$ (se conhecermos uma factorização de n como produto de potências de n).

Corolário 3.27 *Se $n = p_1^{n_1} \cdots p_k^{n_k}$, em que $p_1, \ldots, p_k$ são primos distintos e $n_1, \ldots, n_k \in \mathbb{N}$ então*

- $\tau(n) = (1 + n_1) \times \cdots \times (1 + n_k)$;
- $\sigma(n) = \frac{p_1^{n_1+1}-1}{p_1-1} \times \cdots \times \frac{p_k^{n_k+1}-1}{p_k-1}$. ■

3.4 Exercícios

3.1. Mostre, usando ou não o Teorema de Euler, que:

a) $a^7 \equiv a \pmod{63}$, se $3 \nmid a$;

b) $42 \mid (n^7 - n)$ para todo o n inteiro positivo;

c) $5n^3 + 7n^5 \equiv 0 \pmod{12}$ para todo o n inteiro positivo;

d) $2^{161038} \equiv 2 \pmod{161038}$ (comece por factorizar o número 161038).

3.2. Use o pequeno teorema de Fermat para encontrar:

a) o último digito de 3^{100};

b) o resto da divisão de $2^{1000000}$ por 17;

c) o resto da divisão de $3^{1000000}$ módulo 35;

d) a solução das congruência linear $7x \equiv 12 \pmod{17}$;

e) a solução das congruência linear $4x \equiv 11 \pmod{19}$.

3.3. Mostre que, se a é primo com 32760, então $a^{12} \equiv 1 \pmod{32760}$.

3.4. Existe algum inteiro positivo a menor do que 10 tal que $1000^{1000} + a$ é divisível por 17?

3.5. Use o teorema de Wilson para encontrar o menor resíduo de $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ módulo 7.

3.6. Verifique se existe $a \in \mathbb{N}$ tal que $a1000^{1000} + (a+2)99! \equiv 0 \pmod{101}$.

3.7. Mostre que $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ se a e b são inteiros primos entre si. Em particular, se a e b forem primos distintos, então $a^{b-1} + b^{a-1} \equiv 1 \pmod{ab}$.

3.8. Mostre que, se p e q são primos ímpares tais que $2p = q+1$ e a é um inteiro ímpar não divisível por p nem por q, então $a^{2(p-1)} \equiv 1 \pmod{16pq}$.

3.9. Demonstre a Proposição 3.9.

3.10. Mostre que, se p é primo e a é um inteiro, então $p \mid [a^p + (p-1)!a]$.

3.11. Mostre que, se n é um inteiro ímpar, então n divide $1^n + 2^n + \cdots + (n-1)^n$.

3.12. Seja p um número primo. Mostre que $2, 3, \ldots, p-1$ são soluções da congruência

$$x^{p-2} + x^{p-3} + \cdots + x + 1 \equiv 0 \ \ (\mod p).$$

Sugestão: Use a igualdade $(x^{p-1} - 1) = (x-1)(x^{p-2} + x^{p-3} + \cdots + x + 1)$.

3.13. Calcule todos os números primos p tais que $(p-1)^p + 1$ é divisível por p^{p-1}.

3.14. Seja $p \in \mathbb{N}$ um número primo. Mostre que:

a) p é o menor primo que divide $(p-1)! + 1$.

b) se $n \in \mathbb{N}$ e $p > n$ então $(n-1)!(p-n)! \equiv (-1)^n \pmod{p}$.

c) se $n \geq 1$ então $[(p-1)!]^{p^{n-1}} \equiv -1 \pmod{p^n}$.

3.15. Seja p um número primo ímpar. Mostre que:

a) $(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$.
Sugestão: Note que, se $k \in \mathbb{N}$, $k \equiv -(p-k) \pmod{p}$;

b) se $p \equiv 3 \pmod 4$, então $((p-1)/2)! \equiv \pm 1 \pmod{p}$;

c) se $p \equiv 1 \pmod 4$, então a congruência $x^2 \equiv -1 \pmod{p}$ tem duas soluções.

3.16. Mostre que, se p é um número primo ímpar, então

$$(p-1)! \equiv p-1 \ (\mod (1+2+\cdots+(p-1))).$$

3.17. Seja p um primo ímpar. Mostre que:

$$1^2 3^2 5^2 \cdots (p-2)^2 \equiv 2^2 4^2 6^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \ (\mod p).$$

3.18. Seja $n \in \mathbb{N}$. Mostre que $(n-1)!+1$ é uma potência de n se e só se $n \in \{2,3,5\}$.

Passos da demonstração:

a) se $n \in \mathbb{N} \setminus \{1\}$ e n não é primo então $(n-1)!+1$ não é uma potência de n;

b) se $n \geq 3$, $n^{n-1} > (n-1)!+1$;

c) se $n > 5$ e $n-1$ não é primo então $(n-1)^2 | (n-1)!$;

d) se p é primo $p|(p-1)!+1$;

e) se p é primo e existe $k \in \mathbb{N}$ tal que $(p-1)!+1 = p^k$ então $p-1|p^{k-1}+\cdots+p+1$ e portanto $p-1|k$.

3.19. Sejam N um inteiro positivo ímpar e s,t,p,k,m tais que $N-1 = 2^s t$, t ímpar, $N = p^k m$ e $p \not| m$.

Se $b \in \mathbb{N}$ e $(b,N) = 1$ diz-se que N é um b-ppf (b-pseudoprimo forte) se, $b^t \equiv 1 \ (\mod N)$ ou existe $0 \leq j < s$ tal que $b^{2^j t} \equiv -1 \ (\mod N)$.

Mostre que:

a) se $N = 2047 \ (= 23 \times 89)$ então N é um 2-ppf;

b) se N é um b-ppf então $b^{N-1} \equiv 1 \ (\mod N)$;

c) se $N = p$ então N é um b-ppf para todo $b < N$.

Como curiosidade, refira-se que se N é um b-ppf para todo $b < N$, com $(b,N) = 1$ então N é primo.

3.20. Calcule $\varphi(n)$ para todo o inteiro n menor que 21.

3.21. Determine o valor da função de Euler para cada um dos seguintes inteiros:

a) 100; b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$; c) 256;
d) 10!; e) 1001; f) 20!.

3.22. Seja $n > 1$. Mostre que n não é primo se e só se $\varphi(n) \leq n - \sqrt{n}$.

3.23. Seja n um inteiro positivo. Defina a sequência de inteiros positivos $n_1, n_2, n_3, ...$ recursivamente por; $n_1 = \varphi(n)$ e $n_{k+1} = \varphi(n_k)$ para $k \in \mathbb{N}$. Mostre que, qualquer que seja n, existe um inteiro positivo r tal que $n_r = 1$.

3.24. Mostre que, se $n = 2^{\alpha}m$ em que m é um produto de k potências de primos ímpares distintos e $\alpha \in \mathbb{N}_0$, então $2^{k+max\{0,\alpha-1\}}$ divide $\varphi(n)$.

Em particular, se n é um inteiro positivo divisível por k primos ímpares distintos, então $\varphi(n)$ é divisível por 2^k.

3.25. Mostre que, se $\varphi(n) \equiv 2 \pmod 4$ então $n = 4$ ou $n = p^s$ ou $n = 2p^s$ em que p é um primo da forma $4n + 3$.

3.26. Determine todos os inteiros positivos n tais que $\varphi(n)$ toma o valor:

a) 1; b) 6; c) 2 d) 14; e) 3; f) 24.

3.27. Para que inteiros positivos n, $\varphi(n)$ é:

a) ímpar;
b) divisível por 4;
c) igual a $n/2$?

3.28. Para que valores de n se tem:

a) $\varphi(n) = \varphi(2n)$;
b) $\varphi(n) = 12$;
c) $\varphi(n) = \frac{32}{77}n$;
d) $\varphi(n) = \frac{2}{7}n$;
e) $\varphi(2n) = \varphi(3n)$;
f) $\varphi(n) = \frac{3n}{35}$;

g) $\varphi(n) = \frac{1}{p}n$ (p primo fixo);

h) $\varphi(n)$ é uma potência de 2.

3.29. Encontre $n \in \mathbb{N}$ tal que $\varphi(n) = 475200$.

3.30. Mostre que existe uma infinidade de inteiros positivos n tais que $\varphi(5n) = \varphi(4n)$.

3.31. Encontre um inteiro positivo n que seja um quadrado perfeito e tal que

$$119|\varphi(n), \quad 7 \not| n, \quad 17 \not| n.$$

3.32. Para que valores de $x, y \in \mathbb{N}$, $x^{\varphi(y)} = y$?

3.33. Quais das seguintes afirmações são verdadeiras:

a) se $(m, n) = 1$ então $(\varphi(n), \varphi(m)) = 1$;

b) se n não é primo, então $(n, \varphi(n) > 1$;

c) se m e n são divisíveis pelos mesmos primos então $n\varphi(m) = m\varphi(n)$;

d) se $n\varphi(m) = m\varphi(n)$ então m e n são divisíveis pelos mesmos primos.

3.34. Mostre que, se m e k são inteiros positivos, então $\varphi(m^k) = m^{k-1}\varphi(m)$.

3.35. Para que inteiros positivos m, $\varphi(m)$ divide m?

3.36. Mostre que existe uma infinidade de inteiros n tais que $\varphi(n)$ é um quadrado perfeito.

3.37. Mostre que, se $d = (m, n)$, então

$$\varphi(nm) = \varphi(n)\varphi(m) \cdot \frac{d}{\varphi(d)}.$$

Conclua que $\varphi(nm) = \varphi(n)\varphi(m)$ se e só se $(n, m) = 1$.

3.38. Mostre que $\varphi(n) > \frac{n}{6}$, se n tem no máximo 8 factores primos distintos.

3.39. Seja k um inteiro positivo. Mostre que a equação (na incógnita $n \in \mathbb{N}$)

$$\varphi(n) = k,$$

tem um número finito de soluções?

3.40. Demonstre o Corolário 3.27.

3.41. Determine o número de divisores inteiros positivos de:

a) 36; b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$; c) 99;
d) 144; e) $2 \cdot 3^2 \cdot 5^3 \cdot 7^4 \cdot 11^5 \cdot 13^4 \cdot 17^5 \cdot 19^5$; f) 20!.

3.42. Determine a soma dos divisores inteiros positivos de;

a) 35; b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$; c) 196; d) $2^5 3^4 5^3 7^2 11$;
e) 1000; f) 10!; g) 2^{100}; h) 20!.

3.43. Determine o menor inteiro positivo n tal que $\tau(n)$ é igual a:

a) 1; b) 6; c) 2;
d) 14; e) 3; f) 100.

3.44. Determine todos os inteiros positivos n tal que $\sigma(n)$ é igual a:

a) 12; b) 48; c) 18;
d) 52; e) 24; f) 84.

3.45. Mostre que $\tau(n)$ é ímpar se e só se n é um quadrado.

3.46. Mostre que um inteiro positivo n é composto se e só se $\sigma(n) > n + \sqrt{n}$.

3.47. Mostre que, se p é um número primo e $k \in \mathbb{N}$, então $p^k\sigma(p^k) \equiv p^{k-1}\tau(p^k) \pmod{\varphi(p^k)}$.

3.48. Mostre que, se $n \in \mathbb{N}$ então $\tau(n) \leq 2\sqrt{n}$.

3.49. Seja $n \in \mathbb{N}$. Mostre que o produto dos divisores positivos de n é igual a $n^{\frac{\tau(n)}{2}}$. Quando é que esse produto é igual a n^2?

3.50. Seja n um inteiro positivo maior que 1. Defina a sequência de inteiros $n_1, n_2, n_3, ...$ por $n_1 = \tau(n)$ e $n_{k+1} = \tau(n_k)$ para $k \in \mathbb{N}$. Mostre que existe um inteiro positivo r tal que $n_r = 2$.

3.51. Mostre que, se $k > 1$ é um inteiro, então existe uma infinidade de inteiros com exactamente k divisores.

3.52. Mostre que não existem dois inteiros positivos com o mesmo produto de divisores.

3.53. Seja $n \in \mathbb{N}$. Mostre que n é um número perfeito (isto é, tal que $\sigma(n) = 2n$) par, se e só se existe $p \in \mathbb{N}$ tal que $n = 2^{p-1}(2^p - 1)$, sendo $2^p - 1$ um número primo. **Sug**: Comece por escrever n na forma $n = 2^k m$ em que m é um inteiro ímpar.

3.54. Sejam $k \in \mathbb{N}$ e $a = 2^k$. Mostre que $\sigma(\sigma(a)) = 2a$ se e só se $2^{k+1} - 1$ é um número primo.

4. Congruências quadráticas

Neste capítulo vamos encontrar métodos de resolução de congruências do tipo

$$ax^2 + bx + c \equiv 0 \ (\text{mod } n), \text{ com } n \in \mathbb{N},\ a, b, c \in \mathbb{Z} \text{ e } (a, b, c, n) = 1 \qquad (4.1)$$

É claro que se tivermos uma congruência $ax^2 + bx + c \equiv 0 \pmod{n}$, com $n \in \mathbb{N}$ e $a, b, c \in \mathbb{Z}$ mas com $(a, b, c, n) > 1$ então a congruência é equivalente à congruência $Ax^2+Bx+C \equiv 0 \pmod{N}$ em que $A = \frac{a}{(a,b,c,n)}$, $B = \frac{b}{(a,b,c,n)}$, $C = \frac{c}{(a,b,c,n)}$, $N = \frac{n}{(a,b,c,n)}$ e nesse caso $(A, B, C, N) = 1$.

Abuso de notação: Se a é uma solução de uma congruência quadrática módulo n então $a + tn$, com $t \in \mathbb{Z}$ também é solução da mesma congruência. Deste modo ou a congruência não tem solução ou então tem uma infinidade de soluções.
Por abuso de notação, quando dissermos que **uma congruência quadrática módulo n tem k soluções** estaremos a pensar em k soluções incongruentes módulo n. No fundo estaremos a trabalhar no anel $\mathbb{Z}_n$.

4.1 Redução ao estudo de congruências do tipo $x^2 \equiv a \pmod{p^k}$

Nesta secção vamos mostrar que para resolvermos uma congruência quadrática basta-nos saber resolver equações do tipo $x^2 \equiv a \pmod{p^k}$, para além de sistemas de congruências lineares.

Consideremos a equação (4.1) e seja $d = (a, n)$ e suponhamos que $d > 1$ (não esquecer que $(a, b, c, n) = 1$). Note-se que

$$\begin{aligned} ax^2 + bx + c \equiv 0 \ (\mod n) &\implies ax^2 + bx + c \equiv 0 \ (\mod d) \\ &\implies bx + c \equiv 0 \ (\mod d), \quad \text{pois } a \equiv 0 \ (\mod d). \end{aligned}$$

Vamos agora resolver a congruência $bx + c \equiv 0 \pmod{d}$. Seja $d^* = (b, d) = (b, a, n)$.

- Se d^* não divide c então a congruência não tem solução e portanto a congruência (4.1) também não tem solução.
- Se d^* divide c então $d^* = 1$ pois d^* é um divisor de a, b, c e n e sabemos que $(a, b, c, n) = 1$. A solução desta congruênca linear é da forma $x = \alpha + d\,t$ com $t \in \mathbb{Z}$ em que α é uma solução particular. Substituindo na congruência (4.1) obtemos

  $$ad^2\,t^2 + (2a\alpha d + bd)\ t + \left(a\alpha^2 + b\alpha + c\right) \ \equiv \ 0 \ (\mod n)$$

  ou seja, porque $a\alpha^2 + b\alpha + c$ e n são múltiplos de d,

  $$ad\,t^2 + (2a\alpha + b)\ t + \frac{a\alpha^2 + b\alpha + c}{d} \ \equiv \ 0 \ (\mod \frac{n}{d}).$$

  Se o máximo divisor comum entre ad e $\frac{n}{d}$ for maior que 1 repetimos o processo.

Cada vez que aplicarmos este processo obtemos uma congruência sem solução ou então uma congruência módulo um inteiro positivo menor que o original. Deste modo, mais cedo ou mais tarde o processo termina. Isso acontece quando a congruência não tem solução ou quando chegamos a uma congruência em que o coeficiente do termo quadrático e o módulo da congruência são primos entre si.

Conclusão: Aplicando sucessivamente este raciocínio podemos concluir que para resolver congruências quadráticas basta-nos saber resolver congruências do tipo

$$ax^2 + bx + c \ \equiv \ 0 \ (\mod n) \tag{4.2}$$

em que $n \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$ e $(a, n) = 1$.

Por outro lado, se $n = p_1^{n_1} \cdots p_k^{n_k}$ em que $s \in \mathbb{N}$, $p_1, \ldots, p_s$ são números primos distintos e $n_1, \ldots, n_s \in \mathbb{N}$ então esta congruência é equivalente ao sistema

$$\begin{cases} ax^2 + bx + c & \equiv & 0 \ (\mod p_1^{n_1}) \\ \vdots & \vdots & \vdots \\ ax^2 + bx + c & \equiv & 0 \ (\mod p_s^{n_s}) \end{cases}$$

Utilizando o teorema chinês dos restos concluímos que o número de soluções da congruência original é igual ao produto do números de soluções de cada uma das congruências do sistemas.

Ficamos assim reduzidos ao estudo das congruências do tipo

$$ax^2 + bx + c \equiv 0 \ (\mod p^k) \tag{4.3}$$

em que p é um número primo, $k \in \mathbb{N}$ e $a, b, c \in \mathbb{Z}$ e p não divide a.

Vamos analisar em separado os caso em que $p = 2$ e o caso em que p é ímpar. Mas antes disso vamos enunciar um resultado que nos "é familiar".

Proposição 4.1 *Sejam $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}$ tais que n* **é ímpar e primo com** *a. Se denotarmos por $(2a)^{-1}$ o inverso de $2a$ módulo n então as soluções da congruência $ax^2 + bx + c \equiv 0 \pmod{n}$, são os inteiros da forma*

$$\Big\{(-b + \alpha) * (2a)^{-1} : \ \alpha^2 = b^2 - 4ac\Big\}.$$

Demonstração: Basta notar que

$$\begin{aligned} ax^2 + bx + c \equiv 0 \ (\mod n) &\Leftrightarrow 4a^2x^2 + 4abx + 4ac \equiv 0 \ (\mod n) \quad \text{pois } (4a, n) = 1 \\ &\Leftrightarrow (2ax + b)^2 + (4ac - b^2) \equiv 0 \ (\mod n) \\ &\Leftrightarrow (2ax + b)^2 \equiv b^2 - 4ac \ (\mod n). \end{aligned}$$

Deste modo, para cada α tal que $\alpha^2 = b^2 - 4ac \pmod{n}$ resolvemos a congruência $2ax + b \equiv \alpha \pmod{n}$, que sabemos ter uma só solução, módulo n: $(-b + \alpha) * (2a)^{-1}$. ■

Vejamos um exemplo. Considere-se as congruências do tipo $x^2+x+c \equiv 0 \pmod{15}$, com $c \in \mathbb{Z}$. Recorde-se que estas congruências têm 0, 1, 2 ou 4 soluções (ver página (65)). Para calcular as soluções temos de encontrar α tal que $\alpha^2 \equiv 1 - 4c \pmod{15}$.

- Se $c = 3$ obtemos $\alpha^2 \equiv 4 \pmod{15}$ ou seja $\alpha \in \{2, 7, 8, 13\}$. Assim 8, 3, 11 e 6 são as soluções da congruência original (note que o inverso de 2 módulo 15 é 8).
- Se $c = -3$ a congruência não tem solução pois não existe $\alpha \in \mathbb{Z}$ tal que $\alpha^2 \equiv 13 \pmod{15}$.
- Se $c = 4$ a congruência tem uma só solução (7) pois 0 é a única solução de $\alpha^2 \equiv 0 \pmod{15}$,
- Se $c = -6$ a congruência tem duas soluções (2 e 12) pois 5 e 10 são as únicas soluções de $\alpha^2 \equiv 25 \pmod{15}$,

4.1.1 Caso em que $p = 2$

Suponhamos que $p = 2$ e a é ímpar (recorde-se que estamos a supor que $(a, n) = 1$). Separemos em casos:

- Se b é par, temos

$$\begin{aligned} ax^2 + bx + c \equiv 0 \pmod{2^k} &\Leftrightarrow a^2x^2 + abx + ac \equiv 0 \pmod{2^k} \quad \text{porque } (a, 2) = 1 \\ &\Leftrightarrow (ax + \frac{b}{2})^2 \equiv \frac{b^2}{4} - ac \pmod{2^k}. \end{aligned}$$

  Ficamos assim numa situação análoga à que foi vista na Proposição 4.1. Se denotarmos por a^{-1}, o inverso de a módulo 2^k, as soluções da congruência são,

$$x \equiv (-\frac{b}{2} + \alpha) * a^{-1} \pmod{2^p} : \quad \alpha^2 = \frac{b^2}{4} - 4ac.$$

- Se b é ímpar então $ax^2 + bx$ é sempre par e portanto c tem de ser par para a congruência ter solução (note-se que $ax^2 + bx + c$ é par pois é múltiplo de 2^k). Nesse caso, vamos procurar soluções pares, fazendo $x = 2y$ e soluções ímpares, fazendo $x = 2y + 1$.

- Se $x = 2y$ obtemos a congruência $4ay^2 + 2by + c \equiv 0 \pmod{2^k}$ ou seja $2ay^2 + 2by + \frac{c}{2} \equiv 0 \pmod{2^{k-1}}$ (recorde-se que c é par).
- Se $x = 2y + 1$ obtemos $4ay^2 + (4a + 2b)y + (a^2 + b + c) \equiv 0 \pmod{2^k}$ ou seja $2ay^2 + (2a + b)y + \frac{a^2+b+c}{2} \equiv 0 \pmod{2^{k-1}}$ (recorde-se que $a^2 + b + c$ é par pois a e b são ímpares e c é par).

Repetindo o processo obtemos, mais cedo ou mais tarde, obtemos uma congruência que sabemos resolver (porquê?).

4.2 Congruências do tipo $x^2 = a \pmod{p^k}$

O modo de resolver as congruências do tipo $x^2 = a \pmod{p^k}$ em que p é um número primo e $a, k \in \mathbb{Z}$ varia consoante $p = 2$ ou $p \neq 2$.

Em qualquer dos casos, se $p \mid a$ então $p \mid x^2$ e, portanto $p \mid x$. Deste modo, se a congruência tiver solução então admite solução na forma $x = py$ em que $y \in \mathbb{Z}$. Substituindo na congruência e simplificando obtemos $py^2 = a^* \pmod{p^{k-1}}$, em que $a = pa^*$. Assim, se $k > 1$ então $p \mid A$ pois $p \mid (py^2 - a^*)$ e portanto podemos simplificar, obtendo a congruência $y^2 = a^{**} \pmod{p^{k-2}}$ em que $a^* = pa^{**}$.

Repetindo o processo, concluímos que a congruência não tem solução ou chegamos a uma congruência do tipo $x^2 \equiv A \pmod{p^s}$ em que p não divide A.

> A partir daqui vamos considerar congruências do tipo $x^2 \equiv a \pmod{p^k}$ em que p é um número primo que não divide a.
>
> Note-se que as (hipotéticas) soluções desta congruência são primas com p.

A demonstração do seguinte resultado segue os passos da demonstração do Lema 3.17.

Proposição 4.2 *Sejam $a \in \mathbb{Z}$ e p um primo que não divide a.*

$$\textit{A congruência } x^2 \equiv a \pmod{p} \textit{ tem } \begin{cases} 0 \textit{ ou } 2 \textit{ soluções, módulo } p & \textit{se } p \neq 2. \\ 1 \textit{ solução, módulo } p & \textit{se } p = 2 \end{cases}$$

Demonstração: Se $p = 2$ então $a \equiv 1 \pmod 2$ e, portanto a solução da congruência é $x \equiv 1 \pmod 2$.

Suponhamos agora que $p \neq 2$ e que α é uma solução da congruência. Deste modo, se x é uma solução da congruência então

$$(x-\alpha)(x+\alpha) \;=\; x^2 - \alpha^2 \;\equiv\; a - a \;\equiv\; 0 \;(\bmod p)$$

e, portanto, p divide $(x-\alpha)(x+\alpha)$. Como p é primo temos p divide $x-\alpha$ ou $x+\alpha$, ou seja $x \equiv \pm\alpha \pmod p$. Note-se que, $\alpha \not\equiv -\alpha \pmod p$ pois $p > 2$. ■

Teorema 4.3 *Se $a \in \mathbb{Z}$, $k \in \mathbb{N}$ e p é um primo* **ímpar** *que não divide a então a congruência*

$$x^2 \equiv a \;(\bmod p^k)$$

admite 2 ou 0 soluções módulo p^k consoante a congruência $x^2 \equiv a \pmod p$ tem ou não solução.

Demonstração: Vamos fazer a demonstração por indução sobre k. O passo de indução pode ser feito do seguinte modo.

Note-se que basta-nos mostrar que, se α é uma solução de

$$x^2 \;\equiv\; a \;(\bmod p^k) \tag{4.4}$$

então existe uma e uma só solução de

$$x^2 \;\equiv\; a \;(\bmod p^{k+1}) \tag{4.5}$$

que é congruente com α módulo p^k.

Por hipótese, $\alpha + tp^k$ é solução de (4.4), para todo $t \in \mathbb{Z}$. Para terminar basta mostrar que existe um e um só t (módulo p) tal que $\alpha + tp^k$ é solução de (4.5). Deste modo, se $s \in \mathbb{Z}$ é tal que $\alpha^2 = a + sp^k$, temos sucessivamente

$$\begin{aligned}
(\alpha + tp^k)^2 &\equiv a \;(\bmod p^{k+1}) \\
\alpha^2 + 2\alpha t p^k + t^2 p^{2k} &\equiv a \;(\bmod p^{k+1}) \\
a + sp^k + 2\alpha t p^k &\equiv a \;(\bmod p^{k+1}) \\
s + 2\alpha t &\equiv 0 \;(\bmod p).
\end{aligned}$$

Esta última congruência admite uma só solução módulo p, pois $(2\alpha, p) = 1$. ■

A resolução de congruências da forma $x^2 \equiv a \pmod{p^k}$, com p primo ímpar, fica assim reduzida à resolução de congruências da forma $x^2 \equiv a \pmod{p}$, que neste momento serão resolvidas apenas por tentativas.

Note-se que, se α for uma solução da congruência $x^2 \equiv a \pmod{p^k}$ então a solução geral da congruência é dada por $x \equiv \pm\alpha \pmod{p^k}$.

Vejamos um exemplo.

Exemplo 4.4 *Consideremos a congruência* $x^2 \equiv 17141 \pmod{11^5}$.

Seguindo o processo descrito acima começamos por resolver a congruência $x^2 \equiv 17141 \pmod{11}$ *ou seja* $x^2 \equiv 3 \pmod{11}$. *Por tentativas concluímos que* $x = 5$ *é uma solução desta última congruência.*

De seguida procuramos $t \in \mathbb{Z}$ *de tal modo que* $5 + 11t$ *é solução da congruência* $x^2 \equiv 17141 \pmod{11^2}$ *ou seja* $x^2 \equiv 80 \pmod{11^2}$. *Substituindo, obtemos* $10\,t \equiv 5 \pmod{11}$ *(ou* $-t \equiv 5 \pmod{11}$*) que admite* $t = -5$ *como solução. Assim,* $x = 5 + 11(-5) = -50$ *é uma solução da congruência* $x^2 \equiv 17141 \pmod{11^2}$. *E o processo continua.*

Em geral é mais fácil não voltar logo à congruência $x^2 \equiv 17141 \pmod{11}$ *mas começar por analisar as congruências*

$$x^2 \equiv 17141 \ (\bmod 11^t) \qquad \textit{com } 1 \leq t \leq 5$$

e verificamos se alguma delas admite uma resolução (quanto maior for o valor de t*, menos contas vamos ter que fazer).*

Neste caso obtemos

$$\begin{cases} x^2 \equiv 17141 \ (\bmod 11^5) \\ x^2 \equiv 17141 \ (\bmod 11^4) \\ x^2 \equiv 17141 \ (\bmod 11^3) \\ x^2 \equiv 17141 \ (\bmod 11^2) \\ x^2 \equiv 17141 \ (\bmod 11) \end{cases} \quad \textit{ou seja} \quad \begin{cases} x^2 \equiv 17141 \ (\bmod 11^5) \\ x^2 \equiv 2500 \ (\bmod 11^4) \\ x^2 \equiv 1169 \ (\bmod 11^3) \\ x^2 \equiv 80 \ (\bmod 11^2) \\ x^2 \equiv 3 \ (\bmod 11) \end{cases}$$

Note-se que a congruência $x^2 \equiv 2500 \pmod{11^4}$ *é fácil de resolver. Uma solução é* $x = 50$.

A partir daqui aplicamos o método descrito atrás para resolver a congruência $x^2 \equiv 17141 \pmod{11^5}$. *Basta então procurar* $t \in \mathbb{Z}$ *tal que* $(50 + 11^4 t)^2 \equiv 17141 \pmod{11^5}$ *ou seja* $2 \times 50 \times 11^4 t \equiv 17141 - 2500 \pmod{11^5}$.

