Teoria Aritmética dos Números

MA553 – 2º semestre de 2024

Tiago J. Fonseca*

Sumário

Introdução **5**

Notas de aula **7**

Aula 1 (12/08) **7**

1) Aquecimento 7

Aula 2 (14/08) **10**

1) Aquecimento (cont.) 10

Aula 3 (19/08) **15**

2) Fundamentos 15

Aula 4 (21/08) **19**

2) Fundamentos (cont.) 19

Aula 5 (26/08) **23**

3) Divisibilidade (em $\mathbb{Z}$) 23

Aula 6 (28/08) **27**

3) Divisibilidade (cont.) 27

Aula 7 (02/09) **30**

*Notas digitalizadas com o auxílio de inteligência artificial a partir do manuscrito do professor, sem revisão cuidadosa; veja a Introdução.

3) Divisibilidade (cont.) 30

Aula 8 (04/09) **33**

3) Divisibilidade (cont.) 33

4) Equações diofantinas lineares 34

Aula 9 (09/09) **37**

4) Equações diofantinas lineares (cont.) 37

Aula 10 (11/09) **40**

5) Primos 40

Aula 11 (16/09) **43**

5) Primos (cont.) 43

Aula 12 (18/09) **46**

5) Primos (cont.) 46

6) Racionais e irracionais 48

Aula 13 (30/09) **51**

7) Congruências 51

Aula 14 (07/10) **54**

7) Congruências (cont.) 54

Aula 15 (09/10) **57**

8) O anel de inteiros módulo m 57

Aula 16 (14/10) **60**

8) O anel de inteiros módulo m (cont.) 60

Aula 17 (16/10) **64**

9) Teorema chinês dos restos 64

Aula 18 (21/10) **68**

10) Teoremas de Fermat e Euler 68

Aula 19 (23/10) **72**

10) Teoremas de Fermat e Euler (cont.) 72

Aula 20 (04/11) **76**
11) Criptografia RSA 76

Aula 21 (06/11) **79**
11) Criptografia RSA (cont.) 79

Aula 22 (11/11) **83**
12) Resíduos quadráticos 83

Aula 23 (13/11) **86**
12) Resíduos quadráticos (cont.) 86

Aula 24 (18/11) **90**
12) Resíduos quadráticos (cont.) 90
13) Somas de quadrados 91

Listas de exercícios **93**

1. Aquecimento **93**

2. Fundamentos **93**

3. Divisibilidade **95**

4. Equações diofantinas lineares **96**

5. Primos **97**

6. Racionais e irracionais **97**

7. Congruências **98**

8. O anel de inteiros módulo m **98**

9. Teorema chinês dos restos **99**

10. Teoremas de Fermat e Euler **100**

11. Criptografia RSA **100**

12. Resíduos quadráticos **102**

13. Somas de quadrados **102**

Aula de exercícios (30/10) **102**

Provas **104**

Prova 1 (02/10/2024) **104**

Prova 2 (27/11/2024) **107**

Anexo **110**

O trabalho do curso **110**

Introdução

Estas são as notas de aula da disciplina *MA553 – Teoria Aritmética dos Números* (turma Z), oferecida para a licenciatura em matemática no Instituto de Matemática, Estatística e Computação Científica (IMECC) da Unicamp no segundo semestre de 2024. Cada seção destas notas corresponde a uma aula.

Conteúdo. O curso começa com um "aquecimento" sobre as ternas pitagóricas, resolvidas de duas maneiras (aritmeticamente e pela geometria dos pontos racionais no círculo), e uma breve menção aos números congruentes. Em seguida, revisitamos os fundamentos: os axiomas de Peano, a soma, o produto e a ordem nos naturais, relações de equivalência e a construção dos inteiros. O núcleo do curso é a aritmética dos inteiros: divisão euclidiana e representação em bases, divisibilidade, máximo divisor comum, o algoritmo de Euclides e o teorema de Bézout, equações diofantinas lineares, números primos e o teorema fundamental da aritmética, e uma breve discussão sobre números racionais e irracionais. Depois estudamos as congruências e o anel $\mathbb{Z}/m\mathbb{Z}$, os teoremas de Wilson, Fermat e Euler, a função φ de Euler, o teorema chinês dos restos, ordens e raízes primitivas, com a aplicação à criptografia RSA e a testes de primalidade. O curso termina com os resíduos quadráticos (critério de Euler, símbolo de Legendre e a lei de reciprocidade quadrática) e com o teorema de Fermat sobre somas de dois quadrados.

Organização. O curso contou com o auxílio do PED (Programa de Estágio Docente) Nelson Serrano. Além das aulas, o curso teve duas provas (02/10 e 27/11), aulas de exercícios (algumas delas de revisão para as provas) e um trabalho para entregar (um plano de aula ou um artigo expositório). Ao final destas notas, incluímos as listas de exercícios do curso (com os exercícios da aula de exercícios de 30/10), as duas provas com os respectivos gabaritos e, como anexo, as especificações do trabalho.

Ementa oficial. Segundo o catálogo da Unicamp, a ementa da disciplina MA553 é:

> Estruturas algébricas (operações binárias, grupos, anéis e corpos). Axiomas de Peano e construção do anel dos números inteiros e racionais. Outros exemplos de anéis e corpos (polinômios, corpos quadráticos, inteiros de Gauss, $\mathbb{Z}_m$). Domínios euclideanos. Representação de números inteiros em bases diversas. Máximo divisor comum, mínimo múltiplo comum e o Algoritmo de Euclides. Elementos irredutíveis e primos e critérios de divisibilidade. Domínios principais, fatoriais e o teorema fundamental da aritmética. Equações diofantinas de grau um.

Sistemas residuais, congruências lineares e o teorema chinês do resto. Os teoremas de Euler e Wilson. Congruências de grau dois, símbolos de Legendre e Jacobi e Lei da Reciprocidade Quadrática. Ternas pitagóricas e números que podem ser escritos como soma de dois quadrados. Equações diofantinas notáveis. Ordem multiplicativa e raízes primitivas. Noções de criptografia.

Bibliografia. A bibliografia oficial da disciplina é

[1] J. P. de Oliveira Santos, *Introdução à Teoria dos Números*, 3ª ed. Coleção Matemática Universitária, IMPA, Rio de Janeiro, 2012.

[2] I. Niven, H. S. Zuckerman e H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5ª ed. Wiley, Nova York, 1991.

[3] M. Artin, *Algebra*, 2ª ed. Pearson, Boston, 2010.

Como bibliografia complementar, recomendamos também

[4] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha e E. Tengan, *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. Projeto Euclides, IMPA, Rio de Janeiro.

Sobre estas notas. Estas são *notas de aula*: elas reproduzem o que foi feito em sala, e por isso o estilo é casual e informal, com demonstrações às vezes apenas esboçadas e detalhes deixados como exercício. Elas não pretendem ser tão completas nem tão cuidadosas quanto um livro-texto; para isso, recomendamos a bibliografia acima.

Atenção: estas notas foram digitalizadas com o auxílio de inteligência artificial a partir do manuscrito usado em sala de aula, e **não foram revisadas cuidadosamente** pelo autor. Elas certamente contêm erros, tanto de transcrição quanto matemáticos, e devem ser lidas com cautela. Correções e sugestões são bem-vindas.

Notas de aula

Aula 1 (12/08)

Este é um curso de teoria dos números para a licenciatura. Os tópicos principais do curso são: divisibilidade, congruências, números primos e equações diofantinas. Como aplicação dos três primeiros, veremos a criptografia RSA.

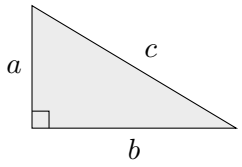
1) Aquecimento

Lembre que $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$ denota o conjunto dos números inteiros.

Definição 1.1. Uma *terna pitagórica* é uma terna (a, b, c) de inteiros tais que

$$a^2 + b^2 = c^2.$$

No caso em que $a, b, c \geqslant 1$, uma terna pitagórica corresponde a um triângulo retângulo de lados inteiros:[1]



Exemplo 1.2. São ternas pitagóricas:

- $(3, 4, 5)$;
- $(4, 3, 5)$;
- $(4, -3, 5)$, $(-4, 3, 5)$, $\ldots$;
- $(6, 8, 10) = (2 \cdot 3, 2 \cdot 4, 2 \cdot 5)$.

Estes exemplos não deveriam contar como exemplos "realmente diferentes", pois todos derivam de $(3, 4, 5)$. Já

- $(5, 12, 13)$

é um exemplo "novo" $(25 + 144 = 169)$.

Exercício 1.3. Verifique que, se (a, b, c) é uma terna pitagórica e u é um inteiro, então (ua, ub, uc) é uma terna pitagórica.

[1] Procure por "Plimpton 322", uma tábua de argila babilônica (c. 1800 a.C.) que contém uma lista de ternas pitagóricas.

Definição 1.4. Uma terna pitagórica (a, b, c) é dita *primitiva* se:

- $a, b, c \geqslant 1$;
- a, b, c não têm fatores em comum.

Exemplo 1.5. São ternas pitagóricas primitivas:

- $(3, 4, 5)$, $(4, 3, 5)$;
- $(5, 12, 13)$, $(12, 5, 13)$;
- $(8, 15, 17)$, $(15, 8, 17)$ $\quad (64 + 225 = 289)$.

Pergunta. Existem outros exemplos? Quantos? Podemos descrevê-los explicitamente (com uma fórmula)?

Queremos "resolver" a *equação diofantina*

$$a^2 + b^2 = c^2.$$

Definição 1.6. Uma *equação diofantina* é qualquer equação para a qual buscamos soluções em $\mathbb{Z}$ (ou em $\mathbb{Q}$).

Exemplo 1.7.

- Equação de Fermat: $x^n + y^n = z^n$, com $n \geqslant 3$.
- Equação diofantina linear: $2x + 5y = 1$.
- Equação de Catalan: $x^a - y^b = 1$ (por exemplo, $3^2 - 2^3 = 1$); resolvida por Mihăilescu em 2002.

Teorema 1.8 (Matiyasevich, 1970)**.** *Não existe um algoritmo que decide se equações diofantinas polinomiais têm solução.*[2]

Voltando às ternas pitagóricas...

Lema 1.9. *Se (a, b, c) é uma terna pitagórica primitiva, então a e b têm paridades distintas. (Equivalentemente: c é ímpar.)*

Demonstração. Por absurdo, suponha que a e b têm a mesma paridade. Como $(\text{par})^2 = (\text{par})$ e $(\text{ímpar})^2 = (\text{ímpar})$, temos

$$c^2 = (\text{par})^2 + (\text{par})^2 = (\text{par}) + (\text{par}) = (\text{par})$$

ou

$$c^2 = (\text{ímpar})^2 + (\text{ímpar})^2 = (\text{ímpar}) + (\text{ímpar}) = (\text{par}).$$

[2]Este era o 10º problema de Hilbert (1900).

Logo, c é par. Como (a, b, c) é primitiva, a e b não podem ser ambos pares. Assim, a e b são ímpares e c é par:

$$a = 2r + 1, \qquad b = 2s + 1, \qquad c = 2t,$$

com $r, s, t \in \mathbb{Z}$. Logo,

$$\begin{aligned} a^2 + b^2 = c^2 &\iff (2r+1)^2 + (2s+1)^2 = (2t)^2 \\ &\iff 4(r^2 + r + s^2 + s) + 2 = 4t^2 \\ &\iff \underbrace{2(r^2 + r + s^2 + s) + 1}_{\text{ímpar}} = \underbrace{2t^2}_{\text{par}}. \end{aligned}$$

Absurdo! □

Seja (a, b, c) primitiva. Sem perda de generalidade, podemos supor a ímpar, b par e c ímpar. Temos:

$$a^2 + b^2 = c^2 \iff a^2 = c^2 - b^2 \iff a^2 = (c - b)(c + b).$$

Exemplo 1.10.

- $(3, 4, 5)$: $3^2 = (5 - 4)(5 + 4) = 1 \cdot 9 = 1^2 \cdot 3^2$;
- $(5, 12, 13)$: $5^2 = (13 - 12)(13 + 12) = 1 \cdot 25 = 1^2 \cdot 5^2$;
- $(15, 8, 17)$: $15^2 = (17 - 8)(17 + 8) = 9 \cdot 25 = 3^2 \cdot 5^2$.

Exercício 1.11. Mostre que $c - b$ e $c + b$ não têm fatores em comum.

Lema 1.12. *Se $x, y \geqslant 1$ não têm fatores em comum e xy é um quadrado, então x e y são quadrados.*

Isto segue do "teorema fundamental da aritmética", que veremos mais tarde.

Logo,

$$\boxed{c - b = t^2}, \qquad \boxed{c + b = s^2}, \qquad t, s \in \mathbb{Z},$$

e

$$a^2 = (c - b)(c + b) = t^2 s^2 = (ts)^2 \implies \boxed{a = ts}.$$

Teorema 1.13. *(a, b, c) é uma terna pitagórica primitiva com a ímpar se, e somente se, existem inteiros ímpares $s > t \geqslant 1$, sem fatores em comum, tais que*

$$(a, b, c) = \left(ts, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2} \right).$$

Exemplo 1.14. Para $t = 5$, $s = 101$, obtemos $(505, 5088, 5113)$.

Exercício 1.15. Escreva a demonstração do teorema.

Aula 2 (14/08)

1) Aquecimento (cont.)

Aula passada. Ternas pitagóricas: (a, b, c) tais que $a^2 + b^2 = c^2$. Vimos o seguinte resultado.

Teorema 2.1. *Uma terna de inteiros (a, b, c), com a ímpar, é uma terna pitagórica primitiva se, e somente se, existem inteiros ímpares sem fatores em comum $s > t \geqslant 1$ tais que*

$$(a, b, c) = \left(ts, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2}\right) \qquad \textit{(“fórmula de Euclides”).}$$

Exercício 2.2. Escreva a demonstração cuidadosamente.

Exercício 2.3. Seja n o dobro de um número ímpar $(2, 6, 10, 14, \ldots)$. Existe uma terna pitagórica primitiva tal que $b = n$?

Hoje: ternas pitagóricas (de novo!) e além.

Abordagem geométrica. Temos

$$a^2 + b^2 = c^2 \iff \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

Ternas pitagóricas (a, b, c) correspondem a pontos com coordenadas *racionais* $(x, y) = (a/c, b/c)$ no círculo unitário de equação

$$x^2 + y^2 = 1.$$

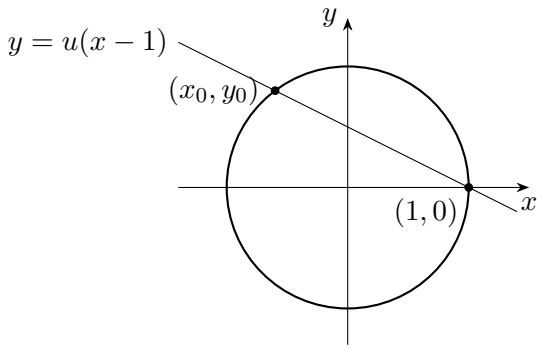
Resolver a equação diofantina $a^2 + b^2 = c^2$ equivale a descrever os “pontos racionais” no círculo. (Note que $\mathbb{Z}$ é um anel, enquanto $\mathbb{Q}$ é um corpo.)

Se $(x_0, y_0) \neq (1, 0)$ é um tal ponto, a reta determinada por (x_0, y_0) e $(1, 0)$ tem inclinação racional

$$u \coloneqq \frac{y_0}{x_0 - 1} \in \mathbb{Q},$$

e sua equação é

$$y = u(x - 1).$$



Reciprocamente, dado $u \in \mathbb{Q}$, a interseção da reta $y = u(x-1)$ com o círculo é dada por:

$$\begin{aligned} x^2 + \big(u(x-1)\big)^2 = 1 &\iff x^2 - 1 + u^2(x-1)^2 = 0 \\ &\iff (x-1)\big(x+1+u^2(x-1)\big) = 0 \\ &\iff (x-1)\big((u^2+1)x - (u^2-1)\big) = 0 \\ &\iff x = 1 \quad \text{ou} \quad \boxed{x = \frac{u^2-1}{u^2+1}}. \end{aligned}$$

Neste último caso,

$$y = u(x-1) = u\left(\frac{u^2-1}{u^2+1} - 1\right) = -\frac{2u}{u^2+1}.$$

Assim, obtemos o ponto *racional*

$$(x,y) = \left(\frac{u^2-1}{u^2+1}, \frac{-2u}{u^2+1}\right) \qquad \text{(“parametrização do círculo unitário”).}$$

Todos os pontos racionais do círculo diferentes de $(1,0)$ são dessa forma!

Escrevendo $u = t/s$, com t, s inteiros,

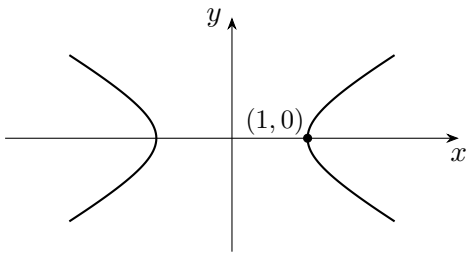
$$\begin{aligned} \left(\frac{u^2-1}{u^2+1}\right)^2 + \left(\frac{-2u}{u^2+1}\right)^2 = 1 &\iff (u^2-1)^2 + (-2u)^2 = (u^2+1)^2 \\ &\iff \left(\frac{t^2}{s^2} - 1\right)^2 + \left(\frac{2t}{s}\right)^2 = \left(\frac{t^2}{s^2}+1\right)^2 \\ &\iff (t^2-s^2)^2 + (2ts)^2 = (t^2+s^2)^2, \end{aligned}$$

e obtemos a terna pitagórica

$$(a,b,c) = (2ts,\, t^2-s^2,\, t^2+s^2).$$

O método acima funciona para *qualquer* equação de grau 2 (cônica) que possui pelo menos um ponto racional.

Exercício 2.4. Encontre uma fórmula para parametrizar todos os pontos com coordenadas racionais na hipérbole $x^2 - 3y^2 = 1$.

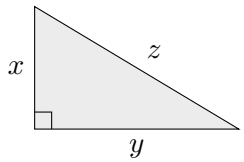


Descreva todas as soluções (inteiras) da equação diofantina $a^2 - 3b^2 = c^2$.

Equações diofantinas de grau 1 e 2: ok (veremos com mais detalhes no curso). O que acontece com grau $\geqslant 3$?

Problema dos números congruentes. Quais são os inteiros n que ocorrem como a área de um triângulo retângulo com lados *racionais*? Isto é, $x, y, z \in \mathbb{Q}$ com

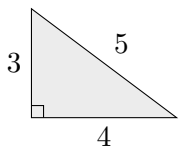
$$x^2 + y^2 = z^2, \qquad n = \frac{xy}{2} \in \mathbb{Z}.$$

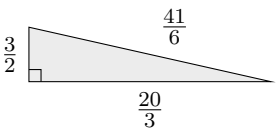


Tais inteiros n são chamados de *números congruentes*.

Exemplo 2.5.

1. $n = 6$ é congruente: triângulo de lados 3, 4 e 5, pois $6 = \frac{3 \cdot 4}{2}$.
2. $n = 5$ é congruente: triângulo de catetos $\frac{3}{2}$ e $\frac{20}{3}$ e hipotenusa $\frac{41}{6}$, pois $5 = \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{20}{3}$. Note que os lados não são inteiros!
3. $n = 1$ *não* é congruente (Fermat).





O problema dos números congruentes foi proposto no século X (num manuscrito árabe) e está *aberto* até hoje!

Dados $x, y, z \in \mathbb{Q}$ com $x^2 + y^2 = z^2$ e $\frac{xy}{2} = n$, temos

$$\begin{cases} \left(\dfrac{x+y}{2}\right)^2 = \left(\dfrac{z}{2}\right)^2 + n, \\ \left(\dfrac{x-y}{2}\right)^2 = \left(\dfrac{z}{2}\right)^2 - n. \end{cases}$$

Exercício 2.6. Verifique as identidades acima. Reciprocamente, mostre que, se existe um número racional w tal que $w^2 - n$ e $w^2 + n$ são quadrados, então n é congruente. (Ou seja: "n é a razão de uma PA de quadrados com 3 termos".)

Multiplicando as duas equações:

$$\left(\frac{x^2 - y^2}{4}\right)^2 = \left(\frac{z}{2}\right)^4 - n^2.$$

Multiplicando os dois lados por $\left(\frac{z}{2}\right)^2$:

$$\left(\underbrace{\frac{z(x^2 - y^2)}{8}}_{Y}\right)^2 = \left(\underbrace{\left(\frac{z}{2}\right)^2}_{X}\right)^3 - n^2 \left(\frac{z}{2}\right)^2.$$

Conclusão: a todo número congruente n podemos associar uma equação

$$Y^2 = X^3 - n^2 X$$

com uma solução racional

$$(X, Y) = \left(\left(\frac{z}{2}\right)^2, \frac{z(x^2 - y^2)}{8}\right).$$

Reciprocamente, pode-se mostrar que, dado um inteiro n, se a equação (de grau 3)

$$Y^2 = X^3 - n^2 X$$

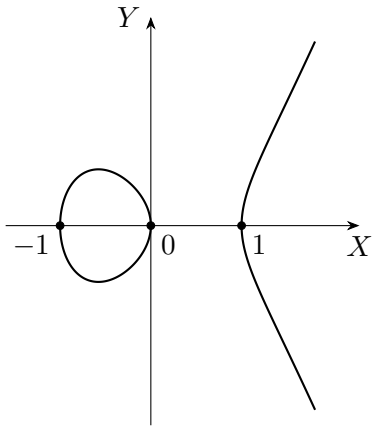
admite uma solução racional com $Y \neq 0$, então n é congruente.

Definição 2.7. Em geral, uma equação da forma

$$Y^2 = X^3 + aX + b \qquad (\text{com } 4a^3 + 27b^2 \neq 0)$$

é dita uma *curva elíptica*.

Exemplo 2.8 ($n = 1$)**.** Gráfico de $Y^2 = X^3 - X$ em $\mathbb{R}^2$:



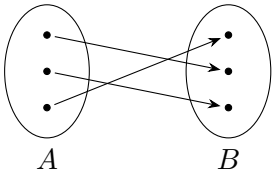
Não existe um método *geral* para calcular pontos racionais em curvas elípticas. (O método anterior não funciona. Por quê?) Este é um tópico de pesquisa atual... Veja, por exemplo, a conjectura de Birch e Swinnerton-Dyer.

Aula 3 (19/08)

2) Fundamentos

O que é um número natural? Há dois pontos de vista:

- *ordinal*: "ordem", "posição";
- *cardinal*: "quantidade", "medida". Dois conjuntos A e B têm a mesma *cardinalidade* se existe uma bijeção $A \to B$.



Axiomas de Peano. São uma caracterização axiomática do conjunto dos números naturais $\mathbb{N}$ (ponto de vista ordinal). Símbolos: 0 (zero) e s (sucessor; pense em "+1").

Axiomas:

(P1) $0 \in \mathbb{N}$. ("zero é um número natural")

(P2) Para todo $n \in \mathbb{N}$, $s(n) \in \mathbb{N}$. ("o sucessor de um número natural é um número natural")

(P3) Para todo $n \in \mathbb{N}$, $s(n) \neq 0$. ("zero não é sucessor de um número natural")

(P4) Para todos $m, n \in \mathbb{N}$, $s(m) = s(n)$ se, e somente se, $m = n$.

(P5) (Indução) Seja $P(x)$ uma propriedade sobre elementos de $\mathbb{N}$. Se valem:

(a) $P(0)$ ("base"),

(b) para todo $n \in \mathbb{N}$, $P(n)$ implica $P(s(n))$ ("passo indutivo"; $P(n)$ é a "hipótese de indução"),

então vale $P(n)$ para todo $n \in \mathbb{N}$.

Usualmente, denotamos

$$s(0) = 1, \quad s(1) = 2, \quad s(2) = 3, \quad \ldots$$

Observação 3.1. Há um modelo de $\mathbb{N}$ dentro da teoria dos conjuntos (isto não é importante para nós):

$$0 = \varnothing, \qquad s(n) = n \cup \{n\},$$

isto é,

$$0 = \varnothing, \quad 1 = \{\varnothing\}, \quad 2 = \{\varnothing, \{\varnothing\}\}, \quad \dots$$

Lema 3.2. *Para todo $n \in \mathbb{N}$, $s(n) \neq n$.*

Demonstração. Demonstração por indução (axioma (P5)). Seja $P(x)$ a propriedade $s(x) \neq x$.

- Base: pelo axioma (P3), vale $s(0) \neq 0$.
- Passo indutivo: se vale $s(n) \neq n$, pelo axioma (P4), $s(s(n)) \neq s(n)$. □

Exercício 3.3. Mostre que, se $n \in \mathbb{N}$ e $n \neq 0$, então existe $m \in \mathbb{N}$ tal que $n = s(m)$ (m é o "antecessor" de n). Por que m é único?

Definição 3.4. A *soma* (ou *adição*) em $\mathbb{N}$ é uma função

$$\mathbb{N} \times \mathbb{N} \to \mathbb{N}, \qquad (m, n) \mapsto m + n,$$

tal que:

1. Para todo $m \in \mathbb{N}$, $m + 0 = m$.
2. Para todos $m, n \in \mathbb{N}$, $m + s(n) = s(m + n)$.

Exercício 3.5. Mostre, por indução, que a soma é única.

Teorema 3.6 (Propriedades da soma)**.** *Para todos $m, n, p \in \mathbb{N}$, valem:*

1. $m + n = n + m$ *(comutatividade);*
2. $(m + n) + p = m + (n + p)$ *(associatividade);*
3. *se $m + n = m + p$, então $n = p$ (cancelamento);*
4. $s(n) = n + 1$, *onde* $1 \coloneqq s(0)$.

Demonstração (só de (1)). Indução em n:

- Base: $m + 0 = 0 + m$. Mostramos isto por indução em m:
  - Base: $0 + 0 = 0 = 0 + 0$.

– Passo indutivo: se $m + 0 = 0 + m$, então

$$s(m) + 0 = s(m) = s(m + 0) = s(0 + m) = 0 + s(m).$$

- Passo indutivo: se $m + n = n + m$, então

$$m + s(n) = s(m + n) = s(n + m) = n + s(m).$$

Resta mostrar que $n + s(m) = s(n) + m$. Fixamos n e fazemos indução em m:

- Base: $s(n) + 0 = s(n) = s(n + 0) = n + s(0)$.
- Passo indutivo: se $s(n) + m = n + s(m)$, então

$$s(n) + s(m) = s(s(n) + m) = s(n + s(m)) = n + s(s(m)). \qquad \square$$

Exercício 3.7. Demonstre (4).

Exercício 3.8. Mostre que, se $m + n = 0$, então $m = n = 0$.

Definição 3.9. Dados $m, n \in \mathbb{N}$, denotamos $m \leqslant n$ ("m é menor ou igual a n") se existe $p \in \mathbb{N}$ tal que $m + p = n$.

Proposição 3.10. $\leqslant$ *é uma* relação de ordem*, isto é:*

(i) para todo $n \in \mathbb{N}$, $n \leqslant n$ (reflexiva);

(ii) para todos $m, n \in \mathbb{N}$, se $m \leqslant n$ e $n \leqslant m$, então $m = n$ (antissimétrica);

(iii) para todos $m, n, p \in \mathbb{N}$, se $m \leqslant n$ e $n \leqslant p$, então $m \leqslant p$ (transitiva).

Demonstração. (i) $n \leqslant n$, pois $n + 0 = n$.

(ii) Se $m \leqslant n$ e $n \leqslant m$, então existem $p, q \in \mathbb{N}$ tais que $m + p = n$ e $n + q = m$. Logo, $m + p + q = m$. Pela lei do cancelamento, $p + q = 0$. Pelo exercício, $p = q = 0$, isto é, $m = n$.

(iii) Exercício. $\square$

Comentários sobre indução.

1. Não precisa começar em 0: se vale $P(n_0)$ e, para todo $n \geqslant n_0$, $P(n)$ implica $P(n + 1)$, então vale $P(n)$ para todo $n \geqslant n_0$.

   Exercício 3.11. Descreva *todas* as quantias que podem ser obtidas combinando-se notas de 4 reais e 5 reais. (Exemplo: $13 = 4 + 4 + 5$.)

