

João Filipe Queiró

TEORIA DOS NÚMEROS

Departamento de Matemática - Universidade de Coimbra
2008

As folhas que se seguem contêm um resumo das matérias estudadas na disciplina de Teoria dos Números. Esta disciplina constitui uma boa introdução ao raciocínio dedutivo, com as afirmações a serem rigorosamente demonstradas a partir de outras anteriores.

No presente texto, o fim de uma demonstração é assinalado pelo símbolo ■.

O estudante, seja na demonstração de resultados teóricos seja na resolução de problemas, deve exercitar-se na redacção de textos matemáticos e na correcta exposição de raciocínios lógicos.

Referências bibliográficas:

I. Niven, H. Zuckerman e H. Montgomery, *An Introduction to the Theory of Numbers*
5^a ed., New York, John Wiley & Sons, 1991.

G. Hardy e E. Wright, *An Introduction to the Theory of Numbers*
5^a ed., Oxford, Clarendon Press, 1979.

Índice

1. Os números inteiros	3
2. Divisibilidade nos inteiros	7
3. Os números primos	15
4. Congruências	23
5. Os Teoremas de Euler e Fermat	25
6. Congruências de grau 1. Teorema chinês dos restos	28
7. O Teorema de Wilson. Testes de primalidade	31
8. As funções $\varphi(n)$ e $\sigma(n)$	33
9. Equações Diofantinas	42
10. Aplicações da Teoria dos Números	52

1 Os números inteiros

Nesta disciplina vamos estudar o conjunto dos *números inteiros*

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Dentro dos inteiros vão interessar-nos em especial os *números naturais*

$$1, 2, 3, 4, 5, \dots$$

cujo conjunto denotaremos por $\mathbb{N}$.

Os números naturais intervêm nos processos de *contagem*, que são provavelmente as actividades matemáticas mais antigas e básicas.

Como ponto de partida para o nosso estudo, suporemos conhecidas as operações usuais de adição e multiplicação de números inteiros, bem como as respectivas propriedades:

- existência de elemento neutro para a adição (que é o número 0);
- existência de elemento neutro para a multiplicação (que é o número 1);
- existência de simétrico aditivo de qualquer elemento $a \in \mathbb{Z}$ (notação: $-a$);
- comutatividade e associatividade da adição:

$$\forall_{a,b \in \mathbb{Z}} \quad a + b = b + a \quad , \quad \forall_{a,b,c \in \mathbb{Z}} \quad (a + b) + c = a + (b + c) ;$$

- comutatividade e associatividade da multiplicação:

$$\forall_{a,b \in \mathbb{Z}} \quad ab = ba \quad , \quad \forall_{a,b,c \in \mathbb{Z}} \quad (ab)c = a(bc) ;$$

- distributividade da multiplicação em relação à adição:

$$\forall_{a,b,c \in \mathbb{Z}} \quad a(b + c) = ab + ac .$$

A notação $b - a$ significa $b + (-a)$.

Suporemos conhecida a relação de ordem usual nos inteiros, denotada pelo símbolo $<$. Dados dois inteiros a e b distintos, tem-se que ou $a < b$ ou $b < a$. A relação de ordem nos inteiros relaciona-se com as operações através das seguintes propriedades (onde a e b designam inteiros arbitrários):

- $a < b \wedge b < c \implies a < c$
- $a < b \implies a + c < b + c \quad \forall c \in \mathbb{Z}$
- $a < b \implies ac < bc \quad \forall c \in \mathbb{N}$

(Note-se que na segunda propriedade tem-se $c \in \mathbb{Z}$, e na terceira $c \in \mathbb{N}$.)

Usaremos também o símbolo $\leq$, assim definido: $a \leq b$ significa que $a < b \vee a = b$. A relação $\leq$ tem propriedades análogas às da relação $<$.

Admitiremos que em $\mathbb{N}$ é satisfeito o *princípio de boa ordenação*, que afirma que qualquer subconjunto de $\mathbb{N}$ não vazio possui elemento mínimo:

$$\forall S \subseteq \mathbb{N}, S \neq \emptyset \quad \exists m \in S \quad \forall s \in S \quad m \leq s.$$

Finalmente, admitiremos o *princípio de indução matemática*, que afirma o seguinte: Seja $P(n)$ uma afirmação sobre a variável natural n . Se $P(1)$ é verdadeira e, para todo o $k \in \mathbb{N}$, a verdade de $P(k)$ implica a verdade de $P(k+1)$, então $P(n)$ é verdadeira para todo o $n \in \mathbb{N}$.

Cada um destes dois princípios pode ser demonstrado a partir do outro:

Demonstração do princípio de indução matemática a partir do princípio de boa ordenação:

Seja $P(n)$ uma afirmação sobre a variável natural n tal que $P(1)$ é verdadeira e, para todo o $k \in \mathbb{N}$, a verdade de $P(k)$ implica a verdade de $P(k+1)$.

Vamos proceder por redução ao absurdo, isto é, vamos supor que $P(n)$ não é verdadeira para todo o $n \in \mathbb{N}$.

Então o conjunto

$$S = \{s \in \mathbb{N} : P(s) \text{ não é verdadeira}\}$$

é não vazio. Pelo princípio de boa ordenação, S possui elemento mínimo. Chamemos m ao elemento mínimo de S . Como $P(1)$ é verdadeira, m não pode ser 1, pelo que $m-1 \in \mathbb{N}$. Como $m-1 < m$ e m é o mínimo de S , tem-se que $m-1 \notin S$, pelo que $P(m-1)$ é verdadeira. Mas então, pela hipótese, $P(m-1+1)$ também tem que ser verdadeira, o que está em contradição com o facto de m pertencer a S . ■

Demonstração do princípio de boa ordenação a partir do princípio de indução matemática:

Seja S um subconjunto de $\mathbb{N}$ não vazio. Seja $P(n)$ a afirmação

$$\forall_{s \in S} \quad n \leq s .$$

$P(1)$ é verdadeira mas, como é evidente, $P(n)$ não é verdadeira para todo o $n \in \mathbb{N}$ (por exemplo, sendo $s \in S$, seguramente $P(s+1)$ é falsa, pois $s+1 > s$). Logo, pelo princípio de indução, podemos afirmar que existe $k \in \mathbb{N}$ tal que $P(k)$ é verdadeira e $P(k+1)$ é falsa. Vamos ver que tal k é necessariamente o mínimo de S . Por um lado, como $P(k)$ é verdadeira, tem-se $k \leq s$ para todo o $s \in S$. Por outro lado, tem-se que $k \in S$; se não, ter-se-ia $k < s$ para todo o $s \in S$, e portanto $k+1 \leq s$ para todo o $s \in S$, e $P(k+1)$ seria verdadeira: contradição. Como $k \in S$ e $k \leq s$ para todo o $s \in S$, tem-se que k é o mínimo de S . ■

O princípio de indução matemática tem várias variantes úteis, de que registamos duas.

Primeira variante do princípio de indução matemática: Seja $P(n)$ uma afirmação sobre a variável natural n . Se $P(1)$ é verdadeira e, para todo o $k \in \mathbb{N}$, a verdade de $P(1), P(2), \dots, P(k)$ implica a verdade de $P(k+1)$, então $P(n)$ é verdadeira para todo o $n \in \mathbb{N}$.

Segunda variante do princípio de indução matemática: Seja $a \in \mathbb{N}$. Seja $P(n)$ uma afirmação sobre a variável natural $n \geq a$. Se $P(a)$ é verdadeira e, para todo o $k \geq a$, a verdade de $P(k)$ implica a verdade de $P(k+1)$, então $P(n)$ é verdadeira para todo o $n \geq a$.

Exercício. Demonstre estas duas variantes do princípio de indução matemática a partir do princípio de boa ordenação.

Como acima se disse, o conjunto de propriedades que reunimos até aqui é o ponto de partida para o nosso estudo dedutivo dos números inteiros. Mas seria possível começar “mais de trás”, por exemplo com a chamada *axiomática de Peano*, que inicia o estudo do conjunto $\mathbb{N}$ a partir do seguinte conjunto de *afirmações primitivas* ou *axiomas* :

- $1 \in \mathbb{N}$
- A cada $n \in \mathbb{N}$ faz-se corresponder um único natural a que se chama o *sucessor* de n (notação: $\text{suc}(n)$)
- $\forall_{n \in \mathbb{N}} \quad \text{suc}(n) \neq 1$
- $\text{suc}(m) = \text{suc}(n) \implies m = n$
- Se um subconjunto S de $\mathbb{N}$ satisfaz $1 \in S$ e $k \in S \implies \text{suc}(k) \in S$, então $S = \mathbb{N}$.

A partir destes axiomas é possível definir todos os conceitos e demonstrar todas as propriedades acima mencionados.¹

¹O leitor interessado pode consultar, por exemplo, a obra de E. Landau *Foundations of Analysis*, 3rd ed., Chelsea, New York, 1966.

2 Divisibilidade nos inteiros

Definição. Dados inteiros a e b , com $a \neq 0$, dizemos que a *divide* b (ou a é um *divisor* de b , ou b é *múltiplo* de a , ou b é *divisível* por a) se existir um inteiro x tal que $b = ax$. A notação que usamos para esta relação é $a \mid b$. Se a não dividir b escrevemos $a \nmid b$.

Exemplos. Tem-se que $2 \mid 6$, porque $6 = 2 \cdot 3$, mas $2 \nmid 5$, porque não existe nenhum número inteiro que multiplicado por 2 dê 5. Note-se que, por convenção, numa relação $a \mid b$ nunca admitimos $a = 0$.

Observação. O interesse da relação de divisibilidade está em ser definida nos inteiros. Se a apresentássemos nos números racionais, ou nos reais, a relação perdia o interesse, porque qualquer número dividiria qualquer outro. Por exemplo, dentro dos racionais podemos escrever $5 = 2 \cdot \frac{5}{2}$.

Propriedades.

- $\forall a \in \mathbb{Z} \quad a \mid 0; \quad \forall a \in \mathbb{Z} \quad a \mid a \text{ e } -a \mid a; \quad \forall a \in \mathbb{Z} \quad 1 \mid a$
- $a \mid b \iff -a \mid b \iff a \mid -b$
- $\forall m \neq 0 \quad a \mid b \iff ma \mid mb$
- $a \mid b \wedge b \mid c \implies a \mid c$
- $\forall x, y \in \mathbb{Z} \quad a \mid b \wedge a \mid c \implies a \mid bx + cy$
- $\forall c \in \mathbb{Z} \quad a \mid b \implies a \mid bc$
- $a \mid 1 \implies a = \pm 1$
- $a \mid b \wedge b \mid a \implies a = \pm b$
- Se $a, b \in \mathbb{N}$ e $a \mid b$, então $a \leq b$
- Um inteiro não nulo tem um número finito de divisores

Demonstração. Exercício. ■

Teorema. (Divisão inteira.) Sendo a e b inteiros, com $a > 0$, existem inteiros q e r , com $0 \leq r < a$, tais que

$$b = qa + r.$$

Os inteiros q e r , designados, respectivamente, por *quociente* e *resto* da divisão de b por a , são unicamente determinados por a e b .

Demonstração. Consideremos o conjunto

$$\{\dots, b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, \dots\}.$$

Este conjunto contém de certeza inteiros não negativos. Designemos por r o menor deles. Então r é da forma $b - qa$ para certo inteiro q , donde $b = qa + r$. Pela sua própria definição, tem-se que $r \geq 0$. Vejamos agora que $r < a$. Se se tivesse $r \geq a$, o inteiro $r - a$, que pertence ao conjunto acima referido, seria não negativo. Como $r - a < r$, isto iria contra a definição de r .

Provemos agora a unicidade de q e r . Suponhamos que também se tem $b = q_1a + r_1$, com $0 \leq r_1 < a$. Vamos ver primeiro que é de certeza $r_1 = r$. Suponhamos que se tinha $r_1 > r$ (no caso $r_1 < r$ o raciocínio seria análogo). Então $r_1 - r > 0$ e, claramente, $r_1 - r < a$, já que $r < a$ e $r_1 < a$. Mas, por outro lado, tem-se

$$r_1 - r = b - q_1a - (b - qa) = (q - q_1)a$$

donde $a \mid r_1 - r$, pelo que não pode ter-se $r_1 - r < a$. Portanto, tem que ser $r_1 = r$, e daqui sai que $q_1a = qa$, donde $q_1 = q$. ■

Observações.

1. Na prática, dados $a, b \in \mathbb{N}$, o quociente e o resto da divisão de b por a obtêm-se pelo conhecido algoritmo que se aprende na instrução primária.
2. Se $a < 0$, a divisão inteira de b por a também é possível, bastando proceder à divisão de b por $-a$ e depois trocar o sinal ao quociente. A condição sobre o resto é portanto, no caso geral, $0 \leq r < |a|$.

Sejam b e c dois inteiros. Um inteiro a é um *divisor comum* de b e c se os dividir a ambos. Se b e c forem ambos iguais a zero, todos os inteiros (não nulos) são divisores comuns de b e c . Mas se b e c não forem ambos nulos, o número de divisores comuns de b e c é finito.

Definição. Sejam b e c inteiros não ambos nulos. Ao maior dos divisores comuns de b e c chama-se *máximo divisor comum* de b e c . A notação é (b, c) .

Observações. 1) O máximo divisor comum de dois inteiros não ambos nulos existe e é um inteiro positivo.

2) Outra notação habitual para o máximo divisor comum de b e c é $\text{mdc}(b, c)$.

Teorema. Sejam b e c inteiros não ambos nulos, e seja d o seu máximo divisor comum. Então existem inteiros x_0 e y_0 tais que

$$d = bx_0 + cy_0.$$

Demonstração. Consideremos o conjunto

$$C = \{bx + cy : x, y \in \mathbb{Z}\}.$$

Este conjunto contém de certeza inteiros positivos. Seja t o menor desses elementos positivos de C . Então t é da forma $bx_0 + cy_0$ para certos inteiros x_0 e y_0 . Vamos ver que $t = d$.

Começemos por mostrar que $t \mid b$. Procedendo à divisão inteira de b por t obtemos $b = qt + r$, com $0 \leq r < t$. Tem-se que

$$r = b - qt = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0)$$

que é um elemento do conjunto C . Se r fosse positivo, seria um elemento de C positivo menor do que t , contra a definição deste. Logo, r tem que ser zero, o que significa que a divisão de b por t é exacta, isto é, que $t \mid b$.

Com um raciocínio análogo prova-se que $t \mid c$. Logo, t é um divisor comum de b e c .

Para vermos que $t = d$ basta observar que d , sendo um divisor comum de b e c , tem que dividir $bx_0 + cy_0$, isto é, tem que dividir t . Logo, tem-se $d \leq t$. Como d é o máximo divisor comum de b e c , tem que ser $d = t$. ■

Observações. 1) Da demonstração deste teorema concluímos que o máximo divisor comum de dois inteiros b e c tem as seguintes caracterizações alternativas:

- é o menor elemento positivo do conjunto $\{bx + cy : x, y \in \mathbb{Z}\}$ e divide todos os elementos desse conjunto;
- é um divisor comum positivo de b e c que é múltiplo de qualquer outro divisor comum de b e c .

