A teoria dos números (elementar) é no essêncial a teoria dos números inteiros $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Encontram-se de entre os problemas postos nas olimpíadas matemáticas frequentemente uns que se referem a este ramo da matemática.

O presente texto preliminar, na sua estrutura altamente influenciado pelos primeiros dois capítulos do livro de Ivan Niven e Herbert S. Zuckerman, 'An Introduction to the Theory of Numbers', J. Wiley 1960, pretendemos familiarizar os participantes das olimpíadas com uns conceitos e ferramentas necessárias para tratar os problemas referidos. (Por razões redaccionais que se prendem com a possível extensão deste texto no futuro e os inerentes perigos de gralhas em necessárias re-numerações dos teoremas, a numeração dos mesmos segue, para já, no essêncial N.&Z; facto que explica certas irregularidades da mesma.)

É coisa de extraordinária importância debruçar-se sobre exercícios e problemas. O texto contém uma gama de exercícios fáceis que visam a consolidação da matéria transmitida, e um bom número de problemas mais difíceis que precisam para a resolução já de duas ou mais ideias.

O leitor experimente regularmente as suas capacidades com problemas que acha difíceis. Contudo, para que não gaste demasiado de seu tempo com uns poucos problemas que não consegue fazer sugere-se que não trabalhe mais que uma hora por dia num determinado problema e que voltem a tais problemas nos dias seguintes e tente entretanto outros.

Os problemas dos olimpíadas são raramente fáceis. Exigem para além de conhecimentos básicos e domínio de ferramentas adequadas ainda ideias adicionais. Revimos problemas típicos de olimpíadas internacionais e incluímo-los neste texto. Assinalámos problemas particularmente recomendados por um asterisco (*). De ideias para resolver problemas mais difíceis lembrar-se-ão por vezes melhor depois de terem feito certos outros exercícios; eles vos darão pistas para a solução.

1. Divisibilidade

Por um 'número' ou um 'inteiro' entendemos neste texto, salvo menção em contrário um número inteiro, isto é um elemento do conjunto $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Mesmo estas palavras podem faltar se o contexto implica, ou se for implicitamente entendido, que se trata dum inteiro.

Definição 1.1. Um inteiro b diz-se *divisível* por inteiro $a \neq 0$ se existir um inteiro x tal que $b = ax$; escreve-se $a \,|\, b$.

Assim por exemplo $4 \,|\, 12$, $23 \,|\, 69$, mas 7 não divide 9: $7 \not| 9$.

O conjunto de todos os a tal que $a \,|\, b$ diz-se o conjunto dos *divisores* de b.

Exercício 1.1. Escreve o conjunto dos divisores de 84 e de 115. (Números negativos podem também ser divisores!)

Teorema 1.1. *i.* $a \,|\, b$ *implica* $a \,|\, bc$.
ii. $a \,|\, b$ *e* $b \,|\, c$ *implica* $a \,|\, c$.
iii. Se $a \,|\, b$ *e* $a \,|\, c$ *então* $a \,|\, (bx + yc)$.
iv. Se $a \,|\, b$ *e* $b \,|\, a$ *então* $a = \pm b$.
v. Se $a \,|\, b$, $a > 0, b > 0$ *então* $a \leq b$.

Demonstração. As afirmações são consequências imediatas das definições; assim por exemplo se $a \,|\, b$, então existe um x tal que $b = ax$; portanto $bc = axc$. Sendo xc um inteiro tem-se $a \,|\, bc$, o que prova (i). Os restantes factos deixamo como exercício. ■

Teorema 1.2. *Dados* a, b *com* $a > 0$. *Então:*
i. Existem inteiros q, r *tal que* $b = qa + r$ *e* $0 \leq r < a$.
ii. $a \,|\, b$ *se e somente se* $r = 0$.
Os inteiros q *e* r *nas condições expressas em (i) são determinados por* a *e* b *e únicos.*

Demonstração. Consideremos a sucessão aritmética $\{b + qa\}_{q=-\infty}^{+\infty}$ obtida, percorrendo com q os inteiros. Obtemos

$$\ldots, b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, \ldots; \qquad (*)$$

uma sucessão que se estende indefinidamente para as direções negativa e positiva. Seleccionamos o número não-negativo mais pequeno. A este chamemos r. Como a diferênça entre dois números sucessivos de (*) é a, obtém-se a desigualdade em (i). Agora (ii) é óbvio. ■

Exercício 1.2. Para o caso $a = 7, b = 51$, escreve os elementos da sucessão contidos num intervalo que contém 0, por exemplo em $[-30, 20]$. Qual o valor de r? Verifica o enunciado do teorema.

Se $a|b_1, \ldots, a|b_n$, então a diz se *divisor comum* de $b_1, b_2, \ldots, b_n$. O *máximo* divisor comum destes números (que obviamente sempre existe e que é único e positivo) denota-se por $(b_1, \ldots, b_n)$.

Teorema 1.3. *Dados inteiros não zeros* b, c *existem inteiros* x_0, y_0 *tal que* $(b, c) = bx_0 + cy_0$

Demonstração. Consideremos o conjunto dos inteiros $\{bx + cy : x, y \in \mathbb{Z}\}$. Seja l =menor número positivo do conjunto: $l = \min\{bx + cy : bx + cy > 0, x, y \in \mathbb{Z}\}$. Existem x_0, y_0 tais que $l = bx_0 + cy_0$. Afirmamos: $l \,|\, b$ e $l \,|\, c$.

