P.PORTO

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

Textos de

Matemática Discreta

Teoria dos Números

Eliana Costa e Silva

eos@estg.ipp.pt

Para os cursos de:

Licenciatura em Segurança Informática

em Redes de Computadores

Licenciatura em Engenharia Informática

Felgueiras, 2021/2022

O uso destes apontamentos como **único** material de estudo é fortemente desaconselhado.

O aluno deve também consultar a bibliografia recomendada indicada na Ficha da Unidade Curricular e disponível neste documento, nomeadamente, [4], [3], [1], [2].

Conteúdo

Teoria dos Números

Teoria dos Números é uma área da Matemática que se dedica ao estudo de conjuntos de inteiros e às suas propriedades. Tem muitas aplicações práticas de entre as quais se destaca a Criptografia.

Na Secção 1 serão abordados a divisibilidade e aritmética modular. De seguida na Seção 2 é apresentada a resolução de congruências. São também mostradas algumas das suas aplicações. A Criptografia usa várias da propriedades de Teoria de Número. a Secção 3 é feita uma (muito) pequena introdução à Criptografia, sendo o objetivo mostrar a aplicação das propriedades e técnicas apresentadas nas secções anteriores. Finalmente, na Secção 4 são apresentadas alguns conceitos e propriedades de técnicas de contagem, probabilidades e ainda introduzidas as Cadeias de Markov.

1 Divisibilidade e Aritmética Modular

Na divisão de um número inteiro por outro número inteiro não nulo, podemos obter um quociente inteiro ou não. Por exemplo, a divisão de 20 por 5 é o número inteiro 4, enquanto que a divisão de 20 por 8 não é inteiro ($20/8 = 2,5$).

Definição 1:

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 1:

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 ($5 \not| 12$) uma vez que $12/5 = 2,4 \notin \mathbb{Z}$.

Exemplo 2:

Sejam n e d dois números inteiros positivos. Diga quantos números inteiros positivos menores ou iguais a n são divisíveis por d.

Resolução:

Para que um número seja divisível por d ele tem de ser da forma dk, onde k é um número inteiro positivo. Portanto, os divisores positivos de n menores ou iguais a n são $0 < dk \leq n$ ou $0 < k \leq n/d$. Temos assim, $k = \lfloor n/d \rfloor$ divisores positivos de n menores ou iguais a n.

Exercício 1:

Diga quantos números menores ou iguais a 254 são divisíveis por 3.

Fazer!

Teorema 1:

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 $a|bc$ para todo $c \in \mathbb{Z}$;

(iii) se $a|b$ e $b|c$ então $a|c$.

□

Exercício 2:

Faça a prova do Teorema anterior.

Corolario 1:

Sejam a, b e c inteiros, $a \neq 0$, tais que $a|b$ e $a|c$ então $a|mb + nc$ para $m, n \in \mathbb{Z}$. □

Por (ii) do Teorema anterior temos que se $a|b$ então $a|mb, m \in \mathbb{Z}$ e se $a|c$ então $a|nc, n \in \mathbb{Z}$.

Assim, por (i) temos que $a|mb + nc$.

Teorema 2:

Algoritmo de divisão

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

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

Exemplo 3:

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 2:

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

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

Exemplo 4:

Identifique o quociente e o resto da divisão de 101 por 11.

Resolução:

Temos que $101 = 11 \times 9 + 2$.

Portanto, o quociente é $q = 9 = 101$ div 11 e o resto é $r = 2 = 101 \bmod 11$.

Exemplo 5:

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

Resolução:

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

Portanto, o quociente é $q = -3 = -13$ 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`.

Em muitas aplicações estamos apenas interessados no resto da divisão entre dois inteiros.

Definição 3:

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 $a \equiv b(\mathrm{mod}m)$ e $a \bmod m = b$ incluem "mod" mas representam conceitos distintos!

$a \equiv b(\mathrm{mod}m)$ representa uma relação no conjuntos dos números inteiros, enquanto que, $a \bmod m = b$ representa uma operação. O Teorema seguinte estabelece a relação entre as duas.

Teorema 3:

Sejam a e b dois números inteiros e m um inteiro positivo.

Então $a \equiv b(\mathrm{mod}m)$ **se e só se** $a \bmod m = b \bmod m$. □

Observação:

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

Exemplo 6:

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

Resolução:

Como 6 divide 17-5=12, temos que $17 \equiv 5(\mathrm{mod}6)$.

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

Teorema 4:

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 $a = b + km$. □

O Teorema anterior mostra-se facilmente.

Se $a \equiv b\,(\mathrm{mod}m)$, então por definição m divide $a - b$, ou seja, existe um inteiro k tal que $a - b = km$ ou $a = b + km$.

Reciprocamente se existe um inteiro k tal que $a = b + km$ então $a - b = km$, ou seja, m divide $a - b$, e portanto, por definição $a \equiv b\,(\mathrm{mod}m)$.

Teorema 5:

Seja m um inteiro positivo.

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

Exercício 3:

Aplique o Teorema anterior à seguinte situação:

Como $7 \equiv 2\,(\mathrm{mod}5)$ e $11 \equiv 1(\mathrm{mod}5)$, então ...

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

Corolario 2:

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

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

□

A prova deste Teorema é deixada como exercício!

Aritmética módulo m

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

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

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

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 4:

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 $a + mb = b +_m a$ 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., $a +_m (m-a) = 0$ 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[1]. 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

Usando aritmética modular temos uma maneira simples de codificar e descodificar informação. Por exemplo podemos multiplicar por 7 módulo 10 para codificar a informação e multiplicar por 3 módulo 10 para descodificar. 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

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

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

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

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

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!).

```
-->modulo(9*7,10)
 ans  =

    3.
-->modulo(7*7,10)
 ans  =

    9.
    -->modulo(8*7,10)
 ans  =

    6.
```

[1] Voltaremos a este assunto na página 13.

```
-->modulo(3*7,10)
 ans  =

    1.
```

Algoritmo de Euclides, que será visto mais adiante é também uma aplicação da aritmética modular.