2. Formas equivalentes:

   - *Indução forte*: se vale $P(0)$ e, para todo n, "$P(k)$ para todo $k \leqslant n$" implica $P(n+1)$, então vale $P(n)$ para todo n.
   - *Princípio da boa ordem*: todo subconjunto não vazio $S \subset \mathbb{N}$ admite um *elemento mínimo*, isto é, $m \in S$ tal que $m \leqslant n$ para todo $n \in S$.

Aula 4 (21/08)

2) Fundamentos (cont.)

Definição 4.1. O *produto* (ou *multiplicação*) em $\mathbb{N}$ é uma função

$$\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}, \qquad (m, n) \longmapsto m \cdot n,$$

tal que:

(1) Para todo $m \in \mathbb{N}$, $m \cdot 0 = 0$;

(2) Para todos $m, n \in \mathbb{N}$, $m \cdot (n + 1) = m \cdot n + m$.

Observação 4.2. O produto também é único.

Teorema 4.3 (Propriedades do produto)**.** *Para todos $m, n, p \in \mathbb{N}$, valem:*

(1) $m \cdot n = n \cdot m$ *(comutativa)*

(2) $m \cdot (n + p) = m \cdot n + m \cdot p$ *(distributiva)*

(3) $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ *(associativa)*

(4) $1 \cdot m = m$ *(elemento neutro)*

(5) Se $m \cdot n = 0$, então $m = 0$ ou $n = 0$.

Demonstração. Faremos apenas (4) e (5).

(4) Por indução em m. Base: $1 \cdot 0 = 0$. Passo indutivo: se $1 \cdot m = m$, então

$$1 \cdot (m + 1) = 1 \cdot m + 1 = m + 1.$$

(5) Suponha $m \cdot n = 0$ e $n \neq 0$. Então existe $p \in \mathbb{N}$ tal que $n = p + 1$. Logo,

$$0 = m \cdot n = m \cdot (p + 1) = m \cdot p + m.$$

Pelo exercício da aula passada (se a soma de dois naturais é 0, então ambos são 0), temos $m \cdot p = m = 0$. □

Exercício 4.4.

1) Mostre que existe uma única função

$$\mathbb{N} \longrightarrow \mathbb{N}, \qquad n \longmapsto n!,$$

tal que $0! = 1$ e $(n + 1)! = n! \cdot (n + 1)$.

2) Mostre que o número de maneiras de enfileirar n objetos distintos é $n!$.

Exercício 4.5. Dados $m, n, p \in \mathbb{N}$, mostre que, se $m \leqslant n$, então $mp \leqslant np$.

Interlúdio: relações de equivalência.

Definição 4.6. Uma relação $\sim$ em um conjunto A é uma *relação de equivalência* se:

(1) Para todo $a \in A$, $a \sim a$ (reflexiva)

(2) Para todos $a, b \in A$, se $a \sim b$, então $b \sim a$ (simétrica)

(3) Para todos $a, b, c \in A$, se $a \sim b$ e $b \sim c$, então $a \sim c$ (transitiva)

Exemplo 4.7. A igualdade $=$ é uma relação de equivalência.

Exercício 4.8 (Relação de paridade)**.** Verifique que a relação $\sim$ em $\mathbb{N}$ tal que $n \sim m$ se n e m têm a mesma paridade é uma relação de equivalência. (Exemplos: $0 \sim 6$, $1 \sim 3$.)

Definição 4.9. Seja A um conjunto com uma relação de equivalência $\sim$.

- A *classe de equivalência* de um elemento $a \in A$ é o conjunto
$$\overline{a} = \{b \in A : b \sim a\}.$$
Qualquer $b \in \overline{a}$ é dito um *representante* de $\overline{a}$.
- O *conjunto quociente* é o conjunto das classes de equivalência:
$$A/\sim = \{\overline{a} : a \in A\}.$$

Exemplo 4.10. Considere $\mathbb{N}$ com a relação de paridade. Temos
$$\overline{0} = \{0, 2, 4, 6, \ldots\} = \{n \in \mathbb{N} : n \text{ é par}\},$$
$$\overline{1} = \{1, 3, 5, \ldots\} = \{n \in \mathbb{N} : n \text{ é ímpar}\}.$$
Note que $\overline{0} = \overline{2} = \overline{4} = \cdots$ e $\overline{1} = \overline{3} = \overline{5} = \cdots$. Logo,
$$\mathbb{N}/\sim = \{\overline{0}, \overline{1}\} \qquad (\text{“par e ímpar”}).$$

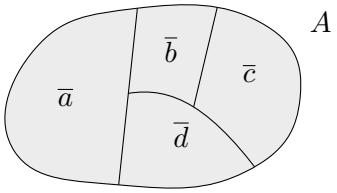
Exercício 4.11. Seja A um conjunto com uma relação de equivalência $\sim$. Mostre que:

1) Se $a \in A$ e $b \in \overline{a}$, então $\overline{b} = \overline{a}$.

2) Se $a, b \in A$ e $\overline{a} \cap \overline{b} \neq \emptyset$, então $\overline{a} = \overline{b}$.

3) $A = \bigcup_{a \in A} \overline{a}$.

(“As classes de equivalência formam uma partição de A.”)



Números inteiros. Ideia: pensar números inteiros como "$m - n$", com $m, n \in \mathbb{N}$. Pares (m, n) diferentes podem *representar* o mesmo inteiro. Por exemplo:

$$0 - 1 = 2 - 3.$$

Definição 4.12. O conjunto dos *números inteiros* é o quociente $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$, onde $\sim$ é a relação de equivalência tal que

$$(m, n) \sim (p, q) \quad \text{se} \quad m + q = n + p.$$

(Pense: "$m - n = p - q$".)

Exercício 4.13. Verifique que $\sim$ acima é de fato uma relação de equivalência.

Operações.

- Soma: $\overline{(m, n)} + \overline{(p, q)} = \overline{(m + p,\, n + q)}$.
- Produto: $\overline{(m, n)} \cdot \overline{(p, q)} = \overline{(mp + nq,\, mq + np)}$.

(Para o produto, pense: $(m - n) \cdot (p - q) = mp + nq - (mq + np)$.)

Teorema 4.14. *Valem as seguintes propriedades:*

1) A soma e o produto são comutativos e associativos.

2) $\overline{(m, n)} + \overline{(n, m)} = \overline{(0, 0)}$ *e* $\overline{(0, 0)} + \overline{(m, n)} = \overline{(m, n)}$.

3) Vale a distributiva:

$$\overline{(m, n)} \cdot (\overline{(p, q)} + \overline{(r, s)}) = \overline{(m, n)} \cdot \overline{(p, q)} + \overline{(m, n)} \cdot \overline{(r, s)}.$$

4) $\overline{(1, 0)} \cdot \overline{(m, n)} = \overline{(m, n)}$.

Isto é: $\mathbb{Z}$ é um *anel* comutativo com unidade $\overline{(1, 0)}$ e zero $\overline{(0, 0)}$. O inverso aditivo é $-\overline{(m, n)} = \overline{(n, m)}$.

Simplificando a representação.

Proposição 4.15. *Dado* $\overline{(m, n)} \in \mathbb{Z}$*, existe um único* $k \in \mathbb{N}$ *tal que* $\overline{(m, n)} = \overline{(k, 0)}$ *ou* $\overline{(m, n)} = \overline{(0, k)}$.

Demonstração.

- Se $m = n$, então $\overline{(m, n)} = \overline{(0, 0)}$ $(k = 0)$.
- Se $n < m$, existe $k \neq 0$ tal que $m = n + k$; logo, $\overline{(m, n)} = \overline{(k, 0)}$.

- Se $m < n$, existe $k \neq 0$ tal que $m + k = n$; logo, $\overline{(m,n)} = \overline{(0,k)}$. $\square$

Definição 4.16. Um elemento de $\mathbb{Z}$ da forma $\overline{(k,0)}$ (resp. $\overline{(0,k)}$) é dito *positivo* (resp. *negativo*) e denotamos $k = \overline{(k,0)}$ (resp. $-k = \overline{(0,k)}$).

Assim, um *número inteiro* é algo da forma

$$k \quad \text{ou} \quad -k,$$

onde $k \in \mathbb{N}$. Note que $0 = -0$. Temos

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Exercício 4.17.

1) Mostre que positivo $\cdot$ positivo = positivo, positivo $\cdot$ negativo = negativo e negativo $\cdot$ negativo = positivo.

2) Explique como estender a ordem $\leqslant$ em $\mathbb{N}$ para uma ordem em $\mathbb{Z}$, de maneira que $\{n \in \mathbb{Z} : n \geqslant 0\}$ seja o conjunto dos números positivos e $\{n \in \mathbb{Z} : n \leqslant 0\}$ o conjunto dos negativos.

Aula 5 (26/08)

3) Divisibilidade (em $\mathbb{Z}$)

Divisão euclidiana. A divisão euclidiana é a "divisão com resto" que aprendemos na escola. Por exemplo,

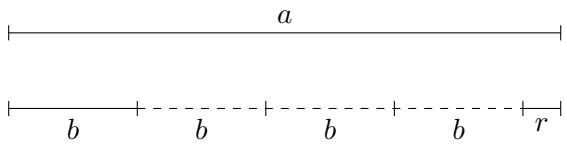
$$11 = \underbrace{2}_{\text{quociente}} \cdot 4 + \underbrace{3}_{\text{resto}}, \qquad \begin{array}{r|l} 11 & 4 \\ \cline{2-2} 3 & 2 \end{array}$$

Teorema 5.1. *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então existem únicos inteiros q (*quociente*) e r (*resto*) tais que*

$$a = qb + r, \qquad 0 \leqslant r < |b|.$$

(Lembre que $|b| = b$ se $b \geqslant 0$ e $|b| = -b$ se $b < 0$.)

Observação 5.2. Para Euclides, números positivos representam medidas de segmentos:



O quociente q é o número de segmentos de tamanho b que cabem em um segmento de tamanho a; o resto r é o que sobra.

Demonstração. Faremos apenas o caso $a, b > 0$.

Existência. Seja q o maior natural tal que

$$qb \leqslant a$$

(ele existe pelo princípio da boa ordem: o conjunto $\{n \in \mathbb{N} : nb > a\} \neq \emptyset$ tem um mínimo) e defina

$$r = a - qb \geqslant 0.$$

Pela maximalidade de q, temos $a < (q+1)b$. Logo,

$$r = a - qb < (q+1)b - qb = b.$$

Unicidade. Se q', r' são tais que $0 \leqslant r' < b$ e $a = q'b + r'$, então

$$qb + r = a = q'b + r' \iff (q - q')b = r' - r.$$

Como $0 \leqslant r, r' < b$, temos $|r - r'| < b$. Logo,

$$|q - q'|\, b = |r - r'| < b.$$

Como o valor absoluto de um inteiro não nulo é $\geqslant 1$, a única possibilidade é $q = q'$ e $r = r'$. □

Exemplo 5.3. Os números inteiros que deixam resto 3 na divisão por 7 são

$$\ldots, -11, -4, 3, 10, 17, \ldots$$

Trata-se de uma PA de razão 7. Fórmula do termo geral: $7q + 3$.

Exemplo 5.4. A sequência de Fibonacci $F_0, F_1, F_2, \ldots$ é dada por $F_0 = 0$, $F_1 = 1$ e $F_{n+2} = F_{n+1} + F_n$:

n	0	1	2	3	4	5	6	7	8	$\cdots$
F_n	0	1	1	2	3	5	8	13	21	$\cdots$

Qual é o resto da divisão de F_{n+2} por F_{n+1}? Pela unicidade,

$$F_{n+2} = \underbrace{1}_{\text{quociente}} \cdot F_{n+1} + \underbrace{F_n}_{\text{resto}}, \qquad 0 \leqslant F_n < F_{n+1}$$

(para $n \neq 1$).

Exemplo 5.5. Qual é o resto da divisão de 7^{2024} por 6? Pela fórmula

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1),$$

obtemos

$$\begin{aligned} & 7^{2024} - 1 = (7-1) \cdot (7^{2023} + \cdots + 1) \\ \iff \quad & 7^{2024} = \underbrace{(7^{2023} + \cdots + 1)}_{\text{quociente}} \cdot 6 + \underbrace{1}_{\text{resto}}. \end{aligned}$$

Exercício 5.6.

1) Encontre todos os inteiros cujos quociente e resto são iguais na divisão por 6 (exemplo: $14 = 2 \cdot 6 + 2$). Generalize para $b \geqslant 1$ qualquer no lugar de 6.

2) Mostre que um quadrado ímpar deixa resto 1 na divisão por 4.

3) Encontre um inteiro positivo que deixa resto 4 na divisão por 5 e resto 7 na divisão por 13.

Aplicação: representação de inteiros em uma base. Notação decimal:

$$\begin{aligned} 2024 &= 2 \cdot 1000 + 0 \cdot 100 + 2 \cdot 10 + 4 \\ &= 2 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0, \end{aligned}$$

onde os coeficientes $2, 0, 2, 4$ são os "dígitos". Podemos trocar o 10 por uma "base" b qualquer.

Teorema 5.7. *Seja $b \geqslant 2$ um inteiro. Todo inteiro $a \geqslant 0$ se escreve de maneira única na forma*

$$a = r_n b^n + \cdots + r_1 b + r_0,$$

onde $n \in \mathbb{N}$ e os r_i são inteiros tais que $0 \leqslant r_i < b$.

Demonstração (só da existência). Se $a < b$, não há nada a fazer: $a = r_0$. Se não, dividimos a por b:

$$a = q_0 b + r_0, \qquad 0 \leqslant r_0 < b.$$

Se $q_0 < b$, acabamos ($q_0 = r_1$). Se não, dividimos q_0 por b:

$$q_0 = q_1 b + r_1, \qquad 0 \leqslant r_1 < b,$$

donde

$$a = (q_1 b + r_1)b + r_0 = q_1 b^2 + r_1 b + r_0.$$

Se $q_1 < b$, acabamos ($q_1 = r_2$). Se não, ...

Este processo termina (isto é, existe n tal que $q_n < b$) pois $q_i < q_{i-1}$ em cada etapa. □

Exercício 5.8. Demonstre a unicidade.

Notação. $a = (r_n \cdots r_1 r_0)_b$.

Exemplo 5.9. Vamos escrever 2024 em base 2 ("números binários"):

$$\begin{aligned}
2024 &= 2 \cdot 1012 = 2^2 \cdot 506 = 2^3 \cdot 253 \\
&= 2^3 \cdot (2 \cdot 126 + 1) = 2^4 \cdot 126 + 2^3 \\
&= 2^5 \cdot 63 + 2^3 = 2^5 \cdot (2 \cdot 31 + 1) + 2^3 \\
&= 2^6 \cdot 31 + 2^5 + 2^3 \\
&= 2^6 \cdot (2 \cdot 15 + 1) + 2^5 + 2^3 \\
&= 2^7 \cdot 15 + 2^6 + 2^5 + 2^3 \\
&= 2^7 \cdot (2 \cdot 7 + 1) + 2^6 + 2^5 + 2^3 \\
&= 2^8 \cdot 7 + 2^7 + 2^6 + 2^5 + 2^3 \\
&= 2^9 \cdot 3 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3 \\
&= 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3.
\end{aligned}$$

Logo, $2024 = (11111101000)_2$.

Exercício 5.10.

1) Escreva 1472 em base 5 e em base 16 (considere os símbolos $A = 10$, $B = 11, \ldots, F = 15$).

2) Determine os inteiros cuja representação em base 3 é da forma $(22 \cdots 2)_3$.

Aula 6 (28/08)

3) Divisibilidade (cont.)

Aula passada. Divisão euclidiana: $a = qb + r$, com $0 \leqslant r < |b|$.

Hoje: a "divisão exata", isto é, o caso $r = 0$.

Definição 6.1. Sejam $a, b \in \mathbb{Z}$. Dizemos que b *divide* a se existe $q \in \mathbb{Z}$ tal que $a = qb$. Notação: $b \mid a$.

Terminologias alternativas:

- "b é um fator de a";
- "b é um divisor de a";
- "a é um múltiplo de b";
- "a é divisível por b".

Se b *não* divide a, denotamos $b \nmid a$.

Exemplo 6.2.

- $10 \mid 4590$, pois $4590 = 459 \cdot 10$.
- $3 \nmid 10$.

Observação 6.3. 0 é divisível por todo outro número!

Exemplo 6.4. Os divisores positivos de 12 são $1, 2, 3, 4, 6, 12$.

Exemplo 6.5. Os múltiplos de 3 são

$$\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots,$$

isto é, os números da forma $3q$, $q \in \mathbb{Z}$.

Exercício 6.6. Mostre que o produto de três inteiros consecutivos quaisquer é divisível por 6, isto é, $6 \mid n(n+1)(n+2)$ para todo $n \in \mathbb{Z}$.

Exercício 6.7. Mostre que a diferença de dois quadrados ímpares é divisível por 8, isto é, $8 \mid m^2 - n^2$ para m, n ímpares.

Proposição 6.8 (Propriedades básicas)**.**

(1) (Combinação linear) Se $b \mid a_1$ e $b \mid a_2$, então $b \mid x_1 a_1 + x_2 a_2$ para quaisquer $x_1, x_2 \in \mathbb{Z}$.

(2) (Transitividade) Se $c \mid b$ e $b \mid a$, então $c \mid a$.

(3) ("Divisores são menores") Se $b \mid a$ e $a \neq 0$, então $|b| \leqslant |a|$.

Demonstração. (1) Se $b \mid a_1$ e $b \mid a_2$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $a_1 = q_1 b$ e $a_2 = q_2 b$. Logo,

$$x_1 a_1 + x_2 a_2 = x_1 q_1 b + x_2 q_2 b = (x_1 q_1 + x_2 q_2) b.$$

(2) Se $c \mid b$ e $b \mid a$, então existem $p, q \in \mathbb{Z}$ tais que $b = pc$ e $a = qb$. Logo,

$$a = qb = (qp)c.$$

(3) Se $b \mid a$ e $a \neq 0$, então existe $q \neq 0$ tal que $a = qb$. Como $|q| \geqslant 1$, obtemos

$$|a| = |q|\,|b| \geqslant |b|. \qquad \square$$

Exemplo 6.9. Encontremos todos os $n \in \mathbb{Z}$ tais que $2n - 1 \mid n^3 + 1$.

Ideia: usar as propriedades para diminuir o grau de $n^3 + 1$. Como $2n - 1 \mid 2n - 1$ e $2n - 1 \mid n^3 + 1$, temos

$$2n - 1 \mid 2 \cdot (n^3 + 1) - n^2 \cdot (2n - 1) = 2 + n^2.$$

(Usamos a combinação linear com $a_1 = 2n - 1$, $a_2 = n^3 + 1$, $x_1 = -n^2$ e $x_2 = 2$.) Analogamente,

$$2n - 1 \mid 2 \cdot (2 + n^2) - n \cdot (2n - 1) = 4 + n.$$

Mais uma vez:

$$2n - 1 \mid 2 \cdot (4 + n) - (2n - 1) = 9.$$

Os divisores de 9 são

$$-9,\ -3,\ -1,\ 1,\ 3,\ 9$$

(encontramos a lista dos divisores de 9 usando a propriedade "divisores são menores"). Temos 6 possibilidades:

$2n-1$	n	n^3+1
-9	-4	-63
-3	-1	0
-1	0	1
1	1	2
3	2	9
9	5	$126 = 14 \cdot 9$

Em todos os casos acima, $2n - 1 \mid n^3 + 1$. Logo, a lista dos inteiros n que satisfazem $2n - 1 \mid n^3 + 1$ é:

$$-4,\ -1,\ 0,\ 1,\ 2,\ 5.$$

Exercício 6.10. Encontre todos os inteiros positivos n tais que $2n^2 + 1 \mid n^3 + 9n - 17$.

Exercício 6.11. Mostre que, se $n \mid a - b$, então $n \mid a^k - b^k$ para todo $k \in \mathbb{N}$.

Definição 6.12. Sejam $a, b \in \mathbb{Z}$ (não ambos nulos). O *máximo divisor comum* de a e b é o maior inteiro d tal que $d \mid a$ e $d \mid b$. Notação: $\text{mdc}(a, b)$ ou (a, b).

Observação 6.13. O mdc está bem definido pois, pela propriedade "divisores são menores", o conjunto $\{d \in \mathbb{Z} : d \mid a \text{ e } d \mid b\}$ é limitado superiormente (e portanto tem um máximo).

Exemplo 6.14.

- $(10, 12) = 2$;
- $(10, -12) = 2$;
- $(a, 0) = |a|$.

O mdc sempre é positivo!

Teorema 6.15 (Bézout)**.** *Dados $a, b \in \mathbb{Z}$, não ambos nulos, existem $x, y \in \mathbb{Z}$ tais que $ax + by = (a, b)$.*

Exemplo 6.16.

- $(10, 12) = 2$:

$$-1 \cdot 10 + 1 \cdot 12 = 2, \qquad 5 \cdot 10 - 4 \cdot 12 = 2$$

  (x, y não são únicos!).

- $(16, 7) = 1$: $\quad -3 \cdot 16 + 7 \cdot 7 = 1$.

Como calcular o mdc e os inteiros x, y? Próximas aulas!

Corolário 6.17. *Se $c \mid a$ e $c \mid b$, então $c \mid (a, b)$. Além disso, (a, b) é o menor inteiro positivo com esta propriedade.*

Demonstração. Sejam $x, y \in \mathbb{Z}$ tais que $ax + by = (a, b)$. Pelas propriedades de transitividade e de combinação linear, se $c \mid a$ e $c \mid b$, então $c \mid ax+by$. Se d é um inteiro positivo com a mesma propriedade, então $(a, b) \mid d$ (pois $(a, b) \mid a$ e $(a, b) \mid b$). Pela propriedade "divisores são menores", $(a, b) \leqslant d$. □

Exercício 6.18. Mostre que $d = (a, b)$ se, e somente se, existem $a_1, b_1 \in \mathbb{Z}$ tais que $a = da_1$, $b = db_1$ e $(a_1, b_1) = 1$. (Exemplo: $(10, 12) = 2$, $10 = 2 \cdot 5$, $12 = 2 \cdot 6$ e $(5, 6) = 1$.)

Aula 7 (02/09)

3) Divisibilidade (cont.)

Aula passada. Máximo divisor comum: $\mathrm{mdc}(a,b) = (a,b)$.

Teorema 7.1 (Bézout)**.** *Dados $a, b \in \mathbb{Z}$, não ambos nulos, existem $x, y \in \mathbb{Z}$ tais que*

$$ax + by = (a,b).$$

Demonstração. Por hipótese, $a \neq 0$ ou $b \neq 0$. Seja

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

e $d = ax_0 + by_0$ o menor elemento > 0 de I (que existe pelo princípio da boa ordem, pois $a^2 + b^2 \in I$ é positivo).

Afirmação: d divide todos os elementos de I. De fato, se $m = ax+by \in I$, então, pela divisão euclidiana,

$$\begin{aligned} m = qd + r, \quad 0 \leqslant r < d &\iff ax + by = q(ax_0 + by_0) + r \\ &\iff r = a(x - qx_0) + b(y - qy_0) \in I. \end{aligned}$$

Pela minimalidade de d, temos $r = 0$. Logo, $d \mid m$.

Em particular, $d \mid a$ e $d \mid b$. Logo, $d \leqslant (a,b)$.

Por outro lado, como $(a,b) \mid a$ e $(a,b) \mid b$, então $(a,b) \mid d = ax_0 + by_0$. Logo, $(a,b) \leqslant d$. □

Definição 7.2. Dizemos que a e b são *coprimos*[3] se $(a,b) = 1$. Pelo teorema de Bézout, isso é equivalente a existirem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.

Exemplo 7.3. Os números 5 e 12 são coprimos: $5 \cdot 5 - 2 \cdot 12 = 1$.

Exercício 7.4. Mostre que dois termos consecutivos da sequência de Fibonacci são coprimos.

Corolário 7.5. *Se a e b são coprimos e $a \mid b \cdot c$, então $a \mid c$.*

Demonstração. Existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Logo, $acx + bcy = c$. Como $a \mid acx$ e $a \mid bcy$, temos $a \mid c$. □

Definição 7.6. Dados $a, b \geqslant 1$ inteiros, o *mínimo múltiplo comum* de a e b é o menor inteiro $m \geqslant 1$ tal que $a \mid m$ e $b \mid m$. Notação: $\mathrm{mmc}(a,b) = [a,b]$.

Exemplo 7.7. $[12, 10] = 60$. Note que $12 \cdot 10 = 120 = 2 \cdot 60 = (12, 10) \cdot [12, 10]$.

[3] Também se diz "primos entre si", ou "sem fatores em comum".

Proposição 7.8. *Dados $a, b \geqslant 1$ inteiros, temos*

$$a \cdot b = (a, b) \cdot [a, b].$$

Demonstração. Seja $d = (a, b)$ e $m = [a, b]$. Pelo exercício da aula passada, podemos escrever $a = d \cdot a_1$ e $b = d \cdot b_1$, com a_1 e b_1 coprimos. Como $a \mid m$, podemos escrever $m = aq = da_1q$. Como

$$b \mid m \iff db_1 \mid da_1q,$$

obtemos $b_1 \mid a_1q$ ("cancelando d"). Pelo corolário, concluímos que $b_1 \mid q$. Pela minimalidade de m, devemos ter $b_1 = q$, isto é, $m = da_1b_1$. Logo,

$$d \cdot m = d^2a_1b_1 = (da_1)(db_1) = ab. \qquad \square$$

Em outras palavras: "para calcular o mmc, basta saber calcular o mdc".

Lema 7.9 (Euclides)**.** *Se $a = qb + r$, então $(a, b) = (b, r)$.*

Observação 7.10. No enunciado acima, r não precisa satisfazer $0 \leqslant r < |b|$.

Demonstração. Se $d \mid a$ e $d \mid b$, então $d \mid a - qb = r$. Isto mostra que $(a, b) \leqslant (b, r)$. Por outro lado, se $d \mid b$ e $d \mid r$, então $d \mid qb + r = a$. Logo, $(b, r) \leqslant (a, b)$. $\square$

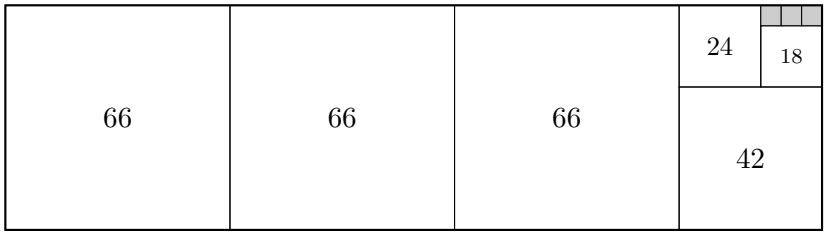
Algoritmo de Euclides. Aplicar o lema acima para a divisão euclidiana repetidamente, até obter resto 0.

Exemplo 7.11. Calculemos $(240, 66)$.

$$\begin{aligned}
240 &= 3 \cdot 66 + 42 && \overset{\text{Lema}}{\Longrightarrow} && (240, 66) = (66, 42) = ? \\
66 &= 1 \cdot 42 + 24 && \overset{\text{Lema}}{\Longrightarrow} && (66, 42) = (42, 24) = ? \\
42 &= 1 \cdot 24 + 18 && \overset{\text{Lema}}{\Longrightarrow} && (42, 24) = (24, 18) = ? \\
24 &= 1 \cdot 18 + 6 && \overset{\text{Lema}}{\Longrightarrow} && (24, 18) = (18, 6) = ? \\
18 &= 3 \cdot 6 + 0 && \overset{\text{Lema}}{\Longrightarrow} && (18, 6) = (6, 0) = 6.
\end{aligned}$$

Logo, $(240, 66) = 6$.

Observação 7.12 (Interpretação geométrica). O algoritmo de Euclides tem uma interpretação geométrica simples. Do retângulo 240×66, retiramos o maior número possível de quadrados de lado 66 (três); do retângulo 42×66 que sobra, retiramos quadrados de lado 42 (um); e assim por diante. Os lados dos quadrados são os sucessivos divisores e restos, e o processo termina quando o retângulo restante é preenchido exatamente por quadrados, cujo lado (6, em cinza) é o mdc.



Em particular, 6 é o maior lado de um quadrado com o qual se pode ladrilhar o retângulo 240×66.

