Teoria de Números

POTI/TOPMAT UFPR

Nível 3

3ª edição

2024

UNIVERSIDADE FEDERAL DO PARANÁ
DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE FORMAÇÃO EM
MATEMÁTICA OLÍMPICA

Coordenador Geral:	Prof. Dr. José Carlos Corrêa Eidam
Coordenadores:	Fernanda de Oliveira de Jesus Leonardo Knelsen Mahmut Telles Cansiz
Site:	http://poti.ufpr.br/
E-mail:	poti@ufpr.br
Capa:	Luciana Laroca
Impressão:	Imprensa UFPR

Curitiba, janeiro de 2024.

Apresentação

Prezado Estudante,

É com grande satisfação que apresentamos a terceira edição do material de treinamento do POTI/TOPMAT - Programa de Formação em Matemática Olímpica da Universidade Federal do Paraná (UFPR).

O POTI/TOPMAT, que conta com o apoio do Instituto Nacional de Matemática Pura e Aplicada (IMPA), do Departamento de Matemática da UFPR (DMAT/UFPR) e da Pró-Reitoria de Graduação da UFPR (PROGRAD/UFPR), envolvendo docentes do DMAT e alunos de graduação e pós-graduação da UFPR, é um projeto que visa fornecer embasamento teórico e prático para os estudantes de Ensino Fundamental e Médio que desejam se aprofundar nos interessantes temas abordados nas olimpíadas matemáticas nacionais. Este projeto constitui-se em uma experiência única para todos os envolvidos e também oportuniza a aproximação e interlocução da Universidade com a Educação Básica.

A iniciativa do projeto POTI, capitaneada pelo IMPA em todo o território nacional, teve seu início na UFPR em 2016 e, desde então, nosso polo, sediado no campus Centro Politécnico da UFPR, em Curitiba, tem crescido bastante e impactado positivamente todos os envolvidos. Em particular, envolve de forma intensa os estudantes de graduação da UFPR, especialmente do Curso de Matemática, que atuam como professores e monitores das disciplinas do programa.

O programa TOPMAT iniciou em 2019, com o intuito de pro-

duzir material de formação adequado para treinamento em matemática olímpica. A princípio, o material inicial foi produzido para formação de professores e posteriormente passamos ao trabalho de redação do material de formação para os alunos. Este material foi sendo aperfeiçoado ao longo do tempo, a partir da experiência didática dos estudantes, e o resultado é o que temos hoje em mãos. Em resumo, o presente material foi desenvolvido pelos professores atuantes no programa e servirá como base para todas as atividades desenvolvidas durante o treinamento.

Por fim, gostaria de agradecer de forma expressiva aos estudantes de graduação da UFPR envolvidos neste projeto pelo afinco e esmero na realização deste árduo trabalho. Sem a participação de cada um deles, este projeto não seria possível.

Bons estudos!

Prof. Dr. José Carlos Eidam
Coordenador do POTI/TOPMAT - 2024
Departamento de Matemática - UFPR
Janeiro de 2024

Sumário

Introdução

Este livro apresenta um modo especial de se fazer Matemática. O conteúdo é basicamente o mesmo que você vê na escola, mas em uma abordagem mais aprofundada e, por vezes, acompanhada de algum formalismo que provavelmente será uma novidade para você. No entanto, o principal propósito não é expor conteúdos, mas de conduzi-lo num treinamento em *Matemática Olímpica*.

Mas... Em que consiste essa tal Matemática?

Do ponto de vista do conteúdo, tudo o que você precisa para resolver problemas de olimpíadas de Matemática está disponível nos livros didáticos escolares ou, mais raramente, em livros mais avançados. Todavia, saber todos esses conteúdos, com suas fórmulas, teoremas e proposições, não garante de forma alguma o sucesso na resolução dos problemas. Mesmo os seus professores na escola e também nós, graduandos em Matemática e de outros cursos de Exatas, frequentemente ficamos travados diante de uma questão de olimpíada, sem que todo o nosso conhecimento matemático possa nos prestar qualquer auxílio. Ou seja, estar bem informado nunca é o suficiente por aqui.

De modo geral, para se preparar para o enfrentamento de problemas matemáticos, nada melhor que... *enfrentar problemas matemáticos!*

O que torna a matemática olímpica especial não é um conjunto de conhecimentos, mas o *modo* de lidar com eles, forçando o estudante a relacionar conteúdos entre si, mudar um ponto de vista que lhe era muito familiar e buscar estratégias de resolução. Problemas

olímpicos lhe arrancam daquele comodismo do tipo "eu já sei, já estudei isso". Aqui, você já sabe tudo o que precisa saber, mas não sairá do lugar se não se arriscar em caminhos de raciocínio não habituais. E essa descrição não está aqui para desestimulá-lo. Pelo contrário, queremos mostrar que problemas olímpicos são instigantes justamente porque são difíceis e inesperados. Afinal de contas, resolver problemas olímpicos é como um jogo – e você sabe como jogos podem ser desafiadores, não é mesmo?

É por conta desse espírito de Matemática Olímpica que optamos por incluir no material muitos problemas – retirados de diversas olimpíadas e livros ou elaborados por nós mesmos. Este é essencialmente um livro de *treinamento e enfrentamento de problemas matemáticos*, não de exposição de conteúdos. Os conteúdos (tanto aqueles que você já tem na escola quanto alguns novos que lhe apresentaremos) só serão introduzidos na medida em que forem necessários para resolver as questões. Nós o ajudaremos com exemplos, modelos de estratégias de resolução, dicas de organização do raciocínio, entre outras coisas. Porém, o mais importante é que você – por conta própria – faça muitos exercícios, mesmo aqueles que estão resolvidos. E lembre-se sempre do ditado: a prática leva à perfeição.