Números primos e máximo divisor comum

Números primos são essenciais em sistemas de Criptologia modernos[2]. E o tempo de fatorização de números inteiros grandes é o que torna fortes alguns dos mais importantes e modernos sistemas de criptologia.

De seguida veremos algumas propriedades úteis relativas a números primos. Será também apresentado o **algoritmo de Euclides** - um importante algoritmo para cálculo de máximos divisores comuns.

Definição 4:

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 7:

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.

Explore as funções `primes` e `factor`.

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.

Teorema 6:

Teorema Fundamental da aritmética

Todo o número inteiro maior que 1 pode ser escrito de modo único como um número primo ou por um produto de dois ou mais fatores primos onde cada fator é escrito por ordem não decrescente. □

[2]Veja o vídeo disponível em disponibilizado no moodle que explica a importância de números primos na Criptologia.

Exemplo 8:

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, por exemplo, números primos grandes são usados para codificar mensagens[3]. 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 [4].

Teorema 7:

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

Este resultado garante que um número inteiro é primo se não é divisível por nenhum número primo menor ou igual que a sua raiz quadrada, o que nos sugere que "basta" verificar se o número em questão não é divisível por todos os números primos menores ou iguais que a sua raiz quadrada. Vejamos o seguinte exemplo.

Exemplo 9:

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.

Crivo de Eratóstenes

De seguida será ilustrado o **Crivo de Eratóstenes** para a determinação dos números primos menores que 100.

Comecemos por notar que 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.

Assim, começamos por dispor todos os números inteiros positivos menores ou iguais a 100 numa grelha (ver Figura 1.1).

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.

[3] Veja o vídeo disponível em https://www.youtube.com/watch?v=56fa8Jz-FQQ.

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

Figura 1.1: Crivo de Eratóstenes

Mas afinal quantos números primos existem?

A resposta a esta questão é dada pelo Teorema abaixo cuja prova pode ser feita por redução ao absurdo (ver, por exemplo, [4]).

Teorema 8:

Existe um número infinito de números primos. □

Números primos de Mersenne

Um **número de Mersenne**[4] 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 10:

$2^2 - 1 = 4 - 1 = 3$ 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 $p = 2, 3, 5, 7, 13, 17, 19, 31$.

Desde 1996 que o projeto de computação distribuída "*Great Internet Mersenne Prime Search*" 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**[5]- extremamente eficiente para verificar se o número é primo.

[4]Este nome foi dado em homenagem ao monge Francês Marin Mersenne que estudou estes números no século dezassete.

[5]Ver mais informações em `http://www.mersennewiki.org/index.php/Lucas-Lehmer_Test`.

Adicionalmente, não existem atualmente outros testes que permitam fazer esta verificação para números que não sejam desta forma ou de outras formas particulares.

Sabemos que existe um número infinito de números primos, no entanto, a questão de saber quantos número primos são menores que um dado número x foi tema de interesse de muitos matemáticos durante muitos anos. O Teorema seguinte dá-nos uma ideia da distribuição dos números primos.

Teorema 9:

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 resultado anterior pode ser usado para estimar as chances de que um número qualquer (escolhido aleatoriamente) seja primo. O Teorema diz-nos que o número de números primos menores ou iguais a x pode ser aproximado por $\frac{x}{\ln x}$. 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

Existem inúmeras perguntas sem resposta relativas a números primos. De facto, Teoria dos Números é um tema em que facilmente se formulam conjeturas mas encontrar a sua prova tem-se mostrado uma tarefa difícil e em inúmeros casos continuam a ser perguntas sem reposta!

Por exemplo, para a Criptologia, assim como em muitas outras aplicações, seria extremamente útil conseguir definir uma função $f(n)$ tal que para todo o n, $f(n)$ fosse um número primo.

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.

Mínimo múltiplo comum e máximo divisor comum

Definição 5:

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** de a e b, e escreve-se $d = \text{mdc}(a, b)$.

Exercício 5:

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

Definição 6:

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

Exercício 6:

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

Definição 7:

O **mínimo múltiplo comum** entre dois números inteiros positivos é o menor inteiro positivo que divide simultaneamente a e b. Escreve-se $\text{mmc}(a, b)$.

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

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

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 7:

Encontre o mdc e o mmc entre 120 e 500.

 Explore as funções `gcd` e `lcm`.

Teorema 10:

Sejam a e b dois números inteiros positivos.

Então,

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

□

Exercício 8:

Verifique o resultado acima no exercício anterior.

Algoritmo de Euclides

Determinar diretamente o mdc entre dois números inteiros não é eficiente, uma vez que temos de despender muito tempo na fatorização. O **Algoritmo de Euclides**, conhecido desde a antiguidade, é uma alternativa mais eficiente. Este algoritmo será introduzido no exemplo seguinte (Ver também a Figura 1.2).

Exemplo 11:

Pretende-se determinar mdc(91,287).

Comecemos por dividir o maior dos dois números pelo menor. Neste caso obtemos $287 = 91 \times 3 + 14$.

Qualquer divisor de 91 e de 287 também tem de ser divisor de $287 - 91 \times 3 = 14$. De igual modo, qualquer divisor de 91 e 14 também tem de ser divisor de $287 = 91 \times 3 + 14$.

Portanto, o mdc de 91 e 287 é o mesmo que o mdc(91,14).

De seguida divida-se 91 por 14, obtendo-se $91 = 14 \times 6 + 7$.

Como qualquer divisor comum de 91 e 14 é também é divisor de 7 e qualquer comum divisor de 14 e 7 é também divisor de 91, temos que mdc(91,14)=mdc(14,7).

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

Como mdc(91,287)=mdc(91,14) = mdc(14,7), concluímos assim que mdc(91,287)=7.

O algoritmo de Euclides assenta no seguinte resultado.

Lema 1:

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

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

Exercício 9:

Usando o Algoritmo de Euclides determine mdc(414,662).

