publicação do departamento de matemática
da universidade do minho

publicado pelo departamento de matemática
da universidade do minho
campus de gualtar, 4710-054
braga, portugal

primeira edição, Fevereiro 2009

ISBN 978-972-8810-15-3

número dezassete

matemática discreta

paula marques smith
paula mendes martins

"Do not worry about your difficulties in mathematics.
I assure you that mine are greater."
Albert Einstein

O plano curricular do 1º Ciclo de Matemática e do 1º Ciclo de Ciências de Computação da Universidade do Minho prevê que a unidade curricular (uc) Matemática Discreta seja leccionada no 2º semestre, com uma escolaridade semanal de duas horas teóricas e três horas teórico-práticas. O programa desta unidade curricular contempla um estudo introdutório da Teoria de Grafos e da Teoria de Números. O objectivo da unidade curricular Matemática Discreta é familiarizar os alunos com conceitos e resultados básicos da Teoria de Grafos e da Teoria de Números. Mais concretamente, esperamos que com o aproveitamento em Matemática Discreta os alunos

- apliquem o Algoritmo de Euclides para o cálculo do m.d.c. de dois inteiros
- resolvam equações diofantinas
- apliquem critérios de primalidade
- identifiquem números congruentes módulo n e propriedades desta relação
- resolvam congruências lineares e sistemas de congruências lineares
- identifiquem e caracterizem classes de grafos.

Para além destes objectivos específicos de aprendizagem, a unidade curricular Matemática Discreta tem também objectivos gerais, igualmente importantes na formação do aluno:

- Ajudar o aluno a raciocinar com correcção e segurança;
- Desenvolver capacidades de apresentação dos seus raciocínios de forma organizada e clara;

- Levar o aluno a compreender a importância do rigor no estudo das matérias;
- Fomentar o trabalho individual e em grupo;
- Estimular o espírito crítico do aluno.

O presente livro é um texto de apoio à unidade curricular Matemática Discreta e tem assim o objectivo de ser uma apresentação simples, mas cuidada, de conceitos e resultados básicos da Teoria de Grafos e da Teoria de Números. Ao longo do texto são apresentados bastantes exemplos que deverão ser verificados e explorados pelo aluno. As demonstrações deverão ser encaradas como parte fundamental da aprendizagem: é importante que o aluno as entenda não com o objectivo de as reproduzir posteriormente mas antes com a finalidade de adquirir experiência e destreza na construção de provas. Dentro de cada capítulo, as secções terminam com exercícios. Incitamos os alunos a resolvê-los: não se aprende matemática sem resolver problemas! Os de índole mais prática e de resolução de certo modo mecanizada desenvolverão no aluno técnicas básicas e ajudá-lo-ão a perceber e a interiorizar os conceitos. Exercícios de natureza mais teórica, para além do desafio que constituem, são um contributo essencial na aprendizagem da construção de argumentos e na organização dos mesmos.

Os conceitos e os resultados teóricos estarão sempre, neste e noutros livros semelhantes, à disposição do aluno. A nossa esperança é que, acompanhado pelo empenho do aluno no processo de aprendizagem, este trabalho consiga ajudá-lo a resolver algumas das suas dificuldades em matemática.

Paula Marques Smith
Paula Mendes Martins
Fevereiro de 2009

Conteúdo

1. introdução à teoria de grafos

"As the island of knowledge grows, the surface
that makes contact with mystery expands."
W. Mark Richardson

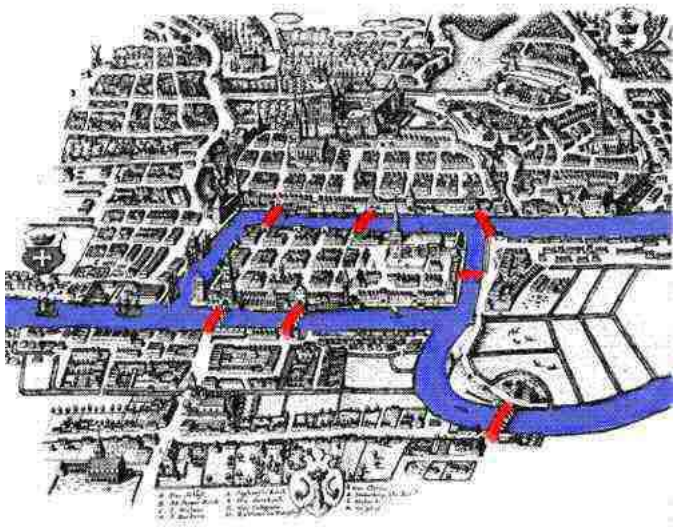
Um grafo é uma colecção de vértices (também chamados nós) e de arestas, cada uma das quais liga dois nós. Para visualizar um grafo, podemos pensar nos nós como pontos do espaço, do plano ou de qualquer outra superfície e representar as arestas por linhas ligando os nós. Esta representação não é única. A única característica importante de um grafo é a incidência de nós e arestas. Todos os elementos de um grafo podem sofrer continuamente deslocações ou deformações, continuando, no entanto e sempre, a representar o mesmo grafo, i.e., a mesma colecção de nós e de arestas.

1.1 alguns problemas históricos

Frequentemente, a resolução de um problema concreto, numa qualquer área do conhecimento, é encontrada recorrendo à teoria de grafos. Como veremos nos quatro problemas que de seguida se enunciam, o procedimento para obter uma solução do problema é o seguinte: começamos por construir um grafo que seja um modelo matemático do problema. Recorrendo à Teoria de Grafos resolvemos, de seguida, o problema teórico e abstracto do grafo que construímos e, finalmente, interpretamos, nos termos do problema real, a solução encontrada.

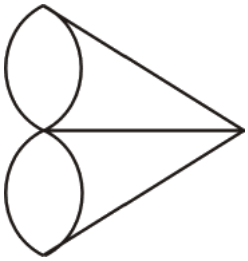
Nesta secção do curso, apresentamos quatro problemas históricos e construímos os grafos que os modelam. A resolução dos problemas será discutida nas secções seguintes.

As sete pontes de Königsberg. A cidade de Königsberg (hoje Kaliningrad na Rússia) é atravessada pelo rio Pregel e tinha, no século XVIII, duas ilhas ligadas entre si e às duas margens do rio por sete pontes.



Conta a história que os habitantes da cidade caminhavam tradicionalmente ao domingo pela cidade, tentando encontrar um caminho que permitisse passear pela cidade atravessando todas as pontes uma só vez. Tendo tido dificuldade em encontrar tal caminho, apresentaram, numa carta, o problema ao matemático suíço Leonard Euler (1707-1783). Em 1736, Euler provou que o caminho pretendido não existia!

A técnica de Euler para resolver o problema consistiu basicamente em considerar o mapa de Königsberg e "transformá-lo"naquilo a que hoje chamamos um grafo, no qual as margens do rio e as ilhas são consideradas os vértices do grafo, estando estes ligados por arestas do mesmo modo que as margens e as ilhas estavam ligadas pelas pontes. O grafo de Euler tinha o seguinte aspecto:



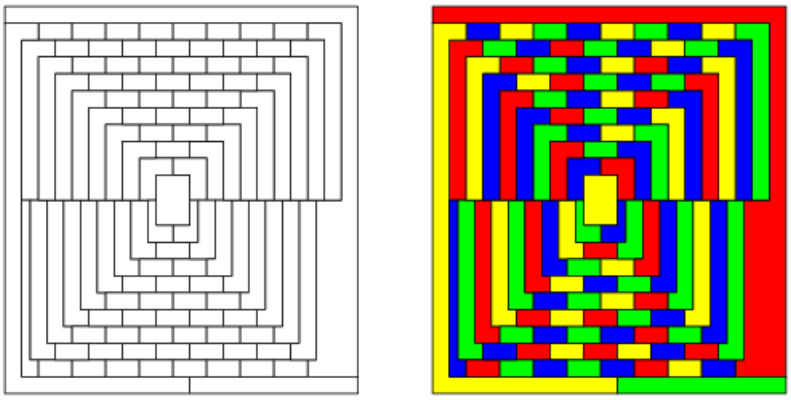
O problema das quatro cores. Este famoso teorema é particularmente interessante porque é um exemplo de um problema em matemática que é extremamente fácil de expor

mas também extremamente difícil de resolver.

O resultado foi conjecturado inicialmente em 1852 quando Francis Guthrie, ao tentar colorir o mapa das províncias de Inglaterra de acordo com aquela regra, reparou que apenas necessitava de quatro cores diferentes. Nessa altura, Fredrick Guthrie, seu irmão e aluno de Augustus De Morgan, colocou a questão a este último, que entretanto, escreveu a Arthur Cayley, a expor o problema. Foi Cayley quem publicou pela primeira vez o problema, atribuindo os créditos a De Morgan.

Assistiu-se desde então a várias tentativas de provar o resultado. Uma "demonstração" foi apresentada por Alfred Kempe in 1879. No entanto, Percy Heawood provou, em 1890, que a "demonstração" de Kempe estava incorrecta. Mais ainda, Heawood provou que todos os grafos planares podíam ser coloridos com pelo menos cinco cores.

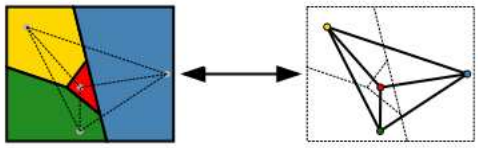
Em 1 de Abril de 1975, Martin Gardner elaborou um mapa de 110 regiões, afirmando serem precisas exactamente 5 cores para o colorir.



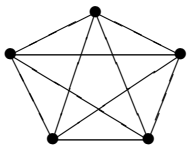
Confrontado posteriormente com a coloração desse mesmo mapa com apenas 4 cores, Gardner respondeu que aquele mapa era apenas uma brincadeira própria do dia em que foi apresentado.

Foi já em 1976 que surgiu a primeira demonstração do resultado. No entanto, esta demonstração era computacional e não matemática. Appel e Haken, usando a informática, estudaram 1476 casos distintos de regiões e provaram que qualquer outro mapa se reduz a um daqueles. Em 1994, simplificando a demonstração de Appel e Haken, Seymour, Robertson, Sanders e Thomas reduziram o número de mapas distintos de 1476 para 633.

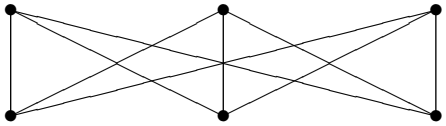
A resolução do problema passa por construir um grafo a partir do mapa dado, criando um vértice para cada país do mapa e ligando dois vértices por arestas sempre que os países que esses vértices representam partilham uma fronteira.



O problema do rei com cinco filhos. Este problema foi apresentado pelo matemático alemão August F. Möbius (1790-1868) por volta do ano de 1840 e consiste no seguinte: Havia um rei que tinha cinco filhos. No seu testamento determinou que, após a sua morte, os filhos dividiriam o seu reino em cinco províncias de tal modo que cada província fizesse fronteira com cada uma das restantes. O rei determinou ainda que os filhos ligassem as capitais de cada província por estradas, de tal modo que duas quaisquer dessas estradas não se intersectassem. O problema que se coloca é o de saber se é possível cumprir as determinações do rei! Tal como nos problemas anteriores, começamos por construir um grafo que traduza o problema enunciado: os vértices do grafo correspondem às capitais das cinco províncias e as arestas às estradas que as ligam. Traduzido em termos de grafos, o primeiro desejo do rei consiste em desenhar um grafo com cinco vértices, no qual dois quaisquer vértices são adjacentes. Ainda em termos de grafos, a segunda vontade do rei prende-se com o problema de construir aquele grafo de tal modo que ele seja planar (i.e., de tal modo que duas quaisquer arestas não se cruzam no plano). Prova-se que a construção de um tal grafo não é possível. Assim, a segunda vontade do rei não pode ser cumprida!



O problema das três casas. A origem deste problema não é conhecida mas sabe-se que foi pela primeira vez referido em 1913 pelo matemático Henry Ernest Dudeney (1857-1930). O problema envolve a ligação de cada uma de três casas às redes de água, de electricidade e de gás, sem que qualquer uma das ligações se cruze. O grafo que modela este problema designa-se por $K_{3,3}$ e é o seguinte:

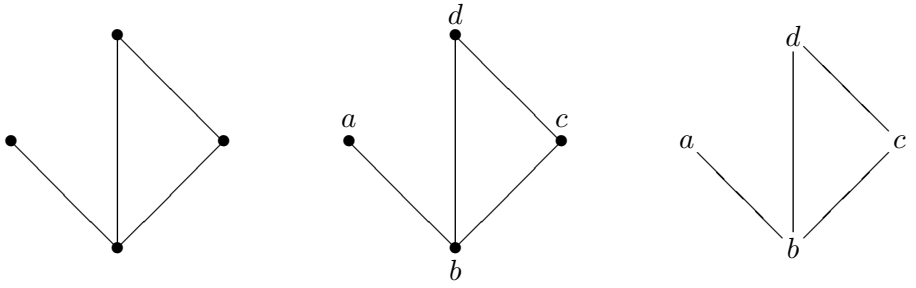


Os vértices do grafo correspondem às três casas e às três redes de abastecimento e as arestas às ligações entre as casas e as redes. Do ponto de vista dos grafos, o problema consiste em saber se o grafo $K_{3,3}$ é planar. Tal como no problema anterior, prova-se que tal grafo não é planar pelo que as ligações pretendidas não se podem efectuar!

A resolução dos dois últimos problemas revelou-se fundamental na caracterização dos grafos planares, estabelecida pelo matemático polaco Kazimierz Kuratowski (1896-1980) em 1930.

1.2 conceitos básicos

Um *grafo* é uma representação de um conjunto de pontos e do modo como eles estão ligados. Aos pontos de um grafo chamamos *vértices* e às ligações (que representamos por linhas) chamamos *arestas*. Essa representação pode ser feita de várias formas. De seguida apresentamos 3 formas diferentes de representação de um mesmo grafo.

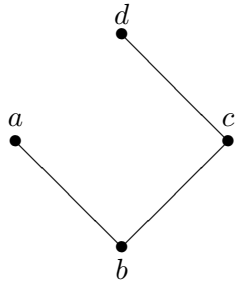


Podemos considerar vários tipos de grafos, de acordo com o número de arestas que ligam dois vértices e/ou a existência de uma orientação de arestas. Em alguns casos é possível os conceitos serem formalizados através da Teoria de Conjuntos. É o caso dos conceitos de grafo simples e de digrafo.

Definição 1.1 *Um* grafo simples *é um par ordenado $G = (V, E)$ no qual V é um conjunto não vazio e E é um conjunto de subconjuntos de V com exactamente dois elementos. Aos elementos de V chamamos* vértices *e aos elementos de E chamamos* arestas.

O conjunto dos vértices não tem que ser necessariamente finito. Podem considerar-se grafos com um conjunto numerável de vértices. No nosso curso estudaremos apenas grafos com um número finito de vértices.

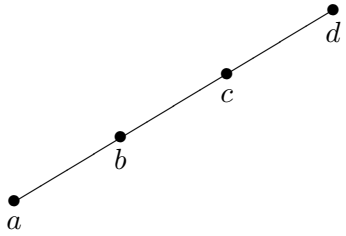
Exemplo 1.1 *O grafo*



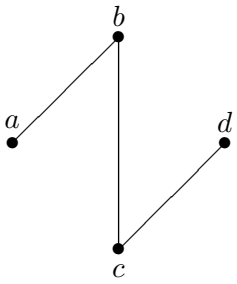
é simples. De facto, $V = \{a, b, c, d\}$ *e* $E = \{\{a, b\}, \{b, c\}, \{c, d\}\}$.

Tendo em conta a definição, dois grafos $G = (V, E)$ e $G' = (V', E')$ são iguais se $V = V'$ e $E = E'$.

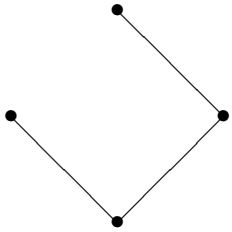
Observações: 1 - Existem representações "aparentemente"diferentes de um mesmo grafo. Numa representação de um grafo, o importante é o número de vértices, o número de arestas e o modo como estas se dispõem em relação àqueles. Por exemplo, o grafo do Exemplo 1.1 pode ser representado por



ou



2 - Uma mesma representação pode descrever grafos que, por definição, são distintos. Por exemplo, a descrição



tanto pode representar o grafo $G_1 = (V_1, E_1)$, onde

$$V_1 = \{a, b, c, d\} \; e \; E_1 = \{\{a, b\}, \{b, c\}, \{c, d\}\},$$

como o grafo $G_2 = (V_2, E_2)$, onde

$$V_2 = \{1, 2, 3, 4\} \; e \; E_2 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}.$$

Vamos "abusar da linguagem"e afirmar que G_1 e G_2 são o mesmo grafo. Neste curso, não distinguiremos grafos que diferem apenas na natureza dos seus vértices.

Um digrafo não é mais do que um grafo simples no qual consideramos a orientação das arestas. Assim,

Definição 1.2 *Chama-se* digrafo *a um par $G = (V, E)$ onde V é um conjunto não vazio e $E \subseteq V \times V$. Aos elementos de V chamamos* vértices *e aos elementos de E,* arestas.

Da definição de digrafo resultam algumas observações pertinentes:

1 - Por definição, as arestas de um digrafo são um par ordenado. Assim, dados dois vértices distintos a e b, as arestas (a, b) e (b, a) são distintas.

2 - Para cada vértice a, o par (a, a) é uma aresta.

Na representação de um digrafo, uma aresta (a, b) é representada por uma linha orientada. Em particular, para cada vértice a, a aresta (a, a) é representada por um lacete orientado.

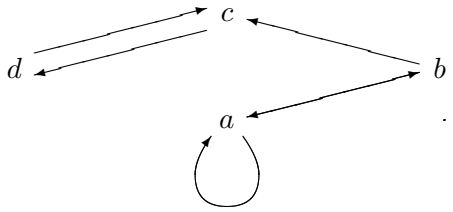
Exemplo 1.2 *O digrafo $G = (V, E)$, onde*

$$V = \{a, b, c, d\}$$

e

$$E = \{(a, a), (a, b), (b, a), (b, c), (c, d), (d, c)\},$$

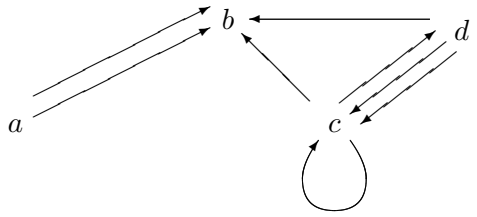
pode ser representado por



Um *multigrafo* (respectivamente, *multidigrafo*) é um grafo no qual se admite a existência de múltiplas arestas (respectivamente, arestas orientadas) entre dois vértices .

No caso de um multigrafo (respectivamente, multidigrafo) não faz sentido representar as arestas à custa dos vértices, pois há ambiguidade, uma vez que dois vértices podem estar ligados por mais do que uma aresta (respectivamente, mais do que duas arestas orientadas).

Exemplo 1.3 *O grafo*



é um multidigrafo com 4 vértices.

Neste curso estudaremos sobretudo os grafos simples. Não havendo ambiguidade e se nada for dito em contrário, referirmo-nos-emos aos grafos simples apenas como *grafos*.

1.2.1 incidência e adjacência

Seja $G = (V, E)$ um grafo com n vértices e m arestas ($n \in \mathbb{N}$ e $m \in \mathbb{N}_0$). Para melhor facilitar a escrita, consideremos $V = \{v_i : 1 \leq i \leq n\}$ e $E = \{e_j : 1 \leq j \leq m\}$.

Definição 1.3 *Diz-se que $e_j \in E$ é* incidente *a $v_i \in V$ se existe $v_k \in V$ tal que aresta e_j liga os vértices v_i e v_k.*

Definição 1.4 *Uma matriz $[a_{ij}] \in \mathcal{M}_{n\times m}(\mathbb{Z})$ diz-se uma* matriz de incidência *de G se*

$$a_{i\,j} = \begin{cases} 0 & \text{se } e_j \text{ não é incidente a } v_i \\ 1 & \text{se } e_j \text{ é incidente a } v_i \end{cases} .$$

Exemplo 1.4 *Seja $G = (V, E)$ o grafo onde $V = \{a, b, c, d\}$ e $E = \{\{a, b\}, \{b, c\}, \{c, d\}\}$. Considerando $v_1 = a$, $v_2 = b$, $v_3 = c$, $v_4 = d$, $e_1 = \{a, b\}$, $e_2 = \{b, c\}$ e $e_3 = \{c, d\}$, obtemos a matriz de incidência*

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Observemos que temos 4 linhas, pois existem 4 vértices, e 3 colunas, correspondentes às 3 arestas.

Definição 1.5 *Dois vértices v_i e v_j de G dizem-se* adjacentes *se existe uma aresta em G incidente a ambos.*

Definição 1.6 *Diz-se que uma matriz $[a_{ij}] \in \mathcal{M}_{n\times n}(\mathbb{Z}\}$ é uma* matriz de adjacência *de G se*

$$a_{ij} = \begin{cases} 0 & \text{se } v_i \text{ e } v_j \text{ não são adjacentes} \\ 1 & \text{se } v_i \text{ e } v_j \text{ são adjacentes} \end{cases}.$$

Exemplo 1.5 *A matriz*

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

é uma matriz de adjacência do grafo do exemplo anterior. Observemos que esta matriz, sendo de adjacência, é uma matriz quadrada. Como estamos perante um grafo simples, a matriz é simétrica e a diagonal é preenchida por zeros.

Dado um grafo, a construção de uma matriz de incidência (ou de adjacência) depende da ordem pela qual se consideram os vértices e as arestas. Assim, o mesmo grafo admite várias matrizes de incidência e de adjacência. No entanto, duas quaisquer matrizes de incidência (ou de adjacência) de um mesmo grafo são semelhantes, pois uma obtém-se da outra por troca de linhas e/ou colunas.

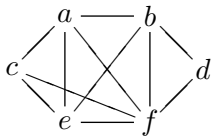
1.2.2 caminhos

Grande parte da Teoria de Grafos envolve sequências especiais de vértices. Nesta secção, apresentamos as mais relevantes.

Definição 1.7 *Um* caminho *de um grafo G é uma sequência de vértices de G no qual dois vértices sucessivos definem uma aresta. Representa-se um caminho por $\langle v_1, v_2, \ldots, v_n \rangle$, onde $v_1, v_2, ..., v_n$ são vértices de G. Ao primeiro vértice da sequência chamamos* origem do caminho *ou* vértice inicial *e ao último vértice, chamamos* destino do caminho *ou* vértice final.

Por convenção, chama-se caminho trivial *à sequência $\langle a \rangle$, onde $a \in V$.*

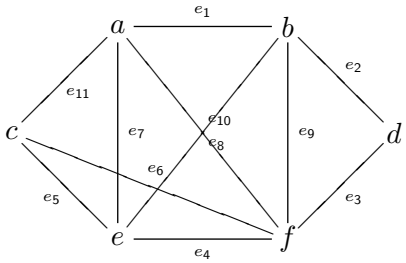
Exemplo 1.6 *No grafo*



$\langle a, b, d, f, c, e, f, b \rangle$ é um caminho de a a b.

Observação. Um caminho pode ser também definido como uma sequência de arestas na qual quaisquer duas arestas sucessivas têm um vértice em comum.

Exemplo 1.7 *No grafo*



o caminho $\langle a, b, d, f, c, e, f, b \rangle$ pode também ser representado por $\langle e_1, e_2, e_3, e_6, e_5, e_4, e_9 \rangle$.

Definição 1.8 *Chama-se* comprimento *de um caminho ao número de arestas que definem esse caminho.*

Exemplo 1.8 *O caminho apresentado no Exemplo 1.6 tem comprimento 7.*

Definição 1.9 *Chama-se* caminho elementar *a um caminho onde nenhum vértice é repetido.*

Exemplo 1.9 *O caminho apresentado no Exemplo 1.6 não é elementar. No mesmo grafo, o caminho* $\langle a, f, d, b\rangle$ *é um caminho elementar.*

Definição 1.10 *Um* caminho simples *ou* atalho *é um caminho sem arestas repetidas.*

Exemplo 1.10 *O caminho apresentado no Exemplo 1.6 é um atalho. Neste grafo, o caminho* $\langle a, b, d, f, c, e, f, c, e, b\rangle$ *não é um atalho.*

Definição 1.11 *Um* circuito *é um caminho no qual o vértice inicial coincide com o vértice final.*

Exemplo 1.11 *No grafo do Exemplo 1.6, o caminho* $\langle f, c, e, f\rangle$ *é um circuito.*

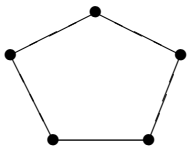
Definição 1.12 *Um* circuito simples *é um caminho que é, simultaneamente, circuito e atalho.*

Definição 1.13 *Um* ciclo *é um circuito simples, não trivial, onde não há repetição de vértices com a excepção dos vértices inicial e final.*

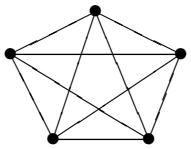
1.2.3 subgrafos

Definição 1.14 *Um subgrafo de um grafo* $G = (V, E)$ *é um grafo* $G' = (V', E')$ *onde* $V' \subseteq V$ *e* $E' \subseteq E$.

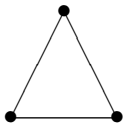
Exemplo 1.12 *O grafo*



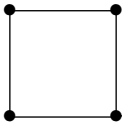
é subgrafo do grafo



Exemplo 1.13 *O grafo*



não é subgrafo do grafo



Exemplo 1.14 *Seja $G = (V, E)$ onde*

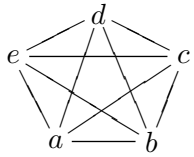
$$V = \{a, b, c, d\} \text{ e } E = \{\{a, b\}, \{b, d\}, \{c, d\}, \{b, c\}, \{a, c\}\}.$$

O par (V', E') onde $V' = \{a, c\}$ e $E' = \{\{a, c\}, \{b, d\}\}$ não é um subgrafo de G.

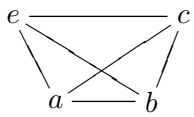
Definição 1.15 *Sejam $G = (V, E)$ um grafo e $V' \subseteq V$. Chama-se* subgrafo de G induzido por V' *ao grafo $G' = (V', E')$ onde*

$$E' = \left\{\{v_i, v_j\} \in E : v_i, v_j \in V'\right\}.$$

Exemplo 1.15 *Dado o grafo*



o subgrafo induzido por $\{a, b, c, e\}$ é



1.2.4 alguns grafos especiais

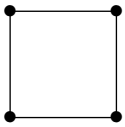
Nesta secção apresentamos alguns grafos que, por terem características próprias, merecem destaque especial.

Definição 1.16 *Um* grafo trivial *é um grafo $G = (V, E)$ onde $\#V = 1$ e $\#E = 0$.*

Definição 1.17 *Um* grafo nulo *é um grafo $G = (V, E)$ onde $\#E = 0$.*

Definição 1.18 *Seja $n \geq 3$. Um grafo com n vértices e n arestas diz-se um* grafo ciclo de comprimento n *se as n arestas definirem um ciclo. Um grafo ciclo de comprimento n representa-se por C_n.*

Exemplo 1.16 *O grafo C_4 pode ser representado por*

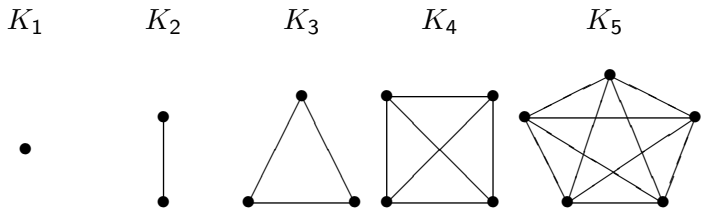


Definição 1.19 *Seja $n \geq 1$. Um grafo com $n+1$ vértices e n arestas diz-se um* grafo linha de comprimento n *se dois dos vértices são adjacentes a um e um só vértice e todos os outros são adjacentes a dois e só dois vértices. O grafo linha de comprimento n representa-se por P_n.*

Exemplo 1.17 *O grafo linha de comprimento 4, P_4 pode ser representado por*

Definição 1.20 *Um* grafo completo *é um grafo no qual dois quaisquer vértices são adjacentes. Um grafo completo com n vértices representa-se por K_n.*

Exemplo 1.18 *Para $n = 1, 2, 3, 4, 5$, os grafos completos são:*



Um raciocínio indutivo mostra que o grafo completo K_n tem $\binom{n}{2}$ arestas.

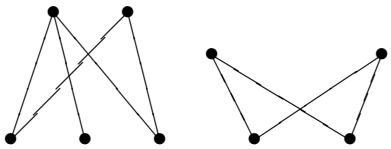
A proposição seguinte caracteriza os subgrafos de um grafo completo que são por si grafos completos.

Proposição 1.1 *Sejam $m, n \in \mathbb{N}$. Então K_m é subgrafo de K_n se e só se $m \leq n$.*

Demonstração: Trivial. □

Definição 1.21 *Um grafo $G = (V, E)$ diz-se* grafo bipartido *se existir uma partição $\{X, Y\}$ de V de tal modo que cada vértice de X é adjacente apenas a vértices de Y e cada vértice de Y é adjacente apenas a vértices de X.*

Exemplo 1.19 *Os dois grafos seguintes são bipartidos*



O seguinte resultado é uma caracterização importante dos grafos bipartidos.

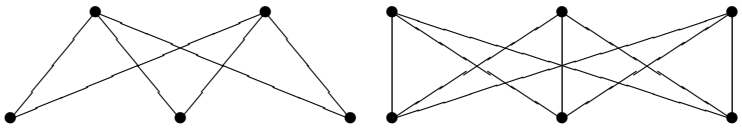
Proposição 1.2 *Um grafo G é bipartido se e só se não admite ciclos de comprimentos ímpar.*

Demonstração: Sejam $G = (V, E)$ e $\{X, Y\}$ uma partição de V de tal modo que cada vértice de X é adjacente apenas a vértices de Y e cada vértice de Y é adjacente apenas a vértices de X. Seja $C = \langle v_1, v_2, \ldots, v_n, v_1 \rangle$ um ciclo de G. Se $v_1 \in X$, então, $v_2 \in Y$, $v_3 \in X$, ..., $v_{2k+1} \in X$, $v_{2k} \in Y$, ... Como $v_n \in Y$, concluímos que n é par. Logo, o comprimento de C é par.