Ora, pelo último teorema achamos q e $0 \leq r < l$ tal que $b = lq + r$ ou seja:

$$\begin{aligned} r &= b - lq = b - q(bx_0 + cy_0) \\ &= b(1 - qx_0) + c(-qy_0) \in \{bx + cy\}. \end{aligned}$$

Sendo $r \in \{bx + cy\}$ temos necessariamente por definição de l e a propriedade de r, que $r = 0$, e portanto $l \,|\, b$.

Exercício 1.3. i. Escreva uns elementos do conjunto $\{bx + cy : x, y \in \mathbb{Z}\}$ para o caso $b = 21, c = -24$. Verifique que o menor elemento positivo que se pode gerar é de facto o máximo divisor comum de $21, -24$.
ii. Mostre por raciocínio análogo do acima que tambem $l \,|\, c$. Assim arranjámos um divisor comum, a saber l, de b, c.

Provaremos agora que l é o máximo divisor comum de b, c. Ora $l = bx_0 + cy_0$. Se g é divisor comum de b, c isto é se e $g \,|\, b$ e $g \,|\, c$, então é óbvio (v. teorema 1.1 iii) que $g \,|\, l$, logo (teorema 1.1 (v)) $g \leq l$. O teorema fica provado. ■

Observação . Exercícios e problemas são enumerados continuamente; designamos por 'problema' exercícios que, julgamos, são mais dificeis.

Problema 1.1. *i. Achar inteiros x_0, y_0 que servem para provar simultaneamente que $(4, 3) = 1$, $(25, 17) = 1$, $(46, 31) = 1$, isto é tais que $4x_0 + 3y_0 = 1$, $25x_0 + 17y_0 = 1$ e $46x_0 + 31y_0 = 1$.*
ii. Mostra que os números $4, 25, 46$ são elementos sucessivos dum certo conjunto $\{an + b : n \in \mathbb{Z}\}$ (procura a, b) , e os números $3, 17, 31$ elementos sucessivos dum certo outro tal conjunto $\{a'n + b' : n \in \mathbb{Z}\}$.
iii. Mostra que para todos os n o máximo divisor comum de $an + b$ e $a'n + b'$ é 1.

Por raciocínio análogo ao do teorema 1.3 prova-se:
O máximo divisor comum de n inteiros $b_1, \ldots, b_n$, nem todos zeros, é o menor número positivo assumido pela expressão $b_1x_1 + b_2x_2 + \ldots b_nx_n$ quando $x_1, \ldots, x_n$ percorre os inteiros.

Expressões do tipo $b_1x_1 + b_2x_2 + \ldots b_nx_n$ dizem-se *combinações lineares* de $b_1, \ldots, b_n$; $x_1, \ldots, x_n$ dizem-se coeficientes. (Noutras teorias matemáticas, os coeficientes são escritos frequentemente antes dos elementos da estrutura-base - aqui os b_i.)

Assim, o que acabamos de dizer é o seguinte:

O máximo divisor comum de n inteiros $b_1, \ldots, b_n$, nem todos zeros, é o menor número positivo assumido pelas combinações lineares de $b_1, \ldots, b_n$ com coeficientes inteiros.

O seguinte teorema tem uma demonstração simples:

Teorema 1.4. *i. Se $m > 0$, então: $(ma, mb) = m(a, b)$.*
ii. Se $d|a, d|b$ e $d > 0$ então $(\frac{a}{d}, \frac{b}{d}) = \frac{(a,b)}{d}$.
iii. Se $(a, b) = g$ então $(\frac{a}{g}, \frac{b}{g}) = 1$.

Demonstração. Deixado aos alunos ■

Teorema 1.5. *Se $(a, m) = (b, m) = 1$, então $(ab, m) = 1$.*

Demonstração. Por teorema 1.3 achamos inteiros x_0, y_0, x_1, y_1 tais que $ax_0 + my_0 = 1 = bx_1 + my_1$. Multiplicando obtemos

$$\begin{aligned} 1 &= (ax_0 + my_0)(bx_1 + my_1) \\ &= abx_0x_1 + m(ax_0y_1 + bx_1y_0 + my_0y_1), \end{aligned}$$

ou seja, o número 1, o menor dos positivos, é uma combinação linear de ab e m. Por teorema 1.3 obtemos que isto é $(ab, m) = 1$, como queriamos demonstrar. ■

Dois inteiros a, b dizem-se *relativamente primos* ou *coprimos* se tiverem máximo divisor comum 1. Por exemplo 7 e 15 são coprimos, bem como 24 e 91.

Problema 1.2. *Seja K um subconjunto de $k + 1$ números de $\{1, 2, \ldots, 2k\}$ Mostra que existem $a, b \in K$ que são coprimos.*

Os seguintes factos simples também são uteis:

Teorema 1.6. *i. Sejam a, b, c, x inteiros. Então*
$$(a, b) = (b, a) = (a, -b) = (a, b + ax)\,.$$
ii. Se $c|ab$ e $(b, c) = 1$ então $c|a$.

Demonstração. Deixada ao leitor. ■

O teorema 1.3 não nos dá nenhuma ferramenta eficaz para construir o máximo divisor comum; assegura apenas que, dados a, b, ele tem a forma $ax_0 + by_0$.