Equipe POTI/TOPMAT
Nível 3
2024

Aula 1

Divisibilidade e Algoritmo de Divisão

No conjunto dos números inteiros, a equação $bx = a$ nem sempre admite solução. Isso significa simplesmente que nem sempre a divisão é *exata*. Se existir uma solução nessas condições, recaímos no caso em que b divide a, ou, mais formalmente:

Definição 1.1. Divisibilidade:
Dados dois números inteiros a, b, dizemos que b divide a se existe c *inteiro* tal que $a = bc$. Neste caso, b é dito divisor de a, e denotaremos simplesmente $b|a$

A divisibilade apresenta algumas propriedades que merecem ser mencionadas, as quais enunciaremos agora:

Proposição 1.1. Sejam a, b, c, d números inteiros, e cada divisor um número diferente de zero. Então valem:

1. Limitação: Se $a|b$, então, ou $b = 0$ ou $|a| \leq |b|$;
2. Transitividade: Se $a|b$ e $b|c$, então $a|c$;
3. Se $a|b$ e $a|c$, então, para quaisquer $m, n \in \mathbb{Z}, a|(mb + nc)$.

Um importante resultado de divisibilidade que merece ser mencionado é apresentado no exemplo a seguir:

Exemplo 1.1. Para quaisquer x, y, vale que:

$x^n - y^n = (x-y)(x^{n-1}+x^{n-2}y+x^{n-3}y^2+\ldots+x^2y^{n-3}+xy^{n-2}+y^{n-1})$

Portanto, para quaisquer $x, y \in \mathbb{Z}$, se $x \neq y$, segue que $x-y|x^n-y^n$. Apresentamos a seguir dois casos particulares da igualdade acima

- Se n é impar, vale que:

  $$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1})$$

  De fato, basta tomar $x^n + y^n = x^n - (-y)^n$

- Se $n = 2k$ é par, vale que:

  $x^{2k} - y^{2k} = (x^2 - y^2)(x^{2k-2} + x^{2k-4}y^2 + \ldots + x^2y^{2k-4} + y^{2k-2})$

  Tomando ainda $x^2 - y^2 = (x-y)(x+y)$, podemos fazer mais uma decomposição no número acima:

  $x^{2k}-y^{2k} = (x-y)(x+y)(x^{2k-2}+x^{2k-4}y^2+\ldots+x^2y^{2k-4}+y^{2k-2})$

Nos casos em que não existe um inteiro satisfazendo tal condição, isto é, se b não divide a, ainda assim, em geral, podemos efetuar um processo de divisão com resto. Por exemplo, se $a = 123, b = 5$, fazemos simplesmente:

$$\begin{array}{r|l} 123 & 5 \\ \underline{-10} & 24 \\ 23 & \\ \underline{-20} & \\ 3 & \end{array}$$

Neste exemplo, temos que 5 "cabe"24 vezes em 123, deixando um resto 3 no processo de divisão.
Certamente, para aplicar tal processo de divisão, precisamos que $b \neq 0$. Com essa condição, para qualquer inteiro a conseguimos garantir sempre que a divisão com resto de a por b está bem definida. Tal resultado é conhecido como Algoritmo da Divisão, que enunciamos a seguir:

Teorema 1.1. Algoritmo da Divisão
Sejam a e b inteiros, com $b \neq 0$. Então existe um único par de inteiros não negativos (q,r) tal que:

$$a = bq + r, 0 \leq r < |b|$$

Neste par, o número q é chamado **quociente** e r o **resto** da divisão de a por b.

Apresentamos a seguir uma aplicação do algoritmo de divisão na resolução de problemas:

Exemplo 1.2. Seja a um inteiro. Mostre que se a é da forma $3k + 2, k \in \mathbb{Z}$ então a não é o quadrado de outro inteiro.

Solução:
Seja $b, q \in \mathbb{Z}$. Analisemos o quadrado de b com base no resto de b na divisão por 3:

- se $b = 3q$: $\quad b^2 = (3q)^2 = 3(3q^2) + 0$
- se $b = 3q + 1$: $\quad b^2 = (3q + 1)^2 = 3(3q^2) + 3(2q) + 1 = 3(3q^2 + 2q) + 1$
- se $b = 3q + 2$: $\quad b^2 = (3q + 2)^2 = 3(3q^2) + 3(4q) + 3 \cdot 1 + 1 = 3(3q^2 + 4q + 1) + 1$

Com isso concluímos que os únicos restos possíveis para o quadrado de um inteiro na divisão por 3 são 0 e 1. Ou seja, se a é da forma $3k + 2, k \in \mathbb{Z}$, então a não é o quadrado de outro inteiro. ■

Como o leitor pode observar, da maneira como definimos divisibilidade, temos que $b|a$ precisamente quando o resto do algoritmo da divisão de a por b é zero.

Para avaliar se um certo número inteiro diferente de zero divide outro inteiro, sempre podemos efetuar o processo de divisão e verificar se o resto é zero. Contudo, alguns números admitem estratégias alternativas, em geral mais econômicas, para avaliarmos se eles dividem algum número inteiro dado. Essas estratégias são chamadas de

Critérios de divisibilidade. Enunciaremos a seguir alguns critérios de divisibilidade pelos números de 2 a 11:

- **Critério de Divisibilidade por 2:** Um número é divisível por 2 se e somente se seu algarismo das unidades for par;
  E.g.: 1234 é divisível por 2, pois seu último dígito, 4, é par.

- **Critério de Divisibilidade por 3:** Um número é divisível por 3 se e somente se a soma de seus dígitos também for;
  E.g.: 543 é divisível por 3, pois $5+4+3=12$ é múltiplo de 3.