Simplificando (recorda-se que é sempre possível obter uma congruência módulo p) temos $100\,t \equiv 1 \pmod{11}$. *Uma solução desta congruência é* $t = 1$. *Concluímos assim que* $50 + 11^4$ *é uma solução da congruência original.*

O caso em que $p = 2$ tem um método de resolução, e uma resposta, diferente:

- se $k = 1$ então só temos uma congruência, a saber, $x^2 \equiv 1 \pmod{2}$ que admite 1 como única solução (módulo 2);
- se $k = 2$ temos as congruências $x^2 \equiv 1 \pmod{4}$ que tem duas soluções módulo 4 ($x = 1$ e $x = 3$) e $x^2 \equiv 3 \pmod{4}$ que não tem solução;
- se $k = 3$ então, como $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod{8}$ a congruência $x^2 \equiv a \pmod{2^k}$ tem 4 soluções (módulo 8) se $a \equiv 1 \pmod{8}$) e zero soluções, caso contrário.
- se $k \geq 3$ e atendendo ao caso anterior, se a congruência tem solução então necessariamente $a \equiv 1 \pmod{8}$.

Lema 4.5 *Se* $k \geq 3$ *e* α *é solução da congruência* $x^2 \equiv a \pmod{2^k}$ *então*

$$\alpha,\ -\alpha,\ \alpha + 2^{k-1} \text{ e } -\alpha + 2^{k-1}$$

são soluções da congruência, incongruentes módulo 2^k.

Demonstração: "Basta substituir". Se $s = 0$ ou $s = 1$ então

$$\begin{aligned} \left(\pm\alpha + s2^{k-1}\right)^2 = \alpha^2 \pm s\alpha 2^k + s^2 2^{2(k-1)} &\equiv \alpha^2 \ (\bmod 2^k) \qquad \text{porque } 2(k-1) \geq k \\ &\equiv a \ (\bmod 2^k) \end{aligned}$$

■

Teorema 4.6 *Se* $k \geq 3$ *e* $a \in \mathbb{Z}$ *então a congruência*

$$x^2 \equiv a \ (\bmod 2^k)$$

admite 4 *soluções módulo* 2^k *se* $a \equiv 1 \pmod{8}$ *e* 0 *soluções caso contrário.*

Além disso, se α *é uma solução então toda a solução da congruência é congruente, módulo* 2^k, *com* α, $-\alpha$, $\alpha + 2^{k-1}$ *ou* $-\alpha + 2^{k-1}$.

Demonstração: A segunda parte do teorema é uma consequência da primeira parte e do lema anterior.

Vamos demonstrar a primeira parte do teorema por indução sobre k.

Se $k = 3$ já foi verificada a veracidade da afirmação.

Suponhamos que o resultado vale para k e sejam α, $-\alpha$, $\alpha+2^{k-1}$ e $-\alpha+2^{k-1}$ quatro soluções da congruência $x^2 \equiv a \pmod{2^k}$ que são incongruentes módulo 2^k.

Deste modo as soluções da congruência

$$x^2 \equiv a \ (\bmod 2^{k+1}) \tag{4.6}$$

são da forma: $\alpha + t2^k$, $-\alpha + t\,2^k$, $\alpha + 2^{k-1} + t\,2^k$ ou $-\alpha + 2^{k-1} + t\,2^k$, com $t \in \mathbb{Z}$, que escreveremos abreviadamente $\pm\alpha + \mu\,2^{k-1} + t\,2^k$, em que $\mu \in \{0, 1\}$.

Substituindo na congruência $x^2 \equiv a \pmod{2^{k+1}}$ obtemos sucessivamente

$$\begin{aligned}
\left(\pm\alpha + \mu\,2^{k-1} + t2^k\right)^2 &\equiv a \ (\bmod 2^{k+1}) \\
\alpha^2 + \mu^2 2^{2k-2} \pm \alpha\,\mu\,2^k + t^2 2^{2k} + (\pm\alpha + \mu\,2^{k-1})\,t\,2^{k+1} &\equiv a \ (\bmod 2^{k+1}) \\
\alpha^2 \pm \alpha\mu\,2^k &\equiv a \ (\bmod 2^{k+1}) \\
&\text{porque } 2k,\ 2k-2 \geq k+1.
\end{aligned}$$

Como $\alpha^2 \equiv a \pmod{2^k}$ existe $s \in \mathbb{Z}$ tal que $\alpha^2 = a + 2^k s$. Temos assim

$$2^k s \pm \alpha\mu\,2^k \equiv 0 \ (\bmod 2^{k+1}) \quad \text{ou seja} \quad s \pm \alpha\mu \equiv 0 \ (\bmod 2)$$

Como a é ímpar então α também é ímpar. Analisando os diversos casos para s e μ temos, para $t \in \mathbb{Z}$,

- se s é ímpar então $\pm\alpha + t2^k$ são soluções de (4.6) e $\pm\alpha + 2^{k-1} + t2^k$ não são soluções de (4.6);
- se s é par então $\pm\alpha + t2^k$ não são soluções de (4.6) e $\pm\alpha + 2^{k-1} + t2^k$ são soluções de (4.6);

Deste modo as soluções, módulo 2^{k+1}, de (4.6) são:

- se s é ímpar, α, $\alpha + 2^k$, $-\alpha$ e $-\alpha + 2^k$;

- se s é par, $\alpha + 2^{k-1}$, $-\alpha + 2^{k-1}$, $\alpha + 2^{k-1} + 2^k$ e $-\alpha + 2^{k-1} + 2^k$.

Para concluir basta notar que, em qualquer dos casos, as 4 soluções apresentadas são incongruentes módulo 2^{k+1}. ■

Nota 4.7 *O método descrito na demonstração do teorema permite-nos concluir que, se α é uma solução de $x^2 \equiv a \pmod{2^k}$ então α ou $\alpha + 2^{k-1}$ é uma solução da congruência $x^2 \equiv a \pmod{2^{k+1}}$. Além disso, o* **ou** *referido é* **disjunto**.

Na prática para resolver uma congruência do tipo $x^2 \equiv a \pmod{2^k}$ com a ímpar fazemos o seguinte:

- verificamos se $a \equiv 1 \pmod 8$. Se a resposta for negativa então a congruência não tem solução. A partir daqui vamos supor que $a \equiv 1 \pmod 8$. Em particular a é um quadrado módulo 8, pois $1^2 \equiv a \pmod 8$;
- verificamos se "é óbvio" que a é um quadrado módulo 2^i, para algum $i \in \{3, \ldots, k\}$. Quanto maior foi o i menos contas teremos no futuro. Em último caso consideramos $i = 3$;
- aplicamos a Nota 4.7 para verificar que a é um quadrado módulo 2^{i+1}. A aplicação sucessiva desta nota permite-nos resolver a congruência inicial.

Vejamos um exemplo.

Exemplo 4.8 *Consideremos a congruência $x^2 \equiv 217 \pmod{256}$. Note-se que, como $256 = 2^8$ e $217 \equiv 1 \pmod 8$, a congruência inicial tem 4 soluções incongruentes módulo 256. Basta-nos encontrar uma!!*

Note-se que:

- *1 é solução de $x^2 \equiv 217 \pmod 8$, ou equivalentemente $x^2 \equiv 1 \pmod 8$.*
- *usando a nota acima, 5 é solução de $x^2 \equiv 217 \pmod{16}$ (porque 1 não é solução dessa congruência);*
- *como $5^2 \equiv 217 \pmod{32}$, $5^2 \equiv 217 \pmod{64}$ e $5^2 \not\equiv 217 \pmod{128}$ podemos concluir, usando a nota, que $5 + 32 = 37$ é solução de $x^2 \equiv 217 \pmod{128}$;*

- *como* $37^2 \not\equiv 217 \pmod{256}$ *podemos concluir que* $37 + 64 = 101$ *é solução de* $x^2 \equiv 217 \pmod{256}$.

Deste modo, usando o teorema anterior, toda a solução desta última congruência é congruente com 101, -101, $101 + 128$ *ou com* 27.

É claro que seria menos trabalhoso se tivéssemos verificado que era fácil resolver a congruência módulo 64, *porque* $217 \equiv 25 \pmod{64}$. *Vemos então que* $x = 5$ *é uma solução de* $x^2 \equiv 217 \pmod{64}$. *De seguida aplicamos o método já referido para encontrar uma solução da congruência* $x^2 \equiv 217 \pmod{128}$ *e depois de* $x^2 \equiv 217 \pmod{256}$.

Como consequência do Teorema 4.3, do Teorema 4.6 e do teorema chinês dos restos temos o seguinte resultado.

Corolário 4.9 *Se* $n \in \mathbb{N}$ *e* a *é um inteiro primo com* n *e* r *é o número de primos ímpares que dividem* n *então a congruência*

$$x^2 \equiv a \pmod{n}$$

tem:

- 0 *soluções se* 8 *divide* n *e* $a \not\equiv 1 \pmod{8}$*;*
- 0 *soluções se existir algum primo ímpar* p *que divida* n *e tal que a congruência* $x^2 \equiv a \pmod{p}$ *não tenha solução;*
- 2^{r+s} *soluções se não acontecer nenhuma das hipóteses referidas nos anteriores itens, sendo*
  - $s = 0$ *se* $4 \nmid n$*;*
  - $s = 1$ *se* $4 \mid n$ *e* $8 \nmid n$*;*
  - $s = 2$ *se* $8 \mid n$. ■

4.3 Símbolo de Legendre

Nesta secção introduziremos o chamado símbolo de Legendre que em última análise nos vai permitir saber se uma dada congruência do tipo $x^2 \equiv a \pmod{n}$ tem ou não solução. Pelo que foi dito até aqui esta questão fica resolvida se soubermos verificar quando uma congruência do tipo $x^2 \equiv a \pmod{p}$, com p primo ímpar, tem solução, sem "muitos cálculos".

Nota 4.10 *Ficaremos a saber, utilizando símbolos de Legendre, se uma congruência do tipo* $x^2 \equiv a \pmod{p}$*, com* p *primo ímpar tem solução* $\boxed{\textit{sem de facto a sabermos resolver}}$.

Definição 4.11 *Se* p *é um primo ímpar e* $a \in \mathbb{Z}$ *define-se,* símbolo de Legendre *de* a*, módulo* p*, e denota-se por* $\left(\frac{a}{p}\right)$ *como sendo*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{se } p \textit{ não divide } a \textit{ e existe } x \in \mathbb{Z} \textit{ tal que } x^2 \equiv a \pmod{p} \\ -1 & \textit{se } p \textit{ não divide } a \textit{ e não existe } x \in \mathbb{Z} \textit{ tal que } x^2 \equiv a \pmod{p} \\ 0 & \textit{se } p \textit{ divide } a. \end{cases}$$

Note-se que na definição acima consideramos p ímpar uma vez que qualquer número inteiro é um quadrado módulo 2.

Vejamos o chamado critério de Euler para o cálculo do símbolo de Legendre. Note-se que, se p é um primo ímpar e $a \in \mathbb{Z}$ então $a^{\frac{p-1}{2}}$ é congruente com 0, 1 ou -1 módulo p, uma vez que, se p não divide a então $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$.

Proposição 4.12 (Critério de Euler) *Se* p *é um número primo ímpar e* $a \in \mathbb{Z}$ *então* $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$.

Demonstração: Se p divide a então o resultado é trivial. Se p não divide a vamos considerar dois casos.

- Existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod{p}$.
  Nesse caso $\left(\frac{a}{p}\right) = 1$ e $a^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod{p}$ pelo teorema de Euler.
- Não existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod{p}$.

Como dado $c \in \{1, 2, \ldots, p-1\}$ a congruência $cx \equiv a \pmod{p}$ tem solução única (módulo p) que é necessariamente diferente de c por hipótese, temos

$$\forall c \in \{1, \ldots, p-1\}\ \exists^{!} d \in \{1, \ldots, p-1\} \setminus \{c\} \quad cd \equiv a\ (\bmod p)$$

Utilizando esta observação podemos concluir que os números $1, 2, \ldots, p-1$ podem ser agrupados dois a dois de modo a que o produto dos elementos de cada um desse grupos seja congruente com a módulo p. Como existem $\frac{p-1}{2}$ desses grupos, temos $(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$. A conclusão segue do Teorema de Wilson. ■

Podemos já concluir que, por exemplo a congruência $x^2 \equiv -1 \pmod{1229}$ tem solução uma vez que $\left(\frac{-1}{1229}\right) = (-1)^{614} = 1$.

Como consequência imediata deste critério temos os seguintes resultados.

Proposição 4.13 *Se p é um primo ímpar e $a, b \in \mathbb{Z}$ então:*

a) *se $a \equiv b \pmod{p}$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;*

b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

c) $\left(\frac{a^2}{p}\right) = 1$;

d) $\left(\frac{-1}{p}\right) = 1$ *se e só se* $p \equiv 1 \pmod{4}$. ■

Nota 4.14 *Como consequência da proposição anterior, se $a = q_1^{n_1} \cdots q_k^{n_k}$ em que $k, n_1, \ldots, n_k \in \mathbb{N}$, $q_1, \ldots, q_k$ são primos distintos então*

$$\left(\frac{a}{p}\right) = \left(\frac{q_1^{n_1}}{p}\right) \cdots \left(\frac{q_k^{n_k}}{p}\right) = \prod_{n_j \text{ ímpar}} \left(\frac{q_j}{p}\right).$$

Por exemplo $\left(\frac{-2^3 \times 3 \times 5^2}{1229}\right) = \left(\frac{-1}{1229}\right)\left(\frac{2^3 \times 3 \times 5^2}{1229}\right) = \left(\frac{-1}{1229}\right)\left(\frac{2}{1229}\right)\left(\frac{3}{1229}\right)$.

Para o cálculo do símbolo de Legendre (em geral) precisaremos da chamada *lei da reciprocidade quadrática* que veremos mais à frente e do cálculo de $\left(\frac{2}{p}\right)$ para qualquer primo ímpar p.

Note-se que, se p é um número ímpar então um dos números $p-1$ ou $p+1$ é um múltiplo de 4 e, portanto, $(p-1)(p+1)$ é um múltiplo de 8.

Teorema 4.15 *Se p é um número primo ímpar então*

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

ou seja, $\left(\frac{2}{p}\right) = 1$ (isto é, 2 é um quadrado módulo p) se e só se $p \equiv \pm 1 \pmod 8$.

Demonstração: Vamos mostrar, usando o critério de Euler, que $2^{\frac{p-1}{2}} \equiv 1 \pmod p$ se e só se $p \equiv \pm 1 \pmod 8$.

Note-se que

$$\begin{aligned} 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= 2^{\frac{p-1}{2}}\left(1 \times 2 \times \cdots \times \frac{p-1}{2}\right) \\ &= 2 \times 4 \times \cdots \times (p-1) \end{aligned}$$

A partir daqui vamos considerar dois casos.

- Se $\frac{p-1}{2}$ é par então

$$\begin{aligned} 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= 2 \times 4 \times \cdots \times (p-1) \\ &= \underbrace{\left(2 \times \cdots \times \frac{p-1}{2}\right)}_{\frac{p-1}{4}\text{ factores}} \times \underbrace{\left(\frac{p+3}{2} \times \cdots \times (p-3) \times (p-1)\right)}_{\frac{p-1}{4}\text{ factores}} \\ &\equiv \left(2 \times \cdots \times \frac{p-1}{2}\right)\left(-\frac{p-3}{2}\right) \times \cdots \times (-3) \times (-1) (\bmod p) \\ &= (-1)^{\frac{p-1}{4}}\left(\frac{p-1}{2}\right)!. \end{aligned}$$

- Se $\frac{p-1}{2}$ é ímpar então

$$\begin{aligned} 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= 2\times 4\times\cdots\times(p-1) \\ &= \underbrace{\left(2\times\cdots\times\frac{p-3}{2}\right)}_{\frac{p-3}{4}\text{ factores}}\times\underbrace{\left(\frac{p+1}{2}\times\cdots\times(p-3)\times(p-1)\right)}_{\frac{p+1}{4}\text{ factores}} \\ &\equiv \left(2\times\cdots\times\frac{p-3}{2}\right)\left(-\frac{p-1}{2}\right)\times\cdots\times(-3)\times(-1)(\bmod p) \\ &= (-1)^{\frac{p+1}{4}}\left(\frac{p-1}{2}\right)!. \end{aligned}$$

Deste modo

$$\begin{aligned} 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &\equiv (-1)^{\frac{p-1}{4}}\left(\frac{p+1}{2}\right)!\ (\bmod p) \quad \text{se } \tfrac{p-1}{2} \text{ é par} \\ 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &\equiv (-1)^{\frac{p+1}{4}}\left(\frac{p-1}{2}\right)!\ (\bmod p) \quad \text{se } \tfrac{p-1}{2} \text{ é ímpar} \end{aligned}$$

ou seja, usando a lei do corte,

$$2^{\frac{p-1}{2}} \equiv \begin{cases} (-1)^{\frac{p-1}{4}}\ (\bmod p) & \text{se } \tfrac{p-1}{2} \text{ é par} \\ \\ (-1)^{\frac{p+1}{4}}\ (\bmod p) & \text{se } \tfrac{p-1}{2} \text{ é ímpar.} \end{cases}$$

Para concluir basta analisar os diversos casos possíveis para p, módulo 8. Deste modo,

$$\begin{cases} p\equiv 1\ (\bmod 8) \Rightarrow 2^{\frac{p-1}{2}}=1, & \text{porque } \frac{p-1}{2} \text{ e } \frac{p-1}{4} \text{ são pares} \\ p\equiv 3\ (\bmod 8) \Rightarrow 2^{\frac{p-1}{2}}=-1, & \text{porque } \frac{p-1}{2} \text{ e } \frac{p+1}{4} \text{ são ímpares} \\ p\equiv 5\ (\bmod 8) \Rightarrow 2^{\frac{p-1}{2}}=-1, & \text{porque } \frac{p-1}{2} \text{ é par e } \frac{p-1}{4} \text{ é impar} \\ p\equiv 7\ (\bmod 8) \Rightarrow 2^{\frac{p-1}{2}}=1, & \text{porque } \frac{p-1}{2} \text{ é ímpar e } \frac{p+1}{4} \text{ é par.} \end{cases}$$

■

Usando este teorema e a Proposição 4.13 podemos mostrar que, se p é um número primo ímpar,

$$\left(\frac{-2}{p}\right)=1 \iff p\equiv 1\ (\bmod 8) \text{ ou } p\equiv 3\ (\bmod 8). \tag{4.7}$$

Estamos agora em condições de enunciar a lei da reciprocidade quadrática que compara $\left(\frac{q}{p}\right)$ com $\left(\frac{p}{q}\right)$ se p e q forem dois números primos distintos. Não será feita aqui a demonstração deste teorema.

Teorema 4.16 (lei da reciprocidade quadrática) *Se p e q são dois números primos ímpares distintos então*

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

ou seja, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ se e só se p ou q é congruente com 1 módulo 4. ■

Usando este teorema e a fórmula que temos para calcular $\left(\frac{2}{p}\right)$ podemos facilmente calcular o símbolo de Legendre de qualquer inteiro módulo um primo p.

Por exemplo,

$$\begin{aligned}
\left(\frac{-42}{67}\right) &= \left(\frac{-1}{67}\right)\left(\frac{2}{67}\right)\left(\frac{3}{67}\right)\left(\frac{7}{67}\right) \\
&= -\left(\frac{2}{67}\right)\left(\frac{3}{67}\right)\left(\frac{7}{67}\right) && \text{pois } 67 \not\equiv 1 \pmod 4 \\
&= \left(\frac{3}{67}\right)\left(\frac{7}{67}\right) && \text{pois } 67 \equiv 3 \pmod 8 \\
&= \left(\frac{67}{3}\right)\left(\frac{67}{7}\right) && \text{usando a lei da reciprocidade quadrática} \\
& && \text{e notando que 67, 7 e 3} \\
& && \text{não são congruentes com 1 módulo 4} \\
&= \left(\frac{1}{3}\right)\left(\frac{4}{7}\right) && \text{pois } 67 \equiv 1 \pmod 3 \text{ e } 67 \equiv 4 \pmod 7 \\
&= 1.
\end{aligned}$$

Para o cálculo de $\left(\frac{n}{p}\right)$, com p número primo ímpar que não divide n é suficiente o uso das seguintes regras, que no fundo sintetizam o que foi dito nesta secção:

- se n é um quadrado então $\left(\frac{n}{p}\right) = 1$;
- se $n = -1$, usamos a alínea d) da Proposição 4.13;

- se $n = 2$, usamos o Teorema 4.15;
- substituímos n pelo resto r da divisão de n por p obtendo $\left(\frac{n}{p}\right) = \left(\frac{r}{p}\right)$ com $1 \leq r < p$;
- reduzimos ao caso em que n é primo usando a Nota 4.14;
- se n é primo e menor do que p, usamos a lei da reciprocidade.

Corolário 4.17 *Se p é um primo maior do que 3 então*

$$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \ (\text{mod } 12).$$

Demonstração: Se r é o resto da divisão de p por 3 então

$$\begin{aligned}\left(\frac{3}{p}\right) &= (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) \quad \text{usando a lei da reciprocidade quadrática} \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{r}{3}\right).\end{aligned}$$

Para concluir basta notar que $(-1)^{\frac{p-1}{2}}\left(\frac{r}{3}\right) = 1$ se e só se $p \equiv 1 \pmod 4$ e $r = 1$ ou $p \equiv -1 \pmod 4$ e $r = -1$, ou seja, se e só se $p \equiv \pm 1 \pmod{12}$. ■

4.4 Exercícios

Três tipos de exercícios se podem resolver escolhendo $a \in \mathbb{Z}$, p número primo ímpar e $m \in \mathbb{N}$:

- calcule $\left(\frac{a}{p}\right)$. Neste caso é dado um primo ímpar e $a \in \mathbb{Z}$;
- quantas soluções tem a congruência $x^2 \equiv a \pmod n$? Neste caso é dado $n \in \mathbb{N}$ e $a \in \mathbb{Z}$.
- calcule $\left(\frac{a}{q}\right)$, para q primo ímpar. Aqui o a é dado (o caso a igual a -1, 2 e 3 já foi visto). e espera-se que a resposta dependa do valor de q módulo algum valor (o caso a igual a -1, 2 e 3 já foi visto).

4.1. Calcule $\left(\frac{3}{p}\right)$ se p é um primo de Mersenne ou de Fermat (isto é, se é da forma $2^n - 1$ ou da forma $2^{2^n} + 1$).

4.2. Sejam $a \in \mathbb{N}$ e p um número primo ímpar tais a congruência $x^2 \equiv a \pmod{p}$ tem solução. Mostre que, se p é congruente, módulo 8, com :

a) 3 ou com 7, então $a^{\frac{p+1}{4}}$ é solução da congruência;

b) 5, então $a^{\frac{p+3}{8}}$ ou $a^{\frac{p+3}{8}} \cdot \left(\frac{p-1}{2}\right)!$ é solução da congruência.

4.3. Considere a congruência $ax^2 + bx + c \equiv 0 \pmod{p}$ em que $a, b, c \in \mathbb{Z}$ p é um primo ímpar que não divide a. Mostre que, se $\Delta = b^2 - 4ac$, então a congruência tem 0, 1 ou 2 soluções módulo p consoante $\left(\frac{\Delta}{p}\right) = -1, \left(\frac{\Delta}{p}\right) = 0$ ou $\left(\frac{\Delta}{p}\right) = 1$.

4.4. Mostre que, se p é um primo ímpar, então

$$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = 0.$$

4.5. Mostre que, se p é um primo ímpar e q é o menor inteiro positivo tal que $\left(\frac{q}{p}\right) = -1$ então q é primo.

4.6. Seja p um primo ímpar. Mostre que:

a) se $a \in \mathbb{Z}$ e $p \nmid a$ então $\left(\frac{a(a+1)}{p}\right) = \left(\frac{a^*+1}{p}\right)$ se a^* é o inverso, módulo p de a:

b) $\left(\frac{1\cdot 2}{p}\right) + \left(\frac{2\cdot 3}{p}\right) + \cdots + \left(\frac{(p-2)(p-1)}{p}\right) = -1$;

c) existem $b, c \in \mathbb{Z}$ tais que

$$\left(\frac{b}{p}\right) = \left(\frac{b+1}{p}\right) = 1, \quad \left(\frac{c}{p}\right) = \left(\frac{c+1}{p}\right) = -1.$$

4.7. Use o critério de Euler para verificar se 83 divide $2^{41} + 1$ e se 1999 divide $2^{999} - 1$.

4.8. Seja n um inteiro positivo congruente com 3 módulo 4. Mostre (usando o critério de Euler para calcular $\left(\frac{2}{p}\right)$) que, se $2n + 1$ é primo então divide $2^n - 1$. Conclua que, se $n \equiv 3 \pmod{4}$ e $2n + 1$ é primo então $2^n - 1$ é primo se e só se $n = 3$.

4.9. Mostre que, se q é um inteiro ímpar e $p = 4q + 1$ é primo, então $\left(\frac{2}{p}\right) = -1$ e p divide $4^q + 1$.

4.10. Seja $p \in \mathbb{P}$. Mostre que existe uma infinidade de inteiros $n \in \mathbb{N}$ tais que $(n^2-3)(n^2-5)(n^2-15)$ é múltiplo de p. **Sugestão:** Para $p > 2$, separe em casos consoante o valor de $\left(\frac{3}{p}\right)$ e de $\left(\frac{5}{p}\right)$.

4.11. Mostre que, se $n \in \mathbb{N}$ então $N = 1! + 2! + \cdots + n!$ nunca é um quadrado perfeito. **Sugestão:** Comece por calcular $\left(\frac{N}{5}\right)$.

4.12. Dado $n \in \mathbb{N}$ seja $N = 5(n!)^2 - 1$. Mostre que:

a) se p divide N então $p > n$ e $\left(\frac{5}{p}\right) = 1$. Conclua que $p \equiv \pm 1 \pmod 5$.

b) existe um primo p que divide N tal que $p \equiv -1 \pmod 5$.

c) existe um primo p que divide N tal que $p \equiv -1 \pmod{10}$.

Conclua que existe uma infinidade de primos congruentes com -1 módulo 10, ou seja, cujo último dígito é 9.

4.13. Seguindo o raciocínio do exercício anterior mostre que existe uma infinidade de primos congruentes com: 3 módulo 8; 5 módulo 8; 7 módulo 8; 1 módulo 6.

Sugestão: Considere, se $p_1 \cdots p_n$ são da forma pedida, N igual a: $(p_1 \cdots p_n)^2 + 2$; $(p_1 \cdots p_n)^2 + 4$;$(p_1 \cdots p_n)^2 - 2$;$(p_1 \cdots p_n)^2 + 3$.

4.14. Mostre que, se p e q são primos ímpares congruentes módulo 26 então $\left(\frac{13}{p}\right) = \left(\frac{13}{q}\right)$.

5. Raízes primitivas

5.1 Ordem de um inteiro módulo n

Vimos no Capítulo 3 que, se $n \in \mathbb{N}$, $< \mathbb{Z}_n^*, \cdot_n >$ é um grupo com $\varphi(n)$ elementos.

Neste capítulo procuramos saber em que condições este grupo é cíclico, ou seja, em que condições existe $a \in \mathbb{Z}_n^*$ tal que

$$\mathbb{Z}_n^* = \{a^k : k \in \mathbb{N}_0,\ 0 \leq k < \varphi(n)\}.$$

Chegamos assim às seguintes definições:

Definição 5.1 *Sejam $n \in \mathbb{N}$ e $a \in \mathbb{Z}$ tais que $(a, n) = 1$. Diz-se que:*

a) *a tem* **ordem** *k módulo n, se k é o menor inteiro positivo tal que $a^k \equiv 1$ (mod n);*

b) *a é uma* **raiz primitiva** *de n (ou módulo n) se a ordem de a módulo n, é igual a $\varphi(n)$.*

As definições acima têm sentido uma vez que, pelo Teorema de Euler,

$$a^{\varphi(n)} \equiv 1 \text{ (mod } n).$$

Escreveremos $ord_n a = k$ (ou simplesmente $ord\, a = k$, caso daí não advenham confusões) para significar que a ordem de a módulo n é k.

Note-se que, se $a \in \mathbb{Z}$ é tal que $(a, n) = 1$ e r é o resto da divisão de a por n, então $r \in \mathbb{Z}_n^*$ e $r \equiv a \pmod{n}$.

Usando estas observações e o que foi dito na Secção 1.2 temos os seguintes resultados.

