

# Matemática Discreta

Licenciatura em Segurança Informática  
em Redes de Computadores

Licenciatura em Engenharia Informática  
**Teoria dos Números**

Eliana Costa e Silva – eos@estg.ipp.pt

Aldina Correia – aic@estg.ipp.pt



Felgueiras, maio de 2020

# Divisibilidade e Aritmética Modular

## Definição 46

Sejam  $a$  e  $b$  dois inteiros com  $a \neq 0$ .

Dizemos que  $a$  **divide**  $b$  se existe um inteiro  $c$  tal que  $b = ac$ , ou equivalentemente, se  $b/a$  é inteiro.

Quando  $a$  divide  $b$  dizemos que  $a$  é um **divisor** de  $b$  e que  $b$  é um **múltiplo** de  $a$ .

Se  $a$  divide  $b$  escrevemos  $a|b$ .

Se  $a$  **não** divide  $b$  escrevemos  $a \nmid b$ .

## Exemplo 112

Verifique se  $3|12$  e  $5|12$ .

Resolução:

3 divide 12 ( $3|12$ ) uma vez que  $3 \times 4 = 12$  ou  $12/3 = 4$ .

5 não divide 12 ( $5 \nmid 12$ ) uma vez que  $12/5 = 2,4 \notin \mathbb{Z}$ .

*ao dividir e multiplicar tem que dar o mesmo número.*

## Teorema 19

Sejam  $a, b$  e  $c$  inteiros tais que  $a \neq 0$ . Então:

- (i) se  $a|b$  e  $a|c$  então  $a|(b+c)$ ;
- (ii) se  $a|b$  então  $a|bc$ ;
- (iii) se  $a|b$  e  $b|c$  então  $a|c$ .

## Corolário

Sejam  $a, b$  e  $c$  inteiros tais que  $a|b$  e  $a|c$  então  $a|mb + nc$  para  $m, n \in \mathbb{Z}$ .

## Teorema 20 – Algoritmo de divisão

Sejam  $a \in \mathbb{Z}$  e  $d \in \mathbb{Z}^+$ .

Então existem inteiros únicos  $q$  e  $r$ , com  $0 \leq r < d$ , tais que  $a = dq + r$ .

## Exemplo 114

Consideremos os inteiros 7 e 3. Temos que  $7 = 3 \times 2 + 1$ .

Portanto,  $a = 7$  é o **dividendo**,  $d = 3$  é o **divisor**,  $q = 2$  é o **quociente** e  $r = 1$  é o **resto**.

## Definição

Na igualdade  $a = dq + r$  dizemos que  $a$  é o **dividendo**,  $d$  é o **divisor**,  $q$  é o **quociente** e  $r$  é o **resto**.

Escreve-se

$$q = a \operatorname{div} d \quad \text{e} \quad r = a \bmod d$$

## Exemplo 116

Identifique o quociente e o resto da divisão de  $-13$  por  $5$ .

Resolução: *dividendo* *divisor* *quociente* *resto*

Temos que  $-13 = 5 \times (-3) + 2$ .

Portanto, o quociente é  $q = -3 = -13 \operatorname{div} 5$  e o resto é  $r = 2 = -13 \bmod 5$ .

**Atenção que o resto nunca pode ser negativo!**

**Observação** As linguagens de programação têm um ou mais operadores para aritmética modular. Alguns exemplos são, **mod** em BASIC, Maple, Mathematica, EXCEL and SQL; **%** em C, C++, Java e Python; **rem** em Matlab, Apa e Lisp.

**Atenção** que:

- alguns destes operadores, para  $a < 0$ , devolvem  $a - m\lceil a/m \rceil$  em vez de  $a \bmod m = a - m\lfloor a/m \rfloor$ ;
- ao contrário de  $a \bmod m$ , alguns destes operadores estão definidos para  $m \leq 0$ .



Explore as funções *modulo*, *pmodulo* e *fix*.

- $modulo(n, m)$  calcula  $i = n(modulo\ m)$  i.e. o resto da divisão de  $n$  por  $m$ .
- A função  $modulo(n, m)$  pode dar um resto negativo, nesse caso deve usar  $i = pm modulo(n, m)$ , com esta função o resultado dá sempre positivo ou nulo.
- $fix(M)$  retorna uma matriz inteira com a dimensão de  $M$  e com elementos inteiros obtidos por aproximar os elementos  $x_i$  de  $M$  por inteiros em direção a zero, ou seja,  $y = sign(x_i) * floor(abs(x_i))$ .