2. Algoritmo de Euclides

O **Algoritmo de Euclides** para construir o máximo divisor comum de dois inteiros $b, c > 0$ baseia-se no teorema 1.2. Consiste no seguinte: põe-se $r_{-1} = b$ e $r_0 = c$. Agora faz-se, enquanto se puder, o seguinte:

- Procuram-se números q_1 e $0 < r_1 < c$ tal que $r_{-1} = r_0 q_1 + r_1$.
- Procuram-se números q_2 e $0 < r_2 < r_1$ tal que $r_0 = r_1 q_2 + r_2$.
- Procuram-se números q_3 e $0 < r_3 < r_2$ tal que $r_1 = r_2 q_3 + r_3$.
- Procuram-se números q_4 e $0 < r_4 < r_3$ tal que $r_2 = r_3 q_4 + r_4$.

$\vdots \qquad \vdots \qquad \vdots$

- Procuram-se números q_j e $0 < r_j < r_{j-1}$ tal que $r_{j-2} = r_{j-1} q_j + r_j$.
- Procura-se um número q_{j+1} tal que $r_{j-1} = r_j q_{j+1}$.

Nota que os restos $r_1, r_2, \ldots$ produzidos são cada vez menores:$r_1 > r_2 > \ldots$. Portanto executando os passos chegamos a um, digamos, $j-$esimo passo, tal que no próximo passo, à procura dum resto tal que $r_{j-1} = r_j q_{j+1} + \text{resto}$ obtemos que necessariamente $\text{resto} = 0$. Então, diz o teorema de Euclides, o máximo divisor comum de r_{-1} e r_0 é r_j.

Exemplo . Queremos encontrar o máximo divisor comum de 963 e 657. Pomos primeiro $r_{-1} = 963$ e $r_0 = 657$.

Agora aplicamos o algoritmo: Com $q_1 = 1$ e $r_1 = 306$ obtemos a primeira linha do seguinte esquema cujas restantes linhas podes verificar tu:

$$\begin{aligned} 963 &= 657 \cdot 1 + 306 \\ 657 &= 306 \cdot 2 + 45 \\ 306 &= 45 \cdot 6 + 36 \\ 45 &= 36 \cdot 1 + 9 \\ 36 &= 9 \cdot 4 \end{aligned}$$

Pelo teorema de Euclides achamos portanto que 9 é máximo divisor comum de 963 e 657, ou seja $(963, 657) = 9$.

Esboço da prova do teorema de Euclides. A ideia da prova é facilmente explicada se nós nos limitarmos a um caso particular com j pequeno: Suponhamos que a última linha dos cálculus seria $r_3 = r_4 q_5$. (Isto é o caso $j = 4$ em cima.) Então temos 5 linhas no nosso esquéma. Vemos que $r_4 | r_3$. Então decorre da linha 4 que $r_4 \,|\, r_2$, depois da linha 3 que $r_4 \,|\, r_1$, depois da linha 2 que $r_4 \,|\, r_0$, e, finalmente, da linha 1 que $r_4 \,|\, r_{-1}$. Portanto r_4 é divisor comum de r_0 e r_{-1}. Seja, de modo recíproco, g um divisor de r_0 e r_{-1}. Nota que $(r_{-1} - r_0 q_1) = r_1$. Vemos da primeira linha que $g | r_1$, depois da segunda linha que $g | r_2$, da terceirea que $g | r_3$, da quarta que $g | r_4$.

Em suma: Qualquer divisor g de r_0 e r_{-1} divide r_4. Como r_4 é divisor dos números r_0 e r_{-1} dados, é o máximo divisor comum. ■

Podemos perguntar agora: Como escrever o máximo divisor comum de dois números b, c explicitamente na forma $r_j = bx_0 + cy_0$? Bom, na prática faz-se isto assim: r_j podemos exprimir à custa de r_{j-1}, r_{j-2} , os últimos dois depois à custa de r_{j-2} r_{j-3} etc. ... até chegarmos à uma expressão em r_{-1}, r_0.

Melhor que mil palavras serve o seguinte exemplo:

Devemos falar ainda por do 'irmão' do máximo divisor comum: do mínimo múltiplo comum. Dado um conjunto de inteiros não zeros existe obviamente um outro inteiro que é múltiplo de todos esses: por exemplo o produto $a_1 a_2 \dots a_n$. De entre todos os múltiplos, comuns aos inteiros $a_1, \dots, a_n$, existe então um (único) número mínimo positivo com esta propriedade. O assim chamado *mínimo múltiplo comum* desses números é denotado $[a_1, a_2, \dots, a_n]$.

Teorema 2.1. *Se b é múltiplo de $a_1, \dots, a_n$, então $[a_1, a_2, \dots, a_n] \,|\, b$.*

Demonstração. Seja $h = [a_1, a_2, \dots, a_n]$. Por teorema 1.2 existe um quociênte q e resto r tal que $b = qh + r$ com $0 \leq r < h$. Como $a_i \mid b$ e $a_i \mid h$, obtemos $a_i \mid r$. Ou seja: r é multiplo dos a_i. Com vista à definição de h, fica só a possibilidade $r = 0$, logo $h \,|\, b$. ■

Teorema 2.2. *Sejam a, b, m inteiros, $m > 0$. Então $[ma, mb] = m[a, b]$ e $[a, b] \cdot (a, b) = |ab|$.*

Demonstração. Prova. Primeira parte: Sendo $[ma, mb]$ múltiplo de ma portanto multiplo de m, existe um h_1 tal que $[ma, mb] = mh_1$. Seja $h_2 = [a, b]$. Temos $a \,|\, h_2$, $b \,|\, h_2$ e daí $ma \,|\, mh_2$, $mb \,|\, mh_2$. Logo mh_2 é múltiplo de ma, mb de modo que, por 1.12, $mh_1 \,|\, mh_2$ logo $h_1 \,|\, h_2$. Mas $ma \,|\, mh_1, mb \,|\, mh_1$ logo $a \,|\, h_1, b \,|\, h_1$ e daí $h_2 \,|\, h_1$ Concluimos $h_1 = h_2$.