Proposição 5.2 *Sejam $a, b \in \mathbb{Z}$, $n, s \in \mathbb{N}$ com $(a, n) = 1$. Então:*

a) *se $a \equiv b \pmod{n}$, então $ord_n a = ord_n b$. Em particular se a é uma raiz primitiva de n e $a \equiv b \pmod{n}$ então b também é uma raiz primitiva de n;*

b) *se r é o resto da divisão de a por n, então $ord_n a$ é a ordem de r no grupo $\mathbb{Z}_n^*$. Em particular $ord_n a$ divide $\varphi(n)$ e $ord_n a = \varphi(n)$ se e só se $\mathbb{Z}_n^*$ é um grupo cíclico gerado por r;*

c) *$ord_n a = \varphi(n)$ se e só se $\{1, a, a^2, \ldots, a^{\varphi(n)-1}\}$ é um* **srr** *de n;*

d) *$a^s \equiv 1 \pmod{n}$ se e só se $ord_n a$ divide s;*

e) *$ord_n a^s = \frac{ord_n a}{(ord_n a, s)}$;*

f) *$ord_n a^s = ord_n a$ se e só se $(ord_n a, s) = 1$. Em particular, se a é uma raiz primitiva de n, então a^s é uma raiz primitiva de n se e só se $(s, \varphi(n)) = 1$.* ■

Corolário 5.3 *Se $n \in \mathbb{N}$ admite raízes primitivas, então n admite $\varphi(\varphi(n))$ raízes primitivas incongruentes módulo n.*

Demonstração: Seja r um raiz primitiva de n. Então $\{r, r^2, \ldots, r^{\varphi(n)}\}$ é um **srr** de n. Deste modo o conjunto formado pelos inteiros s pertencentes a $\{1, 2, \ldots, \varphi(n)\}$ tais que r^s é uma raiz primitiva é, atendendo à última alínea da proposição anterior,

$$\Big\{ s \in \{1, 2, \ldots, \varphi(n)\} : (\varphi(n), s) = 1 \Big\}.$$

Em particular existem $\varphi(\varphi(n))$ raízes primitivas de n, incongruentes módulo n. ■

A procura de raízes primitivas não é simples, nem as raízes primitivas, quando existem, estão distribuídas de um modo "previsível". Na prática quase só por tentativas se conseguem encontrar as raízes primitivas. Por outro lado, pelo corolário anterior, se as raízes primitivas estiverem bem distribuídas, espera-se que uma tentativa tenha a probabilidade de $\frac{\varphi(\varphi(n))}{\varphi(n)-1}$ de ser bem sucedida.

Exemplos 5.4 *Para alguns valores de n vou construir tabelas de duas colunas. Na primeira coluna coloco os elementos de* $\mathbb{Z}_n^*$ *e na outra a respectiva ordem.*

a	$ord_2 a$
1	1

a	$ord_3 a$
1	1
2	2

a	$ord_4 a$
1	1
3	2

a	$ord_5\ a$
1	1
2	4
3	4
4	2

a	$ord_8 a$
1	1
3	2
5	2
7	2

a	$ord_{10} a$
1	1
3	4
7	4
9	2

a	$ord_{12} a$
1	1
5	2
7	2
11	2

a	$ord_7\ a$
1	1
2	3
3	6
4	3
5	6
6	2

a	$ord_9\ a$
1	1
2	6
4	3
5	6
7	3
8	2

a	$ord_{14}\ a$
1	1
3	6
5	6
9	3
11	3
13	2

a	$ord_{18}\ a$
1	1
5	6
7	3
11	6
13	3
17	2

Assim, destes inteiros positivos, apenas o 8 e o 12 não admitem raízes primitivas.

5.2 Inteiros admitindo raízes primitivas

Para encontrarmos as raízes primitivas de um inteiro n, basta procurar no conjunto $\mathbb{Z}_n^*$, ou em qualquer **srr**.

É claro que, se n admite uma raiz primitiva (por exemplo r), então n admite uma infinidade de raízes primitivas (por exemplo $r+kn$, com $k \in \mathbb{Z}$). Por abuso de notação, quando dissermos que n tem s raízes primitivas, estaremos a pensar em s raízes primitivas incongruentes módulo n (ou, se quisermos, n tem s raízes primitivas em qualquer **srr**).

Nas subsecções seguintes vamos estudar os diferentes valores de n e procurar caracterizar aqueles que admitem raízes primitivas.

5.2.1 Redução ao caso em $n = p^k$ ou $n = 2p^k$, com p primo ímpar

Comecemos por notar que todo o inteiro positivo é de uma das seguintes formas:

- igual a 1, 2 ou 4;
- uma potência de 2 de expoente maior do que 2;
- uma potência de um primo ímpar;
- o dobro de uma potência de um primo ímpar;
- da forma $r \cdot s$ em que $(r,s) = 1$ e $r, s > 2$.

Se $n = 1$, 2 ou 4, então n admite raízes primitivas, como vimos acima.

Proposição 5.5 *Se $n = r \cdot s$ em que $(r,s) = 1$ e $r, s > 2$ então n não admite raízes primitivas.*

Demonstração: Seja $a \in \mathbb{Z}$ um inteiro primo com n. Vejamos que a ordem de a módulo n é menor do que $\varphi(n)$.

Notando que $\varphi(n)$, $\varphi(r)$ e $\varphi(s)$ são números pares, temos

$$\begin{cases} a^{\frac{\varphi(n)}{2}} = a^{\frac{\varphi(r)\varphi(s)}{2}} = \left(a^{\varphi(r)}\right)^{\frac{\varphi(s)}{2}} \equiv 1 \ (\mod r) \\ a^{\frac{\varphi(n)}{2}} = a^{\frac{\varphi(r)\varphi(s)}{2}} = \left(a^{\varphi(s)}\right)^{\frac{\varphi(r)}{2}} \equiv 1 \ (\mod s) \end{cases}$$

e portanto, como $(r, s) = 1$,

$$a^{\frac{\varphi(n)}{2}} = \ \equiv \ 1 \ (\mod n).$$

Concluímos assim que a ordem de a, módulo n é menor ou igual a $\frac{\varphi(n)}{2}$. Em particular, a não é raiz primitiva de n. ■

Para terminar esta subsecção vamos mostrar que os inteiros da forma 2^k com $k \geq 3$ também não admitem raízes primitivas.

Proposição 5.6 *Se n é um inteiro da forma 2^k, com $k \geq 3$ então,*

$$\forall\, a \in \mathbb{Z} \ \left[\ (a, n) = 1 \ \Rightarrow \ ord_n a \middle| 2^{k-2} \right].$$

Em particular n não admite raízes primitivas.

Demonstração: Para a primeira parte basta mostrar que

$$a^{2^{k-2}} \equiv 1 \ (\mod 2^k).$$

A demonstração será feita por indução sobre k.

Se $k = 3$, basta consultar a tabela da página 85.

Suponhamos o resultado válido para k e demonstremos para $k + 1$.

$$\begin{aligned} a^{2^{k-1}} &= \left[a^{2^{k-2}}\right]^2 \\ &= \left[1 + d2^k\right]^2, \quad \text{para algum } d \in \mathbb{Z}, \text{ por hipótese de indução} \\ &= 1 + d2^{k+1} + d^2 2^{2k} \\ &\equiv 1 \ (\mod 2^{k+1}). \end{aligned}$$

Para a segunda parte basta usar a definição de raiz primitiva e notar que $\varphi(2^k) = 2^{k-1}$. ■

Pelo que acabamos de ver, os inteiros da forma 2^k com $k \geq 3$ não admitem raízes primitivas (ou seja, os grupos $\mathbb{Z}_{2^k}^*$ não são cíclicos). Contudo admitem elementos (o 5, por exemplo) que funciona quase como uma raiz primitiva. Mais concretamente o 5 tem ordem 2^{k-2} e

$$\left\{5^\beta : \beta \in \{1, \ldots, 2^{k-2}\}\right\} \cup \left\{-5^\beta : \beta \in \{1, \ldots, 2^{k-2}\}\right\}$$

é um sistema reduzido de resíduos módulo 2^k (ver Exercício 6.35).

5.2.2 Caso p primo

Comecemos por recordar alguns resultados sobre anéis de polinómios.

Se $f(X)$ é um polinómio com grau n de coeficientes num anel, então o número de zeros de $f(X)$ pode ser maior, menor ou igual a n como podemos ver pelos exemplos apresentados na seguinte tabela:

Anel dos coeficientes	polinómio	grau	números de zeros
$\mathbb{Z}_6$	$X(X+1)(X+2)$	3	6
$\mathbb{Z}_5$	$X^2 - X - 1$	2	1
$\mathbb{Z}_5$	$X^2 + 2$	2	0
$\mathbb{Z}_5$	$X^2 - 3X + 2$	2	2
$\mathbb{Z}_8$	$X^2 - 1$	2	4

Se o anel em questão for um corpo então o número de zeros de $f(X)$ é no máximo igual a n como diz o seguinte teorema (de Lagrange).

Teorema 5.7 *Se $\mathbb{K}$ é um corpo e $f(X)$ um polinómio de coeficientes em $\mathbb{K}$ de grau n (com $n \in \mathbb{N}$) então a equação*

$$f(X) = 0$$

tem no máximo n soluções.

Demonstração: A demonstração pode ser feita por indução sobre n começando por mostrar que, se a é um zero de $f(X)$ então existe um polinómio $g(X)$ de grau $n-1$ tal que $f(X) = (X-a)g(X)$ (até aqui, não usamos o facto de $\mathbb{K}$ ser um corpo).

Note-se que $f(\alpha) = 0$ se e só se $(\alpha - a)g(\alpha)$ ou seja, como $\mathbb{K}$ é um corpo, $\alpha = a$ ou $g(\alpha) = 0$. Deste modo

$$\{\text{zeros de } f(X)\} \quad = \quad \{\text{zeros de } g(X)\} \cup \{a\}.$$

Por hipótese de indução, uma vez que $g(X)$ tem grau $n-1$, podemos concluir que $g(X)$ tem no máximo $n-1$ zeros e, portanto $f(X)$ tem no máximo n zeros. ■

Se p é um número primo e $\mathbb{K} = \mathbb{Z}_p$ este teorema pode ser escrito na forma seguinte.

Corolário 5.8 *Sejam p um número primo e $f(X)$ um polinómio de coeficientes inteiros cujo coeficiente guia não é divisível por p. Se n é o grau de $f(X)$, então a congruência*

$$f(X) \equiv 0 \ (\bmod p)$$

tem no máximo n soluções incongruentes módulo p. ■

O seguinte resultado, de teoria de grupos, é crucial na demonstração da existência de raízes primitivas módulo um inteiro primo.

Lema 5.9 *Sejam $(G, \cdot)$ um grupo e $a, b \in G$ tais que $ab = ba$. Se a tem ordem n, b tem ordem m e $(n, m) = 1$ então ab tem ordem nm.*

Demonstração: Seja e o elemento neutro do grupo e k a ordem de ab. Como $(ab)^{nm} = (a^n)^m (b^m)^n = e$ podemos concluir que k divide nm. Para mostrar que nm divide k basta-nos mostrar (porque $(n, m) = 1$) que m e n dividem k.

Note-se que

$$\begin{aligned} b^{kn} &= a^{kn} b^{kn} && \text{porque } a^n = e \\ &= \left[(ab)^k\right]^n && \text{porque } a \text{ comuta com } b \\ &= e && \text{porque } (ab)^k = e. \end{aligned}$$

Como m é a ordem de b e $b^{kn} = e$ podemos concluir que m divide kn e, como $(m, n) = 1$, m divide k. De modo análogo se vê que n divide k. ■

Vejamos agora que todo o número primo admite raízes primitivas.

Teorema 5.10 *Se p é um número primo então existe $\varphi(p-1)$ raízes primitivas de p, incongruentes módulo p.*

Demonstração: Atendendo ao Corolário 5.3 basta mostrar que existe **uma** raiz primitiva de p. É claro que basta também considerar o caso em que $p > 2$.

Sejam $s \in \mathbb{N}$, $q_1, q_2, \ldots, q_s$ primos distintos e $r_1, r_2, \ldots r_s \in \mathbb{N}$ tais que

$$p - 1 = q_1^{r_1} q_2^{r_2} \cdots q_s^{r_s}$$

Para cada $i = 1, 2, \ldots, s$ sejam:

- $a_i \in \mathbb{N}$, que não é solução da congruência $X^{\frac{p-1}{q_i}} \equiv 1 \pmod{p}$ (a existência de a_i é garantida pelo Corolário 5.8);
- $x_i = a_i^{\frac{p-1}{q_i^{r_i}}}$.

Como $x_i^{q_i^{r_i}} = a_i^{p-1} \equiv 1 \pmod{p}$ e $x^{q_i^{r_i-1}} = a_i^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}$, podemos concluir que x_i tem ordem $q_i^{r_i}$.

Utilizando repetidamente o Lema 5.9 vemos que o $x_1 x_2 \cdots x_s$ tem ordem $q_1^{r_1} q_2^{r_2} \cdots q_s^{r_s}$ que é igual a $p - 1$. Daqui concluímos que $x_1 x_2 \cdots x_s$ é uma raiz primitiva de n. ■

Exemplo 5.11 *Pretende-se calcular as raízes primitivas de $p = 13$. Comecemos por calcular a ordem de 2. Para isso podemos começar por calcular, módulo 13, as potências de 2 até 2^6 (note-se que $6 = \frac{\varphi(13)}{2}$).*

k	0	1	2	3	4	5	6	7	8	9	10	11	12
2^k	1	2	4	8	3	6	-1	·	·	·	·	·	·

Note-se que, desta tabela podemos concluir que $ord_{13}2 \notin \{1, 2, 3, 4, 6\}$. Como $ord_{13}2$ divide $\varphi(13)$ então $ord_{13}2 = 12$, ou seja, que 2 é uma raiz primitiva de 13.

Além disso, podemos concluir que as raízes primitivas de 13 são os inteiros que são congruentes módulo 13 com algum elemento da forma 2^i, com $(i, 12) = 1$. Deste modo

as outras raízes primitivas de 13 *no conjunto* $\{0, 1, 2, \ldots, 12\}$ *são:* 6, 7 *e* 11, *que são congruentes módulo* 13 *com* 2^5, 2^{11} *e* 2^7 *respectivamente.*

Assim,

$$\Big\{\textit{raízes primitivas de } 13\Big\} = \Big\{a \in \mathbb{Z} : \exists\, b \in \{2, 6, 11, 7\} : a \equiv b \ (\bmod 13)\Big\}.$$

5.2.3 Caso p^k e $2p^k$, em que p é primo

Nesta secção vamos mostrar que os inteiros da forma p^k ou $2p^k$, com p primo ímpar, admitem raízes primitivas. Começamos com três lemas auxiliares.

Lema 5.12 *Se p é um número primo ímpar e r é uma raiz primitiva de p tal que $r^{p-1} \not\equiv 1 \pmod{p^2}$ então*

$$\forall\, k \geq 2, \quad r^{p^{k-2}(p-1))} \not\equiv 1 \ (\bmod p^k).$$

Demonstração: Vamos fazer a demonstração por indução sobre k.

Para $k = 2$ não há nada a demonstrar.

Vejamos a demonstração do passo de indução:

Suponhamos que $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$.

Pelo teorema de Euler $r^{\varphi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}$ ou seja $r^{p^{k-2}(p-1)} = 1 + tp^{k-1}$ para algum $t \in \mathbb{Z}$. Uma vez que $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$, t não é divisível por p.

Assim,

$$\begin{aligned} r^{p^{k-1}(p-1)} &= \left[r^{p^{k-2}(p-1)}\right]^p = (1 + tp^{k-1})^p \\ &= 1 + \binom{p}{1} tp^{k-1} + \text{múltiplo de } p^{k+1} \\ &\equiv 1 + tp^k \ (\bmod p^{k+1}). \end{aligned}$$

Como $p \nmid t$, temos $tp^k \not\equiv 0 \pmod{p^{k+1}}$ e, portanto, $r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$. ■

Exercício 5.13 *Onde é que no lema anterior foi usado o facto de p ser ímpar?*

Lema 5.14 *Se r é uma raiz primitiva de um número primo ímpar p, então*

$$r^{p-1} \not\equiv 1 \ (\mod p^2) \quad ou \quad (r+p)^{p-1} \not\equiv 1 \ (\mod p^2).$$

Demonstração: Suponhamos que $r^{p-1} \equiv 1 \pmod{p^2}$. Então

$$\begin{aligned} (r+p)^{p-1} &= r^{p-1} + (p-1)\, r^{p-2} p + \text{múltiplo de } p^2 \\ &\equiv 1 - p\, r^{p-2} \ (\mod p^2) \\ &\not\equiv 1 \ (\mod p^2). \end{aligned}$$

A última conclusão é uma consequência do facto de p não dividir r. ■

Nota 5.15 *Usando estes dois lemas podemos concluir que todo o número primo ímpar p admite uma raiz primitiva r tal que $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ para todo $k \geq 2$.*

Lema 5.16 *Sejam $n \in \mathbb{N}$ e $a \in \mathbb{Z}$ tais que $(a, n) = 1$. Então, se a e n são ímpares,*

$$ord_n a = ord_{2n} a.$$

Demonstração: Basta mostrar que, se $k \in \mathbb{N}$, então

$$a^k \equiv 1 \ (\mod n) \Leftrightarrow a^k \equiv 1 \ (\mod 2n).$$

Para mostrar esta equivalência, note-se que,

$$\begin{aligned} a^k \equiv 1 \ (\mod 2n) &\Leftrightarrow \begin{cases} a^k \equiv 1 \ (\mod n) \\ a^k \equiv 1 \ (\mod 2) \end{cases} \quad \text{porque } (2, n) = 1 \\ &\Leftrightarrow a^k \equiv 1 \ (\mod n), \text{ porque } a \text{ é um número ímpar.} \end{aligned}$$

■

Teorema 5.17 *Se p é um número primo ímpar e $k \in \mathbb{N}$, então p^k e $2p^k$ admitem raízes primitivas.*

Demonstração: Usando a Nota 5.15, seja r uma raiz primitiva de p tal que

$$r^{p^{k-2}(p-1)} \not\equiv 1 \ (\mod p^k).$$

Seja $n = ord_{p^k} r$.

Como $a^n \equiv 1 \pmod{p}$ e r é uma raiz primitiva de p então, usando a alínea d) da Proposição 5.2, $p-1$ divide n. Deste modo, como n divide $\varphi(p^k) = p^{k-1}(p-1)$, existe $j \leq k-1$ tal que $n = p^j(p-1)$.

Se $j < k-1$ então, n divide $p^{k-2}(p-1)$ e portanto, por definição de n,

$$r^{p^{k-1}(p-2)} \equiv 1 \ (\mod p^k)$$

o que contradiz a hipótese sobre r. Conclusão $j = k-1$ e $ord_{p^k} r = p^{k-1}(p-1)$ ou seja, r é uma raiz primitiva de p^k.

Para a segunda parte do teorema, sejam r uma raiz primitiva de p^k e

$$s \ = \ \begin{cases} r & \text{se } r \text{ é ímpar} \\ r + p^k & \text{se } r \text{ é par} \end{cases}$$

Então s é uma raiz primitiva ímpar de p^k. Por outro lado

$$\begin{aligned} ord_{2p^k} s &= ord_{p^k} s \quad \text{Pelo Lema 5.16} \\ &= \varphi(p^k) \quad \text{porque } s \text{ é uma raiz primitiva de } p^k \\ &= \varphi(2p^k) \quad \text{porque } \varphi(2p^k) = \varphi(2)\varphi(p^k). \end{aligned}$$

Daqui concluímos que s é uma raiz primitiva de $2p^k$. ■

Nota 5.18 *Na prática, se pretendermos encontrar uma raiz primitiva de um inteiro da forma p^k, com p primo ímpar, fazemos o seguinte:*

- *encontramos uma raiz primitiva r de p (por tentativas);*
- *verificamos se r^{p-1} é congruente com 1 módulo p^2;*
- *se $r^{p-1} \not\equiv 1 \pmod{p^2}$, então r é uma raiz primitiva de p^k;*

- *se* $r^{p-1} \equiv 1 \pmod{p^2}$*, então* $r+p$ *é uma raiz primitiva de* p^k*.*

Note-se que, "em princípio", a probabilidade de r^{p-1} *ser congruente com* 1 *módulo* p^2 *é pequena* $(= \frac{1}{p(p-1)})$*.*

Para o cálculo de uma raiz primitiva de $2p^k$ *(*p *primo ímpar) procedemos do seguinte modo:*

- *encontramos uma raiz primitiva* r *de* p^k*;*
- *se* r *for ímpar então* r *é uma raiz primitiva de* $2p^k$*;*
- *se* r *for par, então* $r+p^k$ *é uma raiz primitiva de* $2p^k$ *(porque* $r+p^k$ *é uma raiz primitiva ímpar de* p^k*).*

Vemos assim que a dificuldade maior está em encontrar raízes primitivas de números primos. Apenas a título informativo vejamos uma tabela com a menor raiz primitiva de cada um dos números primos menores que 71 (p designa o número primo e r designa a raiz primitiva de p).

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
r	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5	2	2	2	2	7

5.3 Aplicações. Tabelas de índices

Vejamos agora uma aplicação do estudo das raízes primitivas na resolução de algumas congruências.

Comecemos por recordar que, se r é uma raiz primitiva de um inteiro n, então

$$\left\{r^k : k \in \{0,1,\ldots,\varphi(n)-1\}\right\}$$

é um **srr** módulo n. Tem então sentido a seguinte definição:

Definição 5.19 *Sejam* n *um inteiro que admite raízes primitivas,* r *uma raiz primitiva de* n *e* $a \in \mathbb{Z}$ *tal que* $(a,n)=1$*. Define-se,* **índice de** a **módulo** n**, relativamente a** r*, como sendo o único inteiro* $k \in \{0,1,\ldots,\varphi(n)-1\}$ *tal que* $a \equiv r^k \pmod{n}$*.*

Notação: escreveremos $ind_r^n a$ para designar o índice de a módulo n, relativamente a r. Se não houver dúvidas quanto a n escreveremos $ind_r a$ em vez de $ind_r^n a$.

Vejamos algumas propriedades (que nos fazem lembrar as propriedades da função logaritmo) cujas demonstrações são deixadas como exercício.

Proposição 5.20 *Sejam n um inteiro que admite raízes primitivas, r e s raízes primitivas de n e $a, b \in \mathbb{Z}$ tais que $(a, n) = (b, n) = 1$. Então:*

- $a \equiv b \pmod{n}$ *se e só se* $ind_r a = ind_r b$;
- $ind_r(ab) \equiv ind_r a + ind_r b \pmod{\varphi(n)}$;
- *se* $k \in \mathbb{N}$, $ind_r a^k \equiv k\, ind_r a \pmod{\varphi(n)}$;
- $ind_r a \equiv (ind_s a)(ind_r s) \pmod{\varphi(n)}$. ■

Definição 5.21 *Uma* **tabela** *de índices módulo n relativamente a uma raiz primitiva a é uma tabela da forma*

$ind_r a$	0	1	$\cdots$	$\varphi(n)-1$
a				

em que, em cada célula da segunda linha aparece o elemento do **srr** *cujo índice é o número que está na primeira linha e na mesma coluna.*

Exemplos 5.22 *Vejamos alguns exemplos.*

a) $n = 4$, $r = 3$.

Usando o **srr** $\{1, 3\}$.

$ind_3 a$	0	1
a	1	3

b) $n = 7$, $r = 3$.

Usando o **srr** $\{1, 2, 3, 4, 5, 6\}$.

$ind_3 a$	0	1	2	3	4	5
a	1	3	2	6	4	5

c) $n = 7$, $r = 3$.

Usando o **srr** $\{1, 2, 3, -3, -2, -1\}$.

$ind_3 a$	0	1	2	3	4	5
a	1	3	2	-1	-3	-2

d) $n = 13$, $r = 2$.

Usando o **srr** $\{1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

$ind_2 a$	0	1	2	3	4	5	6	7	8	9	10	11
a	1	2	4	8	3	6	12	11	9	5	10	7

e) $n = 13$, $r = 2$.

Usando o **srr** $\{1, 2, 4, 8, 3, 6, -1, -2, -4, -8, -3, -6\}$.

$ind_2 a$	0	1	2	3	4	5	6	7	8	9	10	11
a	1	2	4	8	3	6	-1	-2	-4	-8	-3	-6

f) $n = 17$, $r = 3$.

Usando o **srr** $\{a \in \mathbb{N} : 1 \leq a \leq 17, (a, 17) = 1\}$.

$ind_3 a$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

g) $n = 17$, $r = 5$.

Usando o **srr** $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5 \pm 6, \pm 7, \pm 8\}$.

$ind_3 a$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1	5	8	6	-4	-3	2	-7	-1	-5	-8	-6	4	5	-2	7

h) $n = 25$, $r = 2$.

Usando o **srr** $\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7, \pm 8, \pm 9 \pm 11, \pm 12\}$.

$ind_2 a$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a	1	2	4	8	-9	7	-11	3	6	12	-1	-2	-4	-8	9

15	16	17	18	19
-7	11	-3	-6	-12

Exercício 5.23 *Mostre que, se r é uma raiz primitiva de n então $ind_r(-1) = \frac{\varphi(n)}{2}$.*

Atendendo a este exercício, podemos preencher a segunda linha da tabela de índices de tal modo que os elementos da segunda metade da linha sejam os simétricos dos elementos que aparecem na primeira metade da linha (ver exemplos atrás).

A justificação é simples: se r é um raiz primitiva de n, e $(a, n) = 1$ então

$$ind_r(-a) = ind_r(-1) + ind_r(a) = \frac{\varphi(n)}{2} + ind_r(a).$$

5.3.1 Congruências do tipo $aX^m \equiv b \pmod{n}$

Se $a, b \in \mathbb{Z}$ e $m, n \in \mathbb{N}$, a congruência (na variável inteira X) $aX^m \equiv b \pmod{n}$ é equivalente ao sistema:

$$\begin{cases} aX^m & \equiv & b \pmod{p_1^{n_1}} \\ & \ddots & \\ aX^m & \equiv & b \pmod{p_s^{n_s}} \end{cases}$$

em que $n = p_1^{n_1} \cdots p_s^{n_s}$, sendo $s, n_1, \ldots, n_s \in \mathbb{N}$ e $p_1, \ldots, p_s$ números primos distintos.

Assim, basta-nos considerar o caso em que $n = p^k$ em que p é um primo e $k \in \mathbb{N}$.

Vejamos os diversos casos:

1. p não divide b nem a. Este é o caso típico que será resolvido de seguida;
2. p não divide b e p divide a. A congruência não tem solução;
3. p divide b e a. Podemos simplificar a congruência obtendo uma congruência do tipo $a'X^m \equiv b' \pmod{p^s}$ em que $s < k$;
4. p divide b e p não divide a. Neste caso as soluções são da forma $X = pY$. Substituindo e simplificando obtemos congruência da forma $a'Y^m \equiv b' \pmod{p^s}$ em que $s < k$.

De qualquer das maneiras a congruência inicial é sempre equivalente (simplificando várias vezes, se necessário) a uma congruência de um dos dois primeiros tipos.

Resta assim saber resolver congruências do tipo $aX^m \equiv b \pmod{p^k}$ em que p não divide a nem b.

Se $p = 2$ e $k \geq 3$ a resolução será feita por tentativas! Nos outros casos podemos usar índices. É claro que em alguns casos, o mais fácil é usar o método das tentativas.

Proposição 5.24 *Sejam p um primo ímpar, $k \in \mathbb{N}$ e r uma raiz primitiva de p^k. Se $a, b \in \mathbb{Z}$ são tais que p não divide a nem b então a congruência $aX^m \equiv b \pmod{p^k}$ tem solução se e só se $(m, \varphi(p^k))$ divide $(ind_r b - ind_r a)$.*

Se a congruência tiver solução então admite $(m, \varphi(p^k))$ soluções módulo p^k.

Demonstração: Usando a Proposição 5.20 temos,

$$\begin{aligned} aX^m \equiv b \ (\bmod p^k) &\Leftrightarrow ind_r(aX^m) = ind_r b \\ &\Leftrightarrow ind_r a + ind_r(X^m) \equiv ind_r b \ (\bmod \varphi(p^k)) \\ &\Leftrightarrow ind_r a + m\, ind_r X \equiv ind_r b \ (\bmod \varphi(p^k)) \\ &\Leftrightarrow m\, ind_r X \equiv ind_r b - ind_r a \ (\bmod \varphi(p^k)). \end{aligned}$$

Deste modo a congruência original tem tantas soluções módulo p^k, como o número de soluções módulo $\varphi(p^k)$, da congruência linear, na incógnita inteira Y,

$$m\,Y \equiv ind_r b - ind_r a \ (\bmod \varphi(p^k)).$$

Para concluir basta utilizar o que já sabemos sobre congruências lineares. ■

Exemplo 5.25 *Consideremos a congruência $37X^{1230} \equiv 11 \pmod{17 \times 13}$.*

Esta congruência é equivalente ao sistema

$$\begin{cases} 37X^{1230} \equiv 11 \ (\bmod 17) \\ 37X^{1230} \equiv 11 \ (\bmod 13) \end{cases}$$

Para a resolução da primeira congruência usamos 3 como raiz primitiva de 17.