Exemplo 7.13. Calculemos $(1001, 109)$:

$$\begin{aligned} 1001 &= 9 \cdot 109 + 20 \\ 109 &= 5 \cdot 20 + 9 \\ 20 &= 2 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Logo, $(1001, 109) = (109, 20) = (20, 9) = (9, 2) = (2, 1) = (1, 0) = 1$.

Exemplo 7.14. Calculemos $[2^{1012} - 1,\ 2^{1012} + 1]$. Como $2^{1012} + 1 = (2^{1012} - 1) + 2$, temos

$$(2^{1012} + 1,\ 2^{1012} - 1) = (2^{1012} - 1,\ 2) = 1,$$

pois $2^{1012} - 1$ é ímpar. Logo,

$$[2^{1012} - 1,\ 2^{1012} + 1] = \frac{(2^{1012} - 1)(2^{1012} + 1)}{(2^{1012} - 1,\ 2^{1012} + 1)} = 2^{2024} - 1.$$

Exercício 7.15.

1) Calcule $(12345, 67890)$.

2) Encontre todos os pares de inteiros a, b tais que $(a, b) = 18$ e $[a, b] = 720$.

3) Mostre que $7k + 5$ e $4k + 3$ são coprimos para qualquer inteiro k.

Aula 8 (04/09)

3) Divisibilidade (cont.)

Aula passada. Algoritmo de Euclides.

O algoritmo de Euclides também pode ser usado para encontrar $x, y \in \mathbb{Z}$ explícitos tais que $ax + by = (a, b)$ ("coeficientes de Bézout").

Exemplo 8.1 ($a = 30$, $b = 22$)**.**

$$\begin{array}{lrcl}
\text{Eq. 1:} & 30 = 1 \cdot 22 + 8 & \iff & 8 = 30 - 1 \cdot 22 \\
\text{Eq. 2:} & 22 = 2 \cdot 8 + 6 & \iff & 6 = 22 - 2 \cdot 8 \\
\text{Eq. 3:} & 8 = 1 \cdot 6 + \boxed{2} & \iff & \boxed{2} = 8 - 1 \cdot 6 \\
\text{Eq. 4:} & 6 = 3 \cdot 2 + 0 & &
\end{array}$$

Aqui $2 = (30, 22)$ é o último resto não nulo. Pela Eq. 3,

$$2 = 1 \cdot 8 - 1 \cdot 6.$$

Substituindo o valor 6 da Eq. 2:

$$2 = 1 \cdot 8 - 1 \cdot (22 - 2 \cdot 8) = -1 \cdot 22 + 3 \cdot 8.$$

Substituindo o valor 8 da Eq. 1:

$$2 = -1 \cdot 22 + 3 \cdot (30 - 1 \cdot 22) = 3 \cdot 30 - 4 \cdot 22.$$

Obtemos $x = 3$, $y = -4$.

Pensando de maneira matricial:

$$\text{Eq. 1:} \quad \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 30 \\ 22 \end{pmatrix} = \begin{pmatrix} 22 \\ 8 \end{pmatrix}, \qquad \text{Eq. 2:} \quad \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 22 \\ 8 \end{pmatrix} = \begin{pmatrix} 8 \\ 6 \end{pmatrix},$$

$$\text{Eq. 3:} \quad \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 8 \\ 6 \end{pmatrix} = \begin{pmatrix} 6 \\ 2 \end{pmatrix}, \qquad \text{Eq. 4:} \quad \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 6 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Logo,

$$\begin{aligned}
\begin{pmatrix} 2 \\ 0 \end{pmatrix} &\overset{\text{Eq. 4}}{=} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 6 \\ 2 \end{pmatrix} \overset{\text{Eq. 3}}{=} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 8 \\ 6 \end{pmatrix} \\
&\overset{\text{Eq. 2}}{=} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 22 \\ 8 \end{pmatrix} \\
&\overset{\text{Eq. 1}}{=} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}}_{\begin{pmatrix} 3 & -4 \\ -11 & 15 \end{pmatrix}} \begin{pmatrix} 30 \\ 22 \end{pmatrix},
\end{aligned}$$

e a primeira linha da matriz produto nos dá os coeficientes $x = 3$, $y = -4$. Esta forma é útil para implementar o algoritmo no computador.

Exercício 8.2. Calcule a matriz A_n tal que

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = A_n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Quantas etapas o algoritmo de Euclides necessita neste caso?

Observação 8.3. Pode-se mostrar, usando a sequência de Fibonacci, que o "custo computacional" do algoritmo de Euclides é da ordem de $\log(\min\{a, b\})$, pois $n \approx \log F_n$.

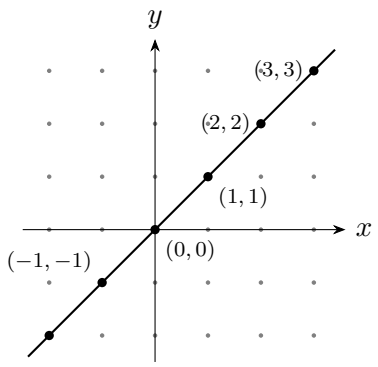
Exercício 8.4. Encontre $x, y \in \mathbb{Z}$ tais que $240x + 66y = 6$.

4) Equações diofantinas lineares

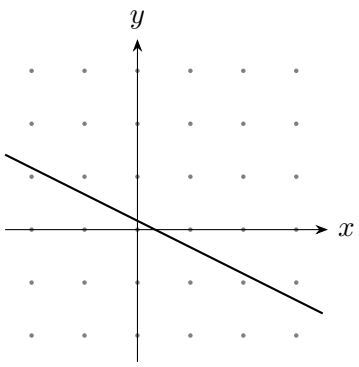
Dados $a, b, c \in \mathbb{Z}$, queremos resolver (em $x, y \in \mathbb{Z}$) a equação

$$ax + by = c.$$

Observação 8.5 (Interpretação geométrica). O gráfico em $\mathbb{R}^2$ de uma tal equação é uma reta L. Buscamos encontrar $L \cap \mathbb{Z}^2$ (os pontos da reta com coordenadas inteiras).



$x - y = 0$



$3x + 6y = 1$: não intersecta $\mathbb{Z}^2$!

Teorema 8.6. *Sejam $a, b \in \mathbb{Z}$ e $d = (a, b)$.*

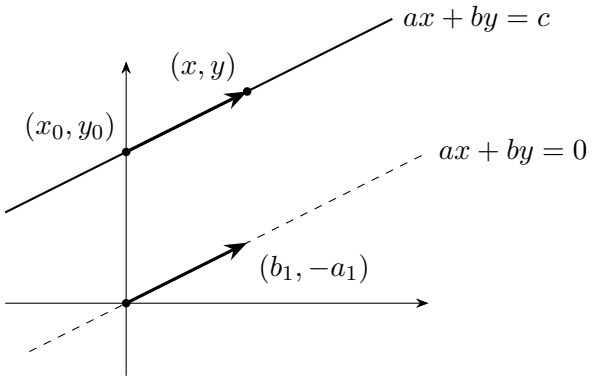
(1) Se $d \nmid c$, então a equação $ax + by = c$ não possui nenhuma solução com $x, y \in \mathbb{Z}$.

(2) Se $d \mid c$, então a equação $ax + by = c$ possui infinitas soluções com $x, y \in \mathbb{Z}$. Dada uma solução particular x_0, y_0, todas as outras são da forma

$$\begin{cases} x = x_0 + tb_1 \\ y = y_0 - ta_1 \end{cases}, \qquad t \in \mathbb{Z},$$

onde $a = da_1$, $b = db_1$.

Observação 8.7. Pensando geometricamente: as soluções são obtidas a partir de (x_0, y_0) andando sobre a reta $ax + by = c$ por múltiplos inteiros do vetor $(b_1, -a_1)$, que é paralelo à reta $ax + by = 0$.



Demonstração. (1) Pela contrapositiva: se existem $x, y \in \mathbb{Z}$ tais que $ax + by = c$, então, como $d \mid a$ e $d \mid b$, temos $d \mid ax + by = c$ (combinação linear).

(2) Pelo teorema de Bézout, existem $u, v \in \mathbb{Z}$ tais que $au + bv = d$. Se $q \in \mathbb{Z}$ é tal que $c = qd$, então

$$a(uq) + b(vq) = qd = c.$$

Logo, existe pelo menos uma solução inteira.

Seja x_0, y_0 uma solução qualquer. Então $x_0 + tb_1$, $y_0 - ta_1$ também é uma solução, pois

$$a(x_0 + tb_1) + b(y_0 - ta_1) = ax_0 + by_0 + t(\underbrace{ab_1 - ba_1}_{=0}) = c.$$

Reciprocamente, seja x, y outra solução. Então

$$a(x - x_0) + b(y - y_0) = ax + by - ax_0 - by_0 = c - c = 0.$$

Logo, $a(x - x_0) = -b(y - y_0)$ e, dividindo por d,

$$a_1(x - x_0) = -b_1(y - y_0). \qquad (*)$$

Em particular, $b_1 \mid a_1(x - x_0)$. Como $(a_1, b_1) = 1$, obtemos $b_1 \mid x - x_0$. Seja $t \in \mathbb{Z}$ tal que $x - x_0 = tb_1$. Substituindo em $(*)$,

$$a_1 tb_1 = -b_1(y - y_0) \iff y - y_0 = -a_1 t. \qquad \square$$

Observação 8.8. Na prática, usamos como solução particular $x_0 = qu$, $y_0 = qv$, onde u e v são os coeficientes de Bézout dados pelo algoritmo de Euclides e q é tal que $c = qd$.

Exemplo 8.9. Encontremos todas as soluções x, y de $3x + 2y = 5$. Uma solução particular é $x_0 = 1$, $y_0 = 1$. Como $(3, 2) = 1$, segue do teorema que as soluções são da forma

$$x = 1 + 2t, \quad y = 1 - 3t, \qquad t \in \mathbb{Z}.$$

Exercício 8.10.

1) Determine se a equação admite solução com $x, y \in \mathbb{Z}$ e, caso positivo, dê uma fórmula para a solução geral:

   (a) $144x + 34y = 20$;

   (b) $119x - 29y = 8$.

2) Sejam $a, b \in \mathbb{N}$ tais que $(a, b) = 1$ e $x_0, y_0 \in \mathbb{Z}$ uma solução particular de $ax_0 + by_0 = c$. Mostre que o número de soluções positivas $(x, y > 0)$ de $ax + by = c$ é o número de inteiros k tais que

   $$-\frac{x_0}{b} < k < \frac{y_0}{a}$$

   (os extremos são números racionais).

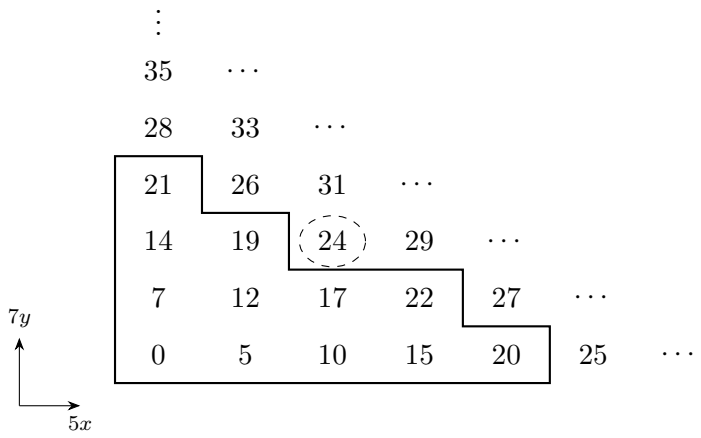
3) Gastei R$ 1770 no mercado com muitos pacotes de café a R$ 31 e algumas barras de chocolate a R$ 21. Quantos pacotes de café e barras de chocolate eu comprei?

Aula 9 (09/09)

4) Equações diofantinas lineares (cont.)

Se $a, b, c \geqslant 0$, quando existe solução $x, y \geqslant 0$ para $ax + by = c$?

Exemplo 9.1. Quais os possíveis valores de c tais que $5x+7y = c$ $(x, y \geqslant 0)$? Como $(5, 7) = 1$, sabemos que podemos obter qualquer valor de c se x, y puderem ser negativos. Com $x, y \geqslant 0$, dispomos os valores $5x + 7y$ numa tabela (a coluna indica x e a linha indica y):



A região delimitada contém todos os valores obtidos menores que 24.

Conjectura: além de $0, 5, 7, \ldots, 22$, podemos obter *todos* os números $\geqslant 24$.

Lema 9.2. *Sejam $a, b, c \geqslant 1$ inteiros com $(a, b) = 1$.*

(1) Existem únicos $r, s \in \mathbb{Z}$ *tais que $ar + bs = c$ e $0 \leqslant r < b$.*

(2) Se a equação $ax + by = c$ admite solução com $x, y \geqslant 0$, então a solução r, s acima é uma delas (isto é, $s \geqslant 0$).

Demonstração. (1) Seja x_0, y_0 uma solução qualquer e r o resto da divisão de x_0 por $-b$:

$$x_0 = q \cdot (-b) + r \iff r = x_0 + qb.$$

Tome $s = y_0 - qa$; então $ar + bs = ax_0 + by_0 = c$. A unicidade segue do teorema da aula passada: se r', s' satisfazem $ar' + bs' = c$, então existe t tal que $r' = x_0 + tb$, $s' = y_0 - ta$. Mas

$$r' = x_0 + tb \iff x_0 = t(-b) + r'.$$

Logo, se $0 \leqslant r' < b$, devemos ter $r = r'$ e $q = t$ pela unicidade da divisão euclidiana.

(2) Sejam $x, y \geqslant 0$ tais que $ax + by = c$. Dividindo x por b: $x = qb + r$, $0 \leqslant r < b$. Logo,

$$ax + by = c \iff a(qb + r) + by = c \iff ar + b(y + aq) = c.$$

Pela unicidade do item (1), temos $y + aq = s$, e portanto $s \geqslant 0$. □

Proposição 9.3. *Sejam $a, b, c \geqslant 1$ inteiros com $(a, b) = 1$. Se $c > ab - a - b$, então $ax + by = c$ admite solução com $x, y \geqslant 0$.*

Demonstração. Se $ax + by = c$ *não* admite solução com $x, y \geqslant 0$, então a solução r, s do lema anterior satisfaz

$$0 \leqslant r < b, \qquad s < 0.$$

Logo, o conjunto de tais c é

$$\{ar + bs : 0 \leqslant r < b,\ s < 0\} \cap \mathbb{N}.$$

O maior elemento deste conjunto é

$$a \cdot (b - 1) + b \cdot (-1) = ab - a - b.$$ □

Exemplo 9.4. No exemplo anterior ($a = 5$, $b = 7$): $ab - a - b = 5 \cdot 7 - 5 - 7 = 35 - 12 = 23$.

Exercício 9.5. Quais são todos os valores possíveis de se obter combinando notas de 20 e 50 reais?

Exercício 9.6. Sejam $a, b > 0$ coprimos. Mostre que, se $c \geqslant 0$, a equação $ax - by = c$ tem infinitas soluções $x, y \geqslant 0$.

Mais variáveis? Por exemplo, $ax + by + cz = d$.

Definição 9.7. Dados $a_1, \ldots, a_n \in \mathbb{Z}$, o *máximo divisor comum* de $a_1, \ldots, a_n$ é o maior inteiro d tal que $d \mid a_1, \ldots, d \mid a_n$. Notação: $(a_1, \ldots, a_n)$.

Exercício 9.8. Mostre que $(a_1, a_2, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n)$. (Exemplo: $(6, 15, 35) = 1 = (3, 35) = ((6, 15), 35)$.)

Se $(a, b, c) \nmid d$, então $ax + by + cz = d$ não admite solução com $x, y, z \in \mathbb{Z}$. Vale a volta?

Exemplo 9.9. Consideremos $6x + 15y + 35z = 1$. Ideia: "reduzir ao caso de duas variáveis". Considere as equações

$$\begin{cases} 6x + 15y = 3q \\ 3q + 35z = 1 \end{cases}$$

A equação $3q + 35z = 1$ tem solução, pois $(3, 35) = 1$. Pelo algoritmo de Euclides:

$$\begin{aligned} 35 &= 11 \cdot 3 + 2 & \qquad 1 &= 3 - 1 \cdot 2 \\ 3 &= 1 \cdot 2 + 1 & &= 3 - 1 \cdot (35 - 11 \cdot 3) \\ & & &= 12 \cdot 3 - 1 \cdot 35. \end{aligned}$$

Logo, $q_0 = 12$, $z_0 = -1$ é uma solução de $3q + 35z = 1$. Agora resolvemos

$$6x + 15y = 3 \cdot 12 \iff 2x + 5y = 12,$$

obtendo, por exemplo, $x_0 = 11$, $y_0 = -2$. Assim, $x_0 = 11$, $y_0 = -2$, $z_0 = -1$ é uma solução de $6x + 15y + 35z = 1$ (de fato, $66 - 30 - 35 = 1$).

Exercício 9.10.

1) Encontre uma fórmula com 2 variáveis para parametrizar as soluções inteiras de $6x + 15y + 35z = 1$.

2) Mostre que, se $a_1, \ldots, a_n \in \mathbb{Z}$, então a equação $a_1x_1 + \cdots + a_nx_n = b$ admite solução se, e somente se, $(a_1, \ldots, a_n) \mid b$.

Mais equações? Consideremos um sistema

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \iff Ax = b, \qquad A \in M_{m\times n}(\mathbb{Z}).$$

Pode-se mostrar que o sistema tem solução (inteira) se, e somente se, para todo vetor(-linha) racional u, se uA é inteiro, então ub é inteiro.

Na prática, resolvemos o sistema através de "operações elementares" nas linhas e colunas de A (tipo escalonar matriz); trata-se da "forma normal de Smith".

Exercício 9.11. Encontre uma solução inteira de

$$\begin{cases} 3x + 5y + 7z = 560 \\ 9x + 25y + 49z = 2920 \end{cases}$$

Aula 10 (11/09)

5) Primos

Definição 10.1. Um natural $p > 1$ é dito *primo* se os únicos divisores positivos de p são 1 e p.

Exemplo 10.2. Os números $2, 3, 5, 7, 11, \ldots, 101, \ldots$ são primos.

Um natural $n > 1$ que não é primo é dito *composto*.

Observação 10.3. O número 1 não é primo nem composto!

Exercício 10.4. Mostre que, se $2^p - 1$ é primo, então p é primo. Vale a volta?

Observação 10.5. Um primo da forma $2^p - 1$ é dito *primo de Mersenne*. Por exemplo,

$$3,\ 7,\ \ldots,\ 2^{82589933} - 1.$$

Proposição 10.6. *Seja p um número primo.*

(1) Para qualquer $a \in \mathbb{Z}$, $(p, a) = 1$ ou $(p, a) = p$.

(2) Para quaisquer $a, b \in \mathbb{Z}$, se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração. (1) Como $(p, a) \mid p$, temos $(p, a) = 1$ ou $(p, a) = p$.

(2) Se $(p, a) = p$, então $p \mid a$. Se não, pelo item (1), $(p, a) = 1$. Como $p \mid ab$, segue de um corolário visto em aulas anteriores (se $p \mid ab$ e $(p, a) = 1$, então $p \mid b$) que $p \mid b$. □

Exercício 10.7. Mostre que, se $p \mid a_1 \cdots a_n$, então $p \mid a_i$ para algum $i \in \{1, \ldots, n\}$.

Teorema 10.8 (Teorema Fundamental da Aritmética)**.** *Um número natural $n > 1$ se escreve de maneira* única *como um produto*

$$n = p_1 \cdots p_m,$$

onde $m \geqslant 1$ e $p_1 \leqslant \cdots \leqslant p_m$ são primos.

Exemplo 10.9. $15 = 3 \cdot 5, \quad 12 = 2 \cdot 2 \cdot 3, \quad 49 = 7 \cdot 7.$

Observação 10.10. Se não impusermos a ordem $p_1 \leqslant \cdots \leqslant p_m$, a representação como produto de primos é única a menos de permutação dos primos. Por exemplo,

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2.$$

Agrupando os primos iguais, podemos também escrever, de maneira única,

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

com $k \geqslant 1$, $p_1 < \cdots < p_k$ primos e $e_i > 0$. Às vezes é mais conveniente escrever n como um produto sobre *todos* os números primos:

$$n = \prod_{p \text{ primo}} p^{e_p} = 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdots,$$

com a condição de que $e_p \neq 0$ apenas para um número finito de primos p ($e_p = 0$ se p *não* aparece na fatoração de n).

Demonstração do TFA. Existência. Indução (forte) em n. Se n é primo, não há nada a provar ($m = 1$, $p_1 = n$). Se não, podemos escrever $n = ab$, com $1 < a < n$ e $1 < b < n$. Por hipótese de indução, a e b são produtos de primos. Juntando as fatorações e reordenando os fatores, se necessário, obtemos uma fatoração de n como no enunciado.

Unicidade. Suponha que

$$n = p_1 \cdots p_m = p'_1 \cdots p'_{m'},$$

com $m, m' \geqslant 1$ e $p_1 \leqslant \cdots \leqslant p_m$, $p'_1 \leqslant \cdots \leqslant p'_{m'}$ primos. Como $p_1 \mid p'_1 \cdots p'_{m'}$, segue do Exercício 10.7 que $p_1 \mid p'_i$ para algum $i \in \{1, \ldots, m'\}$. Como p'_i é primo, devemos ter $p_1 = p'_i$ e, portanto, $p_1 \geqslant p'_1$. Analogamente, $p'_1 \mid p_1 \cdots p_m$ e concluímos que $p'_1 \geqslant p_1$. Assim, $p_1 = p'_1$. Logo,

$$n = p_1 \cdots p_m = p'_1 \cdots p'_{m'} \iff \frac{n}{p_1} = p_2 \cdots p_m = p'_2 \cdots p'_{m'}.$$

Repetindo este procedimento, mostramos por indução que $m = m'$ e $p_i = p'_i$ para todo i. □

Revisitando algumas definições anteriores em vista do TFA.

- *Divisibilidade.* Se $a = \prod_p p^{e_p}$ e $b = \prod_p p^{f_p}$, então

$$b \mid a \iff f_p \leqslant e_p \text{ para todo primo } p.$$

(Em particular, se $e_p = 0$, então $f_p = 0$.)

Exemplo 10.11. Temos $18 \mid 1728$, pois

$$1728 = 12^3 = (2^2 \cdot 3)^3 = 2^6 \cdot 3^3, \qquad 18 = 2 \cdot 9 = 2^1 \cdot 3^2,$$

logo

$$1728 = 2^6 \cdot 3^3 = (2^5 \cdot 3^1) \cdot (2^1 \cdot 3^2) = 96 \cdot 18.$$

- *MDC e MMC.* Se $a = \prod_p p^{e_p}$ e $b = \prod_p p^{f_p}$, então

$$(a,b) = \prod_p p^{\min\{e_p,f_p\}}, \qquad [a,b] = \prod_p p^{\max\{e_p,f_p\}}.$$

Note que a fórmula $(a,b)[a,b] = ab$ é equivalente a

$$\Big(\prod_p p^{\min\{e_p,f_p\}}\Big)\Big(\prod_p p^{\max\{e_p,f_p\}}\Big) = \prod_p p^{\min\{e_p,f_p\}+\max\{e_p,f_p\}} = \prod_p p^{e_p+f_p}$$
$$= \Big(\prod_p p^{e_p}\Big)\Big(\prod_p p^{f_p}\Big).$$

Exemplo 10.12. Quanto vale $(1000, 1024)$? Temos

$$1000 = 10^3 = (2\cdot 5)^3 = 2^3 \cdot 5^3, \qquad 1024 = 2^{10},$$

logo $(1000, 1024) = 2^3 = 8$.

- *Coprimos.* Pela fórmula acima, a e b são coprimos se, e somente se, $\min\{e_p, f_p\} = 0$ para todo primo p. Isto é, nenhum primo p pode aparecer ao mesmo tempo na fatoração de a e de b. Ou ainda, a e b são coprimos se, para todo primo p tal que $p \mid a$, temos $p \nmid b$ (e vice-versa).

Exemplo 10.13. Os números 1000 e 81 são coprimos, pois

$$1000 = 10^3 = \underbrace{2^3 \cdot 5^3}_{\text{primos 2 e 5}} \qquad \text{e} \qquad 81 = \underbrace{3^4}_{\text{primo 3}}.$$

Exercício 10.14.

1) Seja $a = \prod_p p^{e_p}$. Mostre que a é uma potência n-ésima (isto é, $a = c^n$ para algum c) se, e somente se, $n \mid e_p$ para todo primo p.

2) Mostre que, se a e b são coprimos e ab é uma potência n-ésima, então a e b são potências n-ésimas.

3) Revisite a demonstração da parametrização das ternas pitagóricas da Aula 1.

Aula 11 (16/09)

5) Primos (cont.)

Como decidir se um número é primo? Isto é o que se chama um *teste de primalidade*.

Crivo de Eratóstenes. Listamos todos os naturais até N. Marcamos o primo 2 e excluímos todos os seus múltiplos. Marcamos o primo 3 e excluímos todos os seus múltiplos. E assim por diante. Por exemplo, para $N = 40$:

	(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~~

Teste até $\sqrt{n}$. Na prática, usamos o teste seguinte.

Proposição 11.1. *Se $n \geqslant 2$ é composto, então n admite um divisor primo $p \leqslant \sqrt{n}$ (isto é, $p^2 \leqslant n$).*

Demonstração. Seja p o menor divisor primo de n e escreva $n = pm$. Como n é composto, $m \neq 1$. Seja q um primo que divide m e escreva $m = qr$. Por hipótese, $p \leqslant q$. Logo,

$$n = pm = pqr \geqslant p^2 r \geqslant p^2.$$ □

Exemplo 11.2. O número 101 é primo: basta testar os primos até $\sqrt{101} \approx 10$, e de fato

$$2 \nmid 101, \quad 3 \nmid 101, \quad 5 \nmid 101, \quad 7 \nmid 101.$$

(Falaremos de critérios de divisibilidade depois de congruências.)

Podemos usar o teste de primalidade para fatorar um número.

Exemplo 11.3. Fatoremos 143. Seu menor fator primo é $\leqslant \sqrt{143} \approx 12$. Temos

$$2 \nmid 143, \quad 3 \nmid 143, \quad 5 \nmid 143, \quad 7 \nmid 143,$$

mas $11 \mid 143$: dividindo, $143 = 11 \cdot 13$, e 13 é primo. Logo, $143 = 11 \cdot 13$.

Saber a fatoração em primos é útil para resolver problemas em geral.

Exemplo 11.4. Encontre todos os inteiros $m, n \geqslant 1$ tais que

$$\frac{1}{m} + \frac{1}{n} = \frac{1}{143}.$$

Temos

$$\begin{aligned}
\frac{1}{m} + \frac{1}{n} = \frac{1}{143} &\iff 143(m+n) = mn \\
&\iff mn - 143m - 143n = 0 \\
&\iff (m-143)(n-143) - 143^2 = 0 \\
&\iff (m-143)(n-143) = 143^2 = 11^2 \cdot 13^2.
\end{aligned}$$

Os fatores $m - 143$ e $n - 143$ não podem ser ambos negativos, pois $m - 143$, $n - 143 \geqslant -142$ e $142^2 < 143^2$. Assim, ambos são positivos. Podemos supor $m \leqslant n$. Pela unicidade da fatoração em primos (TFA), temos as possibilidades:

$m-143$	$n-143$	m	n
1	$11^2 \cdot 13^2$	144	20592
11	$11 \cdot 13^2$	154	2002
13	$11^2 \cdot 13$	156	1716
11^2	13^2	264	312
$11 \cdot 13$	$11 \cdot 13$	286	286

Exercício 11.5.

1) Encontre todos os primos p tais que $11p + 1$ é um quadrado.

2) Seja $n \geqslant 1$. Mostre que a equação diofantina $x^2 - y^2 = n$ tem solução inteira $x, y \geqslant 0$ se, e somente se, n é ímpar ou divisível por 4. Quando a solução é única?