2) Sendo b e c dois inteiros, se existirem $x, y \in \mathbb{Z}$ tais que $bx + cy = 1$, podemos concluir que $(b, c) = 1$, pela primeira das caracterizações alternativas do máximo divisor comum acima referidas. Se tivermos $bx + cy = t$ com $t > 1$ apenas podemos concluir que $(b, c) \mid t$.

Proposição. Sejam b e c inteiros não ambos nulos.

1. Sendo $m \in \mathbb{N}$, tem-se $(mb, mc) = m(b, c)$.
2. Se t for um divisor comum positivo de b e c , tem-se $\left(\frac{b}{t}, \frac{c}{t}\right) = \frac{1}{t}(b, c)$.

Demonstração. 1. Tem-se

$$\begin{aligned}(mb, mc) &= \min(\mathbb{N} \cap \{mbx + mcy : x, y \in \mathbb{Z}\}) \\ &= m \cdot \min(\mathbb{N} \cap \{bx + cy : x, y \in \mathbb{Z}\}) = m(b, c).\end{aligned}$$

2. Usando 1., vemos que

$$(b, c) = \left(t \frac{b}{t}, t \frac{c}{t}\right) = t \left(\frac{b}{t}, \frac{c}{t}\right)$$

o que prova a igualdade pretendida. ■

Outras propriedades do máximo divisor comum:

- $(b, 0) = |b|$
- $(b, c) = (c, b) = (b, -c)$
- $\forall f \in \mathbb{Z} \quad (b, c) = (b, c + bf)$

Demonstração. Exercício. ■

Proposição. $c \mid ab \wedge (b, c) = 1 \implies c \mid a$.

Demonstração. Tem-se $ab = qc$ e $bx + cy = 1$ para certos inteiros q, x, y . Vem então $a = a(bx + cy) = abx + acy = qcx + acy = (qx + ay)c$ e, portanto, $c \mid a$. ■

Corolário. $b \mid a \wedge c \mid a \wedge (b, c) = 1 \implies bc \mid a$.

Demonstração. Exercício. ■

Definição. Se $(b, c) = 1$ dizemos que b e c são *primos entre si* (ou que b é *primo com* c).

Teorema. (Algoritmo de Euclides para a determinação do máximo divisor comum.)
Sejam b e c inteiros. Sem perda de generalidade, podemos supor $b, c \in \mathbb{N}$ e $b > c$.
Proceda-se à seguinte sequência de divisões inteiras:

$$\begin{aligned} b &= q_1c + r_1, \quad 0 < r_1 < c \\ c &= q_2r_1 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= q_3r_2 + r_3, \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{k-2} &= q_kr_{k-1} + r_k, \quad 0 < r_k < r_{k-1} \\ r_{k-1} &= q_{k+1}r_k. \end{aligned}$$

Então r_k (o último resto não nulo) é o máximo divisor comum de b e c .

Demonstração. Começamos por observar que, de facto, na sequência de divisões, os restos não podem permanecer sempre positivos, porque cada um é menor do que o anterior.

Designemos o máximo divisor comum de b e c por d . Vamos ver que $r_k = d$.

Da última das igualdades acima indicadas concluímos que $r_k \mid r_{k-1}$. Desse facto e da penúltima igualdade concluímos que $r_k \mid r_{k-2}$. Da antepenúltima segue-se então que $r_k \mid r_{k-3}$. Prosseguindo desta forma, concluímos que $r_k \mid c$ e, finalmente, da primeira igualdade, que $r_k \mid b$. Então r_k é um divisor comum de b e c e, portanto, $r_k \mid d$.

Como $d \mid b$ e $d \mid c$, da primeira igualdade tira-se que $d \mid r_1$. Da segunda sai então que $d \mid r_2$. Prosseguindo desta forma, concluímos que $d \mid r_k$.

Como $r_k \mid d$ e $d \mid r_k$ e ambos são positivos, tem-se que $r_k = d$. ■

Observação. O algoritmo de Euclides permite também achar inteiros x e y tais que $d = bx + cy$. Da penúltima igualdade tiramos

$$d = r_{k-2} - q_k r_{k-1} .$$

Da antepenúltima sai então que

$$d = -q_k r_{k-3} + (1 + q_k q_{k-1}) r_{k-2} .$$

Prosseguindo desta forma, chegamos a uma igualdade da forma $d = bx + cy$.

Definição. Sejam b e c inteiros não nulos. Ao menor dos múltiplos comuns positivos de b e c chama-se *menor múltiplo comum* de b e c . A notação é $[b, c]$.

Observações. 1) O menor múltiplo comum de dois inteiros não nulos existe e é um inteiro positivo.

2) Outra notação habitual para o menor múltiplo comum de b e c é $\text{mmc}(b, c)$.

Teorema. Sejam b e c inteiros não nulos. Se s for um múltiplo comum de b e c , então é múltiplo de $[b, c]$.

Demonstração. Ponhamos $[b, c] = h$. Dividamos s por h :

$$s = qh + r, \quad 0 \leq r < h .$$

Daqui sai que $r = s - qh$ e, portanto, r é um múltiplo comum de b e c (por s e h o serem). Como é menor do que h , não pode ser positivo, pela definição de h . Logo, tem-se $r = 0$, isto é, $h \mid s$. ■

Observação. Este teorema afirma que o menor múltiplo comum de dois inteiros b e c tem a seguinte caracterização alternativa: é um múltiplo comum positivo de b e c que divide qualquer outro múltiplo comum de b e c .

Proposição. Sejam b e c inteiros não nulos.

1. Sendo $m \in \mathbb{N}$, tem-se $[mb, mc] = m[b, c]$.
2. Se t for um divisor comum positivo de b e c , tem-se $\left[\frac{b}{t}, \frac{c}{t}\right] = \frac{1}{t}[b, c]$.

Demonstração. 1. Ponhamos $[b, c] = h$. Como mh é um múltiplo comum de mb e mc , é múltiplo de $[mb, mc]$. Vejamos agora que $[mb, mc]$ é múltiplo de mh . Tem-se $[mb, mc] = t_1mb = t_2mc$. O número $t_1b = t_2c$ é um múltiplo comum de b e c , logo é múltiplo de h , e portanto $[mb, mc]$ é múltiplo de mh .

2. Exercício. ■

Teorema. Sendo b e c inteiros não nulos, tem-se $[b, c] \cdot (b, c) = |bc|$.

Demonstração. Sem perda de generalidade, supomos que b e c são ambos positivos.

1º caso: b e c são primos entre si. Pretendemos neste caso mostrar que $[b, c] = bc$. Como b divide $[b, c]$, tem-se $[b, c] = qb$. Como c também divide $[b, c]$, tem-se que $c \mid qb$. Uma vez que b e c são primos entre si, segue-se, por uma proposição vista anteriormente, que $c \mid q$, isto é, que $q = tc$, com $t \in \mathbb{N}$. Vem então que $[b, c] = tbc$ e, portanto, $[b, c] \geq bc$. Sendo $[b, c]$, por definição, o menor dos múltiplos comuns positivos de b e c e sendo bc um múltiplo comum positivo de b e c , só pode ser $[b, c] = bc$.

2º caso: Suponhamos $(b, c) = d > 1$. Então $\left(\frac{b}{d}, \frac{c}{d}\right) = 1$. Pelo primeiro caso, tem-se

$$\left[\frac{b}{d}, \frac{c}{d}\right] \left(\frac{b}{d}, \frac{c}{d}\right) = \frac{b}{d} \cdot \frac{c}{d}.$$

Multiplicando ambos os membros por d^2 obtém-se $[b, c] (b, c) = bc$, como desejado. ■

Observação. Este teorema fornece um processo de cálculo do menor múltiplo comum de dois inteiros, reduzindo-o ao do cálculo do seu máximo divisor comum, para o qual dispomos do algoritmo de Euclides.

O resultado permite também obter propriedades do menor múltiplo comum a partir de propriedades do máximo divisor comum.

Os conceitos de máximo divisor comum e menor múltiplo comum definem-se também para mais de dois inteiros.

Definição. Sejam $b_1, b_2, \dots, b_n$ inteiros não todos nulos. Ao maior dos divisores comuns de $b_1, b_2, \dots, b_n$ chama-se máximo divisor comum de $b_1, b_2, \dots, b_n$. A notação é $(b_1, b_2, \dots, b_n)$.

Proposição. Sejam $b_1, b_2, \dots, b_n$ inteiros não todos nulos, e seja d o seu máximo divisor comum. Então existem inteiros $x_1, x_2, \dots, x_n$ tais que

$$d = b_1x_1 + b_2x_2 + \dots + b_nx_n.$$

Além disso, d é o menor inteiro positivo que se escreve dessa forma. d pode ainda ser caracterizado como um divisor comum positivo de $b_1, b_2, \dots, b_n$ que é múltiplo de qualquer outro divisor comum de $b_1, b_2, \dots, b_n$.

Demonstração. Exercício. ■

Exercício. Prove que $(b_1, b_2, \dots, b_n) = ((b_1, b_2, \dots, b_{n-1}), b_n)$.

Definição. Os inteiros $b_1, b_2, \dots, b_n$ dizem-se *primos entre si* se $(b_1, b_2, \dots, b_n) = 1$. Os inteiros $b_1, b_2, \dots, b_n$ dizem-se *primos dois a dois* se $(b_i, b_j) = 1$ sempre que $i \neq j$.

Exercício. Prove que, se $b_1, b_2, \dots, b_n$ forem primos dois a dois, então são primos entre si. Dê um exemplo que mostre que a implicação recíproca não é verdadeira.

Definição. Sejam $b_1, b_2, \dots, b_n$ inteiros não nulos. Ao menor dos múltiplos comuns positivos de $b_1, b_2, \dots, b_n$ chama-se menor múltiplo comum de $b_1, b_2, \dots, b_n$. A notação é $[b_1, b_2, \dots, b_n]$.

Proposição. O menor múltiplo comum de $b_1, b_2, \dots, b_n$ é um múltiplo comum positivo de $b_1, b_2, \dots, b_n$ que divide qualquer outro múltiplo comum de $b_1, b_2, \dots, b_n$.

Demonstração. Exercício. ■

3 Os números primos

Definição. Um número inteiro $p > 1$ diz-se um *número primo* se não existir nenhum divisor d de p satisfazendo $1 < d < p$. Por outras palavras, um número inteiro $p > 1$ é primo se não tiver outros divisores positivos além de 1 e dele próprio. Se um número inteiro $a > 1$ não for primo diz-se *composto*.

Exemplos. Os primeiros números primos são

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \dots$$

A importância dos números primos vem de que qualquer número natural (excepto 1) é um produto de números primos.

Teorema. Qualquer número natural $a > 1$ é um produto de números primos.

Demonstração. Seja $a \in \mathbb{N}$, $a > 1$. Se a for primo, não há nada a provar (temos um produto com um só factor). Suponhamos que a é composto. Então a tem divisores entre 1 e a . Se m for o menor destes divisores, m é de certeza primo (porque, se não, teria divisores menores do que m que seriam também divisores de a). Designemos m por p_1 . Então tem-se

$$a = p_1 a_1$$

com p_1 primo e $1 < a_1 < a$. Se a_1 for primo, já chegámos à conclusão desejada. Se a_1 for composto, repetindo o raciocínio anterior concluimos que a_1 tem um divisor primo p_2 satisfazendo $1 < p_2 < a_1$, donde

$$a = p_1 p_2 a_2$$

com p_1 e p_2 primos e $1 < a_2 < a_1 < a$.

Prosseguindo desta forma, obtemos números naturais $a > a_1 > a_2 > \dots$. Como uma sucessão de números naturais não pode decrescer indefinidamente, há-de haver um momento em que um destes números é primo, digamos p_s , pelo que

$$a = p_1 p_2 \dots p_s. \blacksquare$$

Lema. Se um número primo dividir um produto de números inteiros, tem que dividir pelo menos um dos factores.

Demonstração. Seja p um número primo. Vamos provar que, sendo n um natural qualquer ≥ 2 , se p dividir um produto de n números inteiros, então tem que dividir pelo menos um dos factores.

Vamos proceder por indução. O primeiro caso é $n = 2$. Sejam então a_1, a_2 dois inteiros quaisquer e suponhamos que $p \mid a_1 a_2$. Se p dividir a_1 , não há mais nada a demonstrar. Se p não dividir a_1 , então p e a_1 são primos entre si, porque p não tem outros divisores positivos senão 1 e ele próprio. Então, por uma proposição vista na secção anterior, de certeza que $p \mid a_2$.

Suponhamos agora que a afirmação é verdadeira para produtos de k factores e sejam $a_1, a_2, \dots, a_{k+1}$ inteiros quaisquer tais que $p \mid a_1 a_2 \cdots a_{k+1}$. Se p dividir a_{k+1} , não há mais nada a demonstrar. Se p não dividir a_{k+1} , então, pelo mesmo raciocínio do primeiro caso, p tem que dividir o produto $a_1 a_2 \cdots a_k$ e portanto, pela hipótese de indução, tem que dividir um dos inteiros $a_1, a_2, \dots, a_k$. ■

Teorema. (Teorema Fundamental da Aritmética) Qualquer número natural > 1 escreve-se de forma única como um produto de números primos.

Demonstração. Tomemos um número natural > 1 qualquer. Já sabemos que ele se escreve como um produto de números primos. Suponhamos que era possível escrevê-lo como produto de números primos de duas maneiras diferentes:

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

factorizações em que podemos supor já retirados os factores comuns, de modo que não haja nenhum primo que figure em ambos os membros.

Como p_1 divide o primeiro membro, divide também o segundo, isto é, $p \mid q_1 q_2 \cdots q_t$. Pelo lema anterior, segue-se que p_1 tem que dividir um dos factores do segundo membro, digamos $p \mid q_j$. Como ambos os números são primos, isto só pode acontecer se $p_1 = q_j$, o que contradiz o facto de não haver primos comuns nas duas factorizações. ■

Claro que os factores primos de um número natural a não têm que ser todos distintos. Juntando os primos iguais, podemos dizer que qualquer número natural $a > 1$ se pode escrever, de uma única maneira, na forma $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ onde $p_1, p_2, \dots, p_k$ são primos distintos e os expoentes $\alpha_1, \alpha_2, \dots, \alpha_k$ são números naturais. De um número escrito desta maneira dizemos que está na *forma canónica*.

Dados dois números naturais a e b , pode interessar, em certas situações, escrevê-los como produtos de potências dos mesmos primos. Basta para isso admitir expoentes nulos:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

com $\alpha_1 \geq 0, \alpha_2 \geq 0, \dots, \alpha_k \geq 0, \beta_1 \geq 0, \beta_2 \geq 0, \dots, \beta_k \geq 0$.

Exemplo. $108 = 2^2 3^3 5^0$, $225 = 2^0 3^2 5^2$.

Proposição. Sejam $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ números naturais. Então tem-se $a \mid b$ se e só se $\alpha_i \leq \beta_i$, $i = 1, 2, \dots, k$.

Demonstração. ($\Leftarrow$) Se $\alpha_i \leq \beta_i$, $i = 1, 2, \dots, k$ é evidente que $a \mid b$ (o quociente é $p_1^{\beta_1 - \alpha_1} p_2^{\beta_2 - \alpha_2} \cdots p_k^{\beta_k - \alpha_k}$).