Reciprocamente, se $G = (V, E)$ apenas tem ciclos de comprimento par, definimos a partição $\{X, Y\}$ estabelecendo que vértices adjacentes pertencem a classes de partição diferentes. □

Definição 1.22 *Um* grafo bipartido completo *é um grafo bipartido $G = (V, E)$ tal que, para a partição $\{X, Y\}$ de V da definição, cada vértice de X é adjacente a todos os vértices de Y (e, portanto, cada vértice de Y é adjacente a todos os vértices de X). Representa-se um grafo bipartido completo por $K_{m,n}$ onde $\#X = m$ e $\#Y = n$ com $m \leq n$.*

Exemplo 1.20 *Os grafos $K_{2,3}$ e $K_{3,3}$ são representados, respectivamente, por*



Facilmente se conclui que, dados $m, n \in \mathbb{N}$ com $m \leq n$, o grafo bipartido completo $K_{m,n}$ tem mn arestas.

Proposição 1.3 *Sejam $m, n, p, q \in \mathbb{N}$ tais que $m \leq n$ e $p \leq q$. Então $K_{m,n}$ é subgrafo de $K_{p,q}$ se e só se $m \leq p$ e $n \leq q$.*

Demonstração: Trivial. □

1.2.5 grau de um vértice

Definição 1.23 *Sejam $G = (V, E)$ um grafo e $v \in V$. Chama-se* grau *(ou* valência*) de v, e representa-se por grau(v), ao número de arestas incidentes a v.*

Exemplo 1.21 *No grafo completo K_6 todos os vértices têm grau 5.*

Exemplo 1.22 *No grafo bipartido completo $K_{2,3}$ existem dois vértices com grau 3 e três vértices com grau 2.*

Observações. 1. O grau de um vértice pode ser obtido da matriz de incidência somando todas as entradas referentes à linha correspondente a esse vértice.

2. O grau de um vértice pode também ser obtido da matriz de adjacência somando todas as entradas referentes à linha (ou à coluna) correspondente a esse vértice.

O próximo resultado é fundamental para todo o estudo que faremos nas próximas secções.

Teorema 1.1 *Num grafo $G = (V, E)$ a soma dos graus de todos os vértices é o dobro do número de arestas.*

Demonstração: (Por indução sobre o número de arestas)

Seja $P(n)$ a afirmação:

A soma dos graus de todos os vértices de um grafo com n arestas é $2n$.

Passo 1. Suponhamos que o grafo não tem arestas. Então, cada vértice tem grau 0 e, portanto, a soma dos graus é $0 = 2 \cdot 0$. Então, $P(0)$ verifica-se.

Passo 2. Seja $k \in \mathbb{N}_0$. Suponhamos que a afirmação $P(k)$ é verdadeira. Queremos provar que $P(k+1)$ é verdadeira.

Seja $G = (V, E)$ um grafo com $k+1$ arestas. Consideremos G' um subgrafo de G com os mesmos vértices de G mas com menos uma aresta, digamos, $\{a, b\}$ (com $a, b \in V$). Então, G' tem k arestas e, portanto, por hipótese de indução, a soma dos graus de todos os vértices de G' é $2k$. Para obter G de G' "juntamos"a aresta $\{a, b\}$. Assim, o grau de a é aumentado em 1 e o grau de b é aumentado em 1. Logo, a soma dos graus de todos os vértices de G é $2k + 1 + 1 = 2(k+1)$.

Tendo em conta os passos 1 e 2 e o Princípio de Indução Natural, provamos que $P(n)$ é verdadeira para todo $n \in \mathbb{N}_0$. □

Este Teorema também é conhecido pelo *Teorema do aperto de mãos*. De facto, se um grupo de pessoas derem apertos de mão, o número de mãos apertadas é o dobro do número de apertos.

Corolário 1.1 *Em qualquer grafo, o número de vértices de grau ímpar é par.*

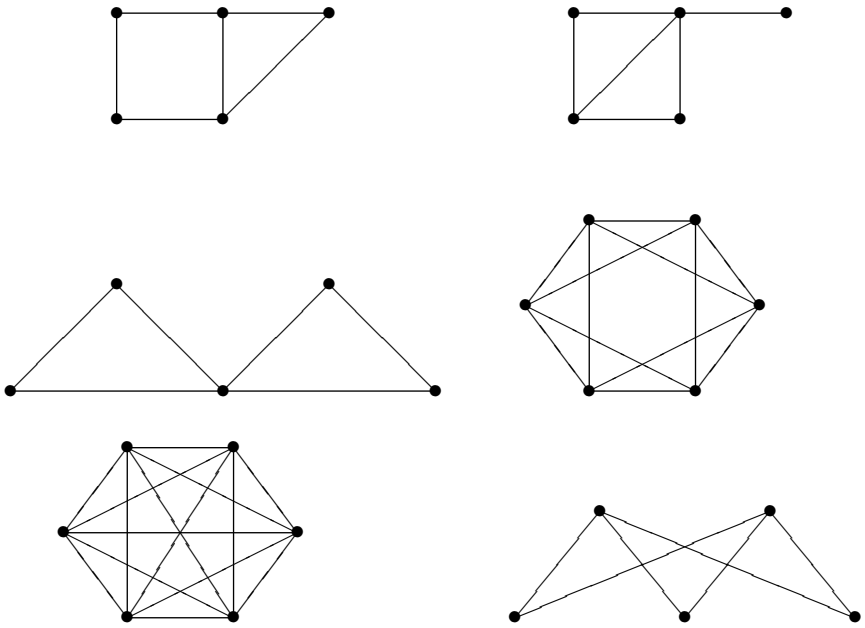
Demonstração: Trivial, tendo em conta que, se $G = (V, E)$ é um grafo com n arestas,

$$\sum_{grau(v)\ \acute{i}mpar} grau(v) \ + \sum_{grau(v)\ par} grau(v) = \sum_{v \in V} grau(v) = 2n.$$

□

1.2.6 Exercícios

Exercício 1.2.1. Escreva uma descrição formal de cada um dos seguintes grafos:



Exercício 1.2.2. Determine as matrizes de incidência e de adjacência de cada um dos grafos apresentados no exercício anterior.

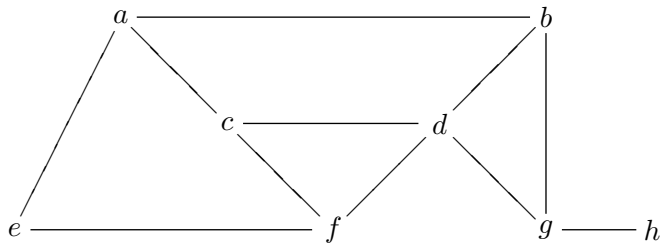
Exercício 1.2.3. Desenhe um grafo que tenha como matriz de adjacência a matriz

$$(a)\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}; \qquad (b)\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

Exercício 1.2.4. Desenhe um grafo que tenha como matriz de incidência a matriz

$$(a)\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}; \qquad (b)\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Exercício 1.2.5. Considere o seguinte grafo G.



(a) Indique um caminho de a a h que não seja simples.

(b) Indique um caminho simples de a a h que não seja elementar.

(c) Indique um caminho elementar de a a h.

(d) Indique um circuito de G que não seja ciclo.

(e) Indique um ciclo de G de comprimento 7.

(f) Verifique se os seguintes grafos são subgrafos de G:

(i) $G_1 = (\{a, b, e, f\}, \{\{a, b\}, \{a, e\}, \{a, f\}, \{e, f\}\})$.

(ii) $G_2 = (\{a, b, d, g, h\}, \{\{a, b\}, \{a, d\}, \{b, g\}, \{d, g\}, \{g, h\}\})$.

(iii) $G_3 = (\{a, c, d, e, f\}, \{\{a, c\}, \{a, e\}, \{c, d\}, \{e, f\}\})$.

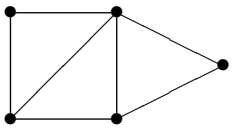
(g) Determine o subgrafo de G induzido por cada um dos subconjuntos de vértices seguintes:

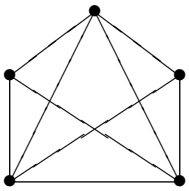
(i) $\{a, b, c, d, e\}$;

(ii) $\{b, c, e, f, g\}$;

(iii) $\{b, c, e\}$.

Exercício 1.2.6. Seja $G = (V, E)$ um grafo. Um *subgrafo de vértice eliminado* é um subgrafo $G' = (V', E')$ induzido de G onde $V' = V \backslash \{v\}$, para algum $v \in V$. Represente os subgrafos de vértice eliminado de:

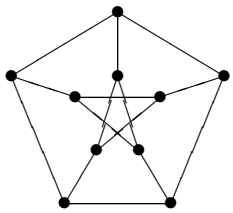
(a) 

(b) 

(c) K_5;

(d) $K_{2,3}$.

Exercício 1.2.7. Considere o grafo de Petersen aqui representado.



Determine:

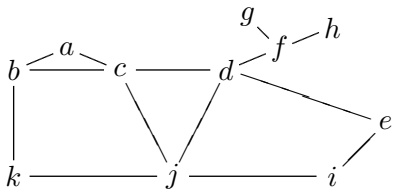
(a) um caminho simples de comprimento 5;

(b) um caminho elementar de comprimento 9;

(c) ciclos de comprimento 5, 6, 8 e 9.

Exercício 1.2.8. Sejam $G = (V, E)$ um grafo e a e b dois vértices distintos em V. Mostre que se existe um caminho entre a e b então existe um caminho elementar entre a e b.

Exercício 1.2.9. (a) Considere o grafo



(i) Determine dois caminhos elementares distintos de f a k.

(ii) Determine um ciclo com vértices usados na alínea anterior.

(b) Seja $G = (V, E)$ um grafo e $x, y \in V$. Mostre que, se existem dois caminhos elementares distintos entre x e y, então, G admite um ciclo.

Exercício 1.2.10. Sejam $G = (V, E)$ um grafo e $u, v \in V$. Seja $d(u, v)$ definido por: Se $u = v$ então $d(u, v) = 0$; se $u \neq v$ e existe um caminho entre u e v, então, $d(u, v)$ é o menor dos comprimentos dos caminhos elementares de u a v; caso contrário, $d(u, v) = \infty$. A $d(x, y)$ chama-se *distância entre* u *e* v.

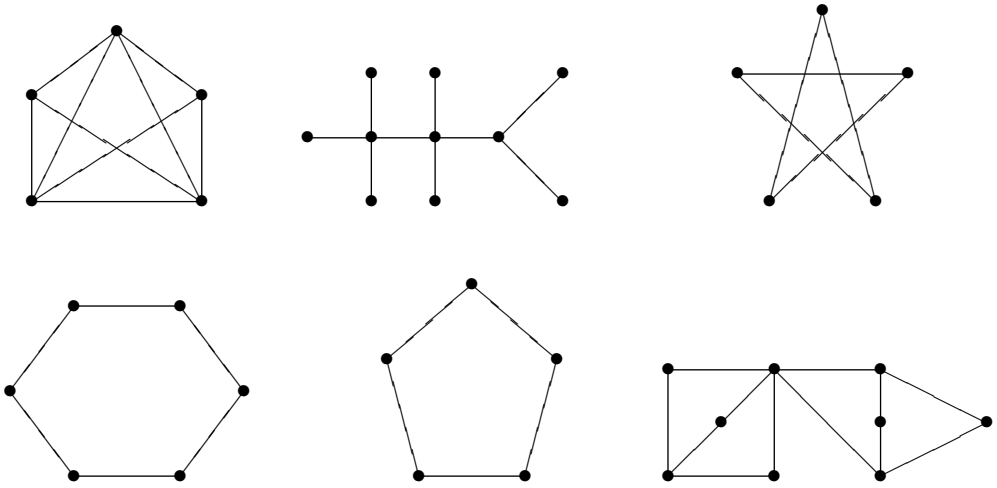
Determine a distância entre dois quaisquer vértices do grafo:

(a) K_5;

(b) $K_{2,3}$;

(c) de Petersen.

Exercício 1.2.11. Dos seguintes grafos, diga quais são bipartidos, indicando uma partição do conjunto dos seus vértices.



Exercício 1.2.12. Seja $G = (V, E)$ o grafo onde $V = \{a, b, c, d, e, f, g, h, i, j\}$ e

$$E = \{\{a, b\}, \{b, c\}, \{b, d\}, \{b, e\}, \{b, j\}, \{c, g\}, \{d, g\},$$
$$\{f, d\}, \{f, e\}, \{h, b\}, \{h, f\}, \{i, a\}, \{i, h\}\}.$$

(a) Represente o grafo G.

(b) Mostre que G é bipartido, indicando uma partição do conjunto dos seus vértices.

Exercício 1.2.13. Dê exemplo, caso exista, de:

(a) um grafo sem vértices de grau ímpar;

(b) um grafo sem vértices de grau par;

(c) um grafo com exactamente um vértice de grau ímpar;

(d) um grafo com exactamente um vértice de grau par;

(e) um grafo com exactamente dois vértices de grau ímpar;

(f) um grafo com exactamente dois vértices de grau par.

Exercício 1.2.14. Prove o Teorema da Amizade: "Em toda a cidade com pelo menos 2 habitantes, residem 2 pessoas com o mesmo número de amigos que habitam nessa mesma cidade".

Exercício 1.2.15. Qual o número mínimo de vértices de um grafo simples com 200 arestas? Porquê?

Exercício 1.2.16. A *sequência gradual* de um grafo é a sequência dos graus dos seus vértices, ordenados do maior ao menor. Por exemplo, a sequência gradual do grafo completo K_4 é $3, 3, 3, 3$ e a sequência gradual do grafo $K_{2,3}$ é $3, 3, 2, 2, 2$. Para cada uma das sequências de números, indique as que são sequência gradual de algum grafo. Neste caso, represente o grafo em questão.

(a) 4,4,4,4;

(b) 3,3,3,2,1;

(c) 1,1,1,1,1,1;

(d) 5,4,4,3,2,2;

(e) 4,3,3,2,2,1;

(f) 4,4,3,3,3,3,3,3,2,2.

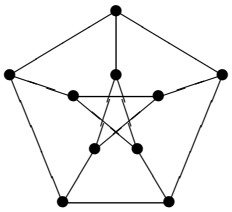
Exercício 1.2.17. Liste todas as sequências graduais de um grafo com 4 vértices.

1.3 grafos conexos

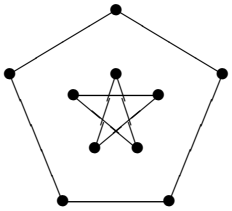
Definição 1.24 *Um* grafo conexo *é um grafo $G = (V, E)$ no qual existe um caminho entre dois quaisquer dos seus vértices.*

Definição 1.25 *Um* grafo desconexo *é um grafo que não é conexo.*

Exemplo 1.23 *O grafo*



é um grafo conexo. O grafo



é um grafo desconexo.

Dado um grafo qualquer, podemos definir uma relação binária no conjunto dos seus vértices. Dizemos que dois vértices distintos estão em relação se e só se existir um caminho entre eles. Esta simples relação binária revela-se bastante importante no estudo dos grafos conexos.

Teorema 1.2 *Seja $G = (V, E)$ um grafo. A relação R definida por, para todos $x, y \in V$,*

$$x \; R \; y \iff x = y \text{ ou existe um caminho de } x \text{ para } y,$$

é uma relação de equivalência em V.

Demonstração: Exercício. □

A relação R, como relação de equivalência que é, determina em V uma partição em classes de equivalência. Para cada $v \in V$, o subgrafo de G induzido pela classe de equivalência de v, determinada por R, é um grafo conexo. Por esta razão, as classes de equivalência determinadas por R designam-se por *componentes conexas de* G.

Do teorema anterior resulta de imediato a seguinte caracterização de grafo conexo.

Corolário 1.2 *Um grafo $G = (V, E)$ é conexo se e só se a relação R definida em V admite uma única classe de equivalência.* □

O próximo resultado permite-nos obter subgrafos de grafos conexos que são, por si, grafos conexos.

Teorema 1.3 *Sejam $G = (V, E)$ um grafo conexo e $a, b, x_1, x_2, ..., x_n \in V$ tais que $\langle a, b, x_1, x_2, ..., x_n, a\rangle$ é um ciclo em G. Então, $G' = (V, E \setminus \{\{a, b\}\})$ é um grafo conexo.*

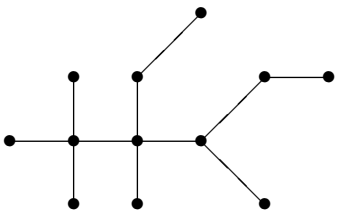
Demonstração: Trivial, tendo em conta que $\langle a, x_n, ..., x_2, x_1, b\rangle$ é um caminho de a a b em G'. □

1.3.1 árvores

Nesta subsecção, apresentamos uma classe de grafos conexos - a classe das árvores.

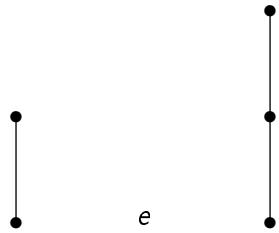
Definição 1.26 *Uma* árvore *é um grafo conexo no qual não existem ciclos.*

Exemplo 1.24 *O grafo*



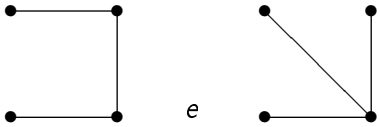
é uma árvore.

Exemplo 1.25 *Os grafos*



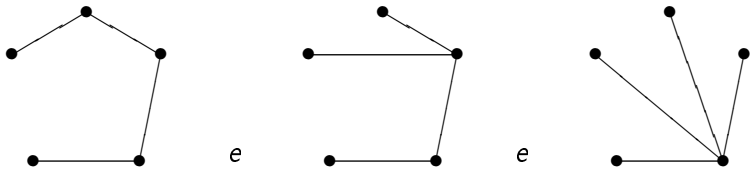
são as únicas árvores com, respectivamente, dois e três vértices.

Exemplo 1.26 *Os grafos*



são as únicas árvores com quatro vértices.

Exemplo 1.27 *Os grafos*



são as únicas árvores com cinco vértices.

Teorema 1.4 *Numa árvore, a diferença entre o número de vértices e o número de arestas é 1.*

Demonstração: Exercício (utilizando o Princípio de Indução Forte). □

Teorema 1.5 *Toda a árvore não trivial tem pelo menos dois vértices de grau 1.*

Demonstração: Seja $G = (V, E)$ uma árvore. Por um lado, se G tem v vértices e a arestas, pelo teorema anterior,

$$a = v - 1.$$

Por outro lado, sabemos que

$$\sum_{v_i \in V} grau(v_i) = 2(v-1) = 2v - 2.$$

Se todos os vértices tiverem grau no mínimo 2, temos que

$$\sum_{v_i \in V} grau(v_i) \geq 2v,$$

e, então, ter-se-ía $2v - 2 \geq 2v$, um absurdo. Logo, pelo menos um vértice tem de ter grau 1. Se houvesse só um vértice nestas condições, teríamos

$$\sum_{v_i \in V} grau(v_i) \geq 2(v-1) + 1 = 2v - 1$$

e, portanto, seria $2v - 2 \geq 2v - 1$, um absurdo. Logo, existem pelo menos dois vértices de grau 1. □

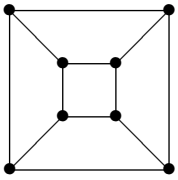
1.3.2 Exercícios

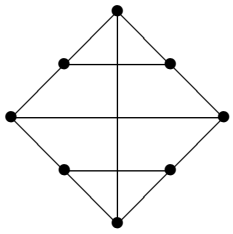
Exercício 1.3.1. Demonstre o Teorema 1.2.

Exercício 1.3.2. Um *conjunto de desconexão* de um grafo conexo G é um conjunto de arestas cuja remoção dá origem a um grafo desconexo.

(a) Encontre conjuntos de desconexão para o grafo de Petersen com 3, 4 e 5 arestas.

(b) Encontre conjuntos de desconexão com o menor número possível de arestas para os grafos seguintes:





Exercício 1.3.3. Construa todas as árvores possíveis com 6 vértices.

Exercício 1.3.4. (a) Demonstre o Teorema 1.4.
(Sugestão: Use o princípio de indução forte sobre o número de arestas.)

(b) Uma *floresta* é um conjunto de árvores. Mostre que se G é uma floresta com c árvores, v vértices e a arestas, então, $a = v - c$.

Exercício 1.3.5. (a) Mostre que um grafo conexo com v vértices tem pelo menos $v - 1$ arestas.

(b) Mostre que um grafo conexo com v vértices e exactamente $v - 1$ arestas é uma árvore.

Exercício 1.3.6. Mostre que qualquer árvore com pelo menos dois vértices é um grafo bipartido. Quais as árvores que são grafos bipartidos completos?

Exercício 1.3.7. O *complemento* de um grafo $G = (V, E)$ é um grafo $\overline{G} = (\overline{V}, \overline{E})$, onde

$$\overline{V} = V \quad \text{e} \quad \overline{E} = \{\{x, y\} \subseteq V : x \neq y,\ \{x, y\} \notin E\}.$$

(a) Determine o complemento de $K_{3,5}$.

(b) Determine $\overline{G}$, onde G é um grafo desconexo com duas componentes conexas que são os grafos K_3 e K_5.

(c) Dado o grafo ciclo C_5, mostre que $\overline{C_5}$ e C_5 são o mesmo grafo.

(d) Considere o grafo linha P_3. Mostre que $\overline{P_3}$ e P_3 são o mesmo grafo.

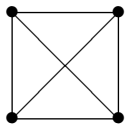
(e) Diga, justificando, se a seguinte afirmação é verdadeira ou falsa: "*O complemento de um grafo conexo é um grafo conexo*".

1.4 grafos planares

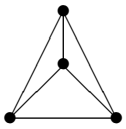
Definição 1.27 *Um* grafo planar *é um grafo que pode ser representado no plano sem se verificarem cruzamentos de arestas, a não ser, eventualmente, nalgum dos vértices que as definem.*

Chamamos a atenção para o facto de, dado um grafo planar, existirem diferentes representações suas no plano sem cruzamentos de arestas. A cada uma destas representações chamamos *representação planar* do grafo planar.

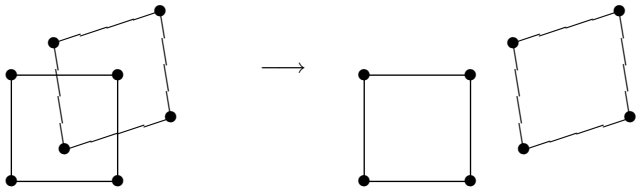
Exemplo 1.28 *O grafo*



é planar pois pode ser representado por

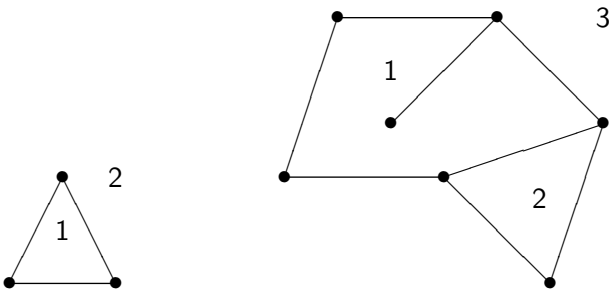


Torna-se importante aqui observar que, quando um grafo é desconexo, podemos reduzir a questão da planaridade a cada uma das componentes conexa do grafo.



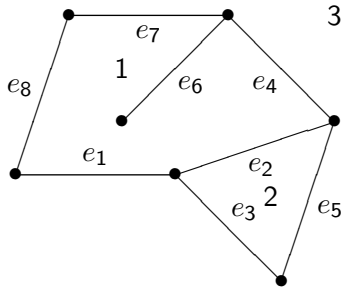
Assim, nesta secção iremos concentrar-nos nos grafos conexos.

Uma representação planar de um grafo planar conexo define no plano regiões, às quais chamamos *faces*. Começamos por observar que, dado um grafo planar, uma sua representação planar define sempre uma região ilimitada, a qual designamos por *face exterior* do grafo.



Numa face limitada por arestas, identificamos um ciclo que a circunda, ao qual chamamos *fronteira da face*. Há arestas que não estão nas fronteiras das faces, mas estão nas faces. São as chamadas *arestas de corte*. Se retirarmos uma aresta à fronteira de uma face, diminuímos o número de faces do grafo em 1.

Exemplo 1.29 *No grafo planar*



a aresta e_6 *é uma aresta de corte da face* 1. *As arestas* e_2, e_3 *e* e_5 *formam a fronteira da face* 2.

1.4.1 fórmula de Euler

Em 1752, Euler estabeleceu o seguinte resultado fundamental na Teoria de Grafos.

Teorema 1.6 *Para um grafo planar conexo com* v *vértices,* a *arestas e* f *faces, tem-se*

$$v - a + f = 2.$$

Demonstração: (Por indução sobre o número de arestas)

1º passo. Se um grafo conexo tem 0 arestas, então, tem 1 vértice e 1 face. Logo,

$$v - a + f = 1 - 0 + 1 = 2.$$

2º passo. Seja $n \in \mathbb{N}_0$. Suponhamos que para qualquer grafo com n arestas, v vértices e f faces, se tem

$$v - n + f = 2.$$

Seja $G = (V, E)$ um grafo com $n + 1$ arestas, v vértices e f faces. Queremos provar que

$$v - (n + 1) + f = 2.$$

Temos dois casos a considerar:

1º caso: G tem um vértice de grau 1. Seja $v_1 \in V$ esse vértice. Então existe uma única aresta incidente a v_1. Seja $\{v_1, v_2\}$ essa aresta. Então, o grafo $G' = (V', E')$, onde $V' = V \backslash \{v_1\}$ e $E' = E \backslash \{\{v_1, v_2\}\}$, é um grafo conexo com menos um vértice (tem $v - 1$ vértices), menos uma aresta (tem n arestas) mas o mesmo número de faces (tem f faces) que G. Aplicando a hipótese de indução a G' obtemos

$$(v - 1) - n + f = 2,$$

i.e.,

$$v - (n + 1) + f = 2.$$

2º caso: G não tem vértices de grau 1. Então, G não é uma árvore e, portanto, tem pelo menos um ciclo.

Consideremos o grafo $G'' = (V'', E'')$, onde $V'' = V$ e $E'' = E \backslash \{\{v_1, v_2\}\}$ e $\{v_1, v_2\}$ é uma aresta de um ciclo. Então, G'' é um grafo conexo com o mesmo número de vértices (tem v vértices), com menos uma aresta (tem n arestas) e menos uma face (tem $f - 1$ faces) que o grafo G. Aplicando a hipótese de indução, temos que

$$v - n + (f - 1) = 2,$$

i.e.,

$$v - (n + 1) + f = 2.$$

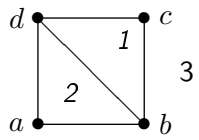
□

1.4.2 a não planaridade de K_5 e $K_{3,3}$

Para provar que os grafos K_5 e $K_{3,3}$ não são planares, necessitamos de conceitos e lemas que apresentamos de seguida.

Definição 1.28 *Seja $G = (V, E)$ um grafo planar. Diz-se que uma face é* incidente *a uma aresta se esta aresta "toca"essa face.*

Exemplo 1.30 *No grafo*



a face 2 é incidente à aresta $\{a, b\}$*, mas não é incidente a* $\{c, d\}$*.*

Lema 1.1 *Seja* G *um grafo conexo, planar com* a *arestas e* f *faces (*$f \geq 2$*). Então,* $f \leq \frac{2}{3}a$*.*

Demonstração: Para cada face, contemos o número de arestas às quais essa face é incidente. Somemos todos esses números. Seja S essa soma.

Por um lado, como para cada aresta existem, no máximo, duas faces às quais a aresta é incidente, temos que

$$S \leq 2a.$$

Por outro lado, como cada face é incidente, no mínimo, a três arestas, temos que

$$3f \leq S.$$

Logo, $3f \leq 2a$, ou seja, $f \leq \frac{2}{3}a$. □

Lema 1.2 *Seja* G *um grafo planar conexo com pelo menos duas faces. Se* G *tem* a *arestas e* v *vértices, então,* $3v - a \geq 6$*.*

Demonstração: Pela fórmula de Euler, temos que

$$v - a + f = 2.$$

Aplicando o lema anterior, temos que

$$v - a + \frac{2}{3}a \geq 2,$$

i.e.,

$$3v - 3a + 2a \geq 6$$

e, portanto,

$$3v - a \geq 6.$$

□

Teorema 1.7 *O grafo K_5 não é planar.*

Demonstração: O grafo K_5 tem 5 vértices e 10 arestas. Se K_5 fosse planar, uma sua representação planar teria, pelo menos, duas faces (existem ciclos em K_5). Aplicando o lema anterior, concluiríamos que

$$5 = 3 \cdot 5 - 10 \geq 6,$$

o que é um absurdo. O absurdo resulta de termos suposto que K_5 é planar. Logo, K_5 não é planar. □

O que acontece com $K_{3,3}$? Será $K_{3,3}$ um grafo planar?

Sabemos que $K_{3,3}$ tem 6 vértices e 9 arestas, pelo que $K_{3,3}$ satisfaz a desigualdade do Lema 1.2 ($3 \cdot 6 - 9 = 9 \geq 6$). Assim, nada podemos concluir sobre a planaridade de $K_{3,3}$ a partir deste resultado. Temos de procurar outro método para verificar se $K_{3,3}$ é ou não planar.

Percorrendo a demonstração do Lema 1.1, tendo em conta que num grafo bipartido completo cada ciclo tem, no mínimo, 4 arestas, podemos substituir a expressão $3f \leq S$ por $4f \leq S$, obtendo assim, o seguinte lema.