Exemplo 11.6. Com quantos zeros termina 100!? Temos

$$100! = 100 \cdot 99 \cdot 98 \cdots 3 \cdot 2 \cdot 1.$$

Queremos a maior potência de 10 que divide 100!. Como $10 = 5 \cdot 2$, basta encontrar as maiores potências de 5 e 2 que dividem 100!:

$$100! = 2^{e_2} \cdot 5^{e_5} \cdot r, \qquad 2, 5 \nmid r.$$

Note que há muito mais fatores de 2 do que de 5 (por exemplo, em $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdots$). Logo, $e_5 \leqslant e_2$ e basta calcular e_5:

$$100! = 10^{e_5}\big(2^{e_2 - e_5} r\big), \qquad 10 \nmid 2^{e_2 - e_5} r.$$

Na expressão de 100!, basta considerar os múltiplos de 5:

$$\{5, 10, 15, \ldots, 100\} = \{5k : 1 \leqslant k \leqslant 20\}.$$

Temos pelo menos $20 = \frac{100}{5}$ fatores de 5. Os múltiplos de $5^2 = 25$ contribuem com pelo menos dois fatores:

$$\{25, 50, 75, 100\} = \{25k : 1 \leqslant k \leqslant 4\}.$$

Temos mais $4 = \frac{100}{25}$ fatores de 5. Como não há múltiplos de $5^3 = 125$ menores que 100, obtemos o total de

$$\frac{100}{5} + \frac{100}{25} = 20 + 4 = 24 = e_5$$

fatores de 5. Logo, 100! termina com 24 zeros.

Proposição 11.7. *Seja p um primo. A maior potência de p que divide $n!$ é p^{e_p}, onde*

$$e_p = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Notação: $\lfloor x \rfloor$ = maior inteiro $\leqslant x$ ("parte inteira").

Demonstração. Igual ao argumento acima. □

Exercício 11.8.

1) Calcule a fatoração em primos de 25!.

2) Determine as maiores potências de 9 e de 14 que dividem 1000!.

Aula 12 (18/09)

5) Primos (cont.)

Teorema 12.1. *Existem infinitos primos.*

Demonstração. Suponha, por absurdo, que exista apenas um número finito de primos:

$$p_1, p_2, \ldots, p_N.$$

Seja $a = p_1 p_2 \cdots p_N + 1$. Como a é um número natural > 1, pelo TFA existe um primo p tal que $p \mid a$. Mas $p \neq p_i$ para todo i (a deixa resto 1 na divisão por p_i), o que é absurdo! □

Existe alguma fórmula simples para gerar números primos?

Exemplo 12.2. Seja $P(n) = n^2 + n + 41$. Temos

n	0	1	2	3	$\cdots$	39
$P(n)$	41	43	47	53	$\cdots$	1601

e $P(n)$ é primo para todo $n \leqslant 39$, mas

$$P(40) = 40^2 + 40 + 41 = 40(40+1) + 41 = 40 \cdot 41 + 41 = 41(40+1) = 41^2$$

não é primo!

Exercício 12.3. Mostre que não existe um polinômio não-constante com coeficientes inteiros $f(n)$ tal que $f(n)$ é primo para todo $n \in \mathbb{N}$. [Dica: se $p = f(0)$, considere $f(p)$.]

Podemos pelo menos entender como os primos se distribuem em $\mathbb{N}$? Alguma regularidade?

Exemplo 12.4. Existem sequências arbitrariamente longas de naturais consecutivos sem nenhum número primo! Dado $n \geqslant 2$, basta considerar

$$n! + 2,\ n! + 3,\ \ldots,\ n! + n :$$

todos estes números são compostos (pois $k \mid n! + k$ para $2 \leqslant k \leqslant n$).

Exemplo 12.5. Existem primos p tais que $p + 2$ também é primo ("primos gêmeos"), como

$$3 \text{ e } 5, \qquad 11 \text{ e } 13, \qquad 101 \text{ e } 103.$$

Nós *não* sabemos se existem infinitos primos gêmeos, mas sabemos (Zhang, 2013) que existe um $N \approx 70 \cdot 10^6$ tal que existem infinitos pares de primos p, q com $|p - q| \leqslant N$.

Outra abordagem: defina

$$\pi(x) = \text{número de primos} \leqslant x.$$

Exemplo 12.6. Quanto vale $\pi(10)$? Entre $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$, os primos são $2, 3, 5, 7$: há 4 primos $\leqslant 10$, logo $\pi(10) = 4$.

A função $\pi\colon [0, \infty) \to \mathbb{R}$ é crescente. A infinitude dos primos é equivalente a

$$\lim_{x \to +\infty} \pi(x) = +\infty.$$

Gráfico para $0 \leqslant x \leqslant 10$:

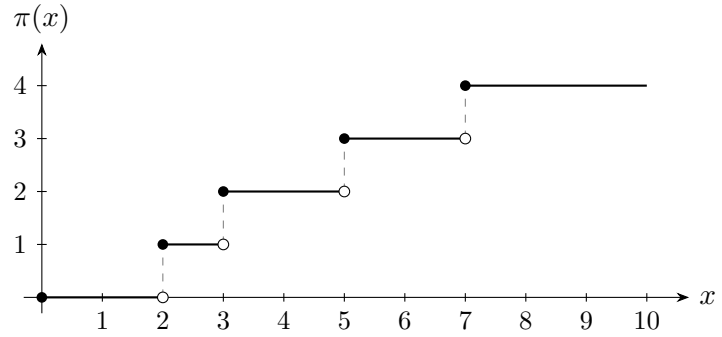
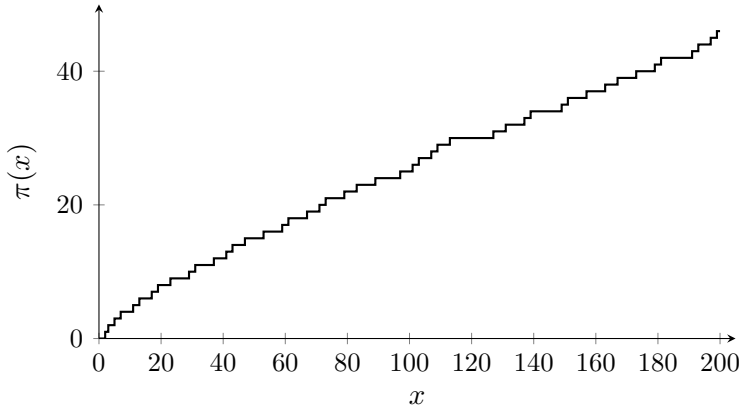


Gráfico para $0 \leqslant x \leqslant N$ grande (aqui $N = 200$):



Quanto maior N, mais "suave" e regular parece o gráfico.

Teorema 12.7 (Teorema dos números primos)**.**

$$\pi(x) \sim \frac{x}{\ln x}.$$

Notação: $f(x) \sim g(x)$ se $\lim_{x \to \infty} f(x)/g(x) = 1$.

Exemplo 12.8. Quantos primos $\leqslant 1000$ existem? Estimativa:

$$\frac{1000}{\ln(1000)} \approx 144{,}76\ldots$$

(De fato, $\pi(1000) = 168$.)

Exercício 12.9. Estime quantos passos são necessários para testar a primalidade de um número com 20 dígitos (usando o algoritmo da aula passada).

6) Racionais e irracionais

Formalmente, o conjunto dos racionais $\mathbb{Q}$ é construído a partir da seguinte relação de equivalência em $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$:

$$(a, b) \sim (c, d) \iff ad = bc, \qquad (*)$$

isto é,

$$\mathbb{Q} = \big(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\big)/\!\sim.$$

A classe de (a, b) em $\mathbb{Q}$ é denotada $\frac{a}{b}$. Note que $(*)$ é equivalente a

$$\frac{a}{b} = \frac{c}{d} \iff ad = cb. \qquad (**)$$

Lema 12.10. *Um número racional admite uma única representação da forma $\frac{a}{b}$ com $b > 0$ e $(a, b) = 1$, dita* fração irredutível.

Demonstração. Seja $r = \frac{m}{n}$ um número racional. Podemos supor $n > 0$ (caso contrário, multiplicamos m e n por -1). Seja $d = (m, n)$ e escreva $m = da$, $n = db$. Por $(**)$, temos

$$\frac{m}{n} = \frac{da}{db} = \frac{a}{b},$$

com $b > 0$ e $(a, b) = 1$. Se

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b, \qquad (***)$$

com $b' > 0$ e $(a', b') = 1$, é uma outra representação como no enunciado, então

$$(a, b) = 1 \overset{(***)}{\Longrightarrow} b \mid b', \qquad (a', b') = 1 \overset{(***)}{\Longrightarrow} b' \mid b.$$

Como ambos são > 0, $b' = b$. Logo, $a' = a$. □

Exercício 12.11. Verifique que a soma e a multiplicação

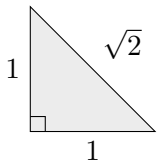
$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}, \qquad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

estão bem definidas e que $\mathbb{Q}$ forma um corpo.

Observação 12.12. Os inteiros $\mathbb{Z} \subset \mathbb{Q}$ são as frações irredutíveis da forma $\frac{n}{1}$.

Definição 12.13. Um *número irracional* é um número real (ou complexo) que não é racional.

Exemplo 12.14. $\sqrt{2}$ é um número irracional (um "irracional quadrático").



Por absurdo, se $\sqrt{2}$ é racional, escreva $\sqrt{2} = \frac{a}{b}$ (fração irredutível). Então

$$\sqrt{2}\, b = a \iff 2b^2 = a^2.$$

Pelo TFA, escreva $a = \prod_p p^{e_p}$, $b = \prod_p p^{f_p}$. Assim,

$$2 \cdot \left(2^{f_2} \cdot 3^{f_3} \cdots\right)^2 = \left(2^{e_2} \cdot 3^{e_3} \cdots\right)^2 \iff 2^{2f_2+1} \cdot 3^{2f_3} \cdots = 2^{2e_2} \cdot 3^{2e_3} \cdots$$

Pela unicidade no TFA, devemos ter

$$2f_2 + 1 = 2e_2,$$

o que é absurdo!

Exemplo 12.15. π é irracional (difícil!).

Exercício 12.16. Seja $n \in \mathbb{N}$. Mostre que $\sqrt{n}$ é racional se, e somente se, n é um quadrado.

Bônus. A sequência de Fibonacci admite a seguinte fórmula fechada envolvendo irracionais quadráticos: se

$$\varphi = \frac{1+\sqrt{5}}{2} \qquad \text{e} \qquad \psi = \frac{1-\sqrt{5}}{2},$$

então

$$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi} = \frac{\varphi^n - \psi^n}{\sqrt{5}}.$$

A demonstração usa "séries formais" (isto é, sem noção de convergência). Considere a série geradora

$$f(x) = F_0 + F_1 x + F_2 x^2 + \cdots = \sum_{n=0}^{\infty} F_n x^n,$$

onde $F_0 = 0$, $F_1 = 1$, $F_2 = 1$. Temos:

$$\begin{aligned} xf(x) &= F_0x + F_1x^2 + F_2x^3 + \cdots \\ x^2f(x) &= \qquad F_0x^2 + F_1x^3 + \cdots \end{aligned}$$

Somando as duas (e usando $F_0 = 0$):

$$\begin{aligned} xf(x) + x^2f(x) &= (F_1 + F_0)x^2 + (F_2 + F_1)x^3 + \cdots \\ &= F_2x^2 + F_3x^3 + \cdots \\ &= f(x) - x, \end{aligned}$$

ou seja,

$$(1 - x - x^2)f(x) = x,$$

e portanto, usando $1 - x - x^2 = (1 - \varphi x)(1 - \psi x)$ e frações parciais,

$$\begin{aligned} f(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \varphi x)(1 - \psi x)} &= \frac{1}{\varphi - \psi}\Big(\frac{1}{1 - \varphi x} - \frac{1}{1 - \psi x}\Big) \\ = \frac{1}{\varphi - \psi}\Big(\sum_{n=0}^{\infty} \varphi^n x^n - \sum_{n=0}^{\infty} \psi^n x^n\Big) &= \sum_{n=0}^{\infty} \underbrace{\Big(\frac{\varphi^n - \psi^n}{\varphi - \psi}\Big)}_{F_n} x^n. \end{aligned}$$

Exercício 12.17. Encontre uma fórmula fechada para a sequência de Lucas: $L_0 = 2$, $L_1 = 1$, $L_{n+2} = L_{n+1} + L_n$.

Aula 13 (30/09)

7) Congruências

As congruências formalizam o que se costuma chamar de "aritmética modular".

Sejam $a, b \in \mathbb{Z}$ e $m \geqslant 1$ inteiros.

Definição 13.1. Dizemos que a é *congruente* a b *módulo* m se a e b deixam o mesmo resto na divisão por m. Notação:

$$a \equiv b \pmod{m}.$$

Exercício 13.2. Verifique que a e b deixam o mesmo resto na divisão por m se, e somente se, $m \mid a - b$.

Ou seja,

$$\boxed{a \equiv b \pmod{m} \iff m \mid a - b.}$$

Exemplo 13.3. $37 \equiv 12 \pmod{5}$ e $6 \equiv -1 \pmod{7}$.

Lema 13.4. *A congruência módulo m é uma relação de equivalência.*

Demonstração.

- *Reflexiva:* $a \equiv a \pmod{m}$, pois $m \mid a - a = 0$.
- *Simétrica:* $a \equiv b \pmod{m} \iff m \mid a - b \iff m \mid b - a \iff b \equiv a \pmod{m}$.
- *Transitiva:* se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m \mid a - b$ e $m \mid b - c$, logo $m \mid (a-b)+(b-c) = a-c$, ou seja, $a \equiv c \pmod{m}$. □

Teorema 13.5 (Propriedades elementares da congruência)**.** *1) (Soma e diferença) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então*

$$a + c \equiv b + d \pmod{m} \qquad e \qquad a - c \equiv b - d \pmod{m}.$$

Em particular, se $a \equiv b \pmod{m}$ e $k \in \mathbb{Z}$, então $ka \equiv kb \pmod{m}$.

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

Em particular, se $a \equiv b \pmod{m}$ e $k \in \mathbb{N}$, então $a^k \equiv b^k \pmod{m}$.

3) (Inverso módulo m) Se $(k, m) = 1$, então existe $k' \in \mathbb{Z}$ tal que $k \cdot k' \equiv 1 \pmod{m}$.

4) (Cancelamento) Se $ka \equiv kb \pmod{m}$ e $(k, m) = 1$, então $a \equiv b \pmod{m}$.

Exemplo 13.6. Qual é o resto de 2^{32} na divisão por 17? (Isto é, calcule 2^{32} módulo 17.)

Não precisamos calcular 2^{32}! Temos $2^2 = 4$, $2^3 = 8$, $2^4 = 16$ e

$$2^5 = 32 \equiv 15 \pmod{17}$$

(aqui "passamos" de 17). Então

$$\begin{aligned}
&2^{10} = (2^5)^2 \equiv 15^2 = 225 \equiv 4 \pmod{17} && (225 = 13 \cdot 17 + 4),\\
&2^{30} = (2^{10})^3 \equiv 4^3 = 64 \equiv 13 \pmod{17},\\
&2^{32} = 2^{30} \cdot 2^2 \equiv 13 \cdot 4 = 52 \equiv 1 \pmod{17}.
\end{aligned}$$

Solução alternativa (mais inteligente): como $2^4 = 16 \equiv -1 \pmod{17}$,

$$2^{32} = (2^4)^8 \equiv (-1)^8 = 1 \pmod{17}.$$

Exercício 13.7. 1) Calcule 2^{36} módulo 11.

2) Mostre que $2^{70} + 3^{70}$ é um múltiplo de 13.

Demonstração do Teorema 13.5. 1) Se $m \mid a - b$ e $m \mid c - d$, então

$$m \mid (a - b) + (c - d) = (a + c) - (b + d)$$

e

$$m \mid (a - b) - (c - d) = (a - c) - (b - d).$$

2) Se $m \mid a - b$ e $m \mid c - d$, então $m \mid (a - b)(c - d) = ac - ad - bc + bd$. Como

$$\begin{aligned}
ac - ad - bc + bd &= ac + bd - ad - bc\\
&= ac - bd - ad - bc + bd + bd\\
&= ac - bd - \underbrace{(a - b) \cdot d}_{\text{múltiplo de } m} - \underbrace{b \cdot (c - d)}_{\text{múltiplo de } m},
\end{aligned}$$

concluímos que $m \mid ac - bd$.

3) Se $(k, m) = 1$, segue do teorema de Bézout que existem $k', m' \in \mathbb{Z}$ tais que $k \cdot k' + m \cdot m' = 1$. Logo, $k \cdot k' \equiv 1 \pmod{m}$.

4) Se $ka \equiv kb \pmod{m}$ e $(k, m) = 1$, tome k' como no item 3). Então

$$\underbrace{k' \cdot k}_{\equiv 1} \cdot a \equiv \underbrace{k' \cdot k}_{\equiv 1} \cdot b \pmod{m} \implies a \equiv b \pmod{m}. \qquad \square$$

Exercício 13.8. Mostre que, se $(m, n) = 1$, então

$$\begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases} \iff a \equiv b \pmod{mn}.$$

Exemplo 13.9. "O produto de 3 inteiros consecutivos é divisível por 6."

Basta mostrar que $6 \mid n^3 - n = (n-1) \cdot n \cdot (n+1)$, isto é, $n^3 \equiv n \pmod 6$, para qualquer n. Pelo exercício acima, basta mostrar que $n^3 \equiv n \pmod 2$ e $n^3 \equiv n \pmod 3$.

- Módulo 2, temos duas possibilidades: $n \equiv 0 \pmod 2$ ou $n \equiv 1 \pmod 2$. E de fato

$$0^3 \equiv 0 \pmod 2, \qquad 1^3 \equiv 1 \pmod 2. \checkmark$$

- Módulo 3, temos três possibilidades: $n \equiv 0$, $n \equiv 1$ ou $n \equiv 2 \pmod 3$. E

$$0^3 \equiv 0 \pmod 3, \qquad 1^3 \equiv 1 \pmod 3, \qquad 2^3 = 8 \equiv 2 \pmod 3. \checkmark$$

Exercício 13.10. Mostre que o produto de quatro inteiros consecutivos é divisível por 24.

Exercício 13.11. Generalize o exercício acima para o produto de n inteiros consecutivos.

Aula 14 (07/10)

7) Congruências (cont.)

Lembrete. $a \equiv b \pmod{m} \iff m \mid a - b$. Em particular,

$$a \equiv 0 \pmod{m} \iff m \mid a.$$

Hoje: dígitos e critérios de divisibilidade.

Lembremos que a notação decimal (base 10) significa

$$a = (r_k r_{k-1} \cdots r_0)_{10} = r_k 10^k + \cdots + r_0, \qquad 0 \leqslant r_i \leqslant 9.$$

Exemplo 14.1. $2024 = 2 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10 + 4$.

Redução módulo 10^i. Para $i = 1$:

$$\begin{aligned} a &= r_k 10^k + \cdots + r_1 10 + r_0 \\ &= (r_k 10^{k-1} + \cdots + r_1) \cdot 10 + r_0 \\ &\equiv r_0 \pmod{10}. \end{aligned}$$

Para $i = 2$:

$$\begin{aligned} a &= r_k 10^k + \cdots + r_2 10^2 + r_1 10 + r_0 \\ &= (r_k 10^{k-2} + \cdots + r_2) \cdot 100 + r_1 \cdot 10 + r_0 \\ &\equiv r_1 \cdot 10 + r_0 \pmod{100}. \end{aligned}$$

E assim por diante: os últimos n dígitos de a se calculam reduzindo a módulo 10^n.

Exemplo 14.2. Quais são os últimos dois dígitos de 3^{200}? Devemos reduzir módulo 100:

$$\begin{aligned} 3^{200} &= (3^2)^{100} = 9^{100} = (10-1)^{100} \\ &= \sum_{i=0}^{100} \binom{100}{i} 10^i (-1)^{100-i} \\ &= \binom{100}{0} - \binom{100}{1} \cdot 10 + \underbrace{\binom{100}{2} \cdot 10^2 - \cdots}_{\text{múltiplos de } 100} \\ &\equiv 1 - 100 \cdot 10 \\ &\equiv 1 \pmod{100}. \end{aligned}$$

Logo, os últimos dois dígitos são 01.

Exercício 14.3. Calcule os últimos 3 dígitos de 3^{2024}.

Exemplo 14.4 ("Prova dos 9")**.** É um método antigo para verificação de contas. Por exemplo, a soma

$$\text{“}9787 + 4526 = 15313\text{”}$$

está errada, pois

- $9 + 7 + 8 + 7 = 31 \to 3 + 1 = 4$;
- $4 + 5 + 2 + 6 = 17 \to 1 + 7 = 8$;
- $1 + 5 + 3 + 1 + 3 = 13 \to 1 + 3 = 4$;

mas

$$4 + 8 = 12 \to 1 + 2 = 3 \neq 4.$$

(De fato, $9787 + 4526 = 14313$.)

Explicação: a operação de soma sucessiva dos dígitos até obter um número com 1 dígito corresponde à redução módulo 9! Por exemplo, como $10 \equiv 1 \pmod 9$,

$$\begin{aligned} 9787 &= 9 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 7 \\ &\equiv 9 \cdot 1^3 + 7 \cdot 1^2 + 8 \cdot 1 + 7 \\ &\equiv 31 = 3 \cdot 10 + 1 \\ &\equiv 3 \cdot 1 + 1 \equiv 4 \pmod 9. \end{aligned}$$

A "prova dos 9" para a soma e o produto corresponde às implicações

$$\begin{aligned} a + b = c &\implies a + b \equiv c \pmod 9, \\ a \cdot b = c &\implies a \cdot b \equiv c \pmod 9. \end{aligned}$$

Exercício 14.5. Construa exemplos para mostrar que a volta da prova dos 9 não vale.

Divisibilidade por 3 ou 9.

$$3 \text{ (ou 9) divide } a \iff 3 \text{ (ou 9) divide a soma dos dígitos de } a,$$

pois, se $a = 10^k r_k + \cdots + 10 r_1 + r_0$, então, como $10 \equiv 1$ módulo 3 e módulo 9,

$$a \equiv r_k + \cdots + r_1 + r_0 \pmod{3 \text{ ou } 9}.$$

Exercício 14.6. Caracterize os inteiros da forma $12121\cdots21$ que são divisíveis por 9.

Divisibilidade por 2, 5 ou 10.

$$2,\ 5 \text{ ou } 10 \text{ divide } a \iff 2,\ 5 \text{ ou } 10 \text{ divide o último dígito de } a,$$

pois, se $a = 10^k r_k + \cdots + 10r_1 + r_0$, então

$$a \equiv r_0 \pmod{2,\ 5 \text{ ou } 10}.$$

Exercício 14.7. Mostre que a é divisível por 4, 20, 25, 50 ou 100 se, e somente se, o número formado pelos seus dois últimos dígitos o é.

Divisibilidade por 7.

$$7 \text{ divide } a = (r_k \cdots r_0)_{10} \iff 7 \text{ divide } (r_k \cdots r_1)_{10} - 2r_0.$$

Exemplo 14.8. $a = 59325$:

$$\begin{aligned} 59325 &\to 5932 - 10 = 5922 \\ &\to 592 - 4 = 588 \\ &\to 58 - 16 = 42, \quad \text{divisível por 7.} \end{aligned}$$

(De fato, $59325 = 7 \cdot 8475$.)

Explicação:

$$a = 10^k r_k + \cdots + 10r_1 + r_0 = 10 \cdot \underbrace{(10^{k-1} r_k + \cdots + r_1)}_{q} + r_0 = 10q + r_0.$$

Então

$$\begin{aligned} a \equiv 0 \pmod 7 &\iff 10q + r_0 \equiv 0 \pmod 7 \\ &\iff \underbrace{-20}_{\equiv 1} q - 2r_0 \equiv 0 \pmod 7 \\ &\iff q - 2r_0 \equiv 0 \pmod 7. \end{aligned}$$

(Usamos que $-2 \equiv 5$ é um inverso de $10 \equiv 3$ módulo 7, e o cancelamento.)

Divisibilidade por 11.

$$11 \text{ divide } a = (r_k \cdots r_0)_{10} \iff 11 \text{ divide } (-1)^k r_k + \cdots + r_0.$$

Exemplo 14.9. Para $a = 6281$: $-6 + 2 - 8 + 1 = -14 + 3 = -11$, que é divisível por 11. Logo, $11 \mid 6281$ (de fato, $6281 = 11 \cdot 571$).

Exercício 14.10. Demonstre o critério de divisibilidade por 11.

Aula 15 (09/10)

8) O anel de inteiros módulo m

Vimos que a relação

$$a \sim b \iff a \equiv b \pmod{m}$$

é uma *relação de equivalência* em $\mathbb{Z}$.

Exemplo 15.1. Qual é a classe de equivalência de 1 módulo 7?

$$\begin{aligned}\overline{1} &= \{a \in \mathbb{Z} : a \equiv 1 \pmod{7}\} \\ &= \text{conjunto dos inteiros que deixam resto 1 na divisão por 7} \\ &= \{7k+1 : k \in \mathbb{Z}\} \\ &= \{\ldots, -13, -6, 1, 8, 15, \ldots\}.\end{aligned}$$

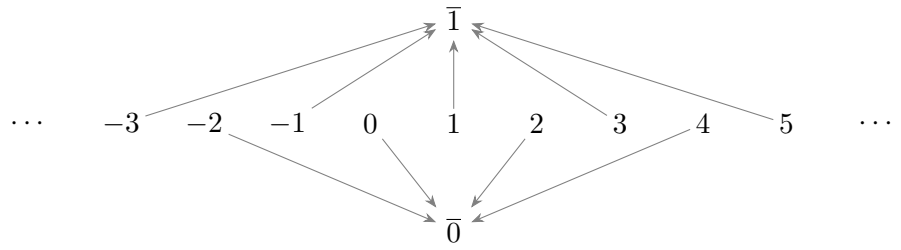
Definição 15.2. O conjunto dos *inteiros módulo m* é o quociente $\mathbb{Z}/\sim$, onde $\sim$ é a relação de congruência módulo m. Notações: $\mathbb{Z}/m\mathbb{Z}$ (é a que usaremos), $\mathbb{Z}/(m)$, $\mathbb{Z}_m$ (evite!).

Ou seja, $\mathbb{Z}/m\mathbb{Z}$ é o conjunto das classes de equivalência da relação $a \equiv b \pmod{m}$.

Exemplo 15.3. $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ ("conjunto par ou ímpar"), onde

$$\begin{aligned}\overline{0} &= \{2k : k \in \mathbb{Z}\} = \{\ldots, -2, 0, 2, 4, \ldots\}, \\ \overline{1} &= \{2k+1 : k \in \mathbb{Z}\} = \{\ldots, -3, -1, 1, 3, \ldots\}.\end{aligned}$$

Note que $\overline{0}$ e $\overline{1}$ formam uma partição de $\mathbb{Z}$: $\overline{0} \cup \overline{1} = \mathbb{Z}$, $\overline{0} \cap \overline{1} = \emptyset$.



Em geral,

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$$

é um conjunto com m elementos, onde

$$\overline{i} = \{a \in \mathbb{Z} : a \equiv i \pmod{m}\} = \{mk + i : k \in \mathbb{Z}\} = i + m\mathbb{Z}.$$

Definição 15.4. Um conjunto de representantes $\{a_1, \ldots, a_m\}$ de $\mathbb{Z}/m\mathbb{Z}$ é dito um *sistema completo de resíduos* ("restos") *módulo* m. Isto é:

(i) $a_i \not\equiv a_j \pmod{m}$ se $i \neq j$;

(ii) dado $a \in \mathbb{Z}$, existe i tal que $a \equiv a_i \pmod{m}$.

Exemplo 15.5. $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \{\overline{-4}, \overline{9}, \overline{2}, \overline{15}\}$. Assim, $\{0, 1, 2, 3\}$ e $\{-4, 9, 2, 15\}$ são sistemas completos de resíduos módulo 4.

Exercício 15.6. Mostre que, se m é ímpar, então

$$\left\{-\frac{m-1}{2}, \ldots, -1, 0, 1, 2, \ldots, \frac{m-1}{2}\right\}$$

é um sistema completo de resíduos módulo m. (Exemplo: $\mathbb{Z}/5\mathbb{Z} = \{\overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}\}$.)

Como a relação de congruência é compatível com a soma e a multiplicação, o conjunto $\mathbb{Z}/m\mathbb{Z}$ tem a estrutura de um *anel*:

$$\begin{aligned} \text{soma:} \quad & \overline{a} + \overline{b} = \overline{a+b}, \\ \text{subtração:} \quad & \overline{a} - \overline{b} = \overline{a-b}, \\ \text{produto:} \quad & \overline{a} \cdot \overline{b} = \overline{a \cdot b}. \end{aligned}$$

Exemplo 15.7. Em $\mathbb{Z}/3\mathbb{Z}$, $\overline{2} + \overline{2} = \overline{2+2} = \overline{4} = \overline{1}$. (Isto é o mesmo que dizer que $2 + 2 \equiv 1 \pmod{3}$.)