## Definição

Sejam  $a$  e  $b$  dois números inteiros e  $m$  um número inteiro positivo. Então  $a$  e  $b$  são **congruentes módulo  $m$**  se  $m$  divide  $a - b$ , ou  $a - b$  é múltiplo de  $m$ .

E escrevemos  $a \equiv b(\text{mod } m)$  para indicar que  $a$  e  $b$  são **congruentes módulo  $m$** . Se  $a$  e  $b$  não são congruentes módulo  $m$ , escrevemos  $a \not\equiv b(\text{mod } m)$ .

**Atenção que as notações  $a \equiv b(\text{mod } m)$  e  $a \text{ mod } m = b$  incluem “mod” mas representam conceitos distintos!**

$a \equiv b(\text{mod } m)$  representa uma relação no conjunto dos números inteiros, enquanto que,  $a \text{ mod } m = b$  representa uma operação.

## Teorema 21

Sejam  $a$  e  $b$  dois números inteiros e  $m$  um inteiro positivo. Então  $a \equiv b(\text{mod } m)$  **se e só se**  $a \text{ mod } m = b \text{ mod } m$ .

**Observação:** Quando escrevemos  $a \equiv b(\text{mod } m)$  estamos a dizer que  $a$  e  $b$  têm o mesmo resto quando divididos por  $m$ .

## Exemplo 117

Determine se 17 e 5 são congruentes módulo 6 e se 24 e 14 são congruentes módulo 6.

Resolução:  $17 - 5 = 12$   $17 \equiv 5 \pmod{6}$

Como 6 divide  $17 - 5 = 12$ , temos que  $17 \equiv 5 \pmod{6}$ .

No entanto, como  $24 - 14 = 10$  não é divisível por 6, temos que  $24 \not\equiv 14 \pmod{6}$ .

## Teorema 22

Seja  $m$  um número inteiro positivo.

Os números inteiros  $a$  e  $b$  são congruentes módulo  $m$  **se e só se** existe um inteiro  $k$  tal que  $a = b + km$ .

## Teorema 23

Seja  $m$  um inteiro positivo.

Se  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$ , então  $(a + c) \equiv (b + d) \pmod{m}$  e  $(ac) \equiv (bd) \pmod{m}$ .

## Exercício 4 - Aplique o teorema anterior:

Como  $7 \equiv 2 \pmod{5}$  e  $11 \equiv 1 \pmod{5}$ , então ...

**Atenção que  $ac \equiv bc \pmod{m}$  não implica que  $a \equiv b \pmod{m}$   
(Encontre um exemplo!).**

## Corolário 3

Sejam  $m$  um número inteiro positivo e  $a$  e  $b$  inteiros.

Então,

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

e

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$



## Aritmética módulo $m$

Seja  $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$  (conjunto dos inteiros não negativos menores que  $m$ ).

Dados  $a, b \in \mathbb{Z}_m$ , definimos:

$$a +_m b = (a + b) \bmod m \quad \text{e} \quad a \times_m b = (a \times b) \bmod m.$$

As operações  $+_m$  e  $\times_m$  são chamadas **adição e multiplicação módulo  $m$**  e quando as usamos dizemos que estamos a efetuar aritmética módulo  $m$ .

### Exercício 5

Calcule em  $\mathbb{Z}_m$ : **(a)**  $7 +_{11} 9$  e **(b)**  $7 \times_{11} 9$ .

## Propriedades de aritmética módulo $m$

**Fecho:** Se  $a, b \in \mathbb{Z}_m$ , então  $a +_m b, a \times_m b \in \mathbb{Z}_m$ .

**Associatividade:** Se  $a, b, c \in \mathbb{Z}_m$ , então  $(a +_m b) +_m c = a +_m (b +_m c)$  e  $(a \times_m b) \times_m c = a \times_m (b \times_m c)$ .

**Comutatividade:** Se  $a, b \in \mathbb{Z}_m$ , então  $a +_m b = b +_m a$  e  $a \times_m b = b \times_m a$ .

**Existência de elemento identidade:** Os elementos 0 e 1 são elementos identidade da adição e multiplicação módulo  $m$ , respetivamente. Ou seja, se  $a \in \mathbb{Z}_m$  então  $a +_m 0 = 0 +_m a = a$  e  $a \times_m 1 = 1 \times_m a = a$ .

**Inverso aditivo:** Se  $a \in \mathbb{Z}_m$  e  $a \neq 0$ , então  $m - a$  é o inverso aditivo de  $a$  módulo  $m$  e 0 é o seu próprio inverso aditivo, i.e.,  $a +_m (m - a) = (m - a) +_m a = 0$  e  $0 +_m 0 = 0$ .

