1 Teoria dos Números

O resultado da divisão de dois números inteiros, dividendo e divisor, nem sempre é um número inteiro. Ao maior número inteiro menor do que a divisão chama-se *quociente* e à diferença entre o dividendo e o produto do divisor pelo quociente chama-se *resto*.

Se a for o dividendo, b o divisor, q o quociente e r o resto tem-se que

$$a = q \times b + r, \;\; com 0 \leq r \leq b - 1 \, .$$

Por exemplo, se dividirmos 31 por 7 obtemos o resultado é 4.428... , e por isso o quociente desta divisão é 4. O resto é igual a $31 - 7 \times 4 = 3$.

1.1 Algoritmo de Euclides

O Algoritmo de Euclides serve para determinar o máximo divisor comum de dois números inteiros.

Exemplo. Determinar o máximo divisor comum de 17154 e 357, mdc(17154,357).

dividendo	divisor	resto	quociente
17154	357	18	48
357	18	15	19
18	15	**3**	1
15	**3**	0	5

O máximo divisor comum é o último resto diferente de zero, que é igualmente o último dividendo, ou seja mdc(17154,357)=3.

1.2 Números Primos

Definição. Um número inteiro $p > 1$ é primo se só é divisível por 1 e por ele próprio.

Os primeiros números primos são: 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091 1093 1097 1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213 1217 1223 1229 1231 1237 1249 1259 1277 1279 1283 1289 1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399 1409 1423 1427 1429 1433 1439 1447 1451 1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543 1549 1553 1559 1567 1571 1579 1583 1597 1601 1607 1609 1613 1619 1621 1627 1637 1657 1663 1667 1669 1693 1697 1699 1709 1721 1723 1733 1741 1747 1753 1759 1777 1783 1787 1789 1801 1811 1823 1831 1847 1861 1867 1871 1873 1877 1879 1889 1901 1907 1913 1931 1933 1949 1951 1973 1979 1987 1993 1997 1999.

Teorema. Todo o número natural (diferente de 1) escreve-se de forma única como um produto de números primos.

Este Teorema é conhecido por Teorema Fundamental da Aritmética.

Exemplos: $108 = 2^2 \times 3$; $225 = 3^2 \times 5^2$; $3260 = 2^2 \times 163$.

Definição Dois números naturais a e b são primos entre si se mdc(a, b)=1.

Quaisquer dois números primos são primos entre si, mas o recíproco não é verdadeiro.

1.3 Congruências

Definição. Seja m um número natural. Dois números a e b são *congruentes módulo* m se $a - b$ é divisível por m. Escreve-se $a \equiv b \pmod{m}$.

Proposição. $a \equiv b \pmod{m}$ se e só se a e b têm o mesmo resto na divisão por m.

Exemplos: $13 \equiv 1751 \pmod{2}$; $352 \equiv 1272 \pmod{10}$; $5 \equiv 19 \pmod{7}$.

Somas, produtos e potências módulo m.

- $a \underset{m}{\oplus} b = r$ se r é o resto da divisão de $a + b$ por m. (Lê-se a mais b módulo m.)
- $a \underset{m}{\otimes} b = s$ se s é o resto da divisão de $a \times b$ por m. (Lê-se a vezes b módulo m.)
- $a \overset{b}{\underset{m}{\otimes}} = t$ se t é o resto da divisão de a^b por m. (Lê-se a elevado a b módulo m.)

Exemplos:

$$3 \underset{8}{\oplus} 7 = 2; \qquad 59 \underset{100}{\oplus} 73 = 32;$$

$$59 \underset{60}{\otimes} 7 = 53; \qquad 7 \underset{13}{\otimes} 11 = 2;$$

$$2 \overset{9}{\underset{7}{\otimes}} = 1; \qquad 63 \overset{3}{\underset{17}{\otimes}} = 11.$$

1.4 Exercícios

1. Calcule o máximo divisor comum e diga quais dos pares são primos entre si.

   (a) $\text{mdc}(12, 72)$; (a) $\text{mdc}(5552, 3471)$;

   (b) $\text{mdc}(1112, 144)$; (b) $\text{mdc}(12739, 14544)$.

