1 Divisão Inteira

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 $31 - 7 \times 4 = 3$.

2 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.

3 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.

4 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:

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

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

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

5 Exercícios

1. Calcule o máximo divisor comum e diga quais dos pares são primos entre si.
   (a) $\text{mdc}(12, 72)$;
   (b) $\text{mdc}(1112, 144)$;
   (a) $\text{mdc}(5552, 3471)$;
   (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) $345 \underset{13}{\oplus} 1020$; $\qquad$ (b) $17 \underset{1050}{\oplus} 164$; $\qquad$ (c) $9994 \underset{11200}{\oplus} 10763$;

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

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

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

5. Calcule o valor das seguintes expressões módulo 11, 12 e 23, respectivamente.
   (a) $7 \times 5 + 3^7 - 6 \times 9$; $\quad 5^5 \times 2^7$. $\quad \pmod{11}$
   (b) $6 \times 9 + 3 + 10^2$; $\quad 7^2 + 10^{99}$. $\quad \pmod{12}$
   (c) $22 \times 22 \times 22$; $\quad 4^{45} + 6$. $\quad \pmod{23}$