($\Rightarrow$) Reciprocamente, suponhamos que $a \mid b$. Então $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} = q \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ para certo número natural q . Se se tivesse $\alpha_j > \beta_j$ para algum j , o primo p_j apareceria mais vezes como factor no segundo membro do que no primeiro membro, contra a unicidade da factorização de um número natural como produto de primos. ■

Corolário. Sejam $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ e $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ números naturais. Então tem-se $(b, c) = p_1^{\min\{\beta_1, \gamma_1\}} p_2^{\min\{\beta_2, \gamma_2\}} \cdots p_k^{\min\{\beta_k, \gamma_k\}}$ e $[b, c] = p_1^{\max\{\beta_1, \gamma_1\}} p_2^{\max\{\beta_2, \gamma_2\}} \cdots p_k^{\max\{\beta_k, \gamma_k\}}$.

Demonstração. Exercício.

Exemplo. $(108, 225) = 2^0 3^2 5^0 = 9$, $[108, 225] = 2^2 3^3 5^2 = 2700$.

Observação. Como processo geral de determinar o m.d.c. de dois números, o algoritmo de Euclides é mais eficaz do que o método baseado neste Corolário, dado que este exige o conhecimento da factorização dos dois números como produtos de primos, o que pode ser trabalhoso.

Definição. Sendo a um número natural, designamos por $\tau(a)$ o número de divisores positivos de a (incluindo 1 e a).

Exemplos. $\tau(5) = 2$, $\tau(6) = 4$.

Proposição. Seja $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ um número natural. Então tem-se

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

Demonstração. Pela proposição anterior, a forma geral dos divisores de a é

$$p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

com $0 \leq \gamma_1 \leq \alpha_1$, $0 \leq \gamma_2 \leq \alpha_2$, ... $0 \leq \gamma_k \leq \alpha_k$. Quantos são os números naturais desta forma? Para o expoente γ_1 há exactamente $\alpha_1 + 1$ possibilidades, que são $0, 1, \dots, \alpha_1$. Para cada uma destas possibilidades, há $\alpha_2 + 1$ escolhas possíveis para γ_2 . E assim sucessivamente, até γ_k , para o qual há $\alpha_k + 1$ possibilidades, número que se deve multiplicar pelo produto dos anteriores. O número total de possibilidades para a sequência de expoentes $\gamma_1, \gamma_2, \dots, \gamma_k$ é portanto $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$. ■

Exemplo. $\tau(108) = \tau(2^2 3^3) = (2 + 1)(3 + 1) = 12$. Isto é, 108 tem 12 divisores positivos.

Teorema.² Existe uma infinidade de números primos.

Demonstração. Suponhamos que havia apenas um número finito de números primos, digamos $p_1, p_2, \dots, p_k$. Designemos por n o número natural $p_1 p_2 \cdots p_k + 1$. Como n é maior do que todos os primos $p_1, p_2, \dots, p_k$, tem que ser divisível pelo menos por um deles, porque n é um produto de primos. Suponhamos que n é divisível por p_1 (se for por qualquer outro o raciocínio é análogo). Então $n = qp_1$ para certo inteiro q . Daqui tira-se que

$$p_1(q - p_2 \cdots p_k) = 1$$

e p_1 dividiria 1, o que é impossível. ■

² Euclides, *Elementos*, Livro IX, Proposição 20. A demonstração que apresentamos é, em linguagem moderna, a original de Euclides.

São conhecidas várias demonstrações deste teorema. Uma demonstração muito simples foi descoberta recentemente:

Segunda demonstração.¹ Seja N_1 um número natural qualquer maior que 1. Então N_1 é de certeza divisível por um número primo. Como N_1 e $N_1 + 1$ são primos entre si, o número $N_2 = N_1(N_1 + 1)$ tem que ser divisível por dois números primos diferentes. Analogamente, como N_2 e $N_2 + 1$ são primos entre si, o número $N_3 = N_2(N_2 + 1)$ tem que ser divisível por três números primos diferentes. Como este processo pode ser continuado indefinidamente, existe uma infinidade de números primos. ■

Não existe nenhuma fórmula (pelo menos simples) que dê todos os números primos, nem nenhum processo geral prático de os identificar.² Um processo sistemático de construir listas de primos é devido ao matemático grego Eratóstenes (276-194 a.C.).

Lema. Se um número n for composto, tem de certeza um factor primo $\leq \sqrt{n}$.

Demonstração. O produto de dois (ou mais) números $> \sqrt{n}$ é maior que n . ■

Crivo de Eratóstenes. Escrevemos alguns termos da sucessão dos números naturais a partir de 2. Sublinhamos o 2 e cortamos todos os seus múltiplos: 4, 6, 8,... . Agora sublinhamos o primeiro número não cortado, que é o 3, e cortamos todos os seus múltiplos ainda não cortados: 9, 15, 21,... . De novo sublinhamos o primeiro número não cortado, neste caso o 5, e cortamos todos os seus múltiplos ainda não cortados: 25, 35, 55,... . Prosseguindo desta forma é óbvio que vamos obtendo, sublinhados, os vários números primos. Se quisermos conhecer todos os primos até um dado número n , basta, pelo lema anterior, que repitamos o processo até sublinharmos um número $\geq \sqrt{n}$. Depois disso, todos os números não cortados até n são primos e só resta sublinhá-los.

¹ F. Saidak, *A New Proof of Euclid's Theorem*, The American Mathematical Monthly 113 (2006), 937-938.

² É por essa razão que é difícil encontrar números primos muito grandes. O maior número primo actualmente conhecido foi descoberto por Edson Smith em 23 de Agosto de 2008. O número é $2^{43112609}-1$. Tem 12978189 algarismos. Havia um prémio de 100000 dólares da Electronic Frontier Foundation para a primeira pessoa que descobrisse um número primo com dez milhões de algarismos.

Os números primos parecem distribuir-se irregularmente entre os números naturais. Por exemplo, por um lado conjectura-se (sem que ninguém o tenha conseguido provar até hoje) que há uma infinidade de pares de “primos gémeos”, isto é, pares de primos que diferem de duas unidades (como 3 e 5, 17 e 19, 4967 e 4969). Por outro lado, há lacunas de comprimento arbitrariamente grande na sucessão dos primos, como mostra o resultado seguinte.

Proposição. Qualquer que seja $k \in \mathbb{N}$, é possível achar k números compostos seguidos.

Demonstração. Os k números

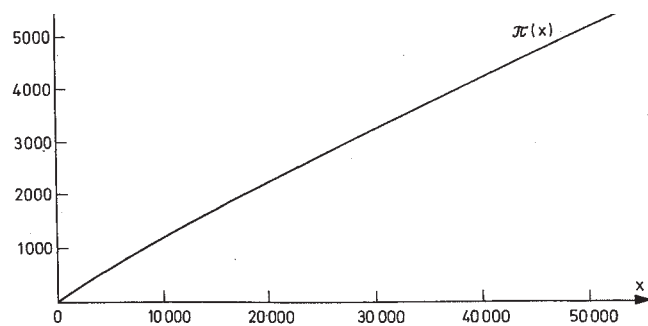
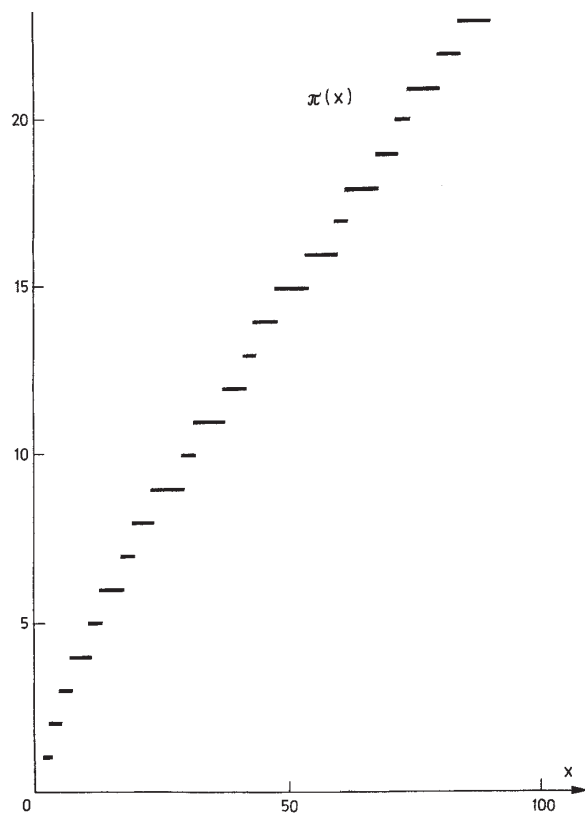
$$(k+1)! + 2, (k+1)! + 3, \dots, (k+1)! + k, (k+1)! + k + 1$$

são seguidos e são todos compostos (o primeiro é divisível por 2, o segundo por 3, etc., até ao último, que é divisível por $k+1$). ■

E, no entanto, *existe* uma grande regularidade na distribuição dos números primos. Isso nota-se se abstrairmos dos primos tomados individualmente e atentarmos apenas na frequência *média* com que eles surgem por entre os números naturais. Por exemplo: nos cinco primeiros milhares de números naturais existem, respectivamente, 168, 135, 127, 120 e 119 primos. Nos últimos cinco milhares antes de 10000000 aparecem, respectivamente, 62, 58, 67, 64 e 63. O que se constata analisando tabelas de primos é um ligeiro e gradual decréscimo do número de primos em cada milhar de números naturais.

Precisemos estas observações: para cada número real positivo x , designemos por $\pi(x)$ o número de primos que são $\leq x$. Assim, por exemplo, $\pi(1) = 0$, $\pi(7/2) = 2$, $\pi(10) = 4$, $\pi(11) = 5$, etc. Obter uma expressão exacta para esta função seria tão difícil como obter uma fórmula para os primos. Mas vejamos qual é o seu comportamento “macroscópico”. Nas figuras seguintes¹ temos representações gráficas da função $\pi(x)$ para $x \leq 100$ e $x \leq 50000$ (usando unidades diferentes nos dois eixos para se ver melhor o que se passa).

¹ D. Zagier, *The First 50 Million Prime Numbers*, The Mathematical Intelligencer 0 (1977), 7-19.



A regularidade com que $\pi(x)$ cresce foi detectada por Gauss, ainda jovem. Analisando tabelas de primos, Gauss apercebeu-se da proximidade entre $\pi(x)$ e a função $\frac{x}{\log x}$.

Na tabela seguinte comparam-se alguns valores de $\pi(x)$ e de $\frac{x}{\log x}$ (estes arredondados para o inteiro mais próximo).

x	$\pi(x)$	$\frac{x}{\log x}$
10	4	4
100	25	22
1000	168	145
2000	303	263
3000	430	375
4000	550	482
5000	669	587

No final do século XIX, Hadamard e La Vallée Poussin, independentemente um do outro, demonstraram o seguinte resultado, conhecido por *Teorema dos Números Primos*:¹

Teorema. Tem-se $\lim_{x \rightarrow +\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$.

Posteriormente descobriram-se ainda melhores aproximações para a função $\pi(x)$.

¹ A demonstração deste teorema está fora do âmbito desta disciplina.

4 Congruências

Definição. Seja m um número natural. Dois inteiros a e b dizem-se *congruentes módulo m* se tiverem o mesmo resto na divisão por m . A notação é $a \equiv b \pmod{m}$.

Proposição. Tem-se $a \equiv b \pmod{m}$ se e só se $m \mid a - b$.

Demonstração. ($\implies$) Se $a \equiv b \pmod{m}$, então a e b têm o mesmo resto na divisão por m , digamos $a = qm + r$ e $b = q'm + r$. Segue-se que $a - b = (q - q')m$, donde $m \mid a - b$.

($\impliedby$) Suponhamos que $a = qm + r$ e $b = q'm + r'$ para certos inteiros q e q' , e $0 \leq r < m$, $0 \leq r' < m$. Queremos provar que $r = r'$. Suponhamos que isso não acontece, sendo por exemplo $r' < r$ (se fosse $r' > r$ o raciocínio era análogo). Então tem-se $a - b = (q - q')m + (r - r')$ e, além disso, $0 < r - r' < m$. Isto significa que o resto da divisão de $a - b$ por m não é zero, contra a hipótese. ■

Observações. 1) Dado um natural m e um inteiro a , os números congruentes com a módulo m são os inteiros da forma $a + km$, $k \in \mathbb{Z}$.

2) a é congruente módulo m com o seu resto na divisão por m .

3) Dizer que $a \equiv 0 \pmod{m}$ é a mesma coisa que dizer que $m \mid a$.

Propriedades da relação de congruência. Seja $m \in \mathbb{N}$. Quaisquer que sejam os inteiros indicados, tem-se:

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$
- $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \implies a + c \equiv b + d \pmod{m}$
- $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$
- $a \equiv b \pmod{m} \wedge d \mid m \implies a \equiv b \pmod{d}$

Demonstração. Exercício.

Observações. 1) As três primeiras propriedades significam que a relação de congruência módulo um natural m é uma *relação de equivalência* em $\mathbb{Z}$. As classes de equivalência em que esta relação particiona o conjunto $\mathbb{Z}$ dos números inteiros chamam-se *classes de congruência módulo m* . Como os restos possíveis na divisão por m são em número de m , vemos que há exactamente m classes de congruência módulo m . A classe de congruência módulo m de um inteiro a costuma representar-se por $[a]_m$, ou simplesmente $[a]$ se o natural m estiver implícito do contexto. Outra notação comum para essa classe é $\bar{a}$. O conjunto das classes de congruência módulo m designa-se por $\mathbb{Z}_m$. Os elementos de $\mathbb{Z}_m$ são portanto os m conjuntos

$$[0]_m = \{\dots, -3m, -2m, -m, 0, m, 2m, 3m, \dots\}$$

$$[1]_m = \{\dots, -3m+1, -2m+1, -m+1, 1, m+1, 2m+1, 3m+1, \dots\}$$

$$\vdots$$

$$[m-1]_m = \{\dots, -2m-1, -m-1, -1, m-1, 2m-1, 3m-1, 4m-1, \dots\}$$

2) Da quinta propriedade indicada segue-se que se $a \equiv b \pmod{m}$ então $a^k \equiv b^k \pmod{m}$ para qualquer expoente k .

Outras propriedades:

- $a \equiv b \pmod{m} \implies (a, m) = (b, m)$
- $a \equiv b \pmod{m_1} \wedge a \equiv b \pmod{m_2} \implies a \equiv b \pmod{[m_1, m_2]}$

Demonstração. Exercício.

Proposição. $ax \equiv ay \pmod{m} \implies x \equiv y \pmod{\frac{m}{(a, m)}}$.

Demonstração. Ponhamos $(a, m) = d$. Então $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, como sabemos. A hipótese diz-nos que m divide $ax - ay = a(x - y)$, donde se tira facilmente que $\frac{m}{d}$ divide $\frac{a}{d}(x - y)$. Como $\frac{m}{d}$ e $\frac{a}{d}$ são primos entre si, segue-se que $\frac{m}{d}$ divide $x - y$, como pretendido. ■

Corolário. $ax \equiv ay \pmod{m} \wedge (a, m) = 1 \implies x \equiv y \pmod{m}$.