Exercício 10:

Implemente em Scilab o Algoritmo de Euclides (Figura 1.2).

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

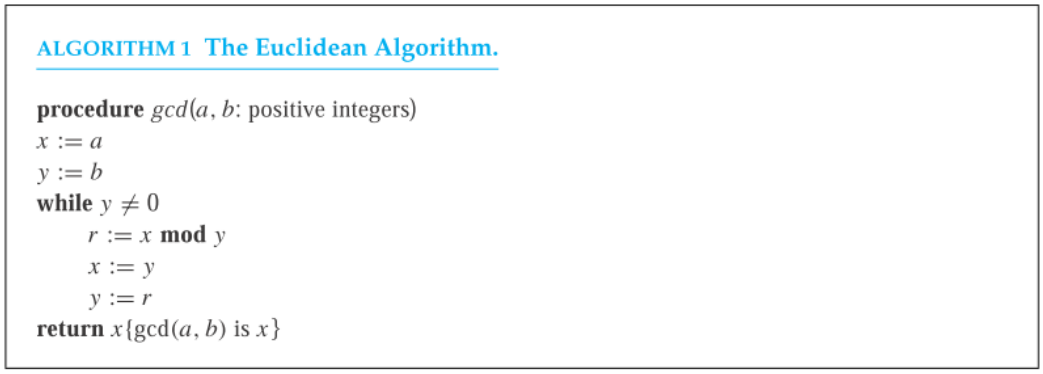
Teorema 11:

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 $t = 1$.

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

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



ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\text{gcd}(a, b) \text{ is } x\}$

Figura 1.2: Algoritmo de Euclides (in [4]).

Exemplo 12:

Expresse mdc$(252, 198)$ como combinação linear de 252 e 198.

Usando o Algoritmo de Euclides temos que mdc$(252, 198)$ = mdc$(198, 54)$ =mdc$(54, 36)$=mdc$(36, 18)$=18, uma vez que

$252 = 1 \times 198 + 54$, $198 = 3 \times 54 + 36$, $54 = 1 \times 36 + 18$ e $36 = 2 \times 18$.

Assim, temos que $18 = 54 - 1 \times 36$ e $36 = 198 - 3 \times 54$, 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.

2 Resolução de Congruências e suas Aplicações

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.

Estas são muito frequentemente usadas em Teoria dos Números e nas suas aplicações. Mais adiante veremos um exemplo da sua aplicação à geração de números aleatórios.

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!

Para se caraterizar os elemento de $\mathbb{Z}_m$ que admitem inverso em $\times_m$ basta que o seguinte resultado se verifique.

Teorema 12:

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

Exemplo 13:

Encontre, se possível, os inversos de $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

Como $\text{mdc}(1, 5) = 1$, $\text{mdc}(2, 5) = 1$, $\text{mdc}(3, 5) = 1$, $\text{mdc}(4, 5) = 1$ temos que todos os elementos não nulos de $\mathbb{Z}_5$ são invertíveis:

$$1 \times_5 1 = 1; \quad 2 \times_5 3 = 1; \quad 3 \times_5 2 = 1; \quad 4 \times_5 4 = 1.$$

De facto, **se m é primo então todos os elementos não nulos de $\mathbb{Z}_m$ são invertíveis.**

Exercício 11:

Identifique os elementos invertíveis em: **(a)** $\mathbb{Z}_4$; **(b)** $\mathbb{Z}_6$; **(c)** $\mathbb{Z}_{10}$.

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

Exemplo 14:

Encontre o inverso de 3 módulo 7.

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 12:

Verifique que 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, $6, 13, 20, \ldots$ e $-1, -8$-$15, \ldots$.

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

Teorema 13:

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

$$x \equiv a_1 (\mathrm{mod} m_1)$$
$$x \equiv a_2 (\mathrm{mod} m_2)$$
$$\ldots$$
$$x \equiv a_n (\mathrm{mod} m_n)$$

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

Aplicações

Geração de números (pseudo-)aleatórios

Em qualquer software de Matemática é possível gerar números aleatórios, uma vez que a geração destes números é muito útil em simulações computacionais.

O método mais comummente usado é o chamado **método das congruências lineares**, que descrevemos de seguida.

Escolhemos quatro inteiros:

o módulo m, o multiplicador a, o incremento c e a raiz x_0, com $2 \leq a < m, 0 \leq c < m$ e $0 \leq x_0 < m$.

A sequência de números pseudo-aleatórios $\{x_n\}$, com $0 \leq x_n < m$ para qualquer n é obtida pela fórmula de recorrência $x_{n+1} = (ax_n + c) \bmod m$.

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

$$x_1 = (7x_0 + 4) \bmod 9 = 25 \bmod 9 = 7$$
$$x_2 = (7x_1 + 4) \bmod 9 = 53 \bmod 9 = 8$$
$$x_3 = (7x_2 + 4) \bmod 9 = 60 \bmod 9 = 6$$
$$x_4 = (7x_3 + 4) \bmod 9 = 46 \bmod 9 = 1$$
$$x_5 = (7x_4 + 4) \bmod 9 = 11 \bmod 9 = 2$$
$$x_6 = (7x_5 + 4) \bmod 9 = 18 \bmod 9 = 0$$
$$x_7 = (7x_6 + 4) \bmod 9 = 4 \bmod 9 = 4$$
$$x_8 = (7x_7 + 4) \bmod 9 = 32 \bmod 9 = 5$$
$$x_9 = (7x_8 + 4) \bmod 9 = 39 \bmod 9 = 3$$

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:

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

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.

No seguinte resultado (a) deve-se ao matemático Pierre de Fermat e (b) a Leonard Euler.

Teorema 14:

Teorema de Fermat-Euler

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

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

e para todo o inteiro a temos:

(b) $a^p \equiv a (\mathrm{mod} p)$. □

Exercício 13:

Determine 7^{222} mod 11.