**Distributividade:** Se  $a, b, c \in \mathbb{Z}_m$ , então  $a \times_m (b +_m c) = (a \times_m b) +_m (a \times_m c)$  e  $(a +_m b) \times_m c = (a \times_m c) +_m (b \times_m c)$ .

Não existe, no entanto, propriedade para o inverso multiplicativo para qualquer elemento de  $\mathbb{Z}_m$ . Por exemplo, 2 não tem inverso multiplicativo módulo 6.

**Mas para alguns inteiros é possível encontrar o seu inverso multiplicativo. Isto é para um determinado número  $a$  módulo  $m$  pode existir um  $b$  módulo  $m$  tal que  $a \times_m b = 1$ .**

Por exemplo, temos que  $7 \times 3 = 21 = 2 \times 10 + 1$ , então  $7 \times_{10} 3 = 1$ , ou seja 7 é o inverso de 3, módulo 10.

## Aplicações – Códigos – Codificar e decodificar informação

- Por exemplo podemos multiplicar por 7 módulo 10 para codificar a informação e multiplicar por 3 módulo 10 para decodificar. Se efetuarmos as duas operações de forma consecutiva ficamos com a informação inicial, i.e.,  $a \times_{10} 7 \times_{10} 3 = a$ .
- Consideremos o caso do código de um cartão multibanco constituído por 4 algarismos. Não é prudente escrever este código num papel, no entanto, podemos multiplicar cada algarismo por 7 módulo 10 e guardar o número assim obtido, depois basta multiplicar por 3 módulo 10 para obter o código multibanco original. Vejamos um exemplo para o código 9783.
- Para codificar fazemos:

$$9 \times_{10} 7 = (9 \times 7) \bmod 10 = 63 \bmod 10 = (6 \times 10 + 3) \bmod 10 = 3$$

$$7 \times_{10} 7 = (7 \times 7) \bmod 10 = 49 \bmod 10 = (4 \times 10 + 9) \bmod 10 = 9$$

$$8 \times_{10} 7 = (8 \times 7) \bmod 10 = 56 \bmod 10 = (5 \times 10 + 6) \bmod 10 = 6$$

$$3 \times_{10} 7 = (3 \times 7) \bmod 10 = 21 \bmod 10 = (2 \times 10 + 1) \bmod 10 = 1$$

obtemos 3961 que podemos escrever num papel sem correr o risco de usarem o nosso cartão sem nossa autorização.

- Para recuperar o código correto basta multiplicar cada algarismos de 3961 por 3 módulo 10 e obtemos o código original (Exercício!).
- **Algoritmo de Euclides**, que será visto mais adiante é também uma aplicação da aritmética modular.

# Números primos e máximo divisor comum

## Definição 49

Um número inteiro  $p$  maior que 1 é designado por **número primo** se os seus únicos divisores são  $p$  e 1.

Um número inteiro maior do que 1 que não seja primo é chamado um **número composto**.

## Exemplo 118

O número 11 é primo pois apenas é divisível por 1 e por si mesmo. Por outro lado, 15 é um número composto pois é divisível por 1, 3, 5 e 15.

Os números primos menores que 100 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

Para ver a lista dos 10000 primeiros números primos visite a página <http://metricconversion.biz/list-of-first-100-prime-numbers.html>.



Explore as funções *primes* e *factor*.

Dado um número real  $x$ :

- $primes(x)$  devolve um vetor com todos os números primos entre 1 e  $x$ . Se  $x < 2$  então o vetor devolvido é vazio.
- $factor(x)$  devolve um vetor com os fatores da decomposição de  $x$  em fatores primos. Note-se que  $factor(0) = 0$  e  $factor(1) = 1$ .

## Teorema Fundamental da Aritmética

Todo o número inteiro maior que 1 pode ser escrito de modo único o produto de fatores primos, onde cada fator é escrito por ordem não decrescente.

### Exemplo 119

O número 100 pode ser decomposto no seguinte produto de fatores primos:

$$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2.$$

Enquanto que 999 tem a seguinte decomposição em fatores primos:

$$999 = 3 \times 3 \times 3 \times 37 = 3^3 \times 37.$$

- Em Criptologia/Criptografia, por exemplo, números primos grandes são usados para codificar mensagens<sup>1</sup>.
- É portanto importante verificar se um determinado número é primo.
- Existem várias formas de o fazer.
- De seguida é apresentado um resultado que ajuda nesta identificação.
- A prova desse resultado pode ser consultada, por exemplo, em Rosen 2012.