5 Os Teoremas de Euler e Fermat

Definição. Seja $m \in \mathbb{N}$. Um *sistema completo de resíduos módulo m* é um conjunto de m inteiros que se obtém escolhendo um e um só elemento em cada classe de congruência módulo m . Por outras palavras, o conjunto $\{r_1, r_2, \dots, r_m\}$ é um sistema completo de resíduos módulo m se

$$\forall a \in \mathbb{Z} \quad \exists!_{r_i} a \equiv r_i \pmod{m}.$$

Observação. Sendo $\{r_1, r_2, \dots, r_m\}$ um sistema completo de resíduos módulo m tem-se que, se $i \neq j$, então r_i não é congruente com r_j módulo m .

Definição. Seja $m \in \mathbb{N}$. Um *sistema reduzido de resíduos módulo m* é um conjunto $\{r_1, r_2, \dots, r_k\}$ de inteiros satisfazendo

$$\begin{aligned} (r_i, m) &= 1, \quad i = 1, \dots, k \\ i \neq j &\implies r_i \text{ não é congruente com } r_j \text{ módulo } m \\ \forall a \in \mathbb{Z}, (a, m) &= 1 \quad \exists!_{r_i} a \equiv r_i \pmod{m}. \end{aligned}$$

Observação. Da definição conclui-se imediatamente que um sistema reduzido de resíduos módulo m se obtém tomando um sistema completo de resíduos módulo m e retirando-lhe os elementos que não são primos com m .

Teorema. Dado $m \in \mathbb{N}$, todos os sistemas reduzidos de resíduos módulo m têm o mesmo número de elementos.

Demonstração. Sejam $\{r_1, r_2, \dots, r_k\}$ e $\{s_1, s_2, \dots, s_t\}$ dois sistemas reduzidos de resíduos módulo m . Vamos provar que $k = t$.

Seja r_i um elemento qualquer do primeiro sistema reduzido de resíduos módulo m . Como $(r_i, m) = 1$, existe um e um só elemento, digamos s_j , do segundo sistema reduzido tal que $r_i \equiv s_j \pmod{m}$. É claro que a dois elementos diferentes do primeiro sistema não pode corresponder o mesmo elemento do segundo sistema, porque se isso acontecesse eles seriam congruentes módulo m , o que não pode ser. Logo, conseguimos definir uma função injectiva do primeiro sistema para o segundo, pelo que $k \leq t$. Trocando os papéis dos dois sistemas e repetindo o raciocínio concluímos que $t \leq k$. Logo, $k = t$. ■

Definição. Seja $m \in \mathbb{N}$. Designamos por $\varphi(m)$ o número de elementos de qualquer sistema reduzido de resíduos módulo m . A φ costuma chamar-se *função de Euler*.

Proposição. Dado $m \in \mathbb{N}$, tem-se que $\varphi(m)$ é igual ao número de naturais $\leq m$ que são primos com m .

Demonstração. Basta considerar o sistema reduzido de resíduos módulo m que se obtém do sistema completo $\{1, 2, \dots, m\}$. ■

Exemplos. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, etc.

Observação. Um número natural p é primo se e só se $\varphi(p) = p - 1$.

Proposição. Seja $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m e seja a um inteiro tal que $(a, m) = 1$. Então $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$ é também um sistema reduzido de resíduos módulo m .

Demonstração. Começamos por observar que $(ar_i, m) = 1$ para $i = 1, \dots, \varphi(m)$. De facto, se m for primo com r_i e também com a , não tem factores primos comuns com r_i nem com a , e portanto também não os tem com o produto ar_i .

Vejamos a seguir que, no conjunto $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$, não há dois inteiros congruentes módulo m . De facto, se $ar_i \equiv ar_j \pmod{m}$, ter-se-ia, por a e m serem primos entre si, $r_i \equiv r_j \pmod{m}$.

Temos então $\varphi(m)$ inteiros, primos com m e não congruentes dois a dois módulo m . Um tal conjunto é necessariamente um sistema reduzido de resíduos módulo m , pois contém representantes de todas as classes de congruência módulo m cujos elementos são primos com m (recorde-se que $a \equiv b \pmod{m} \implies (a, m) = (b, m)$). ■

Proposição. Seja $\{r_1, r_2, \dots, r_m\}$ um sistema completo de resíduos módulo m e seja a um inteiro tal que $(a, m) = 1$. Então $\{ar_1, ar_2, \dots, ar_m\}$ é também um sistema completo de resíduos módulo m .

Demonstração. Exercício.

Teorema de Euler. Seja m um número natural. Se a for um inteiro primo com m então $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Demonstração. Seja $\{r_1, r_2, \dots, r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m . Pela penúltima proposição, $\{ar_1, ar_2, \dots, ar_{\varphi(m)}\}$ é também um sistema reduzido de resíduos módulo m . Para cada elemento ar_i do segundo sistema existe um e um só elemento r_j do primeiro tal que $ar_i \equiv r_j \pmod{m}$.

Multiplicando membro a membro todas estas $\varphi(m)$ congruências obtemos

$$ar_1 ar_2 \cdots ar_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}$$

o que é o mesmo que

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}.$$

Como todos os r_i são primos com m , também o seu produto é primo com m , pelo que o podemos “cortar” nesta congruência. Resulta então que

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

como pretendíamos demonstrar. ■

Observação. Se a e m não forem primos entre si, a conclusão do Teorema pode falhar. Exemplo: $4^{\varphi(2)} \not\equiv 1 \pmod{2}$.

Corolário (Pequeno Teorema de Fermat) Seja a um inteiro e seja p um número primo. Se p não dividir a então $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração. Basta observar que, se p for primo e não dividir a , se tem $(a, p) = 1$ (para além obviamente de $\varphi(p) = p - 1$). ■

6 Congruências de grau 1. Teorema chinês dos restos

Proposição. Sejam m um número natural e a e b inteiros. Se a for primo com m então existe $x_1 \in \mathbb{Z}$ tal que $ax_1 \equiv b \pmod{m}$. Além disso, outro inteiro x_2 satisfaz a mesma congruência se e só se $x_2 \equiv x_1 \pmod{m}$.

Demonstração. Como $(a, m) = 1$, existem inteiros s e t tais que $as + mt = 1$, o que significa que s satisfaz $as \equiv 1 \pmod{m}$; segue-se imediatamente que $x_1 = sb$ é solução de $ax \equiv b \pmod{m}$. Se agora $x_2 \equiv x_1 \pmod{m}$ é evidente que $ax_2 \equiv b \pmod{m}$. Reciprocamente, suponhamos que $ax_2 \equiv b \pmod{m}$. Então $ax_2 \equiv ax_1 \pmod{m}$, donde, por a ser primo com m , $x_2 \equiv x_1 \pmod{m}$. ■

Observação. O que a Proposição afirma é que o conjunto completo das soluções é $[x_1]_m$, a classe de congruência de x_1 módulo m . Podemos assim dizer que a congruência têm essencialmente “só uma solução”, no sentido de que todas as soluções são congruentes entre si módulo m .

O que acontece à congruência $ax \equiv b \pmod{m}$ se a e m não forem primos entre si? Vejamos. Designemos (a, m) por d . Se $ax \equiv b \pmod{m}$ tiver uma solução x_1 , então $ax_1 \equiv b \pmod{d}$, porque $d \mid m$. Mas claro que $a \equiv 0 \pmod{d}$. Então tem-se $b \equiv 0 \pmod{d}$, isto é, $d \mid b$.

Reciprocamente, suponhamos que $d \mid b$. Como $(a, b) = d$, sabemos que $(\frac{a}{d}, \frac{m}{d}) = 1$, e portanto a congruência $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ tem solução. Seja x_1 uma tal solução. Então tem-se $\frac{a}{d}x_1 - \frac{b}{d} = q\frac{m}{d}$ para certo inteiro q . Multiplicando ambos os membros por d , vemos que esta igualdade é equivalente a $ax_1 - b = qm$, isto é, $ax_1 \equiv b \pmod{m}$, ou seja x_1 é solução da congruência $ax \equiv b \pmod{m}$. Concluimos assim:

Proposição. Sendo $(a, m) = d$, a congruência $ax \equiv b \pmod{m}$ tem solução se e só se $d \mid b$. Além disso, nessa situação, um inteiro é solução de $ax \equiv b \pmod{m}$ se e só se for solução de $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Claro que conhecemos todas as soluções de $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$: sendo x_1 uma solução, o conjunto completo das soluções é $[x_1]_{\frac{m}{d}}$, a classe de congruência de x_1 módulo $\frac{m}{d}$,

isto é, o conjunto $\{x_1 + k\frac{m}{d} : k \in \mathbb{Z}\}$. Vamos agora ver como descrever este mesmo conjunto em termos de classes de congruência módulo m .

Proposição. Seja $(a, m) = d$ e suponhamos que $d \mid b$. Sendo x_1 uma solução da congruência $ax \equiv b \pmod{m}$, o conjunto das soluções é a união das d classes de congruência módulo m

$$[x_1]_m, \left[x_1 + \frac{m}{d}\right]_m, \left[x_1 + 2\frac{m}{d}\right]_m, \dots, \left[x_1 + (d-1)\frac{m}{d}\right]_m.$$

Demonstração. Consideremos os d inteiros $x_1 + j\frac{m}{d}$, $j = 0, 1, 2, \dots, d-1$. Conforme já visto, trata-se de soluções da congruência $ax \equiv b \pmod{m}$.

Comecemos por ver que estes d inteiros são dois a dois incongruentes módulo m . Suponhamos que se tinha

$$x_1 + j\frac{m}{d} \equiv x_1 + j'\frac{m}{d} \pmod{m}, \quad \text{com } 0 \leq j < j' < d.$$

Viria então que

$$j\frac{m}{d} \equiv j'\frac{m}{d} \pmod{m}$$

donde

$$(j' - j)\frac{m}{d} \equiv 0 \pmod{m}$$

o que é impossível, porque $0 < j' - j < d$. Concluimos assim que as d classes de congruência módulo m referidas no enunciado são de facto todas distintas.

Vejamos agora que qualquer outra solução de $ax \equiv b \pmod{m}$ pertence necessariamente a uma destas d classes de congruência módulo m . Seja $x_1 + t\frac{m}{d}$ uma tal solução. Dividamos t por d : $t = qd + r$, com $r \in \{0, 1, 2, \dots, d-1\}$. Vem então

$$x_1 + t\frac{m}{d} = x_1 + (qd + r)\frac{m}{d} = x_1 + qm + r\frac{m}{d} \equiv x_1 + r\frac{m}{d} \pmod{m}. \blacksquare$$

Exemplo. A congruência $6x \equiv 3 \pmod{15}$ tem soluções, porque $(6, 15) = 3$ e $3 \mid 3$. As soluções são as mesmas que as da congruência $\frac{6}{3}x \equiv \frac{3}{3} \pmod{\frac{15}{3}}$, isto é, $2x \equiv 1 \pmod{5}$. Uma solução desta é, por exemplo, 3. O conjunto completo das soluções é $[3]_5$. Módulo 15 as soluções são as classes de congruência

$$[3]_{15}, [8]_{15}, [13]_{15}.$$

Uma questão interessante envolvendo congruências de grau 1 é a resolução de várias congruências em simultâneo, todas com a mesma incógnita. O resultado seguinte aborda um caso especial deste problema.

Teorema chinês dos restos. Sejam $m_1, m_2, \dots, m_k$ naturais primos dois a dois e sejam $a_1, a_2, \dots, a_k$ inteiros quaisquer. Então, o sistema de congruências

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

tem solução. Quaisquer duas soluções são congruentes módulo $m_1 m_2 \dots m_k$.

Demonstração. Como $m_1, m_2, \dots, m_k$ são primos dois a dois, tem-se $[m_1, m_2, \dots, m_k] = m_1 m_2 \dots m_k$, pelo que a segunda afirmação do enunciado é consequência de propriedades vistas da relação de congruência, já que se x' e x'' forem duas soluções do referido sistema de congruências tem-se $x' \equiv x'' \pmod{m_1}$, $x' \equiv x'' \pmod{m_2}$, ... , $x' \equiv x'' \pmod{m_k}$.

Vejamos agora a primeira parte. Ponhamos $m = m_1 m_2 \dots m_k$. Para cada $j \in \{1, 2, \dots, k\}$, tem-se $\frac{m}{m_j} \in \mathbb{Z}$, claro, e $(\frac{m}{m_j}, m_j) = 1$ (porquê?). Então, para cada j , a congruência $\frac{m}{m_j} x \equiv 1 \pmod{m_j}$ tem solução. Seja b_j uma solução dessa congruência. Tem-se, para cada $j \in \{1, 2, \dots, k\}$, por um lado

$$\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}$$

e por outro

$$\frac{m}{m_j} b_j \equiv 0 \pmod{m_i} \quad \text{se } i \neq j$$

porque, se $i \neq j$, o inteiro $\frac{m}{m_j}$ é múltiplo de m_i .

Seja

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \dots + \frac{m}{m_k} b_k a_k.$$

Então, para cada $j \in \{1, 2, \dots, k\}$, tem-se

$$x_0 \equiv \frac{m}{m_j} b_j a_j \equiv a_j \pmod{m_j}$$

ou seja x_0 é uma solução do sistema de congruências indicado no enunciado. O conjunto completo das soluções é então $[x_0]_m$. ■

7 O Teorema de Wilson. Testes de primalidade

Lema. Seja p um número primo e a um inteiro. Se $a^2 \equiv 1 \pmod{p}$ então tem-se $a \equiv 1 \pmod{p} \vee a \equiv -1 \pmod{p}$.

Demonstração. A condição $a^2 \equiv 1 \pmod{p}$ significa que p divide $a^2 - 1 = (a - 1)(a + 1)$. Como p é primo, tem que dividir pelo menos um dos factores deste produto, isto é, tem-se $a \equiv 1 \pmod{p}$ ou $a \equiv -1 \pmod{p}$. ■

Teorema de Wilson. Se p é um número primo então $(p - 1)! \equiv -1 \pmod{p}$.

Demonstração. Para $p = 2$ ou $p = 3$, o teorema verifica-se trivialmente. Suponhamos então que p é um número primo ≥ 5 . Tem-se que

$$(p - 1)! = 2 \cdot 3 \cdot \dots \cdot (p - 2) \cdot (p - 1).$$

Como $p - 1 \equiv -1 \pmod{p}$, para demonstrar o que se pretende bastará mostrar que

$$2 \cdot 3 \cdot \dots \cdot (p - 2) \equiv 1 \pmod{p}.$$

O produto no primeiro membro tem um número par de factores. Vamos ver que esses factores se podem “empareilhar” de modo que o produto dos dois números em cada par seja congruente com 1 módulo p .

Seja $a \in \{2, 3, \dots, p - 2\}$. Então $(a, p) = 1$, pelo que existe x tal que $ax \equiv 1 \pmod{p}$, e pela proposição anterior podemos tomar $x \in \{0, 1, \dots, p - 1\}$.

Claramente x não pode ser 0 nem 1. E x também não pode ser $p - 1$, pois se fosse ter-se-ia $a(p - 1) \equiv 1 \pmod{p}$, donde $a \equiv -1 \pmod{p}$, o que não pode ser, porque $a \in \{2, 3, \dots, p - 2\}$.