2. Decomponha em factores primos os seguintes números: 10, 55, 98, 308, 1175, 26569, 30030.

3. (a) Determine os primeiros 10 números naturais congruentes com 7 módulo 9.
   (b) Determine os dois primeiros números naturais congruentes com 137 módulo 11.
   (c) Calcule um número natural n tal que $n \equiv 3 \pmod{6}$ e $n \equiv 5 \pmod{8}$.

4. Calcule o resultado das seguintes operações:

   (a) $345 \underset{13}{\oplus} 1020$; (b) $17 \underset{1050}{\oplus} 164$; (c) $9994 \underset{11200}{\oplus} 10763$;

   (d) $590 \underset{1273}{\otimes} 753$; (e) $16 \underset{60}{\otimes} 53$; (f) $785 \underset{135}{\otimes} 575$;

   (g) $15 \overset{3}{\underset{2}{\otimes}}$; (h) $21 \overset{10}{\underset{11}{\otimes}}$; (i) $63 \overset{31}{\underset{7}{\otimes}}$;

   (j) $2 \overset{19}{\underset{27}{\otimes}}$; (k) $29 \overset{7}{\underset{357}{\otimes}}$; (l) $123 \overset{277}{\underset{1273}{\otimes}}$.

5. Calcule o valor das seguintes expressões módulo 11, 12 e 23, respectivamente.

   (a) $7 \times 5 + 3^7 - 6 \times 9$; $5^5 \times 2^7$. (mod 11)

   (b) $6 \times 9 + 3 + 10^2$; $7^2 + 10^{99}$. (mod 12)

   (c) $22 \times 22 \times 22$; $4^{45} + 6$. (mod 23)

1.5 Simétrico módulo m

Definição. Seja m um número natural. Dois números naturais $0 \leq a, b < m$ são simétricos módulo m se $a \underset{m}{\oplus} b \equiv 0$.

Exemplos.

2 e 3 são simétricos módulo 5 ($2 \underset{5}{\oplus} 3 \equiv 1$).

0 é simétrico de si próprio módulo m ($0 \underset{m}{\oplus} 0 \equiv 0$).

5 é simétrico de si próprio módulo 10 ($5 \underset{m}{\oplus} 5 \equiv 0$).

13 é o inverso módulo 37 de 24 ($13 \underset{37}{\oplus} 24 \equiv 0$).

- O simétrico módulo m de um número natural menor do que m existe e é único.
- Se $a \neq 0$, então o seu simétrico módulo m é igual a $m - a$.

1.6 Inverso módulo m

Definição. Seja m um número natural. Dois números naturais $0 < a, b < m$ dizem-se inversos módulo m se $a \underset{m}{\otimes} b \equiv 1$.

Exemplos.

2 e 3 são inversos módulo 5 ($2 \underset{5}{\otimes} 3 \equiv 1$).

1 é inverso de si próprio módulo m ($1 \underset{m}{\otimes} 1 \equiv 1$).

4 não tem inverso módulo 8. Para $a = 1, 2, ..., 7$; $\quad 4 \underset{8}{\otimes} a \neq 1$.

2 é o inverso módulo 101 de 51 ($2 \underset{101}{\otimes} 51 \equiv 1$).

10 é o inverso módulo 19 de 8 ($10 \underset{19}{\otimes} 8 \equiv 1$).

6 é inverso de si próprio módulo 7 ($6 \underset{7}{\otimes} 6 \equiv 1$).

- Se o inverso módulo m existe, então ele é único.
- O número a tem inverso módulo m se e só se mdc(a,m)=1.
- Se p é primo, então todos os números naturais menores do que p têm inverso módulo p.

1.7 Exercícios

1. Escreva os simétricos módulo 13 de todos os números naturais inferiores a 13.
2. (a) Determine, caso exista, o inverso módulo 11 de todos os números naturais inferiores a 11.
   (b) Determine, caso exista, o inverso módulo 14 de todos os números naturais inferiores a 14.
   (c) Calcule $x < 41$ tal que $x \cdot 5 \equiv 1 \pmod{41}$.
3. (a) Determine $a < 11$ de modo que $a + 2 \times 3 + 3 \times 7 + 4 \times 2 + 5 \times 0 + 6 \times 3 + 7 \times 2 + 8 \times 1 \equiv 0 \pmod{11}$.
   (b) Determine $b < 11$ de modo que $5 + 3 + 4 \times 3 + 6 \times b + 7 \times 3 + 8 \times 2 + 9 \times 7 + 10 \times 9 \equiv 0 \pmod{11}$.
   (c) Determine $c < 22$ de modo que $2 + 13 \times c + 15 \equiv 0 \pmod{22}$.