Lema 1.3 *Seja G um grafo bipartido completo, planar com a arestas e f faces ($f \geq 2$). Então, $f \leq \frac{1}{2}a$.* □

Agora, percorrendo a demonstração do Lema 1.2, usando o Lema 1.3 (e não o Lema 1.1), provamos que:

Lema 1.4 *Seja G um grafo bipartido completo planar com pelo menos duas faces. Se G tem a arestas e v vértices, então, $2v - a \geq 4$.* □

Estamos agora em condições de provar que o grafo $K_{3,3}$ não é planar.

Teorema 1.8 *O grafo $K_{3,3}$ não é planar.*

Demonstração: O grafo bipartido completo $K_{3,3}$ tem 6 vértices e 9 arestas. Se $K_{3,3}$ fosse planar, teria pelo menos duas faces (pois tem um ciclo de comprimento 4) e, pelo Lema 1.4, teríamos

$$3 = 2 \cdot 6 - 9 \geq 4,$$

o que é um absurdo. O absurdo resulta de termos suposto que $K_{3,3}$ é planar. Assim, $K_{3,3}$ não é planar. □

Observemos que os Teoremas 1.7 e 1.8 mostram que dois dos problemas apresentados na secção 1.1 (o do rei com 5 filhos e o das 3 casas) não têm solução. O Teorema 1.8 garante ainda que o Lema 1.2 não é uma caracterização dos grafos planares conexos, já que o grafo $K_{3,3}$ não satisfaz o seu recíproco.

Tendo em conta que, obviamente, qualquer subgrafo de um grafo planar é ainda um grafo planar, terminamos esta secção com a caracterização dos grafos completos e grafos bipartidos completos planares, ambos consequência das considerações feitas anteriormente.

Teorema 1.9 *Seja $n \in \mathbb{N}$. O grafo completo K_n é planar se e só se $n < 5$.* □

Teorema 1.10 *Sejam $m, n \in \mathbb{N}$. O grafo bipartido completo $K_{m,n}$ é planar se e só se $m < 3$.* □

1.4.3 Teorema de Kuratowski

Acabámos de ver que grafos que tenham como subgrafo K_5 ou $K_{3,3}$ não são planares. No entanto, existem grafos que não admitem aqueles dois grafos como subgrafos. Serão esses grafos planares ou não? Para dar resposta a esta pergunta introduzimos o conceito de grafos homeomorfos.

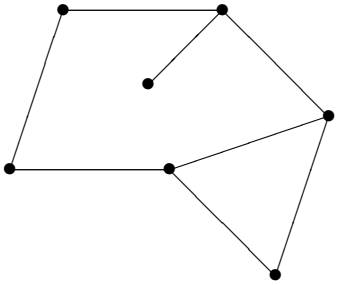
Definição 1.29 *Sejam $G = (V, E)$ um grafo e $a, b \in V$ tal que $\{a, b\} \in E$. Diz-se que $G' = (V', E')$ é um grafo obtido de G por* adição de um vértice de grau 2 *se*

$$V' = V \cup \{x\}$$

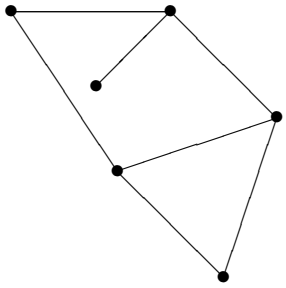
e

$$E' = E \setminus \{\{a, b\}\} \bigcup \{\{a, x\}, \{x, b\}\}.$$

Exemplo 1.31 *O grafo*



é um grafo obtido do grafo



por adição de um vértice de grau 2.

Existe também o processo recíproco para obtenção de um novo grafo.

Definição 1.30 *Sejam* $G = (V, E)$ *um grafo e* $a, b, x \in V$ *tais que grau*$(x) = 2$, $\{a, x\}, \{b, x\} \in E$ *mas* $\{a, b\} \notin E$. *Diz-se que* $G' = (V', E')$ *é um grafo obtido de* G *por* remoção de um vértice de grau 2 *se*

$$V' = V \backslash \{x\}$$

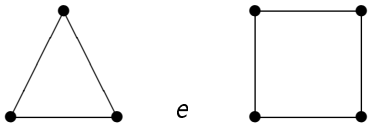
e

$$E' = E \backslash \{\{a, x\}, \{x, b\}\} \bigcup \{\{a, b\}\}.$$

As duas definições anteriores são fundamentais para a definição seguinte.

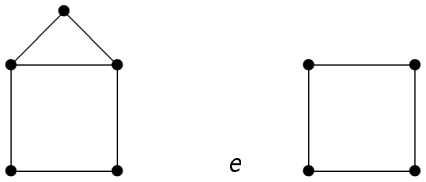
Definição 1.31 *Dois grafos dizem-se* homeomorfos *se um deles puder ser obtido do outro por adição ou remoção de vértices de grau 2.*

Exemplo 1.32 *Os grafos*



são homeomorfos.

Exemplo 1.33 *Os grafos*



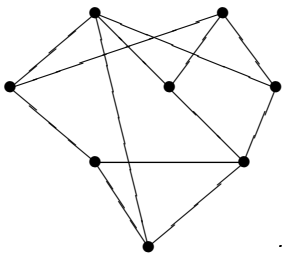
não são homeomorfos.

É claro que dois grafos homeomorfos ou são ambos planares ou são ambos não planares. Assim, tendo em conta os Teoremas 1.7 e 1.8, vimos que a não existência de subgrafos homeomorfos a K_5 ou a $K_{3,3}$ é condição necessária para um grafo ser planar. O Teorema de Kuratowski estabelece que esta condição é também suficiente, caracterizando, deste modo, os grafos planares.

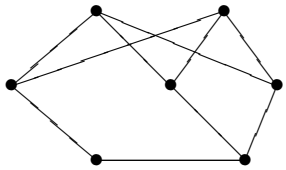
Omitiremos a demonstração da condição necessária por ela envolver conceitos topológicos.

Teorema 1.11 ***(de Kuratowski)*** *Um grafo é planar se e só se não contém um subgrafo homeomorfo a K_5 ou a $K_{3,3}$.* □

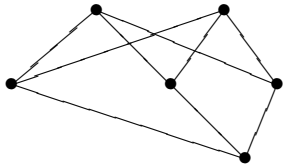
Exemplo 1.34 *Consideremos o grafo*



O grafo



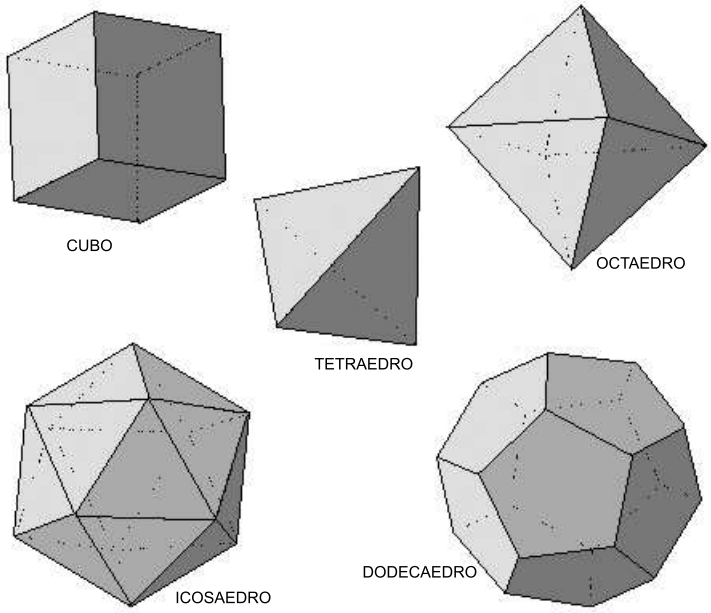
é um subgrafo do primeiro, homeomorfo ao grafo



que não é mais que o grafo bipartido completo $K_{3,3}$. *Assim, concluímos que o primeiro grafo do exemplo é não planar.*

1.4.4 grafos platónicos

Nesta secção estudaremos um caso particular de grafos planares - os grafos platónicos. Este nome deve-se ao facto de estarem relacionados com os cinco poliedros platónicos (ou regulares) celebrizados por Platão (428-347 a.C.) no diálogo *Timaeus*.



Definição 1.32 *Um* grafo platónico *é um grafo conexo, planar, no qual todos os vértices têm o mesmo grau e o número de arestas às quais cada face é incidente é constante.*

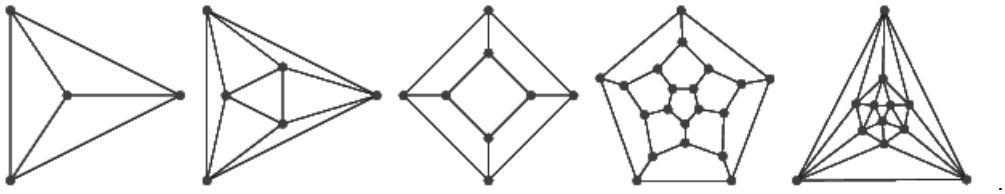
Exemplo 1.35 *O grafo trivial é um grafo platónico.*

Exemplo 1.36 *O grafo K_2 é um grafo platónico.*

Exemplo 1.37 *O grafo ciclo C_n com $n \geq 3$ (i.e., o grafo com n vértices de grau 2 e n arestas representado por uma linha poligonal com n lados) é um grafo platónico.*

O próximo resultado mostra-nos que, supondo que o grau de cada vértice é, no mínimo, 3, os únicos grafos platónicos que existem são os grafos resultantes de representações, em termos de grafos, dos 5 sólidos platónicos.

Teorema 1.12 *Seja $G = (V, E)$ um grafo platónico onde grau$(v) \geq 3$, para qualquer $v \in V$. Então, G é um dos seguintes grafos*



Demonstração: Sejam $G = (V, E)$ um grafo planar com v vértices, a arestas e f faces. Sejam $m, n \in \mathbb{N}$ tais que $m, n \geq 3$ são os números de arestas incidentes a cada um dos vértices e a cada uma das faces de G, respectivamente. Então,

$$mv = nf = 2a$$

e

$$v - a + f = 2,$$

ou seja,

$$v = \frac{2a}{m}, \qquad f = \frac{2a}{n}$$

e

$$\frac{2a}{m} - a + \frac{2a}{n} = 2.$$

Logo,

$$a\left(\frac{1}{m} + \frac{1}{n} - \frac{1}{2}\right) = 1.$$

Como $1 > 0$ e $a > 0$, concluímos que

$$\frac{1}{m} + \frac{1}{n} > \frac{1}{2}. \qquad (*)$$

Vejamos agora quais os valores possíveis para m e n:

- $m = 3$ e $n = 3$. (Corresponde ao primeiro grafo da figura.) Neste caso temos

$$\frac{1}{3} + \frac{1}{3} = \frac{2}{3} > \frac{1}{2}.$$

- $m = 3$ e $n = 4$. (Corresponde ao terceiro grafo da figura.) Neste caso temos

$$\frac{1}{3} + \frac{1}{4} = \frac{7}{12} > \frac{1}{2}.$$

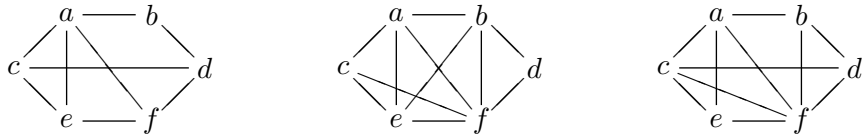
- $m = 3$ e $n = 5$. (Corresponde ao quarto grafo da figura.) Neste caso temos
$$\frac{1}{3} + \frac{1}{5} = \frac{8}{15} > \frac{1}{2}.$$
- $m = 3$ e $n \geq 6$. Aqui, temos
$$\frac{1}{3} + \frac{1}{n} \leq \frac{1}{3} + \frac{1}{6} = \frac{3}{6} = \frac{1}{2},$$
o que contradiz a desigualdade $(*)$.
- $m = 4$ e $n = 3$. (Corresponde ao segundo grafo da figura.) Neste caso temos
$$\frac{1}{4} + \frac{1}{3} = \frac{7}{12} > \frac{1}{2}.$$
- $m = 4$ e $n \geq 4$. Aqui, temos
$$\frac{1}{4} + \frac{1}{n} \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2},$$
o que contradiz a desigualdade $(*)$.
- $m = 5$ e $n = 3$. (Corresponde ao último grafo da figura.) Neste caso temos
$$\frac{1}{5} + \frac{1}{3} = \frac{8}{15} > \frac{1}{2}.$$
- $m = 5$ e $n \geq 4$. Aqui, temos
$$\frac{1}{5} + \frac{1}{n} \leq \frac{1}{5} + \frac{1}{4} = \frac{9}{20} < \frac{1}{2},$$
o que contradiz a desigualdade $(*)$.
- $m \geq 6$ e $n \geq 3$. Aqui, temos
$$\frac{1}{m} + \frac{1}{n} \leq \frac{1}{6} + \frac{1}{3} = \frac{1}{2},$$
o que contradiz a desigualdade $(*)$.

Como percorremos todos os casos possíveis, fica provado que os 5 grafos apresentados são os únicos grafos nas condições do enunciado. □

1.4.5 Exercícios

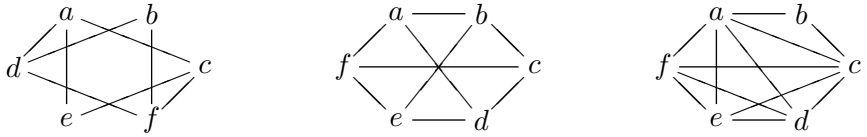
Exercício 1.4.1. Prove que qualquer árvore satisfaz a fórmula de Euler.

Exercício 1.4.2. Para cada um dos seguintes grafos planares encontre uma representação planar e indique o número de faces:



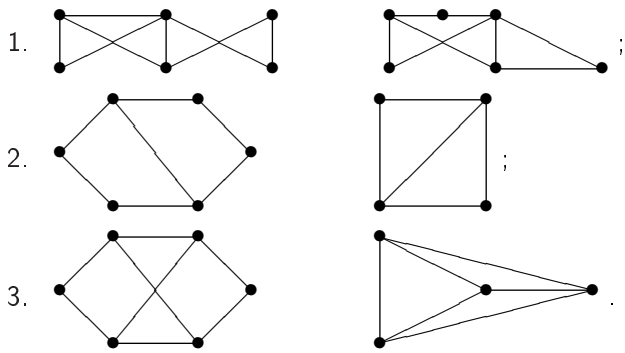
Exercício 1.4.3. Encontre uma representação planar de $K_{2,6}$.

Exercício 1.4.4. Para cada um dos grafos seguintes, encontre uma representação planar ou justifique porque é que não é possível ter tal representação:



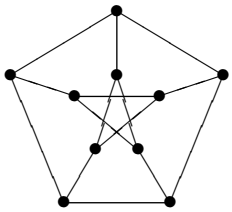
Exercício 1.4.5. Sejam $n \in \mathbb{N}$ e $G_n = (V, E)$ o grafo tal que $V = \{v_1, v_2, ..., v_n\}$ e $E = \{\{v_i, v_j\} \subseteq V : i \neq j \text{ e } m.d.c.(i, j) = 1\}$. Para que valores de n é G_n planar?

Exercício 1.4.6. Mostre que os seguintes pares de grafos são homeomorfos, fazendo a correcta modificação de vértices de grau 2:

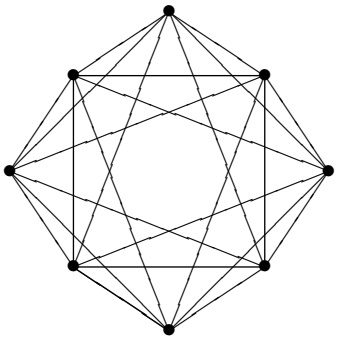


Exercício 1.4.7. Use o Teorema de Kuratowski para provar que os seguinte grafos não são planares:

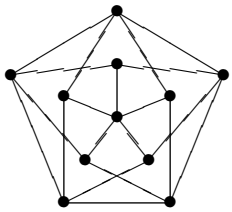
(a)



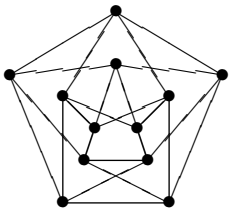
(b)



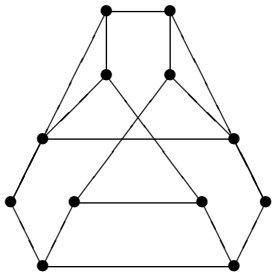
(c)



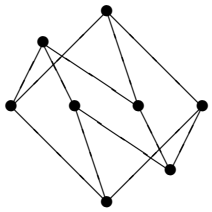
(d)

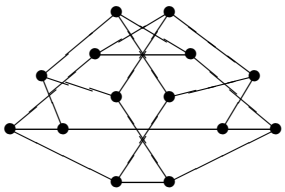


(e)

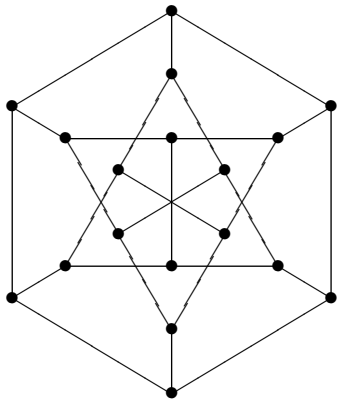


Exercício 1.4.8. Considere os dois seguintes grafos. Prove que o primeiro é planar e o segundo é não planar.





Exercício 1.4.9. Justifique que o grafo de Pappus, a seguir representado, não é planar.



Exercício 1.4.10. Construa um grafo G com 6 vértices, sendo dois deles de grau 4 e quatro de grau 3, tal que

(a) G seja planar;

(b) G não seja planar.

Exercício 1.4.11. Seja G um grafo conexo planar com pelo menos 3 vértices. Mostre que G tem pelo menos um vértice de grau não superior a 5.

1.5 grafos eulerianos e grafos hamiltonianos

1.5.1 grafos eulerianos

O estudo que faremos nesta secção permitir-nos-á responder à questão levantada a Euler sobre as pontes de Könisberg em 1736. Começamos com as seguintes definições.

Definição 1.33 *Seja $G = (V, E)$ um grafo. Um* caminho euleriano *é um caminho simples que contém todas as arestas do grafo.*

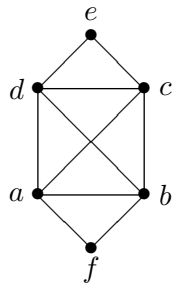
De notar que um caminho eureliano de um grafo conexo G contém, necessariamente, todos os vértices de G.

Definição 1.34 *Seja $G = (V, E)$ um grafo. Um* circuito euleriano *é um caminho euleriano onde o primeiro e último vértices coincidem.*

Definição 1.35 *Um grafo $G = (V, E)$ diz-se um* grafo euleriano *se existir um circuito euleriano em G.*

Definição 1.36 *Um grafo $G = (V, E)$ diz-se um* grafo semieuleriano *se existir, em G, um caminho euleriano que não é circuito.*

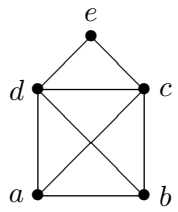
Exemplo 1.38 *O grafo*



é euleriano, pois nele podemos definir o circuito euleriano

$$\langle a, f, b, c, e, d, a, b, d, c, a \rangle.$$

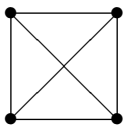
Exemplo 1.39 *O grafo*



é semieuleriano, pois nele podemos definir o caminho euleriano

$$\langle a, b, c, e, d, a, c, d, b \rangle.$$

Exemplo 1.40 *O grafo*



não é euleriano nem semieuleriano, pois não é possível definir, neste grafo, um circuito ou um caminho eulerianos.

O próximo lema é o primeiro passo para a caracterização dos grafos eurelianos e dos grafos semieulerianos.

Lema 1.5 *Seja G um grafo conexo onde todos os vértices têm grau par. Então qualquer caminho simples pode ser estendido a um circuito simples.*

Demonstração: Seja

$$C = \langle v_1, v_2, ..., v_{n-1}, v_n \rangle$$

um caminho simples em G. Temos duas situações:

- $v_1 = v_n$. Neste caso, o caminho simples é, ele próprio, um circuito simples.
- $v_1 \neq v_n$. Seja m o número de vezes que uma qualquer aresta do caminho é incidente a v_n. Então, m é um número ímpar. Como v_n tem grau par, existe pelo menos uma aresta incidente a v_n que não pertence ao caminho. Seja $\{v_n, v_{n+1}\}$ essa aresta. Então,

  $$C' = \langle v_1, v_2, ..., v_{n-1}, v_n, v_{n+1} \rangle$$

  é um caminho simples.

Aplicando agora o raciocínio anterior a C' e repetindo-o um número necessário de vezes, concluímos que existe $v_k \in V$ tal que $\langle v_1, v_2, ..., v_{n-1}, v_n, v_{n+1}, ..., v_k \rangle$ é um caminho simples e $v_1 = v_k$. □

Estamos então em condições de caracterizar os grafos eulerianos conexos.

Teorema 1.13 *Seja G um grafo conexo. Então, G é euleriano se e só se todos os seus vértices têm grau par.*

Demonstração: Seja $G = (V, E)$ um grafo conexo e euleriano. Sejam

$$C = \langle v_1, v_2, ..., v_n \rangle$$

um circuito euleriano em G (estamos a considerar, portanto, v_n=v_1) e x um dos vértices de G. Como G é conexo e o caminho C é euleriano, $x = v_i$ para algum $i \in \{1, 2, ..., n-1, n\}$. Vejamos que v_i tem grau par. Claramente, $\{v_{i-1}, v_i\}$ e $\{v_i, v_{i+1}\}$ são arestas de G. Se existir outra aresta incidente a v_i em C, existe $j \in \{1, 2, ..., n\}$ tal que $j \notin \{i-1, i, i+1\}$ e $v_i = v_j$. Então, $\{v_{j-1}, v_j\}$ e $\{v_j, v_{j+1}\}$ são arestas de C incidentes a v_i distintas das duas encontradas anteriormente. Repetindo o raciocínio até considerarmos todas as arestas incidentes a v_i, concluímos que v_i tem grau par.

Reciprocamente, suponhamos que $G = (V, E)$ é um grafo conexo onde todos os vértices têm grau par. Então existem circuitos simples em G. Seja

$$C = \langle v_1, v_2, ..., v_n, v_1 \rangle$$

um circuito simples com o comprimento máximo possível. Observamos que C tem todos os vértices de G. Se C não é euleriano, então, existe uma aresta que não se encontra em C. Seja $\{v_i, v_{n+1}\}$ essa aresta, para algum $i \in \{1, 2, .., n\}$. Então,

$$C' = \langle v_i, v_{i+1}, v_{i+2}, ..., v_n, v_1, ...v_{i-1}, v_i, v_{n+1} \rangle$$

é um caminho simples que, pelo lema anterior, se pode estender a um circuito simples com mais arestas que C, o que é contradiz o comprimento máximo de C. A contradição resulta de termos suposto que C não era euleriano. Logo, C é euleriano. □

Os grafos semieulerianos conexos caracterizam-se de modo semelhente.

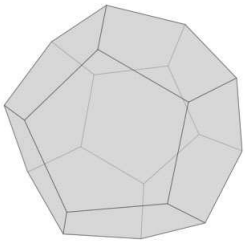
Teorema 1.14 *Um grafo conexo é semieuleriano se e só se existem exactamente dois vértices de grau ímpar.* □

Prova-se que os resultados apresentados são válidos para multigrafos. Em relação ao problema das pontes de Könisberg, tendo em conta os dois últimos teoremas, podemos concluir que o multigrafo que modela o problema não é euleriano, nem semieuleriano, já que cada um dos quatro vértices do multigrafo têm grau ímpar. A solução do problema é encontrar um caminho euleriano naquele multigrafo. Se tal caminho existisse, como o multigrafo não é semieuleriano, teria de ser um circuito euleriano, o que não pode acontecer por o multigrafo não ser euleriano. Assim, o passeio que os habitantes de Könisberg queriam fazer não é possível de realizar.

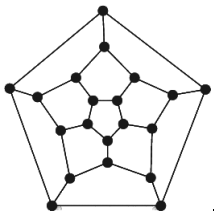
Terminamos observando que se G é um grafo semieuleriano, basta adicionarmos uma nova aresta (incidente aos dois vértices de grau ímpar) para obtermos um grafo euleriano com os mesmos vértices de G.

1.5.2 grafos hamiltonianos

Nesta subsecção estudamos uma classe particular de grafos - os grafos hamiltonianos. O nome *hamiltoniano* vem do matemático e físico irlandês William R. Hamilton (1805-1865), a quem se deve a introdução, em 1857, de um jogo, denominado "A viagem à volta do mundo", também conhecido como "O problema do caixeiro-viajante". Pensando em 20 cidades importantes da época, Hamilton considerou um dodecaedro, fez corresponder as referidas cidades aos 20 vértices do sólido e marcou cada um dos vértices com um alfinete.



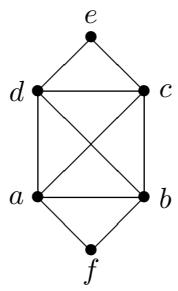
O objectivo do jogo era definir um percurso, ao longo das arestas do sólido, que passasse uma e uma só vez por cada cidade, começando e terminando na mesma cidade. Para não repetir cidades, o jogador usava um fio para construir o percurso. Como já vimos na secção anterior, o dodecaedro pode ser representado pelo grafo



Assim, em termos de grafos, o objectivo do jogo de Hamilton é construir um ciclo deste grafo que contenha todos os seus vértices.

Definição 1.37 *Seja $G = (V, E)$ um grafo. Chama-se* caminho hamiltoniano *a qualquer caminho elementar que passa por todos os vértices de G. Chama-se* ciclo hamiltoniano *a um ciclo que contém todos os vértices de G.*

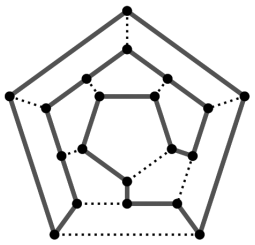
Exemplo 1.41 *No grafo*



o caminho $\langle a, f, b, d, c, e\rangle$ é hamiltoniano e o ciclo $\langle a, f, b, c, e, d, a\rangle$ é hamiltoniano.

Definição 1.38 *Um* grafo hamiltoniano *é um grafo que contém um ciclo hamiltoniano.*

Facilmente se verifica que o jogo de Hamilton tem pelo menos uma solução, que é a apresentada na figura seguinte.



Contrariamente ao que acontece nos grafos eulerianos, não foi ainda encontrada uma caracterização dos grafos hamiltonianos. No entanto, em alguns casos particulares é possível estabelecer uma tal caracterização:

- Um grafo completo K_n é hamiltoniano se e só se $n \geq 3$.
- Um grafo bipartido completo $K_{m,n}$ é hamiltoniano se e só se $n = m \geq 2$.

Existem algumas propriedades que os grafos hamiltonianos satisfazem, que podem ajudar a construir, ou a deduzir que é impossível construir, um ciclo hamiltoniano. De facto, se um grafo $G = (V, E)$ é hamiltoniano, temos que:

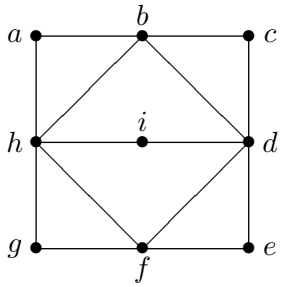
(i) Se um vértice $v \in V$ tem grau 2, então, as duas arestas incidentes a v fazem parte de qualquer ciclo hamiltoniano;

(ii) Na construção de um ciclo hamiltoniano, nenhum ciclo se pode formar até se percorrerem todos os vértices.

(iii) Se na construção de um ciclo hamiltoniano duas arestas incidentes num mesmo vértice têm de ser consideradas na construção do circuito, então, as restantes arestas incidentes a esse vértice não podem ser consideradas na construção do ciclo hamiltoniano.

Vejamos um exemplo em como podemos fazer uso destas propriedades:

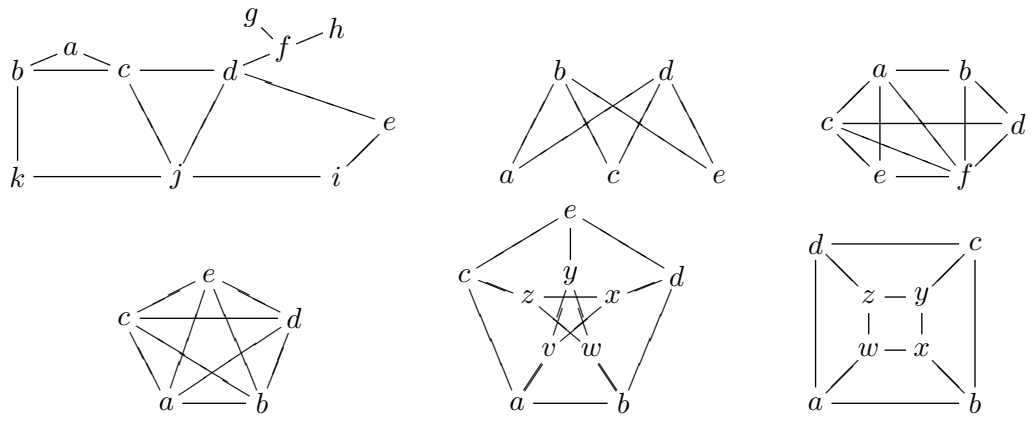
Exemplo 1.42 *Considere-se o grafo*



Este grafo não é hamiltoniano pois se o fosse: por (i), as arestas $\{a,b\}$, $\{a,h\}$, $\{b,c\}$, $\{c,d\}$, $\{e,d\}$, $\{f,e\}$, $\{f,g\}$ e $\{h,g\}$ *estariam em qualquer ciclo hamiltoniano (os vértices* a, c, g e e *são vértices de grau 2); então, por (iii), todas as restantes arestas de* G *não poderiam ser consideradas na construção do ciclo hamiltoniano; obteríamos então o ciclo* $\langle a,b,c,d,e,f,g,h,a\rangle$*, o que contradiz (ii).*

1.5.3 Exercícios

Exercício 1.5.1. Considere os seguintes grafos:



(a) Indique os que são eulerianos.

(b) Indique os que são semieulerianos.