Logo, $x \in \{2, 3, \dots, p - 2\}$. Note-se que também não pode ser $x = a$, pois nesse caso ter-se-ia que $a^2 \equiv 1 \pmod{p}$ e então, pelo Lema, a teria que ser $\equiv 1$ ou $\equiv p - 1$.

Mostrámos assim que, para cada $a \in \{2, 3, \dots, p - 2\}$, existe $x \neq a$ no mesmo conjunto tal que $ax \equiv 1 \pmod{p}$. E existe um só elemento nessas condições, pois se também $ay \equiv 1 \pmod{p}$ com $y \in \{2, 3, \dots, p - 2\}$ ter-se-ia $ay \equiv ax \pmod{p}$ donde $y = x$. ■

O recíproco do Teorema de Wilson também é verdadeiro:

Teorema. Se um número natural n satisfizer $(n-1)! \equiv -1 \pmod{n}$, então n é primo.

Demonstração. Suponhamos que se tem $(n-1)! \equiv -1 \pmod{n}$, mas que n é composto. Seja b um divisor de n , com $1 < b < n$. Então $b \leq n-1$, pelo que $b \mid (n-1)!$. A hipótese diz-nos que $n \mid (n-1)! + 1$. Como $b \mid n$, também $b \mid (n-1)! + 1$. Se b divide $(n-1)!$ e também divide $(n-1)! + 1$, segue-se que b divide 1: absurdo, porque $b > 1$. ■

Exercício. Mostre que, se $n > 4$ for composto, então $(n-1)! \equiv 0 \pmod{n}$.

O Teorema de Wilson e o seu recíproco permitem-nos concluir que um natural n é primo se e só se dividir $(n-1)! + 1$. Este resultado é interessante, porque fornece um processo de verificar se um dado número é primo sem ter de testar qualquer divisor. Mas é claro que esta ideia não tem utilidade prática, dado que os factoriais são números que crescem muito rapidamente, o que torna o método impraticável.

A busca de “testes de primalidade” — métodos para verificar se números dados são ou não primos, sem ser pela definição — constitui um importante campo de investigação. Os testes classificam-se pela sua eficiência, mas também pela natureza das conclusões que permitem tirar: há testes “determinísticos”, que dão respostas categóricas (como o Teorema de Wilson, que não é eficiente), e há outros que são apenas “probabilísticos”, porque as suas conclusões são apenas de que certos números são provavelmente primos (com uma probabilidade que se tenta quantificar).

Um exemplo simples de um teste deste segundo tipo baseia-se no Pequeno Teorema de Fermat, que diz que, se p for primo e a não for múltiplo de p , então $a^{p-1} \equiv 1 \pmod{p}$. Isto é apenas uma condição necessária para um número ser primo. Se para um dado n descobrirmos a tal que $a^{n-1} \not\equiv 1 \pmod{n}$, então n é composto. Mas se $a^{n-1} \equiv 1 \pmod{n}$ para muitos valores de a (por exemplo para $a = 2, \dots, n-1$), então há uma probabilidade grande de n ser primo. Como essas verificações se podem fazer com grande rapidez num computador, temos aqui uma informação que pode ser útil nalguns contextos.

Recentemente, três matemáticos indianos (um professor e dois estudantes) descobriram um teste simples de primalidade que é determinístico e computacionalmente eficiente.²

² Manindra Agrawal, Neeraj Kayal e Nitin Saxena, PRIMES is in P, *Annals of Mathematics*, vol. 160 (2004), p. 781-793.

8 As funções $\varphi(n)$ e $\sigma(n)$

Já se referiu anteriormente a função φ de Euler, assim definida: sendo n um número natural, $\varphi(n)$ é o número de elementos de qualquer sistema reduzido de resíduos módulo n . Pensando no sistema reduzido de resíduos módulo n que se obtém do sistema completo $\{1, 2, \dots, n\}$ retirando os números que não são primos com n , vemos que $\varphi(n)$ é igual ao número de naturais $\leq n$ que são primos com n .

O cálculo de valores de $\varphi(n)$ usando estas caracterizações não é fácil, e a dificuldade é cada vez maior quando n aumenta. Vamos ver que esse cálculo se torna muito simples se conhecermos a factorização de n como produto de primos.

Proposição. Sendo p um número primo e α um número natural, tem-se

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

Demonstração. $\varphi(p^\alpha)$ é o número de naturais $\leq p^\alpha$ que são primos com p^α . Vejamos quais são os números naturais $\leq p^\alpha$ que não são primos com p^α . São exactamente os naturais $\leq p^\alpha$ que têm p como divisor:

$$p, 2p, 3p, \dots, p^{\alpha-1}p.$$

Estes naturais são em número de $p^{\alpha-1}$, pelo que os naturais $\leq p^\alpha$ que são primos com p^α são em número de $p^\alpha - p^{\alpha-1}$. ■

Observação. Note-se que este resultado não é válido se p não for primo. Exemplo: $\varphi(4) = 2$, mas $\varphi(4^2) = 8 \neq 4^2 - 4^1$.

Proposição. Se m e n forem números naturais primos entre si, tem-se

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Observação. Em Teoria dos Números, esta propriedade costuma resumir-se dizendo que a função φ é *multiplicativa*.

Demonstração da proposição. Sejam $R = \{r_1, r_2, \dots, r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m , $S = \{s_1, s_2, \dots, s_{\varphi(n)}\}$ um sistema reduzido de resíduos módulo n e $T = \{t_1, t_2, \dots, t_{\varphi(mn)}\}$ um sistema reduzido de resíduos módulo mn .

Consideremos um elemento qualquer t_k do conjunto T . Sabemos que $(t_k, mn) = 1$. Daqui segue-se que também $(t_k, m) = 1$ e $(t_k, n) = 1$ (porquê?). Pela definição de sistema reduzido de resíduos, podemos então afirmar que

$$\exists_{r_i}^1 t_k \equiv r_i \pmod{m} \quad \text{e} \quad \exists_{s_j}^1 t_k \equiv s_j \pmod{n}.$$

Assim, a cada elemento t_k do conjunto T corresponde por este processo um e um só par (r_i, s_j) , com r_i pertencente ao conjunto R e s_j pertencente ao conjunto S . Note-se que a elementos diferentes do conjunto T correspondem pares diferentes: se a t_h (distinto de t_k) também correspondesse o par (r_i, s_j) , ter-se-ia $t_h \equiv r_i \pmod{m}$ e $t_h \equiv s_j \pmod{n}$, donde $t_h \equiv t_k \pmod{m}$ e $t_h \equiv t_k \pmod{n}$; como m e n são primos entre si, viria então $t_h \equiv t_k \pmod{mn}$, contra o facto de ambos os números pertencerem a um mesmo sistema reduzido de resíduos módulo mn .

Reciprocamente, consideremos um par (r_i, s_j) , com r_i pertencente ao conjunto R e s_j pertencente ao conjunto S . Pelo teorema chinês dos restos (aplicável porque m e n são primos entre si), podemos afirmar que existe um inteiro x satisfazendo

$$\begin{aligned} x &\equiv r_i \pmod{m} \\ x &\equiv s_j \pmod{n} \end{aligned}$$

Por uma propriedade das congruências, como $(r_i, m) = 1$ e $(s_j, n) = 1$ tem-se que $(x, m) = 1$ e $(x, n) = 1$. Daqui segue-se que também $(x, mn) = 1$ (porquê?). Logo, como T é um sistema reduzido de resíduos módulo mn , existe um t_k nesse conjunto tal que $x \equiv t_k \pmod{mn}$ (e não podem existir dois elementos do sistema nessas condições, porque se existissem seriam congruentes módulo mn). Assim, a cada par (r_i, s_j) corresponde por este processo um e um só elemento t_k . Resta notar que a pares diferentes correspondem elementos diferentes do conjunto T : se a $(r_{i'}, s_{j'})$ (distinto de (r_i, s_j)) também correspondesse o elemento t_k , ter-se-ia $r_{i'} \equiv r_i \pmod{m}$ e $s_{j'} \equiv s_j \pmod{n}$, o que não pode ser, por R ser um sistema reduzido de resíduos módulo m e S ser um sistema reduzido de resíduos módulo n .

Estabelecemos assim uma bijecção entre o conjunto T e o conjunto dos pares (r_i, s_j) , com r_i pertencente ao conjunto R e s_j pertencente ao conjunto S . Este conjunto de pares, que é o produto cartesiano $R \times S$, tem $\varphi(m)\varphi(n)$ elementos. ■

Observação. Este resultado não é válido se m e n não forem primos entre si. Exemplo: $\varphi(4) = 2$, mas $\varphi(2)\varphi(2) = 1$.

Teorema. Seja n um número natural > 1 e seja $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ a sua factorização como produto de números primos. Então tem-se

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1}).$$

Demonstração. Aplicando repetidas vezes a última proposição, concluímos que

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$$

pelo que o resultado segue da primeira proposição desta secção. ■

Exemplo. $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = (2^3 - 2^2)(3^2 - 3)(5 - 1) = 96$.

Uma outra função interessante em Teoria dos Números é a função σ assim definida: para cada número natural n , $\sigma(n)$ é a soma dos divisores positivos de n , incluindo 1 e n .

Exemplos. $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 7$, $\sigma(5) = 6$, $\sigma(6) = 12$, etc.

Vamos ver que o cálculo de valores de $\sigma(n)$ se torna muito simples se conhecermos a factorização de n como produto de primos.

Proposição. Sendo p um número primo e α um número natural, tem-se

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}.$$

Demonstração. Isto é consequência imediata do facto de que os divisores de p^α são $1, p, p^2, \dots, p^\alpha$ e de que

$$1 + p + p^2 + \cdots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}.$$

■

Proposição. A função σ é multiplicativa, isto é, se m e n forem números naturais primos entre si, tem-se

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Demonstração. Começamos por observar que, sendo m e n primos entre si, qualquer divisor d de mn se escreve de modo único na forma $d = d'd''$ com d' divisor de m e d'' divisor de n . (Isto porque os conjuntos de primos que aparecem nas factorizações de m e n são disjuntos.)

Reciprocamente, dados d' divisor de m e d'' divisor de n , é evidente que o produto $d = d'd''$ é um divisor de mn . Logo, há uma bijecção entre o conjunto dos divisores d de mn e o conjunto dos pares (d', d'') em que d' é divisor de m e d'' é divisor de n , sendo cada elemento do primeiro conjunto igual ao produto dos elementos do par que lhe corresponde no segundo conjunto.

Sejam $d_1, d_2, \dots, d_{\tau(mn)}$ os divisores de mn , $d'_1, d'_2, \dots, d'_{\tau(m)}$ os divisores de m e $d''_1, d''_2, \dots, d''_{\tau(n)}$ os divisores de n . Tem-se

$$\sigma(mn) = d_1 + d_2 + \dots + d_{\tau(mn)}.$$

Como cada uma destas parcelas é igual ao produto de um divisor de m por um divisor de n , conforme vimos acima, tem-se que $\sigma(mn)$ é igual à soma de todos os possíveis produtos dessa forma, isto é,

$$\begin{aligned} \sigma(mn) &= d'_1 d''_1 + d'_1 d''_2 + \dots + d'_1 d''_{\tau(n)} + \\ &+ d'_2 d''_1 + d'_2 d''_2 + \dots + d'_2 d''_{\tau(n)} + \\ &+ \dots + \\ &+ d'_{\tau(m)} d''_1 + d'_{\tau(m)} d''_2 + \dots + d'_{\tau(m)} d''_{\tau(n)} = \\ &= d'_1 \sigma(n) + d'_2 \sigma(n) + \dots + d'_{\tau(m)} \sigma(n) = \\ &= \sigma(m) \sigma(n). \blacksquare \end{aligned}$$

Observação. Este resultado não é válido se m e n não forem primos entre si. Exemplo: $\sigma(4) \neq \sigma(2)\sigma(2)$.

Teorema. Seja n um número natural > 1 e seja $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ a sua factorização como produto de números primos. Então tem-se

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \right).$$

Demonstração. Aplicando repetidas vezes a última proposição, concluimos que

$$\sigma(n) = \sigma(p_1^{\alpha_1}) \sigma(p_2^{\alpha_2}) \cdots \sigma(p_k^{\alpha_k})$$

pelo que o resultado segue da proposição anterior a essa. ■

Exemplo. $\sigma(360) = \sigma(2^3 \cdot 3^2 \cdot 5) = \left(\frac{2^4 - 1}{2 - 1} \right) \left(\frac{3^3 - 1}{3 - 1} \right) \left(\frac{5^2 - 1}{5 - 1} \right) = 1170.$

Uma das motivações para estudar a função $\sigma(n)$ é o interesse pelos chamados *números perfeitos*.

Definição. Um número natural n diz-se *perfeito* se for igual à soma de todos os seus divisores positivos exceptuando ele próprio. Usando a função σ , isto significa que n é perfeito se $\sigma(n) = 2n$.

Exemplo. 6 é perfeito, porque os divisores positivos de 6, sem contar com ele próprio, são 1, 2 e 3 e tem-se $6 = 1 + 2 + 3$. E, claro, $\sigma(6) = 12$.

É possível descrever todos os números perfeitos pares.

Proposição (Euclides, *Elementos*, Livro 9, Proposição 36) Seja k um número natural. Se $2^k - 1$ for um número primo, então $2^{k-1}(2^k - 1)$ é um número perfeito.

Demonstração. Isto é uma aplicação simples da fórmula vista acima para a função σ (e do facto de que, se p for um número primo, se tem $\sigma(p) = p + 1$):

$$\sigma[2^{k-1}(2^k - 1)] = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)2^k = 2 \cdot [2^{k-1}(2^k - 1)]$$

e portanto $2^{k-1}(2^k - 1)$ é um número perfeito. ■

Vamos agora ver que os números da forma $2^{k-1}(2^k - 1)$ onde $2^k - 1$ é um número primo são os únicos números perfeitos pares.

Proposição (Euler) Se n for um número perfeito par, então existe um número natural k tal que $2^k - 1$ é um número primo e $n = 2^{k-1}(2^k - 1)$.

Demonstração. Como n é par, n é da forma $n = 2^{k-1} \cdot m$, com $k \in \mathbb{N}$, $k \geq 2$, e m ímpar. Por outro lado, como n é perfeito, tem-se $\sigma(n) = 2n$. Mas

$$\sigma(n) = \sigma(2^{k-1} \cdot m) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m),$$

onde usámos o facto de que 2^{k-1} e m são primos entre si. Logo, tem-se

$$(2^k - 1)\sigma(m) = 2n = 2^k m.$$

Como $2^k - 1$ é ímpar e no segundo membro 2 figura com expoente k , tem de ter-se $\sigma(m) = 2^k h$ para algum $h \in \mathbb{N}$. Substituindo na mesma igualdade vem

$$(2^k - 1)2^k h = 2^k m,$$

donde

$$m = (2^k - 1)h = 2^k h - h,$$

ou $m + h = 2^k h$, que é igual a $\sigma(m)$. Mas $\sigma(m)$ é igual à soma dos divisores de m , entre os quais se encontram m e h ; se $\sigma(m)$ é igual a $m + h$, tem que ser $h = 1$ e portanto tem-se que $m = 2^k - 1$ e m é primo (por só ter os divisores positivos 1 e m). ■

Observação. Descrevemos assim todos os números perfeitos pares. Até hoje, nunca ninguém conseguiu descobrir um número perfeito ímpar, e saber se existe algum é um dos mais famosos problemas da Teoria dos Números que permanecem em aberto.