---

<sup>1</sup>Veja o vídeo disponível em <https://www.youtube.com/watch?v=56fa8Jz-FQQ>.

## Teorema 25

Se  $n$  é um número inteiro composto então,  $n$  tem um divisor primo menor ou igual a  $\sqrt{n}$ .

## Exemplo 120

Verifiquemos que 101 é um número primo. Para tal comecemos por verificar que  $\sqrt{101} \approx 10,05$ . Os número primos menores que 10 são: 2, 3, 5 e 7. Como 101 não é divisível por nenhum destes números podemos garantir que 101 é um número primo.

## Teorema 26

Existe um número infinito de números primos.



## Crivo de Eratóstenes – determinação dos números primos menores que 100

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- Pelo Teorema 25 – um número composto menor ou igual a 100 tem de ter um fator primo que não excede 10 (uma vez que  $\sqrt{100} = 10$ ).
- Como os únicos números primos que não excedem 10 são 2, 3, 5, e 7, os números primos menores ou iguais a 100 são estes e os números maiores que 1 e menores que 100 que não são divisíveis por 2, 3, 5, ou 7.

## Crivo de Eratóstenes – determinação dos números primos menores que 100

1	<u>2</u>	<u>3</u>	<u>4</u>	<u>5</u>	<u>6</u>	<u>7</u>	<u>8</u>	<u>9</u>	<u>10</u>
<u>11</u>	<u>12</u>	<u>13</u>	<u>14</u>	<u>15</u>	<u>16</u>	<u>17</u>	<u>18</u>	<u>19</u>	<u>20</u>
<u>21</u>	<u>22</u>	<u>23</u>	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	<u>29</u>	<u>30</u>
<u>31</u>	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	<u>37</u>	<u>38</u>	<u>39</u>	<u>40</u>
<u>41</u>	<u>42</u>	<u>43</u>	<u>44</u>	<u>45</u>	<u>46</u>	<u>47</u>	<u>48</u>	<u>49</u>	<u>50</u>
<u>51</u>	<u>52</u>	<u>53</u>	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	<u>59</u>	<u>60</u>
<u>61</u>	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	<u>67</u>	<u>68</u>	<u>69</u>	<u>70</u>
<u>71</u>	<u>72</u>	<u>73</u>	<u>74</u>	<u>75</u>	<u>76</u>	<u>77</u>	<u>78</u>	<u>79</u>	<u>80</u>
<u>81</u>	<u>82</u>	<u>83</u>	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	<u>89</u>	<u>90</u>
<u>91</u>	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	<u>97</u>	<u>98</u>	<u>99</u>	<u>100</u>

- Assim, começamos por dispor todos os números inteiros positivos menores ou iguais a 100 numa grelha
- Primeiro sublinham-se todos os números, maiores que 2, divisíveis por 2.
- De seguida sublinham-se os números, maiores que 3, divisíveis por 3.
- Repete-se este procedimento para o fator 5 e 7.
- Os números assinalamos a azul são números primos.

## Números primos de Mersenne

Um **número de Mersenne**<sup>2</sup> é um número da forma  $2^p - 1$ .

Para que  $2^p - 1$  seja um número primo  $p$  também tem de ser um número primo, mas não basta!

Note que se  $p$  não é primo então  $2^p - 1$  também não é primo.

### Exemplo 121

$2^2 - 1 = 4 - 1 = 3$  é um número primo.

$2^3 - 1 = 8 - 1 = 7$  é um número primo.

$2^4 - 1 = 16 - 1 = 15$  **não** é um número primo porque  $3 \times 5 = 15$  - de facto 4 não é primo!

$2^5 - 1 = 31 - 1 = 31$  é um número primo.

$2^7 - 1 = 128 - 1 = 127$  é um número primo.

$2^{11} - 1 = 2048 - 1 = 2047$  **não** é um número primo (embora 11 seja!) porque  $2047 = 23 \times 89$ .

Os primeiros números primos de Mersenne são: 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, correspondentes a  $p = 2, 3, 5, 7, 13, 17, 19, 31$ .

---

<sup>2</sup>Este nome foi dado em homenagem ao monge Francês Marin Mersenne que estudou estes números no século dezassete.