Exemplo 15.8. Tabelas de soma e produto em $\mathbb{Z}/3\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Exercício 15.9. Descreva as tabelas de soma e produto em $\mathbb{Z}/6\mathbb{Z}$.

Em um anel qualquer A, as *unidades* são os elementos que possuem inverso multiplicativo. Notação: $A^\times$.

Exemplo 15.10. $\mathbb{Z}^\times = \{-1, +1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

Temos

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{\overline{a} : (a, m) = 1\},$$

pois existe $\overline{b}$ tal que $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{1} \iff ab \equiv 1 \pmod{m}$ (a admite um inverso módulo m) $\iff (a, m) = 1$ (como vimos na Aula 13).

Exemplo 15.11.

m	$(\mathbb{Z}/m\mathbb{Z})^\times$
2	$\{\overline{1}\}$
3	$\{\overline{1},\overline{2}\} = \{\overline{-1},\overline{1}\}$
4	$\{\overline{1},\overline{3}\} = \{\overline{-1},\overline{1}\}$
5	$\{\overline{1},\overline{2},\overline{3},\overline{4}\} = \{\overline{-2},\overline{-1},\overline{1},\overline{2}\}$
6	$\{\overline{1},\overline{5}\} = \{\overline{-1},\overline{1}\}$

Definição 15.12. Um conjunto de representantes $\{u_1, \ldots, u_k\}$ de $(\mathbb{Z}/m\mathbb{Z})^\times$ é dito um *sistema reduzido de resíduos módulo m*. Isto é,

- $u_i \not\equiv u_j \pmod{m}$ se $i \neq j$;
- dado $u \in \mathbb{Z}$ coprimo com m, existe i tal que $u \equiv u_i \pmod{m}$.

Exercício 15.13. Mostre que, se S é um sistema completo de resíduos módulo m, então o subconjunto

$$R = \{a \in S : (a, m) = 1\}$$

é um sistema reduzido de resíduos módulo m.

Um *corpo* é um anel em que todo elemento não-nulo é uma unidade. ($\mathbb{Z}$ não é um corpo, mas $\mathbb{Q}$ é.)

Proposição 15.14. *Seja $m \geqslant 2$. São equivalentes:*

(i) $\mathbb{Z}/m\mathbb{Z}$ é um corpo.

(ii) Todo sistema reduzido de resíduos módulo m tem $m-1$ elementos.

(iii) m é primo.

Demonstração. (i)⇒(ii): $\mathbb{Z}/m\mathbb{Z}$ é um corpo $\iff (\mathbb{Z}/m\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})\backslash\{\overline{0}\}$. Como $\mathbb{Z}/m\mathbb{Z}$ tem m elementos, $(\mathbb{Z}/m\mathbb{Z})^\times$ tem $m-1$ elementos.

(ii)⇒(iii): $S = \{0, 1, \ldots, m-1\}$ é um sistema completo de resíduos módulo m. Logo, $R = \{a \in S : (a, m) = 1\}$ é um sistema reduzido de resíduos módulo m. Como $R \subset \{1, \ldots, m-1\}$ e R tem $m-1$ elementos, devemos ter $R = \{1, \ldots, m-1\}$. Logo, todo $a \in \{1, \ldots, m-1\}$ é coprimo com m, isto é, m é primo.

(iii)⇒(i): Se $\overline{a} \neq \overline{0}$ ($\iff m \nmid a$), então $(a, m) = 1$ (pois m é primo). Logo, $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$. □

Exercício 15.15. Encontre um inverso multiplicativo de $\overline{57}$ em $\mathbb{Z}/101\mathbb{Z}$.

Exercício 15.16. Mostre que, se $\{a_1, \ldots, a_m\}$ é um sistema completo de resíduos módulo m e $u \in \mathbb{Z}$ é coprimo com m, então $\{ua_1, \ldots, ua_m\}$ também é um sistema completo de resíduos módulo m.

Aula 16 (14/10)

Aula passada.

- Anel de inteiros módulo m: $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.
- Unidades: $(\mathbb{Z}/m\mathbb{Z})^\times = \{\overline{u} : 0 \leqslant u \leqslant m-1,\ (u,m) = 1\}$.
- $\mathbb{Z}/p\mathbb{Z}$ é um corpo se p é primo.

8) O anel de inteiros módulo m (cont.)

Lema 16.1. *Se p é primo, as únicas soluções de $x^2 = \overline{1}$ em $\mathbb{Z}/p\mathbb{Z}$ são $\overline{1}$ e $-\overline{1}$.*

(Equivalentemente: se $x^2 \equiv 1 \pmod p$, então $x \equiv \pm 1 \pmod p$.)

Demonstração. Temos

$$\begin{aligned} x^2 \equiv 1 \pmod p &\iff x^2 - 1 \equiv 0 \pmod p \\ &\iff (x-1)(x+1) \equiv 0 \pmod p \\ &\iff p \mid (x-1)(x+1) \\ &\iff p \mid x-1 \ \text{ ou } \ p \mid x+1 \\ &\iff x \equiv 1 \pmod p \ \text{ ou } \ x \equiv -1 \pmod p. \end{aligned}$$ □

Consequência: se $\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ e $\overline{x} \neq \pm\overline{1}$, então $\overline{x}^{-1} \neq \overline{x}$. Em palavras: "módulo um primo, as únicas classes que são seus próprios inversos são $\pm\overline{1}$".

Teorema 16.2 (Wilson)**.** *Se p é primo, então*

$$(p-1)! \equiv -1 \pmod p.$$

Demonstração. Para $p = 2$ e $p = 3$, a verificação é direta: $1! \equiv -1 \pmod 2$ e $2! \equiv -1 \pmod 3$. Suponha $p \geqslant 5$. Em $\mathbb{Z}/p\mathbb{Z}$, escreva

$$\overline{(p-1)!} = \underbrace{\overline{p-1}}_{=-\overline{1}} \cdot \overline{p-2} \cdots \overline{3} \cdot \overline{2} \cdot \overline{1} = -\,\overline{p-2} \cdots \overline{3} \cdot \overline{2}.$$

Pelo lema, cada um dos fatores do produto acima tem um inverso que é um *outro* fator do mesmo produto. Agrupando os inversos aos pares, obtemos

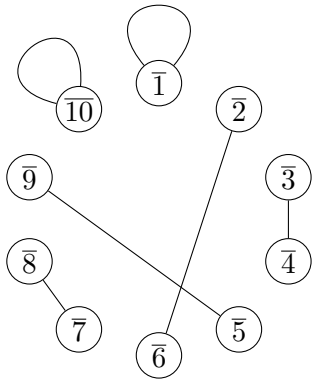
$$\overline{p-2} \cdots \overline{3} \cdot \overline{2} = \overline{1}.$$

Logo, $\overline{(p-1)!} = -\overline{1}$. □

Exemplo 16.3. Em $\mathbb{Z}/7\mathbb{Z}$,

$$\begin{aligned}\overline{6!} &= \overline{6}\cdot\overline{5}\cdot\overline{4}\cdot\overline{3}\cdot\overline{2}\cdot\overline{1} = -\overline{5}\cdot\overline{4}\cdot\overline{3}\cdot\overline{2} = -(\overline{2}\cdot\overline{4})\cdot(\overline{3}\cdot\overline{5}) \\ &= -\overline{8}\cdot\overline{15} = -\overline{1}\cdot\overline{1} = -\overline{1}.\end{aligned}$$

Exemplo 16.4. Em $\mathbb{Z}/11\mathbb{Z}$, os inversos são $\overline{2}^{-1} = \overline{6}$, $\overline{3}^{-1} = \overline{4}$, $\overline{5}^{-1} = \overline{9}$ e $\overline{7}^{-1} = \overline{8}$, enquanto $\overline{1}$ e $\overline{10} = -\overline{1}$ são seus próprios inversos. Na figura, cada classe está ligada ao seu inverso:



Assim, $\overline{10!} = \overline{10}\cdot(\overline{2}\cdot\overline{6})(\overline{3}\cdot\overline{4})(\overline{5}\cdot\overline{9})(\overline{7}\cdot\overline{8})\cdot\overline{1} = -\overline{1}$.

Exercício 16.5. Mostre que vale a volta do teorema de Wilson. Mais precisamente, se $m > 4$ é composto, então $(m-1)! \equiv 0 \pmod{m}$. (Para $m = 4$, temos $3! = 6 \equiv 2 \pmod 4$; em todo caso, $(m-1)! \not\equiv -1 \pmod{m}$ se m é composto.)

Exercício 16.6. Calcule 65! módulo 67.

Observação 16.7. O teorema de Wilson não serve como critério de primalidade prático.

A função φ de Euler. Vimos que $\mathbb{Z}/m\mathbb{Z}$ sempre tem m elementos, mas o número de elementos de $(\mathbb{Z}/m\mathbb{Z})^\times$ pode variar.

Definição 16.8. A *função φ de Euler* é, por definição,

$$\begin{aligned}\varphi(m) &= \text{nº de elementos de } (\mathbb{Z}/m\mathbb{Z})^\times \\ &= \text{nº de inteiros entre 0 e } m \text{ coprimos com } m.\end{aligned}$$

Exemplo 16.9.

m	2	3	4	5	6	7	8	9	10
$\varphi(m)$	1	2	2	4	2	6	4	6	4

Vimos que, se p é primo, $\mathbb{Z}/p\mathbb{Z}$ é um corpo; logo $\varphi(p) = p - 1$.

Proposição 16.10. *Se p é primo e $k \geqslant 1$, então*

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Demonstração. Se $a \in \mathbb{Z}$ com $1 \leqslant a \leqslant p^k$, então

$$(a, p^k) = 1 \iff (a, p) = 1 \iff p \nmid a.$$

Os múltiplos de p entre 1 e p^k são

$$\underbrace{p,\ 2p,\ \ldots,\ p^{k-1} \cdot p}_{p^{k-1} \text{ elementos}}.$$

Logo, $\varphi(p^k) = p^k - p^{k-1}$. □

Exemplo 16.11. $\varphi(125) = \varphi(5^3) = 5^2 \cdot (5-1) = 25 \cdot 4 = 100$.

Teorema 16.12. *Se $(m, n) = 1$, então*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

("φ é uma função aritmética multiplicativa".)

Demonstração. Arranje os inteiros entre 1 e $m \cdot n$ na seguinte forma matricial (m linhas e n colunas):

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n(m-1)+1 & n(m-1)+2 & n(m-1)+3 & \cdots & n(m-1)+n \end{array}$$

O elemento na linha i e coluna j é $n \cdot (i-1) + j$. Pelo lema de Euclides,

$$(n \cdot (i-1) + j,\ n) = (n, j).$$

Logo, se $(j, n) = 1$, todos os elementos da coluna j são coprimos com n; isto é, existem $\varphi(n)$ colunas em que todos os elementos são coprimos com n (e nas demais colunas nenhum elemento é coprimo com n).

Mas, como $(m, n) = 1$, todas as colunas são sistemas completos de resíduos módulo m (veja o exercício da aula passada). Logo, cada coluna contém exatamente $\varphi(m)$ elementos coprimos com m.

Assim, o número total de elementos simultaneamente coprimos com m e com n na matriz (isto é, $\varphi(m \cdot n)$) é $\varphi(n) \cdot \varphi(m)$. □

Exemplo 16.13. Para $m = 3$ e $n = 4$, a matriz da demonstração é mostrada abaixo. As colunas $j = 1$ e $j = 3$ (em cinza) são as $\varphi(4) = 2$ colunas formadas por números coprimos com 4; em cada uma delas, exatamente $\varphi(3) = 2$ números (circulados) são coprimos com 3. Logo, $\varphi(12) = 2 \cdot 2 = 4$: são os números 1, 5, 7 e 11.

$j=1$	$j=2$	$j=3$	$j=4$
①	2	3	4
⑤	6	⑦	8
9	10	⑪	12

Corolário 16.14. *Se $m = p_1^{e_1} \cdots p_k^{e_k}$ é a fatoração em primos de m, então*

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{e_1}) \cdots \varphi(p_k^{e_k}) \\ &= p_1^{e_1-1}(p_1 - 1) \cdots p_k^{e_k-1}(p_k - 1) \\ &= m \cdot \prod_{i=1}^{k} \Big(1 - \frac{1}{p_i}\Big). \qquad \square\end{aligned}$$

Exemplo 16.15.

$$\begin{aligned}\varphi(2024) &= \varphi(2^3 \cdot 11 \cdot 23) = 2^2 \cdot (2-1) \cdot (11-1) \cdot (23-1) \\ &= 4 \cdot 10 \cdot 22 = 880.\end{aligned}$$

Exercício 16.16.

1. Encontre todos os m tais que $\varphi(m) = 6$.
2. Mostre que existem infinitos primos usando φ. Ideia: mostrar que, se $p_1, p_2, \ldots, p_k$ são todos os primos, então $\varphi(p_1 \cdots p_k) = 1$.

Aula 17 (16/10)

9) Teorema chinês dos restos

Problema. Um general chinês possuía 1200 tropas antes da guerra. Após a guerra, ele alinhou as tropas de 5 em 5, e sobraram 3 tropas. Depois, alinhou de 6 em 6, e também sobraram 3. Quando alinhou de 7 em 7, sobrou 1. Finalmente, quando alinhou de 11 em 11, não sobrou nenhuma. Quantas tropas voltaram da guerra?

Queremos encontrar $x \in \mathbb{Z}$ tal que $0 \leqslant x \leqslant 1200$ e

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 6 \\ x \equiv 1 \pmod 7 \\ x \equiv 0 \pmod{11} \end{cases}$$

Por que existe solução?

Exemplo 17.1. Encontre as soluções de

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \end{cases}$$

Temos $x \equiv 2 \pmod 3 \iff x = 2 + 3k$, $k \in \mathbb{Z}$. Agora,

$$2 + 3k \equiv 1 \pmod 5 \iff 3k \equiv -1 \pmod 5 \iff k \equiv -2 \equiv 3 \pmod 5,$$

onde, na última equivalência, usamos que 3 tem inverso módulo 5, isto é, $(3, 5) = 1$. A solução geral do sistema é

$$x = 2 + 3 \cdot (3 + 5\ell) = 11 + \underbrace{15}_{3\cdot 5}\ell, \qquad \ell \in \mathbb{Z}.$$

Observação 17.2. Podemos visualizar o exemplo anterior numa tabela com 3 linhas (os restos módulo 3) e 5 colunas (os restos módulo 5), colocando cada $x \in \{0, 1, \ldots, 14\}$ na casa ($x \bmod 3$, $x \bmod 5$). Ao percorrer $x = 0, 1, 2, \ldots$, andamos uma casa na diagonal (voltando ao início ao sair da tabela), e cada uma das 15 casas recebe exatamente um número. A casa $(2, 1)$, em cinza, recebe $x = 11$.

$x \bmod 3$ \ $x \bmod 5$	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

Teorema 17.3 (Teorema chinês dos restos)**.** *Sejam $m_1, \ldots, m_r$ naturais dois a dois coprimos ($(m_i, m_j) = 1$ para todos $i \neq j$) e $b_1, \ldots, b_r$ inteiros. Então o sistema*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv b_r \pmod{m_r} \end{cases}$$

tem uma única solução módulo $m_1 \cdots m_r$ (em particular, uma única solução x com $0 \leqslant x < m_1 \cdots m_r$).

Demonstração algébrica. Considere a aplicação

$$\begin{array}{rccc} f\colon & \mathbb{Z}/(m_1 \cdots m_r)\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \\ & \overline{a} & \longmapsto & (\overline{a}, \ldots, \overline{a}), \end{array}$$

onde, à esquerda, $\overline{a}$ é a classe de a módulo $m_1 \cdots m_r$ e, na i-ésima coordenada à direita, $\overline{a}$ é a classe de a módulo m_i. Ela está bem definida pois, se $\overline{a} = \overline{a'}$ em $\mathbb{Z}/(m_1 \cdots m_r)\mathbb{Z}$, então $a = a' + k \cdot m_1 \cdots m_r$, onde $k \cdot m_1 \cdots m_r$ é múltiplo de m_i; logo $\overline{a} = \overline{a'}$ em $\mathbb{Z}/m_i\mathbb{Z}$.

Queremos mostrar que f é uma bijeção pois, neste caso, dado $(\overline{b_1}, \ldots, \overline{b_r})$ em $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$, existirá um único $\overline{x}$ em $\mathbb{Z}/m_1 \cdots m_r\mathbb{Z}$ tal que $f(\overline{x}) = (\overline{b_1}, \ldots, \overline{b_r})$, isto é, $x \equiv b_i \pmod{m_i}$ para todo i.

Como $\mathbb{Z}/m_1 \cdots m_r\mathbb{Z}$ e $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ têm o mesmo número de elementos, basta mostrar que f é injetiva. Como f é compatível com a subtração, basta ver que $f(\overline{a}) = 0$ implica $\overline{a} = 0$. Se $f(\overline{a}) = 0$, então $\overline{a} = 0$ em $\mathbb{Z}/m_i\mathbb{Z}$, isto é, $m_i \mid a$, para todo i. Como os m_i são dois a dois coprimos, então $m_1 \cdots m_r \mid a$, isto é, $\overline{a} = 0$ em $\mathbb{Z}/m_1 \cdots m_r\mathbb{Z}$. □

Exercício 17.4. Mostre, usando o TFA, que se $m_1, \ldots, m_r$ são dois a dois coprimos e $m_i \mid a$ para todo i, então $m_1 \cdots m_r \mid a$.

Observação 17.5. A bijeção f é um "isomorfismo de anéis", isto é, é compatível com a soma e o produto. Isto implica que f induz uma bijeção entre as unidades:

$$(\mathbb{Z}/m_1 \cdots m_r\mathbb{Z})^\times \xrightarrow{\text{bij.}} (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})^\times.$$

Em particular, $\varphi(m_1 \cdots m_r) = \varphi(m_1) \cdots \varphi(m_r)$. Esta é outra demonstração da multiplicatividade da função φ de Euler.

Exercício 17.6. Descreva explicitamente a bijeção $(\mathbb{Z}/15\mathbb{Z})^\times \xrightarrow{\text{bij.}} (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$ e verifique que ela é compatível com o produto.

Como encontrar x explicitamente? Sejam $M = m_1 \cdots m_r$ e $M_i = \dfrac{M}{m_i}$. Como $(m_i, M_i) = 1$, existe $u_i \in \mathbb{Z}$ tal que

$$M_i u_i \equiv 1 \pmod{m_i}.$$

Proposição 17.7. *O inteiro*

$$x = b_1 M_1 u_1 + \cdots + b_r M_r u_r$$

é solução do sistema de congruências

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv b_r \pmod{m_r} \end{cases}$$

Demonstração. Como $M_j \equiv 0 \pmod{m_i}$ para todo $j \neq i$, temos

$$x \equiv b_1 M_1 u_1 + \cdots + b_r M_r u_r \equiv b_i \underbrace{M_i u_i}_{\equiv 1} \equiv b_i \pmod{m_i}. \qquad \square$$

Observação 17.8. O x acima não satisfaz necessariamente $0 \leqslant x < M$.

Exemplo 17.9 (Problema do general chinês)**.** Queremos x entre 0 e 1200 tal que

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 3 \pmod{6} \\ x \equiv 1 \pmod{7} \\ x \equiv 0 \pmod{11} \end{cases} \qquad M = 5 \cdot 6 \cdot 7 \cdot 11 = 2310.$$

Encontramos $u_1, \ldots, u_4$:

- $M_1 = \dfrac{M}{m_1} = 6 \cdot 7 \cdot 11 \equiv 1 \cdot 2 \cdot 1 \equiv 2 \pmod{5}$. Podemos tomar $u_1 = 3$.
- $M_2 = \dfrac{M}{m_2} = 5 \cdot 7 \cdot 11 \equiv (-1) \cdot 1 \cdot (-1) \equiv 1 \pmod{6}$. Podemos tomar $u_2 = 1$.
- $M_3 = \dfrac{M}{m_3} = 5 \cdot 6 \cdot 11 \equiv (-2) \cdot (-1) \cdot 4 \equiv 8 \equiv 1 \pmod{7}$. Podemos tomar $u_3 = 1$.
- $M_4 = \dfrac{M}{m_4} = 5 \cdot 6 \cdot 7 \equiv 5 \cdot (-5) \cdot (-4) \equiv 25 \cdot 4 \equiv 3 \cdot 4 \equiv 12 \equiv 1 \pmod{11}$. Podemos tomar $u_4 = 1$.

Assim, uma solução para o sistema é

$$x = 3 \cdot M_1 \cdot 3 + 3 \cdot M_2 \cdot 1 + 1 \cdot M_3 \cdot 1 + 0 \cdot M_4 \cdot 1 = 5643.$$

Este número é maior que 1200. Como

$$x \equiv 5643 - 2 \cdot \underbrace{2310}_{M} \equiv 1023 \pmod{2310},$$

e 1023 é a única solução com $0 \leqslant x < 2310$, concluímos que sobraram 1023 tropas.

Exercício 17.10. Resolva o sistema

$$\begin{cases} x \equiv 7 \pmod 9 \\ x \equiv 9 \pmod{10} \\ x \equiv 3 \pmod 7 \end{cases}$$

Exercício 17.11. Resolva o sistema

$$\begin{cases} 2x \equiv 1 \pmod 5 \\ 3x \equiv 1 \pmod{11} \end{cases}$$

Aula 18 (21/10)

10) Teoremas de Fermat e Euler

O tema deste tópico são as "potências módulo m". Considere as potências de 2 módulo 17:

n	$2^n \bmod 17$	
0	1	
1	2	
2	4	
3	8	
4	16	
5	15	
6	13	
7	9	
8	1	repete a partir daqui, pois $2^8 \equiv 1 \pmod{17}$
9	2	
10	4	
$\vdots$	$\vdots$	

Em geral, se $(a, m) = 1$, então a sequência

$$1 = a^0,\ a^1,\ a^2,\ a^3,\ \ldots \mod m$$

sempre será periódica e 1 sempre será o primeiro número a repetir.

Demonstração. Como $\{0, 1, \ldots, m-1\}$ é finito, existem naturais $r < s$ tais que

$$a^s \equiv a^r \pmod{m} \iff a^{s-r} \equiv 1 \pmod{m},$$

onde a equivalência usa que $(a, m) = 1$. Isto mostra que a sequência repete a partir do n-ésimo termo, onde $n = s - r$.

Seja $n > 0$ o menor possível com a propriedade $a^n \equiv 1 \pmod{m}$. Se $k < \ell$ são naturais $< n$ tais que $a^\ell \equiv a^k \pmod{m}$, então $a^{\ell-k} \equiv 1 \pmod{m}$, com $\ell - k < n$. Logo $\ell - k = 0 \iff \ell = k$, o que é absurdo pois $k < \ell$. □

Observação 18.1. Se $(a, m) \neq 1$, o enunciado acima *não* vale. Exemplo:

n	0	1	2	3	4	5	$\cdots$
$2^n \bmod 6$	1	2	4	2	4	2	$\cdots$

Definição 18.2. Se $(a, m) = 1$, o período da sequência $a^n \bmod m$ é a *ordem* de a módulo m. Notação: $\mathrm{ord}_m(a)$.

Equivalentemente, $\mathrm{ord}_m(a)$ é o menor natural $n > 0$ tal que $a^n \equiv 1 \pmod{m}$.

Exemplo 18.3. $\mathrm{ord}_{17}(2) = 8$. Note que $\mathrm{ord}_m(a) \leqslant m - 1$.

Exemplo 18.4 (módulo 5)**.**

- $\mathrm{ord}_5(1) = 1$.
- $\mathrm{ord}_5(2) = 4$:

$$\begin{aligned} 2^0 &\equiv 1 \pmod 5 & \qquad 2^3 &\equiv 2 \cdot 4 \equiv 3 \pmod 5 \\ 2^1 &\equiv 2 \pmod 5 & \qquad 2^4 &\equiv 2 \cdot 3 \equiv 1 \pmod 5 \\ 2^2 &\equiv 4 \pmod 5 \end{aligned}$$

- $\mathrm{ord}_5(3) = 4$:

$$\begin{aligned} 3^0 &\equiv 1 \pmod 5 & \qquad 3^3 &\equiv 3 \cdot 4 \equiv 2 \pmod 5 \\ 3^1 &\equiv 3 \pmod 5 & \qquad 3^4 &\equiv 3 \cdot 2 \equiv 1 \pmod 5 \\ 3^2 &\equiv 3 \cdot 3 \equiv 4 \pmod 5 \end{aligned}$$

- $\mathrm{ord}_5(4) = 2$:

$$\begin{aligned} 4^0 &\equiv 1 \pmod 5 \\ 4^1 &\equiv 4 \equiv -1 \pmod 5 \\ 4^2 &\equiv (-1)^2 \equiv 1 \pmod 5 \end{aligned}$$

Exercício 18.5. Calcule $\mathrm{ord}_m(a)$ para todo a coprimo com m, para $m = 7$ e $m = 10$.

Em geral, não existe uma fórmula simples para calcular $\mathrm{ord}_m(a)$.

Teorema 18.6 (Pequeno teorema de Fermat)**.** *Se p é primo, então, para todo inteiro a,*

$$a^p \equiv a \pmod p.$$

Em particular, se $p \nmid a$, então

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

Demonstração. Basta mostrar para a natural. Por indução em a.

- Caso base $a = 0$: $0^p \equiv 0 \pmod p$.

- Passo indutivo: se $a^p \equiv a \pmod{p}$, mostremos que $(a+1)^p \equiv a+1 \pmod{p}$. Temos

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

  Como $p \mid \binom{p}{i}$ para todo $i = 1, \ldots, p-1$ (é crucial que p seja primo aqui!), concluímos que

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

Por fim, se $p \nmid a$, então $\overline{a}$ é invertível em $\mathbb{Z}/p\mathbb{Z}$, e podemos cancelar a em $a^p \equiv a \pmod{p}$. □

Exemplo 18.7. $2^{50} + 3^{50}$ é divisível por 13, pois:

- $2^{12} \equiv 1 \pmod{13} \implies (2^{12})^4 = 2^{48} \equiv 1 \pmod{13} \implies 2^{50} \equiv 2^{48} \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod{13}$;
- $3^{12} \equiv 1 \pmod{13} \implies \cdots \implies 3^{50} \equiv 3^2 \equiv 9 \pmod{13}$;

logo $2^{50} + 3^{50} \equiv 4 + 9 \equiv 13 \equiv 0 \pmod{13}$.

Em geral, se $p \nmid a$, então

$$a^n \equiv a^r \pmod{p},$$

onde $r \in \{0, 1, \ldots, p-2\}$ é o resto da divisão de n por $p-1$.

Exemplo 18.8. -1 não é um quadrado módulo 7 (isto é, não existe n tal que $n^2 \equiv -1 \pmod{7}$; ou ainda, $7 \nmid n^2 + 1$ para qualquer n). De fato, se $n^2 \equiv -1 \pmod{7}$, então

$$n^6 \equiv (-1)^3 \equiv -1 \pmod{7}.$$

Mas, por Fermat, $n^6 \equiv 1 \pmod{7}$. Absurdo!

Observação 18.9. Se m é composto, em geral *não* é verdade que $a^{m-1} \equiv 1 \pmod{m}$ para $(a, m) = 1$. Exemplo:

$$3^9 \equiv (3^2)^4 \cdot 3 \equiv (-1)^4 \cdot 3 \equiv 3 \pmod{10}.$$

Exercício 18.10. Um número composto m é dito *pseudoprimo em base a* se $a^{m-1} \equiv 1 \pmod{m}$. Verifique que 341 é pseudoprimo em base 2.

Voltando à ordem...

Proposição 18.11. *Se* $(a, m) = 1$ *e* $a^n \equiv 1 \pmod{m}$*, com* n *natural, então* $\mathrm{ord}_m(a) \mid n$.