Solução: 7^{222} mod $11 = 5$

3 Criptografia

Em Criptografia a Teoria dos Números tem um grande papel. Nesta pretende-se transformar a informação de forma a que esta não possa ser recuperada sem algum conhecimento especial. Nesta seção damos alguns exemplos da utilização da Teoria dos Números na Criptografia.

Cifra de César

A **Cifra de César** trata-se de um método de escrita de mensagens secretas proposto por César que consistia em transladar cada letra do alfabeto para três "casas" mais adiante, como se mostra de seguida:

A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Z	A	B	C

Este sistema de encriptação pode ser descrito Matematicamente de forma muito abreviada do seguinte modo:

substituímos cada letra por um inteiro de 0 até 22, baseado na sua posição no alfabeto, onde $A \leftrightarrow 0, \ldots,$ $Z \leftrightarrow 22$.

Portanto o método de César é definido pela função f que aplica cada inteiro n, $0 \leq n \leq 22$, no inteiro $f(n) = (n + 3)$ mod 23.

Por exemplo, $X \leftrightarrow 21 \longrightarrow f(21) = 24 \bmod 23 = 1 \leftrightarrow B$.

Exercício 14:

Como fica a mensagem "DISCRETA" depois de encriptada pela cifra de César?

Para recuperar a mensagem original a partir da mensagem encriptada basta considerar a função inversa f^{-1} que transforma um inteiro $n, 0 \leq n \leq 22$, em $f^{-1}(n) = (n-3) \bmod 23$.

Podemos generalizar a cifra de César transladando b casas em vez de três da seguinte forma: $f(n) = (n+b) \bmod 23$.

Este é um método muito simples e muito pouco seguro que pode ser melhorado definindo

$$f(n) = (an + b) \bmod 23,$$

com a e b inteiros escolhidos de modo a garantir que f é uma bijeção (**Porquê?**)

O sistema RSA de chave pública

Este sistema foi desenvolvido em 1976 por Rivest, Shamir e Adleman. De seguida apresenta-se um exemplo.

Suponhamos que a Ana pretende enviar uma mensagem x ao Bruno, pedindo-lhe que gere um par de chaves. Uma chave pública u (conhecida por toda a gente) e uma chave privada v (conhecida apenas pelo Bruno). As chaves u e v são aplicações do espaço das mensagens para o espaço das mensagens e, para que o sistema funcione bem e permita manter o secretismo na comunicação, devem ter as seguintes propriedades:

(P1) $v(u(x)) = x$ para qualquer mensagem x.

(P2) deve ser difícil obter x conhecendo $u(x)$ e não conhecendo v.

O protocolo funciona do seguinte modo:

[1] A Ana envia a mensagem $u(x)$ ao Bruno pelo canal público.

[2] O Bruno recupera a mensagem original x aplicando v a $u(x)$.

Ao definirmos um sistema criptográfico deveremos explicitar o espaço das mensagens bem como as aplicações u e v.

Os sistemas criptográficos do tipo RSA são definidos do seguinte modo:

- Espaço de mensagens: $Z_m = \{0, 1, 2, \ldots, m-1\}$, onde $m = p \times q$ para algum par de primos p, q;
- $u(x) = x^a \bmod m$, para qualquer $x \in \mathbb{Z}_m$;
- $v(y) = y^b \bmod m$, para qualquer $y \in \mathbb{Z}_m$;

onde a e b são tais que $a \times b \bmod [(p-1) \times (q-1)] = 1$.

A confirmação se um sistema que respeita (P1) e (P2) é um bom sistema é ainda uma pergunta em aberto visto ainda não ter sido provada (P2)!

Este sistema permite enviar mensagens encriptadas por uma chave pública a, mas para que o recetor seja capaz de desencriptar a mensagem precisa de ter uma chave privada b, apenas do seu conhecimento.

Sejam p e q dois números primos, $m = pq$, $n = (p-1)(q-1)$.

Consideremos ainda a tal que $\text{mdc}(a, n) = 1$ e seja b a solução da congruência $ab \equiv 1 \bmod n$. No sistema RSA, podemos começar por traduzir as mensagens (sequências de letras) em sequências de números inteiros (tal como na cifra de César).

O inteiro x daí resultante é depois transformado, com a ajuda da chave pública a, num inteiro $u(x) = x^a \bmod m$.

O recetor quando recebe a mensagem desencripta-a com a ajuda da chave privada b que apenas ele conhece: $v(u(x)) = u(x)^b \bmod m$.

Exercício 15:

Codifique a mensagem "SOS" usando o sistema RSA com $p = 43, q = 59$ e $a = 13$.

Resolução:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

Como S $\to$ 18 e O $\to$ 14. Assim,
$18^{13} \bmod (2537) = 2222$ e $1418^{13} \bmod (2537) = 1289$

```
-->x=18; x_new=1;  for k=1:13, x_new=pmodulo(x*x_new,2537);end,x_new
 x_new  =

    2222.

-->x=1418; x_new=1;  for k=1:13, x_new=pmodulo(x*x_new,2537);end,x_new
 x_new  =

    1289.
```

A mensagem encriptada é: 2222 1289.

Exercício 16:

Desencripte a mensagem seguinte, recebida usando o sistema RSA do exemplo anterior: 2081 2182.

Resolução:

$2081^{937} \bmod (2537) = 1819$ e $2182^{937} \bmod (2537) = 1415$

```
-->x=2081; x_new=1;  for k=1:937, x_new=pmodulo(x*x_new,2537);end,x_new
 x_new  =

    1819.

-->x=2182; x_new=1;  for k=1:937, x_new=pmodulo(x*x_new,2537);end,x_new
 x_new  =

    1415.
```

Como 18 → S; 19 → T; 14 → O; 15 → P.

A mensagem original é STOP.

Proposição 1: Sejam p e q primos distintos, $m = pq$ e $n = (p-1)(q-1)$.
Se a e b são inteiros tais que $ab \equiv 1 \bmod n$, então $v(u(x)) = x$ para qualquer inteiro $x < p, q$.