- **Critério de Divisibilidade por 4:** Um número é divisível por 4 se e somente se seus dois últimos algarismos, das dezenas e das unidades, formam um número divisível por 4;
  E.g.: 432116 é divisível por 4, pois seus dois últimos dígitos são 16, um múltiplo de 4.

- **Critério de Divisibilidade por 5:** Um número é divisível por 5 se seu algarismo das unidades for 0 ou 5;
  E.g. : 3115 é divisível por 5, pois seu dígito das unidades é 5

- **Critério de Divisibilidade por 6:** Um número é divisível por 6 se e somente se satisfaz simultaneamente os critérios para 2 e 3;
  E.g. : 3132 é múltiplo de 6, pois é par e $3+1+3+2=9$.

- **Critério de Divisibilidade por 7:** Um número é divisível por 7 se e somente se, ao apagarmos o último dígito e subtrairmos seu dobro do número resultante, obtivermos um número múltiplo de 7.
  E.g. : 434 é divisível por 7, pois $43-(4.2)=43-8=35$ é múltiplo de 7.

- **Critério de Divisibilidade por 8:** Um número é divisível por 8 se seus três últimos algarismos formam um número divisível por 8

- **Critério de Divisibilidade por 9:** Um número é divisível por 9 se e somente se a soma de seus algarismos é um número múltiplo de 9;
- **Critério de Divisibilidade por 10:** Um número é divisível por 10 se simplesmente seu último algarismo é nulo;
- **Critério de Divisibilidade por 11:** Um número é divisível por 11 se e somente se a diferença entra a soma dos algarismos de posição ímpar e a soma dos algarismos de posição par for múltipla de 11.

Problemas Propostos

Os problemas estão classificados por nível de dificuldade:

●	▲	♦	★
Fácil	Médio	Difícil	Desafio

1. ● Para todo inteiro a, prove que 4 não divide $(a^2 + 2)$.
2. ● Mostre que $3|7^n - 4^n$, para todo $n \geq 1$.
3. ● Prove que se a e b são ímpares, então $8|(a^2 - b^2)$.
4. ● Mostre que se $7|3a + 2b$ então $7|4a - 2b$.
5. ▲ Mostre que 9 divide $n \cdot 4^{n+1} - (n + 1) \cdot 4^n + 1$
6. ▲ Prove o critério de divisibilidade por 7.
7. ▲ Prove o critério de divisibilidade por 9.
8. ▲ Mostre que se $19|3x + 7y$ então $19|43x + 75y$.
9. ▲ Sejam $a = bq+r = (b+1)q'+r'$, com a, b positivos, $0 \leq r < b$, e $0 \leq r' < (b + 1)$. Provar que $q = q'$ se, e somente se, $r \geq q$
10. ▲ Prove que se $f(x)$ é um polinômio de coeficientes inteiros e a e b são inteiros quaisquer, então $a - b|f(a) - f(b)$.

11. ♦ Prove que nenhum inteiro da sequência $11, 111, 1111, \ldots$ é um quadrado perfeito.

12. ♦ Encontre todos os inteiros positivos n tais que $2n^2 + 1 | n^3 + 9n - 17$.

13. ♦ Seja $n > 1$ e k um inteiro positivo. Prove que $(n-1)^2 | (n^k - 1)$ se, e somente se, $(n-1)|k$.

14. ♦ (OBM 2011) Qual é o maior inteiro positivo n tal que $(2011!)!$ é divisível por $((n!)!)!$?

15. ♦ Defina uma função dos inteiros neles mesmos por $f(x) = \epsilon x^n + c$, com $\epsilon \in \{-1, 1\}$ e c um inteiro qualquer. Mostre que $f(x) - f(y) | x^m - y^m$ sempre que $n|m$.

16. ♦ (CONE SUL, Prova de Seleção, 2015) Para cada número natural n, denotamos $g(n)$ o maior divisor ímpar de n. Calcule a soma dos 2^{2015} termos:

$$g(1) + g(2) + g(3) + \ldots + g(2^{2015})$$

17. ♦ (OBM 2000) É possível encontrar duas potências de 2, distintas e com o mesmo número de algarismos, tais que uma possa ser obtida através de uma reordenação dos dígitos da outra?

18. ♦ (OBM 2005) Prove que a soma $1^k + 2^k + \ldots + n^k$, onde n é um inteiro positivo e k é ímpar, é divisível por $1 + 2 + \ldots + n$.

19. ♦ (IMO 2011) Seja f uma função do conjunto dos inteiros no conjunto dos inteiros positivos. Sumponha que, para quaisquer dois inteiros m e n, a diferença $f(m) - f(n)$ é divisível por $f(m-n)$. Prove que, para todos os inteiros m, n com $f(m) \leq f(n)$, o número $f(n)$ é divisível por $f(m)$.

20. ★ (IMO 2007) Sejam a e b inteiros positivos. Mostre que, se $4ab - 1$ divide $(4a^2 - 1)^2$, então $a = b$.

Aula 2

Máximo Divisor Comum, Mínimo Múltiplo Comum

Aqui, prosseguiremos com o estudo de divisibilidade a partir de outros conceitos elementares da teoria de números. Salvo menção em contrário, assumiremos nesta aula sempre a, b inteiros não simultaneamente nulos.