- Desde 1996 que o projeto de computação distribuída “*Great Internet Mersenne Prime Search*” tem encontrado números primos cada vez maiores.
- Visite a página deste projeto em <http://www.mersenne.org/>.
- A razão para os maiores números primos descobertos nos últimos anos serem de Mersenne deve-se ao facto de existir um teste - **Teste de Lucas-Lehmer**<sup>3</sup>- extremamente eficiente para verificar se o número é primo.

---

<sup>3</sup>Ver mais informações em [http://www.mersennewiki.org/index.php/Lucas-Lehmer\\_Test](http://www.mersennewiki.org/index.php/Lucas-Lehmer_Test).

## Teorema 27 – O Teorema dos números primos

A razão entre o número de números primos menores ou iguais a  $x$  e  $\frac{x}{\ln x}$  aproxima-se de 1 à medida que  $x$  aumenta.

- O Teorema diz-nos que o número de números primos menores ou iguais a  $x$  pode ser aproximado por  $\frac{x}{\ln x}$ .
- Então a chance de um número próximo de  $x$  ser primo é de aproximadamente

$$\frac{\frac{x}{\ln x}}{x} = \frac{1}{\ln x}$$

- Por exemplo, a chance de um número próximo de  $10^{1000}$  ser primo é de aproximadamente  $\frac{1}{\ln 10^{1000}} = \frac{1}{1000 \ln 10} \approx \frac{1}{23000} \approx 0,0000435$ .

## Conjeturas e problemas por resolver relacionados com números primos

Algumas das conjeturas existentes atualmente são:

- **Conjetura de Goldbach:** foi proposta em 1742 e diz que todo o número primo  $n > 2$  é a soma de dois números primos. A maioria dos matemáticos acredita que esta conjetura é verdadeira, no entanto, não existe ainda uma prova deste resultado!  
Veja mais informações, por exemplo em, <https://plus.maths.org/content/mathematical-mysteries-goldbach-conjecture>.
- **Conjetura dos números primos gémeos:** Dois números primos dizem-se gémeos se diferem em 2 unidades. Por exemplo, 3 e 5 são números primos gémeos porque  $5 - 3 = 2$ ; 4967 e 4969 também são números primos gémeos. A conjetura diz-nos que existe um número infinito de números primos gémeos. Veja mais informações em <http://www.businessinsider.com/yitang-zhang-genius-fellow-twin-prime-conjecture-2014-9>.

**Exercícios:** 91 a 108.

# Mínimo múltiplo comum e máximo divisor comum

## Definição 50

Sejam  $a$  e  $b$  dois números inteiros não nulos.

O maior número inteiro  $d$  tal que  $d|a$  e  $d|b$  é designado de **máximo divisor comum** (*greatest common divisor – gcd*) de  $a$  e  $b$ , e escreve-se  $d = \text{mdc}(a, b)$ .

## Definição 51

Os número inteiros  $a$  e  $b$  dizem-se **primos entre si** se  $\text{mdc}(a, b) = 1$ .

## Definição 52

O **mínimo múltiplo comum** (*least common multiple – lcm*) entre dois números inteiros positivos é o menor inteiro positivo que é divisível simultaneamente por  $a$  e  $b$ , e escreve-se  $\text{mmc}(a, b)$ .

Considere a decomposição em fatores primos dos números  $a$  e  $b$ :

$$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} p_n^{a_n} \quad \text{e} \quad b = p_1^{b_1} p_2^{b_2} p_3^{b_3} p_n^{b_n}$$

onde  $a_i, b_i \geq 0$ , temos que:

O **máximo divisor comum** entre  $a$  e  $b$  é dado por:

$$\text{mdc}(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

O **mínimo múltiplo comum** entre  $a$  e  $b$  é dado por:

$$\text{mmc}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$$



## Exercício

Calcule  $\text{mdc}(24, 36)$ .

Como

$$24 = 2 \times 2 \times 2 \times 3 = 2^3 \times 3$$

e

$$36 = 2 \times 2 \times 3 \times 3 = 2^2 \times 3^2,$$

então

$$\text{mdc}(24, 36) = 2^2 \times 3 = 12.$$

## Exercício


Dê exemplo de dois números primos entre si maiores que 20.

Como  $21 = 3 \times 7$  e  $22 = 2 \times 11$  não têm fatores primos comuns, tem-se que  $\text{mdc}(21, 22) = 1$ , ou seja 21 e 22 são números primos entre si.

## Exercício

Encontre o mdc e o mmc entre 120 e 500.

### Sugestão:

Explore as funções *gcd* e *lcm* do  SciLab

```
//least common (positive) multiple  
--> lcm([120,500])  
ans =
```

3000.

```
//Greatest (positive) Common Divisor  
--> gcd([120,500])  
ans =
```

20.