Mas como se desenrola na realidade o processo de troca de mensagens secretas entre a Ana e o Bruno?

O recetor, o Bruno:

1. escolhe dois números primos p e q - que pode ser difícil quando se procuram números p e q muito grandes;
2. calcula os produtos $m = pq$ e $n = (p-1)(q-1)$ - é muito fácil!
3. escolhe $a \in \mathbb{Z}_n$ (a chave pública) tal que $\text{mdc}(a, n) = 1$ - é fácil se conhecemos um algoritmo eficaz para calcular o mdc de 2 números!
4. usando o algoritmo de Euclides, determina $b \in \mathbb{Z}_n$ (a chave privada) tal que $ab \equiv 1 \bmod n$ - é fácil se conhecemos um algoritmo eficaz para calcular o inverso de um elemento em $\mathbb{Z}_n$!
5. envia os valores de m e a para a Ana, mantendo a chave privada b apenas do seu conhecimento - não havendo garantias de segurança no canal de comunicação, os valores de m e a passam a ser eventualmente públicos!

A Ana tem agora os elementos para encriptar as suas mensagens com a função u e enviá-las ao Bruno. Como apenas o Bruno conhece o valor de b, apenas ele poderá decifrar a mensagem aplicando a função v.

E que trabalho tem que fazer uma terceira pessoa mal intencionada, que conhece apenas a função de encriptação, para desencriptar uma mensagem?

1. fatorizar o número m para recuperar os primos p e q - o que pode ser muito difícil quando m é muito grande;
2. usando o algoritmo de Euclides, determinar $b \in \mathbb{Z}_n$ (a chave privada) tal que $ab \equiv 1 \bmod n$ - o que será fácil se conhecemos um algoritmo eficaz para calcular o inverso de um elemento em $\mathbb{Z}_n$.

Portanto,

- para criar o código é preciso encontrar dois números primos p e q;
- para decifrar o código é preciso fatorizar o produto $n = pq$.

4 Técnicas de Contagem, Probabilidades e Cadeias de Markov

4.1 Técnicas de Contagem

Regra do produto

Suponha que um **Acontecimento 1** pode ocorrer de n_1 maneiras diferentes e que um **Acontecimento 2** pode ocorrer de n_2 maneiras diferentes. Suponha, também, que cada ocorrência do Acontecimento 1 pode ser seguida por qualquer das ocorrências do Acontecimento 2.
O Acontecimento formado por:
Acontecimento 1 seguido de Acontecimento 2
poderá ser executado de $n_1 \times n_2$ maneiras distintas.

Esta regra pode ser generalizada para qualquer número de acontecimentos. Se existirem m acontecimentos e o i-ésimo acontecimentos puder ocorrer de n_i maneiras distintas, $i = 1, 2, \ldots, m$, então o acontecimento formado por 1, seguido por 2, ..., seguido do acontecimento k, poderá ser executado de $n_1 \times n_2 \times \cdots \times n_m$ maneiras.

A regra do produto pode ser escrita sobre a forma de conjuntos do seguinte modo:
Se $A_1, A_2, \ldots, A_m$ são conjuntos finitos, então

$$\#(A_1 \times A_2 \times \cdots \times A_m) = \#A_1 \times \#A_2 \times \cdots \times \#A_m$$

Exemplo 15:

Uma nova empresa tem apenas dois funcionários S e J. A empresa alugou um edifício com 12 gabinetes. De quantos modos diferentes a empresa pode atribuir os gabinetes aos dois trabalhadores?

Podemos escolher de 12×11 maneiras diferentes.

Arranjos com Repetição ou Arranjos Completos

Chamam-se **arranjos com repetição** dos n elementos p a p (onde n e p são números naturais) a todas as sequências de p elementos, sendo estes diferentes ou não, que se podem formar a partir de um conjunto de n elementos. O número de arranjos com repetição de n elementos p a p, representa-se por

$$^{n}A'_{p} = n^{p}.$$

Arranjos sem Repetição ou Arranjos Simples Dados n elementos diferentes, chamam-se **Arranjos sem Repetição** ou **Arranjos Simples** de n elementos p a p (onde n e p são números naturais tais que $n \geq p$) às sequências de p elementos distintos (sem repetição) que é possível formar com esses n elementos. O número de arranjos sem repetição de n elementos p a p, é dado por:

$$^{n}A_p = \frac{n!}{(n-p)!}, \text{ com } n \geq p.$$

Permutações

Chamam-se **permutações** de n elementos às sequências de n elementos distintos (sem repetição) que é possível formar com esses n elementos (isto é, com os elementos de um conjunto de cardinal n). O número de permutações de n elementos é dado por:

$$P_n = n!$$

Observações

- As permutações de n elementos coincidem com os arranjos simples desses n elementos tomados n a n:
$$^{n}A_n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = \frac{n!}{1} = n! = P_n$$
- Duas permutações diferem apenas na ordem dos seus elementos.

Exemplo 16:

De quantas formas diferentes se pode escolher primeiro, segundo e terceiros classificados de conjuntos de 100 participantes? Trata-se de arranjos de 100, 3 a 3:

$$^{100}A_3 = \frac{100!}{(100-3)!} = \frac{100 \times 99 \times 98 \times 97!}{97!} = 100 \times 99 \times 98$$

Suponhamos que temos n elementos, tais que n_1 são de uma primeira espécie, n_2 são de uma segunda espécie, $\ldots$, n_m são de uma m-ésima espécie, com $n_1 + n_2 \cdots + n_m = n$. Neste caso, o número de permutações possíveis desses n elementos (considerando idênticos os da mesma espécie) é dado por:

$$P_n(n_1, n_2, \ldots, n_m) = \frac{n!}{n_1! n_2! \ldots n_m!}.$$

Combinações

Chamam-se **Combinações de** n elementos p a p (onde n e p são números naturais tais que $0n \geq p \geq 0$) aos subconjuntos de p elementos formandos a partir de um conjunto com n elementos. O número de **combinações** de n elementos p a p é dado por:

$$^{n}C_p = \frac{n!}{(n-p)!p!}$$

Observações:

Designação	**Fórmula**	**Exemplo**	**Comparação de dois agrupamentos**
Arranjos com Repetição ${}^{n}A'_{p}$	${}^{n}A'_{p} = n^{p}$	${}^{8}A'_{4} = 8^{4}$	São diferentes se diferirem na ordem ou em pelo menos um elemento (pode haver repetição)
Arranjos sem Repetição ${}^{n}A_{p}$	${}^{n}A_{p} = \frac{n!}{(n-p)!}$	${}^{8}A_{4} = \frac{8!}{(8-4)!}$	São diferentes se diferirem na ordem ou em pelo menos um elemento (não há repetição)
Permutações P_n	$P_n = n!$	$P_8 = 8!$	São diferentes se diferirem na ordem
Combinações ${}^{n}C_{p}$ ou $\binom{n}{p}$	${}^{n}C_{p} = \frac{n!}{(n-p)!p!}$	${}^{8}C_{4} = \frac{8!}{(8-4)!4!}$	São diferentes se diferirem em pelo menos um elemento. (não há repetição e a ordem é indiferente)

Tabela 1.1: Tabela resumo.

- Como, nas combinações a ordem não interessa, formamos subconjuntos e não sequências, e, por isso, nesta definição, utilizamos a notação relativa aos conjuntos.
- Para valores grandes de n e r a expressão ${}^{n}C_{p} = \frac{n!}{(n-p)!p!}$ não é útil por razões computacionais. Por exemplo:

```
-->factorial(200)/(factorial(200-3)*factorial(3))
 ans  =

    Nan
```

Para estes casos simplificamos a expressão de ${}^{n}C_{p}$ e calculamos

$$ {}^{n}C_{p} = \frac{n!}{(n-p)!p!} = \frac{n(n-1)(n-2)\dots(n-p+1)}{p!} $$

Para o exemplo anterior temos:

```
-->200*(200-1)*(200-2)/factorial(3)
 ans  =

    1313400.
```

- Temos que ${}^{n}C_{p} \times P_n = {}^{n}A_{p}$

Exemplo 17:

Um grupo de 30 pessoas foram treinadas para a primeira missão em Marte. De quantas formas se pode selecionar uma tripulação de seis pessoas, assumindo que todos os membros da tripulação têm as mesmas tarefas?

$$^{30}C_6 = \frac{30!}{(30-6)!6!} = \frac{30 \times 29 \times 28 \times 27 \times 26 \times 25}{6 \times 5 \times 4 \times 3 \times 2} = 593\ 775.$$

Regra da soma

$$\#A_1 \cup A_2 \cup \ldots A_m) = \#A_1 + \#A_2 + \cdots + \#A_m, \text{ onde } A_i \cap A_j = \emptyset, \text{ para todo } i, j.$$

Regra da subtração – Princípio da inclusão-exclusão

$$\#(A_1 \cup A_2) = \#A_1 + \#A_2 - \#(A_1 \cap A_2)$$

4.2 Probabilidades (Discreta)

Uma **experiência** aleatória é um procedimento cujo resultado é um entre todos os possíveis resultados.

O **espaço amostral** de uma experiência é o conjunto de todos os resultados possíveis.

Um **acontecimento** é um subconjunto do espaço amostral.

Definição 8:

Lei de Laplace

Seja S um conjunto finito não vazio e A um acontecimento de S. Temos que a probabilidade de A é

$$p(A) = \frac{\#A}{\#S}.$$

Definição 9:

Chamamos frequência relativa do acontecimento A, nas n repetições de uma experiência, ao número obtido por:

$$f_A = \frac{n_A}{n},$$

onde n_A é o número de que o acontecimento A ocorre em n experiências.

Propriedades 1:

A frequência relativa f_A apresenta as seguintes propriedades:

- $0 \leq f_A \leq 1$;
- $f_A = 1$ se, e só se, A ocorrer em todas as n repetições
- $f_A = 0$ se, e só se, A nunca ocorrer nas n repetições
- Se A e B forem acontecimentos mutuamente exclusivos, e se $f_{A\cup B}$for a frequência relativa associada ao acontecimento $A \cup B$, então

$$f_{A\cup B} = f_A + f_B$$

Se o número de repetições da experiência for aumentando, o valor da frequência relativa f_A tenderá a "estabilizar" próximo de um determinado valor numérico bem definido:

$$p(A) = \lim_{n\to\infty} f_A.$$

Axioma 1:

Seja S o espaço amostral associada a uma experiência. Temos que:

- $p(A) \geq 0$, para todo o acontecimento A de S.
- $p(S) = 1$.
- $p(A \cup B) = p(A) + p(B)$, onde A e B são dois acontecimentos mutuamente exclusivos.
- $p\left(\cup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} p(A_i)$, onde $A_i \cap A_j = \emptyset$.

Teorema 15:

- $p(\emptyset) = 0$
- $p(\bar{A}) = 1 - p(A)$
- $p(B \setminus A) = p(B) - p(A \cap B)$
- Se $A \subset B$ então $p(B \setminus A) = p(B) - p(A)$
- $p(A \cup B) = p(A) + p(B) - p(A \cap B)$
- Se A e B forem acontecimentos tais que $A \subset B$, então $p(A) \leq p(B)$.
- $p(A) \leq 1$

□

Exemplo 18:

Qual a probabilidade de um número inteiro selecionado aleatoriamente de um conjunto de números inteiros não superiores a 100 serem divisíveis por 2 ou por 5? Seja A o acontecimento o número selecionado ser divisível por 2 e B o acontecimento o número selecionado ser divisível por 5. Temos que $A \cap B$ é o acontecimento o número ser simultaneamente divisível por 2 e 5. Pretende-se determinar $p(A \cup B)$. Assim,

$$p(A \cup B) = p(A) + p(B) - p(A \cap B) = \frac{50}{100} + \frac{20}{100} - \frac{10}{100} = \frac{3}{5}.$$

Veja o Exemplo 10, página 450 de (Rosen, 2014).