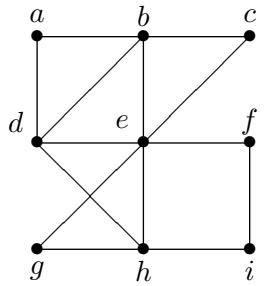
(c) Indique os que são hamiltonianos.

Exercício 1.5.2. Quais dos grafos platónicos são eulerianos? E hamiltonianos?

Exercício 1.5.3. Para que valores de $n, m \in \mathbb{N}$ o grafo $K_{n,m}$ é euleriano?

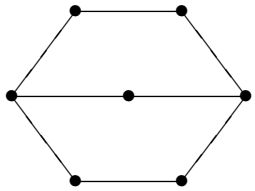
Exercício 1.5.4. Para que valores de $n, m \in \mathbb{N}$ o grafo $K_{n,m}$ é hamiltoniano?

Exercício 1.5.5. Considere o grafo G representado por



Mostre que o grafo é euleriano mas não é hamiltoniano.

Exercício 1.5.6. Mostre que o seguinte grafo não é euleriano nem hamiltoniano:



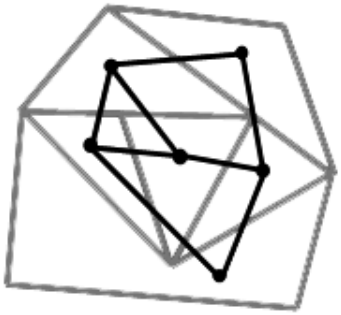
Exercício 1.5.7. Sejam G e G' dois grafos conexos homeomorfos. Mostre que G é euleriano se e só se G' é euleriano.

1.6 número cromático

O Teorema das quatro cores estabelece que dado qualquer plano dividido em regiões disjuntas (como, por exemplo, o planisfério), essas regiões podem ser coloridas usando, no mínimo, quatro cores, de tal modo que duas regiões conexas adjacentes não são pintadas com a mesma cor. Duas regiões dizem-se adjacentes se partilharem uma linha de fronteira. Estão também excluídas regiões desconexas (no planisfério, por exemplo, não se consideram os enclaves).

1.6.1 a coloração dos vértices de um grafo

À semelhança de problemas do mundo real que analisámos anteriormente, o problema da coloração de um mapa pode também ser traduzido em termos de grafos planares. Para tal, basta identificarmos cada uma das regiões como um vértice e dizermos que dois vértices são adjacentes se as regiões que eles representam são também adjacentes.



Definição 1.39 *Sejam $G = (V, E)$ um grafo e C um conjunto a cujos elementos chamaremos* cores. *Uma* coloração de G *é uma aplicação $f : V \to C$ tal que, dados $v, w \in V$, $f(v) \neq f(w)$ se $\{v, w\} \in E$. Uma k-*coloração *é uma coloração f tal que $\#f(V) = k$.*

Definição 1.40 *Seja $G = (V, E)$ um grafo. Chama-se* número cromático de G, *e representa-se por $\chi(G)$, ao menor $k \in \mathbb{N}$ tal que existe uma k-coloração de G.*

Exemplo 1.43 *Sejam $m, n \in \mathbb{N}$. Então, $\chi(K_{m,n}) = 2$.*

Exemplo 1.44 *Para todo $n \in \mathbb{N}$, K_n tem número cromático n.*

Estamos agora em condições de reescrever o Teorema de Headwood de 1890

Teorema 1.15 *Seja G um grafo conexo planar. Então, $\chi(G) \leq 5$.* □

A conjectura de Guthrie de 1852, posteriormente provada em 1976, pode ser reescrita do seguinte modo

Conjectura 1.1 *O número cromático de qualquer grafo conexo planar é não superior a 4.* □

Finalizamos com a apresentação de um algoritmo para colorir grafos, da autoria de Welch e Powell.

Algoritmo de Welch-Powell

1º Passo. Liste todos os vértices por ordem decrescente dos seus graus;

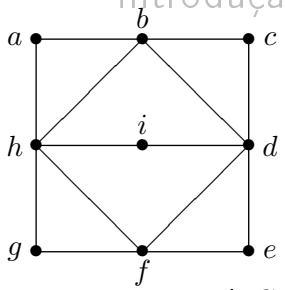
2º Passo. Atribua uma cor C_1 ao 1º vértice da lista e, seguindo a ordem da lista, atribua a cor C_1 a cada vértice não adjacente aos vértices ao quais foi anteriormente atribuída a cor C_1;

3º Passo. Repita o 1º Passo com os vértices ainda não coloridos;

4º Passo. Repita o 2º Passo usando uma segunda cor;

Repita os dois passos anteriores com cores diferentes até colorir todos os vértices.

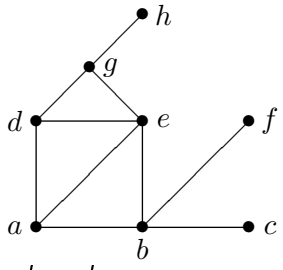
Exemplo 1.45 *Considere-se o grafo G*



Coloquemos, por ordem decrescente de grau, os vértices de G*:* $d, h, b, f, a, c, i, g, e$*. Atribui-se a coloração* R *a* d*. Como* h *não é adjacente a* d*, atribui-se a coloração* R *também a* h*. Mais nenhum vértice da lista pode ser colorido com* R*. Considere-se então o vértice* b *ao qual atribuímos a coloração* G*. Os vértices* f *e* i*, e só estes, também devem ser coloridos com* G*. Os restantes 4 vértices podem ser coloridos com uma mesma cor, por exemplo,* B*.*

Embora este seja um bom algoritmo para colorir grafos, não é eficaz na determinação do número cromático de um grafo, já que o número de cores usadas a que ele pode conduzir não é necessariamente o número cromático. Vejamos o seguinte exemplo.

Exemplo 1.46 *Considere-se o grafo* G



Comecemos por listar os vértices por ordem decrescente segundo o seu grau:

grau	*vértice*
4	b, e
3	a, d, g
1	c, f, h

Como a ordem com que consideramos os vértices de, por exemplo, grau 3, é aleatória, podemos obter duas colorações distintas:

$$f_1 = \begin{pmatrix} a & b & c & d & e & f & g & h \\ C_3 & C_2 & C_1 & C_2 & C_1 & C_1 & C_3 & C_1 \end{pmatrix}$$

e

$$f_2 = \begin{pmatrix} a & b & c & d & e & f & g & h \\ C_3 & C_2 & C_1 & C_4 & C_1 & C_1 & C_2 & C_1 \end{pmatrix}.$$

É óbvio que, ao processar o algoritmo para a segunda coloração, não estamos a usar o número mínimo de cores.

1.6.2 Exercícios

Exercício 1.6.1. Determine o número cromático dos grafos platónicos.

Exercício 1.6.2. Construa um grafo planar conexo cujo número cromático seja 4.

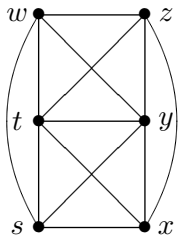
Exercício 1.6.3. Construa um grafo cujo número cromático seja 6.

Exercício 1.6.4. Seja $n \geq 3$. Prove que o número cromático de um grafo ciclo de comprimento n é 2 se n é par e é 3 se n é ímpar.

Exercício 1.6.5. Seja G um grafo conexo com pelo menos 2 vértices. Mostre que G é bipartido se e só se tem número cromático 2.

1.7 Exercícios de revisão

Exercício 1.7.1. Considere o grafo G representado por



(a) Mostre que G não é planar.

(b) Mostre que $\chi(G) = 4$.

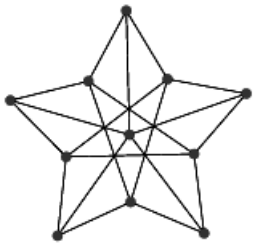
(c) Verifique se G é bipartido.

(d) O *complemento* de um grafo $H = (V, E)$ é um grafo $\overline{H} = (\overline{V}, \overline{E})$, onde

$$\overline{V} = V \quad \text{e} \quad \overline{E} = \{\{a,b\} \subseteq V : a \neq b,\ \{a,b\} \notin E\}.$$

Determine o complemento de G.

Exercício 1.7.2. Considere o seguinte grafo (conhecido por grafo de Grötzsche)



Mostre que o grafo

(a) não é planar;

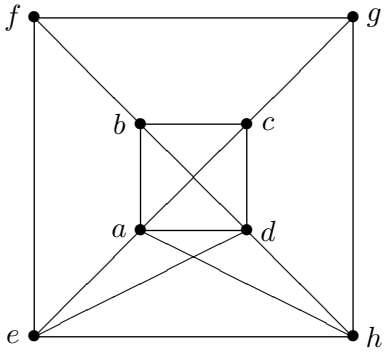
(b) tem número cromático 4;

(c) não é bipartido;

(d) é hamiltoniano;

(e) não é euleriano.

Exercício 1.7.3. Considere o grafo



Mostre que o grafo

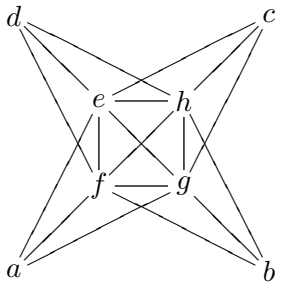
(a) tem número cromático 4;

(b) não é bipartido;

(c) é hamiltoniano;

(d) não é euleriano.

Exercício 1.7.4. Considere o grafo $G = (V, E)$ representado por



(a) Mostre que G não é bipartido.

(b) Sabendo que G é planar, determine o número de faces que terá uma representação planar de G.

(c) Determine o número cromático de G.

2. introdução à teoria de números

"A great discovery solves a great problem but there is a grain of discovery in the solution of any problem."
George Polya

2.1 teoria da divisibilidade nos números

2.1.1 algoritmo da divisão

Nesta secção estabelecemos e provamos um resultado que nos é, de certo modo, familiar e que constitui o alicerce onde assenta todo o estudo que faremos no capítulo 2: o Algoritmo da Divisão – qualquer inteiro pode ser "dividido" por qualquer inteiro não nulo. Este conceito de "ser dividido por" tem, naturalmente, que ser formalizado.

Teorema 2.1 ***(Algoritmo da Divisão)*** *Dados dois números inteiros a e b tais que $b > 0$ existe um e um só inteiro q e existe um e um só inteiro r tais que*

$$a = bq + r \quad e \quad 0 \leq r < b.$$

Demonstração: *Existência.* Consideremos o conjunto

$$S = \{a - xb \in \mathbb{N}_0 : x \in \mathbb{Z}\}.$$

Se $0 \in S$, então, 0 é o elemento mínimo de S. Se $0 \notin S$, então, $S \subseteq \mathbb{N}$. Temos

$$\begin{aligned} b \geq 1 \quad &\Rightarrow |a|b \geq |a| \\ &\Rightarrow a + |a|b \geq a + |a| \geq 0 \\ &\Rightarrow a - (-|a|)b \geq 0. \end{aligned}$$

Como $-|a| \in \mathbb{Z}$, $a - (-|a|)b \in S$ e, portanto, $S \neq \emptyset$. Logo, Pelo Princípio da Boa Ordenação de $\mathbb{N}$ [1], existe o elemento mínimo de S. Seja $r = \min S$. Então, existe $q \in \mathbb{Z}$ tal que

$$r = a - qb \text{ e } r \geq 0,$$

i.e., existe $q \in \mathbb{Z}$ tal que

$$a = qb + r \text{ e } r \geq 0.$$

Suponhamos agora que $b \leq r$. Então,

$$a - (q+1)b = a - qb - b = r - b \geq 0,$$

pelo que $a - (q+1)b \in S$, i.e., $r - b \in S$. Assim, $r - b \geq \min S = r$, o que é um absurdo, pois $b > 0$. O absurdo resulta de termos suposto que $b \leq r$. Logo, $r < b$.

Unicidade. Sejam $q, q', r, r' \in \mathbb{Z}$ tais que

$$a = bq + r,\ a = bq' + r',\ 0 \leq r < b \text{ e } 0 \leq r' < b.$$

Por um lado,

$$b(q - q') = r' - r$$

e, portanto,

$$b|q - q'| = |r' - r|. \qquad (*)$$

Por outro lado,

$$\begin{cases} 0 \leq r < b \\ 0 \leq r' < b \end{cases} \iff \begin{cases} 0 \leq r' < b \\ -b < -r \leq 0 \end{cases} \implies -b < r' - r < b \iff |r' - r| < b.$$

Logo, de $(*)$, temos que $b|q - q'| < b$, pelo que $0 \leq |q - q'| < 1$. Como $q - q' \in \mathbb{Z}$, concluímos que $q - q' = 0$, i.e., $q = q'$. Novamente de $(*)$, concluímos que $r = r'$. □

O resultado seguinte é uma consequência do Algoritmo da Divisão e estende a divisão de qualquer inteiro por qualquer inteiro positivo à divisão de qualquer inteiro por qualquer inteiro não nulo.

[1] Princípio da Boa Ordenação de $\mathbb{N}$: *Todo o subconjunto não vazio de* $\mathbb{N}$ *tem elemento mínimo.*

Corolário 2.1 *Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Então, existem inteiros q e r, univocamente determinados, tais que $a = bq + r$ e $0 \leq r < |b|$.*

Demonstração: Tendo em conta o teorema anterior, resta-nos estudar o caso em que $b \in \mathbb{Z}^-$. Como $|b| > 0$, aplicando o teorema anterior, temos que existem um e um só $q' \in \mathbb{Z}$ e um e um só $r' \in \mathbb{Z}$ tais que

$$a = q'|b| + r' \text{ e } 0 \leq r' < |b|.$$

Então, como $|b| = -b$, obtemos

$$a = (-q')b + r' \text{ e } 0 \leq r' < |b|,$$

o que prova o resultado pretendido. □

Dados $a, b \in \mathbb{Z}$ e $b \neq 0$, os números q e r tais que $a = bq+r$ e $0 \leq r < |b|$, univocamente determinados em $\mathbb{Z}$, designam-se, respectivamente, por *quociente da divisão de a por b* e *resto da divisão de a por b*. "Dividir a por b" significa obter o quociente e o resto da divisão de a por b.

Exemplo 2.1 *Para $a = 7$ e $b = 6$, temos $a = 7 = 1 \times 6 + 1 = 1 \times b + 1$ e $0 \leq 1 < 6$.*

Exemplo 2.2 *Para $a = 1$ e $b = 6$, temos $a = 0 \times 6 + 1 = 0 \times b + 1$ e $0 \leq 1 < 6$.*

Exemplo 2.3 *Para $a = -2$ e $b = -7$, temos $a = 1 \times (-7) + 5 = 1 \times b + 5$ e $0 \leq 5 < |-7|$.*

Exemplo 2.4 *Para $a = 61$ e $b = -7$, temos $a = (-8) \times (-7) + 5 = -8 \times b + 5$ e $0 \leq 5 < |-7|$.*

Apresentamos, de seguida, a título de exemplo, algumas propriedades dos números inteiros cuja demonstração é uma aplicação do Algoritmo da Divisão.

- *O resto da divisão do quadrado de qualquer número inteiro por 4 ou é 0 ou é 1.*

  Sejam $a \in \mathbb{Z}$ e $b = 2$. Aplicando o algoritmo da divisão, podemos dividir a por b e obtemos $q, r \in \mathbb{Z}$ tais que $a = 2q + r$ e $r \in \{0, 1\}$. Assim,

  - se $r = 0$, temos que $a = 2q$ (para algum $q \in \mathbb{Z}$) e, portanto, $a^2 = 4q = 4q + 0$;

  - se $r = 1$, temos que $a = 2q + 1$ (para algum $q \in \mathbb{Z}$) e, portanto, $a^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$.

- *O quadrado de qualquer número inteiro ímpar é da forma* $8k + 1$ *para certo inteiro* k.

  Sejam $a \in \mathbb{Z}$ um número ímpar e $b = 4$. Ao dividir a por b, obtemos $a = bq + r$ onde $q \in \mathbb{Z}$ e $r \in \{0, 1, 2, 3\}$. Como a é ímpar, teremos necessariamente que ter $r \in \{1, 3\}$, já que se $r \in \{0, 2\}$, o número a é par. Assim,

  - se $r = 1$, $a = 4q + 1$ e

    $$a^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1;$$

  - se $r = 3$, $a = 4q + 3$ e

    $$a^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1.$$

- *Para qualquer inteiro* $a \geq 1$, $\frac{a(a^2+2)}{3}$ *é um inteiro.*

  Seja $a \in \mathbb{Z}$. Dizer que o número $\frac{a(a^2+2)}{3}$ é um inteiro é equivalente a dizer que $a(a^2 + 2)$ é divisível por 3. Façamos, portanto, a divisão de a por 3. Apenas 3 situações distintas podem ocorrer:

  $$\text{ou } a = 3q \text{ ou } a = 3q + 1 \text{ ou } a = 3q + 2, \text{ para algum } q \in \mathbb{Z}.$$

  - Se $a = 3q$, então, $a(a^2 + 2) = 3q(9q^2 + 2) = 3k$ onde $k = q(9q^2 + 2)$;
  - Se $a = 3q + 1$, então, $a(a^2 + 2) = (3q + 1)(9q^2 + 6q + 3) = 3k'$ onde $k' = (3q + 1)(3q^2 + 2q + 1)$;
  - Se $a = 3q + 2$, temos que $a(a^2 + 2) = (3q + 2)(9q^2 + 12q + 6) = 3k''$ onde $k'' = (3q + 2)(3q^2 + 4q + 2)$.

2.1.2 máximo divisor comum

Nesta subsecção, vamos estudar um caso particular da divisão inteira – o caso onde o resto obtido é nulo.

Definição 2.1 *Sejam* $a, b \in \mathbb{Z}$. *Diz-se que* a divide b, *e escreve-se* $a \mid b$, *se existe* $c \in \mathbb{Z}$ *tal que* $b = ac$.

Observação. As expressões a *divide* b, a *é divisor de* b, a *é um factor de* b, b *é divisível por* a e b *é múltiplo de* a têm todas o mesmo significado.

Escrevemos $a \nmid b$ para significar que a *não divide* b.

Teorema 2.2 *Sejam* $a, b, c, d \in \mathbb{Z}$ *números inteiros. Então:*

(1) $a \mid 0$, $1 \mid a$ *e* $a \mid a$;

(2) $a \mid 1 \Leftrightarrow a = \pm 1$ *e* $0 \mid a \Leftrightarrow a = 0$;

(3) $a \mid b$ *e* $c \mid d \Rightarrow ac \mid bd$;

(4) $a \mid b$ *e* $b \mid c \Rightarrow a \mid c$;

(5) $a \mid b$ *e* $b \mid a \Rightarrow a = \pm b$;

(6) $a \mid b$ *e* $b \neq 0 \Rightarrow |a| \leq |b|$;

(7) $a \mid b$ *e* $a \mid c \Rightarrow a \mid (bx + cy)$, *para todos* $x, y \in \mathbb{Z}$.

Demonstração: Demonstraremos as alíneas (3), (6) e (7). As outras são deixadas como exercício.

(3) Se $a \mid b$ e $c \mid d$, então, existem $q, q' \in \mathbb{Z}$ tais que $b = aq$ e $d = cq'$, pelo que $bd = (aq)(cq') = ac(qq')$, com $qq' \in \mathbb{Z}$, i.e., $ac \mid bd$;

(6) Seja $b \neq 0$ tal que $a \mid b$. Então, existe $c \neq 0$ tal que $b = ac$. Assim, $|b| = |a||c|$ com $|c| \geq 1$ e, portanto, $|a| \leq |b|$;

(7) Se $a \mid b$ e $a \mid c$, existem $q, q' \in \mathbb{Z}$ tais que $b = aq$ e $c = aq'$. Logo, para quaisquer $x, y \in \mathbb{Z}$, temos que

$$bx + cy = (aq)x + (aq')y = a(qx + q'y).$$

Como $qx + q'y \in \mathbb{Z}$, concluímos que $a \mid (bx + cy)$.

□

Um raciocínio indutivo permite generalizar a alínea (7) do teorema anterior.

Corolário 2.2 *Sejam* $k \in \mathbb{N}$ *e* $a, b_1, b_2, ..., b_k \in \mathbb{Z}$. *Se, para cada* $i \in \{1, 2, ..., k\}$, $a \mid b_i$, *então,*

$$a \mid \sum_{i=1}^{k} b_i x_i,$$

quaisquer que sejam $x_1, x_2, ..., x_k \in \mathbb{Z}$. □

Sejam $a, b \in \mathbb{Z}$. Como $1 \mid a$ e $1 \mid b$, temos que

$$D = \{d \in \mathbb{N} : d \mid a \text{ e } d \mid b\} \neq \emptyset.$$

Se $a = b = 0$, então, $D = \mathbb{N}$;

Se $a \neq 0$ ou $b \neq 0$, então, existe um número finito de elementos em D. De todos eles podemos considerar o *maior*: será então o maior número inteiro positivo que divide simultaneamente a e b. A existência deste número dá sentido à seguinte definição.

Definição 2.2 *Sejam* $a, b \in \mathbb{Z}$, $a \neq 0$ *ou* $b \neq 0$. *Chama-se* máximo divisor comum de a e b, *e representa-se por* m.d.c.(a, b), *ao inteiro positivo* d *tal que:*

(i) $d \mid a$ *e* $d \mid b$;

(ii) $\forall c \in \mathbb{N}$, $c \mid a$ *e* $c \mid b \Rightarrow c \leq d$.

Teorema 2.3 *Para quaisquer* $a, b \in \mathbb{Z}$, *com* $a \neq 0$ *ou* $b \neq 0$, *existem* $x, y \in \mathbb{Z}$ *tais que*

$$\text{m.d.c.}(a, b) = ax + by.$$

Demonstração: Sejam $a, b \in \mathbb{Z}$ e suponhamos, sem perda de generalidade, que $a \neq 0$. Consideremos o seguinte subconjunto de $\mathbb{N}$:

$$S = \{au + bv \in \mathbb{N} \, : \, u, v \in \mathbb{Z}\}.$$

Tomando

$$v = 0 \text{ e } u = \begin{cases} 1 & se \ a > 0 \\ -1 & se \ a < 0 \end{cases},$$

temos que

$$au + bv = |a| \in S,$$

pelo que $S \neq \emptyset$.

Assim, S é um subconjunto não vazio de $\mathbb{N}$ e, pelo Princípio da Boa Ordenação em $\mathbb{N}$, temos que existe $\min S$. Seja $d = \min S$. Como $d \in S$, $d = ax + by$, para alguns $x, y \in \mathbb{Z}$. Provemos que $d = \text{m.d.c.}(a, b)$:

(i) Como $a \in \mathbb{Z}$ e $d > 0$, obtemos, pelo Algoritmo da Divisão,

$$a = qd + r \text{ e } 0 \leq r < d.$$

Logo,

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

Assim, se $r > 0$, então, $r \in S$, pelo que $d \leq r$, o que contradiz o facto de $0 \leq r < d$. Logo, temos que $r = 0$ e, portanto, $a = dq$, ou seja, $d \mid a$.

De modo análogo, provamos que $d \mid b$.

(ii) Seja $c \in \mathbb{N}$ tal que $c \mid a$ e $c \mid b$. Então, pelo Teorema 2.2(7), $c \mid (ax' + by')$, para quaisquer $x', y' \in \mathbb{Z}$. Logo, para $x' = x$ e $y' = y$, $c \mid d$ e, pelo Teorema 2.2(6), $c = |c| \leq |d| = d$. □

Corolário 2.3 *Se a e b são inteiros, não ambos nulos, então, o conjunto*

$$T = \{ax + by : x, y \in \mathbb{Z}\}$$

é exactamente o conjunto de todos os múltiplos de $d = \text{m.d.c.}(a, b)$.

Demonstração: Seja $d = \text{m.d.c.}(a, b)$. Por um lado, pelo teorema anterior, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$d = ax_0 + by_0.$$

Logo, $d \in T$ e, portanto, para todo $n \in \mathbb{Z}$, temos que

$$nd = a(nx_0) + b(ny_0) \in T.$$

Por outro lado,

$$d \mid a,\ d \mid b \Rightarrow (\forall x, y \in \mathbb{Z})\ \ d \mid ax + by.$$

Logo, podemos concluir que qualquer elemento de T é um múltiplo de d. □

O próximo teorema estabelece que a relação entre o máximo divisor comum de dois inteiros, não ambos nulos, e qualquer outro divisor comum desses inteiros é mais do que uma relação de ordem.

Teorema 2.4 *Sejam a e b inteiros, não simultaneamente nulos, e seja d um inteiro positivo. Então, $d =$ m.d.c.(a, b) se e só se d satisfaz as seguintes condições:*

(1) $d \mid a$ *e* $d \mid b$*;*

(2) $\forall c \in \mathbb{Z}$, $c \mid a$ *e* $c \mid b \Rightarrow c \mid d$.

Demonstração: Seja $d =$ m.d.c.(a, b). Por (i) da definição de m.d.c.(a, b), $d \mid a$ e $d \mid b$, o que prova (1). Se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, pelo Teorema 2.2(7), temos que $c \mid ax + by$, para todos $x, y \in \mathbb{Z}$. Assim, pelo Teorema 2.3, concluímos que $c \mid d$, o que prova (2).

Reciprocamente, seja $d \in \mathbb{Z}$ tal que d satisfaz as condições (1) e (2). Então, a condição (i) da definição é obviamente satisfeita. Seja $c \in \mathbb{N}$ tal que $c \mid a$ e $c \mid b$. Então, por (2), $c \mid d$. Logo, pelo Teorema 2.2 (6), $c = |c| \leq |d| = d$, o que prova (ii). Assim, por definição, $d =$ m.d.c.(a, b).

□

2.1.3 números primos entre si

Definição 2.3 *Dois números inteiros a e b, não simultaneamente nulos, dizem-se* primos entre si *se* m.d.c.$(a, b) = 1$.

Teorema 2.5 *Sejam a e b números inteiros, não simultaneamente nulos. Então, a e b são primos entre si se e só se existirem inteiros x e y tais que* $1 = ax + by$.

Demonstração: Se a e b são primos entre si, $1 =$ m.d.c.(a, b) e, pelo Teorema 2.3, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$.

Reciprocamente, se existem inteiros x e y tais que $1 = ax + by$, então, pelo Corolário 2.3, 1 é múltiplo do m.d.c.(a, b). Como são ambos positivos, concluímos pelo Teorema 2.2(2) que $1 =$ m.d.c.(a, b). □

Corolário 2.4 *Sejam a e b números inteiros, não simultaneamente nulos. Se* m.d.c.$(a, b) = d$*, então,* m.d.c.$(\frac{a}{d}, \frac{b}{d}) = 1$.

Demonstração: Temos:

$$\begin{aligned} \text{m.d.c.}(a,b) = d &\Rightarrow \exists x, y \in \mathbb{Z} : \ d = ax + by \\ &\Rightarrow \exists x, y \in \mathbb{Z} : \ 1 = \tfrac{a}{d}x + \tfrac{b}{d}y. \end{aligned}$$

Como $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros (porque $d \mid a$ e $d \mid b$), segue-se que $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si. □

Observação. O recíproco deste corolário não é verdadeiro. Por exemplo,

$$\text{m.d.c.}(\tfrac{-6}{-3}, \tfrac{-9}{-3}) = \text{m.d.c.}(2,3) = 1 \text{ e } -3 \neq 3 = \text{m.d.c.}(-6,-9).$$

Corolário 2.5 *Sejam $a, b, c \in \mathbb{Z}$, com a e b não simultaneamente nulos. Se $a \mid c$, $b \mid c$ e* m.d.c.$(a,b) = 1$*, então, $ab \mid c$.*

Demonstração: Por um lado, como $a \mid c$ e $b \mid c$, temos que existem $x, y \in \mathbb{Z}$ tais que

$$c = ax = by.$$

Por outro lado, como $1 =$ m.d.c.(a,b), temos que existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$1 = ax_0 + by_0.$$

Logo,

$$c = c \cdot 1 = c(ax_0 + by_0) = cax_0 + cby_0 = byax_0 + axby_0 = (ab)(yx_0 + xy_0).$$

Como $yx_0 + xy_0 \in \mathbb{Z}$, concluímos que $ab \mid c$. □

Observação: No Corolário 2.5, a condição de a e b serem primos entre si não pode ser omitida. De facto, existem $a, b, c \in \mathbb{Z}$ tais que $a \mid c$, $b \mid c$ e, no entanto, $ab \nmid c$. Por exemplo, $4 \mid 12$, $6 \mid 12$ e $4 \times 6 = 24 \nmid 12$.

Corolário 2.6 ***(Lema de Euclides)*** *Sejam $a, b, c \in \mathbb{Z}$, com a e b não simultaneamente nulos. Se $a \mid bc$ e* m.d.c.$(a,b) = 1$*, então, $a \mid c$.*

Demonstração: Se $1 =$ m.d.c.(a,b), então, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$. Assim,

$$c = c \cdot 1 = acx + bcy.$$

Como $a \mid ac$ e, por hipótese, $a \mid bc$, temos, pelo Teorema 2.2(7), que $a \mid (ac)x + (bc)y = c$. □

Observação. De novo, a condição m.d.c.$(a, b) = 1$ é necessária para que a conclusão do Lema de Euclides seja verdadeira. De facto, considerando $a = 12$, $b = 8$ e $c = 9$, temos que $12 \mid 9 \times 8$ e, no entanto, $12 \nmid 9$ e $12 \nmid 8$.

2.1.4 o algoritmo de Euclides

Vimos, numa secção anterior, que existe máximo divisor comum de quaisquer dois inteiros não simultaneamente nulos. A prova desta realidade não é, no entanto, construtiva já que não ensina a calcular o máximo divisor comum de dois tais inteiros – ele aparece como o elemento mínimo de um certo subconjunto de inteiros positivos. Como calcular, então, o máximo divisor comum de dois inteiros não simultaneamente nulos? No sétimo livro da obra *Elementos* de Euclides (350 a.C.), o autor apresenta um método eficaz de cálculo do máximo divisor comum, o qual envolve a aplicação sucessiva do Algoritmo da Divisão. Este método tem também a virtude de permitir que se calculem os coeficientes envolvidos na expressão do m.d.c.(a, b) como combinação linear de a e b. Embora exista evidência histórica de que este método tenha sido estabelecido antes do tempo de Euclides, ele é hoje conhecido por todos como o Algoritmo de Euclides.

Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos.

Comecemos por observar que, como m.d.c.$(|a|, |b|) =$ m.d.c.$(a, b) =$ m.d.c.(b, a), podemos estudar apenas o caso em que

$$a \geq b > 0.$$

Lema 2.1 *Sejam a e b inteiros não nulos e $q, r \in \mathbb{Z}$ tais que $a = qb + r$ e $0 \leq r < b$. Então,*

$$d = \text{m.d.c.}(a, b) \Leftrightarrow d = \text{m.d.c.}(b, r).$$

Demonstração: Seja $d =$ m.d.c.(a, b). Então,

(i) $d \mid a$ e $d \mid b$;

(ii) se $c \in \mathbb{N}$ é tal que $c \mid a$ e $c \mid b$, então $c \leq d$.

Queremos provar que $d =$ m.d.c.(b, r), i.e., que

(i') $d \mid b$ e $d \mid r$;

(ii') se $c \in \mathbb{N}$ é tal que $c \mid b$ e $c \mid r$, então, $c \leq d$.

Por um lado, de (i), temos que $d \mid a$ e $d \mid b$, pelo que $d \mid 1 \cdot a + (-q)b$, ou seja, $d \mid r$. Concluímos, assim, (i'). Por outro lado, se $c \in \mathbb{N}$ é tal que $c \mid b$ e $c \mid r$, então, $c \mid qb + r$, ou seja $c \mid a$. Logo, por (ii), $c \leq d$, o que prova (ii').

O recíproco prova-se de modo análogo. □

Teorema 2.6 ***(Algoritmo de Euclides)*** *Sejam a e b inteiros tais que $a \geq b > 0$. Se existem $q_1, q_2, ..., q_{n+1}, r_1, r_2, ..., r_n \in \mathbb{Z}$ tais que*

$$\begin{aligned} a &= q_1 b + r_1 \quad \text{e} \quad 0 < r_1 < b \\ b &= q_2 r_1 + r_2 \quad \text{e} \quad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \quad \text{e} \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \quad \text{e} \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0, \end{aligned}$$

então, m.d.c.$(a, b) = r_n$.

Demonstração: Imediata, tendo em conta que, pelo lema anterior, temos que

$$\text{m.d.c.}(a, b) = \text{m.d.c.}(b, r_1) = \text{m.d.c.}(r_1, r_2) = \cdots = \text{m.d.c.}(r_{n-1}, r_n) = \text{m.d.c.}(r_n, 0) = r_n.$$

□

Observação. Usando as sucessivas expressões das divisões inteiras, podemos determinar $x, y \in \mathbb{Z}$ tais que m.d.c.$(a, b) = ax + by$. O exemplo seguinte ilustra o processo a seguir.

Exemplo 2.5 *Queremos calcular o* m.d.c.$(12378, 3054)$ *e escrevê-lo como combinação linear de* 12378 *e* 3054*. Para tal, procedemos às seguintes divisões inteiras*

$$\begin{aligned} 12378 &= 4 \times 3054 + 162 \qquad (1) \\ 3054 &= 18 \times 162 + 138 \qquad (2) \\ 162 &= 1 \times 138 + 24 \qquad (3) \\ 138 &= 5 \times 24 + 18 \qquad (4) \\ 24 &= 1 \times 18 + 6 \qquad (5) \\ 18 &= 3 \times 6 + 0. \end{aligned}$$

Logo, m.d.c.$(12378, 3054) = 6$. *Mais ainda, temos que*

$$\begin{aligned}
6 &= 24 - 1 \times 18 && \text{por (5)}\\
&= 24 - (138 - 5 \times 24) && \text{por (4)}\\
&= 6 \times 24 - 1 \times 138\\
&= 6(162 - 1 \times 138) - 138 && \text{por (3)}\\
&= 6 \times 162 - 7 \times 138\\
&= 6 \times 162 - 7(3054 - 18 \times 162) && \text{por (2)}\\
&= 132 \times 162 - 7 \times 3054\\
&= 132(12378 - 4 \times 3054) - 7 \times 3054 && \text{por (1)}\\
&= 132 \times 12378 - 535 \times 3054.
\end{aligned}$$

Assim, determinámos dois inteiros x *e* y *(*$x = 132$ *e* $y = -535$*) de tal modo que* m.d.c.$(12378, 3054) = 6 = 12378x + 3054y$.

Observação. Os dois inteiros encontrados com o raciocínio apresentado no exemplo anterior, i.e., usando o Algoritmo de Euclides, não são únicos. Por exemplo, cálculos simples mostram que

$$6 = 12378 \times 3186 + 3054 \times (-12913).$$

2.1.5 mínimo múltiplo comum

Sejam $a, b \in \mathbb{Z}\backslash\{0\}$. Sabemos que

$$a \mid \pm ab \text{ e } b \mid \pm ab,$$

pelo que podemos afirmar que o conjunto

$$\{k \in \mathbb{N} : a \mid k \text{ e } b \mid k\}$$

é não vazio. Pelo Princípio da Boa Ordenação de $\mathbb{N}$, existe

$$m = \min\{k \in \mathbb{N} : a \mid k \text{ e } b \mid k\},$$

i.e., existe o menor inteiro positivo simultaneamente múltiplo de a e b. Chamamos-lhe *mínimo múltiplo comum de* a *e* b. Mais precisamente, temos a seguinte definição.

Definição 2.4 *Sejam* $a, b \in \mathbb{Z}\backslash\{0\}$. *Chama-se* mínimo múltiplo comum de a e b, *e representa-se por* m.m.c.(a, b), *ao* $\min\{k \in \mathbb{N} : a \mid k \,e\, b \mid k\}$, *i.e., ao inteiro positivo* m *tal que:*

(i) $a \mid m$ *e* $b \mid m$;

(ii) se $c \in \mathbb{N}$ *é tal que* $a \mid c$ *e* $b \mid c$, *então,* $m \leq c$.

Se $a = 0$ *ou* $b = 0$, *diz-se que* m.m.c.$(a, b) = 0$.

Observação. Para quaisquer inteiros a e b, m.m.c.$(a, b) \leq |ab|$.

Lema 2.2 *Sejam* a *e* b *inteiros não nulos e* $m \in \mathbb{Z}$. *Então,* $m =$ m.m.c.(a, b) *se e só se* m *é tal que:*

(i) $a \mid m$ *e* $b \mid m$;

(ii) se $c \in \mathbb{Z}$ *é tal que* $a \mid c$ *e* $b \mid c$, *então,* $m \mid c$.

Demonstração: Exercício. □

Teorema 2.7 *Para quaisquer inteiros positivos* a *e* b,

$$\text{m.m.c.}(a, b) = \frac{ab}{\text{m.d.c.}(a, b)}.$$

Demonstração: Começamos por observar que, sendo $a, b > 0$, temos que m.d.c.$(a, b) \neq 0$.

Sejam $d =$ m.d.c.(a, b), $x, y \in \mathbb{Z}$ tais que $a = dx$ e $b = dy$ e $x', y' \in \mathbb{Z}$ tais que $d = ax' + by'$.

Consideremos o número $m = \frac{ab}{d}$. Então,

(i) $m = \frac{dxb}{d} = bx$ e $m = \frac{ady}{d} = ay$. Assim, $m \in \mathbb{Z}$ é tal que $b \mid m$ e $a \mid m$;

(ii) se $c \in \mathbb{N}$ é tal que $b \mid c$ e $a \mid c$, existem $u, v \in \mathbb{Z}$ tais que

$$c = bu \quad \text{e} \quad c = av.$$

Assim,

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax' + by')}{ab} = \frac{c}{b}x' + \frac{c}{a}y' = ux' + vy' \in \mathbb{Z}$$

e, portanto, $m \mid c$. Logo, $m = |m| \leq |c| = c$.

Por (i) e (ii), concluímos que m.m.c.$(a, b) = \frac{ab}{\text{m.d.c.}(a,b)}$. □

Corolário 2.7 *Dados dois inteiros positivos a e b, tem-se que*

$$\text{m.m.c.}(a,b) = ab \iff \text{m.d.c.}(a,b) = 1.$$

□

2.1.6 Exercícios

Exercício 2.1.1. Sejam $a, b \in \mathbb{Z}$ tais que $a < 0$ e $b > 0$. Sejam $q, r, q_1, r_1 \in \mathbb{Z}$ tais que $-a = bq_1 + r_1$ e $0 \leq r_1 < b$, $a = bq + r$ e $0 \leq r < b$. Mostre que:

(a) se $r_1 = 0$ então $q = -q_1$ e $r = 0$;

(b) se $r_1 \neq 0$ então $q = -(q_1 + 1)$ e $r = b - r_1$.

Exercício 2.1.2. Determine o quociente e o resto na divisão de:

(a) 310156 por 197;

(b) 32 por 45;

(c) 0 por 28;

(d) -19 por 6;

(e) -234 por -9.

Exercício 2.1.3. Mostre que, se a e b são inteiros e $b > 0$, então, existem, e são únicos, q e r inteiros tais que $a = qb + r$ e $2b \leq r < 3b$.

Exercício 2.1.4. Utilizando o Algoritmo da Divisão, mostre que:

(a) o quadrado de um inteiro é da forma $3k$ ou $3k+1$, para certo inteiro não negativo k;

(b) $3a^2 - 1$ não é um quadrado perfeito, para todo o inteiro a.

Exercício 2.1.5. Na divisão de 392 por 45, determine:

(a) o maior inteiro que se pode somar ao dividendo sem alterar o quociente;

(b) o maior inteiro que se pode subtrair ao dividendo sem alterar o quociente.

Exercício 2.1.6. Verifique que, para todo o inteiro $n \geq 1$, $\dfrac{n(n+1)(2n+1)}{6}$ é um inteiro.

Exercício 2.1.7. Dê exemplos de inteiros a, b e c tais que $a \mid bc$ mas $a \nmid b$ e $a \nmid c$.

Exercício 2.1.8. Mostre que, se $a \mid b$, então $(-a) \mid b, a \mid (-b)$ e $(-a) \mid (-b)$.

Exercício 2.1.9. Mostre que, se $a \mid (2x - 3y)$ e $a \mid (4x - 5y)$, então $a \mid y$.

Exercício 2.1.10. Justifique que, dados dois inteiros quaisquer a e b, os inteiros a e $a + 2b$ têm a mesma paridade.

Exercício 2.1.11. Mostre que, para todo o inteiro a, um dos inteiros $a, a + 2$, ou $a + 4$ é divisível por 3.

Exercício 2.1.12. Recorrendo ao Princípio de Indução, verifique que são verdadeiras as seguintes afirmações, para $n \geq 1$:

(a) $8 \mid (5^{2n} + 7)$;
[Sugestão: Observe que $5^{2(n+1)} + 7$ pode ser escrito como $5^2(5^{2n} + 7) + (7 - 5^2 \times 7)$.]

(b) $15 \mid (2^{4n} - 1)$.

Exercício 2.1.13. Verifique que, se a e b são ambos inteiros ímpares, então $16 \mid (a^4 + b^4 - 2)$.

Exercício 2.1.14. Prove que o produto de quatro inteiros consecutivos é divisível por 24.

Exercício 2.1.15. Mostre que m.d.c.$(a, b) = 1 =$ m.d.c.(a, c) se e só se m.d.c.$(a, bc) = 1$.

Exercício 2.1.16. Mostre que, dado um inteiro $a \neq 0$, se tem m.d.c.$(a, 0) = |a| =$ m.d.c.(a, a) e m.d.c.$(a, 1) = 1$.

Exercício 2.1.17. Verifique que, dados um inteiro positivo n e um inteiro a, m.d.c.$(a, a+n)$ divide n. Conclua que dois inteiros consecutivos são primos entre si.

Exercício 2.1.18. Sejam a e b inteiros. Mostre que:

(a) existem inteiros x e y tais que $c = ax + by$ se e só se m.d.c.$(a, b) \mid c$.

(b) se x e y são inteiros tais que $ax + by =$ m.d.c.(a, b), então m.d.c.$(x, y) = 1$.

Exercício 2.1.19. Mostre que, se $a = qb + r$, então m.d.c.$(a, b) =$ m.d.c.(b, r).

Exercício 2.1.20. Utilizando o Algoritmo de Euclides, determine o máximo divisor comum de cada par de inteiros a e b e escreva-o como combinação linear de a e b:

(a) $a = 1001, b = 357$;

(b) $a = 1001, b = 33$;

(c) $a = 56, b = 126$;

(d) $a = -90, b = 1386$;

(e) $a = -2860, b = -2310$.

Exercício 2.1.21. Exprima o m.d.c.$(2, 3)$ como combinação linear de 2 e 3, de dois modos distintos.

Exercício 2.1.22. Determine, usando o Algoritmo de Euclides, inteiros x e y que satisfaçam:

(a) m.d.c.$(56, 72) = 56x + 72y$;

(b) m.d.c.$(24, 138) = 24x + 138y$.

Exercício 2.1.23. Sabendo que m.d.c.$(a, b) = 1$, conclua que:

(a) m.d.c.$(a + b, a - b) = 1$ ou m.d.c.$(a + b, a - b) = 2$;

(b) m.d.c.$(a + b, ab) = 1$.

Exercício 2.1.24. Determine o menor inteiro positivo k da forma $k = 22x + 55y$, onde x e y são inteiros.

Exercício 2.1.25. Sejam $a, b \in \mathbb{Z}$, $a \neq 0$ e $b \neq 0$. Mostre que:

(a) se $a \mid b$, então $|a| =$ m.d.c.(a, b) e $|b| =$ m.m.c.(a, b);

(b) se $d =$ m.d.c.(a, b), então $|k|d =$ m.d.c.(ka, kb), para qualquer $k \in \mathbb{Z}$ e $k \neq 0$.

Exercício 2.1.26. Sejam a e b inteiros positivos. Verifique que as seguintes afirmações são verdadeiras:

(a) m.d.c.$(a, b) =$ m.m.c.(a, b) se e só se $a = b$;

(b) se $k > 0$, então m.m.c.$(ka, kb) = k \times$ m.m.c.(a, b);

(c) se m é um múltiplo comum de a e b, então m.m.c.$(a, b) \mid m$.
[Sugestão: Use o Algoritmo da Divisão para escrever m na forma $qt + r$, onde $t =$ m.m.c.(a, b) e $0 \leq r < t$. Mostre que r é um múltiplo comum de a e b.]

2.2 números primos

De entre os números inteiros, existe uma classe de números que desempenham um papel fundamental, de facto, alicerçante em toda a teoria de números – a classe dos números primos.

2.2.1 teorema fundamental da aritmética

Começamos esta secção recordando que, para qualquer $a \in \mathbb{Z}$, se tem $\pm 1 \mid a$ e $\pm a \mid a$. Assim, qualquer número inteiro não nulo diferente da identidade, admite no mínimo 4 divisores. Faz, então, sentido a seguinte definição.

Definição 2.5 *Um inteiro $p > 1$ diz-se um* número primo *se 1 e p forem os únicos divisores positivos de p.*

Um inteiro $k > 1$ diz-se um número composto *se não for um número primo.*

Teorema 2.8 *Sejam $a, b, p \in \mathbb{Z}$. Se p é um número primo e $p \mid ab$, então, $p \mid a$ ou $p \mid b$.*

Demonstração: Suponhamos que p é um número primo tal que $p \mid ab$ e $p \nmid a$. Então, m.d.c.$(a, p) = 1$ e, portanto, pelo Lema de Euclides, $p \mid b$. □

Corolário 2.8 *Sejam $n \in \mathbb{N}$ e $p, a_1, a_2, ..., a_n \in \mathbb{Z}$. Se p é primo e $p \mid a_1 a_2 \cdots a_n$, então, $p \mid a_k$ para algum $k \in \{1, 2, ..., n\}$.* □

Corolário 2.9 *Seja $n \in \mathbb{N}$. Se p, q_1, q_2, ..., q_{n-1} e q_n são números primos tais que $p \mid q_1 q_2 \cdots q_n$, então, $p = q_k$ para algum $k \in \{1, 2, ..., n\}$.* □

O próximo teorema estabelece um resultado que consta no Livro IX da Obra *Elementos* de Euclides: todo o número inteiro maior que 1 pode decompor-se, de modo único, num produto de primos. Compreende-se, assim, que os primos constituem os "tijolos"de que são feitos todos os números inteiros! Não surpreende, portanto, que os números primos tenham despertado e continuem a despertar a atenção de tantos matemáticos. Se por um lado se provaram muitos teoremas importantes relativos, por exemplo, à distribuição dos primos, muitos outros resultados igualmente notáveis permanecem ainda por provar!

Teorema 2.9 ***(Teorema Fundamental da Aritmética)*** *Todo o número $n > 1$ exprime-se como produto de um número finito de primos. Esta representação é única a menos da ordem de factores.*

Demonstração: Seja $n \in \mathbb{Z}^+$.

Existência. Se n é primo, temos que n se escreve como produto de um único factor primo.

Se n não é primo, existe $d \in \mathbb{Z}$ tal que $1 < d < n$ e $d \mid n$. Seja p_1 o menor inteiro positivo tal que $p_1 \mid n$. Então, p_1 é primo (de facto, se p_1 não fosse primo, existiria $p_1' \in \mathbb{Z}$ tal que $1 < p_1' < p_1$ e $p_1' \mid p_1$, e, portanto, $1 < p_1' < n$ e $p_1' \mid n$, o que contradiz o facto de p_1 ser o mais pequeno inteiro positivo nestas condições). Assim, existe $n_1 \in \mathbb{Z}$ tal que

$$n = p_1 n_1 \text{ em que } p_1 \text{ é primo e } 1 < n_1 < n.$$

Retomemos o raciocínio efectuado para n, aplicando-o agora a n_1. Concluímos que ou n_1 é primo (e, portanto, n é produto de dois números primos) ou n_1 não é primo e existem p_2 primo e $n_2 \in \mathbb{Z}^+$ tais que $n = p_1 p_2 n_2$ e $1 < n_2 < n_1 < n$.

Repetindo sucessivamente o raciocínio, obtemos uma cadeia decrescente de inteiros positivos

$$n > n_1 > n_2 > \cdots > 1$$

que tem um número finito de elementos, o que significa que, ao fim de um número finito de passos obtemos um número primo e, portanto,

$$n = p_1 p_2 \cdots p_k.$$

Unicidade (a menos da ordem dos factores). Sejam $r, s \in \mathbb{N}$ e p_1, p_2, ..., p_r, q_1, q_2, ..., q_s números primos tais que

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

Suponhamos, ainda, sem perda de generalidade, que $r \leq s$ e que

$$p_1 \leq p_2 \leq \cdots \leq p_r \text{ e } q_1 \leq q_2 \leq \cdots \leq q_s.$$

Como $p_1 \mid n$,

$$p_1 \mid q_1 q_2 \cdots q_s$$

e, portanto, pelo Corolário 2.9, existe $k \in \{1, 2, ..., s\}$ tal que $p_1 = q_k$. Logo, $q_1 \leq p_1$. Como $q_1 \mid n$, de modo análogo, concluímos que $p_1 \leq q_1$. Logo, $p_1 = q_1$. Então,

$$p_1 p_2 \cdots p_r = p_1 q_2 \cdots q_s,$$

pelo que

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

Repetindo o raciocínio sucessivamente ($r-1$ vezes) e tendo em conta que $r \leq s$, concluímos que se $r < s$,

$$1 = q_{r+1} q_{r+2} \cdots q_s > 1,$$

um absurdo. Logo, $r = s$ e as duas factorizações são iguais. □

Corolário 2.10 *Todo o número inteiro $n > 1$ pode escrever-se, de modo único, como*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

em que, para $i \in \{1, 2, ..., r\}$, $k_i \in \mathbb{N}$ e p_i é um número primo e

$$p_1 < p_2 < \cdots < p_r.$$

□

Proposição 2.1 *Se $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ é a factorização de $n > 1$ em números primos, então, o conjunto dos divisores positivos de n é o conjunto de todos os números da forma*

$$p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k} \text{ onde, para todo } i \in \{1, 2, ..., k\},\ 0 \leq c_i \leq a_i.$$

Demonstração: Exercício. □

A proposição anterior permite estabelecer um método para o cálculo do máximo divisor comum e do mínimo múltiplo comum de quaisquer inteiros maiores que 1. Este método assenta na decomposição de cada um dos inteiros no produto de números primos.

Proposição 2.2 *Sejam $a = \prod_{i=1}^{k} p_i^{a_i}$ e $b = \prod_{i=1}^{k} p_i^{b_i}$, onde, para todo $i \in \{1, 2, ..., k\}$, $a_i \geq 0$, $b_i \geq 0$ e p_i é primo.*

Para cada $i \in \{1, 2, ..., k\}$, sejam $c_i = \min\{a_i, b_i\}$ e $d_i = \max\{a_i, b_i\}$. Então,

$$\text{m.d.c.}(a,b) = \prod_{i=1}^{k} p_i^{c_i} \qquad e \qquad \text{m.m.c.}(a,b) = \prod_{i=1}^{k} p_i^{d_i}.$$

Demonstração: Exercício. □

Exemplo 2.6 *Consideremos os números* 990 *e* 462. *Para determinar o* m.d.c.(990, 462) *e o* m.m.c.(990, 462)*, começamos por factorizar os números dados em números primos. Como*

$$990 = 2 \times 3^2 \times 5 \times 11$$

e

$$462 = 2 \times 3 \times 7 \times 11,$$

concluímos que

$$\text{m.d.c.}(990, 462) = 2 \times 3 \times 5^0 \times 7^0 \times 11 = 66$$

e

$$\text{m.m.c.}(990, 462) = 2 \times 3^2 \times 5 \times 7 \times 11 = 6930.$$

Uma questão importante no estudo dos números primos é a de saber como reconhecer, de um modo expedito, se um dado inteiro maior do que 1 é um número primo. De seguida apresentamos um propriedade que pode ajudar a determinar se um dado número é ou não um número primo.

Proposição 2.3 *Todo o número composto $a \in \mathbb{N}$ tem um divisor primo p tal que $p \leq \sqrt{a}$.*

Demonstração: Seja $a = a_1 a_2$ com $a_1, a_2 \in \mathbb{N}\backslash\{1\}$. Suponhamos que $a_1 \leq a_2$. Então, terá que ser $a_1 \leq \sqrt{a}$. De facto,

$$a_1 > \sqrt{a} \Rightarrow a = a_1 a_2 \geq a_1 a_1 > \sqrt{a}\sqrt{a} = a,$$

o que é um absurdo.

Como $a_1 > 1$, existe p primo tal que $p \leq a_1$ e $p \mid a_1$. Logo, existe p primo tal que $p \leq \sqrt{a}$ e $p \mid a$. □

Exemplo 2.7 *Consideremos o número* 509. *Como*

$$22^2 = 484 \leq 509 \leq 529 = 23^2,$$

temos que

$$22 < \sqrt{509} < 23.$$

Os primos não superiores a $\sqrt{509}$ *são, assim, os números 2, 3, 5, 7, 11, 13, 17 e 19. Como qualquer um destes números não divide* 509, *podemos concluir que* 509 *é um número primo.*

Exemplo 2.8 *Consideremos o número* 2093. *Como*

$$45^2 = 2025 \leq 2093 \leq 2116 = 46^2,$$

temos que

$$45 < \sqrt{2093} < 46.$$

Os primos não superiores a $\sqrt{2093}$ *são, assim, os números 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 e 43. Verificamos que* $2 \nmid 2093$, $3 \nmid 2093$ *e* $5 \nmid 2093$, *mas,* $7 \mid 2093$. *De facto,*

$$2093 = 7 \times 299.$$

Consideremos então o número 299. Como

$$17 = \sqrt{289} < \sqrt{299} < \sqrt{324} = 18,$$

temos que os primos não superiores a $\sqrt{299}$ *são 2, 3, 5, 7, 11, 13 e 17. Simples cálculos mostram que* $2 \nmid 299$, $5 \nmid 299$, $7 \nmid 299$, $11 \nmid 299$ *e*

$$299 = 13 \times 23.$$

Como 23 é primo, concluímos que 2093 é um número composto e pode ser escrito como

$$2093 = 7 \times 13 \times 23.$$

Eratóstenes (276 - 194 a.C.), matemático, geógrafo e astrónomo grego, elaborou um algoritmo para determinar todos os números primos inferiores a um dado número natural n.

Este algoritmo, baseado na proposição anterior, ficou conhecido como *crivo de Eratóstenes* e consiste no seguinte:

(1) Listam-se todos os inteiros de 2 a n de acordo com a ordem usual;

(2) Eliminam-se, sistematicamente, todos os números compostos, cancelando todos os múltiplos de primos p, com p tais que $p \leq \sqrt{n}$;

(3) Os elementos restantes (i.e., os números que não passaram no crivo) são os **primos inferiores a** n.

Exemplo 2.9 *Determinemos os números primos inferiores a 100. Para isso, consideramos a lista de todos os números de 2 a 100:*

	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

A aplicação do passo 2 (cancelando, neste caso, todos os múltiplos de 2, de 3, de 5 e de 7) permite-nos eliminar todos os números compostos não superiores a 100:

	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		

Concluímos então que os 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 *e* 97.

Outra questão que se coloca é a de saber se existe um número primo maior do que todos os outros. A resposta foi encontrada por Euclides que provou a existência de uma infinidade de números primos.

Teorema 2.10 *Existe uma infinidade de números primos.*

Demonstração: Suponhamos que existe um número primo, p, maior que todos os outros primos, i.e., suponhamos que

$$2, 3, 5, 7, 11, ..., p \qquad (*)$$

é a sucessão finita de todos os números primos.

Consideremos $s = 2 \times 3 \times \cdots \times p$. Como $s + 1 > 1$, o inteiro $s + 1$ admite pelo menos um divisor primo q, ou seja, admite um divisor q que pertence à lista $(*)$. Logo,

$$q \mid s + 1 \text{ e } q \mid s$$

e, portanto,

$$q \mid (s+1) - s = 1.$$

Assim, $q = \pm 1$, o que contradiz o facto de q ser primo. A contradição resulta de termos suposto que existia um número finito de primos. Logo, existe uma infinidade de primos. □

2.2.2 Exercícios

Exercício 2.2.1. Mostre que:

(a) se p é primo e $p \mid a_1 a_2 ... a_n$, então $p \mid a_k$, para algum k tal que $1 \leq k \leq n$;

(b) se $p, q_1 q_2 ... q_n$ são todos primos e $p \mid q_1 q_2 ... q_n$, então $p = q_k$, para algum k tal que $1 \leq k \leq n$.

Exercício 2.2.2. Prove que:

(a) todo o primo da forma $3n + 1$ é da forma $6m + 1, (m, n \in \mathbb{N})$;

(b) o único primo da forma $n^3 - 1$, com $n \in \mathbb{N}$, é o 7; [Sugestão: Escreva $n^3 - 1$ como $(n-1)(n^2 + n + 1)$.]

(c) se $p \geq 5$ é um número primo, então $p^2 + 2$ é um número composto; [Sugestão: p é da forma $6k + 1$ ou $6k + 5$.]

(d) todo o inteiro da forma $n^4 + 4$, em que $n > 1$, é composto.

Exercício 2.2.3. Factorize os inteiros 105, 684, 1375 e 139 como produto de números primos.

Exercício 2.2.4. Sejam $m = p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$ e $n = p_1^{t_1} p_2^{t_2} ... p_k^{t_k}$, em que $p_1, p_2, ... p_k$ são primos distintos, $s_i \geq 0$ para $1 \leq i \leq k$ e $t_i \geq 0$ para $1 \leq i \leq k$. Para cada i, sejam $u_i = min\{s_i, t_i\}$ e $v_i = max\{s_i, t_i\}$. Prove que:

(a) m.d.c.$(m, n) = p_1^{u_1} p_2^{u_2} ... p_k^{u_k}$;

(b) m.m.c.$(m, n) = p_1^{v_1} p_2^{v_2} ... p_k^{v_k}$.

Exercício 2.2.5. Usando a factorização de 507 e 1287 em factores primos, determine m.d.c.$(507, 1287)$ e m.m.c.$(507, 1287)$.

Exercício 2.2.6. Verifique que 701 é um número primo, testando todos os primos $p \leq \sqrt{701}$ como possíveis divisores.

Exercício 2.2.7. Prove que:

(a) $\sqrt{p}$ é irracional para todo o primo p;

(b) se $a \in \mathbb{N}$ e $\sqrt[n]{a}$ é racional, então $\sqrt[n]{a}$ é um inteiro.

Exercício 2.2.8. (a) Mostre que é condição necessária para que um número $p \neq 2$ seja primo que satisfaça $p = 4n \pm 1, n \in \mathbb{N}$.

(b) Esta condição é também suficiente? Justifique.

Exercício 2.2.9. Mostre que há uma infinidade de primos da forma $6n + 5$.

2.3 equações diofantinas

Definição 2.6 *Uma* equação diofantina *é uma equação do tipo*

$$a_1 x_1^{n_1} + a_2 x_2^{n_2} + \cdots + a_k x_k^{n_k} = c,$$

onde, para cada $i \in \{1, 2, ..., k\}$, $n_i \in \mathbb{N}$, $a_i \in \mathbb{Z}$ *e* $c \in \mathbb{Z}$.

O nome "diofantina"é devido ao matemático Diophantus (250 a.C.), autor de uma série de 13 livros chamada *Arithmetica* onde a solubilidade algébrica de equações é estudada.

Nesta secção vamos estudar as equações diofantinas lineares com duas variáveis, i.e., equações do tipo

$$ax + by = c \text{ em que } a, b, c \in \mathbb{Z} \text{ e } a, b \neq 0.$$

Chama-se *solução da equação* $ax + by = c$ a qualquer par $(x', y') \in \mathbb{Z}^2$ de tal modo que $ax' + by' = c$. *Resolver a equação diofantina* $ax + by = c$ é determinar o conjunto das suas soluções. A equação $ax + by = c$ diz-se *solúvel* se admite pelo menos uma solução.