Como 17 *não divide* 11*, temos*

$$\begin{aligned}
37X^{1230} \equiv 11 \ (\text{ mod } 17) &\Leftrightarrow ind_3(37X^{1230}) = ind_3 11 \\
&\Leftrightarrow ind_3(37) + ind_3(X^{1230}) \equiv ind_3 11 \ (\text{ mod } 16) \\
&\Leftrightarrow ind_3(37) + 1230\, ind_3(X) = ind_3 11 \ (\text{ mod } 16) \\
&\Leftrightarrow ind_3(3) + 14\, ind_3(X) = ind_3 11 \ (\text{ mod } 16) \\
&\quad \textit{porque } 37 \equiv 3 \ (\text{ mod } 17) \textit{ e } 1230 \equiv 14 \ (\text{ mod } 16) \\
&\Leftrightarrow 1 + 14\, ind_3(X) \equiv 7 \ (\text{ mod } 16) \\
&\quad \textit{usando a tabela de índices da página 96} \\
&\Leftrightarrow 14\, ind_3(X) \equiv 6 \ (\text{ mod } 16).
\end{aligned}$$

Fazendo $Y = ind_3(X)$ *obtemos a equação* $14Y \equiv 6 \pmod{16}$*. As soluções desta equação são:* $Y = 5$ *e* $Y = 13$*. Usando novamente a tabela e a igualdade* $Y = ind_3(X)$*, concluímos que as soluções da congruência são:* $X \equiv 5 \pmod{17}$ *e* $X \equiv 12 \pmod{17}$*.*

Para a resolução da segunda congruência do sistema usamos 2 *como raiz primitiva de* 13*. Como* 13 *não divide* 11*, temos*

$$\begin{aligned}
37X^{1230} \equiv 11 \ (\text{ mod } 13) &\Leftrightarrow 11X^6 \equiv 11 \ (\text{ mod } 13) \\
&\quad \textit{porque } X^{12} \equiv 1 \ (\text{ mod } 12) \textit{ e } 1230 \equiv 6 \ (\text{ mod } 12) \\
&\Leftrightarrow X^6 \equiv 1 \ (\text{ mod } 13) \\
&\quad \textit{porque } (11, 13) = 1 \\
&\Leftrightarrow ind_2(X^6) \equiv ind_2 1 \ (\text{ mod } 12) \\
&\Leftrightarrow 6\, ind_2(X) = 0 \ (\text{ mod } 12)
\end{aligned}$$

Fazendo $Y = ind_3(X)$ *obtemos a equação* $6Y \equiv 0 \pmod{12}$*. As soluções (módulo* 12*) desta equação são:* $Y = 0$*,* $Y = 2$*,* $Y = 4$*,* $Y = 6$*,* $Y = 8$ *e* $Y = 10$*. Usando novamente a tabela e a igualdade* $Y = ind_3(X)$*, obtemos como soluções da congruência:* X *congruente, módulo* 13*, com* 1*,* 3*,* 4*,* 9*,* 10 *ou* 12*.*

Assim as soluções do sistema

$$\begin{cases} 37X^{1230} \equiv 11 \ (\text{ mod } 17) \\ 37X^{1230} \equiv 11 \ (\text{ mod } 13) \end{cases}$$

são as soluções de cada um dos sistemas

$$\begin{cases} X & \equiv & a \ (\mod 17) \\ X & \equiv & b \ (\mod 13) \end{cases}$$

em que $a \in \{5, 12\}$ *e* $b \in \{1, 3, 4, 9, 10, 12\}$. *Cada um destes sistemas pode ser resolvido pelo método descrito na Secção 2.2.*

As soluções, módulo 17×13*, da congruência inicial são:* 12*,* 22*,* 29*,* 56*,* 90*,* 107*,* 114*,* 131*,* 165*,* 192*,* 199 *e* 209*.*

5.3.2 Congruências do tipo $ab^X \equiv c \pmod{n}$

Consideremos agora congruências do tipo $ab^X \equiv c \pmod{n}$ (na variável inteira X), em que $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$.

Usando argumentos análogos aos que foram usados na secção anterior, ficamos reduzidos ao caso em que $n = p^k$ em que p é um primo ímpar.

Vejamos as várias situações possíveis:

1. p não divide c, a nem b. É o caso típico que vamos tratar de seguida;
2. p não divide c e divide b ou a. A equação não tem solução;
3. p divide c e divide a. Podemos simplificar, obtendo uma congruência do tipo $db^X \equiv f \pmod{p^s}$ em que $s < k$;
4. p divide c e b e não divide a. A congruência tem solução trivial;
5. p divide c e não divide a nem b. A equação não tem solução.

Deste modo as congruências do primeiro tipo são as que precisamos de estudar. O método para as resolver é semelhante ao aplicada nas congruências da subsecção anterior.

Neste caso, se r é uma raiz primitiva de p^k,

$$\begin{aligned} ab^X \equiv c \ (\mod p^k) &\Leftrightarrow ind_r(ab^X) = ind_r c \\ &\Leftrightarrow ind_r a + X \ ind_r b \equiv ind_r c \ (\mod \varphi(p^k)) \\ &\Leftrightarrow (ind_r b) \ X \equiv ind_r c - ind_r a \ (\mod \varphi(p^k)). \end{aligned}$$

Ficamos novamente com uma congruência linear (na variável X) que já sabemos resolver, se tivermos uma tabela de índices de p^k relativamente a r.

Concluímos assim o seguinte resultado.

Proposição 5.26 *Sejam p um primo ímpar, $k \in \mathbb{N}$ e r uma raiz primitiva de p^k. Se $a, b, c \in \mathbb{Z}$ são tais que p não divide a, b nem c então a congruência $a\,b^X \equiv c \pmod{p^k}$ tem solução se e só se $(\varphi(p^k), ind_r b)$ divide $(ind_r c - ind_r a)$.*

Se a congruência tiver solução então admite $(\varphi(p^k), ind_r b)$ soluções módulo p^k.

Demonstração: Usando novamente a Proposição 5.20 temos

$$\begin{aligned} ab^X \equiv c \ (\bmod p^k) &\Leftrightarrow ind_r(ab^X) = ind_r c \\ &\Leftrightarrow ind_r a + X\ ind_r b \equiv ind_r c \ (\bmod \varphi(p^k)) \\ &\Leftrightarrow (ind_r b)\ X \equiv ind_r c - ind_r a \ (\bmod \varphi(p^k)). \end{aligned}$$

Basta usar usar o que sabemos sobre congruências lineares. ■

Exemplo 5.27 *Consideremos a equação $13 \cdot 12^X \equiv 1 \pmod{25}$. Usando a raiz primitiva 2 e a tabela feita acima obtemos,*

$$\begin{aligned} 13 \cdot 12^X \equiv 1 \ (\bmod 25) &\Leftrightarrow ind_2(13 \cdot 12^X) = ind_2 1 \\ &\Leftrightarrow ind_2 13 + X\, ind_2 12 \equiv 0 \ (\bmod 20) \\ &\Leftrightarrow 19 + 9X \equiv 0 \ (\bmod 20) \\ &\Leftrightarrow 9X \equiv 1 \ (\bmod 20) \\ &\Leftrightarrow X \equiv 9 \ (\bmod 20). \end{aligned}$$

5.4 Exercícios

5.1. Determine a ordem de:

a) 2 módulo 5;

b) 10 módulo 13;

c) 3 módulo 10;

d) 11 módulo 20;

e) 31^{10} módulo 17.

5.2. Mostre que, se $\overline{a}$ é um inverso de a módulo n, então $ord_n a = ord_n \overline{a}$. Conclua que a é uma raiz primitiva de n se e só se $\overline{a}$ é uma raiz primitiva de n.

5.3. Mostre que, se n é um inteiro positivo e a e b são inteiros primos com n tais que $(ord_n a, ord_n b) = d$, então $ord_n(ab) = \text{m. m. c.}\,(ord_n a, ord_n b)$.

Compare com o Lema 5.9.

5.4. Mostre que, se $(m, 583) = 1$, então $ord_{583} m \leq 260$.

5.5. Mostre que $ord_{2^n-1} 2 = n$. Conclua que $\varphi(2^n - 1)$ é um múltiplo de n $(n > 1)$.

5.6. Sejam p um número primo ímpar, $a > 1$, $(a, p) = 1$ e $r = ord_p\, a$. Mostre que

a) $a^{r-1} + a^{r-2} + \cdots + a + 1 \equiv 0 \pmod{p}$;

b) se $r = 3$ então $(a+1)^2 \equiv a \pmod{p}$ e $(a+1)^3 \equiv -1 \pmod{p}$;

c) se $r = 3$ então $ord_p(a+1) = 6$.

5.7. Seja p um primo divisor do número de Fermat, $F_n = 2^{2^n} + 1$.

a) Mostre que, $ord_{F_n} 2 \leq 2^{n+1}$, onde $F_n = 2^{2^n} + 1$.

b) Mostre que, $ord_p 2 = 2^{n+1}$.

c) Use a alínea anterior para mostrar que, $2^{n+1} | (p-1)$ e assim p é da forma $2^{n+1}k + 1$.

d) Mostre que F_5 não é primo.

5.8. Sejam g e h raízes primitivas de um primo ímpar p. Mostre que:

a) existe um inteiro ímpar k tal que $h \equiv g^k \pmod{p}$;

b) $(gh)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$;

c) gh não é raiz primitiva de p.

5.9. Encontre todas as raízes primitivas (caso existam) módulo cada um dos seguintes inteiros: 4, 5, 6, 10, 11, 12, 13, 14, 16, 17, 18, 22, 26, 28, 50 e 71.

5.10. Encontre uma raiz primitiva (caso exista) módulo cada um dos seguintes inteiros: 338, 11^2, 17^2, 13^2, 19^2, 71^2 e 2×71^2.

5.11. Determine uma raiz primitiva, para todo o inteiro positivo k, módulo: 3^k, 13^k, 11^k e 17^k.

5.12. Determine o número de raízes primitivas de: 7, 19, 13, 29, 17, 47, 625, 686, 242, 4394 e 11×2662.

5.13. Dê um exemplo, se existir, de um inteiro positivo n entre 30 e 40 com 17 raízes primitivas módulo n.

5.14. Dê um exemplo, se existir, de um inteiro positivo entre 30 e 70 com mais de 20 raízes primitivas.

5.15. Existe algum inteiro m que tenha exactamente 1248 raízes primitivas?

5.16. Sabendo que 3 é raiz primitiva de 31 e que 7 é raiz primitiva de 41, calcule um inteiro que seja raiz primitiva de 31 e de 41.

5.17. Use a teoria de índices para calcular o resto da divisão de $3^{34} \times 5^{13}$ por 17.

5.18. Mostre que, r é uma raiz primitiva módulo um primo ímpar p se e só se $r^{\frac{p-1}{q}}$ não é congruente com 1 módulo p, para todo primo q que divida $p-1$.

5.19. Seja p um número primo ímpar e r uma raiz primitiva de p. Mostre que:

a) se $p \equiv 1 \pmod 4$, então $-r$ é uma raiz primitiva de p;

b) se $p \equiv 3 \pmod 4$, então $ord_p(-r) = \frac{p-1}{2}$.

5.20. Mostre que, se m tem uma raiz primitiva r, então as únicas soluções da congruência $x^2 \equiv 1 \pmod m$ são $x \equiv \pm 1 \pmod m$. Conclua que $r^{\frac{\varphi(m)}{2}} \equiv -1 \pmod m$.

5.21. Seja r uma raiz primitiva de um primo p ímpar. Mostre que o produto das raízes primitivas (menores que p) de primo p é congruente com $r^{\frac{\varphi(p-1)}{2}}$.

5.22. Encontre o número de zeros incongruentes módulo n dos polinómios:

a) $x^2 - x$, se $n = 6$;

b) $x^2 - 1$, se $n = 15$;

c) $x^2 + 21$, se $n = 33$.

5.23. Seja p um número primo.

a) Mostre que se $f(x)$ é um polinómio de grau n com coeficientes inteiros e com mais de n raízes módulo p, então p divide todos os coeficientes de $f(x)$.

b) Use (a) para mostrar que, todo o coeficiente do polinómio

$$(x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$$

é divisível por p.

c) Use as alíneas anteriores para demonstrar o teorema de Wilson.

5.24. Seja p um número primo ímpar. Mostre que:

a) se $k \in \mathbb{N}$ é primo com $p-1$, então $\{1^k, 2^k, \ldots, (p-1)^k\}$ é um sistema reduzido de resíduos módulo p;

b) $1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} -1 \pmod{p} & \text{se } (p-1)|n \\ 0 \pmod{p} & \text{caso contrário} \end{cases}$

5.25. Sabendo que 2 é uma raiz primitiva de 29 resolva a congruência

$$7x^{34} \equiv -1 \ \ (\text{ mod } 29).$$

$ind_2 a$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	$\cdots$
a	1	2	4	8	16	3	6	12	24	19	9	18	7	14	28	$\cdots$

5.26. Resolva as congruências:

a) $7x^3 \equiv 3 \pmod{11}$;

b) $3x^4 \equiv 5 \pmod{11}$;

c) $x^8 \equiv 10 \pmod{11}$;

d) $7x^{12} \equiv 13 \pmod{17}$;

e) $2x^{48} \equiv 9 \pmod{17}$;

f) $9x^8 \equiv 8 \pmod{17}$;

g) $3x^5 \equiv 1 \pmod{23}$;

h) $3x^{14} \equiv 2 \pmod{23}$.

i) $x^8 \equiv 17 \pmod{43}$;

j) $x^8 \equiv 2 \pmod{41}$;

k) $x^6 \equiv 2 \pmod{31}$;

l) $x^{85} \equiv 1 \pmod{102}$;

m) $3x^4 \equiv 5 \pmod{29}$;

n) $36x^6 \equiv 168 \pmod{37}$;

o) $7x^{1001} \equiv 943 \pmod{37}$;

p) $25x^6 \equiv 168 \pmod{391}$;

q) $44x^8 + 127 \equiv 0 \pmod{667}$.

5.27. Resolva as congruências:

a) $7^x \equiv 7 \pmod{17}$;

b) $3^x \equiv 2 \pmod{23}$;

c) $13^x \equiv 5 \pmod{23}$;

d) $8^x \equiv 3 \pmod{43}$;

e) $3 \cdot 11^x \equiv 12 \pmod{37}$).

5.28. A congruência $29x^2 \equiv 1000 \pmod{701}$ tem solução?

5.29. Mostre que a congruência $x^2 \equiv 211 \pmod{159}$ tem exactamente 4 soluções.

5.30. Para que inteiros positivos a, a congruência $ax^4 \equiv 5 \pmod{23}$ tem solução?

5.31. Para que inteiros positivos b, a congruência $8x^7 \equiv b \pmod{29}$ tem solução?

5.32. Determine as soluções de:

a) $2^x \equiv x \pmod{13}$;

b) $x^x \equiv x \pmod{23}$;

c) $y^2 \equiv 5x^3 \pmod{7}$.

5.33. (O seguinte resultado generaliza o Teorema de Wilson) Seja n um inteiro positivo com uma raiz primitiva. Usando esta raiz primitiva, prove que o produto de todos os inteiros positivos menores que n e primos com n é congruente com -1 módulo n.

5.34. Mostre que, se p é primo e $p = 2q + 1$, para q um inteiro primo e a um inteiro positivo tal que $1 < a < p - 1$, então $p - a^2$ é uma raiz primitiva módulo p.

5.35. (Ver página 88) Seja $k \geq 3$. Mostre que:

a) $5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}$;

b) $ord_{2^k} 5 = 2^{k-2}$;

c) $\mathbb{Z}_{2^k}^* = \left\{5^\beta : \beta \in \{1, \ldots, 2^{k-2}\}\right\} \cup \left\{-5^\beta : \beta \in \{1, \ldots, 2^{k-2}\}\right\}$.

5.36. Seja r uma raiz primitiva de um primo p. Mostre que

$$\nexists\, k \in \mathbb{N} : \ r^{k+2} \equiv r^{k+1} + 1 \equiv r^k + 2 \ (\bmod\ p).$$

5.37. Mostre que a congruência $x^3 \equiv 3 \pmod{19}$ não tem solução, enquanto que a congruência $x^3 \equiv 11 \pmod{19}$ tem três soluções incongruentes módulo p.

5.38. Determine os valores de $a \in \{1, 2, \ldots, 12\}$ de tal modo que, para $b \in \{2, 5, 6\}$, a congruência $ax^4 \equiv b \pmod{13}$ tem solução.

5.39. Determine os valores de $a \in \{1, 2, \ldots, p - 1\}$ tais que, para $p \in \{7, 11, 13\}$, a congruência $x^4 \equiv a \pmod{p}$ tem solução.

5.40. Seja p um primo ímpar congruente com 2 módulo 3. Mostre que a congruência $x^3 \equiv a \pmod{p}$ tem solução para todo o a não divisível por p.

5.41. Considere a congruência $x^3 \equiv a \pmod{p}$, em que p é um primo maior ou igual a 5 e $(a,p) = 1$. Mostre que:

a) se $p \equiv 1 \pmod 6$ então a congruência não tem solução ou tem 3 soluções módulo p;

b) se $p \equiv 5 \pmod 6$ então a congruência tem uma única solução módulo p.

5.42. Seja p um número primo que não divide a nem n. Mostre que, se $k \in \mathbb{N}$ a congruência $x^n \equiv a \pmod{p}$ tem solução se e só se a congruência $x^n \equiv a \pmod{p^k}$ tiver solução.

5.43. Seja p um primo ímpar. Mostre que, a congruência $x^4 \equiv -1 \pmod{p}$ tem solução se e só se p é da forma $8k+1$.

5.44. Prove que, existe uma infinidade de primos da forma $8k+1$. **Obs.:** Assuma que $p_1, p_2, \ldots, p_n$ são primos desta forma e mostre que, $Q = (p_1 p_2 \cdots p_n)^4 + 1$ é divisível por um primo ímpar diferente de $p_1, p_2, \ldots, p_n$, que pelo exercício anterior, é necessariamente da forma $8k+1$.

5.45. Para que valores de b a congruência $9^x \equiv b \pmod{13}$ tem solução?

5.46. Mostre que, se $n \in \mathbb{N}$ e $p \in \mathbb{P}$ então a congruência $x^{p-1} - 1 \equiv 0 \pmod{p^n}$ tem $p-1$ soluções módulo p^n.

5.47. Sejam t, n e a inteiros positivos, sendo n e a ímpares e $t > 2$. Mostre que a congruência $x^n \equiv a \pmod{2^t}$ tem uma e uma só solução (módulo 2^t).

5.48. Usando o facto de 2 ser uma raiz primitiva de 83 mostre que se $1 < n < 82$:

a) $ind_2\, n \notin \{0, 41\}$;

b) $\Big(ind_2\,(-n^2), 82\Big) = 1$;

c) $-n^2$ é uma raiz primitiva de 83.

5.49. Seja a tal que a congruência $x^2 \equiv a \pmod{m}$ tem solução. Mostre que a congruência tem exactamente duas soluções se e só se m admite raiz primitiva.

5.50. Sejam $p, k, n \in \mathbb{N}$. Mostre que, se p é um número primo e n um divisor ímpar de $p-1$ então a congruência $x^n \equiv -1 \pmod{p^k}$ tem n soluções.

5.51. Seja p um primo da forma $2^{2^k}+1$ e seja g um inteiro menor que p. Mostre que g é uma raiz primitiva se e só se a equação $x^2 \equiv g \pmod{p}$ não tem solução.

5.52. Sejam $k \in \mathbb{N}$, $a \in \mathbb{Z}$, r uma raiz primitiva de um número primo p e $d = (p-1, k)$. Mostre que a congruência

$$x^k \equiv a \ (\bmod p)$$

tem solução se e só se existe $j \in \{1, 2, \ldots, \frac{p-1}{d}\}$ tal que $a \equiv r^{jd} \pmod{p}$.

5.53. Seja $n \in \mathbb{N}$. Mostre que existe $k \in \mathbb{N}$ tal que a congruência $x^2 \equiv 1 \pmod{k}$ tem mais do que n soluções.

5.54. Seja p um número primo que admite 10 como raiz primitiva. Pretende-se mostrar que a expansão de $\frac{1}{p}$ como dízima periódica tem período $p-1$.

Sejam $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}_0}$ sucessões de números reais tais que

$$\begin{cases} b_0 = 1 \\ 10b_{k-1} = pa_k + b_k & \text{se } k \geq 1 \\ 0 \leq b_k < p & \text{se } k \geq 1 \end{cases}$$

a) Mostre que $b_k \equiv 10^k \pmod{p}$.

b) Verifique que as sucessões $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}_0}$ estão univocamente determinadas.

c) Mostre que $\frac{1}{p} = 0, a_1 a_2 \cdots a_n \cdots$ e que

$$a_r = a_s \Leftrightarrow p-1 | r-s.$$

d) Use estes resultado para calcular a expansão decimal de $\frac{1}{17}$.

5.55. Seja $n = p_1^{n_1} \cdots p_k^{n_k}$ em que $p_1, \ldots, p_k$ são primos distintos, $n_1, \ldots, n_k$ e 2^3 não divide n. Seja $M = [\varphi(p_1^{n_1}), \ldots, \varphi(p_k^{n_k})]$. Mostre que:

a) se $a \in \mathbb{Z}$ é um inteiro primo com n então $ord_n\, a$ divide M;

b) existe um inteiro a^* que é raiz primitiva de $p_i^{n_i}$ para todo $i = 1, \dots k$;

c) $ord_n\, a^* = M$.

5.56. Seja $n = p_1^{n_1} \cdots p_k^{n_k}$ em que $p_1, \dots, p_k$ são primos distintos e $n_1, \dots, n_k$. Suponhamos que $p_1 = 2$ e $n_1 \geq 3$ e seja $N = [\frac{\varphi(2^{n_1})}{2}, \dots, \varphi(p_k^{n_k})]$. Mostre que:

a) se $a \in \mathbb{Z}$ é um inteiro primo com n então $ord_n\, a$ divide N;

b) existe um inteiro a^* que é raiz primitiva de $p_i^{n_i}$ para todo $i = 2, \dots k$ e cuja ordem módulo 2^{n_1} é igual a $\frac{\varphi(2^{n_1})}{2}$;

c) $ord_n\, a^* = N$.

6. Triângulos Pitagóricos

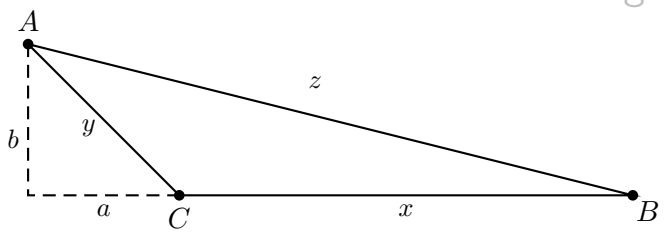
Neste capítulo vamos calcular todos os chamados "triângulos pitagóricos", que são os triângulos rectângulos cujas medidas dos lados são inteiras. Vamos também responder a algumas perguntas sobre tais triângulos.

6.1 Preliminares - O teorema de Pitágoras

Se tivermos um triângulo então a medida de qualquer dos lados é menor que a soma das medidas dos outros dois. Inversamente se tivermos 3 números inteiros positivos, x, y e z, e o maior deles for menor que a soma dos outros dois então existe um triângulo cujos lados medem x, y e z. Para ver isso comecemos por marcar um segmento de extremos A e B com medida do maior dos números (z, por exemplo). O vértice C terá de estar na circunferência centrada em A (ou B) de raio x e na circunferência centrada em B (ou A) de raio y. Como $z < x + y$ as duas circunferências intersectam-se em dois pontos. Escolhemos C um desses pontos.

Uma outra questão que se coloca é a de saber em que condições (sobre x, y e z) é que o triângulo obtido é rectângulo. Pelo teorema de Pitágoras se o triângulo for rectângulo então $x^2 + y^2 = z^2$. Vejamos que esta relação não se verifica se o triângulo não for rectângulo. Recorde-se que, num triângulo, ao maior lado opõe-se o maior ângulo!

Se tivermos um triângulo obtusângulo, como o representado no desenho abaixo,

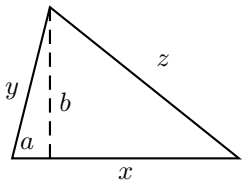


Aplicando o teorema de Pitágoras obtemos sucessivamente

$$(x+a)^2+b^2=z^2, \qquad x^2+2ax+a^2+b^2=z^2, \qquad x^2+y^2+2ax=z^2.$$

Em particular $z^2>x^2+y^2$.

Do mesmo modo se considerarmos um triângulo acutângulo



então $(x-a)^2+b^2=z^2$ ou seja (usando os mesmos argumentos que acima) $z^2=x^2+y^2-2ax$. Em particular $z^2<x^2+y^2$.

Conclusão: Um triângulo é rectângulo se e só se o quadrado da medida do lado maior for igual à soma dos quadrados das medidas dos outros dois lados.

6.2 Triângulos Pitagóricos

Neste capítulo pretende-se estudar os triângulos rectângulos cujas medidas dos lados são números inteiros. Estes triângulos dizem-se **pitagóricos**. Atendendo ao que foi dito acima, definir triângulos pitagóricos equivale a resolver a equação,

$$\mathbf{x}^2+\mathbf{y}^2=\mathbf{z}^2, \quad \mathbf{x},\mathbf{y},\mathbf{z}\in\mathbb{N}. \tag{6.1}$$

Note-se que se soubermos resolver a equação acima também sabemos resolver a equação

$$\mathbf{x}^2+\mathbf{y}^2=\mathbf{z}^2, \quad \mathbf{x},\mathbf{y},\mathbf{z}\in\mathbb{Z}.$$

Usaremos a notação $[x, y, z]$ para designar a classe dos triângulos pitagóricos cuja hipotenusa mede z e x e y são a medida dos catetos. Por abuso de notação diremos: o triângulo pitagórico $[x, y, z]$.

Conhecemos já alguns desses triângulos: $[3, 4, 5]$ e $[5, 12, 13]$, por exemplo.

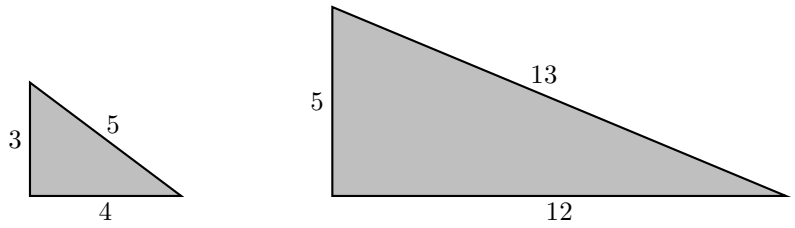


Figura 6.1: Os triângulos $[3, 4, 5]$ e $[5, 12, 13]$.

Vejamos algumas consequências (cujas demonstrações são deixadas como exercício) que podemos tirar do facto de um terno $[x, y, z]$ ser um triângulo pitagórico:

1. $[x, y, z] = [y, x, z]$;
2. se $k \in \mathbb{N}$, $[kx, ky, kz]$ é um triângulo pitagórico;
3. se $s|x$ e $s|y$ então $s|z$ e $[\frac{x}{s}, \frac{y}{s}, \frac{z}{s}]$ é um triângulo pitagórico;
4. $(x, y) = (y, z) = (x, z) = (x, y, z)$.

Um triângulo pitagórico $[x, y, z]$ tal que $(x, y) = 1$ diz-se **primitivo**. Note-se que todo o triângulo pitagórico $[x, y, z]$ é da forma $[k\,x_0, k\,y_0, k\,z_0]$ (ou $k\,[x_0, y_0, z_0]$) em que $k \in \mathbb{N}$ e $[x_0, y_0, z_0]$ é primitivo (basta considerar $k = (x, y)$).

Atendendo ao que foi dito, ficamos reduzidos ao estudo da equação

$$\mathbf{x}^2 + \mathbf{y}^2 = \mathbf{z}^2, \quad \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{N}, \quad (\mathbf{x}, \mathbf{y}) = 1. \tag{6.2}$$

6.3 Cálculo dos triângulos pitagóricos

Vamos agora encontrar todos os triângulos pitagóricos primitivos. Comecemos por um resultado auxiliar cuja demonstração é deixada como exercício.

Lema 6.1 *Se $k \in \mathbb{N}$ e $a_1, a_2, \ldots, a_k$ são inteiros positivos primos entre si cujo produto $a_1 a_2 \cdots a_k$ é um quadrado perfeito, então, para todo i, a_i é um quadrado perfeito.* ■

De seguida vamos enunciar um resultado que será usado continuamente.

Proposição 6.2 *Num triângulo pitagórico primitivo a medida da hipotenusa e de um dos catetos é ímpar enquanto a medida do outro cateto é par.*

Demonstração: Seja $[x, y, z]$ um triângulo pitagórico primitivo. Como $(x, y) = (y, z) = (x, z) = 1$ então apenas um dos inteiros x, y e z pode ser par.

Por outro lado, se x e y fossem ambos ímpares então z seria par e portanto

$$z^2 \equiv 0 \ (\mod 4) \quad \text{e} \quad x^2 \equiv y^2 \equiv 1 \ (\mod 4)$$

o que contradiz a igualdade $x^2 + y^2 = z^2$.

Deste modo x é par e y é ímpar ou y é par e x é ímpar. Em qualquer dos casos z tem de ser ímpar. ■

Chegamos agora ao resultado mais importante deste capítulo.