Quando é que um número da forma $2^k - 1$ é primo? Algumas experiências com expoentes k pequenos sugerem que tal acontece precisamente quando k é primo. Essa conjectura não é verdadeira, porque, por exemplo, $2^{11} - 1 = 2047 = 23 \cdot 89$. Mas tem-se o seguinte resultado:

Proposição. Seja $k \in \mathbb{N}$. Se $2^k - 1$ for um número primo, então k é primo.

Demonstração. Usamos a fatorização

$$x^a - 1 = (x - 1)(1 + x + x^2 + \cdots + x^{a-1})$$

válida para qualquer número real x e qualquer número natural a .

Suponhamos que k é composto, digamos $k = ab$, com $a, b > 1$. Tem-se então

$$2^k - 1 = 2^{ab} - 1 = (2^b)^a - 1 = (2^b - 1)(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b})$$

e $2^k - 1$ seria composto, contra a hipótese. ■

Põe-se assim um problema: para que primos p é que $2^p - 1$ é primo? A primeira pessoa a investigar a questão explicitamente foi um frade francês, Marin Mersenne, no século XVII. Por isso os números da forma $2^p - 1$, com p primo, chamam-se hoje *números de Mersenne*. A notação mais comum para $2^p - 1$ é M_p .

Para valores pequenos de p pode ver-se “à mão” se M_p é primo ou não. Quando p aumenta isso fica cada vez mais difícil. Para tal efeito é útil o resultado seguinte:

Teste de Lucas-Lehmer. Defina-se a seguinte sucessão:

$$u_1 = 4, \quad u_2 = 4^2 - 2 = 14, \quad u_3 = 14^2 - 2 = 194, \quad \dots, \quad u_n = u_{n-1}^2 - 2, \quad \dots$$

Então, sendo p um primo > 2 , tem-se que M_p é primo se e só se $M_p | u_{p-1}$.

A demonstração do Teste de Lucas-Lehmer não é muito difícil, mas está fora do âmbito desta disciplina, pois usa conhecimentos da disciplina de Álgebra do 2º ano.

Na tabela seguinte registam-se os primos de Mersenne descobertos até hoje (Setembro de 2008). Na primeira coluna indica-se o número de ordem dos sucessivos primos de Mersenne: o primeiro, o segundo, etc. Nos sete últimos números indicados encontra-se aí um ponto de interrogação, pois embora os p indicados nessas linhas (20996011, 24036583, 25964951, 30402457, 32582657, 37156667 e 43112609) dêem origem a primos de Mersenne, não se sabe de momento se se trata dos 40º, 41º, 42º, 43º, 44º, 45º e 46º primos de Mersenne.

A busca de números primos de Mersenne

#	p	Nº de algarismos de M_p	Ano	Autor da descoberta
1	2	1	—	—
2	3	1	—	—
3	5	2	—	—
4	7	3	—	—
5	13	4	—	—
6	17	6	1588	Cataldi
7	19	6	1588	Cataldi
8	31	10	1772	Euler
9	61	19	1883	Pervushin
10	89	27	1911	Powers
11	107	33	1914	Powers
12	127	39	1876	Lucas
13	521	157	1952	Robinson
14	607	183	1952	Robinson
15	1279	386	1952	Robinson
16	2203	664	1952	Robinson
17	2281	687	1952	Robinson
18	3217	969	1957	Riesel
19	4253	1281	1961	Hurwitz
20	4423	1332	1961	Hurwitz
21	9689	2917	1963	Gillies
22	9941	2993	1963	Gillies
23	11213	3376	1963	Gillies
24	19937	6002	1971	Tuckerman
25	21701	6533	1978	Noll e Nickel
26	23209	6987	1979	Noll
27	44497	13395	1979	Nelson e Slowinski
28	86243	25962	1982	Slowinski
29	110503	33265	1988	Colquitt e Welsh
30	132049	39751	1983	Slowinski
31	216091	65050	1985	Slowinski
32	756839	227832	1992	Slowinski e Gage
33	859433	258716	1994	Slowinski e Gage
34	1257787	378632	1996	Slowinski e Gage
35	1398269	420921	1996	Armengaud, Woltman, etc.
36	2976221	895932	1997	Spence, Woltman, etc.
37	3021377	909526	1998	Clarkson, Woltman, Kurowski, etc.
38	6972593	2098960	1999	Hajratwala, Woltman, Kurowski, etc.
39	13466917	4053946	2001	Cameron, Woltman, Kurowski, etc.
?	20996011	6320430	2003	Shafer, Woltman, Kurowski, etc.
?	24036583	7235733	2004	Findley, Woltman, Kurowski, etc.
?	25964951	7816230	2005	Nowak, Woltman, Kurowski, etc.
?	30402457	9152052	2005	Cooper, Boone, Woltman, Kurowski, etc.
?	32582657	9808358	2006	Cooper, Boone, Woltman, Kurowski, etc.
?	37156667	11185272	2008	Elvenich, Woltman, Kurowski, etc.
?	43112609	12978189	2008	Smith, Woltman, Kurowski, etc.

A partir de M_{521} todos os números de Mersenne primos foram descobertos usando computadores. A partir de $M_{1398269}$ todos os números de Mersenne primos foram descobertos usando computadores funcionando em rede através da Internet.

Qualquer pessoa com um computador pessoal ligado à Internet pode colaborar no esforço computacional, usando o Teste de Lucas-Lehmer, para descobrir novos números primos de Mersenne (ver www.mersenne.org).

Exercício. O número $M_{29} = 2^{29} - 1$ é composto. Usando um computador, factorize M_{29} como produto de números primos.

Tal como os números da forma $2^k - 1$, também os números da forma $2^k + 1$, com $k \in \mathbb{N}$, despertam interesse, nomeadamente para saber quais os números dessa forma que são primos. Algumas experiências com expoentes k pequenos sugerem que tal acontece precisamente quando k é uma potência de 2.

Exercício. Prove que, se $2^k + 1$ for um número primo, então k é uma potência de 2. (Sugestão: Utilize — depois de a demonstrar — a seguinte factorização, válida para qualquer número real x e qualquer número natural a :

$$x^{2a+1} + 1 = (x + 1)(1 - x + x^2 - x^3 + \cdots + x^{2a-2} - x^{2a-1} + x^{2a}).$$

Será verdadeira a afirmação recíproca? Se k for uma potência de 2, será $2^k + 1$ necessariamente um número primo?

Exercício. Verifique que $2^k + 1$ é um número primo para $k = 1$, $k = 2$, $k = 4$, $k = 8$ e $k = 16$.

Exercício. Usando um computador, mostre que o número $2^{32} + 1$ é composto.

Os números da forma $2^{2^n} + 1$ são conhecidos por *números de Fermat*. Com excepção dos cinco acima indicados, não se conhece nenhum número de Fermat que seja primo.

9 Equações Diofantinas.

Costuma chamar-se *equações Diofantinas*³ a equações, com uma ou mais incógnitas, de que se procuram soluções inteiras (ou naturais). Este campo de estudo é vastíssimo, e não existem processos gerais de análise de tal tipo de problema.⁴

Nesta secção vamos apenas fazer algumas referências:

- ao caso de equações polinomiais com coeficientes inteiros e uma só incógnita;
- a uma técnica que pode por vezes ser usada para mostrar que certas equações *não têm* soluções;
- e, finalmente, a um tipo especial de equações – com três incógnitas — que se tornou famoso nos últimos séculos.

A busca de soluções⁵ inteiras, ou mesmo racionais, de equações polinomiais com coeficientes inteiros e uma só incógnita é muito simples. O resultado seguinte fornece uma condição necessária para um número racional ser raiz de uma tal equação.

Proposição. Suponhamos que um número racional $\frac{b}{c}$, onde b e c são inteiros primos entre si (isto é, a fracção já se encontra simplificada), é raiz da equação

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

onde $a_n, a_{n-1}, \dots, a_2, a_1, a_0$ são números inteiros. Então tem-se que

$$b \mid a_0 \quad \text{e} \quad c \mid a_n.$$

Em particular, se um inteiro for raiz da equação, tem que dividir o termo independente do polinómio que se encontra no primeiro membro.

³ Esta designação vem do nome do matemático grego Diofanto (séc. III d.C.), que estudou o assunto numa obra intitulada *Arithmetica*.

⁴ A questão de saber se existe algum algoritmo finito universal para decidir se uma equação polinomial, com coeficientes inteiros e com mais do que uma incógnita, tem soluções inteiras foi um dos mais famosos problemas matemáticos do século XX. Foi proposto pelo alemão David Hilbert em 1900 e resolvido – com resposta negativa – em 1970 pelo russo Yuri Matiyasevich (então com 22 anos), a partir de trabalhos da americana Julia Robinson.

⁵ Também se diz *raízes*.

Demonstração. Se $\frac{b}{c}$ é raiz da equação, tem-se

$$a_n \left(\frac{b}{c}\right)^n + a_{n-1} \left(\frac{b}{c}\right)^{n-1} + \cdots + a_2 \left(\frac{b}{c}\right)^2 + a_1 \frac{b}{c} + a_0 = 0.$$

Multiplicando ambos os membros por c^n , obtém-se

$$a_n b^n + a_{n-1} b^{n-1} c + \cdots + a_2 b^2 c^{n-2} + a_1 b c^{n-1} + a_0 c^n = 0$$

donde

$$a_0 c^n = -a_n b^n - a_{n-1} b^{n-1} c - \cdots - a_2 b^2 c^{n-2} - a_1 b c^{n-1}$$

o que é o mesmo que

$$a_0 c^n = b(-a_n b^{n-1} - a_{n-1} b^{n-2} c - \cdots - a_2 b c^{n-2} - a_1 c^{n-1}).$$

Ou seja: se $\frac{b}{c}$ é raiz da equação, tem-se que $b \mid a_0 c^n$. Como b é primo com c , também é primo com c^n (porquê?) e portanto $b \mid a_0$.

Analogamente, de

$$a_n b^n = -a_{n-1} b^{n-1} c - \cdots - a_2 b^2 c^{n-2} - a_1 b c^{n-1} - a_0 c^n$$

tira-se

$$a_n b^n = c(-a_{n-1} b^{n-1} - \cdots - a_2 b^2 c^{n-3} - a_1 b c^{n-2} - a_0 c^{n-1}).$$

Ou seja: se $\frac{b}{c}$ é raiz da equação, tem-se que $c \mid a_n b^n$. Como c é primo com b , também é primo com b^n e portanto $c \mid a_n$. ■

Observação. Note-se que esta proposição dá apenas uma condição *necessária* para um número racional ser raiz de uma equação polinomial com coeficientes inteiros e uma incógnita.

Na prática, como é que o resultado se aplica? Dada uma equação

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

com coeficientes inteiros, fazemos uma lista de todos os números racionais cujo numerador é um divisor de a_0 e cujo denominador é um divisor de a_n . Estes são os números racionais que *podem* ser raízes da equação. Em seguida, experimentamos com cada um desses números racionais para ver se é raiz da equação. Se estivermos interessados apenas em raízes inteiras, experimentamos com todos os inteiros que dividem a_0 .

Uma consequência interessante da proposição é a seguinte, relativa a equações em que o coeficiente da maior potência da incógnita é igual 1:

Corolário. As raízes racionais de uma equação da forma

$$x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 = 0$$

(onde $a_{n-1}, \dots, a_2, a_1, a_0$ são números inteiros) são necessariamente inteiras.

Demonstração. Isto é imediato, porque se um número racional $\frac{b}{c}$ for raiz da equação, o denominador c tem que dividir o coeficiente de x^n , que é 1. ■

Deste resultado, com um aspecto tão simples, deduz-se a irracionalidade da maior parte das raízes, de qualquer índice, de números inteiros. Por exemplo:

Proposição. Se um número inteiro a não for um quadrado perfeito, $\sqrt{a}$ é irracional.

Demonstração. Basta mostrar que a equação $x^2 - a = 0$ não tem raízes racionais. Como o coeficiente de x^2 é 1, qualquer raiz racional tem, pelo Corolário, que ser inteira. Mas se houvesse uma raiz inteira, digamos b , ter-se-ia $b^2 = a$ e a seria um quadrado perfeito. ■

Podemos assim afirmar que $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}, \sqrt{10}$, etc., são números irracionais.

Da mesma forma, podemos demonstrar a seguinte

Proposição. Se um número inteiro a não for uma potência de expoente n de um número inteiro, $\sqrt[n]{a}$ é irracional.

Podemos assim afirmar que números como $\sqrt[3]{2}, \sqrt[5]{8}$, etc., etc., são números irracionais.

Observação. Resta notar que a busca de raízes racionais de equações polinomiais com coeficientes *racionais* se reduz facilmente ao caso das equações polinomiais com coeficientes inteiros, porque podemos multiplicar ambos os membros de uma tal equação por um inteiro escolhido de forma a fazer “desaparecer” todos os denominadores, e esta operação não altera as raízes da equação.

O segundo tema desta secção refere-se a uma técnica que pode por vezes ser usada para mostrar que certas equações *não têm* soluções.

A técnica baseia-se numa observação trivial: se dois números inteiros forem iguais, então são congruentes módulo m qualquer que seja o número natural m . Em símbolos: sendo a e b inteiros,

$$a = b \implies [\forall_{m \in \mathbb{N}} a \equiv b \pmod{m}] .$$

Isto é equivalente a dizer que

$$[\exists_{m \in \mathbb{N}} a \not\equiv b \pmod{m}] \implies a \neq b .$$

Assim, dada uma equação Diofantina qualquer, se nós conseguirmos encontrar um número natural m tal que, substituindo na equação o sinal $=$ pelo sinal de congruência módulo m , a congruência resultante não tenha soluções, então a equação original também não tem soluções.

Exemplo. A equação $x^2 + y^2 = 4z + 3$ não tem soluções inteiras.

Demonstração. Tomemos $m = 4$, isto é, substituamos a equação pela correspondente congruência módulo 4. A congruência fica

$$x^2 + y^2 \equiv 3 \pmod{4} .$$

Vamos ver que não há valores inteiros de x e y que satisfaçam esta congruência.

Para isso basta observar o seguinte: o quadrado de qualquer inteiro ou é $\equiv 0 \pmod{4}$ ou é $\equiv 1 \pmod{4}$. Isto porquê? Se o inteiro for par, digamos $2a$, o seu quadrado é $4a^2$, que é $\equiv 0 \pmod{4}$. Se o inteiro for ímpar, digamos $2a + 1$, o seu quadrado é $4a^2 + 4a + 1$, que é $\equiv 1 \pmod{4}$.

Segue-se que uma soma de quadrados ou é $\equiv 0 \pmod{4}$, ou $\equiv 1 \pmod{4}$, ou $\equiv 2 \pmod{4}$. Logo, nunca é $\equiv 3 \pmod{4}$, isto é, não existem inteiros x e y que satisfaçam a congruência $x^2 + y^2 \equiv 3 \pmod{4}$. Concluimos assim que a equação $x^2 + y^2 = 4z + 3$ não tem soluções inteiras. ■

Claro que o problema na aplicação desta técnica está em encontrar um m conveniente.