Prova da segunda parte: Sem perda de generalidade sejam $a, b > 0$. Tratamos primeiro o caso especial $(a, b) = 1$. Ora, $[a, b] = ma$ para certo m. Então $b \,|\, ma$ implica por 1.10ii que $b \,|\, m$, logo $b \leq m, ba \leq ma = [a, b]$, logo $ab = [a, b]$.- Quanto ao caso geral, seja $g = (a, b) > 1$. Então $((a/g), (b/g)) = 1$ por teorema 1.7. Estamos nas condições já tratadas no parágrafo anterior, obtendo $[\frac{a}{g}, \frac{b}{g}](\frac{a}{g}, \frac{b}{g}) = \frac{a}{g}\frac{b}{g}$. Multiplicando por g^2, usando teorema 1.6i e a primeira parte do teorema, obtemos $[a, b](a, b) = ab$. ■

3. Números primos

Um inteiro $p > 1$ diz-se um (número) *primo* se não for divisível por nenhum d com $1 < d < p$. Um inteiro $a > 1$ não primo diz-se *composto*.

Os primeiros elementos da sucessão dos primos são 2, 3, 5, 7, 11, 13 , 17, . . . , enquanto os primeiros compostos são 4, 6, 8, 9, 10, 12, 14, 15 , 16, ...

Teorema 3.1. *Se p é primo e $p|a_1a_2\dots a_n$, então existe um i tal que $p|a_i$.*

Demonstração. A afirmação é óbvia para o caso $n = 1$.

Caso: $n = 2$. Se $p|a_1$ temos a conclusão desejada. Caso oposto consideremos que $(a_1, p) = 1$ e assim $p|a_2$ por teorema 1.10.

Agora aplicamos indução. A nossa hipótese é $n \geq 3$ e que se um número primo p divide um produto de menos que n (i.e. $\leq n-1$) números, então divide um dos inteiros. Seja agora $p|a_1a_2\dots a_{n-1}a_n$. Pondo $b = a_2\dots a_n$ temos $p|a_1b$. Ora a_1b é produto de dois números. Logo $p|a_1$ ou $p|b$. Se $p|a_1$ estamos prontos ($i = 1$ é um indice como desejado). Caso oposto p divide um produto de $n-1$ inteiros; a saber $a_2\dots a_n$. Por hipótese da indução p divide um destes a_i. ■

O próximo teorema diz-se teorema fundamental da aritmética; também chamado teorema da unicidade da decomposição de inteiros em números primos.

Teorema 3.2. *Qualquer inteiro $n > 1$ pode ser escrita de forma única como produto de números primos.*

Observação . A unicidade mencionada deve ser interpretada assim: Se tivermos uma relação

$$p_1^{\alpha_1}\dots p_r^{\alpha_r} = q_1^{\beta_1}\dots q_s^{\beta_s}$$

com números primos $p_1 < \ldots < p_r$ e $q_1 < \ldots < q_s$ e expoentes naturais $\alpha_i, \beta_j > 0$ então necessariamente $r = s$, $p_1 = q_1, \dots, p_r = q_r$ e $\alpha_1 = \beta_1, \dots, \alpha_r = \beta_r$.

Demonstração. a. Existência da decomposição. Vemos que 2 é primo e fornece assim já a sua propria decomposição. Fique já provado que todos os números menores que n são decomponíveis. Se n é primo então fornece a sua própria decomposição. Caso oposto n é divisível por um número estritamente entre 1 e n; ou seja: existem $1 < n_1, n_2 < n$ tais que $n = n_1n_2$. Mas por indução n_1 e n_2 são decomponíveis em produtos de potências de primos; o produto destas decomposições dá nos uma desejada decomposição para n.

b. Unicidade: Dados dois produtos diferentes de potências de primos que representam um número n, cancelamos todos os primos ocorrendo em ambos os produtos. Resultaria uma equação que por extenso (escrevendo ppp para p^3 etc.) pode ser escrito $p_1p_2\dots p_r = q_1q_2\dots q_s$ e onde nenhum primo à esquerda ocorre à direita e nenhum da direita ocorre à esquerda. Mas $p_1|q_1q_2\dots q_s$. Por teorema 1.15 p_1 divide um dos factores q_j. Sendo q_j primo, $p_1 = q_j$; contradição. ■

O teorema é tão fundamental porque contém muita da informação dos teoremas anteriores em forma compacta e conveniente. Além disso, põe em relevo o papel fundamental dos primos para a teoria multiplicativa dos números. Vislumbra que muitas perguntas sobre inteiros se reduzem a perguntas sobre os seus divisores.

A prova do seguinte teorema contém um exemplo clássico de Euclides duma 'argumentação por absurdo'.