Teorema 6.3 *Sejam $x, y, z \in \mathbb{N}$ tais que $(x, y) = 1$. Então $[x, y, z]$ é um triângulo pitagórico primitivo se e só se existirem $m, n \in \mathbb{N}$ tais que:*

$$\begin{cases} x = 2mn \\ y = m^2 - n^2 \\ z = m^2 + n^2 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\mod 2) \end{cases} \quad \textbf{ou} \quad \begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\mod 2). \end{cases}$$

Demonstração: Note-se que a condição $m+n \equiv 1 \pmod 2$ diz apenas que m e n têm paridades diferentes.

$\Longleftarrow$

Sejam $m, n \in \mathbb{N}$ nas condições definidas e sejam $x = 2mn$, $y = m^2 - n^2$ e $z = m^2 + n^2$ (o outro caso é similar). Então

$$x^2 + y^2 = 4m^2n^2 + m^4 + n^4 - 2m^2n^2 = m^4 + n^4 + 2m^2n^2 = (m^2 + n^2)^2 = z^2.$$

Vejamos que o triângulo $[2mn, m^2-n^2, m^2+n^2]$ é primitivo. Para isso basta mostrar que $(m^2 - n^2, m^2 + n^2) = 1$. Suponhamos que não e seja $p \in \mathbb{P}$ tal que $p \mid m^2 - n^2$ e $p \mid m^2 - n^2$. Somando e subtraindo obtemos $p \mid 2m^2$ e $p \mid 2n^2$. Como p é primo ímpar (porquê?) então $p \mid m$ e $p \mid n$, o que é absurdo pois $(m, n) = 1$.

$\Longrightarrow$

Seja $[x, y, z]$ um triângulo pitagórico primitivo.

- Usando a proposição anterior podemos supor que x é par e que y e z são ímpares (o outro caso é tratado de maneira similar).

- Da igualdade $x^2+y^2 = z^2$ obtemos $x^2 = (z+y)(z-y)$, ou seja, $\left(\frac{x}{2}\right)^2 = (\frac{z+y}{2})(\frac{z-y}{2})$ (note-se que x, $z + y$ e $z - y$ são números pares). Com a intenção de aplicar o Lema 6.1 vamos mostrar que $(\frac{z+y}{2}, \frac{z-y}{2}) = 1$. Seja $d = (\frac{z+y}{2}, \frac{z-y}{2})$. Assim

$$\begin{cases} d \text{ divide } \frac{z+y}{2} \\ \\ d \text{ divide } \frac{z-y}{2} \end{cases} \quad \text{e portanto} \quad \begin{cases} d \text{ divide } \frac{z+y}{2} + \frac{z-y}{2} = z \\ \\ d \text{ divide } \frac{z+y}{2} - \frac{z+y}{2} = y \end{cases}$$

  Uma vez que $(z, y) = 1$ concluímos que $d = 1$.

- Usando o Lema 6.1, existem $m, n \in \mathbb{N}$ tais que $\frac{z+y}{2} = m^2$ e $\frac{z-y}{2} = n^2$. Assim

$$\begin{cases} x = 2mn \\ y = m^2 - n^2 & \text{subtraindo as duas igualdades acima} \\ z = m^2 + n^2 & \text{somando as duas igualdades acima.} \end{cases}$$

  Para concluir basta notar que: $m > n$ pois y é positivo; $m + n \equiv 1 \pmod 2$ pois z é ímpar; $(m, n) = 1$ pois $(x, y) = 1$. ∎

Como consequência obtemos o seguinte resultado.

Corolário 6.4 *Sejam $x, y, z \in \mathbb{N}$. Então $[x, y, z]$ é um triângulo pitagórico se e só se existirem $k, m, n \in \mathbb{N}$ tais que:*

$$\begin{cases} x = 2mnk \\ y = (m^2 - n^2)k \\ z = (m^2 + n^2)k \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\mod 2) \end{cases} \quad \textbf{ou} \quad \begin{cases} x = (m^2 - n^2)k \\ y = 2mnk \\ z = (m^2 + n^2)k \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\mod 2). \end{cases}$$

■

Nota 6.5 *O inteiro k que aparece no corolário anterior é o máximo divisor comum entre as medidas de dois quaisquer dos lados do triângulo pitagórico. Por outro lado, se k é ímpar então a medida da hipotenusa e de um dos catetos é ímpar e a medida do outro cateto é par. Note-se ainda que, $m^2 + n^2 \equiv 1 \pmod 4$ e que m, n, $m+n$ e $m-n$ são primos entre si.*

Do corolário anterior podemos concluir o seguinte.

Proposição 6.6 *Num triângulo pitagórico:*

a) *a medida de um dos catetos é múltipla de 4;*

b) *a medida de um dos catetos é múltipla de 3;*

c) *a medida de um dos lados é múltipla de 5.*

Demonstração: Usemos a caracterização dos triângulos pitagóricos dada pelo corolário anterior.

a) Como m ou n é par, concluímos que $2kmn$ é múltiplo de 4.

b) O resultado é trivial se m ou n for múltiplo de 3. Se m e n não forem múltiplos de 3 então $m^2 \equiv n^2 \equiv 1 \pmod 3$ e portanto $k(m^2 - n^2)$ é múltiplo de 3.

c) O resultado é trivial se m ou n for múltiplo de 5.

Note-se que, se $a \in \mathbb{Z}$ então

$$a^2 \equiv \begin{cases} 1 \ (\mod 3), & \text{se } a \equiv 1 \ (\mod 5) \\ 4 \ (\mod 3), & \text{se } a \equiv 2 \ (\mod 5) \\ 4 \ (\mod 3), & \text{se } a \equiv 3 \ (\mod 5) \\ 1 \ (\mod 3), & \text{se } a \equiv 4 \ (\mod 5) \end{cases}$$

Deste modo, se m e n não são múltiplos de 5 então m^2 e n^2 são congruentes módulo 5 com 1 ou com 4. Assim $m^2 - n^2$ ou $m^2 + n^2$ é congruente com 0 módulo 5. Em particular 5 divide $k(m^2 - n^2)$ ou $k(m^2 + n^2)$. ■

Exemplos 6.7

Vejamos dois exemplos:

1. Vamos calcular todos os triângulos pitagóricos da forma $[x, y, x + 1]$.

   Como $(x, x + 1) = 1$ os triângulos têm de ser primitivos. Em particular, $x + 1$ é ímpar (pois é a medida da hipotenusa) e portanto x é par e y é ímpar.

   Assim, existem $m, n \in \mathbb{N}$ tais que

$$\begin{cases} x = 2mn \\ y = m^2 - n^2 \\ x + 1 = m^2 + n^2 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\mod 2) \end{cases}$$

ou seja

$$\begin{cases} x = 2mn \\ y = m^2 - n^2 \\ m^2 + n^2 = 2mn + 1 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\text{ mod } 2). \end{cases}$$

Obtemos assim, sucessivamente

$$\begin{cases} x = 2mn \\ y = m^2 - n^2 \\ (m-n)^2 = 1 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\text{ mod } 2) \end{cases} \quad \begin{cases} x = 2n(n+1) \\ y = 2n + 1 \\ m = n + 1 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\text{ mod } 2) \end{cases} \quad \begin{cases} x = 2n(n+1) \\ y = 2n + 1 \\ n \in \mathbb{N}. \end{cases}$$

Como exemplos temos os triângulos: $[3, 4, 5]$, $[5, 12, 13]$, $[7, 24, 25]$ e $[9, 40, 41]$.

2. Vamos calcular todos os triângulos pitagóricos da forma $[x, y, x + 3]$.

   Como $(x, x + 3) = (x, 3) \in \{1, 3\}$ então usando a Nota 6.5 a hipotenusa é ímpar e portanto x é par. Deste modo existem $m, n \in \mathbb{N}$ tais que

$$\begin{cases} x = 2mn \\ y = m^2 - n^2 \\ x + 3 = m^2 + n^2 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\text{ mod } 2) \end{cases} \quad \textbf{ou} \quad \begin{cases} x = 6mn \\ y = 3(m^2 - n^2) \\ x + 3 = 3(m^2 + n^2) \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\text{ mod } 2). \end{cases}$$

   Do primeiro sistema obtemos $(m - n)^2 = 3$ que é uma condição impossível. Do segundo sistema obtemos $m = n + 1$.

Deste modo as soluções deste problema podem ser obtidas multiplicando por 3 as medidas dos triângulos que são solução do problema anterior.

3. Vamos calcular todos os triângulos pitagóricos cuja medida da hipotenusa seja 100. Seja $[x, y, 100]$ um tal triângulo. Podemos supor, utilizando o Corolário 6.4, que existem $k, m, n \in \mathbb{N}$ tais que:

$$\begin{cases} x = 2mnk \\ y = (m^2 - n^2)k \\ 100 = (m^2 + n^2)k \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\text{ mod } 2). \end{cases}$$

Uma vez que $m^2 + n^2$ é ímpar e $100 = k(m^2 + n^2)$, k tem de ser igual a 4, 20 ou 100. Obtemos assim os seguintes 3 sistemas:

$$\begin{cases} x = 8mn \\ y = 4(m^2 - n^2) \\ 25 = m^2 + n^2 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\text{ mod } 2) \end{cases} \quad \begin{cases} x = 40mn \\ y = 20(m^2 - n^2) \\ 5 = m^2 + n^2 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\text{ mod } 2) \end{cases} \quad \begin{cases} x = 200mn \\ y = 100(m^2 - n^2) \\ 1 = m^2 + n^2 \\ m > n \\ (m, n) = 1 \\ m + n \equiv 1 \ (\text{ mod } 2). \end{cases}$$

Olhando para a terceira equação, em cada um dos sistemas, é fácil calcular m e n: o terceiro é impossível (porque $m^2 + n^2 > 1$); o segundo admite apenas a solução $m = 2$, $n = 1$; o primeiro admite apenas a solução $m = 4$, $n = 3$.

Concluímos assim que existem dois triângulos nas condições pretendidas: $[80, 60, 100]$, $[96, 28, 100]$.

6.4 Outras equações pitagóricas

Vamos de seguida demonstrar a não existência de triângulos pitagóricos em determinadas condições.

Um caso que vamos analisar é o da existência de triângulos pitagóricos cujas medidas de alguns dos seus lados são quadrados perfeitos. Para encontramos um triângulo pitagórico em que a medida de um dos lados é um quadrado perfeito é muito simples se não exigirmos que o triângulo seja primitivo: escolhemos um triângulo pitagórico qualquer $[x, y, z]$ e multiplicamos a medida dos lados por x ou por y ou por z e obtemos os triângulos $[x^2, yx, zx]$, $[xy, y^2, zy]$ ou $[xz, yz, z^2]$.

E se exigirmos que o triângulo seja primitivo? Atendendo ao Teorema 6.3 a questão é equivalente a encontrar $m, n \in \mathbb{N}$ tais que $(m, n) = 1$, $m > n$, $m + n \equiv 1 \pmod 2$ e $2mn$ ou $m^2 - n^2$ ou $m^2 + n^2$ é um quadrado perfeito. Vejamos os 3 casos:

- Atendendo ao Teorema 6.3, $m^2 + n^2$ é um quadrado perfeito se e só se existirem $a, b \in \mathbb{N}$ tais que $(a, b) = 1$, $a > b$, $a + b \equiv 1 \pmod 2$, $m = \max\{2ab, a^2 - b^2\}$ e $n = \min\{2ab, a^2 - b^2\}$ (não esquecer que $m > n$). Temos assim um modo simples de encontrar triângulos pitagóricos primitivos em que a medida da hipotenusa é um quadrado perfeito. Por exemplo,
  - se $a = 2$ e $b = 1$ obtemos $m = 4$ e $n = 3$ e o triângulo $[24, 7, 25]$;
  - se $a = 5$ e $b = 2$ obtemos $m = 21$ e $n = 20$ e o triângulo $[840, 41, 841]$;
  - se $a = 11$ e $b = 9$ obtemos $m = 198$ e $n = 40$ e o triângulo $[15\,840, 37\,604, 40\,804]$.
- Note-se que, atendendo ao Lema 6.1, se $(m, n) = 1$ então $2mn$ é um quadrado perfeito se e só se existirem $a, b \in \mathbb{N}$ tais que $(a, b) = 1$ e m ou n é igual a $2a^2$ e o outro é igual a b^2. Não esquecer ainda que no final teremos de ter $m > n$ e $m + n \equiv \pmod 2$, o que implica b ímpar. Por exemplo,
  - se $a = 2$ e $b = 1$ obtemos $m = 8$ e $n = 1$ e o triângulo $[16, 63, 65]$;
  - se $a = 2$ e $b = 3$ obtemos $m = 9$ e $n = 8$ e o triângulo $[144, 17, 145]$;
  - se $a = 5$ e $b = 11$ obtemos $m = 121$ e $n = 50$ e o triângulo $[12\,100, 12\,141, 17\,141]$.

- Finalmente, atendendo novamente ao Lema 6.1, m^2-n^2 $(=(m+n)(m-n))$ é um quadrado perfeito se e só se existirem $a, b \in \mathbb{N}$ tais que $(a,b)=1$, a e b ímpares, $a>b$ e $m+n=a^2$ e $m-n=b^2$ ou seja $m=\frac{a^2+b^2}{2}$ e $n=\frac{a^2-b^2}{2}$ (note-se que, nestas condições m é ímpar e n é par!). Por exemplo,
  - se $a=3$ e $b=1$ obtemos $m=5$ e $n=4$ e o triângulo $[40,9,41]$;
  - se $a=5$ e $b=3$ obtemos $m=17$ e $n=8$ e o triângulo $[272,225,353]$;
  - se $a=7$ e $b=5$ obtemos $m=37$ e $n=12$ e o triângulo $[888,1\,225,1\,513]$.

De seguida vamos ver que não existem triângulos pitagóricos em que a medida de dois dos seus lados sejam quadrados perfeitos. Por maioria de razão não existem triângulos pitagóricos em que a medida dos três lados sejam quadrados perfeitos, ou seja

$$\nexists x,y,z \in \mathbb{N}: \quad x^4+y^4=z^4,$$

que é um caso particular $(n=4)$ do chamado teorema de Fermat (que só foi demonstrado por Andrew Wiles em 1994).

Comecemos com uma observação.

Lema 6.8 *Se existe um triângulo pitagórico em que am medida de dois dos seus lados é um quadrado perfeito então também existe um triângulo pitagórico primitivo nas mesmas condições.*

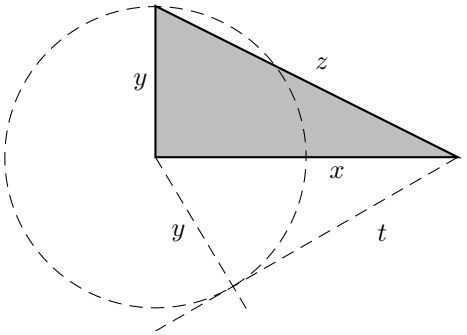
Demonstração: Seja $[a,b,c]$ um triângulo pitagórico em que dois dos números a, b e c são quadrados perfeitos. Se $d=(a,b)$ então $d=(b,c)=(a,c)$. Em particular d é o máximo divisor comum de dois quadrados perfeitos e portando d é um quadrado perfeito. Deste modo $[\frac{a}{d},\frac{b}{d},\frac{c}{d}]$ é um triângulo pitagórico primitivo em a medida de dois dois lados é um quadrado perfeito (recorde que se o quociente entre dois quadrados perfeitos se for um número inteiro é também um quadrado perfeito). ■

Teorema 6.9 (Teorema de Fermat) *Se a soma de dois quadrados perfeitos positivos é um quadrado perfeito, então a diferença desses dois quadrados perfeitos não é um quadrado perfeito. Ou seja, o sistema*

$$\begin{cases} x^2+y^2 &= z^2 \\ x^2-y^2 &= t^2 \end{cases}$$

não tem solução com $x,y,z,t \in \mathbb{N}$.

Demonstração: Geometricamente o enunciado diz que não existe um triângulo pitagórico tal que a medida de um dos catetos seja a hipotenusa de um outro triângulo pitagórico que tenha um cateto com a mesma medida de um dos catetos do triângulo original.



Vamos utilizar o chamado método da descida infinita. Seja $z \in \mathbb{N}$ o menor inteiro positivo tal que existem x, y e t tais que $x^2 + y^2 = z^2$, $x^2 - y^2 = t^2$.

Seja $d = (x, y)$. Note-se que $d = (x, y) = (x, z) = (y, z)$ pois $[x, y, z]$ é um triângulo pitagórico e que $d = (x, y) = (x, t) = (y, t)$ pois $[y, t, x]$ é um triângulo pitagórico. Em particular d divide x, y, z e t e portanto

$$\begin{cases} \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 &= \left(\frac{z}{d}\right)^2 \\ \left(\frac{x}{d}\right)^2 - \left(\frac{y}{d}\right)^2 &= \left(\frac{t}{d}\right)^2. \end{cases}$$

Pela minimalidade imposta sobre z concluímos que $d = 1$.

Recordemos agora a Proposição 6.2. Como estamos na presença de dois triângulos pitagóricos primitivos $[x, y, z]$ e $[y, t, x]$ podemos concluir que z e x são ímpares, pois são as medidas das hipotenusas. Daqui concluímos que y é par e, portanto, t é ímpar.

Voltando ao sistema original, obtemos sucessivamente,

$$\begin{cases} 2x^2 = z^2 + t^2 \\ \\ 2y^2 = z^2 - t^2 \end{cases} \quad \begin{cases} 4x^2 = (z+t)^2 + (z-t)^2 \\ \\ 2y^2 = (z-t)(z+t) \end{cases} \quad \begin{cases} x^2 = \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2 \\ \\ 2y^2 = (z-t)(z+t) \end{cases}$$

Como $\left(\frac{z+t}{2}, \frac{z-t}{2}\right) = 1$ (qualquer número que divida os dois números divide também a sua soma e a sua diferença que são z e t, dois números primos entre si) e utilizando o Teorema 6.3, podemos concluir que existem $m, n \in \mathbb{N}$ tais que

$$\begin{cases} \frac{z-t}{2} = 2mn \\ \frac{z+t}{2} = m^2 - n^2 \\ x = m^2 + n^2 \\ m > n \\ (m,n) = 1 \\ m + n \equiv 1 \ (\mod 2) \end{cases} \quad \textbf{ou} \quad \begin{cases} \frac{z+t}{2} = 2mn \\ \frac{z-t}{2} = m^2 - n^2 \\ x = m^2 + n^2 \\ m > n \\ (m,n) = 1 \\ m + n \equiv 1 \ (\mod 2). \end{cases}$$

Em qualquer dos casos e utilizando a igualdade $2y^2 = (z-t)(z+t)$ obtemos,

$$\left(\frac{y}{2}\right)^2 = \frac{1}{2}\left(\frac{z-t}{2}\right)\left(\frac{z+t}{2}\right) = mn(m^2-n^2) = mn(m-n)(m+n).$$

Como m, n, $m-n$ e $m+n$ são primos entre si (ver Nota 6.5) e o seu produto é um quadrado perfeito podemos concluir, usando o Lema 6.1, que são todos quadrados perfeitos, isto é,

$$\exists a,b,c,d \in \mathbb{N}: \quad m = a^2,\ n = b^2,\ m+n = c^2,\ m-n = d^2.$$

Em particular

$$\begin{cases} a^2 + b^2 &= c^2 \\ a^2 - b^2 &= d^2. \end{cases}$$

Por outro lado $c \leq c^2 = m + n < m^2 + n^2 = x < z$. Chegamos assim a uma contradição (a da minimalidade de z), que foi motivado pelo facto de termos suposto que o sistema original tinha solução. ■

Estamos agora em condições de demonstrar o resultado enunciado na página 121.

Teorema 6.10 *Não existe nenhum triângulo pitagórico em que as medidas de dois dos seus lados são quadrados perfeitos. Ou seja, as equações*

$$x^4 + y^2 = z^4, \quad x^4 + y^4 = z^2 \quad \textit{com } x,y,z \in \mathbb{N}$$

não têm solução.

Demonstração: Atendendo ao Lema 6.8 se existir um tal triângulo então também existe um triângulo primitivo nas mesmas condições.

Primeiro caso: Suponhamos então que existe um triângulo pitagórico primitivo da forma $[x^2, y, z^2]$. Pelo Teorema 6.3, existem $m, n \in \mathbb{N}$ tais que

$$\begin{cases} x^2 = 2mn \\ y = m^2 - n^2 \\ z^2 = m^2 + n^2 \\ m > n \\ (m,n) = 1 \\ m + n \equiv 1 \ (\mod 2) \end{cases} \quad \textbf{ou} \quad \begin{cases} x^2 = m^2 - n^2 \\ y = 2mn \\ z^2 = m^2 + n^2 \\ m > n \\ (m,n) = 1 \\ m + n \equiv 1 \ (\mod 2). \end{cases}$$

Obtemos então

$$\begin{cases} z^2 + x^2 = (m+n)^2 \\ z^2 - x^2 = (m-n)^2; \end{cases} \quad \textbf{ou} \quad \begin{cases} m^2 + n^2 = z^2 \\ m^2 + n^2 = x^2, \end{cases}$$

o que entra em contradição com o teorema anterior.

Segundo caso: Suponhamos então que existe um triângulo pitagórico primitivo da forma $[x^2, y^2, z]$. Vamos utilizar o método da descida infinita, a exemplo do que foi feito na demonstração do Teorema 6.9. Para isso vamos mostrar que conseguimos encontrar outro triângulo pitagórico nas mesmas condições mas em que a medida da hipotenusa é menor que z.

Vamos supor que x^2 é par e y^2 é ímpar (o outro caso é análogo). Deste modo existem $m, n \in \mathbb{N}$ de tal modo que:

$$\begin{cases} \frac{x^2}{2} = mn \\ y^2 = m^2 - n^2 = (m-n)(m+n) \\ z = m^2 + n^2 \\ m > n \\ (m,n) = 1 \\ m + n \equiv 1 \ (\mod 2) \end{cases}$$

Note-se que $\left(\frac{x}{2}\right)^2 = \frac{m}{2} \cdot n$, se m é par e $\left(\frac{x}{2}\right)^2 = m \cdot \frac{n}{2}$, se n é par. Do Lema 6.1 e do facto de y^2 e $\left(\frac{x}{2}\right)^2$ serem produtos de dois números primos entre si existem $a, b, c, d \in \mathbb{N}$ tais que $(a, b) = 1 = (c, d)$ e

$$\begin{cases} m = 2a^2 \\ n = b^2 \\ m - n = c^2 \\ m + n = d^2 \end{cases} \quad \text{ou} \quad \begin{cases} m = a^2 \\ n = 2b^2 \\ m - n = c^2 \\ m + n = d^2 \end{cases}$$

No primeiro caso obtemos

$$c^2 + d^2 \;=\; 2\,m \;=\; (2a)^2$$

Uma vez que $(c, d) = 1$, obtemos assim um triângulo pitagórico primitivo $[c, d, 2a]$ em que a medida da hipotenusa é par, contrariando a Proposição 6.2.

No segundo caso obtemos sucessivamente,

$$\begin{cases} d^2 + c^2 = 2a^2 \\ d^2 - c^2 = 4b^2 \end{cases} \quad \begin{cases} d^2 + c^2 = 2a^2 \\ \left(\frac{d-c}{2}\right)\left(\frac{d+c}{2}\right) = b^2 \end{cases}$$

Como $\frac{d-c}{2}$ e $\frac{d+c}{2}$ são primos entre si, existem $k, s \in \mathbb{N}$ tais que $\frac{d-c}{2} = k^2$ e $\frac{d+c}{2} = s^2$. Em particular, $s^2 + k^2 = d$ e $s^2 - k^2 = c$. Substituindo na primeira equação do último sistema temos $k^4 + s^4 = a^2$. Assim obtivemos uma outra solução da equação inicial. Para concluir a demonstração do teorema basta mostrar que $a < z$. Para isso basta notar que $a < a^2 = m \leq m^2 < m^2 + n^2 = z$. ■

Como aplicação do Teorema 6.9 podemos ver que a área de um triângulo pitagórico nunca é um quadrado perfeito. Com as notações usais, a área de um triângulo pitagórico é $k^2 mn(m-n)(m+n)$, que é um quadrado perfeito se e só se $mn(m-n)(m+n)$ o for. Pelo Lema 6.1 a área do triângulo referido é um quadrado perfeito se e só se os inteiros n, m, $m-n$ e $m+n$ forem quadrados perfeito, contrariando o Teorema 6.9.

Vejamos mais um exemplo, cuja resolução é essencialmente igual à resolução da equação $x^2 + y^2 = z^2$, com $x, y, z \in \mathbb{N}$.

Dado $r \in \mathbb{N}$ consideremos a equação

$$x^2 + r\,y^2 = z^2, \qquad \text{com } x, y, z \in \mathbb{N}.$$

Por exemplo, se $r = 2$ temos a seguinte representação geométrica do problema.

Começamos por desenhar um triângulo rectângulo cujos catetos são números inteiros (x e y) e a hipotenusa de medida real ($= \sqrt{x^2 + y^2}$). Desenhamos de seguida outro triângulo rectângulo no qual um dos catetos é a hipotenusa do triângulo anterior e a medida do outro cateto é y. Queremos saber, em que condições a medida da hipotenusa deste último triângulo é um número inteiro.

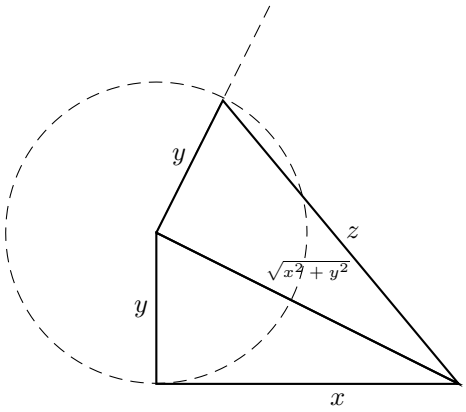


Figura 6.2: "Representação geométrica" da equação $x^2 + 2y^2 = z^2$, com $x, y, z \in \mathbb{N}$.

Para resolver esta equação podemos seguir mais ou menos os passos que foram dados para encontrar os triângulos pitagóricos. Comecemos por notar que, $(x, y) = (x, z) = (z, y)$ e que toda a solução é múltipla de uma solução da forma $[x, y, z]$ em que $(x, y) = 1$.

Nestas condições (isto é, se $(x, y) = 1$), note-se que:

- $(z - x, z + x) = 2$;
- a equação pode-se escrever na forma $y^2 = 2\left(\dfrac{z-x}{2}\right)\left(\dfrac{z+x}{2}\right)$;

Podemos assim concluir (porquê?) que existem m, n tais que

$$\begin{cases} \frac{z-x}{2} = 2m^2 \\ \\ \frac{z+x}{2} = n^2 \\ y = 2mn \\ (m,n) = 1 \end{cases} \quad \text{ou} \quad \begin{cases} \frac{z-x}{2} = m^2 \\ \\ \frac{z+x}{2} = 2n^2 \\ y = 2mn \\ (m,n) = 1. \end{cases}$$

Daqui podemos tirar o valor de x, y e z:

$$\begin{cases} x = n^2 - 2m^2 \\ z = n^2 + 2m^2 \\ y = 2mn \\ (m,n) = 1 \end{cases} \quad \text{ou} \quad \begin{cases} x = 2n^2 - m^2 \\ z = 2n^2 + m^2 \\ y = 2mn \\ (m,n) = 1. \end{cases}$$

Existem alguns pormenores a ter em conta!

De maneira análoga podemos resolver equações do tipo $x^2 + ry^2 = z^2$, com $r \in \mathbb{N}$. A interpretação geométrica deste problema é semelhante à do exemplo anterior.

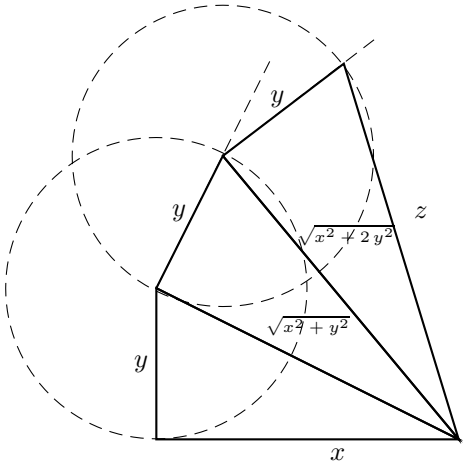


Figura 6.3: "Representação geométrica" da equação $x^2 + 3y^2 = z^2$, com $x, y, z \in \mathbb{N}$.

Começamos por escrever r na forma $r = k^2 s$ em que s é o produto dos números primos que aparecem na factorização de n com potência ímpar. Fazemos a mudança de

variável, $X = x$, $Y = ky$ e $Z = z$ e obtemos a equação $X^2 + sY^2 = Z^2$. Resolvemos esta equação utilizando um processo análogo ao do exemplo anterior ($s = 2$). As soluções da equação original são assim os ternos $(X, \frac{Y}{k}, Z)$ em que $X^2 + sY^2 = Z^2$ e Y é múltiplo de k.

Note-se que, se $x^2 + ry^2 = z^2$ e $d = (x, z)$, então d^2 divide ry^2 mas d não divide necessariamente y. Por exemplo, se $r = 12$, $6^2 + 12 \times 3^2 = 12^2$ e $(6, 12) = 6$ e $(6, 3) = 3$.