Máximo Divisor Comum

Primeiramente, dizemos que um inteiro d é um *divisor comum* de a e b se $c|a$ e $c|b$. Podemos recolher todos esses divisores comuns de a e b em um conjunto que denotaremos $D(a, b)$. Pelas propriedades de divisibilidade, sabemos que, se $a \neq 0, c|a$ implica que $|c| \leq |a|$, logo $D(a, b)$ é limitado. Ainda, para quaisquer a, b não simultaneamente nulos, temos que pelo menos 1 divide ambos, logo $1 \in D(a, b)$, e o conjunto dos divisores comuns é não vazio. Por conta dessas propriedades, faz sentido falar de um *maior elemento* do conjunto $D(a, b)$, o que motiva a seguinte definição:

Definição 2.1. Denominamos *máximo divisor comum* (mdc) de a e b o maior de seus divisores comuns. Assim:

$$mdc(a, b) = max D(a, b)$$

Diante deste conceito, uma dúvida natural é o modo de calculá-lo para um dado par de inteiros. O algoritmo da divisão apresentado anteriormente permite a elaboração de um método capaz de determinar o mdc de dois inteiros dados. Este método é denominado *Algoritmo de Euclides*

Primeiro, verifiquemos brevemente o seguinte resultado:

Lema 2.1. Sejam a, b inteiros, com $b \neq 0$, e q e r os respectivos quociente e resto da divisão de a por b. Então $mdc(a, b) = mdc(b, r)$.

Demonstração. A divisão de a por b resulta na expressão:

$$a = bq + r$$

Basta verificar que todo divisor comum de a e b divide r, e, reciprocamente, todo divisor comum de b e r divide a. Seja $m \in D(a, b)$. Então, pelas propriedades de divisibilidade, temos que $m|a, m|b$ implica $m|a - bq$, mas como $a - bq = r$, resulta que m também divide o resto. A recíproca se prova de modo análogo.

Como todos divisores comuns $D(a, b)$ e $D(b, r)$ coincidem, seus máximos também devem coincidir, verificando o resultado.

■

O *Algoritmo de Euclides*, também por vezes denominado *Algoritmo das divisões sucessivas*, se baseia em aplicações reiteradas da divisão euclidiana. Assim, começamos dividindo a por b, e obtendo um resto r_1. Na sequência, se $r_1 \neq 0$, efetuamos a divisão euclidiana de b por r_1, resultando em um resto r_2. Como os restos da sequência são inteiros não-negativos, dispostos em ordem decrescente, eventualmente o algoritmo alcança o resto 0. Pelo lema, o menor resto r_n maior que 0 será justamente o $mdc(a, b)$.

Exemplo 2.1. Calculando o $mdc(1001, 109)$, obtemos as seguintes

divisões:

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

O último resto não-nulo é 1, logo $mdc(1001, 109) = 1$.

Mínimo Múltiplo Comum

Assim como, dados dois inteiros não-nulos, é possível tratar dos números que dividem ambos, é natural uma definição que abranja os números que *são divididos* por dois inteiros não-nulos quaisquer. Um número c é dito *múltiplo comum* de dois inteiros não-nulos a e b se temos que $a|c$ e $b|c$.

Denotaremos o conjunto de múltiplos comuns de a e b por $M(a, b)$. Note que este conjunto não é vazio, pois pelo menos $a \cdot b \in M(a, b)$. Porém, ao contrário do caso dos divisores comuns, o conjunto de múltiplos comuns é infinito. Ainda assim, se forem considerados apenas os elementos positivos de $M(a, b)$, pelo Princípio da Boa Ordem se segue que entre estes existe um menor elemento, o que motiva a seguinte definição:

Definição 2.2. Denominamos *mínimo múltiplo comum* (mmc) de a e b o menor de seus múltiplos comuns positivos, isto é:

$$mmc(a, b) = minM^+(a, b)$$

em que $M^+(a, b)$ é o conjunto de múltiplos comuns c de a e b tais que $c > 0$.

Teorema de Bachet-Bézout

Dizemos que um número inteiro c é *combinação inteira* de dois inteiros a,b, se existem $x, y \in \mathbb{Z}$ tais que se verifique a equação:

$$c = ax + by$$

O Teorema de Bachet-Bézout, que enunciamos a seguir, garante que sempre é possível escrever o mdc de dois números inteiros como uma combinação inteira desses, isto é:

Teorema 2.1. Sejam a e b inteiros. Então existem x e y inteiros tais que:

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

Duas consequências importantes desse teorema são:

Corolário 2.1. Dados $a, b \in \mathbb{Z}$, a equação:

$$ax + by = c$$

admite solução inteira se, e somente se, $mdc(a, b)|c$

Corolário 2.2. Sejam $a, b, c \in \mathbb{Z}$ tais que $a|bc$. Se $mdc(a, b) = 1$, então $a|c$.

Como vimos, equação $ax+by = mdc(a, b)$ sempre admite solução inteira. Contudo, essa solução não é única. No exemplo a seguir, apresentamos um algoritmo para encontrar o conjunto de todas as soluções inteiras desse tipo de problema.

Exemplo 2.2. Encontre todos os $x, y \in \mathbb{Z}$ tais que $1001x + 109y = mdc(1001,\ 109)$.
Solução:
Fazemos as divisões sucessivas para o cálculo de $mdc(1001, 109) = 1$ utilizando o Algoritmo de Euclides. Em seguida, isolamos os restos:

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

Se isolarmos os restos nas equações acima, obteremos as seguintes igualdades:

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

Note que podemos efetuar sucessivas substituições na equação $1 = 9 - 2 \cdot 4$ e expressar 1 como combinação linear de 1001 e 109. Isso pode ser feito da seguinte forma:
Substituindo o 2:

$$1 = 9 - (20 - 9 \cdot 2) \cdot 4 = 9 \cdot 9 - 4 \cdot 20$$

Substituindo o 9:

$$1 = 9 \cdot (109 - 20 \cdot 5) - 4 \cdot 20 = 9 \cdot 109 - 49 \cdot 20$$

Substituindo o 20:

$$1 = 9 \cdot 109 - 49 \cdot (1001 - 109 \cdot 9) = 1001(-49) + 109(450)$$

Logo, uma solução da equação $1001x + 109y = 1$ é $(x_0,\ y_0) = (-49,\ 450)$.
Para encontrar as demais, escrevemos o lado direito desta equação utilizando a solução particular que acabamos de encontrar:

$$1001x + 109y = 1001x_0 + 109y_0 \Leftrightarrow 1001(x - x_0) = -109(y - y_0)$$

Como $mdc(1001,\ 109) = 1$ temos, pelo Teorema de Euclides, que $1001|y - y_0$, ou seja, $y - y_0 = 1001t$, para algum $t \in \mathbb{Z}$.
Substituindo temos:

$$\begin{aligned} 1001(x - x_0) = -109.1001t \Leftrightarrow 1001(x - x_0) &= 1001.(-109t) \\ \Leftrightarrow x - x_0 = -109t \Leftrightarrow x &= x_0 - 109t \end{aligned}$$

De maneira análoga podemos obter que $y = y_0 + 1001t$
Assim, as soluções da equação dada são todos os pontos da reta $1001x + 109y = 1$ da forma $(x, y) = (x_0 - 109t,\ y_0 + 1001t) = (-49, 450) + (-109, 1001)t$ com $t \in \mathbb{Z}$. ■

Para concluir, apresentamos um resultado que caracteriza a relação entre o máximo divisor comum e o mínimo múltiplo comum de dois números dados. Por simplicidade, enunciaremos o resultado para números naturais, podendo ser facilmente generalizado para os inteiros tomando os valores absolutos adequados.

Teorema 2.2. Sejam $a, b \in \mathbb{N}^*$, então:

$$mdc(a, b).mmc(a, b) = ab$$

Demonstração. Seja $d = mdc(a, b)$. Então podemos escrever $a = a_1 d, b = b_1 d$, com a_1, b_1 inteiros tais que $mdc(a_1, b_1) = 1$. Agora considere o número:

$$x = \frac{ab}{d}$$

Temos, por um lado, que $x = a_1 b$, por outro, que $x = ab_1$. Portanto $a|x, b|x$ e x é múltiplo comum de a, b. Verifiquemos agora que x é o menor inteiro positivo nessas condições. Seja $m \in \mathbb{N}^*$ um múltiplo comum qualquer de a e b. Então, de $a|m$ segue que existe $q \in \mathbb{N}$ com $m = aq = a_1 dq$. Por sua vez, como $b|m$, temos que $b_1 d|a_1 dq$, e portanto, $b_1|a_1 d$. Dado que a_1, b_1 sãp coprimos, temos que $b_1|q$. Escrevemos então $q = b_1 c$. Logo $m = aq = (a_1 d)(b_1 c) = (a_1 d b_1)c = xc$. Logo x divide qualquer outro múltiplo comum positivo de a e b. Assim, por limitação, x deve ser o menor múltiplo comum. ■

Problemas Propostos

Os problemas estão classificados por nível de dificuldade:

●	▲	♦	★
Fácil	Médio	Difícil	Desafio

1. ● Usar o Algoritmo de Euclides para obter números r e s satisfazendo:

- $mdc(56, 72) = 56r + 72s$
- $mdc(24, 138) = 24r + 138s$

2. ● Mostre que $2^{15} - 1$ e $2^{10} + 1$ são primos entre si.

3. ● Mostre que quaisquer dois termos consecutivos da sequência de Fibonacci são coprimos.

4. ● Sejam a, b, c inteiros. Prove que:

   (a) $mdc(-a, b) = mdc(a, -b)$

   (b) $mdc(a, b) = mdc(a, a + b)$

5. ▲ Prove a seguinte proposição:
   A equação $ax + by = c$ admite solução inteira em x e y se, e somente se, $mdc(a, b)|c$.

6. ▲ Prove que se $mdc(a, b) = 1$ e $a|bc$, então $a|c$.

7. ▲ Prove que se $mdc(a, b) = 1$, então $mdc(ac, b) = mdc(c, b)$.

8. ▲ Para todo $n \in \mathbb{Z}, n \neq 0, -1$, calcular:

   - $mmc(n, n + 1)$;
   - $mmc(2n - 1, 2n + 1)$
   - $mmc(nc, (n + 1)c), c \in \mathbb{Z}^*$

9. ▲ (OBM 2011) Qual é o maior valor possível do mdc de dois números distintos pertencentes ao conjunto $\{1, 2, 3, \ldots, 2011\}$?

10. ▲ (OBM 2011) Os inteiros positivos 30, 72 e N possuem a propriedade de que o produto de quaisquer dois é divisível pelo terceiro. Qual o menor valor possível de N?

11. ♦ (OBMEP - Banco de Questões 2015) Em uma lousa são escritos os 2014 inteiros positivos de 1 até 2014. A operação permitida é escolher dois números a e b, apagá-los e escrever

em seus lugares os números $mdc(a,b)$ e $mmc(a,b)$. Essa operação pode ser feita com quaisquer dois números que estão na lousa, incluindo os números que resultaram de operações anteriores. Determine qual a maior quantidade de números 1 que podemos deixar na lousa.

12. ♦ Sejam $a_n = 100 + n^2$ e $d_n = mdc(a_n, a_{n+1})$. Calcular d_n para todo n.

13. ♦ Demonstrar que se $mdc(a, 2^{n+1}) = 2^n$ e $mdc(b, 2^{n+1}) = 2^n$, então $mdc(a+b, 2^{n+1}) = 2^{n+1}$.