## Teorema 28

Sejam  $a$  e  $b$  dois números inteiros positivos.

Então,

$$a \times b = \text{mmc}(a, b) \times \text{mdc}(a, b).$$

O algoritmo de Euclides assenta no seguinte resultado.

## Lema

Seja  $a = b \times q + r$ , onde  $a, b, q$  e  $r$  são números inteiros. Então,

$$\text{mdc}(a, b) = \text{mdc}(b, r).$$

# Algoritmo de Euclides

Determinar diretamente o mdc entre dois números inteiros positivos não é eficiente, uma vez que temos de despendar muito tempo na fatorização.

O **Algoritmo de Euclides**, conhecido desde a antiguidade, é uma alternativa mais eficiente.

## ALGORITHM 1 The Euclidean Algorithm.

**procedure**  $\text{gcd}(a, b: \text{positive integers})$

$x := a$

$y := b$

**while**  $y \neq 0$

$r := x \bmod y$

$x := y$

$y := r$

**return**  $x \{\text{gcd}(a, b) \text{ is } x\}$

Figura: Algoritmo de Euclides (Rosen 2012).

# Algoritmo de Euclides

Assim, o Algoritmo de Euclides para determinar o mdc entre dois números inteiros  $a$  e  $b$  positivos consiste em:

- 1 Dividir o maior número pelo menor;
  - 1 Se o resto da divisão for zero, o algoritmo termina e  $\text{mdc}(a, b) = \min\{a, b\}$ .
  - 2 Se o resto da divisão for  $r_1$  (diferente de zero), então sendo  $\min a, b = m$ , então  $\text{mdc}(a, b) = \text{mdc}(m, r_1)$  e continua-se no passo seguinte.
- 2 Dividir  $m$  por  $r_1$ ;
  - 1 Se o resto da divisão for zero, o algoritmo termina e  $\text{mdc}(a, b) = \text{mdc}(m, r_1) = \min\{m, r_1\}$ .
  - 2 Se o resto da divisão for  $r_2$  (diferente de zero), então  $\text{mdc}(a, b) = \text{mdc}(m, r_1) = \text{mdc}(r_1, r_2)$  e continua-se no passo seguinte.
- 3 ...
- 4 até obtermos resto 0.

## Exemplo 122

Pretende-se determinar  $\text{mdc}(91, 287)$ .



Começamos por dividir o maior dos dois números pelo menor.

Obtemos  $287 = 91 \times 3 + 14$ .

Portanto, o  $\text{mdc}$  de 91 e 287 é o mesmo que o  $\text{mdc}(91, 14)$ .

```
fix(287/91)
//ans  =3.
pmodulo(287,91)
//ans  =14.
```

De seguida divide-se 91 por 14, obtendo-se  $91 = 14 \times 6 + 7$  e temos que  $\text{mdc}(91, 14) = \text{mdc}(14, 7)$ .

```
fix(91/14)
//ans  =6.
pmodulo(91,14)
//ans  =7.
```

Dividindo 14 por 7 obtemos  $14 = 7 \times 2$ , portanto 7 divide 14 e  $\text{mdc}(14, 7) = 7$ .

```
fix(14/7)
//ans  =2.
pmodulo(14,7)
//ans  =0.
// Termina o algoritmo
```

Como  $\text{mdc}(91, 287) = \text{mdc}(91, 14) = \text{mdc}(14, 7)$ , concluímos assim que  $\text{mdc}(91, 287) = 7$ .

## Exercício

Usando o Algoritmo de Euclides determine  $\text{mdc}(414, 662)$ .

# Coeficientes de Bézout

O seguinte resultado permite escrever o mdc entre dois número como uma combinação linear desses números, e designa-se por **Teorema de Bézout**.

## Teorema 29 – Teorema de Bézout

Se  $a$  e  $b$  são números inteiros positivos, então existem dois inteiros  $s$  e  $t$  tais que  $\text{mdc}(a, b) = sa + tb$ .

Por exemplo,  $\text{mdc}(6, 14) = 2$  e  $2 = (-2) \times 6 + 1 \times 14$ . Neste caso  $s = -2$  e  $t = 1$ .

## Definição

A  $s$  e  $t$  chamamos os **coeficientes de Bézout**.

A equação  $\text{mdc}(a, b) = sa + tb$  chamamos **identidade de Bézout**.



## Exemplo

Expresse  $\text{mdc}(252, 198)$  como combinação linear de 252 e 198.