Exemplo 2.10 *A equação* $3x + 6y = 18$ *tem várias soluções. Por exemplo,* $(x_0, y_0) = (4, 1)$ *e* $(x_1, y_1) = (-6, 6)$ *são soluções da equação.*

Exemplo 2.11 *A equação* $2x + 10y = 17$ *não tem solução, já que, para quaisquer* $x, y \in \mathbb{Z}$, $2x + 10y$ *é um número par (nunca igual a 17, que é um número ímpar).*

Estes dois exemplos levantam duas questões: 1) Quando é que uma equação diofantina do tipo $ax + by = c$ tem solução? 2) Se uma equação diofantina tiver solução, será essa solução única ou haverá outras? Com os resultados seguintes responderemos a estas questões.

Proposição 2.4 *Sejam $a, b, c \in \mathbb{Z}$ com a e b não nulos. A equação diofantina $ax + by = c$ tem solução se e só se* m.d.c.$(a, b) \mid c$.

Demonstração: Seja $d =$ m.d.c.(a, b). Então, existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$. Mais ainda, como $d \mid a$ e $d \mid b$, temos que $d \mid ax + by$, para todos $x, y \in \mathbb{Z}$.

Por um lado, se $ax + by = c$ tem solução, então, trivialmente, $d \mid c$.

Por outro lado, se $d \mid c$, existe $k \in \mathbb{Z}$ tal que $c = dk = (ax_0 + by_0)k = a(x_0k) + b(y_0k)$ e, portanto, (x_0k, y_0k) é solução da equação diofantina $ax + by = c$. □

Proposição 2.5 *Se $ax + by = c$ admite uma solução, então, admite uma infinidade de soluções.*

Demonstração: Seja (x_0, y_0) uma solução particular de $ax + by = c$. Se (x', y') é também solução de $ax + by = c$, temos que

$$ax' + by' = ax_0 + by_0,$$

i.e.,

$$a(x' - x_0) = b(y_0 - y'). \qquad (*)$$

Seja $d =$ m.d.c.(a, b). Então,

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y').$$

Como $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, vem que $\frac{a}{d} \mid y_0 - y'$, ou seja, existe $t \in \mathbb{Z}$ tal que $y_0 - y' = \frac{a}{d}t$, i.e.,

$$y' = y_0 - \frac{a}{d}t.$$

Substituindo em $(*)$, vem que

$$a(x' - x_0) = b\frac{a}{d}t,$$

ou seja

$$x' = x_0 + \frac{b}{d}t.$$

Logo, se (x_0, y_0) é solução de $ax + by = c$, $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$ é também solução da equação, qualquer que seja $t \in \mathbb{Z}$. Assim, a equação $ax + by = c$ tem uma infinidade de soluções. □

É importante observar aqui que, seguindo a demonstração da proposição anterior, verificamos que não só provamos que temos uma infinidade de soluções, mas também provamos que todas as soluções são do mesmo tipo. Assim, faz sentido a seguinte definição.

Definição 2.7 *Chama-se* solução geral da equação $ax + by = c$ *ao par* (x', y') *em que*

$$\begin{cases} x' = x_0 + \frac{b}{d}t \\ y' = y_0 - \frac{a}{d}t \end{cases}, t \in \mathbb{Z},$$

sendo (x_0, y_0) *uma solução da equação* $ax + by = c$.

Exemplo 2.12 *Determine a solução geral da equação* $172x + 20y = 1000$.

Começamos por determinar m.d.c.$(172, 20)$. *Como*

$$\begin{aligned} 172 &= 8 \times 20 + 12 \\ 20 &= 1 \times 12 + 8 \\ 12 &= 1 \times 8 + 4 \\ 8 &= 2 \times 4 + 0, \end{aligned}$$

concluímos que

$$\text{m.d.c.}(172, 20) = 4.$$

Mais ainda, como $4 \mid 1000$, *concluímos que a equação admite soluções.*

Para determinar a solução geral da equação, começamos por determinar uma solução particular. Como

$$\begin{aligned} 4 &= 12 - 1 \times 8 \\ &= 12 - 1 \times (20 - 1 \times 12) \\ &= 2 \times 12 - 1 \times 20 \\ &= 2 \times (172 - 8 \times 20) - 1 \times 20 \\ &= 2 \times 172 - 17 \times 20, \end{aligned}$$

temos que

$$1000 = 4 \times 250 = 500 \times 172 + (-4250) \times 20$$

e, portanto, $(500, -4250)$ *é uma solução particular da equação.*

Logo, $(x', y') \in \mathbb{Z}^2$*, com*

$$\begin{cases} x' = 500 + \frac{20}{4}t \\ y' = -4250 - \frac{172}{4}t \end{cases}, t \in \mathbb{Z} \text{ , } i.e., \begin{cases} x' = 500 + 5t \\ y' = -4250 - 43t \end{cases}, t \in \mathbb{Z} ,$$

é a solução geral pretendida.

2.3.1 Exercícios

Exercício 2.3.1. Quais das seguintes equações diofantinas têm solução?

(a) $6x + 51y = 22$;

(b) $33x + 14y = 115$;

(c) $14x + 35y = 93$.

Exercício 2.3.2. Determine as soluções inteiras das seguintes equações diofantinas:

(a) $56x + 72y = 40$;

(b) $24x + 138y = 18$;

(c) $221x + 35y = 11$.

Exercício 2.3.3. Determine as soluções inteiras positivas das seguintes equações diofantinas:

(a) $18x + 5y = 48$;

(b) $54x + 21y = 906$;

(c) $5x - 11y = 29$.

Exercício 2.3.4. Exprima 100 como soma de dois inteiros positivos de modo que o primeiro seja divisível por 7 e o segundo seja divisível por 11.

Exercício 2.3.5. Determine as soluções inteiras não negativas da equação $39x + 26y = 104$.

Exercício 2.3.6. Justifique se a equação $30x + 17y = 300$ tem soluções inteiras positivas.

Exercício 2.3.7. De quantas maneiras se pode exprimir o número 4 como diferença de dois inteiros positivos, dos quais o primeiro é divisível por 8 e o segundo é múltiplo de 15? Indique três delas.

Exercício 2.3.8. Determine dois inteiros, um positivo e outro negativo, cuja soma é 42 e tais que um deles é múltiplo de 126 e o outro é divisível por 56.

Exercício 2.3.9. Diga, justificando, se é possível exprimir o número 104 como soma de dois inteiros positivos, tais que um deles é múltiplo de 6 e o outro é divisível por 11.

Exercício 2.3.10. (a) Para que valores inteiros de x e de y se tem $11x + 7y = 200$?

(b) Para que valores encontrados em (a) se tem $3x + y$ múltiplo de 3?

Exercício 2.3.11. Determine, caso existam, o menor inteiro não negativo x e o menor inteiro não negativo y, tais que $55x - 121y = 319$.

Exercício 2.3.12. Determine, caso existam, as soluções (x, y) da equação $297x + 349y = 3$, tais que $x, y \in \mathbb{Z}$, $x \in]-\infty, 557]$ e $y \in]-\infty, 417[$.

Exercício 2.3.13. Determine as soluções inteiras não negativas da equação $39x + 26y = 104$.

Exercício 2.3.14. Um teatro amador cobra 1,80 euros de entrada a cada adulto e 75 cêntimos a cada criança. Num espectáculo, as receitas totais somaram 90 euros. Sabendo que estiveram presentes mais adultos do que crianças, diga quantas pessoas estiveram a assistir a esse espectáculo.

Exercício 2.3.15. Um turista espanhol e um guia subiram a correr os degraus da pirâmide Keops perseguidos por um leão! O turista conseguia subir cinco degraus de uma só vez, o guia seis degraus e o leão sete degraus. A dada altura, o turista estava a um degrau do topo da pirâmide, o guia a nove degraus e o leão a dezanove degraus. Quantos degraus pode ter a pirâmide?

Exercício 2.3.16. Tenho um certo número de pérolas. Se fizer 76 pulseiras com o mesmo número de pérolas, faltam-me 50 pérolas para fazer a 77^a pulseira. Mas se fizer 78 pulseiras com o mesmo número de pérolas, uso a totalidade das pérolas que possuo. Qual o número mínimo de pérolas que tenho?

Exercício 2.3.17. Quando morreu, a idade de um homem era $\frac{1}{29}$ do ano do seu nascimento. Que idade tinha o homem em 1940?

2.4 congruências módulo n

2.4.1 conceitos e resultados básicos

A teoria das congruências é uma abordagem a questões de divisibilidade que assenta na aritmética dos restos. O conceito de congruência e a notação a ele associado foram introduzidos pelo matemático alemão Karl Friedrich Gauss (1777 - 1855) na sua obra *Disquisitiones Arithmeticas*. Com a publicação deste livro, aos 24 anos de idade, Gauss lançou os alicerces da Teoria de Números.

Citando Gauss, "se um inteiro positivo n mede a diferença entre dois números a e b então a e b dizem-se congruentes em relação a n. Caso contrário, a e b dizem-se incongruentes." Mais precisamente, temos a seguinte definição.

Definição 2.8 *Seja $n \in \mathbb{N}$. Diz-se que um inteiro a é* congruente módulo n com um inteiro b, *e escreve-se $a \equiv b (\mathrm{mod}\, n)$, se n é um divisor de $a - b$, i.e., se $a - b = nk$, para algum $k \in \mathbb{Z}$. Se a não é congruente módulo n com b, escreve-se $a \not\equiv b (\mathrm{mod}\, n)$ e diz-se que a é* incongruente com b módulo n.

Gauss explicou que foi levado a adoptar o símbolo $\equiv$ pela grande analogia desta relação com a igualdade algébrica. Mais adiante, precisaremos esta analogia evidenciando as diferenças mais relevantes!

Teorema 2.11 *Para quaisquer inteiros a e b,*

$$a \equiv b (\mathrm{mod}\, n) \iff a \text{ e } b \text{ têm o mesmo resto na divisão por } n.$$

Demonstração: Suponhamos que $a \equiv b (\mathrm{mod}\, n)$. Então, para algum $k \in \mathbb{Z}$, $a - b = nk$ ou, equivalentemente, $a = b + kn$, para algum $k \in \mathbb{Z}$.

Pelo Algoritmo da Divisão, existem $q, r \in \mathbb{Z}$ tais que

$$b = qn + r \quad \text{e} \quad 0 \leq r < n.$$

Logo,

$$a = qn + r + kn = (q + k)n + r \text{ e } 0 \leq r < n.$$

Assim, a e b têm o mesmo resto na divisão por n.

Reciprocamente, suponhamos que existem $q, q', r \in \mathbb{Z}$ tais que

$$a = qn + r, \ \ b = q'n + r \text{ e } 0 \leq r < n.$$

Então,

$$a - b = qn + r - q'n - r = (q - q')n,$$

pelo que

$$n \mid a - b,$$

ou seja,

$$a \equiv b (\text{mod}\, n).$$

□

Antes de estudarmos as propriedades da relação binária $\equiv (\text{mod}\, n)$ observemos que, fixado $n \in \mathbb{N}$, para qualquer inteiro $a \in \mathbb{Z}$ existem e estão univocamente determinados, inteiros $q, r \in \mathbb{Z}$ tais que

$$a = qn + r \text{ e } o \leq r < n,$$

i.e., tais que

$$a - r = qn \text{ e } 0 \leq r < n.$$

Portanto, a é congruente módulo n com o resto da sua divisão por n.

Assim, cada inteiro a é congruente módulo n com um e um só dos inteiros

$$0, 1, 2, \cdots, n - 2, n - 1.$$

Faz sentido, então, a seguinte definição.

Definição 2.9 *Seja $n \in \mathbb{N}$. Um conjunto de n inteiros $\{a_1, a_2, \cdots, a_n\}$ diz-se um* conjunto de resíduos módulo n *se todo o inteiro é congruente módulo n com um e um só a_k ($k \in \{1, 2, ..., n\}$).*

Exemplo 2.13 *Os conjuntos* $A = \{0, 1, 2, 3\}$ *e* $B = \{4, 50, -5, -3\}$ *são conjuntos de resíduos módulo 4. De facto, em relação ao conjunto* B*, como* $4 \equiv 0 (\mathrm{mod}\, 4)$*,* $-3 \equiv 1 (\mathrm{mod}\, 4)$*,* $50 \equiv 2 (\mathrm{mod}\, 4)$ *e* $-5 \equiv 3 (\mathrm{mod}\, 4)$*, todo o inteiro é congruente módulo 4 com um e um só dos elementos de* B*. No entanto, o conjunto* $\{0, 1, 2, 4\}$ *não é conjunto de resíduos módulo 4 pois* $3 \in \mathbb{Z}$ *e*

$$3 \not\equiv 0 (\mathrm{mod}\, 4),\ 3 \not\equiv 1 (\mathrm{mod}\, 4),\ 3 \not\equiv 2 (\mathrm{mod}\, 4) \text{ e } 3 \not\equiv 4 (\mathrm{mod}\, 4).$$

O próximo resultado estabelece propriedades da relação $\equiv (\mathrm{mod}\, n)$.

Teorema 2.12 *Sejam* $a, b, c, d \in \mathbb{Z}$*. Então,*

(i) $a \equiv a (\mathrm{mod}\, n)$*;*

(ii) $a \equiv b (\mathrm{mod}\, n) \Rightarrow b \equiv a (\mathrm{mod}\, n)$*;*

(iii) $a \equiv b (\mathrm{mod}\, n)$ *e* $b \equiv c (\mathrm{mod}\, n) \Rightarrow a \equiv c (\mathrm{mod}\, n)$*;*

(iv) $a \equiv b (\mathrm{mod}\, n)$ *e* $c \equiv d (\mathrm{mod}\, n) \Rightarrow \begin{cases} ac \equiv bd (\mathrm{mod}\, n) \\ a + c \equiv b + d (\mathrm{mod}\, n) \end{cases}$*;*

(v) $a \equiv b (\mathrm{mod}\, n) \Rightarrow \begin{cases} ac \equiv bc (\mathrm{mod}\, n) \\ a + c \equiv b + c (\mathrm{mod}\, n) \end{cases}$*;*

(vi) $a \equiv b (\mathrm{mod}\, n) \Rightarrow a^k \equiv b^k (\mathrm{mod}\, n), \forall k \in \mathbb{N}$.

Demonstração:

(i) Como $n \mid 0$ e $0 = a - a$, temos que $a \equiv a (\mathrm{mod}\, n)$;

(ii) Suponhamos que $a \equiv b (\mathrm{mod}\, n)$. Então, $n \mid a - b$. Logo, $n \mid b - a$ e, portanto, $b \equiv a (\mathrm{mod}\, n)$;

(iii) Suponhamos que $a \equiv b (\mathrm{mod}\, n)$ e $b \equiv c (\mathrm{mod}\, n)$. Então, $n \mid a - b$ e $n \mid b - c$, pelo que $n \mid (a - b) - (b - c)$, ou seja, $n \mid a - c$. Logo, $a \equiv c (\mathrm{mod}\, n)$;

(iv) Suponhamos que $a \equiv b (\text{mod}\, n)$ e $c \equiv d (\text{mod}\, n)$. Então, $n \mid a-b$ e $n \mid c-d$, pelo que, para todos $x, y \in \mathbb{Z}$, $n \mid (a-b)x + (c-d)y$. Por um lado, se considerarmos $x = 1$ e $y = -1$, obtemos que $n \mid (a+c)-(b+d)$ e, portanto, $a+c \equiv b+d (\text{mod}\, n)$. Por outro lado, considerando $x = c$ e $y = -b$, obtemos $n \mid ac - bd$, pelo que $ac \equiv bd (\text{mod}\, n)$;

(v) O resultado é imediato tendo em conta as alíneas (i) e (iv);

(vi) O resultado é imediato tendo em conta a alínea (iv) e aplicando o método de indução.

□

Observação. Tendo em conta (ii) do teorema anterior, sempre que $a \equiv b (\text{mod}\, n)$, diremos, sem ambiguidade, que os inteiros a e b são *congruentes módulo* n.

As alíneas (i), (ii) e (iii) do teorema anterior mostram que $\equiv (\text{mod}\, n)$ é uma relação de equivalência. Assim sendo, ela determina em $\mathbb{Z}$ uma partição em classes de equivalência. Vejamos como são constituídas estas classes. Sejam $a \in \mathbb{Z}$ e $[a]_n$ a classe de equivalência de a para a relação $\equiv (\text{mod}\, n)$. Seja r o resto da divisão de a por n. Como $a \equiv r (\text{mod}\, n)$, temos que $[a]_n = [r]_n$ e, portanto,

$$[a]_n = [r]_n = \{x \in \mathbb{Z} :\ x \equiv r (\text{mod}\, n)\} = \{x \in \mathbb{Z} :\ x = nk + r,\, k \in \mathbb{Z}\} = n\mathbb{Z} + r.$$

Assim, existem tantas classes de equivalência módulo n quanto o número de restos possíveis na divisão por n, i.e., exactamente n classes de equivalência módulo n, a saber: $[0]_n, [1]_n, ..., [n-1]_n$. O conjunto quociente $\mathbb{Z}/_{\equiv (\text{mod}\, n)} = \{[0]_n, [1]_n, ..., [n-1]_n\}$ representa-se por $\mathbb{Z}_n$ e as classes $[0]_n, [1]_n, ..., [n-1]_n$ designam-se por *inteiros módulo* n.

As alíneas (iv) e (v) mostram que a relação $\equiv (\text{mod}\, n)$ respeita a adição e a multiplicação de inteiros. Diz-se que $\equiv (\text{mod}\, n)$ é compatível com a adição e a multiplicação em $\mathbb{Z}$.

Apresentamos, de seguida, exemplo de duas questões de divisibilidade que se resolvem muito simplesmente recorrendo à relação $\equiv (\text{mod}\, n)$, para certo $n \in \mathbb{N}$.

1. Mostre que $41 \mid 2^{20} - 1$.

Note-se que $41 \mid 2^{20} - 1 \iff 2^{20} \equiv 1 (\mathrm{mod}\, 41)$.

Começamos por observar que

$$2^5 = 32 \equiv -9 (\mathrm{mod}\, 41)$$

e, portanto,

$$(2^5)^4 \equiv (-9)^4 (\mathrm{mod}\, 41). \qquad (1)$$

Como

$$(-9)^2 = 81 \equiv -1 (\mathrm{mod}\, 41),$$

segue-se que

$$(-9)^4 = ((-9)^2)^2 \equiv 1 (\mathrm{mod}\, 41). \qquad (2)$$

De (1) e (2), concluímos que

$$2^{20} \equiv 1 (\mathrm{mod}\, 41).$$

2. Determine o resto da divisão de $\sum_{n=1}^{100} n!$ por 12.

Como $4! = 24 \equiv 0 (\mathrm{mod}\, 12)$ temos que, para $n \geq 4$,

$$n! = n(n-1) \cdots 5 \cdot 4! \equiv 0 (\mathrm{mod}\, 12)$$

e, portanto, como $1! = 1 \equiv 1 (\mathrm{mod}\, 12)$, $2! = 2 \equiv 2 (\mathrm{mod}\, 12)$ e $3! = 6 \equiv 6 (\mathrm{mod}\, 12)$,

$$\sum_{n=1}^{100} n! = 1! + 2! + 3! + \sum_{n=4}^{100} n! \equiv 1 + 2 + 6 + 0 (\mathrm{mod}\, 12),$$

ou seja,

$$\sum_{n=1}^{100} n! \equiv 9 (\mathrm{mod}\, 12).$$

Assim, o resto da divisão de $\sum_{n=1}^{100} n!$ por 12 é 9.

As propriedades da relação $\equiv (\mathrm{mod}\, n)$ estabelecidas no Teorema 2.12 são trivialmente satisfeitas pela relação de igualdade em $\mathbb{Z}$. Mas, nem todas as propriedades da relação de igualdade são satisfeitas pela relação $\equiv (\mathrm{mod}\, n)$. A *lei do corte* e a *lei do anulamento do produto* são duas delas.

Lei do corte

Seja $n \in \mathbb{N}$. Será que, dados $a, b, c \in \mathbb{Z}$ e $a \neq 0$, se tem

$$ab \equiv ac (\mathrm{mod}\, n) \Longrightarrow b \equiv c (\mathrm{mod}\, n)?$$

Sejam $n = 6$, $a = 2$, $b = 4$, $c = 1$. Então,

$$ab \equiv ac (\mathrm{mod}\, n) \text{ e, no entanto, } b \not\equiv c (\mathrm{mod}\, n).$$

Portanto, a relação $\equiv (\mathrm{mod}\, n)$ não satisfaz a lei do corte. O próximo teorema permite estabelecer em que condições a lei do corte é válida.

Teorema 2.13 *Sejam $n \in \mathbb{N}$ e $a, b, c \in \mathbb{Z}$. Se $ca \equiv cb (\mathrm{mod}\, n)$, então, $a \equiv b (\mathrm{mod}\, \frac{n}{d})$, onde $d = \mathrm{m.d.c.}(c, n)$.*

Demonstração: Suponhamos que $ca \equiv cb (\mathrm{mod}\, n)$. Então, $n \mid ca - cb$, i.e.,

$$c(a - b) = kn \text{ para algum } k \in \mathbb{Z}. \qquad (*)$$

Como $n > 0$, existe $\mathrm{m.d.c.}(c, n)$. Seja $d = \mathrm{m.d.c.}(c, n)$. Então, existem $r, s \in \mathbb{Z}$ tais que

$$c = dr \text{ e } n = ds.$$

Substituindo em $(*)$, obtemos $dr(a - b) = kds$ e, portanto, $r(a - b) = ks$, para algum $k \in \mathbb{Z}$. Assim, temos que

$$s \mid r(a - b).$$

Como r e s são primos entre si (ver Corolário 2.4), concluímos, pelo Lema de Euclides, que $s \mid a - b$, ou seja,

$$a \equiv b (\mathrm{mod}\, s) \text{ onde } s = \frac{n}{d}.$$

□

A condição para a validade da lei do corte é estabelecida de imediato.

Corolário 2.11 *Sejam* $a, b, c \in \mathbb{Z}$. *Se* $ca \equiv cb (\mathrm{mod}\, n)$ *e* m.d.c.$(c, n) = 1$, *então,* $a \equiv b (\mathrm{mod}\, n)$. □

Lei do anulamento do produto
Seja $n \in \mathbb{N}$. Será que, dados $a, b \in \mathbb{Z}$, se tem

$$ab \equiv 0 (\mathrm{mod}\, n) \Longrightarrow a \equiv 0 (\mathrm{mod}\, n) \text{ ou } b \equiv 0 (\mathrm{mod}\, n)?$$

Como

$$2 \times 3 \equiv 0 (\mathrm{mod}\, 6),\ 2 \not\equiv 0 (\mathrm{mod}\, 6) \text{ e } 3 \not\equiv 0 (\mathrm{mod}\, n),$$

concluímos que a lei do anulamento do produto não é satisfeita pela relação $\equiv (\mathrm{mod}\, n)$. Vejamos em que condições é que ela é válida na aritmética das congruências.

Teorema 2.14 *Sejam* $a, b \in \mathbb{Z}$. *Se* $ab \equiv 0 (\mathrm{mod}\, n)$ *e* m.d.c.$(a, n) = 1$, *então,* $b \equiv 0 (\mathrm{mod}\, n)$.

Demonstração: Consequência imediata do Corolário 2.11, tendo em conta que $0 = a \times 0$. □

2.4.2 critérios de divisibilidade

Dados um inteiro a e um inteiro não nulo b, o Algoritmo da Divisão garante a existência de $q, r \in \mathbb{Z}$ tais que $a = bq + r$. De acordo com aquele algoritmo, a determinação de q e de r é simultânea, não se podendo calcular um sem calcular o outro. Existem, contudo, métodos que nos permitem determinar r sem necessitar de calcular q. Dado um inteiro positivo n, chama-se *critério de divisibilidade por* n a qualquer proposição que permite calcular, mediante um processo rápido e eficaz, o resto da divisão por n de um inteiro positivo a dada a sua representação decimal.

Se $a_0, a_1, ..., a_n \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e $a_n \neq 0$, o número

$$a = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_2 \times 10^2 + a_1 \times 10 + a_0$$

é um inteiro positivo com $n+1$ algarismos. Representamos este número por $\overline{a_n a_{n-1} \cdots a_2 a_1 a_0}$. Não havendo ambiguidade, não se coloca a barra. Por exemplo,

$$459 = 4 \times 10^2 + 5 \times 10 + 9$$

e

$$\overline{5p8} = 5 \times 10^2 + p \times 10 + 8.$$

A esta representação chamamos *representação decimal de* a.

Teorema 2.15 *Seja* $m \in \mathbb{N}$. *Se* $r_1, r_2, ..., r_{n-1}, r_n$ *são os restos da divisão de, respectivamente,* $10, 10^2, ..., 10^{n-1}, 10^n$ *por* m, *então,*

$$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_n r_n + a_{n-1} r_{n-1} + \cdots + a_2 r_2 + a_1 r_1 + a_0 (\text{mod}\, m).$$

Demonstração: A demonstração é imediata tendo em conta a representação decimal do número $\overline{a_n a_{n-1} \cdots a_2 a_1 a_0}$ e as propriedades apresentadas no Teorema 2.12. □

Exemplo 2.14 *Pretendemos determinar o resto da divisão de 1492 por 3.*

Como

$$10 \equiv 1 (\text{mod}\, 3),$$
$$10^2 = 100 \equiv 1 (\text{mod}\, 3),$$
$$10^3 = 1000 \equiv 1 (\text{mod}\, 3),$$

concluímos que

$$1 \times 10^3 + 4 \times 10^2 + 9 \times 10 + 2 \equiv 1 \times 1 + 4 \times 1 + 9 \times 1 + 2 (\text{mod}\, 3),$$

ou seja,

$$1492 \equiv 168 (\text{mod}\, 3).$$

Mas, $168 \equiv 0 (\text{mod}\, 3)$, *pelo que*

$$1492 \equiv 0 (\text{mod}\, 3).$$

Com base no Teorema 2.15, estabeleceremos, de seguida, critérios de divisibilidade para os divisores 2,5,3,9,4 e 11.

- $n = 2$.

  Como $10 \equiv 0 (\mathrm{mod}\, 2)$, temos que $10^i \equiv 0 (\mathrm{mod}\, 2)$, para qualquer inteiro $i \leq 1$. Logo,

  $$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_0 (\mathrm{mod}\, 2).$$

  Critério de divisibilidade por 2: O resto da divisão de um inteiro positivo a por 2 é o resto que se obtém dividindo por 2 o algarismo das unidades de a.

- $n = 5$.

  Como $10 \equiv 0 (\mathrm{mod}\, 5)$, temos que $10^i \equiv 0 (\mathrm{mod}\, 5)$, para qualquer inteiro $i \leq 1$. Logo,

  $$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_0 (\mathrm{mod}\, 5).$$

  Critério de divisibilidade por 5: O resto da divisão de um inteiro positivo a por 5 é o resto que se obtém dividindo por 5 o algarismo das unidades de a.

- $n = 3$.

  Como $10 \equiv 1 (\mathrm{mod}\, 3)$, temos que $10^i \equiv 1 (\mathrm{mod}\, 3)$, para qualquer inteiro $i \leq 1$. Logo,

  $$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 (\mathrm{mod}\, 3).$$

  Critério de divisibilidade por 3: O resto da divisão de um inteiro positivo a por 3 é o resto que se obtém dividindo por 3 a soma de todos os algarismos de a.

- $n = 9$.

  Como $10 \equiv 1 (\mathrm{mod}\, 9)$, temos que $10^i \equiv 1 (\mathrm{mod}\, 9)$, para qualquer inteiro $i \leq 1$. Logo,

  $$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 (\mathrm{mod}\, 9).$$

Critério de divisibilidade por 9: O resto da divisão de um inteiro positivo a por 9 é o resto que se obtém dividindo por 9 a soma de todos os algarismos de a.

- $n = 4$.

  Como $10 \equiv 2 (\mathrm{mod}\, 4)$, temos que $10^2 \equiv 0 (\mathrm{mod}\, 4)$ e, portanto, $10^i \equiv 0 (\mathrm{mod}\, 4)$, para qualquer inteiro $i \geq 2$. Logo,

  $$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv 2 \times a_1 + a_0 (\mathrm{mod}\, 4).$$

Critério de divisibilidade por 4: O resto da divisão de um inteiro positivo a por 4 é o resto que se obtém dividindo por 4 a soma do dobro do algarismo das dezenas de a com o algarismo das unidades de a.

- $n = 11$.

  Como $10 \equiv -1 (\mathrm{mod}\, 11)$, temos que $10^2 \equiv 1 (\mathrm{mod}\, 11)$ e, portanto,

  $$10^i \equiv (-1)^i (\mathrm{mod}\, 11),$$

  para qualquer inteiro $i \geq 1$. Logo,

  $$\overline{a_n a_{n-1} \cdots a_2 a_1 a_0} \equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) (\mathrm{mod}\, 11).$$

Critério de divisibilidade por 11: O resto da divisão de um inteiro positivo a por 11 é o resto que se obtém dividindo por 11 a diferença entre a soma dos algarismos de a de ordem par e a soma dos algarismos de a de ordem ímpar (considerando que o algarismo da unidades é de ordem par).