14. ♦ Demonstrar que, se a, b, c, d, m, n são inteiros tais que $ad - bc = 1, mn \neq 0$, então:

$$mdc(am + bn, cm + dn) = mdc(m, n)$$

15. ♦ Demonstrar que $mdc(2^a - 1, 2^b - 1) = 2^{mdc(a,b)} - 1$ para todo $a, b \in \mathbb{N}$.

16. ♦ (OBM 2011) Existem 2011 inteiros positivos $a_1 < a_2 < \ldots < a_{2011}$ tais que, para todo $1 \leq i < j \leq 2011, mdc(a_i, a_j) = a_j - a_i$?

17. ♦ (OBM 2012) Esmeralda desenhou uma tabela com 100 linhas e 100 colunas, e escreveu, na linha i e coluna j da tabela, mdc(i, j) se $i < j$ e mmc(i, j) se $i \geq j$. Por exemplo, na linha 4, coluna 6 ela escreveu mdc(4,6) = 2, e na linha 15, coluna 10 ela escreveu mmc(15,10) = 30. Qual é o produto de todos os 100^2 números da tabela?

18. ♦ (OBM 2013) Seja $A = \{1, 2, 3, \ldots, 20\}$ o conjunto dos 20 primeiros inteiros positivos. Para cada subconjunto X de 15 elementos de A, calculamos o produto $p(X)$ de seus elementos. Por exemplo $p(\{1, 2, 3, \ldots, 15\}) = 1.2 \ldots .15 = 15!$ Qual é o máximo divisor comum dos $\binom{20}{15}$ produtos $p(X)$ obtidos com todos os subconjuntos com 15 elementos de A?

19. ♦ (IMO 1992) Encontrar todos os inteiros a, b, c, com $1 < a < b < c$, tais que $(a-1)(b-1)(c-1)|abc-1$.

20. ★ Encontrar todas as funções $f : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{Z}$ satisfazendo simultaneamente as propriedades:

    - $f(a,a) = a$;
    - $f(a,b) = f(b,a)$;
    - Se $a > b$, então $f(a,b) = \frac{a}{a-b} f(a-b,b)$.

Aula 3

Teorema Fundamental da Aritmética

O objetivo desta aula é identificarmos o papel importante que os números primos desempenham na Teoria de Números. Isso se dá pelo fato de todo número inteiro diferente de 0, 1 e -1 poder ser escrito de maneira única como o produto de números primos, a menos da ordem dos seus fatores.

Primos

Definição 3.1. Dizemos que p é um **número primo** se possui exatamente dois divisores positivos, 1 e $|p|$.

Observe que pela definição o número 0 não é um número primo, pois possui infinitos divisores positivos. Da mesma forma, vemos que 1 e -1 também não são primos.

Definição 3.2. Dizemos que um inteiro a é um **número composto** quando possuir mais de dois divisores inteiros distintos.

Dado um inteiro a não nulo que seja composto, ele admite um divisor b tal que $|b| \neq 1$ e $|b| \neq a$, assim sendo, $1 \leq |b| \leq |a|$. Um divisor nessas condições será chamado de *divisor próprio* de a.

Proposição 3.1. Seja p um número primo, e sejam a, b inteiros.

1. Se $p \nmid a$, então $\text{mdc}(p, a) = 1$.

2. Se $p|ab$, então $p|a$ ou $p|b$.

Demonstração.

1. Como p é primo e $p \nmid a$, então o único divisor comum positivo entre a e p é 1. Daí, segue o resultado.

2. Por hipótese, temos que $p|ab$. Se tivermos $p|a$, segue o resultado, caso contrário $mdc(p, a) = 1$ o que implica pelo Teorema de Euclides que $p|b$.

■

Exemplo 3.1. 1. Mostre que se p é primo e p divide um produto $a_1 a_2 \cdots a_n$, então $p|a_j$ para algum j, $1 \leq j \leq n$. Conlcua, em particular, que se $p|a^k$, $k \geq 2$, então $p|a$.

Solução:

Primeiramente vamos separar o produto em duas partes:

$$(a_1 \cdot a_2 \cdots a_{n-1}) \cdot a_n$$

Agora analisemos os casos:

- Se $p|a_i$ para algum i, $1 \leq i \leq n-1$, então está provado que $p|a_j$ para algum j.

- Se $p \nmid a_i$, para todo i, $1 \leq i \leq n-1$, então $p \nmid (a_1 \cdot a_2 \cdots a_{n-1}) \implies \text{mdc}(p, a_1 \cdot a_2 \cdots a_{n-1}) = 1$, pois p é primo.

  Com isso, temos que $p|(a_1 \cdot a_2 \cdots a_{n-1}) \cdot a_n$ e $\text{mdc}(p, a_1 \cdot a_2 \cdot \cdots a_{n-1}) = 1$ e, pelo Teorema de Euclides, $p|a_n$. Ou seja, $p|a_j$ para algum j.

Observe que esse exemplo é uma generalização do item (ii) da última proposição.

É muito importante conseguirmos caracterizar a noção dos números primos e fazemos isso estendendo a Proposição 1 para o seguinte Teorema:

Teorema 3.1. Seja p um inteiro diferente de 0,1 e -1. Então, p é primo se e somente se, toda vez que p divide um produto de dois números, p divide pelo menos um dos fatores.

Demonstração.
($\Longrightarrow$) Essencialmente, a ida já foi provada no exemplo anterior.