Teorema 3.3. *O conjunto dos primos é infinito. Isto é: A sucessão* $2, 3, 5, 7, 11, 13, \ldots$ *dos primos não termina.*

Demonstração. Suponhamos que existe apenas um número finito de primos: p_1, ..., p_r. Formamos então o número $n = 1 + p_1 p_2 \ldots p_r$. Então n não é divisível nem por p_1, nem por p_2, ..., nem por p_r. Logo qualquer divisor primo p de n difere de $p_1, \ldots, p_r$. Tal divisor existe conforme o teorema fundamental. Logo existe um primo diferente de $p_1, \ldots, p_r$. ■

4. Congruências

Vimos atrás que o conceito da divisibilidade é fundamental na teoria dos números. Podemos dar maior transparência a este conceito introduzindo notação adequada. Esta facilitará também a descoberta de novos teoremas.

Definição 4.1. Sejam a, b, m inteiros. Se m divide a diferença $a - b$ (i.e. se $m|(a-b)$), então escreve-se $a \equiv b \pmod{m}$ e diz-se que a *é congruente* b *módulo* m.

Exemplo . $8 \equiv -3 \pmod{11}$ porque $8 - (-3) = 11$ e $11|11$. Do mesmo modo $33 \equiv 3 \pmod{15}$, ou $-27 \equiv 34 \pmod{61}$, ou $248 \equiv 162 \pmod{43}$. Dizer $a \equiv 0 \pmod{m}$ é o mesmo que dizer $m|a$.

As afirmações do teorema seguinte referem-se todas ao mesmo módulo m pelo que resolvemos escrever $a \equiv b$ em lugar de $a \equiv b \pmod{m}$ etc.

Teorema 4.1. *Sejam* a, b, c, d, x, y *inteiros. Tem-se o seguinte:*
a. $a \equiv b$ *se e somente se* $b \equiv a$ *se e somente se* $a - b \equiv 0$.
b. Se $a \equiv b$ *e* $b \equiv c$, *então* $a \equiv c$.
c. Se $a \equiv b$, $c \equiv d$, *então* $ac \equiv bd$,
d. $ax + cy \equiv bx + dy$.
e. Se $a \equiv b$ *e* $d|m$, *então* $a \equiv b \pmod{d}$.

Demonstração. Quanto a c., observamos que por hipótese
$m|a-b$ e $m|c-d$. Portanto $m|(a-b)c + b(c-d) = ac - bd$. A provas simples das restantes alíneas são deixadas ao leitor. ■

Observação . Note-se que as alíneas teorema 4.1 a. e b. exprimem respectivamente as propriedades de simetria e transitividade da relação $\equiv$.

Teorema 4.2. *Seja f um polinómio com coeficientes inteiros.*
Se $a \equiv b \pmod{m}$ então $f(a) \equiv f(b) \pmod{m}$.

Demonstração. Podemos escrever $f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_0$ c om inteiros c_i, $i = 0, 1, \ldots, n$. Como $a \equiv b$, deduzimos $a^2 \equiv b^2, a^3 \equiv b^3, \ldots, a^n \equiv b^n$ (tudo módulo m), e depois $c_i a^i \equiv c_i b^i$ por teorema 2.1ci; finalmente por 2.1dii, $c_n a^n + c_{n-1}a^{n-1} + \ldots + c_0 \equiv c_n b^n + c_{n-1}b^{n-1} + \ldots + c_0 \pmod{m}$. ■

Teorema 4.3. *a. $ax \equiv ay \pmod{m}$ se e somente se $x \equiv y \pmod{\frac{m}{(a,m)}}$.*
b. Se $ax \equiv ay$ e $(a, m) = 1$, então $x \equiv y$; cálculos $\pmod{m}$.
c. $x \equiv y \pmod{m_i}$ para $i = 1, 2, \ldots, r$ se e somente se $x \equiv y \pmod{[m_1, m_2 \ldots, m_r]}$.

Esboço da Demonstração. Deduz-se da divisibilidade de $ax - ay$ por m facilmente que $\frac{m}{(a,m)} | \frac{a}{(a,m)}(y - x)$. Ora as duas fracções que constam aqui, têm máximo divisor comum 1; donde se deduz a cogruência da direita de (a) por teorema 1.10. A implicação ($\Leftarrow$) deixamos ao leitor. (b) é um caso especial de (a). (c) é consequência imediata das definições e dos teoremas anteriores. ■

Notamos a seguinte consequência imediata do teorema 4.3 b.

Corolário 4.1. *Seja p primo e $p \not| a$. Então $ax \equiv ay \pmod{p}$ se e somente se $x \equiv y \pmod{p}$.*

Ao tratar inteiros módulo m lidamos essencialmente com os restos nas divisões por m.

Definição 4.2. Se $x \equiv y \pmod{m}$, então y diz-se *resto de x modulo m*. Um conjunto $\{x_1, \ldots, x_m\}$ diz-se *sistema completo de restos módulo m* se para todo o inteiro y existe um e um só inteiro x_j tal que $y \equiv x_j \pmod{m}$. Um *sistema reduzido de restos modulo m* é um conjunto de inteiros r_i tal que
i. $(r_i, m) = 1$ para todos os r_i.
ii. $r_i \not\equiv r_j \pmod{m}$ se $i \neq j$.
iii. Para qualquer x com $(x, m) = 1$ tem-se $x \equiv r_i \pmod{m}$ para certo r_i.