6.5 Exercícios

6.1. Mostre que a área de um triângulo pitagórico é múltipla de 6.

6.2. Mostre que não existem triângulos pitagóricos isósceles.

6.3. Mostre que não existem triângulos pitagóricos primitivos em que a medida de um dos lados é congruente com 2 módulo 4.

6.4. Mostre que, se $n \geq 3$ existe um triângulo pitagórico em que um dos lados mede n.

6.5. Mostre que, se $[x, y, z]$ é um triângulo pitagórico e x é um número primo, então y e z são inteiros consecutivos. O que pode dizer se $x = pq$ em que p e q são primos distintos?

6.6. Mostre, apenas a partir da definição de triângulo pitagórico que os únicos triângulos pitagóricos cujas medidas dos lados estão em progressão aritmética são os da forma $[3k, 4k, 5k]$.

6.7. Mostre que, se $[x, y, z]$ é um triângulo pitagórico e 4 divide z então 4 divide x e y. Que inteiros podem substituir o 4 na afirmação anterior?

6.8. Encontre todos os triângulos pitagóricos $[x, y, z]$ tais que (recorde que $m^2 + n^2 \equiv 1 \pmod 4$):

a) $z \in \{30, 65, 120, 481, 377, 1885\}$;

b) um dos lados mede 18;

c) um dos lados mede 60;

d) um dos lados mede 15;

e) $z = 77$ e x ou y é um quadrado perfeito;

f) $x = 9^2$ e $(x, y) = 1$;

g) $40 \leq z \leq 50$ e $[x, y, z]$ primitivo;

h) $x = 187$ e y é um quadrado perfeito;

i) $y + x = 64$.

6.9. Encontre todos os triângulos pitagóricos $[x, y, z]$ tais que

a) $z = 2^2 \times 5 \times 17$ e 17 não divide x;

b) $(x, y) = 7$ e $[x, y] = 84$;

c) $(x, y) = 10$ e $[x, y] = 2\,000$;

d) $(x, y) = 1$ e $5(x + y) = 7z$;

e) $(x, y) = 7$ e $y = 7(z - x)$.

6.10. Dê exemplos de triângulos pitagóricos (x, y, z) tais que:

a) $y = 2^3 \times 7^4$;

b) $x + y \geq 1000001$ e $(x, y) = 5$;

c) $y = x + 16$ e $x > 50$;

d) $(x, y) = 7$ e existe $a \in \mathbb{N}$ tal que $x = 5a^2$;

e) $x + y > 2005$ e $(x, y) = 1$;

f) $x - y > 2005$ e $(x, y) = 1$.

6.11. Calcule todos os triângulos pitagóricos cujo perímetro é 1716.

6.12. Verifique se existem triângulos pitagóricos primitivos cuja hipotenusa é divisível por 7.

6.13. Calcule todos os triângulos pitagóricos cujas medidas do perímetro e da área sejam iguais.

6.14. Calcule todos os triângulos pitagóricos cuja medida do perímetro seja igual a três vezes a medida da área.

6.15. Encontre todos os triângulos pitagóricos primitivos cuja medida da hipotenusa é um quadrado perfeito.

6.16. Verifique se há uma infinidade de triângulos pitagóricos primitivos cuja área é igual ao produto do perímetro pelo quadrado de algum inteiro.

6.17. Encontre um triângulo pitagórico primitivo em que a diferença das medidas dos catetos é um quadrado perfeito maior que 1.

6.18. Mostre que, se $[x, y, z]$ é um triângulo pitagórico então $x^n + y^n \neq z^n$ para $n \geq 3$.

6.19. Resolva a equação $81x^2 + 4y^4 = z^4$, com $x, y, z \in \mathbb{N}$ e $(x, y) = (x, z) = (y, z) = 1$.

6.20. Encontre $x, y, z \in \mathbb{Z}$ tais que

$$4x^4 + 9y^2 = z^2, \text{ e } x \geq 5000.$$

6.21. Encontre $x, y \in \mathbb{Q}^+$ tais que $x^2 + y^2 = 1$ e $x < \frac{1}{100}$.

6.22. Quais os pontos de coordenadas **racionais** que pertencem ao círculo de equação $x^2 + y^2 = 1$?

6.23. Mostre que as seguintes equações, com $x, y \in \mathbb{N}$, não têm solução

a) $y^2 = x^4 + 1$;

b) $x^4 - 2y^2 = 1$.

6.24. Mostre, usando o método da descida infinita que a equação $7x^3 + y^3 = 49z^3$, com $x, y, z \in \mathbb{N}$ não tem solução.

7. Fracções contínuas

7.1 Preliminares

Um expressão do tipo

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}$$

diz-se uma **fracção contínua**. A fim de garantirmos que nenhum dos denominadores se anule vamos considerar que $a_0 \in \mathbb{R}$ e $a_1, \ldots, a_n \in \mathbb{R}^+$.

Denotaremos esta expressão por $[a_0, a_1, \ldots, a_n]$.

Mais precisamente,

$$\begin{array}{lcll} [a_0] & = & a_0 & \\ [a_0, a_1] & = & a_0 + \frac{1}{a_1} & \\ [a_0, a_1, \ldots, a_n] & = & [a_0, [a_1, \ldots, a_n]\,] & \text{para } n \geq 2. \end{array}$$

Se desenvolvermos a expressão $[a_0, a_1, \ldots, a_n]$ obtemos uma fracção cujos numerador e denominador podem ser encontrados usando a seguinte proposição:

Proposição 7.1 *Sejam $n \in \mathbb{N}$, $a_0 \in \mathbb{R}$ e $a_1, \ldots, a_n \in \mathbb{R}^+$.*

Para cada $k \leq n$, consideremos a fracção contínua $[a_0, a_1, \ldots, a_k]$ e as sucessões (finitas) $(p_k)_{k\leq n}$ e $(q_k)_{k\leq n}$ definidas por,

$$\begin{cases} p_0 = a_0 \\ q_0 = 1 \end{cases} \quad \begin{cases} p_1 = a_0a_1 + 1 \\ q_1 = a_1 \end{cases} \quad \ldots \quad \begin{cases} p_i = a_ip_{i-1} + p_{i-2} \\ q_i = a_iq_{i-1} + q_{i-2}, \quad \textit{se } i \geq 2. \end{cases}$$

Então, para todo $k \leq n$, $[a_0, a_1, \ldots, a_k] = \dfrac{p_k}{q_k}$.

Demonstração: A demonstração pode ser feita por indução sobre k. Vejamos, abreviadamente, o passo de indução.

$$\begin{aligned}
[a_0, a_1, \ldots, a_k, a_{k+1}] &= [a_0, a_1, \ldots, [a_k, a_{k+1}]\,] \\
&= \frac{[a_k, a_{k+1}]p_{k-1} + p_{k-2}}{[a_k, a_{k+1}]q_{k-1} + q_{k-2}} \quad \text{por hipótese de indução} \\
&= \frac{\left(a_k + \frac{1}{a_{k+1}}\right)p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right)p_{k-1} + p_{k-2}} \\
&= \frac{a_kp_{k-1} + p_{k-2} + \frac{p_{k-1}}{a_{k+1}}}{a_kq_{k-1} + q_{k-2} + \frac{q_{k-1}}{a_{k+1}}} \\
&= \frac{p_k + \frac{p_{k-1}}{a_{k+1}}}{q_k + \frac{q_{k-1}}{a_{k+1}}} \quad \text{por definição de } p_k \text{ e } q_k \\
&= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} \\
&= \frac{p_{k+1}}{q_{k+1}} \quad \text{por definição de } p_{k+1} \text{ e } q_{k+1}.
\end{aligned}$$

■

Definição 7.2 *Com as notações acima, chamamos* **convergentes** *às fracções $\dfrac{p_k}{q_k}$, com $k \geq 0$.*

Vejamos uma relação existente entre os convergentes. Começamos com alguns resultados auxiliares.

Lema 7.3 *Se $x, y, z \in \mathbb{R}^+$ e $a \in \mathbb{R}$, então:*

a) $a < [a, x]$;

b) $[a, x] > [a, x, y]$;

c) *se $x < y$ então* $[a, x] > [a, y]$;

d) *se $x < y$ então* $[a, z, x] < [a, z, y]$.

Demonstração: A título de exemplo vamos fazer a demonstração da alínea b). Basta notar que

$$x < x + \frac{1}{y} \implies \frac{1}{x} > \frac{1}{x + \frac{1}{y}} \implies a + \frac{1}{x} > a + \frac{1}{x + \frac{1}{y}}.$$ ■

Lema 7.4 *Se $n \in \mathbb{N}_0$, $a_0 \in \mathbb{R}$ e $a_1, \ldots, a_n, z \in \mathbb{R}^+$ então:*

$$\begin{cases} [a_0, \ldots, a_n] < [a_0, \ldots, a_n, z] & \text{se } n \text{ é par;} \\ [a_0, \ldots, a_n] > [a_0, \ldots, a_n, z] & \text{se } n \text{ é ímpar.} \end{cases}$$

Demonstração: Vamos fazer a demonstração apenas para o caso em que n é par, ou seja, da forma $2k$. O outro caso tem demonstração similar.

Se $k = 0$, basta usar o lema anterior.

Vejamos o passo de indução:

$$\begin{aligned} [a_0, \ldots, a_{2k}, a_{2k+1}, a_{2k+2}] &= [a_0, a_1, [a_2, \ldots, a_{2k}, a_{2k+1}, a_{2k+2}]\,] \\ &< [a_0, a_1, [a_2, \ldots, a_{2k}, a_{2k+1}, a_{2k+2}, z]\,] \\ &\quad \text{usando a hipótese de indução} \\ &\quad \text{e a alínea } d) \text{ do lema anterior.} \end{aligned}$$ ■

Corolário 7.5 *Seja $a_0 \in \mathbb{Z}$ e $(a_n)_{n\in\mathbb{N}}$ uma sucessão de números reais positivos e, para cada $n \in \mathbb{N}_0$, $\gamma_n = [a_0, a_1, \ldots, a_n] = \dfrac{p_n}{q_n}$. Nestas condições:*

a) *a sucessão $(\gamma_{2n})_{n\in\mathbb{N}_0}$ é uma sucessão crescente;*

b) *a sucessão $(\gamma_{2n+1})_{n\in\mathbb{N}_0}$ é uma sucessão decrescente;*

c) *se $n, m \in \mathbb{N}_0$ então $\gamma_{2n} < \gamma_{2m+1}$;*

d) *se $n \in \mathbb{N}_0$, $p_n q_{n+1} - q_n p_{n+1} = (-1)^{n+1}$;*

e) *se $n \in \mathbb{N}_0$, $\gamma_n - \gamma_{n+1} = \dfrac{(-1)^{n+1}}{q_n q_{n+1}}$;*

f) *p_n e q_n são inteiros primos entre si.*

Demonstração: Atendendo a que, se $i < j$, $\gamma_j = [a_0, a_1, \ldots, a_i, [a_{i+1}, \ldots, a_j]\,]$, as três primeiras alíneas deste corolário são uma consequência imediata do lema anterior.

Para a demonstração de *d)* vamos usar indução sobre n. O passo de indução pode ser feito do seguinte modo:

$$\begin{aligned} p_{n+1}q_{n+2} - q_{n+1}p_{n+2} &= p_{n+1}[a_{n+2}q_{n+1} + q_n] - q_{n+1}[a_{n+2}p_{n+1} + p_n] \\ &= p_{n+1}q_n - q_{n+1}p_n \\ &= (-1)[p_n q_{n+1} - q_n p_{n+1}] \\ &= (-1)^{n+2}. \end{aligned}$$

Dividindo ambos os membros da igualdade *d)* por $q_n q_{n+1}$ obtemos a igualdade *e)*.

Nas condições de *f)*, a Proposição 7.1 garante-nos que p_n e q_n são números inteiros. Por outro lado, se p é um número que divide p_n e q_n, então p divide $p_{n-1}q_n - q_{n-1}p_n$. Pela alínea *d)* este último número é ± 1 e portanto $p = 1$. Concluímos assim que p_n e q_n são primos entre si. ■

Nota 7.6 *A partir deste momento:*

- *consideraremos apenas fracções contínuas da forma $[a_0, a_1, \ldots, a_n]$ em que $a_0 \in \mathbb{N}$, $a_1, \ldots, a_{n-1} \in \mathbb{N}$ e $a_n \in [1, +\infty[$;*

- *se* $n \geq 1$ *e* $a_n = 1$ *então* $[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_{n-1} + 1]$. *Deste modo chegamos sempre a uma fracção do tipo* $[a_0]$ *ou do tipo* $[a_0, a_1, \ldots, a_k]$ *em que* $a_k > 1$*;*

Nestas condições, como $\alpha = a_0 + \frac{1}{[a_1, a_1, \ldots, a_n]}$ *e* $[a_1, a_1, \ldots, a_n] > 1$, a_0 *é a característica de* α. *De modo análogo* a_1 *é a característica de* $[a_1, a_1, \ldots, a_n]$ *(ou seja de* $\frac{1}{\alpha - a_0}$*), etc..*

Como consequência obtemos:

Corolário 7.7 *Se* $n \in \mathbb{N}$, $a_1, b_1 \ldots, a_{n-1}, b_{n-1} \in \mathbb{N}$ *e* $a_n, b_n \in]1, +\infty[$ *então:*

$$[a_0, a_1, \ldots, a_n] = [b_0, b_1, \ldots, b_n] \quad \Leftrightarrow \quad \forall i \in \{0, 1, \ldots, n\} \quad a_i = b_i. \qquad \blacksquare$$

Definição 7.8 *Uma fracção* $[a_0, a_1, \ldots, a_n]$ *diz-se* **simples** *se* $a_0 \in \mathbb{Z}$ *e* $a_1, \ldots, a_n \in \mathbb{N}$.

Note-se que, toda a fracção simples representa um número racional.

Nas próximas subsecções vamos mostrar que:

- um número é racional se e só se puder ser escrito como uma fracção contínua simples;
- toda a sucessão do tipo $([a_0, a_1, \ldots, a_n])_{n \in \mathbb{N}}$ é convergente para um número irracional;
- todo o número irracional é o limite de uma única sucessão do tipo $([a_0, a_1, \ldots, a_n])_{n \in \mathbb{N}}$.

7.2 Expansão de números racionais

Vimos acima que toda a fracção simples representa um número racional. Vamos agora mostrar o inverso. Começamos com dois exemplos.

1. Vamos desenvolver $\frac{12}{7}$ como fracção contínua. Atendendo ao que foi dito

$$\frac{12}{7} = 1 + \frac{5}{7} = 1 + \frac{1}{\frac{7}{5}} = 1 + \frac{1}{1 + \frac{2}{5}} = 1 + \frac{1}{1 + \frac{1}{\frac{5}{2}}} = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}.$$

Assim $\frac{12}{7} = [1, 1, 2, 2]$.

Em geral é mais prático (e menos sujeito a erros) fazer o desenvolvimento por "passos":

$$\begin{aligned} \frac{12}{7} &= 1 + \frac{5}{7} = 1 + \frac{1}{\frac{7}{5}} = [1, \frac{7}{5}]; \\ \frac{7}{5} &= 1 + \frac{2}{5} = 1 + \frac{1}{\frac{5}{2}} = [1, \frac{5}{2}]; \\ \frac{5}{2} &= 2 + \frac{1}{2} = [1, 2]. \end{aligned}$$

Daqui concluímos que

$$\frac{12}{7} = [1, \frac{7}{5}] = [1, 1, \frac{5}{2}] = [1, 1, 1, 2].$$

2. Vamos desenvolver $\frac{79}{28}$ como fracção contínua.

$\frac{79}{28} = 2 + \frac{23}{28} = 2 + \frac{1}{\frac{28}{23}} = [2, \frac{28}{23}]$; $\quad \frac{28}{23} = 1 + \frac{1}{\frac{5}{23}} = 1 + \frac{1}{\frac{23}{5}} = [1, \frac{23}{5}]$;

$\frac{23}{5} = 4 + \frac{3}{5} = 4 + \frac{1}{\frac{5}{3}} = [4, \frac{5}{3}]$; $\quad \frac{5}{3} = 1 + \frac{2}{3} = 1 + \frac{1}{\frac{3}{2}} = [1, \frac{3}{2}]$

$\frac{3}{2} = 1 + \frac{1}{2} = [1, 2]$.

Daqui concluímos que

$$\frac{79}{28} = [2, \frac{28}{23}] = [2, 1, \frac{23}{5}] = [2, 1, 4, \frac{5}{3}] = [2, 1, 4, 1, \frac{3}{2}] = [2, 1, 4, 1, 1, 2].$$

Note-se nestes exemplos que os denominadores das fracções que "aparecem" vão diminuindo. Isto acontece porque esses mesmos denominadores são o resto da divisão do numerador "anterior" pelo denominador "anterior". Deste modo "mais cedo ou mais tarde" obtemos uma fracção simples.

Proposição 7.9 *Um número é racional se e só se puder ser escrito como uma fracção racional simples.*

Demonstração: Resta-nos demonstrar que todo o número racional pode ser escrito como uma fracção simples. Começamos por considerar que os números racionais estão escrito sobre a forma $\frac{p}{q}$ em que $p \in \mathbb{Z}$ e $q \in \mathbb{N}$.

A demonstração vai ser feita por indução sobre o denominador.

Se $q = 1$ então $p = [p]$;

Hipótese de indução: Todo o número da forma $\frac{p}{b}$ em que $p \in \mathbb{N}$, $b \in \mathbb{N}$ com $b < q$ escreve-se como uma fracção contínua simples;

Tese de indução: Todo o número da forma $\frac{p}{q}$ em que $p \in \mathbb{N}$ escreve-se como uma fracção contínua simples.

Usando o algoritmo da divisão sejam $t, r \in \mathbb{N}$ tais que $p = qt + r$ e $0 \leq r < q$.

Se $r = 0$, $\frac{p}{q} = [t]$. Se $r > 0$ então,

$$\begin{aligned} \frac{p}{q} &= t + \frac{r}{q} \\ &= t + \frac{1}{\frac{q}{r}} \\ &= [t, \frac{q}{r}] \end{aligned}$$

Por hipótese de indução, $\frac{q}{r}$ escreve-se como uma fracção simples $[b_0, b_1, \cdots, b_k]$ em que $b_0 \in \mathbb{N}$ e $b_1, \ldots, b_k \in \mathbb{N}$. Como $q > r$, b_0 é positivo porque é a característica de $\frac{q}{r}$.

Assim $\frac{p}{q} = [t, \frac{q}{r}] = [t, b_0, b_1, \cdots, b_k]$. ■

Como aplicação resultado vamos de seguida "re-demonstrar" o Teorema 2.3.

Corolário 7.10 *Se $a \in \mathbb{Z}$ e $b \in \mathbb{N}$ são inteiros primos entre si então, para todo $c \in \mathbb{Z}$ a equação*

$$ax + by = c, \quad x, y \in \mathbb{Z}$$

tem solução.

Demonstração: Consideremos a fracção contínua simples $[a_0, \ldots, a_n]$ que representa $\frac{a}{b}$ e sejam $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ os convergentes desta fracção. Deste modo, $\frac{p_n}{q_n} = \frac{a}{b}$ e, portanto, como $(p_n, q_n) = 1 = (a, b)$ e $q_n, b > 0$ podemos concluir que $p_n = a$ e $q_n = b$.

Usando o Corolário 7.5 alínea d), $p_{n-1}b - q_{n-1}a = (-1)^n$. Multiplicando por $(-1)^n c$ obtemos

$$a\left[(-1)^{n+1} c\, q_{n-1}\right] + b\left[(-1)^n c\, p_{n-1}\right] = c.$$

■

7.3 Expansão de números irracionais

Já sabemos que os números irracionais não se podem escrever como fracção simples. De qualquer modo, veremos que se $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ e $n \in \mathbb{N}$, α pode sempre ser escrito na forma $[a_0, a_1, \ldots, a_{n-1}, \alpha_n]$ com $\alpha \in]1, +\infty[$. Comecemos com alguns exemplos.

Exemplos 7.11

1. $\alpha = \sqrt{2}$.

$$\begin{aligned}
\sqrt{2} &= 1 + (\sqrt{2} - 1), \quad \text{note-se que } [\sqrt{2}] = 1 \\
&= 1 + \frac{1}{\frac{1}{\sqrt{2}-1}}, \quad \text{note-se que } \tfrac{1}{\sqrt{2}-1} > 1 \\
&= 1 + \frac{1}{\sqrt{2}+1} = [1, \sqrt{2}+1].
\end{aligned}$$

Por outro lado,

$$\begin{aligned}
\sqrt{2}+1 &= 2 + (\sqrt{2} - 1), \quad \text{note-se que } [\sqrt{2}+1] = 2 \\
&= 2 + \frac{1}{\frac{1}{\sqrt{2}-1}}, \quad \text{note-se que } \tfrac{1}{\sqrt{2}-1} > 1 \\
&= 2 + \frac{1}{\sqrt{2}+1} = [1, 2, \sqrt{2}+1].
\end{aligned}$$

Daqui concluímos que $\sqrt{2} = [1, 2, 2, \ldots, 2, \sqrt{2}+1]$.

2. $\alpha = \sqrt{13}$. Utilizando um processo análogo ao do exemplo anterior,

$$\sqrt{13} = 3 + (\sqrt{13} - 3) = 3 + \frac{1}{\frac{1}{\sqrt{13}-3}} = 3 + \frac{1}{\frac{\sqrt{13}+3}{4}} = [3, \frac{\sqrt{13}+3}{4}];$$

$$\frac{\sqrt{13}+3}{4} = 1 + \frac{\sqrt{13}-1}{4} = 1 + \frac{1}{\frac{4}{\sqrt{13}-1}} = 1 + \frac{1}{\frac{\sqrt{13}+1}{3}} = [1, \frac{\sqrt{13}+1}{3}].$$

Obtemos assim $\sqrt{13} = [3, 1, \frac{\sqrt{13}+1}{3}]$. Continuando este processo obtemos sucessivamente,

$$\begin{array}{lll}
\frac{\sqrt{13}+1}{3} = [1, \frac{\sqrt{13}+2}{3}] & \text{e portanto} & \sqrt{13} = [3, 1, 1, \frac{\sqrt{13}+2}{3}] \\
\frac{\sqrt{13}+2}{3} = [1, \frac{\sqrt{13}+1}{3}] & \text{e portanto} & \sqrt{13} = [3, 1, 1, 1, \frac{\sqrt{13}+1}{3}] \\
\frac{\sqrt{13}+1}{4} = [1, \sqrt{13}+3] & \text{e portanto} & \sqrt{13} = [3, 1, 1, 1, 1, \sqrt{13}+3] \\
\sqrt{13}+3 = [6, \frac{\sqrt{13}+3}{4}] & \text{e portanto} & \sqrt{13} = [3, 1, 1, 1, 1, 6, \frac{\sqrt{13}+3}{4}].
\end{array}$$

Entramos assim num ciclo, uma vez que $\frac{\sqrt{13}+3}{4}$ já tinha aparecido. Assim,

$$\begin{aligned}
\sqrt{13} &= [3, 1, 1, 1, 1, 6, \frac{\sqrt{13}+3}{4}] \\
&= [3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, \frac{\sqrt{13}+3}{4}] \\
&= [3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, \frac{\sqrt{13}+3}{4}] \\
&\vdots \quad \text{etc..}
\end{aligned}$$

Vejamos o caso geral.

Teorema 7.12 *Se $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ e $n \in \mathbb{N}$ então α pode ser escrito (de maneira única) na forma $[a_0, a_i, \ldots, a_{n-1}, \alpha_n]$ em que $a_0 \in \mathbb{N}$, $a_1, \ldots, a_{n-1} \in \mathbb{N}$ e $\alpha_n \in]1, +\infty[$.*

Demonstração: Vamos fazer a demonstração por indução sobre n. Deixo aqui o passo de indução.

Hipótese de indução:

Todo o número irracional pode ser escrito na forma $[a_0, a_1, \ldots, a_{n-2}, \alpha_{n-1}]$, com $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_{n-2} \in \mathbb{N}$ e $\alpha_{n-1} \in]1, +\infty[$.

Tese de indução:

Todo o número irracional pode ser escrito na forma $[a_0, a_1, \ldots, a_{n-1}, \alpha_n]$, com $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_{n-1} \in \mathbb{N}$ e $\alpha_n \in]1, +\infty[$.

Se $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ então

$$\alpha = [\alpha] + (\alpha - [\alpha]) = [\alpha] + \frac{1}{\frac{1}{\alpha - [\alpha]}} = \left[[\alpha], \frac{1}{\alpha - [\alpha]} \right].$$

Por hipótese de indução existem $b_0 \in \mathbb{Z}$, $b_1, \ldots, b_{n-2} \in \mathbb{N}$ e $\beta_{n-1} \in]1, +\infty[$ tais que

$$\frac{1}{\alpha - [\alpha]} = [b_0, b_1, \ldots, b_{n-2}, \beta_{n-1}].$$

Note-se que $b_0 \in \mathbb{N}$ porque $\frac{1}{\alpha - [\alpha]} > 1$.

Daqui concluímos que $\alpha = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$ em que $a_i = b_{i-1}$ para $i \geq 1$ e $\alpha_n = \beta_{n-1}$.

Deixo como exercício demonstrar a "unicidade". ■

Observação: Como consequência deste resultado, dado $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, encontramos duas sucessões

$$(a_n)_{n \in \mathbb{N}_0} \quad \text{e} \quad (\alpha_n)_{n \in \mathbb{N}}$$

tais que, se $n \in \mathbb{N}$, $\alpha = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$.

Teorema 7.13 *Se $a_0 \in \mathbb{N}$ e $(a_n)_{n \in \mathbb{N}}$ é uma sucessão de números inteiros positivos então a sucessão $([a_0, a_1, \ldots, a_n])_{n \in \mathbb{N}}$ é convergente para um número irracional.*

Inversamente, todo o número irracional é o limite de uma sucessão de fracções simples.

Demonstração: Para a primeira parte, basta usar o Corolário 7.5 do seguinte modo:

- para cada $n \in \mathbb{N}$ seja $\gamma_n = [a_0, a_1, \ldots, a_n]$;
- pelas alíneas a), b) e c), as sucessões $(\gamma_{2n})_{n\in\mathbb{N}}$ e $(\gamma_{2n+1})_{n\in\mathbb{N}}$ são convergentes;
- pela alínea e), os dois limites acima referidos são iguais porque

$$\lim_{n\in\mathbb{N}}(\gamma_{2n} - \gamma_{2n+1}) = \lim_{n\in\mathbb{N}} \frac{(-1)^{2n+1}}{q_{2n}q_{2n+1}} = 0,$$

  uma vez que $q_k > k$, para todo o $k \in \mathbb{N}$ (ver Proposição 7.1).

Concluímos assim que a sucessão $([a_0, a_1, \ldots, a_n])_{n\in\mathbb{N}}$ é convergente.

Para a segunda parte do Teorema seja $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Como foi explicado acima consideramos duas sucessões

$$(a_n)_{n\in\mathbb{N}_0} \quad \text{e} \quad (\alpha_n)_{n\in\mathbb{N}}$$

tais que, se $n \in \mathbb{N}$, $\alpha = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$.

Pela primeira parte deste teorema, a sucessão $([a_0, \ldots, a_n])_{n\in\mathbb{N}}$ é convergente para um número γ.

Pelo Lema 7.4, se $n \in \mathbb{N}$,

$$[a_0, \ldots, a_{2n}] < [a_0, \ldots, a_{2n}, \alpha_{2n+1}] = \alpha = [a_0, \ldots, a_{2n+1}, \alpha_{2n+2}] < [a_0, \ldots, a_{2n+1}]\,.$$

Em particular,

$$[a_0, \ldots, a_{2n}] < \alpha < [a_0, \ldots, a_{2n+1}]\,.$$

Aplicando limites obtemos

$$\gamma = \lim_{n\in\mathbb{N}} [a_0, \ldots, a_{2n}] \leq \alpha \leq \lim_{n\in\mathbb{N}} [a_0, \ldots, a_{2n+1}] = \gamma.$$

Concluímos assim que $\alpha = \gamma = \lim_{n\in\mathbb{N}} [a_0, \ldots, a_n]$. ■

Notação: Se $\alpha = \lim_{n\in\mathbb{N}} [a_0, a_1, \ldots, a_n]$ escreveremos $\alpha = [a_0, a_1, \ldots, a_n, \ldots]$.

Chamaremos a esta expansão uma fracção **simples infinita**.

Por exemplo: $\sqrt{2} = [1, 2, 2, 2, \ldots]$, $\sqrt{13} = [3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, \ldots]$ e $\frac{1+\sqrt{5}}{2} = [1, 1, 1, \ldots]$.

Nota 7.14 *Com as notações atrás definidas o que é realmente importante reter é que* $\alpha_n = [\alpha_n] + \frac{1}{\alpha_{n+1}}$.

Exercício 7.15 *Mostre que, se* $\alpha = [a_0, a_1, \ldots, a_n, \ldots]$ *e* $a \in \mathbb{N}$ *então* $\alpha + a = [a_0 + a, a_1, \ldots, a_n, \ldots]$.