2 Códigos de identificação detectores de erros

Uma *Mensagem* é uma sequência de dígitos (algarismos ou não) que pretendemos transmitir. (Enviar por email, escrever num formulário, dizer ao telefone.)

Um *código detector de erros* é um conjunto de regras a que uma mensagem tem que obedecer para estar correcta.

Se a mensagem recebida não obedecer a essas regras, então houve um erro na comunicação. Nesse caso diz-se que o código *detectou o erro*.

Exemplos:

1. Códigos de barras (leitura óptica – pequena possibilidade de erro).
2. Número de cheque (escrito pelo bancário ou lido opticamente).
3. Código ISBN: usado para encomendas de livros,... (para uso humano – maior possibilidade de erro).
4. Número do Bilhete de Identidade (para uso humano – maior possibilidade de erro).
5. Número de série de notas.
   (a) Actualmente é usado para controlo de remessas e outras operações de transferência de notas. O código das notas de Euro é "demasiado" elementar.
   (b) Anteriormente os códigos foram usados para evitar falsificações e feitos de maneira a não serem decifrados. Com a evolução tecnológica, isso deixou de ser necessário. Por exemplo, o código das notas de Marco Alemão era bastante evoluído.
6. Número de cartão crédito (2 dígitos de controlo).
7. Comandos à distância: televisão, leitor de DVD, portão da garagem,... O comando emite uma mensagem (numérica) e o receptor transforma essa mensagem numa acção (mudar de canal, abrir a garagem,...). Neste caso a possibilidade de erro é bastante elevada.

Nos exemplos anteriores o código permite detectar erros mas não os corrige. Em certos casos, existe a necessidade de corrigir os erros. O exemplo mais usual de uma situação onde são usados códigos de identificação correctores de erros é o da transmissão de dados (imagem, som ou texto). Neste tipo de sistemas são usados amplificadores de sinal que permitem corrigir um certo número de erros. A possibilidade de corrigir erros é uma das vantagens dos sistemas digitais: internet, TV digital, gravação de CD's.

2.1 Código de barras

EAN - European Article Number.

O código EAN consiste num número de 13 dígitos. Os dois primeiros dígitos identificam o país onde o artigo foi produzido, os cinco seguintes o fabricante, os próximos cinco identificam o produto e o último dígito é um dígito de controlo.

$$\underbrace{x_1x_2}_{\text{país}}\underbrace{x_3x_4x_5x_6x_7}_{\text{fabricante}}\underbrace{x_8x_9x_{10}x_{11}x_{12}}_{\text{produto}}\underbrace{x_{13}}_{\substack{\text{dígito}\\ \text{controlo}}}$$

Exemplos.
Compal Pêra: 56-01151-54330-6
Compal Limão Light: 56-01151-11700-2
Lipton Yellow Label Black Tea: 80-00099-10001-0

Alguns exemplos de identificação do país produtor: França-30, Japão-49, Reino Unido-50, Portugal-56, Itália-80, Espanha-84, livros-97.

Um código de barras EAN verifica a seguinte regra:

$$x_1 + 3 \times x_2 + x_3 + 3 \times x_4 + x_5 + 3 \times x_6 + x_7 + 3 \times x_8 + x_9 + 3 \times x_{10} + x_{11} + 3 \times x_{12} + x_{13} \equiv 0 (mod 10)$$

Compal Pêra.
$5 + 3 \times 6 + 0 + 3 \times 1 + 1 + 3 \times 5 + 1 + 3 \times 5 + 4 + 3 \times 3 + 3 + 3 \times 0 + 6 = 80 \equiv 0 (mod 10)$
O número 80 é divisível por 10.