Usando o Algoritmo de Euclides temos que

$$\text{mdc}(252, 198) = \text{mdc}(198, 54) = \text{mdc}(54, 36) = \text{mdc}(36, 18) = 18,$$

uma vez que

$$252 = 1 \times 198 + 54,$$

$$198 = 3 \times 54 + 36,$$

$$54 = 1 \times 36 + 18 \text{ e}$$

$$36 = 2 \times 18.$$

Assim, temos que  $18 = 54 - 1 \times 36$  e

$$36 = 198 - 3 \times 54, \text{ donde}$$

$$18 = 54 - 1 \times (198 - 3 \times 54) = 4 \times 54 - 1 \times 198.$$

Além disso,  $54 = 252 - 1 \times 198$ , donde

$$18 = 4 \times (252 - 1 \times 198) - 1 \times 198 = 4 \times 252 - 5 \times 198.$$

Portanto,  $s = 4$  e  $t = -5$  são os coeficientes de Bézout.

**Exercícios:** 109 a 112.

## Definição

**Congruências lineares** são da forma

$$ax \equiv b(\text{mod } m)$$

onde  $m$  é um número inteiro positivo,  $a$  e  $b$  são inteiros e  $x$  é uma variável.

Um método para resolver congruências lineares consiste em encontrar  $\bar{a} \in \mathbb{Z}$  tal que  $\bar{a}a \equiv 1(\text{mod } m)$ , ou seja, encontrar o inverso de  $a$  módulo  $m$ .

O que nem sempre é possível!

## Teorema

Um número inteiro positivo  $a \in \mathbb{Z}_m$  é invertível **se e só se**  $a$  e  $m$  são primos entre si.

**NOTA:** Se  $m$  é primo então todos os elementos não nulos de  $\mathbb{Z}_m$  são invertíveis.

## Exemplo

Encontre o inverso de 3 módulo 7.

Para encontrar o inverso de qualquer elemento de  $\mathbb{Z}_m$  podemos usar os passos do Algoritmo de Euclides, através da determinação dos coeficientes de Bézout.

- Como  $\text{mdc}(3, 7) = 1$  temos a garantia que existe inverso.
- Pelo Algoritmo de Euclides temos que  $7 = 2 \times 3 + 1$ , donde  $1 = 1 \times \mathbf{7} + (-\mathbf{2}) \times \mathbf{3}$ .
- Portanto os coeficientes de Bézout de 7 e 3 são  $s = -2$  e  $t = 1$ .
- Assim, -2 é o inverso de 3 módulo 7.
- Na verdade qualquer inteiro congruente com -2 módulo 7 é inverso de 3 como por exemplo 5, -9, 12, ...

## Exercício

Verifique que 1601 é inverso de 101 módulo 4620.

- Por definição, como  $1601 \times_4 620101 = (1601 \times 101) \bmod 4620 = 1$ , 1601 é inverso de 101 módulo 4620.
- **OU** Pelo Algoritmo de Euclides temos que:

$$4620 = 45 \times 101 + 75$$

$$101 = 1 \times 75 + 26$$

$$75 = 2 \times 26 + 23$$

$$26 = 1 \times 23 + 3$$

$$23 = 7 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$2 = 2 \times 1$$

- Como o último resto da divisão diferente de zero é 1, temos que  $\text{mdc}(101, 4620) = 1$ , pelo que existe a garantia que existe inverso de 101 módulo 4620.

$$\begin{aligned}
4620 &= 45 \times 101 + 75 &\Rightarrow 75 &= 4620 - 45 \times 101 \\
101 &= 1 \times 75 + 26 &\Rightarrow 26 &= 101 - 1 \times 75 \\
75 &= 2 \times 26 + 23 &\Rightarrow 23 &= 75 - 2 \times 26 \\
26 &= 1 \times 23 + 3 &\Rightarrow 3 &= 26 - 1 \times 23 \\
23 &= 7 \times 3 + 2 &\Rightarrow 2 &= 23 - 7 \times 3 \\
3 &= 1 \times 2 + 1 &\Rightarrow 1 &= 3 - 1 \times 2 \\
2 &= 2 \times 1
\end{aligned}$$

$$\begin{aligned}
\text{mdc}(101, 4620) &= s \times 101 + t \times 4620 \\
\text{mdc}(101, 4620) &= 1 \\
&= 3 - 1 \times 2 \\
&= 3 - 1 \times (23 - 7 \times 3) = -1 \times 23 + 8 \times 3 \\
&= -1 \times 23 + 8 \times (26 - 1 \times 23) = 8 \times 26 - 9 \times 23 \\
&= 8 \times 26 - 9 \times (75 - 2 \times 26) = -9 \times 75 + 26 \times 26 \\
&= -9 \times 75 + 26 \times (101 - 1 \times 75) = 26 \times 101 - 35 \times 75 \\
&= 26 \times 101 - 35 \times (4620 - 45 \times 101) = -35 \times 4620 + 1601 \times 101
\end{aligned}$$

Logo os coeficientes de Bézout são:  $s = 1601$  e  $t = -35$ , ou seja, 1601 é inverso de 101 módulo 4620.