7.4 Fracções contínuas periódicas

Vimos nos Exemplos 7.11, que foi fácil encontrar a fracção simples infinita de $\sqrt{2}$ e $\sqrt{13}$ uma vez que as sucessões que definem essas fracções eram sucessões periódicas.

Definição 7.16 *Uma fracção simples infinita* $[a_0, a_1, \ldots, a_n, \ldots]$ *diz-se* **periódica** *se*

$$\exists k \in \mathbb{N}_0 \; \exists r \in \mathbb{N} \; \forall i \in \mathbb{N} \quad [i \geq k \Rightarrow a_i = a_{i+r}].$$

Se $k = 0$ *dizemos que a fracção é* **puramente periódica**.

Notação: *Nas condições desta definição* $a_{k+nr+j} = a_{k+j}$, *para* $n \in \mathbb{N}$ *e* $0 \leq j < r$. *Deste modo, a fracção* $[a_0, a_1, \ldots, a_n, \ldots]$ *fica determinada pelo conhecimento de* $a_0, \ldots, a_{k+r-1}$.

Escreveremos então $[a_0, a_1, \ldots, \dot{a}_k, \ldots, \dot{a}_{k+r-1}]$ *para representar a fracção.*

Chamaremos **período** da fracção ao menor r nas condições referidas.

Nota 7.17 *Com as notações usuais um número* α *expande-se como uma fracção contínua periódica se e só se existem* $k \in \mathbb{N}_0$ *e* $r \in \mathbb{N}$ *tais que* $\alpha_k = \alpha_{k+r}$.

Exemplos 7.18 *Usando a notação indicado,* $\sqrt{2} = [1, \dot{2}]$ *(período 1),* $\frac{1+\sqrt{5}}{2} = [\dot{1}]$ *(período 1) e* $\sqrt{13} = [3, \dot{1}, 1, 1, 1, \dot{6}]$ *(período 5).*

7.4.1 Caracterização das fracções periódicas e das fracções puramente periódicas

Pretende-se agora caracterizar quais os números reais que são representados por uma fracção periódica ou por uma fracção puramente periódica. É claro que esses números não podem ser racionais.

Vamos introduzir alguma notação.

Definição 7.19 *Dizemos que um número irracional α é* **quadrático** *se for um zero de um polinómio de grau dois de coeficientes inteiros. Ao outro zero desse polinómio chamamos* **conjugado** *de α e denotá-mo-lo por $\overline{\alpha}$. Dizemos que um número quadrático α é* **reduzido** *se $\alpha > 1$ e $-1 < \overline{\alpha} < 0$.*

O chamado número de *ouro* ($\frac{1+\sqrt{5}}{2}$) é um exemplo de um número quadrático reduzido.

Nota 7.20 *Vejamos algumas observações cujas demonstrações envolvem apenas cálculos elementares.*

- Usando a chamada formula resolvente das equações polinomiais do segundo grau podemos concluir que todo o número quadrático é da forma $\frac{A\pm\sqrt{D}}{C}$. Deste modo os números $\frac{A+\sqrt{D}}{C}$ e $\frac{A-\sqrt{D}}{C}$ são conjugados um do outro.
- Se α é um número quadrático e $n \in \mathbb{N}$ então α_n é também quadrático (basta usar a fórmula de recorrência referida na Nota 7.14 e

$$\overline{\alpha}_n = a_n + \frac{1}{\overline{\alpha}_{n+1}} \quad \text{e} \quad \overline{\alpha} = \frac{\overline{\alpha}_{n+1}p_n + p_{n-1}}{\overline{\alpha}_{n+1}q_n + q_{n-1}}.$$

- Se $d \in \mathbb{Q}$, $\sqrt{d} \notin \mathbb{Q}$, $d > 1$ e $\alpha = \sqrt{d}$ então α é um número quadrático não reduzido mas α_1 ($= \frac{1}{\sqrt{d}-[\sqrt{d}]}$) é reduzido.

Por opção vou apresentar primeiro todos os resultados desta secção deixando as demonstrações para o final.

Em todos esses resultado, α é um número irracional,

$$(a_n)_{n\in\mathbb{N}_0}\,, \quad (\alpha_n)_{n\in\mathbb{N}_0}\,, \quad (p_n)_{n\in\mathbb{N}_0} \quad \text{e} \quad (q_n)_{n\in\mathbb{N}_0}$$

são tais que $a_0 \in \mathbb{N}$ e, se $n \in \mathbb{N}$, $a_n \in \mathbb{N}$ e

$$\alpha = \alpha_0 = [a_0, a_1, \ldots, a_{n-1}, \alpha_n] \quad \text{e} \quad [a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

Lema 7.21 *Um número irracional α é quadrático se e só se puder ser escrito na forma $\dfrac{c+\sqrt{d}}{e}$ em que $c \in \mathbb{Z}$, $e \in \mathbb{Z}\setminus\{0\}$, $d \in \mathbb{N}$, $\sqrt{d} \notin \mathbb{N}$, $e|d-c^2$.*

Proposição 7.22 *Se $\alpha = \frac{c+\sqrt{d}}{e}$ é um número quadrático reduzido então*

$$0 < c < \sqrt{d} \quad e \quad \sqrt{d} - c < e < \sqrt{d} + c.$$

Em particular $0 < c < \sqrt{d}$ e $0 < e < 2\sqrt{d}$.

Lema 7.23 *Seja $\alpha = \frac{c_0+\sqrt{d}}{e_0}$ nas condições do lema anterior.*
Então para todo $n \in \mathbb{N}$ existem $c_n \in \mathbb{N}$, $e_n \in \mathbb{N}\setminus\{0\}$ tais que

$$\alpha_n = \frac{c_n + \sqrt{d}}{e_n}, \quad e_n | d - c_n^2.$$

Além disso, se existe $n \in \mathbb{N}$ tal que α_n é reduzido então α_{n+k} é também reduzido, para todo $k \in \mathbb{N}$.

Lema 7.24 *Se α é um número irracional quadrático então*

$$\exists k \in \mathbb{N}\ \forall n \geq k \qquad \alpha_n \quad \text{é reduzido.}$$

Estamos agora em condições de enunciar o resultado principal desta secção.

Teorema 7.25 *Seja α um número irracional. Então:*

a) *α é representado por uma fracção simples periódica se e só se for quadrático;*

b) *α é representado por uma fracção simples puramente periódica se e só se for quadrático e reduzido.*

Exemplos 7.26 *Apesar de o número e ser um número transcendente, a sua expansão como fracção simples infinita tem uma regularidade surpreendente:*

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, \ldots]$$

ou seja $a_0 = 2$, $a_1 = 1$, $a_{3k} = a_{3k+1} = 1$ *e* $a_{3k-1} = k$, *se* $k \in \mathbb{N}$. *A demonstração deste resultado é um pouco elaborada mas usa apenas conhecimentos de análise real.*

Em relação ao número π *(*$=[3, 7, 15, 1, 292, 1, 1, 1, 2, \ldots]$*) não é conhecida qualquer regularidade na fracção simples que o representa.*

Nota 7.27 *Note-se que, se pretendermos desenvolver um número quadrático como fracção simples infinita periódica, podemos sempre utilizar o Lema 7.23 e a Proposição 7.22 para descobrir eventuais erros de contas.*

Demonstrações:

Lema 7.21.

Demonstração: Sabemos que os números quadratics são os números da forma $\alpha = \frac{A_0 \pm \sqrt{D}}{C_0}$. Multiplicando eventualmente por -1 o numerador e o denominador posso considerar que α é da forma $\frac{A+\sqrt{D}}{C}$. Para concluir a demonstração basta notar que $\alpha = \frac{A|C|+\sqrt{DC^2}}{C|C|}$. ∎

Proposição 7.22.

Demonstração: Basta atender a que,

$0 < \alpha - \overline{\alpha} = \frac{2\sqrt{d}}{e}$	porque $\alpha > 1$ e $\overline{\alpha} < 0$	e portanto $e > 0$
$0 < \alpha + \overline{\alpha} = \frac{2c}{e}$	porque $\alpha > 1$ e $\overline{\alpha} > -1$	e portanto $c > 0$
$0 > \overline{\alpha} = \frac{c-\sqrt{d}}{e}$		e portanto $c < \sqrt{d}$
$-1 < \overline{\alpha} = \frac{c-\sqrt{d}}{e}$		e portanto $e > \sqrt{d} - c$
$1 > \alpha = \frac{c+\sqrt{d}}{e}$		e portanto $e < \sqrt{d} + c$.

∎

Lema 7.23.

Se $n = 0$, o resultado é válido por hipótese.

Vejamos o passo de indução para a primeira parte:

Hipótese de indução: existem $c_n \in \mathbb{N}$, $e_n \in \mathbb{N}$ tais que $\alpha_n = \frac{c_n+\sqrt{d}}{e_n}$ e $e_n | d - c_n^2$.

Tese de indução: existem $c_{n+1} \in \mathbb{N}$, $e_{n+1} \in \mathbb{N}$ tais que $\alpha_{n+1} = \frac{c_{n+1}+\sqrt{d}}{e_{n+1}}$ e $e_{n+1} | d - c_{n+1}^2$.

Começamos a desenvolver α_n como fracção racional. Assim

$$\begin{aligned} \alpha_n &= [\alpha_n] + \alpha_n - [\alpha_n] \\ &= [\alpha_n] + \frac{1}{\alpha_{n+1}} \quad \text{em que } \alpha_{n+1} = \tfrac{1}{\alpha_n - [\alpha_n]}. \end{aligned}$$

Desenvolvendo obtemos

$$\alpha_{n+1} = \frac{c_{n+1} + \sqrt{d}}{e_{n+1}} \quad \text{em que} \quad c_{n+1} = [\alpha_n]e_n - c_n \quad \text{e} \quad e_{n+1} = \frac{d - ([\alpha_n]e_n - c_n)^2}{e_n}.$$

Uma vez que

$$d - ([\alpha_n]e_n - c_n)^2 = d - c_n^2 + 2[\alpha_n]e_n c_n - [\alpha_n]^2 e_n^2 \quad \text{e} \quad e_n | d - c_n^2,$$

concluímos que $e_{n+1} \in \mathbb{N}$ e $e_{n+1} | d - c_{n+1}^2$.

Para a segunda parte, basta mostrar que se α_n é reduzido então α_{n+1} também o é. Do mesmo modo que acima, $\alpha_n = [\alpha_n] + \frac{1}{\alpha_{n+1}}$ e portanto

$$\overline{\alpha}_n = [\alpha_n] + \frac{1}{\overline{\alpha}_{n+1}} \quad \text{ou seja} \quad \overline{\alpha}_{n+1} = \frac{1}{-[\alpha_n] + \overline{\alpha}_n}$$

Para concluir que α_{n+1} é reduzido basta usar a hipótese de indução ($-1 < \overline{\alpha}_n < 0$), para obter

$$0 > \frac{1}{-[\alpha_n] - 1} > \frac{1}{-[\alpha_n] + \overline{\alpha}_n} > \frac{1}{-[\alpha_n]} \geq -1.$$

■

Lema 7.24.

Com as notações já utilizadas e para $n \in \mathbb{N}_0$ seja $\alpha_n = \frac{c_n+\sqrt{d}}{e_n}$ em que $\alpha_0 = \alpha$. Utilizando a Nota 7.20, se $k \in \mathbb{N}$, $\overline{\alpha} = \frac{\overline{\alpha}_{k+1}p_k+p_{k-1}}{\overline{\alpha}_{k+1}q_k+q_{k-1}}$. Daqui resulta que

$$\overline{\alpha}_{k+1} = -\frac{q_{k-1}\overline{\alpha} - p_{k-1}}{q_k\overline{\alpha} - p_k} = -\frac{q_{k-1}}{q_k}\frac{\overline{\alpha} - \frac{p_{k-1}}{q_{k-1}}}{\overline{\alpha} - \frac{p_k}{q_k}} \tag{7.1}$$

Suponhamos que $e_0 < 0$ (o outro caso seria tratado de maneira similar).

Como $\lim\limits_{n\in\mathbb{N}} \left[\overline{\alpha} - \frac{p_n}{q_n}\right] = \overline{\alpha} - \alpha = -\frac{2\sqrt{d}}{e_0} > 0$ existe r tal que,

$$n \geq r \Rightarrow \overline{\alpha} - \frac{p_n}{q_n} > 0.$$

Utilizando agora a igualdade (7.1), concluímos que $\overline{\alpha}_{n+1} > 0$.

Por outro lado, se k é um número par maior que r então, utilizando o facto de que $\frac{p_{k-1}}{q_{k-1}} > \frac{p_k}{q_k}$ (ver Corolário 7.5),

$$\begin{aligned}
\overline{\alpha}_{k+1} &= -\frac{q_{k-1}}{q_k}\frac{\overline{\alpha} - \frac{p_{k-1}}{q_{k-1}}}{\overline{\alpha} - \frac{p_k}{q_k}} \\
&> -\frac{\overline{\alpha} - \frac{p_{k-1}}{q_{k-1}}}{\overline{\alpha} - \frac{p_k}{q_k}} \quad \text{porque } q_{k-1} < q_k \\
&\geq -1 \quad \text{porque } 0 < \overline{\alpha} - \tfrac{p_{k-1}}{q_{k-1}} < \overline{\alpha} - \tfrac{p_k}{q_k}.
\end{aligned}$$

Mostramos assim que α_{k+1} é reduzido. Utilizando a segunda parte do lema anterior concluímos que α_n é reduzido para todo $n \geq k+1$. ∎

Teorema 7.25.

b) $\Rightarrow$

Suponhamos que α é representado por uma fracção periódica $[\dot{a}_0, a_1, \ldots, \dot{a}_{r-1}]$. Deste modo, $\alpha > 1$ porque $[\alpha] = a_0 = a_r \in \mathbb{N}$ e

$$\begin{aligned}
\alpha &= [\dot{a}_0, a_1, \ldots, \dot{a}_{r-1}] \\
&= [a_0, a_1, \ldots, a_{r-1}, \dot{a}_0, a_1, \ldots, \dot{a}_{r-1}] \\
&= [a_0, a_1, \ldots, a_{r-1}, \alpha] \\
&= \frac{\alpha p_{r-1} + p_{r-2}}{\alpha q_{r-1} + q_{r-2}} \quad \text{usando a Proposição 7.1.}
\end{aligned}$$

Assim α é um zero do polinómio $f(X) = q_{r-1}X^2 + (q_{r-2} - p_{r-1})X - p_{r-2}$, e portanto α é quadrático.

Por outro lado, $f(0) = -p_{r-2} < 0$ e $f(-1) = (q_{r-1} - q_{r-2}) + (p_{r-1} - p_{r-2}) > 0$. Daqui concluímos que $\overline{\alpha}$ que é o outro zero do polinómio pertence ao intervalo $]-1, 0[$.

a) $\Rightarrow$

Suponhamos que α é representado por uma fracção periódica $[a_0, a_1, \ldots, \dot{a}_k, \ldots, \dot{a}_{k+r-1}]$ com $k \geq 1$. Seja $\beta = [\dot{a}_k, \ldots, \dot{a}_{k+r-1}]$.

Atendendo ao que foi dito acima, β é quadrático e portanto é da forma $\frac{c+\sqrt{d}}{e}$ em que $c \in \mathbb{N}$, $e \in \mathbb{N} \setminus \{0\}$, $d \in \mathbb{N}$ e $\sqrt{d} \notin \mathbb{N}$.

Assim,

$$\begin{aligned}
\alpha &= [a_0, a_1, \ldots, a_{k-1}, \beta] \\
&= \frac{\beta p_{k-1} + p_{k-2}}{\beta q_{k-1} + q_{k-2}} \quad \text{usando a Proposição 7.1} \\
&= \frac{\frac{c+\sqrt{d}}{e} p_{k-1} + p_{k-2}}{\frac{c+\sqrt{d}}{e} q_{k-1} + q_{k-2}} \\
&= \frac{(c + ep_{k-2}) + p_{k-1}\sqrt{d}}{(c + eq_{k-2}) + q_{k-1}\sqrt{d}} \\
&= \frac{\left[(c + ep_{k-2}) + p_{k-1}\sqrt{d}\right]\left[(c + eq_{k-2}) - q_{k-1}\sqrt{d}\right]}{(c + eq_{k-2})^2 + q_{k-1}^2 d}
\end{aligned}$$

Desenvolvendo encontramos $A, B \in \mathbb{N}$ e $C \in \mathbb{N}$ tais que $\alpha = \frac{A+B\sqrt{d}}{C}$. Daqui concluímos que α é um zero de um polinómio de segundo grau e com coeficientes inteiros, ou seja, α é um número quadrático.

a) $\Leftarrow$

Suponhamos que α é um número quadrático. Pelo lema anterior, seja $k \in \mathbb{N}$ tal que α_n é reduzido para todo $n \geq k$.

Assim, usando a Proposição 7.22 o conjunto $\{(c_n, e_n) : n \geq k\}$ é um conjunto finito (porquê?). Em particular existem r, s tais que $r > s$ e $(c_r, e_r) = (c_s, e_s)$. Deste modo $\alpha_r = \alpha_s$ e portanto α é representado por uma fracção periódica.

b) $\Leftarrow$

Suponhamos que α é um número quadrático reduzido. Pelo que vimos acima, α é representado por uma fracção periódica $[a_0, a_1, \ldots, \dot{a}_k, \ldots, \dot{a}_{k+r-1}]$. Suponhamos por absurdo que $k \geq 1$ e que $a_{k-1} \neq a_{k+r-1}$. Note-se que $\alpha_k = \alpha_{k+r}$.

Assim,

$$\begin{aligned} \alpha_{k-1} - \alpha_{k+r-1} &= a_{k-1} + \frac{1}{\alpha_k} - a_{k+r-1} + \frac{1}{\alpha_{k+r}} \\ &= a_{k-1} - a_{k+r-1}, \end{aligned}$$

que é um inteiro não nulo. Assim, $\overline{\alpha}_{k-1} - \overline{\alpha}_{k+r-1}$ é também um inteiro não nulo o que é absurdo pois $\overline{\alpha}_{k-1}, \overline{\alpha}_{k+r-1} \in]-1, 0[$. ■

7.4.2 Fracção simples infinita que representa $\sqrt{d}$

A fim de aplicarmos ao estudo das Equações de Pell vamos estudar as fracções simples infinitas que representam números da forma $\sqrt{d}$. Vamos ver que existe uma caracterização muito simples das fracções racionais que representam estes números.

Usando a última observação da Nota 7.20 e o Teorema 7.25 podemos concluir que a fracção que representa o número $\sqrt{d}$ em que d é um número racional maior que 1 e tal que $\sqrt{d} \notin \mathbb{Q}$ é da forma,

$$[a_0, \dot{a_1}, \ldots, \dot{a_r}].$$

Por outro lado, se $d \in]0, 1[$ então $\sqrt{d} = [0, \sqrt{\frac{1}{d}}]$ e, portanto a fracção que representa o número $\sqrt{d}$ é da forma

$$[0, a_0, \dot{a_1}, \ldots, \dot{a_r}].$$

Alguns cálculos simples mostram que:

$$\begin{array}{ll}\sqrt{2}=[1,\dot{2}] & \sqrt{77}=[8,\dot{1},3,2,3,1,\dot{16}]\\ \sqrt{13}=[3,\dot{1},1,1,1,\dot{6}] & \sqrt{493}=[22,\dot{4},1,10,3,3,10,1,4,\dot{44}]\\ \sqrt{34}=[5,\dot{1},4,1,\dot{10}] & \sqrt{\frac{11}{7}}=[1,\dot{3},1,16,1,3,\dot{2}].\end{array}$$

Em todos estes casos as fracções são do tipo $[a_0,\dot{a}_1,a_2,\ldots,a_2,a_1,2\dot{a}_0]$. Vejamos que isto é geral. Na base da demonstração está o seguinte resultado.

Proposição 7.28 *Se $\alpha=[\dot{a}_0,a_1,\ldots,\dot{a}_{r-1}]$ então $-\frac{1}{\overline{\alpha}}=[\dot{a}_{r-1},\ldots,a_1,\dot{a}_0]$, em $\overline{\alpha}$ e α são zeros do mesmo polinómio do segundo grau.*

Demonstração: Notando que $\alpha_r=\alpha$, temos

$$\alpha=a_0+\frac{1}{\alpha_1},\ldots,\alpha_k=a_k+\frac{1}{\alpha_{k+1}},\ldots,\alpha_{r-1}=a_{r-1}+\frac{1}{\alpha_r}=a_{r-1}+\frac{1}{\alpha}.$$

Conjugando, obtemos

$$\overline{\alpha}=a_0+\frac{1}{\overline{\alpha}_1},\ldots,\overline{\alpha}_k=a_k+\frac{1}{\overline{\alpha}_{k+1}},\ldots,\overline{\alpha}_{r-1}=a_{r-1}+\frac{1}{\overline{\alpha}_r}=a_{r-1}+\frac{1}{\overline{\alpha}}.$$

Estas igualdades podem ser escritas do seguinte modo:

$$-\frac{1}{\overline{\alpha}}=a_{r-1}+(-\overline{\alpha}_{r-1}),\ldots,-\frac{1}{\overline{\alpha}_{k-1}}=a_k+(-\overline{\alpha}_k)\ldots,-\frac{1}{\overline{\alpha}_1}=a_0+(-\overline{\alpha})$$

Como α é reduzido, α_n é reduzido para todo $n\in\mathbb{N}$. Deste modo

$$(-\overline{\alpha}_{r-1}),\ldots,(-\overline{\alpha}_k)\ldots,(-\overline{\alpha})\in]0,1[.$$

Assim

$$\left[-\frac{1}{\overline{\alpha}}\right]=a_{r-1},\ldots,\left[-\frac{1}{\overline{\alpha}_{k-1}}\right]=a_k\ldots,\left[-\frac{1}{\overline{\alpha}_1}\right]=a_0$$

e, portanto

$$-\frac{1}{\overline{\alpha}}=\left[a_{r-1},-\frac{1}{\overline{\alpha}_{r-1}}\right],\ldots,-\frac{1}{\overline{\alpha}_{k-1}}=\left[a_k,-\frac{1}{\overline{\alpha}_k}\right],\ldots,-\frac{1}{\overline{\alpha}_1}=\left[a_0,-\frac{1}{\overline{\alpha}}\right].$$

Daqui se conclui que a tese da proposição. ■

Teorema 7.29 *Se α um número irracional positivo então,*

a) *existe $d \in \mathbb{Q}$ com $d > 1$ tal que $\alpha = \sqrt{d}$ se e só se a fracção contínua que representa α é da forma*

$$[a_0, \dot{a}_1, a_2, \ldots, a_2, a_1, 2\dot{a}_0],$$

em que $a_0, a_1, \ldots \in \mathbb{N}$.

b) *existe $d \in \mathbb{Q}$ com $d < 1$ tal que $\alpha = \sqrt{d}$ se e só se a fracção contínua que representa α é da forma*

$$[0, a_0, \dot{a}_1, a_2, \ldots, a_2, a_1, 2\dot{a}_0],$$

em que $a_0, a_1, \ldots \in \mathbb{N}$.

Demonstração:

a) Suponhamos que $\alpha = \sqrt{d}$ com d número racional maior que 1.

Uma vez que $\sqrt{d} = \left[[\sqrt{d}], \frac{1}{\sqrt{d}-[\sqrt{d}]} \right]$ e $\frac{1}{\sqrt{d}-[\sqrt{d}]}$ é um número reduzido, existem $a_1, \ldots, a_r \in \mathbb{N}$ tais que $\frac{1}{\sqrt{d}-[\sqrt{d}]} = [\dot{a}_1, \ldots, \dot{a}_r]$.

Deste modo,

$$\sqrt{d} + [\sqrt{d}] = \begin{cases} [\dot{a}_r, \ldots, \dot{a}_1] & \text{pela proposição anterior} \\ \\ [2a_0, \dot{a}_1, \ldots, \dot{a}_r] & \text{usando o Exercício 7.15.} \end{cases}$$

Igualando as duas fracções anteriores, concluímos que a fracção que define $\sqrt{d}$ é da forma desejada.

Inversamente, suponhamos que a fracção contínua que representa α é da forma $[a_0, \dot{a}_1, a_2, \ldots, a_2, a_1, 2\dot{a}_0]$.

Neste caso, α é um número quadrático e, portanto, existem $a, b \in \mathbb{Z}$ com $b \neq 0$ e $d \in \mathbb{N}$ tais que $\alpha = \frac{a+\sqrt{D}}{b}$.

Da igualdade $\alpha = [a_0, \dot{a}_1, a_2, \ldots, a_2, a_1, 2\dot{a}_0]$ resulta que

$$\alpha + a_0 = [2a_0, \dot{a}_1, a_2, \ldots, a_2, a_1, 2\dot{a}_0] = [2\dot{a}_0, \dot{a}_1, a_2, \ldots, a_2, \dot{a}_1]$$

Usando as igualdades $\alpha = a_0 + \frac{1}{\alpha_1}$ e $\alpha_1 = [\dot{a}_1, a_2, \ldots, a_2, a_1, 2\dot{a}_0]$ e a Proposição 7.28 temos

$$-\frac{1}{\overline{\alpha}_1} = a_0 + \alpha.$$

Conjugando com a igualdade $\overline{\alpha} = a_0 + \frac{1}{\overline{\alpha}_1}$ obtemos $\alpha + \overline{\alpha} = 0$ o que mostra que $a = 0$ e, portanto $\alpha = \sqrt{\frac{D}{b^2}}$.

b) Por um lado se $\alpha = [0, a_0, \dot{a}_1, a_2, \ldots, a_2, a_1, 2\dot{a}_0]$ então $\frac{1}{\alpha} = [a_0, \dot{a}_1, a_2, \ldots, a_2, a_1, 2\dot{a}_0]$ e, usando a), existe $d > 1$ tal que $\frac{1}{\alpha} = \sqrt{d}$. Deste modo $\alpha = \sqrt{\frac{1}{d}}$.

Por outro lado, se $\alpha = \sqrt{d}$ com $d \in]0, 1[$ então $\alpha = [0, \frac{1}{\alpha}] = \left[0, \sqrt{\frac{1}{d}}\right]$. Para concluir basta usar novamente a alínea a). ■

Teorema 7.30 *Sejam $d \in \mathbb{N}$, $\sqrt{d} \notin \mathbb{N}$, $\alpha = \sqrt{d}$, $n \in \mathbb{N}_0$ e r o período da fracção simples infinita que representa $\sqrt{d}$.*

Então:

a) *se $n \in \mathbb{N}$, $e_n, c_n \in \mathbb{N}$;*

b) *$e_n = 1$ se e só se r divide n.*

c) *$(-1)^n e_n = -1$ se e só se r é ímpar e $n = rk$ para algum k inteiro positivo ímpar.*

Demonstração:

a) Basta usar a Proposição 7.22 atendendo ao facto de que α_n é reduzido.

b) Comecemos por notar que $\alpha_0, \ldots, \alpha_r$ são distintos e que $\alpha_1 = \alpha_{r+1}$. Assim

$$\alpha_r = 2a_0 + \frac{1}{\alpha_{r+1}} = 2a_0 + \frac{1}{\alpha_1} = 2a_0 + (\sqrt{d} - a_0) = a_0 + \sqrt{d}$$

e portanto $e_r = 1$. Por outro lado $\alpha_{rk} = \alpha_r$ e portanto $e_{rk} = e_r = 1$.

Inversamente, se $e_n = 1$ então $\alpha_n = c_n + \sqrt{d}$. Deste modo $a_n = [\alpha_n] = c_n + [\sqrt{d}] = c_n + a_0$. Temos assim sucessivamente

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}}, \qquad c_n + \sqrt{d} = c_n + a_0 + \frac{1}{\alpha_{n+1}} \qquad \sqrt{d} = a_0 + \frac{1}{\alpha_{n+1}},$$

o que mostra que $\alpha_1 = \alpha_{n+1}$ (pois $\sqrt{d} = a_0 + \frac{1}{\alpha_1}$) e, portanto n divide r.

c) Note-se que, como $e_n \in \mathbb{N}$, $(-1)^n e_n = -1$ se e só se $e_n = 1$ e n é ímpar. A conclusão segue agora da alínea anterior. ■

7.5 Equações de Pell

Vamos ver uma aplicação das fracções contínuas no estudo das chamadas equações de Pell, que são equações (nas variáveis inteiras x e y) do tipo $x^2 - dy^2 = m$ em que $d \in \mathbb{N}$, $m \in \mathbb{Z}$. Note-se que, se $d = k^2$, com $k \in \mathbb{N}$ então

$$x^2 - dy^2 = n \iff (x - ky)(x + ky) = n$$

que tem solução simples se tivermos uma factorização de n. Por este motivo vamos supor, a partir de agora, que $\sqrt{d} \notin \mathbb{N}$.

Diremos que um par (x, y) é uma solução da equação se $x^2 - dy^2 = m$. Diremos que a solução é não trivial se $x, y \neq 0$.

Seja $\mathbb{Z}[\sqrt{d}] = \left\{x + y\sqrt{d} : x, y \in \mathbb{Z}\right\}$. Então a função $\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z}[\sqrt{d}] \\ (x, y) & \mapsto & x + y\sqrt{d} \end{array}$ é uma bijecção.