Lipton
$8 + 3 \times 0 + 0 + 3 \times 0 + 0 + 3 \times 9 + 9 + 3 \times 1 + 0 + 3 \times 0 + 0 + 3 \times 1 + 0 \equiv 0 (mod 10)$

2.2 Exercícios

1. Verifique se os seguintes números EAN estão correctos.
   (a) 97-80201-34292-5
   (b) 97-80301-34292-5
   (c) 55-00000-11111-6
   (d) 12-12345-54321-0
2. Determine os dígitos de controlo dos seguintes códigos de barras.
   (a) 56-01163-12081-
   (b) 49-00012-35070-
   (c) 20-11253-05932-

2.3 Número ISBN

ISBN - International Standard Nook Number

O código ISBN de um livro é um "número" de 10 dígitos. Os primeiros dígitos identificam a língua em que foi escrito ou o país onde foi publicado, conforme os casos, os números seguintes a editora e o livro e o último é um dígito de controlo, tal como nos caso dos códigos de barras.
O livro "Numbers and Beyond" de Stephen Barnett é identificado com o seguinte número

$$\underbrace{0}_{\text{inglês}} - \underbrace{201}_{\text{Prentice Hall}} - 34292 - \underbrace{8}_{\text{dígito controlo}}$$

Um número $x_{10}x_9x_8x_7x_6x_5x_4x_3x_2x_1$ é um número ISBN se verifica a seguinte regra:

$$x_1 + 2 \times x_2 + 3 \times x_3 + 4 \times x_4 + 5 \times x_5 + 6 \times x_6 + 7 \times x_7 + 8 \times x_8 + 9 \times x_9 + 10 \times x_{10} \equiv 0 (mod 11)$$

Nota: Os códigos que usam números primos, como neste caso o 11, permitem detectar um maior número de erros.
O dígito de controlo é adicionado ao ISBN de tal modo que o número resultante verifique o teste de controlo.

Como se calcula o dígito de controlo x_1?
1. Calcula-se o resto R da divisão inteira de
$2 \times x_2 + 3 \times x_3 + 4 \times x_4 + 5 \times x_5 + 6 \times x_6 + 7 \times x_7 + 8 \times x_8 + 9 \times x_9 + 10 \times x_{10}$ por 11, ou seja
$R = 2 \times x_2 + 3 \times x_3 + 4 \times x_4 + 5 \times x_5 + 6 \times x_6 + 7 \times x_7 + 8 \times x_8 + 9 \times x_9 + 10 \times x_{10} = 0 \, (mod 11)$.
2. Se $R = 0$, então $x_1 = 0$. Se $R \neq 0$, então $x_1 = 11 - R$.
E se $R = 1$? Neste caso $x_1 = 10$. Por conveniência usa-se o dígito X (dez romano) para substituir o número dez, que é usualmente representado por dois dígitos.

Exemplo. O livro "As Aranhas Douradas" de Rex Stout tem o ISBN

$$972 - 611 - 697 - X$$

O código do número ISBN detecta: erros singulares e trocas de dois algarismos.

Proposição. Se na leitura de um número ISBN ocorre apenas um erro num dígito ou apenas uma troca de algarismos, então o número resultante da leitura não verifica o teste de controlo.

2.4 Bilhete de Identidade

O número $10052174 - 6$ é um número de BI.

Podemos reparar que $6 + 2 \times 4 + 3 \times 7 + 4 \times 1 + 5 \times 2 + 6 \times 5 + 7 \times 0 + 8 \times 0 + 9 \times 1 = 0\,(mod 11)$.

Podemos verificar para outros números e chegar á mesma conclusão. A verdade é que o código do BI é idêntico ao código ISBN, com uma diferença.

Já alguém viu o dígito de controlo do BI igual a 10 ou a outro dígito que o identifique?

Não, porque o 10 foi substituído por 0!!!

Assim o número 9371405-0 é um número de BI existente em Portugal cujo a soma de controlo é $166 = 1(mod 11)$

O número 9373405-0 também é um número de BI e difere do número anterior em apenas um dígito.

Conclusão Devido à substituição do número 10 por 0, o código do BI não detecta erros singulares.