Teorema 4.4. *Se $x \equiv y \pmod{m}$ então $(x, m) = (y, m)$;.*

Observação . a. Equivalente é a afirmação: $(x, m) \neq (y, m) \Rightarrow x \not\equiv y \pmod{m}$.
b. A implicação recíproca é falsa.

Demonstração. Temos $(x, m)|m$ e $m|(x - y)$ logo pela transitividade de $\equiv$, que $(x, m)|(x - y)$. Como $(x, m)|x$, decorre $(x, m)|y$. Logo $(x, m)|(y, m)$. Assim $(x, m) \leq (y, m)$. De forma análoga, $(y, m) \leq (x, m)$ e daí a igualdade. ■

Exercício 4.1. Construa uma prova alternativa para este teorema.

Prova das observações. A observação (a) é óbvia porque uma implicação $A \Rightarrow B$ ('se A então B') equivale sempre à implicação $\neg A \Leftarrow \neg B$ também escrita $\neg B \Rightarrow \neg A$ e dita 'se não B então não A'. Para ver que a implicação recíproca é falsa considera $m = 15$, $x = 12$, $y = 6$. Então $(x, m) = 3 = (y, m)$, mas $m \not| (x - y)$. ■

Corolário 4.2. *Se se afastar dum sistema completo de restos módulo m todos os elementos não relativamente primos a m obtém-se um sistema reduzido módulo m. Todos os sistemas reduzidos módulo m têm a mesma cardinalidade.*

Demonstração. Se x_1 faz parte dum sistema completo de restos, mas $(x_1, m) \neq 1$ podemos tirá-lo sem prejuizo: se $(y, m) = 1$ então $(x_1, m) \neq (y, m)$, logo $y \not\equiv x_1 \pmod{m}$; isto é: tirados todos os elementos não relativamente primos a m encontraremos ainda para qualquer y com $(y, m) = 1$ um r resto sobrevivente tal que $y \equiv r \pmod{m}$. Além disso: dois sistemas completos de restos $\pmod{m}$ têm sempre a mesma cardinalidade, a saber m, e os seus elementos estão em correspondência biunívoca natural pela sua congruência modulo m. Isto implica os mesmos máximos divisores comuns com m. Logo os sistemas completos dão origem a dois sistemas reduzidos da mesma cardinalidade. ■

5. Função de Euler

Definição 5.1. A cardinalidade comum a todos os sistemas reduzidos de restos módulo m denota-se $\phi(m)$. A função $m \mapsto \phi(m)$ diz-se *função ϕ de Euler* ou *função tociente*.

Como $0, 1, 2, \ldots, m-1$ é um sistema completo de restos modulo m vemos a seguinte caracterização desta função:

Teorema 5.1. *O número $\phi(m)$ é o número dos inteiros positivos menores que m e primos relativo a m.*

Teorema 5.2. *Seja $(a, m) = 1$ e $r_1, \ldots, r_n$ um sistema reduzido de restos modulo m. Então $ar_1, \ldots, ar_n$ é outro tal sistema.*

Demonstração. Por teorema 1.5, $(ar_i, m) = 1$, para todos os r_i. Seja $i \neq j$. Se fosse $ar_i \equiv ar_j \pmod{m}$, então viria por teorema 4.3b que $r_i \equiv r_j \pmod{m}$, contradizendo a definição 4.2. Provámos assim que as alíneas i,ii da definição 4.2 estão satisfeitas. Para cada $i = 1, \ldots, n$ encontramos um $\sigma(i)$ tal que $ar_i \equiv r_{\sigma(i)} \pmod{m}$. σ é uma permutação (i.e. uma aplicação bijectiva) de $\{1, \ldots, n\}$ para $\{1, \ldots, n\}$: a r_*s distintos correspondem ar_*s distintos; logo σ é injectiva. É sobrejectiva porque a cardinalidade

dos dois sistemas são iguais. Para concluir a prova, consideremos um inteiro x com $(x, m) = 1$. Existe por hipótese um i tal que $x \equiv r_i$. Ora como $r_i \equiv ar_{\sigma^{-1}(i)}$, obtemos pela transitividade da relação $\equiv$ que o sistema $ar_1, \ldots, ar_n$ satisfaz tambem a definição 4.2 iii; logo é sistema reduzido de restos modulo m. ■

Uma linda aplicação da teoria desenvolviada é o teorema seguinte:

Teorema 5.3. *a.(Euler): $(a, m) = 1$ implica $a^{\phi(m)} \equiv 1 \pmod{m}$.*
b.(Fermat): Se p é primo com $p \nmid a$ então $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração. Usando notação e observações usadas no teorema 5.2, sabemos que existe uma permutação σ tal que para qualquer $i \in 1, 2, \ldots, \phi(m)$ se tem $ar_i \equiv r_\sigma(i) \pmod{m}$. Do teorema 4.1c obtemos

$$a^{\phi(m)} \prod_{j=1}^{m} r_i \equiv \prod_{i=1}^{m} ar_i \equiv \prod_{i=1}^{m} r_\sigma(i) \equiv \prod_{i=1}^{m} r_i \pmod{m}.$$

Aplicando teorema 4.3 (b) podemos, considerando $(r_j, m) = 1$ para os j em causa, cancelar os r_i, obtendo (a). O enunciado (b), chamado 'pequeno teorema de Fermat', é consequência imediata de (a), porque $p \nmid a$, p primo, implica $(a, p) = 1$. Além disso $0, 1, \ldots, p-1$ é sistema reduzido (e completo) de restos módulo p. Assim $\phi(p) = p - 1$. ■