Deste modo, e para simplificar a notação, escreveremos por vezes: "a solução $x + y\sqrt{d}$" em vez de "a solução (x, y)". Em particular podemos comparar duas soluções!

Note-se que $\mathbb{Z}[\sqrt{d}]$ é um subanel cujos elementos invertíveis são os elementos da forma $x + y\sqrt{d}$ tais que $x^2 - dy^2 = \pm 1$.

Teorema 7.31 *Sejam d um inteiro positivo que não é um quadrado perfeito e $m, m^* \in \mathbb{Z}$. Deste modo:*

a) *se existe $n \in \mathbb{N}$ tal que $m = (-1)^n e_n$ a equação $x^2 - dy^2 = m$ tem solução não trivial. Mais concretamente, $(p_{n-1})^2 - d(q_{n-1})^2 = (-1)^n e_n$;*

b) *a equação $x^2 - dy^2 = 1$ admite solução não trivial;*

c) *se o período da fracção racional que representa $\sqrt{d}$ for ímpar, a equação $x^2 - dy^2 = -1$ admite solução;*

d) *se $x + y\sqrt{d}$ é solução de $x^2 - dy^2 = m$ e $x^* + y^*\sqrt{d}$ é solução de $x^2 - dy^2 = m^*$ então $(x + y\sqrt{d})(x^* + y^*\sqrt{d})$ é solução de $x^2 - dy^2 = mm^*$;*

e) *se a equação $x^2 - dy^2 = m$ admite solução, então admite uma infinidade de soluções;*

f) *se $x_0 + y_0\sqrt{d}$ é a menor solução maior que 1 (ver Lema7.32 da equação $x^2 - dy^2 = 1$ então o conjunto de soluções dessa equação é:*

$$\left\{\varepsilon(x_0 + y_0\sqrt{d})^n : n \in \mathbb{Z},\ \varepsilon \in \{1, -1\}\right\}.$$

Demonstração:

a) Sejam $\alpha = \sqrt{d}$, $a_0, \ldots, a_{n-1} \in \mathbb{N}$ e $\alpha_n = \frac{c_n + \sqrt{d}}{e_n}$ tais que $\sqrt{d} = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$.

Assim,

$$\begin{aligned}
\sqrt{d} &= \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} \\
&= \frac{\frac{c_n + \sqrt{d}}{e_n} p_{n-1} + p_{n-2}}{\frac{c_n + \sqrt{d}}{e_n} q_{n-1} + q_{n-2}} \\
&= \frac{(c_n + \sqrt{d}) p_{n-1} + p_{n-2} e_n}{(c_n + \sqrt{d}) q_{n-1} + q_{n-2} e_n}
\end{aligned}$$

Daqui obtemos,

$$\sqrt{d}\left[(c_n+\sqrt{d})q_{n-1}+q_{n-2}e_n\right] \;=\; \left[(c_n+\sqrt{d})p_{n-1}+p_{n-2}e_n\right]$$

ou, equivalentemente,

$$dq_{n-1}+(c_nq_{n-1}+e_nq_{n-2})\sqrt{d} \;=\; (c_np_{n-1}+p_{n-2}e_n)+p_{n-1}\sqrt{d}.$$

Daqui concluímos que,

$$\begin{cases} c_nq_{n-1}+e_nq_{n-2} &= p_{n-1} \\ c_np_{n-1}+p_{n-2}e_n &= dq_{n-1}. \end{cases}$$

Multiplicando a primeira equação por p_{n-1} e a segunda equação por q_{n-1} e subtraindo obtemos

$p_{n-1}^2-dq_{n-1}^2=[p_{n-1}q_{n-2}-q_{n-1}p_{n-2}]e_n=(-1)^ne_n$ usando o Corolário 7.5.

b) e c) São uma consequência de a) e do Teorema 7.30.

d) Basta notar que $(x+y\sqrt{d})(x^*+y^*\sqrt{d})=(xx^*+dyy^*)+(x^*y+xy^*)\sqrt{d}$ e que

$$\begin{aligned}(xx^*+dyy^*)^2-d(x^*y+xy^*)^2 &= (xx^*)^2+d^2(yy^*)^2-d(x^*y)^2-d(xy^*)^2 \\ &= x^2[x^{*2}-dy^{*2}]-dy^2[x^{*2}-dy^{*2}] \\ &= [x^{*2}-dy^{*2}]\,[x^2-dy^2]=m^*m.\end{aligned}$$

e) Seja $x+y\sqrt{d}$ uma solução de $x^2-dy^2=m$ e consideremos $x^*+y^*\sqrt{d}$ uma solução de $x^2-dy^2=1$, com $x^*,y^*\in\mathbb{N}$. Utilizando sucessivamente a alínea anterior mostramos que, se $n\in\mathbb{N}$, $(x+y\sqrt{d})(x^*+y^*\sqrt{d})^n$ é uma solução da equação $x^2-dy^2=m$. Note-se que

$$n\neq m \implies (x+y\sqrt{d})(x^*+y^*\sqrt{d})^m\neq(x+y\sqrt{d})(x^*+y^*\sqrt{d})^n.$$

f) Seja $A=\left\{\varepsilon(x_0+y_0\sqrt{d})^n : n\in\mathbb{N},\ \varepsilon\in\{1,-1\}\right\}$.

Comecemos por mostrar que $(x_0 + \sqrt{d}y_0)^{-1}$ é solução da equação $x^2 - dy^2 = 1$. Para isso basta notar que $x_0 - \sqrt{d}y_0$ é uma solução da equação e que,

$$(x_0 + \sqrt{d}y_0)^{-1} = \frac{1}{x_0 + \sqrt{d}y_0} = \frac{x_0 - \sqrt{d}y_0}{x_0^2 - dy_0^2} = x_0 - \sqrt{d}y_0.$$

Usando repetidamente a alínea d) concluímos que todo o elemento de A é solução da equação $x^2 - dy^2 = 1$.

Vamos agora demonstrar que toda a solução da equação $x^2 - y^2 = 1$ pertence a A. Seja $x_1 + \sqrt{d}y_1$ uma tal solução.

Suponhamos que $x_1, y_1 > 0$. Uma vez que a sucessão $\left((x_0 + \sqrt{d}y_0)^n\right)_{n\in\mathbb{N}}$ é uma sucessão estritamente crescente com limite $+\infty$, existe $n \in \mathbb{N}$ tal que,

$$(x_0 + \sqrt{d}y_0)^n \leq x_1 + \sqrt{d}y_1 < (x_0 + \sqrt{d}y_0)^{n+1}.$$

Daqui resulta que

$$1 \leq (x_1 + \sqrt{d}y_1)(x_0 + \sqrt{d}y_0)^{-n} < x_0 + \sqrt{d}y_0.$$

Utilizando d), $(x_1 + \sqrt{d}y_1)(x_0 + \sqrt{d}y_0)^{-n}$ é uma solução da equação $x^2 - dy^2 = 1$. Pela minimalidade de $x_0 + \sqrt{d}y_0$, $(x_1 + \sqrt{d}y_1)(x_0 + \sqrt{d}y_0)^{-n} = 1$, ou seja $x_1 + \sqrt{d}y_1 = (x_0 + \sqrt{d}y_0)^n \in A$.

Se x_1, y_1 não são ambos positivos então $x_1 + \sqrt{d}y_0 = \varepsilon(|x_1| + \sqrt{d}|y_1|)^\delta$ em que ε e δ são respectivamente o sinal de x_1 e de y_1. Pelo que vimos acima existe $n \in \mathbb{N}$ tal que $|x_1| + \sqrt{d}|y_1| = (x_0 + \sqrt{d}y_0)^n$ e portanto $x_1 + \sqrt{d}y_1 \in A$. ∎

Lema 7.32 *Uma solução $(a, b) \in \mathbb{Z}^2$ da equação $x^2 - dy^2 = 1$ é positiva se e só se $a + b\sqrt{d} > 1$.*

Demonstração: Se $a, b > 0$ então $a + b\sqrt{d} \geq 1 + \sqrt{d} > 1$.

Suponhamos agora que $a + b\sqrt{d} > 1$, o que implica que a e b não podem ser ambos negativos.

Se a ou b é positivo e o outro é negativo então $|a - b\sqrt{d}| \geq |a + b\sqrt{d}| = a + b\sqrt{d}$ e portanto

$$1 = a^2 - db^2 = |a - b\sqrt{d}|\,|a + b\sqrt{d}| \geq (a + b\sqrt{d})^2 > 1,$$

o que é absurdo. ■

Nota: Gostaria de fazer algumas (das muitas possíveis) considerações (sem demonstração) acerca deste último teorema.

- Se r é o menor inteiro tal que $(-1)^r e_r = 1$ (r é o período da fracção que representa $\sqrt{d}$) então a menor solução positiva de $x^2 - dy^2 = 1$ é $x = p_{r-1}$, $y = q_{r-1}$.

- Se p, q são inteiros positivos, $p^2 - dq^2 = m$, $|m| < \sqrt{d}$ e m é livre de quadrados então existe $n \in \mathbb{N}$ tal que $m = (-1)^n e_n$ e existe $k \in \mathbb{N}$ tal que $\frac{p}{q} = \frac{p_k}{q_k}$. Em particular se p e q são primos entre si então $p = p_k$ e $q = q_k$.

  Note-se que se (p, q) é uma solução de uma equação do tipo $x^2 - dy^2 = m$ então p e q não têm de ser primos entre si (essa conclusão seria válida se m fosse primo). Por exemplo $10^2 - 24 \times 2^2 = 4$. De qualquer modo $\frac{10}{2} = \frac{5}{1}$ que é um convergente de $\sqrt{24}$.

- Seja r o período da fracção contínua que representa $\sqrt{d}$. Então se r é par, a equação $x^2 - dy^2 = -1$ não tem solução e as soluções positivas de $x^2 - dy^2 = 1$ são todas da forma (p_{kr-1}, q_{kr-1}). Se r é ímpar então a equação $x^2 - dy^2 = -1$ admite como soluções positivas exactamente os pares da forma (p_{kr-1}, q_{kr-1}) em que k é ímpar. Se r é ímpar então a equação $x^2 - dy^2 = 1$ admite como soluções positivas exactamente os pares da forma (p_{kr-1}, q_{kr-1}) em que k é par.

- Se $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $c \in \mathbb{Z}$ e $d \in \mathbb{N}$ são tais que $|\alpha - \frac{c}{d}| < |\alpha - \frac{p_k}{q_k}|$ para algum k, então $d > q_k$.

Termino com uma tabela contendo as fracções contínuas dos números da forma $\sqrt{d}$ em que d é um inteiro entre 2 e 52 que não é um quadrado perfeito.

d	$\sqrt{d}$	d	$\sqrt{d}$	d	$\sqrt{d}$
2	$\left[1,\dot{2}\right]$	20	$\left[4,\dot{2},\dot{8}\right]$	37	$\left[6,\dot{1}\dot{2}\right]$
3	$\left[1,\dot{1},\dot{2}\right]$	21	$\left[4,\dot{1},1,2,1,1,\dot{8}\right]$	38	$\left[6,\dot{6},\dot{1}\dot{2}\right]$
5	$\left[2,\dot{4}\right]$	22	$\left[4,\dot{1},2,4,2,1,\dot{8}\right]$	39	$\left[6,\dot{4},\dot{1}\dot{2}\right]$
6	$\left[2,\dot{2},\dot{4}\right]$	23	$\left[4,\dot{1},3,1,\dot{8}\right]$	40	$\left[6,\dot{3},\dot{1}\dot{2}\right]$
7	$\left[2,\dot{1},1,1,\dot{4}\right]$	24	$\left[4,\dot{1},\dot{8}\right]$	41	$\left[6,\dot{2},2,\dot{1}\dot{2}\right]$
8	$\left[2,\dot{1},\dot{4}\right]$	26	$\left[5,\dot{1}\dot{0}\right]$	42	$\left[6,\dot{2},\dot{1}\dot{2}\right]$
10	$\left[3,\dot{6}\right]$	27	$\left[5,\dot{5},\dot{1}\dot{0}\right]$	43	$\left[6,\dot{1},1,3,1,5,1,3,1,1,\dot{1}\dot{2}\right]$
11	$\left[3,\dot{3},\dot{6}\right]$	28	$\left[5,\dot{3},2,3,\dot{1}\dot{0}\right]$	44	$\left[6,\dot{1},1,1,2,1,1,1,\dot{1}\dot{2}\right]$
12	$\left[3,\dot{2},\dot{6}\right]$	29	$\left[5,\dot{2},1,1,2,\dot{1}\dot{0}\right]$	45	$\left[6,\dot{1},2,2,2,1,\dot{1}\dot{2}\right]$
13	$\left[3,\dot{1},1,1,1,\dot{6}\right]$	30	$\left[5,\dot{2},\dot{1}\dot{0}\right]$	46	$\left[6,\dot{1},3,1,1,2,6,2,1,1,3,1,\dot{1}\dot{2}\right]$
14	$\left[3,\dot{1},2,1,\dot{6}\right]$	31	$\left[5,\dot{1},1,3,5,3,1,1,\dot{1}\dot{0}\right]$	47	$\left[6,\dot{1},5,1,\dot{1}\dot{2}\right]$
15	$\left[3,\dot{1},\dot{6}\right]$	32	$\left[5,\dot{1},1,1,\dot{1}\dot{0}\right]$	48	$\left[6,\dot{1},\dot{1}\dot{2}\right]$
17	$\left[4,\dot{8}\right]$	33	$\left[5,\dot{1},2,1,\dot{1}\dot{0}\right]$	50	$\left[7,\dot{1}\dot{4}\right]$
18	$\left[4,\dot{4},\dot{8}\right]$	34	$\left[5,\dot{1},4,1,\dot{1}\dot{0}\right]$	51	$\left[7,\dot{7},\dot{1}\dot{4}\right]$
19	$\left[4,\dot{2},1,3,1,2,\dot{8}\right]$	35	$\left[5,\dot{1},\dot{1}\dot{0}\right]$	52	$\left[7,\dot{4},1,2,1,4,\dot{1}\dot{4}\right]$

7.6 Exercícios

7.1. Escreva na forma $\frac{a}{b}$ com $a \in \mathbb{Z}$ e $b \in \mathbb{N}$ os números: $[2,3,4,5]$, $[-2,3,4,5]$, $[1,2,4,8]$, $[-1,1,1,1]$, $[2,2,2,2]$ e $[3,3,3,3]$.

7.2. Calcule as fracções contínuas que representam cada um dos seguintes números reais: $\frac{181}{101}$, $-\frac{181}{101}$, $\frac{383}{101}$, $\sqrt{5}$, $\sqrt{7}$, $\sqrt{11}$, $\sqrt{19}$, $2+\sqrt{5}$, $\frac{2+3\sqrt{7}}{3}$ e $-\frac{2+3\sqrt{7}}{3}$.

7.3. Use o exercício anterior para encontrar uma solução das equações diofantinas: $181x + 101y = 5$ e $383x - 101 = 23$.

7.4. Encontre os 4 primeiros termos das fracções contínuas representando $\sqrt[3]{2}$, e, π.

7.5. "Quais os números representados pelas fracções":

a) $[\dot{2}]$;

b) $[1, \dot{2}]$;

c) $[\dot{3}, 2, \dot{1}]$;

d) $[6, 1, \dot{3}, 2, \dot{1}]$;

e) $[1, 2, \dot{2}, \dot{3}]$.

7.6. Quais dos seguintes números são representados por uma fracção contínua puramente periódica: $\frac{1+\sqrt{11}}{3}$; $\frac{2+\sqrt{6}}{2}$; $\frac{7+\sqrt{101}}{3}$?

7.7. Mostre que, se $x = [a_0, a_1, a_2, \ldots]$ e $x > 1$ então $\frac{1}{x} = [0, a_0, a_1, a_2, \ldots]$.

7.8. Sejam $a, b \in \mathbb{N}$. Considere $\alpha = [\dot{a}, \dot{b}]$. Encontre uma equação do segundo grau que seja satisfeita por α. Mostre que $\frac{-1}{[\dot{b}, \dot{a}]}$ satisfaz essa equação.

7.9. Com as notações usuais mostre que

$$\alpha = [\alpha] + \sum_{k=0}^{\infty} \frac{(-1)^k}{q_k q_{k+1}}.$$

7.10. Escreva o número $[\dot{1}, \dot{2}]$ na forma $\frac{a+\sqrt{d}}{c}$, com $a \in \mathbb{Z}$, $c \in \mathbb{Z} \setminus \{0\}$ e $d \in \mathbb{N}$ e $e|d - c^2$.

7.11. Seja $\alpha = [a_0, a_1, \ldots] \in \mathbb{R} \setminus \mathbb{Q}$ o único zero real positivo de um polinómio $f(x)$ de coeficientes inteiros e cujo coeficiente guia é positivo.

a) Mostre que a_0 é o maior inteiro k tal que $f(k) < 0$;

b) Mostre que a_1 é o maior inteiro k tal que $f_1(k) < 0$, em que $f_1(x) = -x^d f(\frac{1}{x} + a_0)$ sendo d o grau de f.

c) Mais geralmente, mostre que a_i é o maior inteiro k tal que $f_i(k) < 0$, em que $f_i(x) = -x^d f_{i-1}(\frac{1}{x} + a_0)$ sendo d o grau de f.

7.12. Aplique o "algoritmo" referido no Exercício 11 para calcular os primeiros termos das fracções contínuas que representam: $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[3]{3}$, $\sqrt[3]{4}$, $\sqrt[3]{5}$.

7.13. Aplique o "algoritmo" referido no Exercício 11 para calcular os primeiros termos da fracção contínua que representa o zero real do polinómio $x^5 - x - 1$.

7.14. Mostre que:

a) $\sqrt{n^2+1} = \left[n, \dot{2n}\right]$ para $n \geq 1$;

b) $\sqrt{n^2+2} = \left[n, \dot{n}, \dot{2n}\right]$ para $n \geq 1$;

c) $\sqrt{n^2-1} = \left[n-1, \dot{1}, \dot{2n-2}\right]$ para $n \geq 2$;

d) $\sqrt{n^2-n} = \left[n-1, \dot{2}, \dot{2n-2}\right]$ para $n \geq 2$;

e) $\sqrt{n^2-2} = \left[n-1, \dot{1}, n-2, 1, \dot{2n-2}\right]$ para $n \geq 3$.

f) $\sqrt{9n^2+6} = \left[3n, \dot{n}, \dot{6n}\right]$ para $n \in \mathbb{N}$.

7.15. Mostre que, se $\sqrt{n}$ é representada por uma fracção contínua com período 1 então existe $k \in \mathbb{N}$ tal que $n = d^2 + 1$.

7.16. Com as notações da Proposição 7.1 mostre que $q_k \geq 2^{\frac{k}{2}}$ se $k \geq 2$.

7.17. Sabendo que $\sqrt{29} = [5, \dot{2}, 1, 1, 2, \dot{10}]$ encontre $x, y \in \mathbb{N}$ tais que $x^2 - 29y^2 = -1$.

7.18. Sabendo que $(1068)^2 - 73(125)^2 = -1$, encontre $x, y \in \mathbb{N}$ tais que $x^2 - 73y^2 = 1$.

7.19. Considere $d \in \mathbb{N}$ e a fracção contínua que o representa $[a_0, \dot{a_1}, a_2, \ldots, a_2, a_1, \dot{2a_0}]$. Mostre que $a_i \leq a_0$ para todo $i \neq 0$. **Sugestão:** Use a igualdade $a_i = [\alpha_i] = [\frac{c_i + \sqrt{d}}{e_i}]$ e as desigualdades $e_i \geq 2$ e $0 < c_i < \sqrt{d}$.

7.20. Resolva as equações:

a) $x^2 - 31y^2 = 1$;

b) $x^2 - 30y^2 = -1$;

c) $x^2 - 14y^2 = 1$.

d) $x^2 - 14y^2 = 2$;

e) $x^2 - 29y^2 = 4$;

f) $x^2 - 29y^2 = 12$;

g) $x^2 - 43y^2 = 2$;

h) $x^2 - 14y^2 = 1$.

7.21. Seja $\alpha \in \mathbb{R}$ e suponhamos que $\left[a_0, a_1, a_2, a_3 \ldots\right]$ é a fracção contínua infinita que representa α. Mostre que, se $a_1 > 1$ então $-\alpha = \left[-a_0 - 1, 1, a_1 - 1, a_2, a_3, \ldots\right]$.

7.22. Encontre a única solução (a, b) da equação $x^2 - 14y^2 = 1$ com $10^6 < a + b\sqrt{14} < 10^8$.

7.23. Sabendo que $(2, 1)$ é uma solução de $x^2 - 5y^2 = -1$ encontre o sétimo convergente $\frac{p_7}{q_7}$ de $\sqrt{5} = [2, \dot{4}]$.

7.24. Mostre que, se m é um quadrado perfeito então a equação $x^2 - dy^2 = m$ (com d inteiro positivo que não é um quadrado perfeito) tem sempre solução.

7.25. Considere os números $a = \frac{27+\sqrt{1023}}{14}$, $b = \frac{-4+\sqrt{1122}}{7}$, $c = 2 + \sqrt[3]{11}$, $d = \frac{245}{58}$. Qual a fracção contínua que representa cada um destes números sabendo que ela pertence ao conjunto

$$\Big\{[\dot{4}, 4, 1, \dot{2}], [4, \dot{4}, 1, 2, \dot{9}], [4, 4, 2, 6, 1, 1, 2, 1, 2, 9, 88, \ldots], [4, 4, 2, 6], [4, \dot{4}, 1, 2, 1, 4, \dot{8}]\Big\}.$$

Nota: Os únicos cálculos (não triviais) que podem ser necessários são: $\sqrt{1023} \sim 31,98$; $\sqrt{1122} \sim 33,49$.

7.26. Mostre que, se $x, y \in \mathbb{N}$ e p é um primo ímpar tais que $x^2 - 2y^2 = p$, então p é congruente com 1 módulo 8.

7.27. Com as notações usuais,

a) Complete a tabela,

n	a_n	p_n	q_n	α_n	$(-1)^n e_n$
0				$\sqrt{57}$	1
1	1				
2			2	$\frac{1+\sqrt{57}}{7}$	
3	4				
4		83		$\frac{6+\sqrt{57}}{7}$	
5	1				
6			291	$7+\sqrt{57}$	1
7		2348			

b) Calcule α_{32}.

c) Encontre uma solução de $x^2 - 57y^2 = 1$, com $x, y \in \mathbb{N}$.

d) Escolha um inteiro m maior que 10 e que não seja um quadrado perfeito e encontre uma solução de $x^2 - 57y^2 = m$, com $x, y \in \mathbb{N}$.

7.28. Escolha $m \in \{10, 11, \ldots, 20\}$ e $d \in \mathbb{N}$ que não seja um quadrado perfeito e encontre uma solução da equação $x^2 - dy^2 = m$. Diga como encontraria uma solução com $x \geq 1111$.

7.29. Pretende-se estudar a existência de inteiros positivos n tais que $n^2 + (n+1)^2$ seja um quadrado perfeito. Dito de outro modo, pretende-se estudar a existência de triângulos pitagóricos da forma $[n, n+1, k]$.

a) Mostre que, se n é igual a 3, 20, 119, 696 ou 4059 então $n^2 + (n+1)^2$ é um

quadrado perfeito.

b) Mostre que a equação $n^2+(n+1)^2=k^2$ é equivalente à equação $(2n+1)^2-2k^2=-1$.

c) Mostre que a equação da alínea anterior tem infinidade de soluções com n par e uma infinidade de soluções com n ímpar.

7.30. Mostre que a soma dos primeiros n inteiros positivos é um quadrado perfeito para uma infinidade de valores pares de n e para uma infinidade de valores ímpares de n. Mostre que os primeiros inteiros n tais que $1+2+\cdots+n$ é um quadrado perfeito são 8, 288 e 9800.

7.31. Pretende-se mostrar que, se o período da representação de $\sqrt{d}$ (com d inteiro positivo que não é um quadrado perfeito) é ímpar então d é uma soma de dois quadrados.

Suponhamos então que $\sqrt{d}=[a_0,\dot{a}_1,a_2\ldots,a_k,a_k,\ldots,a_2,a_1,2\dot{a}_0]$.

Mostre que:

a) $\alpha_{k+1}=[\dot{a}_k,\ldots,a_2,a_1,2a_0,a_1,a_2,\ldots,\dot{a}_k]$.

b) (usando a Proposição 7.28) $\alpha_{k+1}=-\frac{1}{\overline{\alpha}_{k+1}}$.

c) $c_{k+1}^2+e_{k+1}^2=d$.

Nota: O reverso do que se diz acima não é verdadeiro. Por exemplo as fracções que representam $\sqrt{34}$, $\sqrt{650}$ e $\sqrt{9490}$ têm período par mas 34, 650 e 9490 são somas de quadrados. É conhecido que um inteiro positivo escreve-se como soma de dois quadrados se e só se na sua decomposição como produto de potências de primos diferentes os primos da forma $4k+3$ têm expoente par.

7.32. Usando o exercício anterior e as igualdades

$$\sqrt{84922}=[291,\dot{2},2,2,2,5\dot{8}2],\quad \sqrt{115202}=[339,\dot{2},2,2,2,2,2,6\dot{7}8]$$

escreva 84922 e 115202 como soma de dois quadrados.

7.33. Sejam $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, $k \in \mathbb{N}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$ tais que $b \leq q_k$. Sejam $m, n \in \mathbb{Z}$ definidos por

$$\begin{cases} m &= (-1)^k \quad (aq_k - bp_k) \\ n &= (-1)^{k+1}(aq_{k+1} - bp_{k+1}) \end{cases}$$

a) Mostre, usando o Corolário 9.5, alínea d), que

$$\begin{cases} a &= mp_{k+1} + np_k. \\ b &= mq_{k+1} + nq_k \end{cases}$$

b) Mostre que, $b\alpha - a = m(q_{k+1}\alpha - p_{k+1}) + n(q_k\alpha - p_k)$.

c) Mostre que m e n têm sinais contrários (isto é $mn \leq 0$) e que $m(q_{k+1}\alpha - p_{k+1})$ e $n(q_k\alpha - p_k)$ têm o mesmo sinal.

d) Mostre que $|b\alpha - a| \geq |q_k a - p_k|$.

e) Conclua que $|\alpha - \frac{a}{b}| \geq |\alpha - \frac{p_k}{q_k}|$ (ou seja, $\frac{p_k}{q_k}$ é uma "melhor aproximação"de α do que $\frac{a}{b}$).

f) Usando o facto de que $\pi = [3, 7, 15, 1, 292, 1, \ldots]$ calcule o número racional da forma $\frac{a}{b}$ com $a, b \in \mathbb{N}$ e $b \leq 113$ que melhor aproxima π.

7.34. Mostre que as seguintes equações não têm solução:

a) $x^2 - 311y^2 = -3$;

b) $x^4 - 121y^4 = -45$;

c) $x^4 - 441y^4 = -5991$;

7.35. Uma fracção contínua simples $[q_0, \cdots, q_n]$ diz-se simétrica se $q_i = q_{n-i}$ para todo o $i \in \{0, \cdots, n\}$ (por exemplo: $[3, 2, 1, 2, 3]$).

Mostre que se um número racional $\frac{r}{s}$, com $r, s \in \mathbb{N}$ e $(r, s) = 1$ possui uma representação simétrica, então r divide $s^2 + (-1)^n$.

7.36. Considere a equação $x^2 - dy^2 = n$, com d inteiro positivo não quadrado.

a) Mostre que, se $n = 4$, a equação tem sempre solução com $x, y \in \mathbb{N}$.

b) Mostre que, se $n = -1$ e d é um número primo, a equação tem solução se e só se $d = 2$ ou $d \equiv 1 \pmod 4$.

7.37. Seja $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Para cada $n \in \mathbb{N}$ seja $\varepsilon_n = \dfrac{q_{n-1}}{q_n}$.

a) Mostre que, se $k \in \mathbb{N}$, $a_{k+1} + \varepsilon_k = \dfrac{1}{\varepsilon_{k+1}}$.

b) Mostre que, se $k \in \mathbb{N}$,

$$\alpha - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k^2(\alpha_{k+1} + \varepsilon_k)}.$$

7.38. Com as notações do exercício anterior

a) Mostre que, se $k \in \mathbb{N}$,

$$\begin{cases} \alpha_{k+1} + \varepsilon_k & < & \sqrt{5} \\ \alpha_{k+2} + \varepsilon_{k+1} & < & \sqrt{5} \end{cases} \implies \quad \varepsilon_{k+1}^2 - \sqrt{5}\ \varepsilon_{k+1} + 1 < 0.$$

b) Conclua que

$$\forall k \in \mathbb{N}\ \exists i \in \{k, k+1, k+2\} : \quad \left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{\sqrt{5}\ q_i^2}.$$

(para os cálculos relacionados com a matéria deste capítulo pode usar, para além o Maple ou o Mathematica, o endereço http://www.bioinfo.rpi.edu/∼ zukerm/cgi-bin/dq.html para a resolução de congruências do tipo $x^2 - dy^2 = 1$ e o programa "contfrac" que pode ser encontrado em http://wims.unice.fr/wims/ para o cálculo das fracções contínuas e dos convergentes de números reais)