Definição 10:

Probabilidade Condicionada

Sejam A e B dois acontecimentos tais que $p(B) > 0$. A probabilidade de A condicionada a B é dada por

$$p(A|B) = \frac{p(A \cap B)}{p(B)}.$$

Exemplo 19:

Considere um string de bits de comprimento quatro é gerado aleatoriamente tal que cada um dos 16 strings de bits de comprimento quatro sejam igualmente prováveis.

Qual a probabilidade do string de bits conter pelo menos dois 0s consecutivos, dado que o seu primeiro bit é 0? **Solução**: $\frac{5}{8}$

Observações:

- $0 \leq p(A|B) \leq 1$
- $p(S|B) = 1)$
- $p(A_1 \cap A_2|B) = p(A_1|B) + p(A_2|B)$
- $p(A \cap B) = p(A)p(B|A) = p(B)p(A|B)$

Definição 11:

Dois acontecimentos A e B são ***independentes*** se e só se $p(A \cap B) = p(A) \times p(B)$.

Exemplo 20:

Seja A o acontecimento um string de bits de comprimento quatro é gerado aleatoriamente começa com um 1 e B o acontecimento o string de bits contem um número par de 1s. Verifique se A e B são independentes.

Existem oito strings de comprimento quatro que começam por 1: 1000, 1001, 1010, 1011, 1100, 1101, 1110 e 1111.

Existem oito strings de comprimento quatro com um número par de 1s: 000, 0011, 0101, 0110, 1001, 1010, 1100 e 1111.

Como existem 16 strings de comprimento 4 temos que:

$$p(A) = p(B) = \frac{8}{16} = \frac{1}{2}.$$

Por outro lado, $A \cap B = \{1111, 1100, 1010, 1001\}$, donde $p(A \cap B) = \frac{4}{16} = \frac{1}{4}$. Assim,

$$p(A \cap B) = p(A)p(B),$$

donde A e B são acontecimentos independentes.

Definição 12:

Dizemos que $A_1, A_2, \ldots, A_n$ são **independentes dois a dois** se$p(A_i \cap A_j) = p(A_i) \times p(A_j)$, para todos os pares de inteiros i e j com $1 \leq i < j \leq n$.

Estes acontecimentos dizem-se **mutuamente independentes** se

$$p(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m}) = p(A_{i_1})p(A_{i_2}) \ldots p(A_{i_m})$$

onde $i_j, j = 1, 2, \ldots, m$, são inteiros com $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ e $m \geq 2$.

Definição 13:

Seja S um conjunto com n elementos. A *distribuição uniforme* atribuiu a cada elementos de S a probabilidade $1/n$.

Experiências de Bernoulli e Distribuição Binomial

Consideremos uma experiência com apenas dois possíveis resultados, p.e., 0 ou 1. Cada possível resultado é uma experiência de Bernoulli e o seu resultado designamos por **sucesso** ou **insucesso**.

Seja p a probabilidade de sucesso e $q = 1 - p$ a probabilidade de insucesso. A probabilidade de se obterem exatamente k sucessos é dada por

$$^nC_k p^k q^{n-k}.$$

À função $b(k; n, p) = {}^nC_k p^k q^{n-k}$ chamamos **distribuição binomial**.

Exemplo 21:

Suponha que a probabilidade de ser gerado o bit 0 é 0.9 e que os bits 0 e 1 são gerados independentemente. Qual a probabilidade de num string de 10 bits termos exatamente oitos bits 0?

Solução: ≈ 0.1937

Distribuição geométrica

Uma variável aleatória X tem uma distribuição geométrica de parâmetro p se $p(X = k) = (1 - p)^{k-1}$, para $k = 1, 2, 3, \ldots$, onde p é um número real tal que $0 \leq p \leq 1$.

Teorema 16:

Teorema de Bayes

Sejam A e B acontecimentos de S tais que $p(A) \neq 0$ e $p(B) \neq 0$. Então,

$$p(B|A) = \frac{p(A|B)p(B)}{p(A|B)p(B) + p(A|\bar{B})p(\bar{B})}.$$

□

Teorema 17:

Generalização do Teorema de Bayes

Sejam A um acontecimentos de S e $B_1, B_2, \ldots, B_n$ acontecimentos mutuamente exclusivos tais que $\cup_{i=1}^{n} B_i = S$. Assuma que $p(A) \neq 0$ e $p(B_i) \neq 0$, $i = 1, \ldots, n$. Então,

$$p(B_j|A) = \frac{p(A|B_j)p(B_j)}{\sum_{i=1}^{n} p(A|B_i)p(B_i)}$$

□

Uma aplicação dos dois últimos resultados são os filtros Bayesianos de spam de correio eletrónico. Ver (Rosen, 2014) página 472 até 475.

Definição 14:

Seja X uma variável aleatória definida no espaço amostral S.

- O valor esperado ou **valor médio esperado** de X é dado por:

$$E[X] = \sum_{s \in S} p(s)X(s).$$

- A **variância** de X é:

$$V[X] = \sum_{s \in S} (X(s) - E[X])^2 p(s)$$

- O **desvio-padrão** de X é:

$$\sigma[X] = \sqrt{V[X]}.$$

Se o espaço amostral é tal que $S = \{x_1, x_2, \ldots, x_n\}$, então $E[X] = \sum_{i=1}^{n} p(x_i)X(x_i)$.

Teorema 18:

- O valor esperado do número de sucessos em n experiências de Bernoulli, onde p é a probabilidade de sucesso de cada experiência é: np.
- O valor esperado de uma variáveis X com distribuição de geométrica de parâmetro p é $E[X] = 1/p$.