Corolário 5.1. *Dados a, b, se $(a, m) = 1$ então existe x tal que $ax \equiv b \pmod{m}$.*

Demonstração. Obviamente $\phi(m) \geq 1$. Pondo $x = a^{\phi(m)-1}b$ calculamos por teorema 4.3 $ax \equiv a^{\phi(m)}b \equiv 1 \cdot b \equiv b \pmod{m}$. ■

Observação . Uma demonstração mais elementar é a seguinte: Perguntamo-nos se os restos modulo m de $0 = 0a, 1a, 2a, 3a, \ldots, (m-1)a$ são distintos dois a dois. A resposta é sim, pois caso oposto teríamos a divisibilidade de $ka - la = (k-l)a$ por m para certos $k, l \in \{0, 1, 2, \ldots, m-1\}$ diferentes. Mas então por teorema 1.6, $m|(k-l)$. Sendo $0 < |k-l| < m$, isto é impossível. Os restos dos ja, $j = 0, 1, \ldots, (m-1)$, formam portanto um conjunto de m números compreendidos entre 0 e $m-1$. Logo um dos números é igual a 1; ou seja $m|(aj-1)$ para um dos j. Para este j, $aj \equiv 1 \pmod{m}$.

Acabamos a nossa excursão para a teoria dos números com o seguinte, e famoso, teorema dos restos chinês.

Teorema 5.4 (Teorema dos restos chinês). *Sejam $m_1, \ldots, m_r$ r inteiros positivos, primos dois a dois. Sejam $a_1, \ldots, a_r$ quaisquer outros r inteiros. Então existe um x que satisfaz as r congruências $x \equiv a_i \pmod{m}$.*

Observação . Quaisquer duas soluções das congruências são congruentes módulo $m_1 m_2 \dots m_r$.

Demonstração. Esrevendo $m = m_1 m_2 \dots m_r$, vemos que m/m_j é um inteiro tal e $(m/m_j, m_j) = 1$. Por corolário 5.1 existem inteiros b_j tais que $(m/m_j)b_j \equiv 1 \pmod{m_j}$. Além disso, se $i \neq j$, então $m_i | \frac{m}{m_j}$, logo $(m/m_j)b_j \equiv 0 \pmod{m_i}$. Definamos x_0 por

$$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j.$$

com este x_0 vem relativamente a $i-$esima congruência,

$$x_0 \equiv \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \equiv \frac{m}{m_i} b_i a_i \equiv a_i \pmod{m_i}.$$

Como temos tal uma congruência para $i = 1, 2, \dots, r$, fica provada a primeira parte. A segunda parte é quase trivial. Sejam $y \neq x$ tais que $x \equiv y \equiv a_i \pmod{m_i}$ para $i = 1, 2, \dots, r$. Então $y - x \equiv 0 \pmod{m_i}$ por teorema 4.1 a. Logo cada $m_i | (y - x)$, logo $(y - x)$ é múltiplo comum de $m_1, m_2, \dots, m_r$. Mas sendo os m_i primos dois a dois, teorema 2.2 implica que o mínimo múltiplo comum (e divisor de qualquer outro múltiplo comum) é $m_1 m_2 \dots m_r$.- ■

6. Exercícios e problemas

1. Usando o algoritmo de Euclides, determina o máximo divisor comum dos seguintes pares de números:
a. 1109 e 4999, b. 2947 e 3997, c. 721 e 104, d. 1819 e 3587.
No último caso determina também x, y para escrever o máximo divisor comum g na forma $g = 1819x + 3587y$.

2. Determinar, caso existam, inteiros x, y, z tais que $93x - 81y = 3$ e $6x + 10y + 15z = 1$ e $4x - 22z = 3$, e dizer porque não existem nos outros casos.

3. a. Escrever uma tabela dos primeiros números da forma $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$. (Ler $n!$ como 'n factorial'.)
b. Mostrar que o produto de três (respective quatro) números consecutivos é um múltiplo de 6 (respective 24).

4. Provar as seguintes afirmações de divisibilidade:
a. Para todos os n, $2|(n^2 - n)$ e $30|(n^5 - n)$.
b. Para todos os n ímpares, $8|(n^2 - 1)$.
c. Para todos os n, $(n - 1)|(n^k - 1)$
d. Dado inteiro n, tem-se $(n - 1)^2|(n^k - 1)$ se e só se $(n - 1)|k$.

Como no texto, o máximo divisor comum de números $a_1, a_2, \ldots, a_n$ é a seguir abreviado por $(a_1, a_2, \ldots, a_n)$, o mínimo múltiplo comum por $[a_1, a_2, \ldots, a_n]$.

5. a. Mostrar que não há números x, y com $x + y = 100$ e $(x, y) = 3$.
b. As equações $(x, y) = g$ e $xy = b$ são resolúveis simultaneamente apenas quando $g^2|b$.
c. Seja $n \geq 2, k \in \mathbb{N}$. Então $(n-1)|(n^k - 1)$.
d. Seja $n \geq 2, k \in \mathbb{N}$. Então $(n-1)^2|(n^k - 1)$ se e somente se quando $n - 1|k$.