Demonstração. Escreva $n = q\,\mathrm{ord}_m(a) + r$, com $0 \leqslant r < \mathrm{ord}_m(a)$. Então

$$1 \equiv a^n \equiv \left(a^{\mathrm{ord}_m(a)}\right)^q \cdot a^r \equiv a^r \pmod{m}.$$

Pela minimalidade de $\mathrm{ord}_m(a)$, temos $r = 0$. □

Corolário 18.12. *Se* p *é primo e* $p \nmid a$*, então* $\mathrm{ord}_p(a) \mid p - 1$. □

Exercício 18.13. Mostre que, se p é primo ímpar e q é um fator primo do número de Mersenne $2^p - 1$, então $q \equiv 1 \pmod{2p}$. Exemplo: $23 \mid 2^{11} - 1$ e $23 \equiv 1 \pmod{22}$.

Exercício 18.14.

1. Mostre que $11^{84} - 5^{84}$ é divisível por 7.
2. Mostre que -1 é um quadrado módulo p se, e somente se, $p = 2$ ou p é da forma $4n + 1$. (Dica: use o teorema de Wilson para a volta.)

Aula 19 (23/10)

10) Teoremas de Fermat e Euler (cont.)

Aula passada. Se p é primo e $p \nmid a$, então

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

Em particular, $\mathrm{ord}_p(a) \mid p-1$.

Quais são as possíveis ordens módulo p?

Exemplo 19.1 ($p = 11$)**.** Temos $p - 1 = 10$, cujos divisores positivos são $1, 2, 5, 10$. Temos $\mathrm{ord}_{11}(2) = 10$:

n	1	2	5	10
$2^n \bmod 11$	2	4	10	1

Em particular,

$$\begin{aligned} \mathrm{ord}_{11}(2^{10}) &= \mathrm{ord}_{11}(1) = 1, \\ \mathrm{ord}_{11}(2^5) &= \mathrm{ord}_{11}(10) = 2, \\ \mathrm{ord}_{11}(2^2) &= \mathrm{ord}_{11}(4) = 5. \end{aligned}$$

Assim, todos os divisores de 10 são a ordem de algum número módulo 11.

Definição 19.2. Uma *raiz primitiva módulo p* é um inteiro $g \in \mathbb{Z}$ tal que $\mathrm{ord}_p(g) = p - 1$ (a maior ordem possível).

Exemplo 19.3. 2 é raiz primitiva módulo 11.

Exercício 19.4. Mostre que, se g é uma raiz primitiva módulo p, então, para qualquer $d \mid p-1$, $\mathrm{ord}_p\left(g^{\frac{p-1}{d}}\right) = d$.

Exercício 19.5. Encontre uma raiz primitiva módulo 17.

Teorema 19.6. *Para todo primo p, existe raiz primitiva módulo p.*

Precisaremos de dois lemas.

Lema 19.7. *Se $f(x) = a_d x^d + \cdots + a_1 x + a_0$, com $a_i \in \mathbb{Z}$ e $a_d \not\equiv 0 \pmod{p}$, é um polinômio de grau d, então a congruência*

$$f(x) \equiv 0 \pmod{p}$$

tem no máximo *d soluções em um sistema completo de resíduos módulo p.* □

Observação 19.8. Isto é um caso particular de um fato mais geral (de álgebra): uma equação polinomial de grau d em um *corpo* tem no máximo d soluções. Aplique para o corpo $\mathbb{Z}/p\mathbb{Z}$.

Lema 19.9. *Se $d \mid p-1$, então existem exatamente d soluções de*

$$x^d \equiv 1 \pmod{p}$$

em um sistema reduzido de resíduos módulo p.

Demonstração. Seja R um sistema reduzido de resíduos módulo p e escreva $p-1 = d \cdot e$. Então

$$x^{p-1} - 1 = (x^d)^e - 1 = (x^d - 1) \cdot \underbrace{\left(x^{d(e-1)} + \cdots + 1\right)}_{f(x)}.$$

Pelo teorema de Fermat, todo inteiro $a \in R$ satisfaz

$$\begin{aligned} & 0 \equiv a^{p-1} - 1 \equiv (a^d - 1) f(a) \pmod{p} \\ \implies \quad & a^d - 1 \equiv 0 \pmod{p} \text{ ou } f(a) \equiv 0 \pmod{p}. \end{aligned}$$

Pelo lema anterior, $f(x) \equiv 0 \pmod{p}$ tem no máximo $d(e-1) = de - d = p - 1 - d$ soluções em R. Logo, $x^d - 1 \equiv 0 \pmod{p}$ tem pelo menos d soluções em R. Como, pelo lema anterior, ela tem no máximo d soluções, são exatamente d. □

Exercício 19.10. Mostre que, se $\operatorname{ord}_m(a_1) = n_1$, $\operatorname{ord}_m(a_2) = n_2$ e $(n_1, n_2) = 1$, então $\operatorname{ord}_m(a_1 a_2) = n_1 n_2$.

Demonstração do Teorema 19.6. Fatore $p - 1 = q_1^{e_1} \cdots q_k^{e_k}$, com q_i primos distintos. Pelo Exercício 19.10, basta mostrar que, para cada i, existe g_i tal que $\operatorname{ord}_p(g_i) = q_i^{e_i}$, pois, neste caso, a raiz primitiva será $g = g_1 \cdots g_k$.

Pelo Lema 19.9, $x^{q_i^{e_i}} \equiv 1 \pmod{p}$ tem $q_i^{e_i}$ soluções. Se nenhuma destas soluções a tem ordem $q_i^{e_i}$, então todas elas satisfazem $\operatorname{ord}_p(a) \mid q_i^{e_i - 1}$, logo são todas soluções de $x^{q_i^{e_i - 1}} \equiv 1 \pmod{p}$, o que é absurdo pelo Lema 19.9, pois $q_i^{e_i} > q_i^{e_i - 1}$. Logo, existe g_i tal que $\operatorname{ord}_p(g_i) = q_i^{e_i}$. □

Exercício 19.11. Mostre que, se $p \equiv 1 \pmod{4}$ e g é raiz primitiva módulo p, então $-g$ também é. O que acontece se $p \equiv 3 \pmod{4}$?

Observação 19.12. Não se sabe se existem infinitos primos p tais que 2 é raiz primitiva módulo p (conjectura de Artin).

E quando o módulo não é primo?

Teorema 19.13 (Euler)**.** *Se* $(a, m) = 1$*, então*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Exemplo 19.14 ($m = 10$)**.** Temos $\varphi(10) = \varphi(2)\cdot\varphi(5) = (2-1)\cdot(5-1) = 4$, e

n	0	1	2	3	4
$3^n \bmod 10$	1	3	9	7	1

Observação 19.15. Se p é primo, $\varphi(p) = p-1$. O teorema de Euler generaliza o teorema de Fermat.

Lema 19.16. *Se* $\{u_1, \ldots, u_{\varphi(m)}\}$ *é um sistema reduzido de resíduos módulo* m *e* $(a, m) = 1$*, então* $\{au_1, \ldots, au_{\varphi(m)}\}$ *também é um sistema reduzido de resíduos módulo* m*.*

Demonstração. Exercício. □

Exemplo 19.17 ($m = 10$, $a = 3$)**.**

$$\{1, 3, 7, 9\} \rightsquigarrow \{3, 9, 21, 27\},$$

e, de fato, $21 \equiv 1 \pmod{10}$ e $27 \equiv 7 \pmod{10}$.

Demonstração do Teorema 19.13. Seja $R = \{u_1, \ldots, u_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m. Pelo Lema 19.16, $\{au_1, \ldots, au_{\varphi(m)}\}$ também é um sistema reduzido de resíduos módulo m. Logo

$$a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} u_i \equiv \prod_{i=1}^{\varphi(m)} (au_i) \equiv \prod_{i=1}^{\varphi(m)} u_i \pmod{m} \iff a^{\varphi(m)} \equiv 1 \pmod{m},$$

onde, na última equivalência, cancelamos $\prod_i u_i$, que é coprimo com m. □

Corolário 19.18. *Se* $(a, m) = 1$*, então* $\mathrm{ord}_m(a) \mid \varphi(m)$*.* □

Exemplo 19.19 (OBM 1991)**.** Mostre que existem infinitos números da forma $199\cdots91$ que são múltiplos de 1991.

Queremos os n tais que

$$10^n + 9 \cdot 10^{n-1} + \cdots + 9 \cdot 10^1 + 1 \equiv 0 \pmod{1991}.$$

Como $1991 = 10^3 + 9 \cdot 10^2 + 9 \cdot 10 + 1$, isto equivale a

$$10^n + 9 \cdot 10^{n-1} + \cdots + 9 \cdot 10^1 + 1 \equiv 10^3 + 9 \cdot 10^2 + 9 \cdot 10 + 1 \pmod{1991}.$$

Cancelando $9\cdot 10^2+9\cdot 10+1$ dos dois lados, e depois 10^3 (pois $(10, 1991) = 1$):

$$\begin{aligned}
&\iff 10^n + 9\cdot\left(10^{n-1}+\cdots+10^3\right) \equiv 10^3 \pmod{1991}\\
&\iff 10^{n-3} + 9\cdot\underbrace{\left(10^{n-4}+\cdots+1\right)}_{\frac{10^{n-3}-1}{9}} \equiv 1 \pmod{1991}\\
&\iff 10^{n-3} + 10^{n-3} - 1 \equiv 1 \pmod{1991}\\
&\iff 2\cdot 10^{n-3} \equiv 2 \pmod{1991}\\
&\iff 10^{n-3} \equiv 1 \pmod{1991}.
\end{aligned}$$

Pelo teorema de Euler, basta tomar $n-3$ múltiplo de $\varphi(1991)$.

Exercício 19.20. 1) Mostre que, para todo $a \in \mathbb{Z}$, $\overline{a}^{10} \in \{-\overline{1}, \overline{0}, \overline{1}\}$ em $\mathbb{Z}/25\mathbb{Z}$.

2) Mostre que existem infinitos inteiros que *não* são da forma $x_1^6 + x_2^6 + \cdots + x_8^6$. (Dica: olhe módulo 27.)

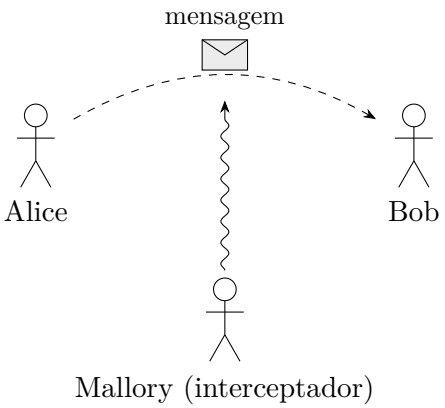
3) Mostre que $a^{12} \equiv 1 \pmod{72}$ para todo a coprimo com 72.

Aula 20 (04/11)

11) Criptografia RSA

O nome RSA vem de Rivest, Shamir e Adleman.

Objetivo: transmissão segura de dados (mensagem) na presença de comportamento adversário.



Criptografia: técnicas para transformar a mensagem original em uma mensagem ininteligível (*encriptar*) e também fazer o processo inverso (*desencriptar*). A encriptação e a desencriptação se fazem através de *chaves*.

Exemplo 20.1 (Cifra de César)**.** Numeramos as letras:

A	B	C	D	$\cdots$	Z
1	2	3	4	$\cdots$	26

Chave: $i \mapsto i + 3 \pmod{26}$, isto é, $A \mapsto D$, $B \mapsto E$, $\ldots$, $Z \mapsto C$.

Mensagem original (criada por Alice): OLA.

Mensagem encriptada pela chave (recebida por Bob, ou interceptada por Mallory): ROD.

Criptografia simétrica: a chave de encriptação é a mesma chave de desencriptação. (Problema: como transmitir a chave?)

Criptografia assimétrica: chaves de encriptação e desencriptação diferentes (*chave pública*).

Protocolo RSA. A mensagem será encriptada por Alice em uma sequência de números naturais, que será transmitida a Bob. Esta sequência é pública (Mallory pode ver), mas somente Bob sabe desencriptar.

Protocolo Bob. Bob quer receber a mensagem. Bob escolhe:

1) Dois números primos distintos p e q.
2) Um natural e (de "expoente") tal que $(e, p-1) = 1$ e $(e, q-1) = 1$.

Bob forma o produto $n = p \cdot q$ e anuncia publicamente o par

$$(n, e) = \text{chave de encriptação}$$

(que é pública!).

Observação 20.2. Bob *não* anuncia os primos p e q separadamente.

Exercício 20.3. Verifique que as condições $(e, p-1) = 1$ e $(e, q-1) = 1$ são equivalentes a $(e, \varphi(n)) = 1$.

Exemplo 20.4. Bob escolhe $p = 7$ e $q = 13$. Como $p - 1 = 6$ e $q - 1 = 12$, podemos tomar $e = 5$ (pois $(5, 6) = 1$ e $(5, 12) = 1$). Bob anuncia $(n, e) = (91, 5)$.

Protocolo Alice. Alice conhece o par (n, e). Para enviar a mensagem, Alice:

1) Transforma a mensagem em uma sequência de dígitos, usando um dicionário público. Por exemplo:

A	B	C	$\cdots$	Z
01	02	03	$\cdots$	26

2) Separa estes dígitos em blocos, cada um representando um número $< n$.

Cada bloco é encriptado e enviado separadamente. Sejam $M_1, \ldots, M_r$ estes blocos.

1) Para cada i, Alice calcula $C_i \in \{0, \ldots, n-1\}$ tal que

$$C_i \equiv M_i^e \pmod{n}.$$

2) Alice transmite $C_1, \ldots, C_r$ a Bob.

Exemplo 20.5. Bob anunciou $(91, 5)$. Alice quer transmitir a mensagem

$$\text{OI} = 1509 \qquad (\text{O} = 15,\ \text{I} = 09).$$

Como $1509 > 91$, separamos em blocos $M_1 = 15$, $M_2 = 09$. Alice calcula

$$C_1 \equiv 15^5 \equiv \cdots \equiv 71 \pmod{91}, \qquad C_2 \equiv 9^5 \equiv \cdots \equiv 81 \pmod{91},$$

e transmite $C_1 = 71$ e $C_2 = 81$ a Bob.

Desencriptando. Bob recebe $C_1, \ldots, C_r$ (mensagem encriptada) e:

1) Calcula, usando o algoritmo de Euclides, d tal que

$$d \cdot e \equiv 1 \pmod{\varphi(n)}.$$

O par (n, d) é a *chave de desencriptação.*

2) Para cada i, calcula $N_i \in \{0, 1, \ldots, n-1\}$ tal que

$$N_i \equiv C_i^d \pmod{n}.$$

3) Transforma $N_1, \ldots, N_r$ em uma mensagem usando o mesmo dicionário de Alice.

Exemplo 20.6. No exemplo anterior, $\varphi(91) = 72$ e tomamos $d = 29$, pois $5 \cdot 29 = 145 \equiv 1 \pmod{72}$. Então

$$71^{29} \equiv \cdots \equiv 15 \pmod{91}, \qquad 81^{29} \equiv \cdots \equiv 9 \pmod{91},$$

e Bob encontra $N_1 = 15 = M_1$ e $N_2 = 09 = M_2$.

Teorema 20.7. *Sejam p, q números primos distintos, $n = pq$, e um natural coprimo com $\varphi(n)$ e $M \in \{0, \ldots, n-1\}$. Se $de \equiv 1 \pmod{\varphi(n)}$, então*

$$M \equiv M^{de} \pmod{n}.$$

"Demonstração". Escreva $de = 1 + \varphi(n) \cdot k$. Se $(M, n) = 1$, o enunciado segue do teorema de Euler:

$$M^{de} = M^{1+\varphi(n)k} = M \cdot \big(\underbrace{M^{\varphi(n)}}_{\equiv 1}\big)^k \equiv M \pmod{n}. \qquad \square$$

Exercício 20.8. Complete a demonstração. [Dica: se $p \mid M$ ou $q \mid M$, mostre que $M \equiv M^{de} \pmod{p}$ e $M \equiv M^{de} \pmod{q}$ separadamente.]

Exercício 20.9. A seguinte mensagem foi encriptada usando a chave RSA $(n, e) = (2881, 5)$:

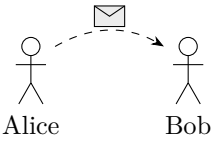
$$1972 \quad 430 \quad 2430 \quad 2773$$

Desencripte a mensagem. (Use uma calculadora de exponenciação modular.)

Aula 21 (06/11)

11) Criptografia RSA (cont.)

Aula passada.



- (n, e): chave pública (encriptação), onde $n = p \cdot q$ e $(e, \varphi(n)) = 1$.
- M = bloco de mensagem, $0 \leqslant M \leqslant n-1$, é encriptado em C = bloco encriptado, $0 \leqslant C \leqslant n-1$, tal que $C \equiv M^e \pmod{n}$.
- Teorema: se $de \equiv 1 \pmod{\varphi(n)}$, então $M \equiv C^d \pmod{n}$.
- (n, d): chave privada (desencriptação).

Segurança? O método RSA será seguro se for *difícil* calcular M a partir de C e (n, e) (o "problema do RSA").

A única maneira conhecida de resolver o problema acima em geral é calculando d, o inverso de e módulo $\varphi(n)$. Se conhecemos $\varphi(n)$, então é fácil calcular d pelo algoritmo de Euclides.

Exemplo 21.1. Sejam $(n, e) = (7597, 4947)$ e $\varphi(n) = 7420$. Queremos d tal que $4947d \equiv 1 \pmod{7420}$, isto é,

$$4947d = 1 - 7420k \text{ para algum } k \iff 7420k + 4947d = 1.$$

Pelo algoritmo de Euclides,

$$\begin{aligned} 7420 &= 1 \cdot 4947 + 2473, \\ 4947 &= 2 \cdot 2473 + 1. \end{aligned}$$

Logo

$$\begin{aligned} 1 &= 4947 - 2 \cdot 2473 \\ &= 4947 - 2 \cdot (7420 - 1 \cdot 4947) \\ &= -2 \cdot 7420 + 3 \cdot 4947. \end{aligned}$$

Isto é, $d = 3$.

Observação 21.2. Se $n = p \cdot q$ (com p e q primos distintos), conhecer n e $\varphi(n)$ é equivalente a conhecer p e q!

Se conhecemos p e q, temos

$$n = p \cdot q \qquad \text{e} \qquad \varphi(n) = (p-1) \cdot (q-1).$$

Se conhecemos n e $\varphi(n)$, note que

$$\begin{aligned}(x-p)(x-q) &= x^2 - (p+q)x + pq \\ &= x^2 - (pq - (p-1)(q-1) + 1)x + pq \\ &= x^2 - (n - \varphi(n) + 1)x + n. \qquad (*)\end{aligned}$$

Logo, podemos recuperar p e q como raízes do polinômio $(*)$.

Exercício 21.3. Sabendo que $n = 10088821$ é um produto de dois primos distintos e $\varphi(n) = 10082272$, fatore n.

A única maneira conhecida de "quebrar a criptografia RSA" em geral é fatorando n. Logo, o método RSA será seguro se a escolha de p e q for tal que seja *difícil* fatorar $n = p \cdot q$.

Existem diversos algoritmos de fatoração de inteiros. Atualmente, o melhor para situações gerais é o *General Number Field Sieve* (1993).

Exemplo 21.4 (Método de Fermat)**.** Queremos fatorar n. Ideia: encontrar a e b tais que

$$n = a^2 - b^2 = (a-b)(a+b).$$

1) Podemos remover todas as potências de 2 e supor que n é ímpar.

2) Seja x o menor inteiro $\geqslant \sqrt{n}$ (isto é, $x = \lceil \sqrt{n} \rceil$).

3) Teste $x^2 - n$, $(x+1)^2 - n$, $(x+2)^2 - n$, ..., até encontrar j tal que

$$\underbrace{(x+j)}_{a}{}^2 - n = b^2.$$

Exemplo 21.5. Seja $n = 2881$. Temos $50^2 = 2500$ e $(50+k)^2 = 2500 + 100k + k^2$, logo $53^2 < 2881 < 54^2$ e

$$x = 54 = \lceil \sqrt{2881} \rceil.$$

Então

$$\begin{aligned}x^2 - n &= 54^2 - 2881 = 2916 - 2881 = 35, \\ (x+1)^2 - n &= 55^2 - 2881 = 3025 - 2881 = 144 = 12^2.\end{aligned}$$

Logo,

$$2881 = 55^2 - 12^2 = (55+12)(55-12) = 67 \cdot 43.$$

Exercício 21.6. 1) Fatore 6077 usando o método de Fermat.

2) Mostre que o algoritmo sempre para em algum $j \leqslant \frac{n+1}{2} - x$ e que n é composto se, e somente se, $j < \frac{n+1}{2} - x$.

Observação 21.7. O método de Fermat é eficiente se $n = pq$ com $|p - q|$ pequeno!

Como escolher p e q no método RSA? Tomamos p e q *grandes* aleatoriamente, garantindo que

- p e q não estão próximos;
- $p-1$, $q-1$, $p+1$ e $q+1$ não têm fatores primos pequenos.

Observação 21.8. Atualmente, a recomendação é que $n = pq$ tenha tamanho 2048 bits (isto é, 2048 dígitos em base 2).

Como tomar primos aleatoriamente? Tomamos números aleatoriamente (em um intervalo $[X, 2X]$, com X grande) e usamos um *teste de primalidade*.

Exemplo 21.9 (Teste de Miller–Rabin)**.** Queremos verificar se n (ímpar) é primo.

1) Escreva $n - 1 = 2^s \cdot t$, com t ímpar.
2) Tome $a \in \{1, \ldots, n-1\}$ e calcule
$$a^t,\ a^{2t},\ \ldots,\ a^{2^{s-1}t} \bmod n.$$
3) Se $a^t \not\equiv 1 \pmod{n}$ e $a^{2^i t} \not\equiv -1 \pmod{n}$ para todo $i \in \{0, 1, \ldots, s-1\}$, então n é composto.

Se não (isto é, se $a^t \equiv 1 \pmod{n}$ ou $a^{2^i t} \equiv -1 \pmod{n}$ para algum $i \in \{0, 1, \ldots, s-1\}$), n é dito *pseudoprimo forte na base a*.

Exercício 21.10. 1) Verifique que um pseudoprimo forte na base a é um pseudoprimo (de Fermat) na base a.

2) Mostre que, se n é primo, então $a^t \equiv 1 \pmod{n}$ ou $a^{2^i t} \equiv -1 \pmod{n}$ para algum $i \in \{0, 1, \ldots, s-1\}$.

Exemplo 21.11. Seja $n = 341$ (pseudoprimo na base 2). Temos $340 = 2^2 \cdot 85$ e
$$2^{85} \equiv \cdots \equiv 32 \not\equiv \pm 1 \pmod{341},$$
$$2^{2 \cdot 85} \equiv 32^2 \equiv \cdots \equiv 1 \not\equiv -1 \pmod{341}.$$
Logo, 341 é composto!

Exercício 21.12. Mostre que 561 é composto usando o teste de Miller–Rabin na base 2.

Na prática, para verificar se um número é primo com alta probabilidade, aplicamos o teste de Miller–Rabin em várias bases diferentes...

Aula 22 (11/11)

12) Resíduos quadráticos

Seja p um primo ímpar (para simplificar). Sabemos resolver congruências lineares

$$\underbrace{ax+b}_{\text{polinômio de grau 1}} \equiv 0 \pmod{p}:$$

basta resolver a equação diofantina linear

$$ax + b = py \iff ax - py = -b.$$

Como resolver uma congruência quadrática

$$\underbrace{ax^2+bx+c}_{\text{polinômio de grau 2}} \equiv 0 \pmod{p} \ ?$$

Exemplo 22.1. Vamos resolver $3x^2 + x \equiv 3 \pmod 7$. O inverso de 3 módulo 7 é 5, pois $5 \cdot 3 = 15 \equiv 1 \pmod 7$. Multiplicando por 5, temos

$$3x^2 + x \equiv 3 \pmod 7 \iff x^2 + 5x \equiv 1 \pmod 7.$$

Lembre-se do *completamento de quadrado*:

$$x^2 + ax = x^2 + 2\,\frac{a}{2}\,x = x^2 + 2\,\frac{a}{2}\,x + \frac{a^2}{4} - \frac{a^2}{4} = \Big(x + \frac{a}{2}\Big)^2 - \Big(\frac{a}{2}\Big)^2.$$

O mesmo truque funciona módulo 7: basta trocar $\frac{1}{2}$ pelo inverso de 2 módulo 7, que é 4, pois $2 \cdot 4 = 8 \equiv 1 \pmod 7$. Assim,

$$\begin{aligned} x^2 + 5x \equiv 1 \pmod 7 &\iff (x + 4\cdot 5)^2 - 4^2 \cdot 5^2 \equiv 1 \pmod 7 \\ &\iff (x-1)^2 - 1 \equiv 1 \pmod 7 \\ &\iff (x-1)^2 \equiv 2 \pmod 7. \end{aligned}$$

Os quadrados módulo 7 são:

x	0	1	2	3	4	5	6
$x^2 \bmod 7$	0	1	4	**2**	**2**	4	1

Logo,

$$\begin{aligned} x^2 + 5x \equiv 1 \pmod 7 &\iff (x-1)^2 \equiv 2 \pmod 7 \\ &\iff x - 1 \equiv 3 \text{ ou } 4 \pmod 7 \\ &\iff x \equiv 4 \text{ ou } 5 \pmod 7. \end{aligned}$$

Observação 22.2. A fórmula de Bhaskara

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

funciona, se devidamente interpretada. No exemplo acima, $a = 3$, $b = 1$ e $c = -3$, e

$$b^2 - 4ac = 1 - 4 \cdot 3 \cdot (-3) \equiv 2 \pmod 7.$$

As "raízes quadradas de 2 módulo 7" são ± 3. Logo,

$$x \equiv (-1 \pm 3) \cdot \underbrace{(4 \cdot 5)}_{\text{inverso de } 2a} \equiv 4 \text{ ou } 5 \pmod 7.$$

Exercício 22.3. Resolva a congruência quadrática $4x^2+x+4 \equiv 0 \pmod{11}$.

Conclusão. Para resolver uma congruência quadrática qualquer, basta saber resolver congruências da forma

$$x^2 \equiv a \pmod p, \tag{1}$$

ou seja:

1. entender quando um dado inteiro a é um *resíduo quadrático* módulo p (isto é, quando (1) admite solução);
2. se a for resíduo quadrático, como encontrar x?

Exemplo 22.4 (Quadrados módulo p)**.** Vamos listar os resíduos quadráticos em um sistema reduzido $\{1, 2, 3, \ldots, p-1\}$; abaixo, os resíduos quadráticos estão destacados com uma caixa.

- $p = 3$: $\boxed{1}$ 2. De fato, $1^2 \equiv 1 \pmod 3$ e $2^2 \equiv 1 \pmod 3$.
- $p = 5$: $\boxed{1}$ 2 3 $\boxed{4}$. De fato,

  $$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 4, \quad 4^2 \equiv 1 \pmod 5.$$

- $p = 7$: $\boxed{1}$ $\boxed{2}$ 3 $\boxed{4}$ 5 6. De fato,

  $$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2, \quad 4^2 \equiv (-3)^2 \equiv 2 \pmod 7, \quad \ldots$$

- $p = 11$: $\boxed{1}$ 2 $\boxed{3}$ $\boxed{4}$ $\boxed{5}$ 6 7 8 $\boxed{9}$ 10.
  De fato,

  $$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9, \quad 4^2 \equiv 5, \quad 5^2 \equiv 3 \pmod{11}, \quad \ldots$$

Em todos os casos acima, exatamente metade dos elementos de um sistema reduzido são resíduos quadráticos!

Lema 22.5. *Seja p um primo ímpar. Em um sistema reduzido de resíduos módulo p, existem exatamente $\frac{p-1}{2}$ resíduos quadráticos.*

Demonstração. Seja Q a imagem de

$$f\colon (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, \qquad \overline{x} \longmapsto \overline{x}^2.$$

Queremos mostrar que Q tem $\frac{p-1}{2}$ elementos. Basta mostrar que, para todo $\overline{a} \in Q$, a pré-imagem

$$f^{-1}(\overline{a}) = \{\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\times : f(\overline{x}) = \overline{a}\}$$

tem exatamente dois elementos, pois isto implica que

$$p - 1 = \operatorname{card}\big((\mathbb{Z}/p\mathbb{Z})^\times\big) = 2 \cdot \operatorname{card}(Q).$$

Se $\overline{x}^2 = \overline{a}$, então $(-\overline{x})^2 = \overline{a}$, e $-\overline{x} \neq \overline{x}$ pois p é ímpar e $p \nmid x$. Logo, $f^{-1}(\overline{a})$ tem pelo menos 2 elementos. Mas vimos que uma equação polinomial de grau d módulo p tem no máximo d raízes módulo p. □

Observação 22.6. No sistema reduzido $\{1, 2, \ldots, p-1\}$, cada par

$$\{1, p-1\}, \quad \{2, p-2\}, \quad \ldots, \quad \left\{\frac{p-1}{2}, \frac{p+1}{2}\right\}$$

corresponde a um resíduo quadrático diferente.