□

Propriedades 2:

Sejam n um número inteiro positivo, $X_1, X_2, \ldots, X_n$, n variáveis aleatórias em S, $a, b \in \mathbb{R}$. Temos que:

- $E[X_1 + X_2 + \cdots + X_n] = E[X_1] + E[X_2] + \cdots + E[X_n]$
- $E[aX + b] = aE[X] + b$
- Se X_1 e X_2 são independentes, então $E[X_1\ X_2] = E[X_1]E[X_2]$
- **Fórmula de Bienaymé**:

  Se X_1 e X_2 são independentes, então $V[X_1 + X_2] = V[X_1] + E[X_2]$

  Se $X_i, i = 1, \ldots, n$ são mutuamente independentes, então

$$V[X_1 + X_2 + \cdots + X_n] = V[X_1] + V[X_2] + \cdots + V[X_n]$$

- **Desigualdade de Cheybyshev**:

$$p(|X(s) - E[X]| \geq r) \leq V[X]/r^2$$

  onde r é um número real positivo.

4.3 Cadeias de Markov

Uma **cadeia de Markov** em tempo discreto (DTMC) é um caso particular de **processo estocástico** com estados discretos (o parâmetro, em geral o tempo, pode ser discreto ou contínuo) com a propriedade de que a *distribuição de probabilidade do próximo estado depende apenas do estado atual e não na sequência de eventos que precederam* – propriedade Markoviana

Memória Markoviana diz-nos que os estados anteriores são irrelevantes para a predição dos estados seguintes, desde que o estado atual seja conhecido.

Cadeias de Markov têm enumeras aplicações como modelos estatísticos de processos do mundo real[6].

Definição 15:

Uma **cadeia de Markov** é uma sequência $X_0, X_1, X_2, X_3, \ldots$ de variáveis aleatórias.
O conjunto de valores que elas podem assumir, é chamado de **espaço de estados**, onde X_n denota o estado do processo no instante de tempo n.
Se a distribuição de probabilidade condicional de X_{n+1} nos estados passados é uma função apenas de X_n, então:

$$\Pr(X_{n+1} = x | X_0, X_1, X_2, \ldots, X_n) = \Pr(X_{n+1} = x | X_n)$$

onde x é algum estado do processo. Esta é a propriedade de Markov.

As cadeias de Markov são frequentemente descritas por uma **sequência de grafos orientados**, onde as arestas do gráfico n são rotulados por as probabilidades de ir de um estado no instante de tempo n para

[6] Ver por exemplo `https://www.google.com/patents/US6285999?hl=pt-PT`

outros estados no tempo $n+1$:

$$\Pr(X_{n+1} = x \mid X_n = x_n).$$

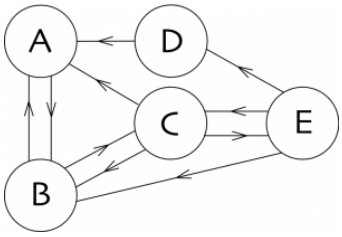
A **matriz de transição**, $T = (t_{ij})$ de uma cadeia de Markov no instante de tempo n para o tempo $n+1$ é uma matriz $m \times m$ cujas entradas são a probabilidade de o sistema se mover do estado i para o estado j, com $i, j = 1, \ldots, m$ e m é o número de estados do sistema:

$$t_{ij} = \Pr(X_{n+1} = j \mid X_n = i).$$

Temos que $0 \leq t_{ij} \leq 1$ e a soma das entradas de cada coluna da matriz de transição tem de ser igual a 1.

Exemplo 22:

Adaptado de `http://blog.kleinproject.org/?p=280`. Considere rede constituída por 5 páginas web A, B, C, D, E com os links mostrados na imagem abaixo:



Em cada instante, a probabilidade de começando numa página qualquer terminar numa oura página é dada pela matriz:

$$T = \begin{bmatrix} 0 & 1/2 & 1/3 & 1 & 0 \\ 1 & 0 & 1/3 & 0 & 1/3 \\ 0 & 1/2 & 0 & 0 & 1/3 \\ 0 & 0 & 0 & 0 & 1/3 \\ 0 & 0 & 1/3 & 0 & 0 \end{bmatrix}$$

Uma pessoa que esteja na página A neste instante, estará em B no instante seguinte, enquanto que se estiver em B neste momento tem 50% de probabilidade de no instante seguinte estar na página A.
A probabilidade após dois passos vai ser dada por T^2. Determine esta matriz e interprete.
Consideremos que uma pessoa no instante inicial está na página A, considere $X_0 = [1\ 0\ 0\ 0\ 0]^\top$. No instante seguinte a probabilidade da pessoa estar numa página é dada por TX_0, e passados dois instantes é T^2X_0. Ou seja, é ceeto que no instante 1 esteja em B e tem 50% de probabilidade de estar em C (ou em A) no instante 2.

```
-->T = [0   1/2   1/3  1  0
-->1  0  1/3  0 1/3
-->0   1/2  0  0  1/3
```

```
-->0  0  0  0  1/3
-->0  0  1/3  0  0 ]
 T  =

    0.    0.5    0.3333333    1.    0.
    1.    0.     0.3333333    0.    0.3333333
    0.    0.5    0.           0.    0.3333333
    0.    0.     0.           0.    0.3333333
    0.    0.     0.3333333    0.    0.
    -->X0=[1 0 0 0 0]'
 X0  =

    1.
    0.
    0.
    0.
    0.

-->X1=T*X0
 X1  =

    0.
    1.
    0.
    0.
    0.
-->X2=T^2*X0
 X2  =

    0.5
    0.
    0.5
    0.
    0.
```

Bibliografia

[1] J. L. Gersting. *Mathematical Structures for Computer Science: A Modern Approach to Discrete Mathematics*. W.H. Freeman & Company, 6th edition edition, 2007.

[2] H. Liebeman. *Introduction to Operations Research*. McGraw-Hill, 8th edition edition, 2007.

[3] S. Lipschutz and M. Lipson. *Matemática Discreta*. Bookman, 3.ª edição edition, 2013.

[4] K.H. Rosen. *Discrete Mathematics and Its Applications*. McGraw-Hill, 7th edition edition, 2012.