# Resolução de congruências lineares

Consideremos a congruência linear  $3x \equiv 4(\text{mod}7)$ .

Vimos que  $-2$  é inverso de  $3$  módulo  $7$ . Assim multiplicando a equação por  $-2$  obtemos:

$$-2 \times 3x \equiv -2 \times 4(\text{mod}7).$$

Como  $-6 \equiv 1(\text{mod}7)$  e  $-8 \equiv 6(\text{mod}7)$ , temos

$$x \equiv -8 \equiv 6(\text{mod}7)$$

Para verificar se esta é a solução fazemos:

$$3x \equiv 3 \times 6 = 18 \equiv 4(\text{mod}7)$$

Portanto, todo o  $x$  que satisfaz  $x \equiv 6(\text{mod}7)$  são soluções da equação, ou seja,  $6, 13, 20, \dots$  e  $-1, -815, \dots$ .

O **Teorema do Resto Chinês**, apresentado de seguida, estabelece as condições para a existência de uma única solução de sistemas de equações congruentes.

### Teorema do Resto Chinês

Sejam  $m_1, m_2, \dots, m_n$  números primos entre si dois a dois tais que  $m_i > 1, \forall i$  e sejam  $a_1, \dots, a_n$  inteiros arbitrários. Então, o sistema

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

$$x \equiv a_n \pmod{m_n}$$

tem uma única solução módulo  $m = m_1 m_2 \dots m_n$ .

# Geração de números (pseudo-)aleatórios

## Método das congruências lineares

- Considere-se o módulo  $m$ , o multiplicador  $a$ , o incremento  $c$  e a raiz  $x_0$ , com  $2 \leq a < m$ ,  $0 \leq c < m$  e  $0 \leq x_0 < m$ , inteiros positivos.
- A **sequência de números pseudo-aleatórios**  $\{x_n\}$ , com  $0 \leq x_n < m$ , para qualquer  $n$ , é obtida pela fórmula de recorrência  $x_{n+1} = (ax_n + c) \bmod m$ .



## Exemplo

A sequência de números pseudo-aleatórios gerada escolhendo  $m = 9$ ,  $a = 7$ ,  $c = 4$  e  $x_0 = 3$  é:

$$x_{n+1} = (ax_n + c) \bmod m$$

$$x_1 = (7x_0 + 4) \bmod 9 = 25 \bmod 9 = 7$$

$$x_2 = (7x_1 + 4) \bmod 9 = 53 \bmod 9 = 8$$

$$x_3 = (7x_2 + 4) \bmod 9 = 60 \bmod 9 = 6$$

$$x_4 = (7x_3 + 4) \bmod 9 = 46 \bmod 9 = 1$$

$$x_5 = (7x_4 + 4) \bmod 9 = 11 \bmod 9 = 2$$

$$x_6 = (7x_5 + 4) \bmod 9 = 18 \bmod 9 = 0$$

$$x_7 = (7x_6 + 4) \bmod 9 = 4 \bmod 9 = 4$$

$$x_8 = (7x_7 + 4) \bmod 9 = 32 \bmod 9 = 5$$

$$x_9 = (7x_8 + 4) \bmod 9 = 39 \bmod 9 = 3$$

Como  $x_9 = x_0$  e cada termo na sequência só depende do anterior, a sequência terá nove números diferentes antes de se começar a repetir:

$$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, \dots$$

É muito utilizado o sistema módulo  $m = 2^{31} - 1$  com incremento  $c = 0$  e multiplicador  $a = 7^5 = 16807$ , que permite gerar  $2^{31} - 2$  números antes que a repetição comece.

## Teorema

### Teorema de Fermat-Euler

Seja  $p$  é um primo que não divide  $a$ , então:

(a)  $a^{p-1} \equiv 1 \pmod{p}$ .

e para todo o inteiro  $a$  temos:

(b)  $a^p \equiv a \pmod{p}$ .

**Exercícios:** Até ao 117.