Exercício 22.7. Mostre que, se g é uma raiz primitiva módulo p, então g^n é resíduo quadrático módulo p se, e somente se, n é par. Assim, um sistema reduzido se divide em

$$\underbrace{\{1, g^2, g^4, \ldots\}}_{\text{resíduos quadráticos}} \qquad \text{e} \qquad \underbrace{\{g, g^3, \ldots\}}_{\text{resíduos não-quadráticos}} .$$

Observação 22.8. Se o módulo não for primo, a propriedade acima não vale. Por exemplo, os resíduos quadráticos módulo 8 no sistema reduzido $\{1, 3, 5, 7\}$ são apenas

$$\boxed{1} \quad 3 \quad 5 \quad 7,$$

pois

$$1^2 \equiv 1, \quad 3^2 \equiv 1, \quad 5^2 \equiv (-3)^2 \equiv 1, \quad 7^2 \equiv (-1)^2 \equiv 1 \pmod 8.$$

Aula 23 (13/11)

12) Resíduos quadráticos (cont.)

Definição 23.1. Um inteiro a é dito *resíduo quadrático* módulo m se existe $b \in \mathbb{Z}$ tal que $b^2 \equiv a \pmod{m}$.

Aula passada. Se p é primo ímpar, exatamente metade dos elementos de $\{1, 2, \ldots, p-1\}$ são resíduos quadráticos.

Proposição 23.2 (Critério de Euler)**.** *Seja p um primo ímpar. Se $p \nmid a$, então a é resíduo quadrático módulo p se, e somente se,*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Demonstração. Pelo teorema de Fermat,

$$a^{p-1} \equiv 1 \pmod{p} \iff a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Como $p-1$ é par, podemos fatorar:

$$0 \equiv a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \pmod{p}.$$

Como p é primo, devemos ter

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \qquad \text{ou} \qquad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Se a é resíduo quadrático, então $a \equiv b^2 \pmod{p}$. Logo, pelo teorema de Fermat,

$$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}.$$

Assim, a equação polinomial de grau $\frac{p-1}{2}$

$$x^{\frac{p-1}{2}} - \overline{1} = \overline{0}$$

tem pelo menos $\frac{p-1}{2}$ soluções em $\mathbb{Z}/p\mathbb{Z}$ (dadas pelos resíduos quadráticos). Por um teorema anterior, estas são *todas* as soluções. □

Exemplo 23.3. O número 2 é resíduo quadrático módulo 101? Vamos calcular 2^{50}:

$$\begin{aligned}
2^{10} &\equiv 1024 \equiv 1024 - 10 \cdot 101 \equiv 14 \pmod{101},\\
2^{20} &\equiv 2^2 \cdot 7^2 \equiv 4 \cdot 49 \equiv 4 \cdot (50 - 1)\\
&\equiv 2 \cdot 100 - 4 \equiv -2 - 4 \equiv -6 \pmod{101},\\
2^{40} &\equiv (-6)^2 \equiv 36 \pmod{101},\\
2^{50} &\equiv 14 \cdot 36 \equiv 2 \cdot 7 \cdot (2 \cdot 3)^2 \equiv 2^3 \cdot 3^2 \cdot 7\\
&\equiv 2^3 \cdot 63 \equiv 2^2 \cdot 126 \equiv 2^2 \cdot 25\\
&\equiv 100 \equiv -1 \pmod{101}.
\end{aligned}$$

Logo, 2 *não* é resíduo quadrático módulo 101.

Exercício 23.4. Verifique se 3 e 6 são resíduos quadráticos módulo 101.

Definição 23.5 (Símbolo de Legendre)**.** Seja p um primo ímpar. Para todo $a \in \mathbb{Z}$, definimos

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{se } a \text{ não é resíduo quadrático módulo } p \text{ (e } p \nmid a), \\ 0, & \text{se } p \mid a, \\ 1, & \text{se } a \text{ é resíduo quadrático módulo } p \text{ (e } p \nmid a). \end{cases}$$

Exemplo 23.6. Vimos que $\left(\frac{2}{101}\right) = -1$.

Observação 23.7. O critério de Euler diz que

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Exemplo 23.8. Para quais p o número -1 é resíduo quadrático módulo p? Pelo critério de Euler,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p}, & \text{se } \frac{p-1}{2} \text{ é par}, \\ -1 \pmod{p}, & \text{se } \frac{p-1}{2} \text{ é ímpar}. \end{cases}$$

Logo,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \pmod 4 \quad (p = 4n+1), \\ -1, & \text{se } p \equiv 3 \pmod 4 \quad (p = 4n+3). \end{cases}$$

Exemplo 23.9. $\left(\frac{-1}{101}\right) = 1$. De fato, $10^2 \equiv 100 \equiv -1 \pmod{101}$.

Exercício 23.10. Determine se a congruência

$$9x^2 - 30x + 26 \equiv 0 \pmod{103}$$

tem solução.

Exemplo 23.11. Para quais p o número 2 é resíduo quadrático módulo p? Pelo critério de Euler,

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod{p}.$$

Multiplicando todos os pares em $\{1, 2, 3, \ldots, p-1\}$, obtemos

$$2 \cdot 4 \cdot 6 \cdots (p-1) = (2 \cdot 1) \cdot (2 \cdot 2) \cdot (2 \cdot 3) \cdots \left(2 \cdot \frac{p-1}{2}\right) = 2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!.$$

Reorganizando o produto e multiplicando o primeiro termo com o último, o segundo com o penúltimo, etc., obtemos

$$\begin{aligned} &(2 \cdot (p-1)) \cdot (4 \cdot (p-3)) \cdot (6 \cdot (p-5)) \cdots \\ &\quad \equiv (2 \cdot (-1)) \cdot (4 \cdot (-3)) \cdot (6 \cdot (-5)) \cdots \\ &\quad \equiv ((-1)^2 \cdot 2 \cdot (-1)^1 \cdot 1) \cdot ((-1)^4 \cdot 4 \cdot (-1)^3 \cdot 3) \cdots \\ &\quad \equiv (-1)^{1+2+\cdots+\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

(O final do produto anterior depende de se $p \equiv 1$ ou $3 \pmod 4$, mas a fórmula acima é sempre verdade.) Como

$$1+2+\cdots+\frac{p-1}{2} = \frac{1}{2}\Big(\frac{p-1}{2}\Big)\Big(\frac{p-1}{2}+1\Big) = \frac{1}{2}\Big(\frac{p-1}{2}\Big)\Big(\frac{p+1}{2}\Big) = \frac{p^2-1}{8},$$

e $(\frac{p-1}{2})!$ é invertível módulo p, obtemos

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p.$$

Exercício 23.12. Verifique que

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{se } p \equiv \pm 1 \pmod 8, \\ -1, & \text{se } p \equiv \pm 3 \pmod 8. \end{cases}$$

Exemplo 23.13. Temos $101 \equiv 10^2 + 1 \equiv (-2)^2 + 1 \equiv 5 \equiv -3 \pmod 8$. Logo, $\left(\frac{2}{101}\right) = -1$ (2 não é resíduo quadrático módulo 101), como já tínhamos visto.

Proposição 23.14 (Propriedades do símbolo de Legendre)**.** *Seja p um primo ímpar.*

(1) Se $a \equiv b \pmod p$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) $\left(\frac{a^2}{p}\right) = 1$ se $p \nmid a$.

(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

(4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(5) (Multiplicatividade) $\left(\frac{a\cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Demonstração.

- (1) e (2) seguem da definição.
- (3) e (4) vimos nos exemplos anteriores.
- Mostremos (5). Pelo critério de Euler,

$$\left(\frac{a\cdot b}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p.$$

  Logo,

$$p \,\Big|\, \left(\frac{a\cdot b}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

  Como $\left|\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right| \leqslant 2$ e $p > 2$, devemos ter $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0$. □

Exemplo 23.15. Vamos calcular $\left(\frac{70}{73}\right)$. Como $73 \equiv 1 \pmod 4$, temos $\left(\frac{-1}{73}\right) = 1$, logo

$$\left(\frac{70}{73}\right) = \left(\frac{-3}{73}\right) = \left(\frac{-1}{73}\right)\left(\frac{3}{73}\right) = \left(\frac{3}{73}\right).$$

Pelo critério de Euler,

$$\left(\frac{3}{73}\right) \equiv 3^{\frac{73-1}{2}} \equiv 3^{36} \pmod{73}.$$

Agora,

$$\begin{aligned} 3^4 &\equiv 81 \equiv 8 \pmod{73}, \\ 3^6 &\equiv 8 \cdot 9 \equiv 72 \equiv -1 \pmod{73}, \\ 3^{36} &\equiv (3^6)^6 \equiv (-1)^6 \equiv 1 \pmod{73}. \end{aligned}$$

Logo, $\left(\frac{70}{73}\right) = 1$.

Exercício 23.16.

1. Calcule $\left(\frac{249}{257}\right)$.
2. Mostre que existem infinitos primos da forma $4n+1$ usando $\left(\frac{-1}{p}\right)$. [Dica: suponha por absurdo que $p_1, \ldots, p_k$ são todos os primos da forma $4n+1$ e considere $N = (2p_1 \cdots p_k)^2 + 1$.]

Aula 24 (18/11)

12) Resíduos quadráticos (cont.)

Aula passada. Vimos o símbolo de Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é um quadrado não nulo módulo } p, \\ 0, & \text{se } p \mid a, \\ -1, & \text{se } a \text{ não é um quadrado módulo } p, \end{cases}$$

e o critério de Euler:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Como calcular $\left(\frac{7}{103}\right)$ sem precisar calcular 7^{51} módulo 103?

Teorema 24.1 (Lei de reciprocidade quadrática)**.** *Se p e q são primos ímpares distintos, então*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

$\left(\textit{ou, equivalentemente, } \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)\right)$.

Exemplo 24.2. Como $103 = 14 \cdot 7 + 5$,

$$\left(\frac{7}{103}\right) = (-1)^{3\cdot 51}\left(\frac{103}{7}\right) = -\left(\frac{5}{7}\right) = -1 \cdot (-1) = 1,$$

pois os quadrados módulo 7 são $1^2 \equiv 1$, $2^2 \equiv 4$ e $3^2 \equiv 2$, e 5 não está entre eles.

Observação 24.3.

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} 1, & \text{se } p \text{ ou } q \equiv 1 \pmod 4, \\ -1, & \text{senão.} \end{cases}$$

Exemplo 24.4. Vamos calcular $\left(\frac{29}{43}\right)$. Como $29 \equiv 1 \pmod 4$ e $43 - 29 = 14$,

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right).$$

Temos $\left(\frac{2}{29}\right) = -1$, pois $29 \equiv -3 \pmod 8$. Logo,

$$\left(\frac{29}{43}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Exemplo 24.5. Vamos calcular $\left(\frac{-2024}{45083}\right)$. O número 45083 é primo e $45083 \equiv 3 \pmod 8$ (logo $45083 \equiv 3 \pmod 4$). Além disso, $2024 = 2^3 \cdot 11 \cdot 23$. Assim,

$$\begin{aligned}\left(\frac{-2024}{45083}\right) &= \left(\frac{-1}{45083}\right)\left(\frac{2}{45083}\right)^3\left(\frac{11}{45083}\right)\left(\frac{23}{45083}\right)\\ &= (-1)\cdot(-1)^3\cdot(-1)\left(\frac{45083}{11}\right)\cdot(-1)\left(\frac{45083}{23}\right)\\ &= \left(\frac{5}{11}\right)\left(\frac{3}{23}\right) = \left(\frac{11}{5}\right)\cdot(-1)\left(\frac{23}{3}\right)\\ &= -\left(\frac{1}{5}\right)\left(\frac{2}{3}\right) = 1.\end{aligned}$$

Exercício 24.6. Calcule os símbolos de Legendre $\left(\frac{44}{103}\right)$ e $\left(\frac{-60}{1019}\right)$.

Exercício 24.7. Determine se 251 é resíduo quadrático módulo 779. [Obs.: $779 = 19 \cdot 41$ não é primo!]

13) Somas de quadrados

Quais primos se escrevem como soma de dois quadrados?

$$2 = 1^2 + 1^2, \quad 3 \text{ não dá}, \quad 5 = 1^2 + 2^2,$$
$$7 \text{ não dá}, \quad 11 \text{ não dá}, \quad 13 = 2^2 + 3^2, \quad \ldots$$

Lema 24.8. *Se p é um primo ímpar tal que existem $a, b \in \mathbb{Z}$ com $p = a^2 + b^2$, então $p \equiv 1 \pmod 4$.*

Contrapositiva: se $p \equiv 3 \pmod 4$, então p *não* se escreve como soma de dois quadrados.

Demonstração. Os quadrados módulo 4 são 0 e 1. Se $p = a^2 + b^2$, então $p \equiv 0$, 1 ou 2 $\pmod 4$; como p é ímpar, $p \equiv 1 \pmod 4$. □

Teorema 24.9. *Se p é um primo ímpar tal que $p \equiv 1 \pmod 4$, então existem $a, b \in \mathbb{Z}$ tais que $p = a^2 + b^2$.*

Demonstração. Como $\left(\frac{-1}{p}\right) = 1$, existe $x \in \{1, \ldots, p-1\}$ tal que $x^2 \equiv -1 \pmod p$.

Afirmação: existem $a, b \in \mathbb{Z}$, não ambos nulos, com $|a|, |b| < \sqrt{p}$, tais que $ax + b \equiv 0 \pmod p$.

De fato, existem $\lfloor\sqrt{p}\rfloor + 1$ escolhas para $0 \leqslant m < \sqrt{p}$, logo $(\lfloor\sqrt{p}\rfloor + 1)^2$ números da forma $mx + n$ com $0 \leqslant m, n < \sqrt{p}$. Como $(\lfloor\sqrt{p}\rfloor + 1)^2 > p$,

segue do princípio da casa dos pombos que existem pares distintos $(m_1, n_1) \neq (m_2, n_2)$ tais que

$$m_1 x + n_1 \equiv m_2 x + n_2 \pmod{p}.$$

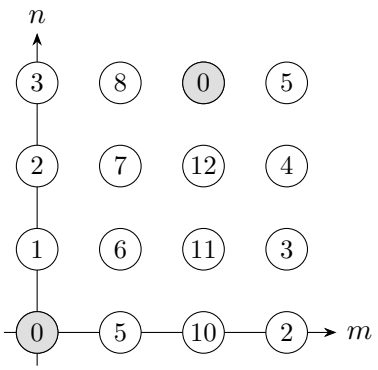
Basta tomar $a = m_1 - m_2$ e $b = n_1 - n_2$.

Logo,

$$ax \equiv -b \pmod{p} \implies -a^2 \equiv a^2 x^2 \equiv b^2 \pmod{p} \implies p \mid a^2 + b^2.$$

Como $|a|, |b| < \sqrt{p}$ e a, b não são ambos nulos, temos $0 < a^2 + b^2 < 2p$. A única possibilidade é $p = a^2 + b^2$. □

Exemplo 24.10. Para $p = 13$, temos $x = 5$, pois $5^2 = 25 \equiv -1 \pmod{13}$, e $\lfloor \sqrt{13} \rfloor = 3$. Os 16 pares (m, n) com $0 \leqslant m, n \leqslant 3$ estão na figura, cada um com o valor de $5m + n$ módulo 13. Como só há 13 restos, há repetições. Por exemplo, os pares $(0, 0)$ e $(2, 3)$ (em cinza) têm ambos valor 0. Tomando $a = 2$ e $b = 3$, obtemos $13 = 2^2 + 3^2$.



Exercício 24.11.

1. Mostre que, se m e n se escrevem como soma de dois quadrados, então $m \cdot n$ também se escreve como soma de dois quadrados.

2. Mostre que m se escreve como soma de dois quadrados se, e somente se,
$$m = 2^e d^2 p_1 \cdots p_r$$
com $e \geqslant 0$ e d inteiros quaisquer e $p_1, \ldots, p_r$ primos da forma $4n + 1$.

Observação 24.12 (Teorema de Lagrange). Todo inteiro positivo se escreve como soma de 4 quadrados...

Listas de exercícios

Exercícios propostos ao longo do curso, organizados por tema.

1. Aquecimento

1.1 Verifique que, se (a, b, c) é uma terna pitagórica e u é um inteiro qualquer, então (ua, ub, uc) é uma terna pitagórica.

1.2 Se (a, b, c) é uma terna pitagórica primitiva com a ímpar, mostre que $c - b$ e $c + b$ não têm fatores em comum.

1.3 Mostre que, se t e s são inteiros ímpares sem fatores em comum satisfazendo $s > t \geqslant 1$, então

$$(a, b, c) = \left(ts, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2} \right)$$

é uma terna pitagórica primitiva, com a ímpar.

1.4 Seja n o dobro de um número ímpar (exemplos: 2, 6, 10, 14, ...). Existe uma terna pitagórica *primitiva* (a, b, c) tal que $b = n$?

1.5 A uma terna pitagórica (a, b, c) associamos o ponto $(x, y) = (a/c, b/c)$ no círculo unitário de equação $x^2 + y^2 = 1$. Determine se esta associação é injetiva ou sobrejetiva.

1.6 Encontre uma fórmula para parametrizar todos os pontos racionais na hipérbole $x^2 - 3y^2 = 1$. Descreva todas as soluções inteiras da equação diofantina $a^2 - 3b^2 = c^2$.

1.7 Mostre que um número n é congruente se, e somente se, existe um racional w tal que $w^2 - n$ e $w^2 + n$ são quadrados.

2. Fundamentos

2.1 Mostre que, se n é um número natural não-nulo, então existe um natural m tal que $n = s(m)$. Por que m é único?

2.2 Mostre, por indução, que a operação de soma em $\mathbb{N}$ definida pelas propriedades $m + 0 = m$ e $m + s(n) = s(m + n)$, para todos $m, n \in \mathbb{N}$, é única.

2.3 Denotando $1 = s(0)$, demonstre que $s(n) = n + 1$ para todo número natural n.

2.4 Mostre que, se m e n são números naturais tais que $m + n = 0$, então $m = n = 0$.

2.5 Demonstre que a relação $m \leqslant n$ é transitiva.

2.6 Descreva *todas* as quantias (em $\mathbb{N}$) que podem ser obtidas combinando-se notas de 4 reais e 5 reais. Por exemplo, 13 reais é uma tal quantia pois $13 = 4 + 4 + 5$.

2.7 Encontre o erro no seguinte argumento para mostrar que todos os gatinhos são da mesma cor. *Procedemos por indução no número de gatinhos. O caso base $n = 1$ vale trivialmente. Considere $n + 1$ gatinhos e suponha que, em todo subconjunto de n gatinhos, todos eles são da mesma cor. Separe um gatinho, digamos A, deste conjunto. Sobram n gatinhos que, por hipótese de indução são todos da mesma cor. Devolva o gatinho A ao conjunto original e separe um outro gatinho, digamos B. Novamente, sobram n gatinhos, que devem ter todos a mesma cor. Logo, o gatinho A tem a mesma cor que todos os outros gatinhos diferentes de B. Mas também o gatinho B tem a mesma cor que todos os outros gatinhos diferentes de A. Assim, todos os gatinhos são da mesma cor.*

2.8 Mostre que existe uma única função

$$\mathbb{N} \to \mathbb{N}, \qquad n \mapsto n!$$

tal que $0! = 1$ e $(n + 1)! = n! \cdot (n + 1)$. Mostre que o número de maneiras de enfileirar n objetos distintos é $n!$.

2.9 Dados $m, n, p \in \mathbb{N}$, mostre que, se $m \leqslant n$, então $m \cdot p \leqslant n \cdot p$.

2.10 Verifique que a relação de paridade $\sim$ em $\mathbb{N}$ (isto é, $n \sim m$ se n e m têm a mesma paridade) é uma relação de equivalência.

2.11 Seja A um conjunto com uma relação de equivalência $\sim$. Mostre que:

- Se $a \in A$ e $b \in \overline{a}$, então $\overline{b} = \overline{a}$.
- Se $a, b \in A$ são tais que a interseção $\overline{a} \cap \overline{b}$ não é vazia, então $\overline{a} = \overline{b}$.
- $A = \bigcup_{a \in A} \overline{a}$.

2.12 Com as definições do curso, mostre que o produto de dois inteiros positivos é positivo, o produto de um positivo com um negativo é negativo e o produto de dois inteiros negativos é positivo.

2.13 Explique como estender a ordem $\leqslant$ em $\mathbb{N}$ para uma ordem em $\mathbb{Z}$, de maneira que $\{n \in \mathbb{Z} : n \geqslant 0\}$ seja o conjunto dos números positivos e $\{n \in \mathbb{Z} : n \leqslant 0\}$ o conjunto dos números negativos.

3. Divisibilidade

3.1 Encontre todos os inteiros cujos quociente e resto são iguais na divisão por 6 (exemplo: $14 = 2 \cdot 6 + 2$). Generalize para qualquer inteiro $b \geqslant 1$ no lugar de 6.

3.2 Mostre que um inteiro quadrado ímpar deixa resto 1 na divisão por 4.

3.3 Encontre um inteiro positivo que deixa resto 4 na divisão por 5 e resto 7 na divisão por 13.

3.4 Demonstre a unicidade da representação de um inteiro $a = (r_n r_{n-1} \cdots r_0)_b$ em uma base $b \geqslant 2$ qualquer.

3.5 Escreva 1472 em base 5 e base 16. Para a base 16, dita *hexadecimal*, considere os símbolos $A = 10$, $B = 11$, ..., $F = 15$.

3.6 Determine os inteiros positivos cuja representação em base 3 só contém o número 2, isto é, os inteiros da forma $(2)_3$, $(22)_3$, $(222)_3$, etc.

3.7 Mostre que o produto de três inteiros consecutivos quaisquer é divisível por 6, isto é, $6 \mid n(n+1)(n+2)$ para qualquer $n \in \mathbb{Z}$.

3.8 Mostre que a diferença entre dois quadrados ímpares é divisível por 8, isto é, $8 \mid m^2 - n^2$ para quaisquer $m, n \in \mathbb{Z}$ ímpares.

3.9 Encontre todos os inteiros positivos n tais que $2n^2 + 1$ divide $n^3 + 9n - 17$.

3.10 Mostre que, se n divide $a - b$, então n divide $a^k - b^k$ para todo k natural.

3.11 Sejam a e b inteiros. Mostre que $d = (a, b)$ se, e somente se, existem inteiros coprimos a_1 e b_1 tais que $a = da_1$ e $b = db_1$.

3.12 Mostre que dois termos consecutivos da sequência de Fibonacci são coprimos.

3.13 Calcule o maior divisor comum de 12345 e 67890.

3.14 Encontre todos os pares de inteiros a e b tais que $(a, b) = 18$ e $[a, b] = 720$.

3.15 Mostre que $7k + 5$ e $4k + 3$ são coprimos para qualquer inteiro k.

3.16 Calcule a matriz $A_n \in M_{2\times 2}(\mathbb{Z})$ tal que

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = A_n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Quantas etapas o algoritmo de Euclides necessita para calcular o maior divisor comum de F_{n+2} e F_{n+1}?

3.17 Encontre inteiros x e y tais que $240x + 66y = 6$.

4. Equações diofantinas lineares

4.1 Determine se a equação admite solução com x e y inteiros e, caso positivo, dê uma fórmula para a solução geral:

(a) $144x + 34y = 20$

(b) $199x - 29y = 8$

4.2 Sejam a, b, c inteiros positivos. Suponha que a e b sejam coprimos e sejam x_0 e y_0 inteiros tais que $ax_0 + by_0 = c$. Mostre que o número de soluções inteiras *positivas* de $ax + by = c$ é o número de inteiros k tais que

$$-\frac{x_0}{b} < k < \frac{y_0}{a}.$$

Note que, em geral, x_0/b e y_0/a são números racionais, não necessariamente inteiros.

4.3 Gastei R$ 1770 no mercado com muitos pacotes de café (gourmet) a R$ 31 e algumas barras de chocolate (Lindt) a R$ 21. Quantos pacotes de café e barras de chocolate eu comprei?

4.4 Quais são todos os valores possíveis de se obter combinando notas de 20 e 50 reais?

4.5 Sejam $a, b \geqslant 1$ inteiros coprimos. Mostre que, se $c \geqslant 0$ é um inteiro, então a equação $ax - by = c$ tem infinitas soluções inteiras não negativas $x, y \geqslant 0$.

4.6 Sejam $a_1, \ldots, a_n$ inteiros e denote por $(a_1, \ldots, a_n)$ o seu maior divisor comum. Mostre que $(a_1, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n)$.

4.7 Encontre uma fórmula com duas variáveis para parametrizar as soluções inteiras de $6x + 15y + 35z = 1$.

4.8 Sejam $a_1, \ldots, a_n, b$ inteiros. Mostre que a equação $a_1x_1 + \cdots + a_nx_n = b$ admite uma solução com $x_1, \ldots, x_n$ inteiros se, e somente se, $(a_1, \ldots, a_n)$ divide b.

4.9 Encontre uma solução do sistema

$$\begin{cases} 3x + 5y + 7z = 560 \\ 9x + 25y + 49z = 2920 \end{cases}$$

com x, y, z inteiros.

5. Primos

5.1 Mostre que, se $2^p - 1$ é primo, então p é primo. Vale a volta? Se não, dê um contra-exemplo.

5.2 Sejam $a_1, \ldots, a_n$ inteiros e p um número primo. Mostre que, se $p \mid a_1 \cdots a_n$, então $p \mid a_i$ para algum $i \in \{1, \ldots, n\}$.

5.3 Seja a um natural e $a = \prod_p p^{e_p}$ a sua fatoração em primos. Mostre que a é uma potência n-ésima (isto é, existe um natural b tal que $a = b^n$) se, e somente se, $n \mid e_p$ para todo primo p.

5.4 Mostre que, se a e b são naturais coprimos e ab é uma potência n-ésima, então a e b são potências n-ésimas.

5.5 Revisite a demonstração da parametrização das ternas pitagóricas da primeira aula.

5.6 Encontre todos os primos p tais que $11p + 1$ é um quadrado.

5.7 Seja $n \geqslant 1$ um inteiro. Mostre que a equação diofantina $x^2 - y^2 = n$ tem solução inteira $x, y \geqslant 0$ se, e somente se, n é ímpar ou divisível por 4. Quando a solução é única?

5.8 Calcule a fatoração em primos de 25!

5.9 Determine as maiores potências de 9 e de 14 que dividem 1000!.

5.10 Mostre que não existe um polinômio não-constante com coeficientes inteiros $f(x)$ tal que $f(n)$ é primo para todo $n \in \mathbb{N}$. [Dica: se $p = f(0)$, considere $f(p)$.]

5.11 Estime quantos passos são necessários para testar a primalidade de um número com 20 dígitos, usando o algoritmo simples em que testamos a divisibilidade por todos os primos até a raiz quadrada.

6. Racionais e irracionais

6.1 Verifique que a soma

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

e a multiplicação

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

estão bem definidas (isto é, não dependem da escolha dos representantes) e que $\mathbb{Q}$ é um corpo com as operações acima.

6.2 Seja n um número natural. Mostre que $\sqrt{n}$ é racional se, e somente se, n é um quadrado.

6.3 Encontre uma fórmula fechada para a *sequência de Lucas*: $L_0 = 2$, $L_1 = 1$, $L_{n+2} = L_{n+1} + L_n$.

7. Congruências

7.1 Verifique que a e b deixam o mesmo resto na divisão por m se, e somente se, m divide $a - b$.

7.2 Calcule o resto da divisão de 2^{36} por 11.

7.3 Mostre que $2^{70} + 3^{70}$ é um múltiplo de 13.

7.4 Mostre que, se m e n são coprimos, então as congruências $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$ valem simultaneamente se, e somente se, $a \equiv b \pmod{mn}$.