Exercício. Mostre que a equação $x^2 + y^2 = 9z + 3$ não tem soluções inteiras.

O terceiro tema desta secção consiste em estudar dois casos especiais da equação

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

conhecida por *equação de Fermat*.

O primeiro caso que vamos estudar é o caso $n = 2$. Interessa-nos portanto encontrar as soluções inteiras da equação

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

e é evidente que basta procurar as soluções naturais.

Uma interpretação geométrica desta questão é que estamos interessados em determinar triângulos rectângulos cujos lados têm medidas inteiras. Devido a esta interpretação geométrica, um trio (x, y, z) de números naturais satisfazendo $x^2 + y^2 = z^2$ diz-se um *trio pitagórico*.

Exemplo. $(3, 4, 5)$ é um trio pitagórico, porque $3^2 + 4^2 = 5^2$.

Uma primeira observação é a seguinte: se (x, y, z) for um trio pitagórico e k for um número natural qualquer, é evidente que (kx, ky, kz) também é um trio pitagórico. Por exemplo, $(6, 8, 10)$ é um trio pitagórico.

Definição. Um trio pitagórico cujos elementos são primos entre si diz-se *primitivo*.

Claramente, basta procurar os trios pitagóricos primitivos. Vamos de seguida ver uma sequência de condições que tais trios têm que satisfazer.

Proposição 1. Se (x, y, z) for um trio pitagórico ~~primitivo~~, x e y não podem ser ambos ímpares.

Demonstração. Vamos por absurdo. Suponhamos que x e y são ambos ímpares, digamos $x = 2a + 1$ e $y = 2b + 1$. Então $x^2 + y^2 \equiv 2 \pmod{4}$. Por outro lado, como x^2 e y^2 também são ímpares, z^2 é par, pelo que também z é par, digamos $z = 2c$. Então $z^2 = 4c^2$, pelo que $z^2 \equiv 0 \pmod{4}$: contradição, uma vez que estamos a supor que $x^2 + y^2 = z^2$. ■

Assim, dos dois números x e y , pelo menos um é par. Sem perda de generalidade, supomos a partir de agora que é o y (se fosse o x o raciocínio era análogo).

Proposição 2. Se (x, y, z) for um trio pitagórico primitivo com y par, x e z têm que ser ímpares.

Demonstração. Se y é par, então x tem que ser ímpar, porque se não 2 era um divisor comum de x , y e z . Sendo x ímpar, z também tem que ser ímpar, porque $x^2 + y^2 = z^2$. ■

Proposição 3. Se (x, y, z) for um trio pitagórico primitivo com y par, tem-se $(z + x, z - x) = 2$.

Demonstração. Claramente $z + x$ e $z - x$ são ambos números pares, pelo que $2 \mid (z + x, z - x)$. Ponhamos $(z + x, z - x) = 2d$. Então $2d \mid z + x$ e $2d \mid z - x$. Daqui tira-se, por um lado, que $2d$ divide a soma e a diferença de $z + x$ e $z - x$, isto é, $2d \mid 2z$ e $2d \mid 2x$, donde $d \mid z$ e $d \mid x$. Por outro lado, multiplicando membro a membro aquelas duas relações de divisibilidade, vemos que $4d^2 \mid (z + x)(z - x)$, isto é, $4d^2 \mid z^2 - x^2$, ou seja $4d^2 \mid y^2$, donde $2d \mid y$ e portanto, claro, também $d \mid y$. Como $d \mid x$, $d \mid y$ e $d \mid z$ e x , y e z são primos entre si, d tem que ser igual a 1. ■

Desta proposição concluímos que $z + x = 2h$ e $z - x = 2k$ com $(h, k) = 1$. Segue-se que

$$y^2 = z^2 - x^2 = (z + x)(z - x) = 4hk.$$

Mas y é par, digamos $y = 2s$. Logo, tem-se $4s^2 = 4hk$, donde $s^2 = hk$, isto é, hk é um quadrado perfeito. Como h e k são primos entre si, o facto de o seu produto ser um quadrado perfeito implica que cada um deles seja também um quadrado perfeito (porquê?). Tem-se assim $h = a^2$ e $k = b^2$, com a e b números naturais ainda primos entre si. Em resumo, tem-se:

$$\begin{cases} z + x = 2a^2 \\ z - x = 2b^2 \\ y^2 = 4a^2b^2 \end{cases} \quad \text{o que é o mesmo que} \quad \begin{cases} x = a^2 - b^2 \\ y = 2ab \\ z = a^2 + b^2 \end{cases}.$$

Note-se que, evidentemente, se tem $a > b$, e que a e b têm que ter paridades diferentes (se não, x e z não seriam ímpares).

Demonstrámos assim o seguinte:

Teorema. Se (x, y, z) for um trio pitagórico primitivo com y par, então existem dois números naturais a e b , primos entre si, de paridades diferentes e com $a > b$, tais que

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2.$$

Reciprocamente, é imediato que três números x , y e z desta forma constituem um trio pitagórico com y par, e podemos também ver que se trata de um trio pitagórico primitivo. (Exercício: Prove isso.)

Descrevemos assim todos os possíveis trios pitagóricos primitivos (x, y, z) com y par.

Exemplos. Tomando $a = 2$ e $b = 1$, obtemos o trio pitagórico $(3, 4, 5)$.

Tomando $a = 4$ e $b = 1$, obtemos o trio pitagórico $(15, 8, 17)$.

Tomando $a = 3$ e $b = 2$, obtemos o trio pitagórico $(5, 12, 13)$.

O segundo caso da equação de Fermat que vamos estudar é o caso $n = 4$. Interessa-nos portanto procurar as soluções naturais da equação

$$x^4 + y^4 = z^4.$$

Já voltaremos a esta equação, mas primeiro analisemos a equação $x^4 + y^4 = z^2$, que foi estudada pelo próprio Fermat.

Suponhamos que um trio (x, y, z) de números naturais é solução desta equação. Tal como no caso anterior, podemos supor que x , y e z são primos entre si e que y é par, donde se segue que x e z têm que ser ímpares.

Do facto de que (x, y, z) é uma solução da equação $x^4 + y^4 = z^2$ concluimos que (x^2, y^2, z) é um trio pitagórico, e é primitivo, porque se x , y e z são primos entre si também x^2 , y^2 e z são primos entre si (porquê?). Como y^2 é par, por y o ser, podemos aplicar o Teorema acima visto. Existem portanto dois números naturais a e b , primos entre si, de paridades diferentes e com $a > b$, tais que

$$x^2 = a^2 - b^2, \quad y^2 = 2ab, \quad z = a^2 + b^2.$$

Observemos que este b tem que ser par. Se b fosse ímpar, a seria par (porque a e b têm paridades diferentes), digamos $a = 2k$ e $b = 2h + 1$. Viria então

$$x^2 = a^2 - b^2 = 4k^2 - (4h^2 + 4h + 1) = 4(k^2 - h^2 - h) - 1 \equiv -1 \pmod{4}$$

o que não pode ser, porque o quadrado de um número ímpar é sempre $\equiv 1 \pmod{4}$.

Por outro lado, temos $x^2 + b^2 = a^2$ e $(x, b, a) = (x, (a, b)) = (x, 1) = 1$. Logo, (x, b, a) é um trio pitagórico primitivo em que o segundo número é par. Aplicando de novo o Teorema sobre os trios pitagóricos, podemos afirmar que existem dois números naturais c e d , primos entre si, de paridades diferentes e com $c > d$, tais que

$$x = c^2 - d^2, \quad b = 2cd, \quad a = c^2 + d^2.$$

Daqui sai que $y^2 = 4cd(c^2 + d^2)$, isto é, $4cd(c^2 + d^2)$ é um quadrado perfeito.

Notemos agora que c , d e $c^2 + d^2$ são primos dois a dois. Porquê? Já sabemos que $(c, d) = 1$. Designemos $(c, c^2 + d^2)$ por δ . Como δ divide c , também divide c^2 . Daqui segue-se, como δ divide $c^2 + d^2$, que δ divide d^2 . Logo, δ divide (c^2, d^2) , que é igual a 1 por (c, d) o ser. Portanto, $\delta = 1$. Analogamente, tem-se que $(d, c^2 + d^2) = 1$.

Como $4cd(c^2 + d^2)$ é um quadrado perfeito e c , d e $c^2 + d^2$ são primos dois a dois, concluímos que c , d e $c^2 + d^2$ também são quadrados perfeitos (porquê?), digamos

$$c = e^2, \quad d = f^2, \quad c^2 + d^2 = g^2.$$

Daqui tiramos, finalmente, que

$$e^4 + f^4 = g^2.$$

Mas agora observemos que

$$g \leq g^2 = c^2 + d^2 = a \leq a^2 < z.$$

Ou seja, tem-se $\underline{g < z}$. Isto é, a partir de um trio solução da equação $x^4 + y^4 = z^2$ chegámos a outro trio solução da mesma equação em que o terceiro número é mais pequeno que o terceiro número do trio original. Podemos agora repetir este processo e vamos obtendo números naturais sempre estritamente mais pequenos. Mas é evidente que isto não pode ser: não é possível arranjar uma sucessão infinita de números naturais estritamente decrescente.

Podemos portanto concluir o seguinte:

Teorema. A equação $x^4 + y^4 = z^2$ não tem soluções inteiras.

E temos a consequência imediata:

Corolário. A equação $x^4 + y^4 = z^4$ não tem soluções inteiras.

Vemos assim que a equação de Fermat $x^n + y^n = z^n$ tem uma infinidade de soluções inteiras quando $n = 2$, mas não tem nenhuma solução inteira quando $n = 4$.

Por volta de 1630, Fermat, estudando uma tradução francesa da *Arithmetica* de Diofanto, escreveu na margem do livro:

“É impossível escrever um cubo como soma de dois cubos, uma quarta potência como soma de duas quartas potências, e em geral uma potência de expoente maior que 2 como soma de duas potências de igual expoente. Descobri uma demonstração maravilhosa desse facto, mas esta margem é demasiado estreita para a conter.”

Ou seja: Fermat afirmou que, para $n > 2$, a equação $x^n + y^n = z^n$ não tem soluções inteiras.

Nenhuma demonstração deste facto foi encontrada nos papéis de Fermat, e desde então muitos matemáticos tentaram demonstrar aquela afirmação, que começou a ser conhecida como o “Último Teorema de Fermat”, embora em rigor se tratasse apenas de uma conjectura.

O próprio Fermat provou o teorema no caso $n = 4$, utilizando a técnica acima descrita, que ficou conhecida como o método da “descida infinita”.

Em 1770, o suíço Euler provou o teorema no caso $n = 3$, que é bastante mais difícil do que o caso $n = 4$.

Note-se que, depois de provado o teorema no caso $n = 4$, basta estudar o caso em que o expoente é um primo ímpar. Isto pela razão seguinte. Consideremos um expoente n qualquer > 2 . Se n for um múltiplo de 4, digamos $n = 4k$, então a equação $x^n + y^n = z^n$ não tem de certeza soluções inteiras, porque, se as tivesse, também a equação com expoente 4 as teria, pois se $n = 4k$ a equação $x^n + y^n = z^n$ é equivalente a $(x^k)^4 + (y^k)^4 = (z^k)^4$.

Se n não for um múltiplo de 4, n é de certeza divisível por um primo ímpar p , digamos $n=qp$. Se a equação $x^n+y^n=z^n$ tiver soluções inteiras, também a equação com expoente p as tem, pois sendo $n=qp$ a equação $x^n+y^n=z^n$ é equivalente a $(x^q)^p+(y^q)^p=(z^q)^p$.

Basta portanto estudar o caso em que o expoente é um primo ímpar.

No século XIX, vários matemáticos foram provando o teorema para expoentes cada vez maiores. O alemão Dirichlet provou em 1825 que o teorema vale para $n=5$. O francês Lamé provou em 1839 que o teorema vale para $n=7$. O alemão Kummer introduziu técnicas algébricas novas que permitiram provar o teorema para outros valores de n .

No século XX muitos autores publicaram demonstrações erradas do resultado geral.

Em 1983, o alemão Faltings (então com 29 anos) provou que, para cada $n > 2$, a equação $x^n + y^n = z^n$ tem no máximo um número finito de soluções (trios de inteiros em que os números são primos entre si), o que foi um grande progresso no sentido da demonstração do resultado geral, que afirma que esse número é zero.

Usando técnicas baseadas no trabalho de Kummer, em 1993 provou-se, com a ajuda de computadores, que o teorema é válido para todos os expoentes $n \leq 4000000$.

Finalmente, em 1995, o inglês Wiles, num trabalho extenso e difícil, demonstrou que o Último Teorema de Fermat é verdadeiro (para todos os expoentes $n > 2$).⁶ Os resultados e técnicas utilizados mostram que o Último Teorema de Fermat não é uma curiosidade isolada da Teoria dos Números, mas tem relações profundas com muitos outros importantes temas da Matemática.

⁶ Andrew Wiles, Modular elliptic curves and Fermat's Last Theorem, *Annals of Mathematics*, vol. 141 (1995), p. 443-531.

10 Aplicações da Teoria dos Números

Neste capítulo estudaremos dois exemplos de aplicação prática da Teoria dos Números.

10.1 Sistemas de identificação numérica⁷

De há umas décadas para cá, tornou-se corrente identificar toda a espécie de entidades ou produtos por números, de forma que a cada entidade ou tipo individual de produto corresponda um número preciso. Esta prática permite simplificar, por exemplo, o processamento de bases de dados, a catalogação de livros, a gestão de *stocks*, etc.

A atribuição de números a entidades ou produtos é em princípio um processo muito simples, bastando aparentemente ter o cuidado de atribuir números diferentes a entidades diferentes.

Mas põe-se um problema. Estes números vão, pela sua natureza, ser frequentemente escritos, armazenados em listas e computadores, lidos e transmitidos por diversas formas. Existe assim a possibilidade de *erros* no seu registo, leitura e transmissão.

Surge então a necessidade de conceber sistemas de identificação numérica que permitam, no decurso das normais actividades de registo, leitura e transmissão dos números, *detectar* esses erros e intervir para corrigir qualquer eventual problema na identificação. A principal técnica usada é a *junção* a cada número de um *algarismo de controlo* de acordo com uma regra bem definida.

A experiência mostra que os principais erros cometidos são de dois tipos: erros num só algarismo – estes são a grande maioria – e erros de troca de dois algarismos consecutivos. É portanto à detecção destes tipos de erros que é dedicada maior atenção.

Vamos aqui referir-nos a dois sistemas muito conhecidos e às suas propriedades.

O primeiro destes sistemas é o EAN (*European Article Number*), um sistema de identificação de produtos comerciais usado na Europa e em muitos países fora da Europa.⁸ O número de cada produto, com treze algarismos, é normalmente acompanhado por uma versão apropriada para leitura por uma máquina, o chamado “código de barras”, visível em todos os produtos de consumo corrente.

⁷ Sobre este tema, com mais desenvolvimento, ver Jorge Picado, A álgebra dos sistemas de identificação, *Boletim da Sociedade Portuguesa de Matemática* n.º 44 (2001), p. 39-73.