2.4.3 congruências lineares

Definição 2.10 *Chama-se* congruência linear *a toda a expressão da forma* $ax \equiv b (\mathrm{mod}\, n)$ *em que* $a, b \in \mathbb{Z}$, $a \neq 0$ *e* x *é um símbolo.*

Chama-se solução *da congruência linear* $ax \equiv b (\mathrm{mod}\, n)$ *a qualquer inteiro* x_0 *tal que "*$ax_0 \equiv b (\mathrm{mod}\, n)$*" é uma afirmação verdadeira.* Resolver *uma congruência linear é determinar o conjunto de todas as soluções dessa congruência linear.*

Exemplo 2.15 *A congruência linear* $4x \equiv 5 (\mathrm{mod}\, 6)$ *não tem soluções em* $\mathbb{Z}$*. De facto, para qualquer* $x_0 \in \mathbb{Z}$, $4x_0 - 5$ *é um número ímpar e, portanto, não divisível por 6.*

Exemplo 2.16 *A congruência linear* $3x \equiv 9 (\mathrm{mod}\, 12)$ *admite, entre outras, as soluções* $x_0 = 3$, $x_1 = -9$ *e* $x_2 = 7$*. Observe-se que* $x_0 \equiv x_1 (\mathrm{mod}\, 12)$ *e* $x_0 \not\equiv x_2 (\mathrm{mod}\, 12)$*, o que nos permite concluir que, de entre as soluções de uma congruência linear, existem soluções que são congruentes entre si e outras que não são congruentes entre si.*

Das equivalências

$$\begin{aligned} ax \equiv b (\mathrm{mod}\, n) &\iff n \mid ax - b \\ &\iff ax - b = ny \qquad (y \in \mathbb{Z}) \\ &\iff ax + (-n)y = b \qquad (y \in \mathbb{Z}), \end{aligned}$$

podemos afirmar que a existência de solução da congruência linear $ax \equiv b (\mathrm{mod}\, n)$ é equivalente à existência de solução da equação diofantina $ax + (-n)y = b$. Assim, temos o seguinte resultado.

Teorema 2.16 *Sejam* $a, b \in \mathbb{Z}$ *e* $a \neq 0$*. A congruência linear* $ax \equiv b (\mathrm{mod}\, n)$ *admite solução se e só se* m.d.c.$(a, n) \mid b$*.* □

A demonstração do teorema seguinte permite determinar o conjunto das soluções de uma dada congruência linear

Teorema 2.17 *Sejam* $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ *e* $d =$ m.d.c.(a, n)*. Se* x_0 *é solução da congruência linear* $ax \equiv b (\mathrm{mod}\, n)$*, então,*

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d}, \cdots,\ x_0 + \frac{(d-1)n}{d}$$

é a lista completa das soluções da congruência linear $ax \equiv b (\mathrm{mod}\, n)$*, não congruentes módulo* n *duas a duas.*

Demonstração: Se x_0 é solução da congruência linear então existe $y_0 \in \mathbb{Z}$ tal que (x_0, y_0) é solução da equação diofantina $ax - ny = b$. Assim, $(x_0 + \frac{-n}{d}k, y_0 - \frac{a}{d}k)$, com $k \in \mathbb{Z}$, é a solução geral daquela equação. Portanto, para cada $k \in \mathbb{Z}$, $x' = x_0 + \frac{-n}{d}k$ é solução da congruência linear dada.

Considerando $k \in \{-(d-1), -(d-2), ..., -1, 0\}$, obtemos as d soluções

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d}, \cdots,\ x_0 + \frac{(d-1)n}{d}$$

da congruência linear $ax \equiv b (\mathrm{mod}\, n)$.

Vejamos que: (a) Estas soluções não são congruentes módulo n duas a duas; (b) Não há mais do que d soluções não congruentes módulo n.

(a) Sejam $0 \leq t_2 < t_1 \leq d-1$ tais que

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 (\mathrm{mod}\, n).$$

Então,

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 (\mathrm{mod}\, n)$$

e, como m.d.c.$(\frac{n}{d}, n) = \frac{n}{d}$ e $\frac{\frac{n}{d}}{\frac{n}{d}} = d$,

$$t_1 \equiv t_2 (\mathrm{mod}\, d).$$

Assim, $d \mid t_1 - t_2$, o que é impossível pois $0 < t_1 - t_2 < d$. Logo,

$$x_0 + \frac{n}{d}t_1 \not\equiv x_0 + \frac{n}{d}t_2 (\mathrm{mod}\, n).$$

(b) Seja $t \in \mathbb{Z}$. Então, existem $q, r \in \mathbb{Z}$ tais que $-t = dq + r$ e $0 \leq r \leq d-1$. Logo,

$$\begin{aligned} x_0 + \tfrac{-n}{d}t &= x_0 + \tfrac{n}{d}(-t) \\ &= x_0 + \tfrac{n}{d}(dq + r) \\ &= x_0 + nq + \tfrac{n}{d}r \\ &\equiv x_0 + \tfrac{n}{d}r (\mathrm{mod}\, n). \end{aligned}$$

Como $0 \leq r \leq d-1$, $x_0 + \frac{-n}{d}t$ é congruente módulo n com um dos inteiros da lista apresentada. □

Corolário 2.12 *Se* m.d.c.$(a, n) = 1$*, então, a congruência linear* $ax \equiv b (\mathrm{mod}\, n)$ *tem uma e uma só solução módulo* n. □

Exemplo 2.17 *Na sequência do Teorema 2.16, a congruência linear*

$$4x \equiv 5 (\mathrm{mod}\, 6)$$

não admite soluções inteiras porque m.d.c.$(4,6) = 2$ *e* $2 \nmid 5$.

Exemplo 2.18 *Queremos resolver a congruência linear*

$$18x \equiv 30 (\mathrm{mod}\, 42).$$

Como m.d.c.$(18,42) = 6$ *e* $6 \mid 30$*, a congruência admite exactamente 6 soluções não congruentes módulo 42, duas a duas. Uma solução possível é 4 porque*

$$18 \times 4 = 72 \equiv 30 (\mathrm{mod}\, 42).$$

Logo, as 6 soluções referidas são

$$x \equiv 4 + \frac{42}{6} t (\mathrm{mod}\, 42), \qquad t \in \{0,1,2,3,4,5\},$$

i.e.,

$$x_1 \equiv 4 (\mathrm{mod}\, 42), \qquad x_2 \equiv 11 (\mathrm{mod}\, 42), \qquad x_3 \equiv 18 (\mathrm{mod}\, 42)$$
$$x_4 \equiv 25 (\mathrm{mod}\, 42), \qquad x_5 \equiv 32 (\mathrm{mod}\, 42), \qquad x_6 \equiv 39 (\mathrm{mod}\, 42).$$

O próximo resultado é fundamental para o estudo que faremos de seguida.

Teorema 2.18 *Seja* $ax \equiv b (\mathrm{mod}\, n)$ *uma congruência linear que admite soluções. Então, existem* $c \in \mathbb{Z}$ *e* $m \in \mathbb{N}$ *tais que* x_0 *é solução de* $ax \equiv b (\mathrm{mod}\, n)$ *se e só se* x_0 *é solução de* $x \equiv c (\mathrm{mod}\, m)$.

Demonstração: Sejam x_0 uma solução de $ax \equiv b (\mathrm{mod}\, n)$ e $d =$ m.d.c.(a,n). Então, $d \mid b$ e, portanto, pelo Teorema 2.13,

$$\frac{a}{d} x_0 \equiv \frac{b}{d} (\mathrm{mod}\, \frac{n}{d}). \qquad (\star)$$

Mais ainda, pelo Corolário 2.4, m.d.c.$(\frac{a}{d}, \frac{n}{d}) = 1$, pelo que existe $\left(\frac{a}{d}\right)^* \in \mathbb{Z}$ tal que

$$\frac{a}{d} \left(\frac{a}{d}\right)^* \equiv 1 (\mathrm{mod}\, \frac{n}{d}).$$

Assim, multiplicando ambos os membros de $(\star)$ por $\left(\frac{a}{d}\right)^*$, obtemos

$$x_0 \equiv \frac{b}{d}\left(\frac{a}{d}\right)^* (\text{mod } \frac{n}{d}),$$

i.e., x_0 é solução de $x \equiv c(\text{mod } m)$ com $c = \frac{b}{d}\left(\frac{a}{d}\right)^*$ e $m = \frac{n}{d}$. Reciprocamente, se x_0 é solução de $x \equiv \frac{b}{d}\left(\frac{a}{d}\right)^* (\text{mod } \frac{n}{d})$, é óbvio que x_0 é também solução de $ax \equiv b(\text{mod } n)$. □

2.4.4 Exercícios

Exercício 2.4.1. Prove que:

(a) se $a \equiv b(\text{mod } n)$ e $m \mid n$, então $a \equiv b(\text{mod } m)$;

(b) se $a \equiv b(\text{mod } n)$ e $c > 0$, então $ca \equiv cb(\text{mod } cn)$;

Exercício 2.4.2. Dê um exemplo que mostre que $a^2 \equiv b^2(\text{mod } n)$ não implica que $a \equiv b(\text{mod } n)$.

Exercício 2.4.3. Verifique que, se $a \equiv b(\text{mod } n)$, então, m.d.c.$(a, n) =$ m.d.c.(b, n).

Exercício 2.4.4. Para que valores de n se tem $25 \equiv 4(\text{mod } n)$?

Exercício 2.4.5. Justifique, se é verdadeira ou falsa cada uma das seguintes afirmações:

(a) $91 \equiv 0(\text{mod } 7)$;

(b) $-2 \equiv 2(\text{mod } 8)$;

(c) $17 \not\equiv 13(\text{mod } 2)$.

Exercício 2.4.6. Verifique se:

(a) o conjunto {-12, -4, 11, 13, 22, 32, 91} é um sistema completo de resíduos módulo 7;

(b) o conjunto {-2, -1, 0, 1, 2} é um sistema completo de resíduos módulo 5.

Exercício 2.4.7. Determine quais dos seguintes conjuntos são sistemas completos de resíduos módulo 4:

(a) {-2, -1, 0, 1};

(b) {0, 4, 8, 12};

(c) {-13, 4, 17, 13};

(d) {-5, 0, 6,22}.

Exercício 2.4.8. Determine um sistema completo de resíduos módulo 7 constituído apenas por números primos.

Exercício 2.4.9. Justifique se, em $\mathbb{Z}_6$, é verdadeira ou falsa cada uma das seguintes afirmações:

(a) $[89]_6 + [13]_6 = [0]_6$ e $[25]_6 \cap [16]_6 = [5]_6$;

(b) $[89]_6 + [13]_6 = [3]_6$ e $[25]_6 \cap [16]_6 = \emptyset$;

(c) $[89]_6 + [13]_6 = [0]_6$ e $[25]_6 \cap [16]_6 = \emptyset$.

Exercício 2.4.10. Indique quatro inteiros, dois positivos e dois negativos, na classe [3]:

(a) como elemento de $\mathbb{Z}_5$;

(b) como elemento de $\mathbb{Z}_6$.

Exercício 2.4.11. Indique, justificando, caso existam:

(a) um inteiro primo x tal que $x \in [-22]_{15} \cap [8]_{15}$;

(b) dois elementos x, y em $[20]_{15} \times ([39]_{15} + [-80]_{15})$ tais que $-40 < x < 0$ e $y > 80$;

(c) um número primo x tal que $x \equiv 6 \pmod{12}$;

(d) dois elementos distintos em $[-182]_9 \cap [20]_9$;

(e) o maior número par n tal que $-89 \equiv 5 \pmod{n}$;

(f) o maior inteiro x par, não positivo, tal que $x \equiv 50 \pmod{109}$.

Exercício 2.4.12. Indique os restos das divisões de 2^{50} e 41^{65} por 7.

Exercício 2.4.13. Calcule o resto de da divisão de 4^{215} por 9.

Exercício 2.4.14. Usando as propriedades das congruências, mostre que, para $n \geq 1$, se tem:

(a) 7 divide $5^{2n} + 3 \times 2^{5n-2}$;

(b) 13 divide $3^{n+2} + 4^{2n+1}$.

Exercício 2.4.15. Na divisão por 5, um inteiro p admite resto 3. Qual é o resto da divisão de $p^2 + 2p - 1$ por 5?

Exercício 2.4.16. Prove que:

(a) se a é um inteiro ímpar, então $a^2 \equiv 1 \pmod 8$;

(b) para todo o inteiro a, $a^3 \equiv 0, 1$ ou $6 \pmod 7$;

(c) para todo o inteiro a, $a^4 \equiv 0$ ou $1 \pmod 5$;

(d) para todo o inteiro a não divisível por 2 e por 3, tem-se $a^2 \equiv 1 \pmod{24}$.

Exercício 2.4.17. Determine o resto da divisão de $2357 \times 1036 + 499$ por 11.

Exercício 2.4.18. Mostre que $11^{10} \equiv 1 \pmod{100}$.

Exercício 2.4.19. Mostre que, para qualquer inteiro n, $n^3 - n = 3k$, para certo inteiro k.

Exercício 2.4.20. Prove que:

(a) dado um inteiro a, o dígito das unidades de a^2 é 0, 1, 4, 5, 6 ou 9;

(b) qualquer um dos inteiros 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 pode ser o dígito das unidades de a^3, para algum inteiro a;

(c) dado um inteiro a, o dígito das unidades de a^4 é 0, 1, 5 ou 6.

Exercício 2.4.21. Indique os dois últimos dígitos de 9^{9^9}.

Exercício 2.4.22. Trabalhando módulo 9 ou 11, indique os dígitos que faltam nos cálculos apresentados:

(a) $\overline{51840} \times \overline{273581} = \overline{1418243x040}$;

(b) $\overline{2x99561} = [3(523 + x)]^2$;

(c) $\overline{246x} = \overline{x} \times 493$;

(d) $512 \times \overline{1x53125} = 1000000000$.

Exercício 2.4.23. Deduza, no sistema decimal, o critério de divisibilidade por 6 e por 8.

Exercício 2.4.24. Determine os algarismos x, y de modo que o inteiro $\overline{3x5y}$ seja simultaneamente divisível por 4 e por 9.

Exercício 2.4.25. Determine os dígitos x e y tais que o número $\overline{34xx58y}$ é simultâneamente divisível por 9 e por 11.

Exercício 2.4.26. Determine os algarismos a e b tais que o número $\overline{279a15b0}$ é simultâneamente divisível por 4 e por 9.

Exercício 2.4.27. Determine os algarismos a e b tais que o número $\overline{56a21b}$ é simultâneamente divisível por 2 e por 11.

Exercício 2.4.28. Resolva as seguintes congruências lineares:

(a) $25x \equiv 15 (\mathrm{mod}\, 29)$;

(b) $5x \equiv 2 (\mathrm{mod}\, 26)$;

(c) $140x \equiv 133 (\mathrm{mod}\, 301)$.

Exercício 2.4.29. Diga, justificando, quais das congruências seguintes são solúveis e, para essas, indique a menor solução não negativa:

(a) $10x \equiv 14 (\mathrm{mod}\, 15)$;

(b) $10x \equiv 14 (\mathrm{mod}\, 16)$;

(c) $12x \equiv 7 (\mathrm{mod}\, 35)$;

(d) $60x \equiv -30 (\mathrm{mod}\, 165)$.

Exercício 2.4.30. Usando congruências, resolva a seguinte equação diofantina: $4x + 51y = 9$.

Sugestão: $4x \equiv 9 (\mathrm{mod}\, 51) \Leftrightarrow x = 15 + 51t$ e $51y \equiv 9 (\mathrm{mod}\, 4) \Leftrightarrow y = 3 + 4s$. Encontre a relação entre t e s.

Exercício 2.4.31. Relativamente à congruência linear $3x \equiv 2 (\mathrm{mod}\, 70)$, determine, caso exista:

(a) a maior solução negativa inferior a -96;

(b) uma solução que seja um número primo.

Exercício 2.4.32. Diga, justificando, se a congruência linear $14x \equiv 18 (\text{mod}\, 60)$ tem soluções pares.

Exercício 2.4.33. Relativamente à congruência linear $13x \equiv 17 (\text{mod}\, 42)$, determine, caso existam,

(a) as soluções negativas superiores a -100;

(b) uma solução par.

Exercício 2.4.34. Relativamente à congruência linear $16x \equiv 9 (\text{mod}\, 11)$, determine, justificando,

(a) duas soluções que sejam números primos;

(b) duas soluções que sejam números pares;

(c) o conjunto das soluções do intervalo $]-\infty, 337]$.

Exercício 2.4.35. Considere a congruência linear $18x \equiv 9 (\text{mod}\, 21)$.

(a) Verifique que a congruência linear dada admite solução.

(b) Quantas soluções tem a congruência linear $18x \equiv 9 (\text{mod}\, 21)$ no intervalo inteiro]-1, 80]? Calcule-as.

2.5 sistemas de congruências lineares

Definição 2.11 *Chama-se* sistema de congruências lineares *a um sistema do tipo*

$$(S) \quad \begin{cases} a_1 x \equiv b_1 (\text{mod}\, n_1) \\ a_2 x \equiv b_2 (\text{mod}\, n_2) \\ \vdots \\ a_k x \equiv b_k (\text{mod}\, n_k) \end{cases}$$

onde $k \in \mathbb{N}\backslash\{1\}$ *e, para todo* $i \in \{1, ..., k\}$, $a_i, b_i \in \mathbb{Z}$ *e* $n_i \in \mathbb{N}$.

Uma *solução de* (S) é qualquer inteiro que é solução de todas as congruências de (S).

Exemplo 2.19 *O sistema de congruências lineares*

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 4) \\ x \equiv 3 (\mathrm{mod}\, 6) \end{cases}$$

admite a solução $x_0 = 9$.

Nem todos os sistemas de congruências lineares admitem soluções. Vejamos o seguinte exemplo.

Exemplo 2.20 *O sistema de congruências lineares*

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 4) \\ x \equiv 4 (\mathrm{mod}\, 6) \end{cases}$$

não admite soluções inteiras. De facto, se x_0 *é solução do sistema, temos que existem* $q_1, q_2 \in \mathbb{Z}$ *tais que*

$$x_0 = 4q_1 + 1 \qquad e \qquad x_0 = 6q_2 + 4.$$

Assim,

$$4q_1 + 1 = 6q_2 + 4$$

i.e.,

$$4q_1 - 6q_2 = 3$$

e, portanto, a equação diofantina

$$4x - 6y = 3$$

é solúvel, ou seja, $2 = \mathrm{m.d.c.}(4, 6) \mid 3$, *o que é um absurdo. O absurdo resultou de termos suposto que* x_0 *é solução do sistema. Logo, o sistema apresentado não admite soluções.*

Definição 2.12 *Um sistema de congruências lineares que admite solução diz-se um* sistema solúvel.

Dois sistemas de congruências lineares dizem-se sistemas equivalentes *se tiverem o mesmo conjunto solução.*

Os sistemas de congruências lineares podem ter um papel relevante na resolução de congruências lineares. Vejamos o seguinte exemplo.

Exemplo 2.21 *Pretende-se resolver a congruência linear*

$$17x \equiv 9 (\mathrm{mod}\, 276).$$

Sabemos que $276 = 2^2 \times 3 \times 23$. *Como* m.d.c.$(17, 276) = 1$, *a congruência linear admite uma e uma só solução módulo 276. Como*

$$17 \times 33 = 561 \equiv 9 (\mathrm{mod}\, 276),$$

temos que essa solução é $x \equiv 33 (\mathrm{mod}\, 276)$. *Observamos agora que esta solução é a mesma do sistema*

$$(S) \begin{cases} 17x \equiv 9 (\mathrm{mod}\, 3) \\ 17x \equiv 9 (\mathrm{mod}\, 4) \\ 17x \equiv 9 (\mathrm{mod}\, 23) \end{cases},$$

i.e., é a mesma do sistema

$$\begin{cases} 2x \equiv 0 (\mathrm{mod}\, 3) \\ x \equiv 1 (\mathrm{mod}\, 4) \\ 17x \equiv 9 (\mathrm{mod}\, 23) \end{cases}.$$

Como 2 *e* 3 *são primos entre si, podemos aplicar a lei do corte na primeira congruência do sistema. Assim, o sistema* (S) *tem as mesmas soluções que o sistema*

$$\begin{cases} x \equiv 0 (\mathrm{mod}\, 3) \\ x \equiv 1 (\mathrm{mod}\, 4) \\ 17x \equiv 9 (\mathrm{mod}\, 23) \end{cases}.$$

Procuremos um inteiro que seja simultaneamente solução das três congruências lineares. Como a primeira congruência admite solução, temos que existe $k \in \mathbb{Z}$ *tal que*

$$x = 3k.$$

Pretendemos que k *seja tal que* $x = 3k$ *é também solução da segunda congruência linear, i.e., seja tal que* $3k \equiv 1 (\mathrm{mod}\, 4)$. *Temos:*

$$\begin{aligned} 3k \equiv 1 (\mathrm{mod}\, 4) &\Rightarrow k \equiv 3 (\mathrm{mod}\, 4) \\ &\Rightarrow 4 \mid k - 3 \\ &\Rightarrow k = 4l + 3 \qquad (l \in \mathbb{Z}) \\ &\Rightarrow x (= 3k) = 12l + 9. \end{aligned}$$

Agora, procuremos l tal que $x = 12l + 9$ seja também solução da terceira congruência linear,i.e., tal que $17(12l + 9) \equiv 9 (\mathrm{mod}\, 23)$. *Temos*

$$\begin{aligned} 17(12l + 9) \equiv 9(\mathrm{mod}\, 23) \quad &\Rightarrow 17 \times 12l \equiv 9 - 9 \times 17(\mathrm{mod}\, 23) \\ &\Rightarrow 17 \times 12l \equiv 9 \times (-16)(\mathrm{mod}\, 23) \\ &\Rightarrow 17 \times 12l \equiv 17(\mathrm{mod}\, 23) \\ &\Rightarrow 12l \equiv 1(\mathrm{mod}\, 23) \\ &\Rightarrow l \equiv 2(\mathrm{mod}\, 23) \\ &\Rightarrow l \equiv 23q + 2 \\ &\Rightarrow x = 12l + 9 = 12(23q + 2) + 9 = 12(23q + 2) + 9 = 276q + 33 \end{aligned}$$

Logo,

$$x \equiv 33(\mathrm{mod}\, 276).$$

Estamos em condições de concluir que a congruência dada inicialmente e o sistema (S) são equivalentes, pois têm o mesmo conjunto de soluções.

Apresentado este exemplo, levanta-se a questão de saber se qualquer congruência linear com solução é ou não equivalente a um sistema de congruências lineares solúvel. A proposição seguinte prova que a situação apresentada no exemplo anterior não é uma coincidência.

Proposição 2.6 *Sejam $n \in \mathbb{N}$ e*

$$n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$$

a factorização de n em factores primos distintos $p_1, p_2, ..., p_k$. Então, para quaisquer inteiros a e b, x_0 é solução da congruência linear $ax \equiv b(\mathrm{mod}\, n)$ se e só se x_0 é solução do sistema

$$(S) \quad \begin{cases} ax \equiv b(\mathrm{mod}\, p_1^{m_1}) \\ ax \equiv b(\mathrm{mod}\, p_2^{m_2}) \\ \vdots \\ ax \equiv b(\mathrm{mod}\, p_k^{m_k}) \end{cases}$$

Demonstração: Suponhamos que x_0 é solução de $ax \equiv b(\mathrm{mod}\, n)$. Então, $n \mid (ax_0 - b)$. Como, para cada $i \in \{1, 2, ..., k\}$, $p_i^{m_i} \mid n$, temos que $p_i^{m_i} \mid (ax_0 - b)$ e, portanto, x_0 é solução das congruências lineares $ax \equiv b(\mathrm{mod}\, p_i^{m_i})$, com $i \in \{1, 2, ..., k\}$.

Reciprocamente, suponhamos que x_0 é solução do sistema (S). Então, para cada $i_{\in}\{1, 2, ..., k\}$, $p_i^{m_i} \mid (ax_0 - b)$. Como $p_1^{m_1}, p_2^{m_2}, \cdots, p_k^{m_k}$ são todos primos entre si dois a dois, aplicando o Corolário 2.5, concluímos que

$$n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \mid (ax_0 - b).$$

Logo, x_0 é solução da congruência linear $ax \equiv b(\mathrm{mod}\, n)$. □

Como determinar as soluções de um sistema de congruências lineares (S) que admita solução?

Se (S) admite soluções, tendo em conta o Teorema 2.18, o conjunto de soluções de (S) é o conjunto de soluções de um sistema

$$(S') \qquad \begin{cases} x \equiv c_1(\mathrm{mod}\, m_1) \\ x \equiv c_2(\mathrm{mod}\, m_2) \\ \vdots \\ x \equiv c_k(\mathrm{mod}\, m_k) \end{cases}$$

onde, para cada $i \in \{1, ..., k\}$, $c_i \in \mathbb{Z}$ e $m_i \in \mathbb{N}$. Assim, o problema de encontrar as soluções de um sistema de congruências lineares solúvel reduz-se ao problema de encontrar as soluções de um sistema do tipo de (S').

Aprendemos, de seguida, como calcular as soluções de qualquer sistema de congruências lineares que admite solução. Para tal, começamos por provar o seguinte teorema, cuja origem remonta ao século I (Problema de Sun-Tsu adiante apresentado).

Teorema 2.19 (Teorema Chinês dos Restos) *Sejam* $k \in \mathbb{N}\backslash\{1\}$, $a_1, a_2, ..., a_k \in \mathbb{Z}$ *e* $n_1, n_2, ..., n_k \in \mathbb{N}$ *tais que*

$$(\forall i, j \in \{1, ..., k\}) \qquad i \neq j \Longrightarrow \mathrm{m.d.c.}(n_i, n_j) = 1.$$

Então, o sistema de congruências lineares

$$(S)\begin{cases} x \equiv a_1 (\mathrm{mod}\, n_1) \\ x \equiv a_2 (\mathrm{mod}\, n_2) \\ \vdots \\ x \equiv a_k (\mathrm{mod}\, n_k) \end{cases}$$

tem uma e uma só solução módulo $n_1 n_2 \cdots n_k$.

Demonstração: Seja $n = n_1 \times n_2 \times \cdots \times n_k$. Para cada $i \in \{1, 2, ..., k\}$, seja $N_i = \frac{n}{n_i} = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$. Como, para $i \neq j$, n_i e n_j são primos entre si, também m.d.c.$(N_i, n_i) = 1$ e, portanto, para cada i, a congruência linear $N_i x \equiv 1 (\mathrm{mod}\, n_i)$ admite solução única módulo n_i. Seja ela x_i. Vamos provar que o inteiro

$$x_0 = x_1 N_1 a_1 + x_2 N_2 a_2 + \cdots + x_k N_k a_k$$

é solução de (S). Comecemos por observar que, para $r, i \in \{1, 2, ..., k\}$ e $r \neq i$, como $n_r \mid N_i$, $N_i \equiv 0 (\mathrm{mod}\, n_r)$ e, portanto,

$$x_0 = x_1 N_1 a_1 + x_2 N_2 a_2 + \cdots + x_k N_k a_k \equiv a_r N_r x_r (\mathrm{mod}\, n_r).$$

Como x_r é solução de $N_r x \equiv 1 (\mathrm{mod}\, n_r)$, obtemos

$$x_0 \equiv a_r (\mathrm{mod}\, n_r).$$

Portanto, o sistema (S) admite a solução x_0.

Suponhamos de seguida que x' é outra solução de (S). Então,

$$x_0 \equiv x' (\mathrm{mod}\, n_r),$$

para qualquer $r \in \{1, 2, ..., k\}$ e, portanto, $n_r \mid x_0 - x'$, para cada $r \in \{1, 2, ..., k\}$. Como m.d.c.$(n_i, n_j) = 1$ $(i \neq j)$, obtemos, pelo Corolário 2.5, $n_1 n_2 \cdots n_k \mid x_0 - x'$. Assim, $x_0 \equiv x' (\mathrm{mod}\, n)$. □

O último resultado desta secção, que apresentamos de seguida, foi provado no séc. VII d.C. por Yih-Hing e generaliza o Teorema Chinês dos Restos para o caso onde os valores dos naturais n_i que definem as congruências não são necessariamente primos entre si.

Teorema 2.20 *Sejam $k \in \mathbb{N}\backslash\{1\}$, $a_1, a_2, ..., a_k \in \mathbb{Z}$ e $n_1, n_2, ..., n_k \in \mathbb{N}$ Então, o sistema de congruências lineares*

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, n_1) \\ x \equiv a_2 (\mathrm{mod}\, n_2) \\ \vdots \\ x \equiv a_k (\mathrm{mod}\, n_k) \end{cases}$$

tem solução se e só se, para todos $i, j \in \{1, ..., k\}$,

$$\text{m.d.c.}(n_i, n_j) \mid (a_j - a_i).$$

Além disso, se o sistema tiver solução, ela é única módulo n, onde n é o mínimo múltiplo comum de $n_1, n_2, \cdots, n_k$.

Demonstração: Suponhamos que m.d.c.$(n_i, n_j) \mid (a_j - a_i)$. Queremos provar que o sistema dado admite solução. A ideia é construir, a partir do sistema dado, um sistema nas condições do Teorema Chinês dos Restos, fazendo uso da Proposição 2.6. Se $n_i = p_{i_1}^{m_{i_1}} p_{i_2}^{m_{i_2}} \cdots p_{i_r}^{m_{i_r}}$ é a factorização de n_i (para cada $i \in \{1, 2, ..., k\}$) em factores primos, substituímos cada congruência linear $x \equiv a_i (\mathrm{mod}\, n_i)$ pelo sistema de congruências lineares

$$\begin{cases} x \equiv a_i (\mathrm{mod}\, p_{i_1}^{m_{i_1}}) \\ x \equiv a_i (\mathrm{mod}\, p_{i_2}^{m_{i_2}}) \\ \vdots \\ x \equiv a_i (\mathrm{mod}\, p_{i_r}^{m_{i_r}}) \end{cases}$$

que, pela Proposição 2.6, lhe é equivalente. Obtemos assim um sistema equivalente ao primeiro, no qual todos os naturais que definem as congruências são potências de primos mas não são, necessariamente, primos entre si. Seja p um número primo da lista de primos obtidos na decomposição dos naturais n_i ($i \in \{1, 2, ..., k\}$) e seja p^e a maior potência de p que ocorre nas referidas decomposições. Seja n_i ($i \in \{1, 2, ..., k\}$) um dos naturais que é divisível por p^e. Assim, se $p^f \mid n_j$, temos que $f \leq e$ e, portanto, $p^f \mid n_i$. Então, $p^f \mid$ m.d.c.(n_i, n_j) e, portanto, $p^f \mid (a_i - a_j)$. Logo, se x_0 é solução de $x \equiv a_i (\mathrm{mod}\, p^e)$, então, também o será de $x \equiv a_i (\mathrm{mod}\, p^f)$ e de $x \equiv a_j (\mathrm{mod}\, p^f)$. portanto, se eliminarmos do sistema as congruências lineares módulo p^l, em que $l < e$, obtemos um sistema equivalente

ao inicial. O sistema obtido pela eliminação destas congruências é, pelo Teorema Chinês dos Restos, um sistema solúvel.