2.5 Exercícios

1. Determine os dígitos de controlo dos seguintes números ISBN incompletos.

   (a) 0-205-04570-

   (b) 0-8162-8604-

   (c) 2-512-43005-

   (d) 972-21-1608-

2. uma biblioteca encomendou vários livros enviando os respectivos números ISBN. O fornecedor recebeu a encomenda, mas dois dos números estavam incompletos: 972-3?-0310-5 e 0-19-850?30-0. Quais são os números completos?

3. Determine duas alternativas correctas para os seguintes números incorrectos:

   (a) 0-13-132334-3

   (b) 3-550-05329-8

   (c) 0-386-05329-8

   (d) 0-110-23142-X

4. Complete os seguintes números de Bilhete de Identidade.

   (a) 12345678-?

   (b) 1023?219-9

   (c) 1531?000-0

   (d) 19235132-?

   (e) 1254432?-1

2.6 O caso geral

Os sistemas de detecção de erros que estudámos, EAN e ISBN, são dois códigos que pertencem a uma classe maior: os *códigos modulares*.

Definição Um código modular de comprimento n e módulo k é constituído por n números naturais, $(p_1, p_2, ..., p_n)$, inferiores a k.

Um número $x_1x_2x_3...x_{n-1}x_n$ pertence a este código se verifica a seguinte regra:

$$p_1 \times x_1 + p_2 \times x_2 + ... + p_{n-1} \times x_{n-1} + p_n \times x_n \equiv 0 (mod\ k)$$

Nota: Os dígitos x_1, ..., x_n podem não ser algarismos. Apenas é necessário que identifiquem um valor numérico. No código ISBN X representa o número 10.

Exemplos. O código ISBN é um código modular de comprimento 10 e módulo 11. O código de barras tem comprimento 10 e é um código módulo 10.

Proposição. Um código modular $(p_1, p_2, ..., p_n)$ de módulo k detecta:

(a) erros singulares na posição i se e só se mdc(p_i, k)=1;

(b) a troca dos dígitos nas posições i e j se e só se mdc$(p_i - p_j, k)$=1.

Deste resultado, conclui-se facilmente que se k é um número primo, então um código módulo k detecta todos os erros singulares. Esse é o caso do código ISBN, uma vez que 11 é primo.

2.7 Exercícios

1. Para se transmitir palavras através de um canal foi construído um código detector de erros, para se ter a certeza que a palavra recebida foi a enviada. Nesse código cada letra corresponde a um número A-0, B-1, ..., Z-22. A cada palavra junta-se um dígito de controlo.

   Uma palavra $x_n...x_2x_1$ (x_1 é o dígito de controlo) pertence ao código se

   $$x_1 + 2 \times x_2 + 3 \times x_3 + ... + n \times x_n \equiv 0 \pmod{23} .$$

   (a) Determine o dígito de controlo da palavra PORTUGAL.

   (b) Foram recebidas as palavras ANOJ e PAULOC. Será que estão correctas.

2. Numa biblioteca foi implementado um sistema de leitura óptica dos cartões de leitor dos utentes. Para evitar erros, ao número de leitor foi acrescentado um dígito de control. Assim, o número $x_1x_2x_3x_4 - x_5$ é um número de leitor se

   $$x_1 + x_2 + x_3 + x_4 + x_5 \equiv 0 \pmod{10} .$$

   Por exemplo 1542-8 é um número deste código, uma vez que $1 + 5 + 4 + 2 + 8 = 20 \equiv 0 \pmod{10}$.

   (a) Verifique se os números 2345-0 e 1841-6 pertencem a este código.

   (b) Determine o algarismo de controlo do número 1370−?.

3. Verifique que o código de barras não detecta todas as trocas de dois algarismos consecutivos. Dê um exemplo.

4. Verifique que o código ISBN detecta todas as trocas de dois algarismos.

5. Os números do cartão de cliente de uma *gasolineira* têm um código detector de erros. Ao número do cartão foram acrescentado dois dígitos de control, f e g Assim, o número $abcde - fg$ é um número de clientes se

   $$a + b + c + d + e + f + g \equiv 0 \pmod{9} \text{ e}$$
   $$a - b + c - d + e - f + g \equiv 0 \pmod{9} .$$

   (a) Verifique se os números 35746-25 e 82356-51 pertencem a este código.

   (b) Determine os algarismos de controlo do número $27025 - xy$.