⁸ Nos Estados Unidos e no Canadá existe um sistema parecido.

Os primeiros sete algarismos do número EAN de um produto identificam o produtor, sendo que, destes sete, um primeiro grupo identifica a instituição – não necessariamente uma por país – emissora deste prefixo identificador da empresa.⁹ Os cinco algarismos seguintes constituem o número do produto dentro do catálogo da empresa produtora, e são da responsabilidade desta. O 13^o e último algarismo é o algarismo de controlo. Como é calculado este algarismo?

Designemos os treze algarismos por

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}.$$

Multipliquemos os algarismos com índice par por 3 e somemos todos esses produtos com a soma dos algarismos com índice ímpar. Ou seja: formemos a soma

$$a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + a_{13}.$$

A esta soma chamamos *soma de controlo*. A condição que impomos para a determinação de a_{13} é que esta soma seja divisível por 10. Isto é, a_{13} é escolhido de forma que

$$\sum_{i \text{ ímpar}} a_i + \sum_{i \text{ par}} 3a_i \equiv 0 \pmod{10}.$$

Note-se que esta condição determina univocamente o algarismo de controlo a_{13} a partir dos outros doze.

Exercício. Se os primeiros doze algarismos do número EAN de um produto forem

$$560104822260$$

qual é o algarismo de controlo?

Sempre que uma máquina lê o número EAN de um produto, calcula a soma de controlo e verifica se a condição exigida é satisfeita. Se não for, há de certeza um erro no número do produto.

Que propriedades de detecção de erros possui este sistema de identificação numérica?

⁹ No caso de Portugal, este primeiro grupo tem os algarismos 560.

Proposição. O sistema EAN permite detectar erros num só algarismo.

Demonstração. Suponhamos que há um erro no algarismo a_i , que está substituído pelo algarismo a'_i . Designemos por S a soma de controlo com os algarismos correctos. Então tem-se

$$S \equiv 0 \pmod{10}.$$

Designemos agora por S' a soma de controlo com o algarismo a'_i na posição de a_i .

Suponhamos que também se tinha $S' \equiv 0 \pmod{10}$ e calculemos a diferença $S - S'$.

Se i for ímpar, tem-se $S - S' = a_i - a'_i$. Como tanto S como S' satisfazem a condição de controlo, ter-se-ia

$$a_i - a'_i \equiv 0 \pmod{10}$$

o que é impossível, porque a_i e a'_i são números distintos entre 0 e 9.

Se i for par, tem-se $S - S' = 3(a_i - a'_i)$. Como tanto S como S' satisfazem a condição de controlo, ter-se-ia

$$3(a_i - a'_i) \equiv 0 \pmod{10}.$$

Daqui viria, como 3 e 10 são primos entre si, que também $a_i - a'_i \equiv 0 \pmod{10}$, o que é impossível, pela mesma razão que atrás. ■

Como as máquinas de leitura de códigos de barras praticamente nunca cometem outros erros além dos erros num só algarismo, o sistema EAN é satisfatório. Note-se que um sistema análogo ao EAN em que a condição de controlo fosse simplesmente

$$\sum_{i=1}^{13} a_i \equiv 0 \pmod{10}$$

também detectaria esses erros, como se vê imediatamente com um raciocínio análogo ao da demonstração vista. A vantagem da introdução dos coeficientes 3 do sistema EAN está em que, conforme vamos ver a seguir, ele detecta também a maioria dos erros de troca de dois algarismos consecutivos, que uma condição de controlo com todos os coeficientes iguais a 1 deixaria evidentemente escapar.

Proposição. O sistema EAN permite detectar os erros de troca de dois algarismos consecutivos desde que a diferença entre estes não seja 5 (ou -5).

Demonstração. Suponhamos que há uma troca entre os algarismos a_i e a_{i+1} . Só interessa considerar o caso em que a_i e a_{i+1} são distintos. Designemos por S a soma de controlo com os algarismos na posição certa. Então tem-se

$$S \equiv 0 \pmod{10}.$$

Designemos agora por S' a soma de controlo com os algarismos a_i e a_{i+1} trocados. Poderá ter-se $S' \equiv 0 \pmod{10}$?

Calculemos a diferença $S - S'$. Se i for par, tem-se $S - S' = 2(a_i - a_{i+1})$. Se i for ímpar, tem-se $S - S' = 2(a_{i+1} - a_i)$. Tem-se então

$$S' \equiv 0 \pmod{10} \iff S - S' \equiv 0 \pmod{10}$$

$$\iff 10 \mid 2(a_i - a_{i+1})$$

$$\iff a_i - a_{i+1} = \pm 5.$$

Ou seja: a condição de controlo para o número com os algarismos a_i e a_{i+1} trocados só é satisfeita se a diferença entre a_i e a_{i+1} for 5 ou -5 . ■

O segundo sistema de que vamos falar é o ISBN (*International Standard Book Number*). Este sistema associa um número¹⁰ a todos (ou quase todos) os livros publicados no mundo. Esse número, composto por dez algarismos, pode ver-se normalmente na contra-capa e na ficha técnica no verso do frontispício do livro.

Como é “construído” o número ISBN de cada livro?

Um primeiro grupo de algarismos (que pode ter um, dois ou mais algarismos) identifica uma língua, um país ou um grupo de países ou regiões.¹¹ Um segundo grupo, também de comprimento variável, identifica a empresa editora. O terceiro grupo de algarismos constitui o número do livro dentro do catálogo da empresa editora. O 10º e último algarismo é o algarismo de controlo. Como é calculado este?

¹⁰ De facto, como veremos, nem sempre é exactamente um número.

¹¹ No caso de Portugal, este primeiro grupo tem os algarismos 972 (ou 989).

Designemos os dez algarismos por

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}.$$

Formemos a *soma de controlo*

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + a_{10}.$$

A condição que impomos para a determinação de a_{10} é que esta soma seja divisível por 11. Isto é, a_{10} é escolhido de forma que

$$\sum_{i=1}^{10} (11 - i) a_i \equiv 0 \pmod{11}.$$

Esta condição determina univocamente o algarismo de controlo a_{10} a partir dos outros dez. Mas há aqui uma diferença relativamente ao sistema EAN. Como estamos a usar congruências módulo 11, os números de 0 a 9 não chegam para esgotar os valores possíveis para a_{10} : a condição de controlo pode fazer com que a_{10} seja igual a 10. Para usar apenas um símbolo, adopta-se nesse caso para a_{10} a letra maiúscula X.

Exercício. Se os primeiros nove algarismos do número ISBN de um livro forem

$$972674315$$

qual é o algarismo de controlo?

Vamos agora ver que propriedades de detecção de erros possui o sistema ISBN.

Proposição. O sistema ISBN permite detectar erros num só algarismo.

Demonstração. Suponhamos que há um erro no algarismo a_i , que está substituído pelo algarismo a'_i . Designemos por S a soma de controlo com os algarismos correctos. Então tem-se

$$S \equiv 0 \pmod{11}.$$

Designemos agora por S' a soma de controlo com o algarismo a'_i na posição de a_i .

Suponhamos que também se tinha $S' \equiv 0 \pmod{10}$ e calculemos a diferença $S - S'$. Tem-se

$$S - S' = (11 - i)(a_i - a'_i)$$

donde, por S e S' satisfazerem a condição de controlo,

$$(11 - i)(a_i - a'_i) \equiv 0 \pmod{11}$$

ou

$$i(a_i - a'_i) \equiv 0 \pmod{11}.$$

Como i é um número entre 1 e 10, tem-se $(i, 11) = 1$. Logo, vem $a_i - a'_i \equiv 0 \pmod{11}$, o que é impossível, porque a_i e a'_i são números distintos entre 0 e 10. ■

Vamos ver a seguir que o sistema ISBN vai mais longe que o sistema EAN na detecção de erros.

Proposição. O sistema ISBN permite detectar os erros de troca de dois algarismos, mesmo que não sejam consecutivos.

Demonstração. Suponhamos que há uma troca entre os algarismos a_i e a_j . Podemos supor $i < j$ e evidentemente só interessa considerar o caso em que a_i e a_j são distintos. Designemos por S a soma de controlo com os algarismos na posição certa. Então tem-se

$$S \equiv 0 \pmod{11}.$$

Designemos agora por S' a soma de controlo com os algarismos a_i e a_j trocados e suponhamos que também se tem $S' \equiv 0 \pmod{11}$. Calculemos a diferença $S - S'$:

$$S - S' = (11 - i)a_i + (11 - j)a_j - (11 - i)a_j - (11 - j)a_i.$$

Como $S - S' \equiv 0 \pmod{11}$, isto significa que

$$-ia_i - ja_j + ia_j + ja_i \equiv 0 \pmod{11}$$

o que é o mesmo que

$$(j - i)(a_i - a_j) \equiv 0 \pmod{11}.$$

Como $j - i$ é um número entre 1 e 9, tem-se $(j - i, 11) = 1$. Logo, vem $a_i - a_j \equiv 0 \pmod{11}$, o que é impossível, porque a_i e a_j são números distintos entre 0 e 10. ■

Recentemente, a *International Standards Organization* (ISO) introduziu uma profunda alteração no sistema ISBN: também os livros passaram a ser identificados por 13 algarismos, como os restantes produtos de consumo corrente. O objectivo principal foi o de alinhar o sistema de numeração dos livros com o sistema EAN, cujo uso se globalizou.

Como funciona o chamado ISBN-13? Muito simplesmente, para cada livro começa-se por calcular os nove algarismos que seria necessário calcular para o ISBN-10 clássico. A estes nove algarismos antepõe-se o prefixo 978. À sequência de doze algarismos assim obtida acrescenta-se no final um algarismo de controlo calculado como no sistema EAN acima descrito.

A partir de 1 de Janeiro de 2007, o uso do ISBN-13 tornou-se obrigatório, mas as recomendações internacionais são no sentido de que, durante algum tempo, e para facilitar a transição, os livros exibam os dois números: o ISBN-10 e o ISBN-13.

Note-se que, como é óbvio, os algarismos de controlo não têm que ser os mesmos nos dois casos. Tomemos o exemplo do livro *An Introduction to the Theory of Numbers*, de I. Niven, H. Zuckerman e H. Montgomery, 5^a ed., New York, John Wiley & Sons, 1991. O seu ISBN-10 é 0471546003 e o seu ISBN-13 é 978-0471546009.

10.2 O sistema criptográfico RSA

A *criptografia* é a ciência que se ocupa das comunicações secretas, comunicações em que há um emissor e um receptor e se pretende que nenhum terceiro tenha acesso à informação transmitida. Para atingir este objectivo, a informação, ou mensagem, é *cifrada*, isto é, substituída por outra, conforme uma regra pré-estabelecida. O receptor tem que *decifrar* a informação recebida, de forma a reconstituir a mensagem original.

A criptografia tem uma longa história, associada principalmente a comunicações militares. Uma das técnicas mais simples, e mais antigas, é a simples substituição de cada letra do alfabeto por outra de acordo com uma tabela fixa.¹² Esta técnica não é muito eficaz, já que é simples decifrar mensagens cifradas desta forma usando tabelas de frequência das letras na língua em causa.

Ao longo dos anos desenvolveram-se técnicas muito variadas e progressivamente mais sofisticadas, que não podemos analisar aqui.¹³

Um método recente, muito interessante, utiliza resultados elementares de Teoria dos Números, nomeadamente o Teorema de Euler, já estudado. Recorde-se que este teorema afirma que, sendo m um número natural, se a for um inteiro primo com m tem-se $a^{\varphi(m)} \equiv 1 \pmod{m}$, onde φ é a função de Euler.

O resultado central é o seguinte:

Proposição. Seja m um número natural e seja a um inteiro primo com m . Sendo k e h números naturais, tem-se que, se $kh \equiv 1 \pmod{\varphi(m)}$, então $a^{kh} \equiv a \pmod{m}$.

Demonstração. Se $kh \equiv 1 \pmod{\varphi(m)}$, tem-se $kh = 1 + t\varphi(m)$ para certo inteiro não-negativo t . Vem então

$$a^{kh} = a^{1+t\varphi(m)} = a \cdot a^{t\varphi(m)} = a \cdot (a^{\varphi(m)})^t \equiv a \pmod{m}$$

onde usámos o Teorema de Euler. ■

¹² Uma técnica de cifragem deste tipo, associada ao nome de Júlio César, consiste na substituição de cada letra pela letra que está três posições à frente no alfabeto: A por D, B por E, etc., até Z por C.

¹³ Uma referência simples é A. Sinkov, *Elementary cryptanalysis: a mathematical approach*, The Mathematical Association of America, Washington, 1966.

O método criptográfico que se baseia neste resultado parte de um número natural m , a escolher pelo receptor de uma forma que já se verá qual é. O receptor divulga também um número natural k primo com $\varphi(m)$.

Para enviar uma mensagem, começamos por representá-la por um inteiro a entre 0 e $m - 1$ e primo com m . Isto pode fazer-se de muitas maneiras, por exemplo representando cada letra da mensagem pelo seu código ASCII.¹⁴ Se necessário, divide-se a mensagem em vários blocos.

A cifragem da mensagem a consiste em calcular a^k módulo m . Mais precisamente, a mensagem cifrada é o resto b da divisão de a^k por m .

O receptor recebe a mensagem cifrada b . Como procede para a decifrar?

Como k é primo com $\varphi(m)$, a congruência $kx \equiv 1 \pmod{\varphi(m)}$ tem solução. Seja h a menor solução positiva desta congruência (que se pode calcular usando o algoritmo de Euclides e adicionando múltiplos convenientes de $\varphi(m)$). Então tem-se $kh \equiv 1 \pmod{\varphi(m)}$, donde, pela Proposição, $a^{kh} \equiv a \pmod{m}$, isto é, $b^h \equiv a \pmod{m}$.

Ou seja: para reaver a a partir de b , o receptor apenas tem de calcular b^h módulo m . Mais precisamente, a mensagem decifrada a é o resto da divisão de b^h por m .

O que é interessante nisto é que o receptor divulga m e k , isto é, divulga publicamente a *chave de cifragem* para as mensagens que lhe são enviadas. Mas *não* divulga h , a chave necessária para a decifragem.

Para isto fazer sentido é necessário que h seja muito difícil de calcular para outra pessoa que não o receptor.

Tudo depende de uma boa escolha de m . Escolham-se dois números primos p e q muito grandes ao acaso e faça-se $m = pq$. O número m é tornado público mas os factores p e q são mantidos secretos pelo receptor.

¹⁴ *American Standard Code for Information Interchange.*

Pelas propriedades já estudadas da função φ , tem-se

$$\varphi(m) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

Para calcular h é necessário conhecer $\varphi(m)$ e, portanto, é necessário conhecer p e q . Ora, se p e q forem muito grandes é muito difícil, mesmo usando computadores poderosos, obter os factores p e q a partir do seu produto m .

Há assim uma assimetria entre os processos de cifragem e de decifragem. Saber cifrar uma mensagem utilizando este método não significa que se consiga depois decifrá-la.

Este método criptográfico, dito “de chave pública”, é conhecido por método RSA, do nome dos três matemáticos que o inventaram.¹⁵

¹⁵ R. L. Rivest, A. Shamir e L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the Association for Computing Machinery*, vol. 21 (1978), p. 120-126.