($\Longleftarrow$) Provemos por absurdo a volta. Para isso, suponha que p não seja primo e que satisfaz as propriedades do enunciado. Como p é um número composto, segue que $|p|$ pode ser escrito da seguinte maneira $|p| = a \cdot b$, onde a e b são seus divisores próprios, ou seja,

$$1 < a < |p|$$

$$1 < b < |p|.$$

Dessas desigualdades, decorre que $p \nmid a$ e $p \nmid b$ o que acaba implicando $p \nmid a \cdot b$, contradizendo nossa hipótese. A nossa contradição ocorreu ao supormos que p não era um número primo. ■

Os próximos resultados serão desenvolvidos com o interesse de chegarmos no Teorema Fundamental da Aritmética, tema dessa aula.

Lema 3.1. Todo inteiro $a > 1$ pode ser escrito como produto de números primos.

Demonstração. Problema 4. ■

Teorema 3.2. Seja $a > 1$ um inteiro. Então, existem primos positivos $p_1 \leq p_2 \leq ... \leq p_t$, tais que $a = p_1 p_2 \cdots p_t$, e essa decomposição é única.

Teorema Fundamental da Aritmética. Seja a um inteiro diferente de 0,1 e -1. Então, existem primos positivos $p_1 < p_2 < ... < p_r$ e inteiros positivos n_1, n_2,...,n_r tais que a admite uma decomposição única na forma $a = E \cdot p_1^{n_1} \cdot_2^{n_2} \cdots p_r^{n_r}$, onde $E = \pm 1$.

Obs. O número E caracteriza se a é um número positivo ou negativo.

Demonstração.

Observe que $a = E|a|$, onde $E = 1$ ou $E = -1$.

Pela definição de módulo, temos que $|a|$ é um inteiro positivo e além disso, pelas condições do enunciado, é estritamente maior que 1. Com isso, decorre pelo Lema 1 que existem primos $p_1 \leq p_2 \leq \cdots p_t$ tais que:

$$|a| = p_1 \cdot p_2 \cdots p_t \tag{3.1}$$

Dependendo do sinal de a, têm-se que:

$$a = E \cdot p_1 \cdot p_2 \cdots p_t$$

Agrupando os fatores primos repetidos, obtemos a seguinte decomposição:

$$a = E \cdot p_1^{n_1} \cdot_2^{n_2} \cdots p_r^{n_r} \tag{3.2}$$

Note que a decomposição (1) é única, pelo Lema 1. Decorre imediatamente a unicidade da decomposição (2), pois ela foi obtida a partir da (1).

■

Problemas Propostos

Os problemas estão classificados por nível de dificuldade:

●	▲	♦	★
Fácil	Médio	Difícil	Desafio

1. ● Considere um inteiro a e suponha que ele não seja divisível por 5. É possível que o número $2a$ seja divisível por 5? Justifique usando o Teorema Fundamental da Aritmética.

2. ● Seja a um inteiro. Temos que o número $2a$ é divisível por 6. É possível que a seja divisível por 6? Novamente, justifque pelo Teorema Fundamental da Aritmética.

3. ● Sejam a um número inteiro e p um número primo. Mostre, por indução em n, que se p divide a^n então p divide a.

4. ● Demonstre o Lema 1.

5. ▲ Mostre que $\sqrt{2 \cdot 3 \cdot 5}$ é irracional.

6. ▲ Seja a um inteiro positivo e suponha que $a = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$ é sua fatoração em produto de primos.

   Mostre que todo divisor de a é da forma $d = u \cdot p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$, com $u = \pm 1$ e $0 \leq k_i \leq r_i$ para $i = 1,2,\cdots,n$.

7. ▲ Usando o item anterior, mostre que o número de divisores positivos de a é $(r_1 + 1) \cdot (r_2 + 1) \cdots (r_n + 1)$.

8. ▲ Mostre que um número inteiro positivo a possui exatamente três divisores positivos se e somente se a é o quadrado de um número primo. Observe os casos com 4 e 5 divisores.

9. ▲ Mostre o caso geral do Problema 8, ou seja, quando possuir um número primo p de divisores positivos.

10. ▲ Sejam $k = p_1^{r_1} \cdot \ldots \cdot p_n^{r_n}$ e $l = q_1^{s_1} \cdot \ldots \cdot q_m^{s_m}$ as fatorações em primos de k e l, respectivamente. Então $k = l \Leftrightarrow n = m$ e $p_i^{r_i} = q_i^{s_i}$ para todo i, $0 \leq i \leq n = m$.

11. ▲ Mostre que se p é um primo positivo então $\sqrt{p}$ é um número irracional.

12. ▲ Mostre que, dados um inteiro n e um primo p, n pode ser escrito na forma $n = p^k \cdot m$, em que $k \geq 0$ e m é um inteiro não divisível por p.

13. ▲ Seja a um inteiro positivo e suponha que $a = p_1^{r_1} \cdot ... \cdot p_n^{r_n}$ é sua fatoração em produto de primos. Mostre que a é um quadrado perfeito se e somente se todos os expoentes r_i são pares.

14. ▲ Use o item anterior para decidir se os números abaixo são quadrados perfeitos.

    (a) 693

    (b) $11 \cdot 025$

    (c) $2 \cdot 475$

15. ♦ Sejam p, q e r três números primos maiores que 3. Sabe-se que o número $p + q + r$ também é primo . Mostre que $p + q$, $p + r$ ou $q + r$ é um múltiplo de 6.

16. ♦ Sejam p,q primos tais que $p \geq q \geq 5$. Prove que $24|(p^2 - q^2)$.

17. ♦ Seja n um inteiro positivo. Prove que:

    (a) Se $n > 4$ não é primo, emtão $n|(n-1)!$

    (b) Nenhum inteiro da forma $8^n + 1$ é primo.