Suponhamos agora que existe uma solução x_0 do sistema dado. Então, $x_0 \equiv a_i (\mathrm{mod}\, n_i)$ para qualquer $i \in \{1, 2, ..., k\}$ e, portanto, $n_i \mid (x_0 - a_i)$, para cada $i \in \{1, 2, ..., k\}$. Para cada $i, j \in \{1, 2, ..., k\}$ tais que $i \neq j$, sejam $n_{ij} = \text{m.d.c.}(n_i, n_j)$. Então, $n_{ij} \mid n_i$ e $n_{ij} \mid n_j$ e, portanto, $n_{ij} \mid (x - a_j) - (x - a_i)$, ou seja, $n_{ij} \mid a_j - a_i$.

Finalmente, provemos que, se o sistema tiver solução, ela é única módulo mínimo múltiplo comum de $n_1, n_2, \cdots, n_k$. Seja x_0 uma solução do sistema. Se x é também solução do sistema, então, $x \equiv x_0 (\mathrm{mod}\, n_i)$, para cada $i \in \{1, 2, ..., k\}$, i.e., $n_i \mid x - x_0$, para cada $i \in \{1, 2, ..., k\}$. Logo, sendo n o mínimo múltiplo comum de $n_1, n_2, ..., n_k$, $n \mid x - x_0$ e, portanto, $x \equiv x_0 (\mathrm{mod}\, n)$. □

Terminamos com alguns exemplos de resolução de sistemas de congruências lineares.

Exemplo 2.22 ***Problema de Sun-Tsu*** (séc. I): Encontre um número que tem resto 2, 3 e 2 na divisão por 3, 5 e 7, respectivamente.

O problema traduz-se na resolução do seguinte sistema de congruências lineares

$$\begin{cases} x \equiv 2 (\mathrm{mod}\, 3) \\ x \equiv 3 (\mathrm{mod}\, 5) \\ x \equiv 2 (\mathrm{mod}\, 7) \end{cases}.$$

Resolvemo-lo utilizando o Teorema Chinês dos Restos. Sejam $n = 3 \times 5 \times 7 = 105$ *e*

$$N_1 = \frac{n}{3} = 35; \qquad N_2 = \frac{n}{5} = 21; \qquad N_3 = \frac{n}{7} = 15.$$

Como $\text{m.d.c.}(35, 3) = \text{m.d.c.}(21, 5) = \text{m.d.c.}(15, 7) = 1$*, temos que cada uma das congruências lineares*

$$35x \equiv 1 (\mathrm{mod}\, 3),$$

$$21x \equiv 1 (\mathrm{mod}\, 5),$$

$$15x \equiv 1 (\mathrm{mod}\, 7)$$

admite uma e uma só solução módulo 3, 5 e 7, respectivamente, a saber,

$$x_1 = 2, \qquad x_2 = 1 \qquad e \qquad x_3 = 1,$$

respectivamente. Então, pelo Teorema Chinês dos Restos,

$$x_0 = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233$$

é uma solução do sistema inicial. Logo, a única solução do sistema módulo 105 é

$$x' \equiv 233 (\text{mod}\, 105),$$

ou seja, é

$$x' \equiv 23 (\text{mod}\, 105).$$

Exemplo 2.23 *Pretende-se resolver o seguinte sistema*

$$(S) \qquad \begin{cases} x \equiv 2 (\text{mod}\, 4) \\ x \equiv 4 (\text{mod}\, 6) \\ x \equiv 1 (\text{mod}\, 3) \end{cases}.$$

Como 4 *e* 6 *não são primos entre si, não podemos resolver o sistema pelo Teorema Chinês dos Restos. No entanto, dado que*

$$\text{m.d.c.}(6,4) = 2 \mid 2 = 4-2, \qquad \text{m.d.c.}(6,3) = 3 \mid 3 = 4-1 \qquad e \qquad \text{m.d.c.}(4,3) = 1 \mid 5 = 6-1,$$

o Teorema 2.20 garante que o sistema tem uma única solução módulo $\text{m.m.c.}(4,6,3) = 12$. *Seguindo a demonstração do Teorema 2.20, concluímos que o sistema dado é equivalente ao sistema do sistema*

$$(S_1) \qquad \begin{cases} x \equiv 2 (\text{mod}\, 4) \\ x \equiv 4 (\text{mod}\, 2) \\ x \equiv 4 (\text{mod}\, 3) \\ x \equiv 1 (\text{mod}\, 3) \end{cases}$$

que é equivalente ao sistema

$$(S_2) \qquad \begin{cases} x \equiv 2 (\text{mod}\, 4) \\ x \equiv 1 (\text{mod}\, 3) \end{cases}.$$

Resolvemos agora o sistema (S_2) *pelo Teorema Chinês dos Restos. Sejam* $n = 12$, $N_1 = 3$ *e* $N_2 = 4$. *A congruência* $3x \equiv 1 (\text{mod}\, 4)$ *tem uma só solução módulo 4, a saber* $x_1 = 3$. *A congruência* $4x \equiv 1 (\text{mod}\, 3)$ *tem uma só solução módulo 3, a saber* $x_2 = 1$. *Assim,*

$$x_0 = 2 \times 3 \times 3 + 1 \times 4 \times 1 = 22$$

é uma solução do sistema (S_1). *Como* $22 \equiv 10 (\mathrm{mod}\, 12)$ *temos que* x' *é solução do sistema* (S_2) *se e só se*

$$x' \equiv 10 (\mathrm{mod}\, 12).$$

Logo, o conjunto das soluções do sistema (S) *é*

$$\{10 + 12t : t \in \mathbb{Z}\}.$$

2.5.1 Exercícios

Exercício 2.5.1. Resolva os seguintes sistemas de congruências lineares:

(a) $\begin{cases} x \equiv 1 (\mathrm{mod}\, 3) \\ x \equiv 2 (\mathrm{mod}\, 5) \\ x \equiv 3 (\mathrm{mod}\, 7) \end{cases}$; (b) $\begin{cases} 2x \equiv 1 (\mathrm{mod}\, 5) \\ 3x \equiv 9 (\mathrm{mod}\, 6) \\ 4x \equiv 1 (\mathrm{mod}\, 7) \\ 5x \equiv 9 (\mathrm{mod}\, 11) \end{cases}$; (c) $\begin{cases} x \equiv 2 (\mathrm{mod}\, 5) \\ x \equiv 3 (\mathrm{mod}\, 6) \\ x \equiv 4 (\mathrm{mod}\, 7) \end{cases}$.

(d) $\begin{cases} x \equiv 3 (\mathrm{mod}\, 11) \\ x \equiv 6 (\mathrm{mod}\, 8) \end{cases}$; (e) $\begin{cases} x \equiv 1 (\mathrm{mod}\, 2) \\ x \equiv 2 (\mathrm{mod}\, 5) \\ x \equiv 5 (\mathrm{mod}\, 7) \end{cases}$.

Exercício 2.5.2. Resolva os seguintes sistemas de congruências lineares:

(a) $\begin{cases} x \equiv 2 (\mathrm{mod}\, 3) \\ x \equiv 4 (\mathrm{mod}\, 5) \\ x \equiv 1 (\mathrm{mod}\, 2) \end{cases}$; (b) $\begin{cases} 3x \equiv 2 (\mathrm{mod}\, 5) \\ 2x \equiv 4 (\mathrm{mod}\, 6) \\ x \equiv 1 (\mathrm{mod}\, 2) \end{cases}$.

Exercício 2.5.3. Utilizando o Teorema Chinês dos Restos, resolva a congruência $17x \equiv 5 (\mathrm{mod}\, 42)$.

Exercício 2.5.4. Determine o menor inteiro $a > 2$ tal que $2 \mid a$, $3 \mid a+1$, $4 \mid a+2$, $5 \mid a+3$ e $6 \mid a+4$.

Exercício 2.5.5. Quando se retiram 2, 3, 4, 5 ovos de cada vez de um determinado cesto, ficam, respectivamente, 1, 2, 3, 4 ovos no cesto. Ao retirar 7 ovos de uma só vez, não sobra qualquer ovo no cesto. Qual o menor número de ovos que o cesto pode conter?

Exercício 2.5.6. Um bando de 17 piratas roubou um saco de moedas. Ao tentarem dividir igualmente por todos eles a fortuna roubada, deram conta que sobravam 3 moedas. Lutaram, para ver quem ficava com as três moedas e, nessa luta, morreu um pirata. Distribuíram, de novo, as moedas por todos e, desta vez, sobraram 10 moedas. Tendo havido nova luta, mais um pirata morreu. Desta vez, a fortuna pôde ser distribuída, na íntegra, por todos! Qual é o número mínimo de moedas que o saco roubado poderia ter contido?

Exercício 2.5.7. Recorrendo ao Teorema Chinês dos Restos, determine as soluções inteiras da congruência linear $19x \equiv 4 (\mathrm{mod}\, 84)$ que pertençam ao intervalo $]-200, 284]$.

Exercício 2.5.8. Um inteiro positivo a dividido por 5 dá resto 3 e dividido por 9 dá resto 4.

(a) Determine o resto da divisão de a por 45.

(b) Calcule os inteiros positivos ímpares, compreendidos entre 100 e 300, que têm, na divisão por 45, o mesmo resto que a.

Exercício 2.5.9. Determine os inteiros positivos x inferiores a 336 e tais que $x \equiv 2 (\mathrm{mod}\, 8)$, $x \equiv 1 (\mathrm{mod}\, 7)$ $x \equiv 2 (\mathrm{mod}\, 6)$.

Exercício 2.5.10. Aplicando o Teorema Chinês dos Restos, indique três inteiros n, dos quais um é negativo e dois são positivos, para os quais se tem, simultaneamente, $3 \mid n$, $5 \mid (n+2)$ e o resto da divisão de $n-3$ por 9 é 6.

Exercício 2.5.11. Recorrendo ao Teorema Chinês dos Restos, resolva a congruência linear $14x \equiv 18 (\mathrm{mod}\, 60)$.

2.6 alguns teoremas relevantes na teoria de números

2.6.1 Pequeno Teorema de Fermat

Em 1640, numa carta a Bessy, funcionário da Casa da Moeda francesa, Fermat escreveu: *"Se p é primo e a é um inteiro não divisível por p, então, p divide $a^{p-1}-1$."* Na mesma carta acrescentou ainda que não mandava a demonstração, pois ela era bastante longa. Quase 100 anos depois, em 1736, esta afirmação foi provada por Euler (na realidade, tudo leva a crer que já Leibnitz a tinha provado em 1683, mas não há qualquer prova escrita). Este resultado ficou conhecido na história como o Pequeno Teorema de Fermat.

Teorema 2.21 (Pequeno Teorema de Fermat) *Se p é primo e a é um inteiro não divisível por p, então, $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.*

Demonstração: Considerem-se os seguintes $p-1$ múltiplos de a:

$$a \qquad 2a \qquad 3a \qquad \cdots \qquad (p-1)a. \qquad\qquad (*)$$

Observamos que, como p não divide a, se tem, para todos $r, s \in \{1, 2, ..., p-1\}$, que

$$ra \not\equiv sa (\mathrm{mod}\, p) \qquad \mathrm{e} \qquad ra \not\equiv 0 (\mathrm{mod}\, p).$$

Temos, assim, em $(*)$, $p-1$ inteiros não congruentes dois a dois módulo p; logo, $a, 2a, 3a, \cdots, (p-1)a$ são congruentes módulo p com um e um só dos números $1, 2, 3, ..., p-1$. Portanto,

$$a \times 2a \times 3a \times \cdots \times (p-1)a \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) (\mathrm{mod}\, p),$$

i.e.,

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

Mas, m.d.c.$(p, (p-1)!) = 1$, pelo que

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

□

Como consequência imediata do Pequeno Teorema de Fermat, temos o seguinte resultado:

Corolário 2.13 *Se p é primo, então $a^p \equiv a (\mathrm{mod}\, p)$, para qualquer inteiro a.*

Demonstração: Por um lado, se $p \mid a$, então, $a \equiv 0 (\mathrm{mod}\, p)$, pelo que $a^p \equiv 0 (\mathrm{mod}\, p)$. Logo, $a^p \equiv a (\mathrm{mod}\, p)$.

Por outro lado, se $p \nmid a$, então, pelo Pequeno Teorema de Fermat, $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, ou seja, $a^p \equiv a (\mathrm{mod}\, p)$. □

Apresentamos de seguida alguns exemplos de aplicação do Pequeno Teorema de Fermat.

Exemplo 2.24 *Queremos provar que* $5^{38} \equiv 4 (\mathrm{mod}\, 11)$. *Como* 11 *é primo e* $11 \nmid 5$, *concluímos, pelo Pequeno Teorema de Fermat, que*

$$5^{10} \equiv 1 (\mathrm{mod}\, 11).$$

Assim,

$$5^{38} = (5^{10})^3 \times 5^8 \equiv 5^8 (\mathrm{mod}\, 11).$$

Como $5^4 = 625 \equiv 11 - 2 (\mathrm{mod}\, 11)$, *ou seja* $5^4 \equiv -2 (\mathrm{mod}\, 11)$, *concluímos que* $5^8 \equiv (-2)^2 (\mathrm{mod}\, 11)$. *Logo,*

$$5^{38} \equiv 4 (\mathrm{mod}\, 11).$$

Usando o contra recíproco do Pequeno Teorema de Fermat (ou do seu corolário), podemos verificar se um dado número é ou não primo. De facto, se existe a tal que $p \nmid a$ e $a^{p-1} \not\equiv 1 (\mathrm{mod}\, p)$ (ou tal que $a^p \not\equiv a (\mathrm{mod}\, p)$), então, concluímos que p não é um número primo.

Exemplo 2.25 *Mostremos que* 117 *não é um número primo. Consideremos* $a = 2$ *e vejamos que* $2^{117} \not\equiv 2 (\mathrm{mod}\, 117)$. *Calculemos o resto da divisão de* 2^{117} *por 117. Sabemos que*

$$2^7 = 128 \equiv 11 (\mathrm{mod}\, 117).$$

(A escolha da potência 2^7 *justifica-se por* 2^7 *ser a potência de* 2 *mais próxima de* 117.*) Assim, temos que*

$$\begin{aligned}
2^{117} = 2^{7\times 16+15} \equiv 11^{16} \times 2^5 (\mathrm{mod}\, 117) &\iff 2^{117} \equiv 121^8 \times 2^5 (\mathrm{mod}\, 117) \\
&\iff 2^{117} \equiv 4^8 \times 2^5 (\mathrm{mod}\, 117) \\
&\iff 2^{117} \equiv 2^{21} (\mathrm{mod}\, 117) \\
&\iff 2^{117} \equiv (2^7)^3 (\mathrm{mod}\, 117) \\
&\iff 2^{117} \equiv 11^3 (\mathrm{mod}\, 117) \\
&\iff 2^{117} \equiv 121 \times 11 (\mathrm{mod}\, 117) \\
&\iff 2^{117} \equiv 4 \times 11 (\mathrm{mod}\, 117) \\
&\iff 2^{117} \equiv 44 (\mathrm{mod}\, 117).
\end{aligned}$$

Logo, $2^{117} \not\equiv 2 (\mathrm{mod}\, 117)$, *pelo que podemos concluir que* 117 *não é primo.*

O exemplo seguinte mostra que o recíproco do Pequeno Teorema de Fermat não é verdadeiro.

Exemplo 2.26 *Vejamos que existem inteiros a e p para os quais $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ e p não é primo. Como $4^2 = 16 \equiv 1 (\mathrm{mod}\, 15)$, temos que $4^{14} \equiv 1^7 (\mathrm{mod}\, 15)$, ou seja, $a^{15-1} \equiv 1 (\mathrm{mod}\, 15)$. No entanto, 15 não é um número primo.*

O Lema seguinte permite-nos fazer alguma aritmética com as congruências em determinadas condições.

Lema 2.3 *Sejam p e q números primos distintos e a um inteiro tal que $a^p \equiv a (\mathrm{mod}\, q)$ e $a^q \equiv a (\mathrm{mod}\, p)$. Então,*

$$a^{pq} \equiv a (\mathrm{mod}\, pq).$$

Demonstração: De $a^p \equiv a (\mathrm{mod}\, q)$ concluímos que $a^{pq} \equiv a^q (\mathrm{mod}\, q)$. Mas, $a^q \equiv a (\mathrm{mod}\, q)$. Assim, $a^{pq} \equiv a (\mathrm{mod}\, q)$. De modo análogo, concluímos que $a^{pq} \equiv a (\mathrm{mod}\, p)$. Logo, como p e q são primos entre si,

$$a^{pq} \equiv a (\mathrm{mod}\, pq).$$

□

2.6.2 Teorema de Euler

Uma dos conceitos com maior impacto na Teoria de Números é o da Função de Euler, que de seguida apresentamos. Entre outras aplicações, esta definição permitiu a Euler generalizar o Pequeno Teorema de Fermat.

Definição 2.13 *Para cada $n \geq 1$, seja $\phi(n)$ o número de inteiros positivos k tais que $k \leq n$ e* m.d.c.$(k, n) = 1$. *À função $\phi : \mathbb{N} \to \mathbb{N}$, definida por $n \mapsto \phi(n)$ chama-se* Função de Euler.

Exemplo 2.27 *Tendo em conta a definição, temos, por exemplo, que $\phi(1) = \phi(2) = 1$, $\phi(3) = \phi(4) = \phi(6) = 2$ e $\phi(5) = 4$.*

Facilmente se conclui que, dado $n \geq 2$, se tem que $\phi(n) \leq n-1$. Mais ainda, se n é um número primo, então, $\phi(n) = n - 1$. Finalmente, se n é um número composto, existe pelo menos um inteiro positivo k tal que m.d.c.$(n, k) \neq 1$, pelo que $\phi(n) \leq n - 2$. Acabámos de provar o seguinte critério de primalidade à custa da Função de Euler.

Lema 2.4 *Um inteiro positivo n é primo se e só se $\phi(n) = n - 1$.*

Lema 2.5 *Se p é primo e $k > 0$, então,*

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}).$$

Demonstração: Dos elementos do conjunto $\{1, 2, 3, ..., p, ..., p^k\}$ existem $\frac{p^k}{p} = p^{k-1}$ elementos que são divisíveis por p, pelo que não são primos com p^k. Todos os outros elementos são primos com p^k. Assim,

$$\phi(p^k) = p^k - p^{k-1}.$$

□

Lema 2.6 *Sejam m e n inteiros positivos tais que* m.d.c.$(m, n) = 1$. *Então, $\phi(mn) = \phi(m)\phi(n)$.*

Demonstração: Se $m = n = 1$, o resultado é trivial já que $\phi(1) = 1$. Suponhamos, então, que $m, n > 1$. Na tabela seguinte, com n linhas e m colunas, apresentamos todos os mn primeiros inteiros positivos:

$$\begin{array}{cccccc} 1 & 2 & 3 & \cdots & m \\ m+1 & m+2 & m+3 & \cdots & 2m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots & nm \end{array}$$

Observamos primeiro que um número desta tabela é primo com mn se o for simultaneamente com m e n. Por um lado, todos os números de uma mesma coluna são congruentes módulo m. Assim, $\phi(m)$ é o número de colunas da tabela que têm algum número primo com m. Por outro lado, os elementos $a, m + a, 2m + a, ..., (n - 1)m + a$ de uma coluna de primos com m constitui o conjunto de resíduos da divisão por n. Então, $\phi(n)$ destes elementos são primos com n. Assim, as $\phi(m)$ colunas têm $\phi(n)\phi(m)$ números primos com mn. Logo, $\phi(mn) = \phi(m)\phi(n)$. □

Exemplo 2.28 *Os inteiros* $m = 5$ *e* $n = 4$ *são primos entre si, pelo que* $\phi(20) = \phi(5)\phi(4) = 4 \times 2 = 8$.

Exemplo 2.29 *O resultado do Lema anterior não é válido se os números considerados não forem primos entre si. Para ilustrar esta situação, basta observar que* $\phi(4) = 2 \neq 4 = \phi(2)\phi(2)$.

O próximo teorema permite calcular $\phi(n)$ a partir da decomposição de n em factores primos.

Teorema 2.22 *Se um inteiro* $n > 1$ *admite a factorização*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

onde $p_1, p_2, ..., p_r$ *são primos distintos dois a dois, então,*

$$\begin{aligned} \phi(n) &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \\ &= n(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_r}). \end{aligned}$$

Demonstração: A demonstração faz-se por indução sobre r e tendo em conta os Lemas 2.5 e 2.6. □

Exemplo 2.30 *Como* $60 = 2^2 \times 3 \times 5$, *temos que*

$$\phi(60) = 60(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 16.$$

Em 1760, Euler apresentou o seguinte resultado que tem como corolário o Pequeno Teorema de Fermat.

Teorema 2.23 (Teorema de Euler) *Se* $a \in \mathbb{Z}$ *e* $n \in \mathbb{N}$ *são tais que* m.d.c.$(a, n) = 1$, *então,*

$$a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n).$$

Demonstração: Sejam $r_1, r_2, ..., r_{\phi(n)}$ os $\phi(n)$ inteiros positivos menores que n e primos com n. Como m.d.c.$(a, n) = 1$, temos que, para cada $i \in \{1, 2, ..., \phi(n)\}$, existe $j \in \{1, 2, ..., \phi(n)\}$ tal que $ar_i \equiv r_j (\mathrm{mod}\, n)$. Mais ainda, para quaisquer $i, j \in \{1, 2, ..., \phi(n)\}$ com $i \neq j$, $ar_i \not\equiv ar_j (\mathrm{mod}\, n)$. Assim,

$$ar_1 \times ar_2 \times \cdots \times ar_{\phi(n)} \equiv r_1 \times r_2 \times \cdots \times r_{\phi(n)} (\mathrm{mod}\, n),$$

ou seja,

$$a^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} (\mathrm{mod}\, n).$$

Como $r_1, r_2, \cdots, r_{\phi(n)}$ são primos com n, podemos simplificar a expressão e obtemos

$$a\phi(n) \equiv 1 (\mathrm{mod}\, n).$$

□

O Pequeno Teorema de Fermat resulta imediatamente do Teorema de Euler tendo em conta o Lema 2.4.

2.6.3 Teorema de Wilson

Em 1770, Edward Waring apresentou, na obra "Meditations algebraicae", a seguinte conjectura de Wilson: *se p é primo, então, p divide $(p+1)! + 1$*. Em 1771, Lagrange não só demonstrou esta conjectura como observou que o seu recíproco é igualmente válido. De seguida, apresentamos esta demonstração.

Teorema 2.24 *[Teorema de Wilson] Se p é um número primo, então, $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.*

Demonstração: Começamos por observar que a condição se verifica para $p = 2$ e $p = 3$. De facto,

$$(2-1)! = 1 \equiv -1 (\mathrm{mod}\, 2)$$

e

$$(3-1)! = 2 \equiv -1 (\mathrm{mod}\, 3).$$

Provemos agora a condição para $p > 3$. Seja $a \in \{1, 2, 3, ..., p-1\}$. Consideramos a congruência linear

$$ax \equiv 1 (\mathrm{mod}\, p).$$

Como m.d.c.$(a,p)=1$, existe uma e uma só solução módulo p desta congruência linear. Seja a^* essa solução. Então,

$$1 \leq a^* \leq p-1 \text{ e } aa^* \equiv 1 (\mathrm{mod}\, p).$$

Se $a = a^*$ temos

$$\begin{aligned} a^2 \equiv 1 (\mathrm{mod}\, p) &\iff p \mid a^2 - 1 \\ &\iff p \mid (a-1)(a+1) \\ &\iff p \mid a-1 \qquad ou \qquad p \mid a+1 \\ &\implies a = 1 \qquad ou \qquad a = p-1. \end{aligned}$$

Se $a \neq a^*$, temos então que

$$a \in \{2, 3, 4, ..., p-3, p-2\}.$$

Os $p-3$ elementos deste conjunto podem ser agrupados em pares (a, a^*) tais que $a \neq a^*$ e $aa^* \equiv 1 (\mathrm{mod}\, p)$. Obtemos $\frac{p-3}{2}$ pares e, portanto, $\frac{p-3}{2}$ expressões do tipo $aa^* \equiv 1 (\mathrm{mod}\, p)$. Pelo Teorema 2.12(iv) obtemos

$$2 \times 3 \times \cdots \times (p-3) \times (p-2) \equiv 1 (\mathrm{mod}\, p),$$

i.e.,

$$(p-2)! \equiv 1 (\mathrm{mod}\, p).$$

Logo,

$$(p-1)! = (p-1)(p-2)! \equiv p-1 (\mathrm{mod}\, p)$$

e, portanto,

$$(p-1)! \equiv -1 (\mathrm{mod}\, p).$$

□

Exemplo 2.31 *Com este exemplo, ilustramos a demonstração do Teorema de Wilson e mostramos que o resto da divisão de* 12! *por* 13 *é* 12. *Seja* $p = 13$. *Da lista* $2 - 3 - 4 -$

$5-6-7-8-9-10-11$ *podemos formar 5 pares de números e com eles formar as 5 congruências*

$$2 \times 7 \equiv 1 (\mathrm{mod}\, 13)$$

$$3 \times 9 \equiv 1 (\mathrm{mod}\, 13)$$

$$4 \times 10 \equiv 1 (\mathrm{mod}\, 13)$$

$$5 \times 8 \equiv 1 (\mathrm{mod}\, 13)$$

$$6 \times 11 \equiv 1 (\mathrm{mod}\, 13).$$

Então,

$$2 \times 7 \times 3 \times 9 \times 4 \times 10 \times 5 \times 8 \times 6 \times 11 \equiv 1 (\mathrm{mod}\, 13),$$

i.e.,

$$11! \equiv 1 (\mathrm{mod}\, 13).$$

Logo,

$$12! = 12 \times 11! \equiv 12 \times 1 (\mathrm{mod}\, 13),$$

i.e.,

$$(13-1)! \equiv -1 (\mathrm{mod}\, 13).$$

O resultado seguinte é o recíproco do Teorema de Wilson, também provado por Lagrange.

Teorema 2.25 *Se* $(n-1)! \equiv -1 (\mathrm{mod}\, n)$*, então,* n *é primo.*

Demonstração: Suponhamos que n não é primo. Então, existe um inteiro d tal que $1 < d \leq n-1$ e $d \mid n$. De $1 < d \leq n-1$ concluímos que $d \mid (n-1)!$. De $d \mid n$, como $n \mid (n-1)! + 1$ por hipótese, concluímos que $d \mid (n-1)! + 1$. Logo,

$$d \mid (n-1)! + 1 - (n-1)!,$$

ou seja, $d \mid 1$, o que contradiz o facto de $1 < d$. Logo, n é primo. □

Os Teoremas 2.24 e 2.25 permitem concluir que um número inteiro positivo n é primo se e só se $(n-1)! \equiv -1 (\mathrm{mod}\, n)$. Apesar de ser uma caracterização dos números primos, não é de modo algum um modo eficaz de verificar se um número é ou não primo.

O Teorema de Wilson garante ainda que existe uma infinidade de números compostos do tipo $n! + 1$. Continua em aberto a questão de se saber se existe ou não uma infinidade de números primos da mesma forma.

2.6.4 Exercícios

Exercício 2.6.1. Recorrendo ao Pequeno Teorema de Fermat, mostre que:

(a) $a^{21} \equiv a (\mathrm{mod}\, 15)$, para todo o inteiro a;

(b) $a^{13} \equiv a (\mathrm{mod}\, 273)$, para todo o inteiro a;

(c) $a^{12} \equiv 1 (\mathrm{mod}\, 35)$, para todo o inteiro a tal que m.d.c.$(a, 35) = 1$.

Exercício 2.6.2. Mostre que 60 divide $a^4 + 59$ se m.d.c.$(a, 30) = 1$.

Exercício 2.6.3. Se $a \in \mathbb{Z}$ é tal que $7 \nmid a$, prove que $a^3 + 1$ ou $a^3 - 1$ é divisível por 7.

Exercício 2.6.4. Seja p um número primo. Mostre que $2 \times (p-3)! \equiv -1 (\mathrm{mod}\, p)$.

Exercício 2.6.5. Determine:

(a) o resto da divisão de 15! por 17;

(b) o resto da divisão de $2 \times 26!$ por 29.

Exercício 2.6.6. Verifique que $4 \times 29! + 5!$ é divisível por 31.

Exercício 2.6.7. Considere a função de Euler ϕ. Calcule $\phi(420)$, $\phi(1001)$ e $\phi(5040)$.

Exercício 2.6.8. Verifique que $\phi(n+2) = \phi(n) + 2$, para $n = 12, 14, 20$.

Exercício 2.6.9. Verifique o Teorema de Euler para $n = 10$ e $a = 3$.

Exercício 2.6.10. Seja $a \in \mathbb{Z}$ tal que m.d.c.$(a, 15) = 1$. Mostre que $a^{17} \equiv a (\mathrm{mod}\, 15)$:

(a) recorrendo ao Pequeno Teorema de Fermat;

(b) recorrendo ao Teorema de Euler.

Exercício 2.6.11. Quais os dois últimos dígitos na representação decimal de 3^{256}?

Exercício 2.6.12. Mostre que se n é um número inteiro ímpar que não é múltiplo de 5 então n divide um inteiro cujos dígitos são todos iguais a 1.

Exercício 2.6.13. Por que é que se tem $\phi(2n) = \phi(n)$ para qualquer inteiro positivo ímpar n?

Bibliografia

[1] Bondy, J.A. & Murty, U.S.R., *Graph Theory with applications*, Elsevier, 5th Printing (1982)

[2] Burton, D.M. *Elementary Number Theory*, Wm. C. Brown Publishers (1989)

[3] Jones, G.A. & Jones, J.M. *Elementary Number Theory*, Springer Undergraduate Mathematics Series, 8th printing, London (2005)

[4] Watkins, J.J. & Wilson, R.J. *Graphs: an introductory approach: a first course in discrete mathematics*, John Wiley and Sons (1990)