7.5 Mostre que o produto de quatro inteiros consecutivos é divisível por 24.

7.6 Generalize o exercício acima para o produto de n inteiros consecutivos.

7.7 Calcule os últimos três dígitos na expansão decimal de 3^{2024}.

7.8 Construa exemplos de soma e multiplicação para ilustrar que a volta da "prova dos nove" não vale.

7.9 Existe um múltiplo de 9 cuja expansão decimal é da forma $12121\cdots21$?

7.10 Mostre que um natural é divisível por 4, 20, 25, 50 ou 100 se, e somente se, os seus dois últimos dígitos na expansão decimal o são.

7.11 Demonstre o critério de divisibilidade por 11: $a = (r_k \cdots r_1 r_0)_{10}$ é divisível por 11 se, e somente se, $(-1)^k r_k + \cdots - r_1 + r_0$ é divisível por 11.

7.12 Invente um critério de divisibilidade por 13.

8. O anel de inteiros módulo m

8.1 Mostre que, se m é ímpar, então o conjunto

$$\left\{-\frac{m-1}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{m-1}{2}\right\}$$

é um sistema completo de resíduos módulo m. Por exemplo, para $m = 5$, temos $\mathbb{Z}/5\mathbb{Z} = \{-\overline{2}, -\overline{1}, \overline{0}, \overline{1}, \overline{2}\}$.

8.2 Descreva as tabelas de soma e produto em $\mathbb{Z}/6\mathbb{Z}$.

8.3 Mostre que, se S é um sistema completo de resíduos módulo m, então o subconjunto $R = \{a \in S : (a, m) = 1\}$ é um sistema reduzido de resíduos módulo m.

8.4 Encontre um inverso multiplicativo de $\overline{57}$ em $\mathbb{Z}/101\mathbb{Z}$.

8.5 Mostre que, se $\{a_1, \ldots, a_m\}$ é um sistema completo de resíduos módulo m, u é um inteiro coprimo com m, e b é um inteiro qualquer, então $\{ua_1 + b, \ldots, ua_m + b\}$ também é um sistema completo de resíduos módulo m. Por exemplo, para $m = 4$, $u = 3$ e $b = 1$, $\{0, 1, 2, 3\}$ e $\{1, 4, 7, 10\}$ são sistemas completos de resíduos módulo 4.

8.6 Mostre que vale a volta do teorema de Wilson. Mais precisamente, mostre que, se $m > 4$ é composto, então $(m-1)! \equiv 0 \pmod{m}$. (O que acontece para $m = 4$?)

8.7 Calcule 65! módulo 67.

8.8 Encontre todos os naturais m tais que $\varphi(m) = 6$.

8.9 Use a função φ para mostrar que existem infinitos primos. Ideia: mostrar que, se $p_1, \ldots, p_k$ são todos os primos, então $\varphi(p_1 \cdots p_k) = 1$.

9. Teorema chinês dos restos

9.1 Mostre, usando o teorema fundamental da aritmética, que, se $m_1, \ldots, m_r$ são dois a dois coprimos e $m_i \mid a$ para todo i, então $m_1 \cdots m_r \mid a$.

9.2 Descreva explicitamente a bijeção

$$(\mathbb{Z}/15\mathbb{Z})^\times \to (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$$

e verifique que ela é compatível com o produto.

9.3 Resolva o sistema de congruências

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 0 \pmod{10} \\ x \equiv 3 \pmod{7} \end{cases}$$

9.4 Resolva o sistema de congruências

$$\begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 1 \pmod{11} \end{cases}$$

10. Teoremas de Fermat e Euler

10.1 Calcule $\text{ord}_m(a)$ para todo a coprimo com m nos casos $m = 7$ e $m = 10$.

10.2 Um número composto m é dito *pseudoprimo* em base a se $a^{m-1} \equiv 1 \pmod{m}$. Verifique que 341 é pseudoprimo em base 2.

10.3 Mostre que, se p é primo ímpar e q é um fator primo do número de Mersenne $2^p - 1$, então $q \equiv 1 \pmod{2p}$. Por exemplo, 23 é um fator primo de $2^{11} - 1$ e $23 \equiv 1 \pmod{22}$.

10.4 Mostre que $11^{84} - 5^{84}$ é divisível por 7.

10.5 Mostre que -1 é um quadrado módulo p se, e somente se, $p = 2$ ou p é da forma $4n + 1$. [Dica: use o teorema de Wilson para a volta.]

10.6 Mostre que, se g é uma raiz primitiva módulo p, então, para qualquer divisor positivo d de $p - 1$, $\text{ord}_p(g^{\frac{p-1}{d}}) = d$.

10.7 Encontre uma raiz primitiva módulo 17.

10.8 Mostre que, se $\text{ord}_m(a_1) = n_1$ e $\text{ord}_m(a_2) = n_2$ com n_1 e n_2 coprimos, então $\text{ord}_m(a_1 a_2) = n_1 n_2$.

10.9 Mostre que, se p é um primo tal que $p \equiv 1 \pmod{4}$ e g é uma raiz primitiva módulo p, então $-g$ também é uma raiz primitiva módulo p. O que acontece no caso $p \equiv 3 \pmod{4}$?

10.10 Mostre que, se $\{u_1, u_2, \ldots, u_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m e a é um inteiro coprimo com m, então $\{au_1, au_2, \ldots, au_{\varphi(m)}\}$ também é um sistema reduzido de resíduos módulo m.

10.11 Mostre que, para todo inteiro a, temos $\overline{a}^{10} \in \{-\overline{1}, \overline{0}, \overline{1}\}$ no anel $\mathbb{Z}/25\mathbb{Z}$.

10.12 Mostre que existem infinitos inteiros que não são da forma $x_1^6 + x_2^6 + \cdots + x_8^6$. [Dica: olhe módulo 27.]

10.13 Mostre que $a^{12} \equiv 1 \pmod{72}$ para todo a coprimo com 72.

11. Criptografia RSA

11.1 Sejam p, q primos distintos e $n = pq$. Verifique que a condição $(e, p - 1) = 1$ e $(e, q - 1) = 1$ é equivalente a $(e, \varphi(n)) = 1$.

11.2 Seja $n = pq$, com p, q primos distintos, e d, e inteiros tais que $de \equiv 1 \pmod{\varphi(n)}$. Mostre que, se M é um inteiro tal que $p \mid M$ ou $q \mid M$, então $M^{de} \equiv M \pmod{n}$. [Dica: mostre que $M^{de} \equiv M \pmod{p}$ e $M^{de} \equiv M \pmod{q}$ separadamente.]

11.3 A seguinte mensagem foi encriptada usando a chave RSA $(n, e) = (2881, 5)$:

$$1972 \quad 430 \quad 2430 \quad 2773$$

Desencripte a mensagem.

11.4 Sabendo que $n = 10088821$ é um produto de dois primos distintos e $\varphi(n) = 10082272$, fatore n.

11.5 Fatore 6077 usando o método de Fermat.

11.6 Seja x o menor inteiro maior ou igual a $\sqrt{n}$. Mostre que o algoritmo de fatoração de Fermat sempre para em algum $j \leqslant \frac{n+1}{2} - x$ e que n é composto se, e somente se, $j < \frac{n+1}{2} - x$.

11.7 Verifique que um pseudoprimo forte na base a é um pseudoprimo (de Fermat) na base a.

11.8 Mostre que, se p é um primo ímpar, $p \nmid a$ e $p - 1 = 2^s t$, com t ímpar, então $a^t \equiv 1 \pmod{p}$ ou $a^{2^i t} \equiv -1 \pmod{p}$ para algum $i \in \{0, \ldots, s-1\}$.

11.9 Mostre que 561 é composto usando o teste de Miller–Rabin em base 2.

Para fazer as contas. Use o SageCell: `https://sagecell.sagemath.org/`

- Para fatorar um número, como 2024, digite: `factor(2024)` e clique em Evaluate. Saída: `2^3*11*23`.
- Para calcular um inteiro módulo outro inteiro, como 2024^{347} módulo 1000, digite: `2024^347%1000` e clique em Evaluate. Saída: `424`.

Tabela para converter palavras em números:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

12. Resíduos quadráticos

12.1 Resolva a congruência quadrática $4x^2 + x + 4 \equiv 0 \pmod{11}$.

12.2 Seja p um primo ímpar. Mostre que, se g é uma raiz primitiva módulo p, então g^n é resíduo quadrático módulo p se, e somente se, n é par.

12.3 Verifique se 3 ou 6 são resíduos quadráticos módulo 101.

12.4 Determine se a congruência $9x^2 - 30x + 26 \equiv 0 \pmod{103}$ tem solução.

12.5 Verifique que

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{se } p \equiv \pm 1 \pmod 8 \\ -1, & \text{se } p \equiv \pm 3 \pmod 8 \end{cases}$$

12.6 Calcule $\left(\frac{249}{257}\right)$.

12.7 Mostre que existem infinitos primos da forma $4n + 1$ usando $\left(\frac{-1}{p}\right)$. [Dica: suponha que $p_1, \ldots, p_k$ são todos os primos da forma $4n + 1$ e considere $N = (2p_1 \cdots p_k)^2 + 1$.]

12.8 Calcule os símbolos de Legendre $\left(\frac{44}{103}\right)$ e $\left(\frac{-60}{1019}\right)$.

12.9 Determine se 251 é resíduo quadrático módulo 779. [Note: $779 = 19{\cdot}41$ não é primo!]

13. Somas de quadrados

13.1 Mostre que, se inteiros m e n se escrevem como soma de dois quadrados, então o produto $m \cdot n$ também se escreve como soma de dois quadrados.

13.2 Mostre que um inteiro m se escreve como soma de dois quadrados se, e somente se,

$$m = 2^e d^2 p_1 \cdots p_k$$

onde $e \geqslant 0$ e d são inteiros quaisquer e p_i são primos da forma $4n + 1$.

Aula de exercícios (30/10)

Exercícios resolvidos na aula de exercícios conduzida pelo PED Nelson Serrano em 30/10.

E.1 Um número da forma $2^{2^n}+1$ sendo n um inteiro não negativo é dito um *número de Fermat*.

(a) Seja p um primo tal que $p \mid 2^{2^n}+1$. Mostre que existe um inteiro c tal que $p = 2^{n+1}c+1$.

(b) Mostre que $(F_n, F_m) = 1$ se $m \neq n$, onde $F_k = 2^{2^k}+1$.

(c) Conclua que há infinitos números primos.

E.2 Seja p um primo e g uma raiz primitiva módulo p.

(a) Seja q um primo. Mostre que g^q é uma raiz primitiva módulo p se, e somente se, $p \not\equiv 1 \pmod{q}$.

(b) Exiba um contra-exemplo para q composto.

(c) Toda raiz primitiva módulo p é da forma g^q?

E.3 Sejam a e $m \geqslant 1$ números inteiros. Dizemos que a é uma *raiz primitiva módulo* m se $(a, m) = 1$ e $\mathrm{ord}_m(a) = \varphi(m)$. Encontre as raízes primitivas módulo m com m sendo:

(a) 4

(b) 8

(c) 9

(d) 15.

E.4 Sejam a e $m \geqslant 1$ inteiros coprimos. Mostre que:

(a) se b é um inverso de a módulo m, então $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$;

(b) se a é uma raiz primitiva módulo m, então b também é;

(c) se $\mathrm{ord}_m(a) = st$, então $\mathrm{ord}_m(a^t) = s$.

E.5 Sejam p e q primos distintos. Dado um inteiro a tal que $a^p \equiv a \pmod{q}$ e $a^q \equiv a \pmod{p}$, mostre que $a^{pq} \equiv a \pmod{pq}$.

E.6 Sejam n um inteiro positivo e p um primo. Dizemos que um número da forma p^n é *legal* se p^n divide $7^{p^n}+1$. Determine a soma de todos os números legais.

Provas

A seguir estão os enunciados das duas provas do curso, cada questão seguida do seu gabarito.

Prova 1 (02/10/2024)

Questão 1 (2 pontos). Os itens abaixo são independentes.

(a) Mostre que a diferença de dois quadrados ímpares é divisível por 8.

(b) Mostre que $21n + 4$ e $14n + 3$ são coprimos para qualquer natural n.

Solução. (a) Dados dois ímpares $2m + 1$ e $2n + 1$, temos

$$\begin{aligned}(2m+1)^2 - (2n+1)^2 &= 4m^2 + 4m + 1 - (4n^2 + 4n + 1) \\ &= 4\big(m(m+1) - n(n+1)\big) \\ &= 8\left(\frac{m(m+1)}{2} - \frac{n(n+1)}{2}\right),\end{aligned}$$

pois $m(m+1)$ e $n(n+1)$ são pares (produtos de dois inteiros consecutivos), de modo que $\frac{m(m+1)}{2}$ e $\frac{n(n+1)}{2}$ são inteiros.

(b) Pelo lema de Euclides,

$$\begin{aligned}(21n+4,\, 14n+3) &= \big(14n+3,\, (21n+4) - (14n+3)\big) \\ &= (14n+3,\, 7n+1) \\ &= \big(7n+1,\, (14n+3) - 2\cdot(7n+1)\big) \\ &= (7n+1,\, 1) = 1.\end{aligned}$$

□

Questão 2 (3 pontos). Um *número de Mersenne* é um número da forma $2^n - 1$, para algum natural n. Por exemplo, $31 = 2^5 - 1$. O item (c) abaixo não depende dos itens (a) e (b).

(a) Mostre que, se um número de Mersenne $2^n - 1$ é primo, então o expoente n é primo.

(b) Fatore 2047 em primos e conclua que a volta do item acima não vale.

(c) Calcule a expansão binária de um número de Mersenne qualquer (isto é, escreva em base 2).

Solução. (a) Por contrapositiva: se $n = a \cdot b$ com $a, b > 1$, então

$$2^n - 1 = 2^{a\cdot b} - 1 = (2^a)^b - 1 = \underbrace{(2^a - 1)}_{>1}\ \underbrace{((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1)}_{>1},$$

logo $2^n - 1$ é composto.

(b) O expoente 11 é primo, mas

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

é composto.

(c) Temos

$$\begin{aligned} 2^n - 1 &= (2-1) \cdot (2^{n-1} + 2^{n-2} + \cdots + 1) \\ &= 1 \cdot 2^{n-1} + 1 \cdot 2^{n-2} + \cdots + 1 \cdot 2 + 1, \end{aligned}$$

isto é,

$$2^n - 1 = (\underbrace{11\cdots1}_{n \text{ dígitos}})_2. \qquad \square$$

Questão 3 (3 pontos). Resolva os itens abaixo em ordem:

(a) Calcule o maior divisor comum entre 152 e 57 usando o algoritmo de Euclides.

(b) Calcule uma fórmula para a solução geral com x, y inteiros da equação diofantina linear $152x + 57y = 1900$.

(c) Usando a fórmula acima, determine quantas soluções com x, y *naturais* existem. Dentre essas soluções, qual é o menor y possível?

Solução. (a) Pelo algoritmo de Euclides,

$$\begin{aligned} 152 &= 2 \cdot 57 + 38 & (152, 57) &= (57, 38) \\ 57 &= 1 \cdot 38 + 19 & &= (38, 19) \\ 38 &= 2 \cdot \underline{19} + 0 & &= (19, 0) = 19. \end{aligned}$$

(b) *Solução particular:* das divisões acima,

$$19 = 57 - 38 = 57 - (152 - 2 \cdot 57) = -1 \cdot 152 + 3 \cdot 57.$$

Multiplicando por 100,

$$1900 = \underbrace{-100}_{x_0} \cdot 152 + \underbrace{300}_{y_0} \cdot 57.$$

Solução geral:

$$x = x_0 + \frac{57}{19}\,t = -100 + 3t, \qquad y = y_0 - \frac{152}{19}\,t = 300 - 8t, \qquad t \in \mathbb{Z}.$$

(c) Temos

$$x \geqslant 0 \iff -100 + 3t \geqslant 0 \iff t \geqslant \frac{100}{3} = 33 + \frac{1}{3},$$
$$y \geqslant 0 \iff 300 - 8t \geqslant 0 \iff t \leqslant \frac{300}{8} = 37 + \frac{1}{2}.$$

Como t é inteiro, existem 4 soluções com $x, y \geqslant 0$, correspondentes a $t = 34, 35, 36, 37$. A solução com o menor $y \geqslant 0$ é a de $t = 37$:

$$x = -100 + 3 \cdot 37 = 11, \qquad y = 300 - 8 \cdot 37 = 4. \qquad \square$$

Questão 4 (3 pontos). O objetivo deste exercício é demonstrar que existem infinitos primos da forma $4n + 3$, como 3, 7, 11, 19, etc.

(a) Mostre que um número ímpar ou é da forma $4n + 1$ ou é da forma $4n + 3$.

(b) Mostre que o produto de números da forma $4n + 1$ é também um número da forma $4n + 1$.

(c) Mostre que, se $p_1, \ldots, p_k$ são primos da forma $4n + 3$, então o natural

$$4p_1 \cdots p_k + 3$$

tem pelo menos um divisor primo da forma $4n + 3$. Conclua, de maneira similar à demonstração por contradição de Euclides, que existem infinitos primos da forma $4n + 3$.

Solução. (a) Dado $a \in \mathbb{Z}$, temos $a = 4q + r$ com $r = 0, 1, 2$ ou 3. Se a é ímpar, r não pode ser 0 ou 2; logo, $a = 4n + 1$ ou $a = 4n + 3$.

(b) Temos

$$(4m + 1) \cdot (4n + 1) = 16mn + 4m + 4n + 1 = 4(4mn + m + n) + 1.$$

(c) Como $4p_1 \cdots p_k + 3$ é ímpar, seus divisores primos são da forma $4n + 1$ ou $4n + 3$, pelo item (a). Pelo item (b), se todos os divisores primos de $4p_1 \cdots p_k + 3$ fossem da forma $4n + 1$, então $4p_1 \cdots p_k + 3$ também seria da forma $4n + 1$, o que contradiz a sua definição.

Suponha, por absurdo, que o conjunto dos primos da forma $4n + 3$ é finito e sejam $3, p_1, p_2, \ldots, p_k$ esses primos (note: $p_i \neq 3$). Pelo parágrafo anterior, $4p_1 \cdots p_k + 3$ tem um divisor primo p da forma $4n + 3$. Note que $p \neq 3$ (caso contrário, teríamos $3 \mid 4p_1 \cdots p_k$, logo $p_i = 3$ para algum i) e $p \neq p_i$ para todo i (caso contrário, teríamos $p_i \mid 3$, logo $p_i = 3$). Portanto, $p \notin \{3, p_1, \ldots, p_k\}$, o que é absurdo. $\square$

Prova 2 (27/11/2024)

Questão 1 (3 pontos). Seja φ a função de Euler.

(a) Relembre a definição de φ.

(b) Calcule $\varphi(1000)$.

(c) Calcule os últimos três dígitos de 7^{803}.

Solução. (a) $\varphi(n)$ é o número de inteiros entre 1 e n coprimos com n (ou, equivalentemente, $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$).

(b) Como $1000 = 10^3 = 2^3 \cdot 5^3$,

$$\varphi(1000) = \varphi(2^3) \cdot \varphi(5^3) = (2-1) \cdot 2^2 \cdot (5-1) \cdot 5^2 = 400.$$

(c) Como $(7, 1000) = 1$, pelo teorema de Euler,

$$7^{\varphi(1000)} = 7^{400} \equiv 1 \pmod{1000}.$$

Logo,

$$7^{803} = (7^{400})^2 \cdot 7^3 \equiv 7^3 = 343 \pmod{1000}.$$

Os últimos três dígitos de 7^{803} são 343. □

Questão 2 (2 pontos).

(a) Enuncie o Teorema Chinês dos Restos.

(b) Determine todos os $x \in \mathbb{Z}$ tais que

$$\begin{cases} 2x \equiv -1 \pmod{9} \\ x \equiv 3 \pmod{10}. \end{cases}$$

Solução. (a) Se $m_1, \ldots, m_r$ são naturais dois a dois coprimos e $b_1, \ldots, b_r$ são inteiros, então o sistema

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv b_r \pmod{m_r} \end{cases}$$

tem uma única solução módulo $m_1 \cdots m_r$.

(b) Como $2 \cdot 5 \equiv 1 \pmod{9}$ e $-5 \equiv 4 \pmod{9}$,

$$\begin{cases} 2x \equiv -1 \pmod{9} \\ x \equiv 3 \pmod{10} \end{cases} \iff \begin{cases} x \equiv 4 \pmod{9} \\ x \equiv 3 \pmod{10}. \end{cases}$$

Note que $x = 13$ é uma solução. Pelo Teorema Chinês dos Restos, todas as outras soluções são da forma $13 + 90k$, com $k \in \mathbb{Z}$. □

Questão 3 (3 pontos).

(a) Enuncie a Lei de Reciprocidade Quadrática.

(b) Calcule o símbolo de Legendre $\left(\frac{-19}{53}\right)$.

(c) Determine se a congruência quadrática possui solução com $x \in \mathbb{Z}$:

$$x^2 - 2x - 33 \equiv 0 \pmod{53}.$$

Solução. (a) Se p e q são primos ímpares distintos, então

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

(b) Temos

$$\begin{aligned}
\left(\frac{-19}{53}\right) &= \left(\frac{-1}{53}\right)\cdot\left(\frac{19}{53}\right) \\
&= (-1)^{\frac{53-1}{2}} \cdot (-1)^{\frac{19-1}{2}\cdot\frac{53-1}{2}} \left(\frac{53}{19}\right) \\
&= \left(\frac{53}{19}\right) = \left(\frac{15}{19}\right) = \left(\frac{3}{19}\right)\cdot\left(\frac{5}{19}\right) \\
&= (-1)^{\frac{3-1}{2}\cdot\frac{19-1}{2}} \left(\frac{19}{3}\right)\cdot(-1)^{\frac{5-1}{2}\cdot\frac{19-1}{2}} \left(\frac{19}{5}\right) \\
&= -\left(\frac{1}{3}\right)\cdot\left(\frac{4}{5}\right) = -1.
\end{aligned}$$

(c) Completando o quadrado,

$$\begin{aligned}
x^2 - 2x - 33 = (x-1)^2 - 34 &\equiv 0 \pmod{53} \\
\iff (x-1)^2 &\equiv 34 \equiv -19 \pmod{53}.
\end{aligned}$$

Como -19 *não* é resíduo quadrático módulo 53, pelo item (b), a congruência não possui solução. □

Questão 4 (4 pontos). Um *número de Fermat* é um número da forma $2^{2^n} + 1$, para algum natural n. Por exemplo, $17 = 2^{2^2} + 1$.

(a) Mostre que, se p é um primo tal que $p \mid 2^{2^n} + 1$, então $\mathrm{ord}_p(2) = 2^{n+1}$.

(b) Conclua que existe a tal que $p = 2^{n+1}a + 1$.

(c) Mostre que, se $n \geqslant 2$, então 2 é resíduo quadrático módulo p.

(d) Use o critério de Euler para concluir que, se $n \geqslant 2$, então existe b tal que $p = 2^{n+2}b + 1$.

Solução. (a) Temos

$$2^{2^n} \equiv -1 \pmod{p} \implies 2^{2^{n+1}} \equiv 1 \pmod{p}.$$

Logo, $\mathrm{ord}_p(2) \mid 2^{n+1}$. Em particular, $\mathrm{ord}_p(2)$ é uma potência de 2. Como $2^{2^n} \not\equiv 1 \pmod{p}$, então $\mathrm{ord}_p(2) = 2^{n+1}$.

(b) Pelo teorema de Fermat, $2^{p-1} \equiv 1 \pmod{p}$. Logo, $2^{n+1} = \mathrm{ord}_p(2) \mid p-1$. Isto é, existe a tal que $p - 1 = 2^{n+1}a$.

(c) Se $n \geqslant 2$, então $n + 1 \geqslant 3$ e

$$p = 2^{n+1}a + 1 \implies p \equiv 1 \pmod{8}.$$

Logo, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$.

(d) Pelo critério de Euler,

$$1 = \left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod{p}.$$

Como $2^{n+1} = \mathrm{ord}_p(2) \mid \frac{p-1}{2} = 2^n a$, temos $2 \mid a$, isto é, $a = 2b$ para algum b. Logo, $p = 2^{n+1}a + 1 = 2^{n+2}b + 1$. □

Bônus. Use os resultados da Questão 4 para decidir se o número de Fermat $2^{2^5} + 1 = 4294967297$ é primo ou composto.

Solução. Pela Questão 4 (com $n = 5$), basta procurar divisores primos da forma $p = 2^7 b + 1 = 128b + 1$.

- $b = 1$: $129 = 3 \cdot 43$ não é primo.
- $b = 2$: $128 \cdot 2 + 1 = 257$ é primo, mas

$$2^8 = 256 \equiv -1 \pmod{257} \implies 2^{32} \equiv 1 \not\equiv -1 \pmod{257}.$$

- $b = 3$: $128 \cdot 3 + 1 = 385 = 5 \cdot 7 \cdot 11$ não é primo.
- $b = 4$: $128 \cdot 4 + 1 = 513 = 3^3 \cdot 19$ não é primo.
- $b = 5$: $128 \cdot 5 + 1 = 641$ é primo e $2^{32} \equiv \cdots \equiv -1 \pmod{641}$.

Logo, $641 \mid 2^{32} + 1$ e $2^{32} + 1$ é composto. □

Anexo

O trabalho do curso

Além das duas provas, o curso teve um trabalho para entregar. Os estudantes tinham duas opções: fazer um *plano de aula* para o ensino médio ou fundamental, ou escrever um *artigo científico expositório*. Em ambos os casos, o trabalho deveria estar relacionado ao tema do curso (teoria dos números). Para ilustrar o formato, foram disponibilizados como exemplos um plano de aula feito em uma edição anterior da disciplina e um artigo expositório de um autor conhecido. Seguem as especificações.

Plano de aula

Um plano de aula para o ensino médio ou fundamental, no qual algum conteúdo relacionado, mas não necessariamente contido, à ementa do curso MA553 é apresentado para estudantes de nível médio ou fundamental, de diferentes formas: desafios, jogos, estações rotativas, sala de aula invertida etc.

Note: não queremos "dar aula" de nível superior para o nível médio ou fundamental, mas sim buscar soluções criativas de apresentação deste conteúdo para o nível de ensino adequado. Contudo, as bases matemáticas avançadas (como definições e teoremas) devem ser propriamente explicadas na parte "para o professor" do plano de aula.

Boas referências para o plano de aula podem ser os livros e as apostilas de formação de professores da SBM, o portal da OBMEP, o livro *Círculos Matemáticos* (disponível na biblioteca do LEM), dissertações e teses, artigos da *Revista do Professor de Matemática* (RPM), livros de história da matemática etc.

Um bom plano de aula contém:

- série/nível;
- quantidade de aulas;
- objetivos;
- metodologia;
- materiais;
- atividades;
- bibliografia;

- anexos (caso necessário). No caso de atividades imprimíveis, sempre colocá-las como anexo, e não como link.

Redação (artigo)

Um artigo científico expositório (em inglês ou português) para alunos de graduação na área de exatas, no qual algum conteúdo relacionado, mas não contido, na ementa do curso MA553 é discutido. O artigo pode apresentar a solução de um ou mais problemas difíceis, uma aplicação diferente dos conteúdos vistos em aula (exemplo: criptografia), uma discussão histórica aprofundada acerca de algum tópico do curso, uma maneira diferente de formular a teoria, um tópico novo que não está coberto na ementa etc. É importante ressaltar que este artigo deve ser acessível a qualquer aluno de graduação na área de exatas; então, caso precise utilizar algum conceito sofisticado, explique os pré-requisitos.

Boas referências para o artigo podem ser a *Revista do Professor de Matemática*, a revista *Eureka!* da OBM, a *Acta Legalicus* (`https://www.cemeai.icmc.usp.br/actalegalicus/`) e a *The American Mathematical Monthly* (em inglês). Também é possível procurar assuntos interessantes em qualquer livro de teoria dos números na biblioteca.

Um artigo deve necessariamente conter:

- título;
- autor;
- resumo;
- introdução;
- referências.

Critério de avaliação

Em ambos os tipos de trabalho, são avaliados três critérios:

1) adequação ao que foi pedido;
2) qualidade da exposição;
3) profundidade do conteúdo.

Importante: não basta copiar algo; é preciso dar a sua cara ao trabalho: desenvolver exemplos, explicar do seu jeito, desenhar figuras ou diagramas etc.