6. Sejam a, m, n números naturais com $m \neq n$. Mostrar:

$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \text{se } a \text{ é par} \\ 2 & \text{se } a \text{ é ímpar} \end{cases} .$$

7. Seja $m > n$. Então $a^{2^n} + 1 | a^{2^m} - 1$.

8. Prova que um inteiro de representação decimal $n_k n_{k-1} \ldots n_3 n_2 n_1$ é divisível
a. por 2 se e somente se $2 \mid n_1$,
b. por 4 se e somente se $4 \mid n_2 n_1$,
c. por 8 se e somente se $8 \mid n_3 n_2 n_1$.

9. Prova que um inteiro de representação decimal $n_k n_{k-1} \ldots n_3 n_2 n_1$ é divisível:
a. por 3 se e somente se $3|(n_k + n_{k-1} + \ldots + n_3 + n_2 + n_1)$,
b. por 9 se e somente se $9|(n_k + n_{k-1} + \ldots + n_3 + n_2 + n_1)$,
c. por 11 se e somente se $11|(n_k - n_{k-1} + n_{k-2} \ldots \pm n_1)$.

10. Se x, y são ímpares, mostra que $x^2 + y^2$ não é quadrado.

11. Se $3 \not| xy$ então $x^2 + y^2$ não é quadrado.

12. Prova que $(a, a + k) \,|\, k$.

13. Prova que qualquer primo da forma $3k + 1$ é da forma $6k + 1$

14. Provar que um inteiro positivo da forma $3k + 2$ tem um factor primo da mesma forma e que afirmações semelhantes são válidas para as formas $4k + 3$ e $6k + 5$.

15. Seja 2^k a maior potência de 2 que ocorre entre os números 1, 2, 3, , ..., n. Então nenhum destes números diferente de 2^k é divisível por 2^k.

16. Mostra que a soma $\sum_{j=1}^{n} \frac{1}{j}$ (i.e. $1 + \frac{1}{2} + \ldots + \frac{1}{n-1} + \frac{1}{n}$) não é inteiro se $n > 1$.

17. Se $2^n + 1$ é primo, então n é uma potência de 2.

18. a. Se $2^n - 1$ é primo, então n é primo.
b. Se $a, b, n > 1$ então $(a^n - b^n) \,|\, (a^n + b^n)$.

19. Existe uma infinidade de primos da forma $4n + 3$, $n \in \mathbb{N}$.

20. Se $f(x)$ é polinómio com coeficientes inteiros, então nem todos os números
$f(1), f(2), f(3), f(4), \ldots$
podem ser primos.

21. Determina todos os n tais que $2^n - 1$ é divisível por 7.

22. Pode existir um n tal que $2^n + 1$ é divisível por 7?

23. Seja S um conjunto de 10 números de dois digitos. Então existem subconjuntos disjuntos de S cujas somas são iguais.

24. Determina o conjunto de todos os números de três digitos cujo valor é 11 vezes a soma dos quadrados dos digitos.

25. Mostra que na sucessão dos números $1, 11, 111, 1111, \ldots$ existe pelo menos um número divisível por 1993.

26. Mostra que o produto de k números sucessivos é divisível por $k!$.

27. Quantos subconjuntos têm os seguintes conjuntos: $\emptyset$, $\{1\}$, $\{1, 2\}$, $\{1, 2, 3\}$, $\ldots$, qualquer conjunto de n elementos? Quantos subconjuntos de k elementos tem um conjunto de n elementos?

28. Em certas condições podem ser úteis conhecimentos de alguns valores das funções inteiras seguintes: $\binom{n}{k}$ para $(n > k)$, 2^n, $n!$. Escreve tabelas para estas funções.

29. Sejam A,B dois conjuntos finitos de números inteiros. Supõe que $\sum_{a\in A} a = \sum_{b\in B} b$. Então existem conjuntos $A' \subseteq A$ e $B' \subseteq B$ tais que $A' \cap B' = \emptyset$ e $\sum_{a\in A'} = \sum_{b\in B'}$.

30. Põe 57 coisas em 21 caixas. Então existe uma caixa que contém 2 coisas. Generaliza!

(Na matemática 'existe' tem o significado 'existe pelo menos um(a)'. Da mesma forma 'conter duas coisas' significa 'conter pelo menos duas coisas'. Se se pretende dar enfâse a um número exacto diz-se: 'Existem exactamente k ...')

31. Considera o conjunto seguinte de números: 3, 84, 35, 21, 44, 23, 71, 82.
a. Determina os restos da divisão destes números por 7.
b. Mostra que existem dois números em S cuja diferença é divisível por 7.
c. Demonstra em geral: 'Um conjunto qualquer de $n > m$ números contém dois números cuja diferença é divisível por m'.

32. Seja p um primo, q um inteiro tal que $p \not| q$. Considera a sucessão dos números $S = \{q, 2q, 3q, \ldots, (p-1)q\}$. Mostra que se $s, s' \in S$ e $s \neq s'$ então $s \not\equiv s' \pmod{m}$. Deduz que existe um k, $1 \leq k \leq p-1$ tal que $kq \equiv 1 \pmod{m}$

33. Seja p um primo. Considera os números $\{2, 3, 4, \ldots, p-2\}$. Mostra que para cada $s \in S$ existe um $t \in S$, $s' \neq s$ tal que $ss' \equiv 1 \pmod{m}$. Deduz o teorema de Wilson: $(p-1)! \equiv -1 \pmod{p}$