18. ♦ (OBM 2016) As raízes de um polinômio P, de coeficientes inteiros e grau 10, são todas inteiras e distintas. Então todo valor não nulo de $P(n), n$ inteiro, tem, no mínimo, quantos divisores positivos?

19. ★ (OlbM1987) A sequência p_n é definida da seguinte maneira:

    (a) $p_1 = 2$

    (b) Para todo $n \geq 2$, p_n é o maior divisor primo da expressão

$$p_1 \cdot p_2 \cdot p_3 \cdot \cdot \cdot p_{n-1} + 1$$

Demonstre que p_n é diferente de 5.

20. ★ (Teorema de Euclides) Existem infinitos primos.

Aula 4

Resultados de Números Primos

O objetivo desta aula é trabalharmos com algumas estratégias para obter números primos, para tratar da seguinte questão: existem infinitos números primos?

Números de Fermat

Inicialmente, vamos estudar os **números de Fermat**, que são definidos a seguir:

$$F_n = 2^{2^n} + 1$$

Em 1640 Fermat afirmou que para todo n tinha-se F_n primo. Mas em 1740, Euler provou que $F(5) = 4294967297$ era um número composto, assim encontrando um contra-exemplo para a afirmação de Fermat. É fácil obervar que para $0 \leq n \leq 4$ têm-se F_n primo e esses são chamados de **primos de Fermat**. Note que a fórmula de F_n é uma função duas vezes exponecial e assim podemos concluir que ela cresce muito rápido, então para valores de n maiores que 4 obtemos um valor F_n cada vez maior e com mais casas decimais dos números anteriores. Dessa forma fica difícil estudar esses números sem um apoio computacional. E mesmo com esse apoio ainda

não sabemos se existem outros primos de Fermat, além desses cinco.

Propriedades dos Números de Fermat

Proposição 4.1. Todo número de Fermat verifica as seguintes relações de recorrência:

1. $F_n = (F_{n-1} - 1)^2 + 1$
2. $F_n = F_{n-1} + 2^{n-1} F_0 \cdots F_{n-2}$
3. $F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$
4. $F_{n+k} - 1 = (F_n - 1)^{2^k}$

Como vimos anterioriormente, os quatro primeiros números de Fermat são co-primos, pois não são compostos; será que isso ocorre para os números de Fermat seguintes? Ou seja, se todos os números de Fermat são co-primos entre si? E a resposta é sim, com isso enunciamos o próximo resultado da aula:

Teorema 4.1. Sejam F_n e F_m números de Fermat tais que $n \neq m$. Então, F_n e F_m são co-primos.

Agora, deixamos para o leitor perguntas que estão abertas na matemática sobre os números de Fermat. Existem infinitos números primos de Fermat? E infinitos números compostos?

Números de Mersenne

Agora, discutiremos os chamados **números de Mersenne**. Esses números são da forma:

$$M_n = 2^n - 1$$

para cada n inteiro não negativo. Pode-se provar que, se n é composto M_n também é (exercício). Assim, se um dado número de Mersenne é primo, então é necessariamente da forma $M_p = 2^p - 1$, em que o próprio p é primo. Note, contudo, que a recíproca *não* é verdadeira. Como contraexemplo, podemos tomar $p = 11$. De fato:

$$M_{11} = 2047 = 23 \cdot 89$$

Uma das questões bastante vinculadas aos primos de Mersenne é a dos números *perfeitos*. Um número natural é dito perfeito se ele é a soma de todos os seus divisores positivos próprios, i.e., todos seus divisores positivos menores do que ele. Assim, por exemplo, 6 é perfeito, pois seus divisores próprios são 1, 2, 3, e $1+2+3=6$. É possível provar que $2^{n-1}(2^n-1)$ é perfeito sempre que $M_n = 2^n-1$ é primo (exercício). De fato, todo número perfeito par é dessa forma. A existência ou não de números perfeitos ímpares permanece em aberto até hoje.

Muitos métodos foram desenvolvidos historicamente para avaliar a primalidade de um número de Mersenne dado. Dada a eficiência de alguns desses algoritmos para números grandes, os maiores números primos conhecidos são justamente primos de Mersenne.

Infinidade de Primos

Um dos fatos mais conhecidos sobre o conjunto dos números primos diz respeito à sua infinidade. A demonstração de que existem infinitos primos que apresentamos a seguir é conhecida desde a Antiguidade, constando já nos *Elementos* de Euclides.

Teorema 4.2. Existem infinitos números primos.

Demonstração. Suponhamos, por absurdo, que o conjunto dos números primos seja finito. Assim, sejam $p_1, p_2 \ldots, p_n$ todos os números primos existentes. Então, podemos considerar o número:

$$P = p_1 p_2 \ldots p_n + 1$$

Sabemos que P admite um divisor primo p_i. No entanto, temos que $p_i | p_1 p_2 \ldots p_n$, logo segue que $p_i | P - p_1 p_2 \ldots p_n = 1$, mas $p_i > 1$, e com isso obtemos uma contradição.

■

Entre outras demonstrações deste fato fundamental sobre números primos, cabe mencionar a prova formulada por Euler. A ideia do matemático suíço consistiu em considerar o produto:

$$P = \left(\frac{1}{1-\frac{1}{2}}\right)\left(\frac{1}{1-\frac{1}{3}}\right)\left(\frac{1}{1-\frac{1}{5}}\right)\cdots\left(\frac{1}{1-\frac{1}{p}}\right)\cdots$$

onde cada número primo p aparece em exatamente uma parcela. Se assumirmos, por absurdo novamente, que a quantidade de números primos é finita, o produto acima deve ser um número real (positivo). Euler verificou que a igualdade acima é equivalente à seguinte:

$$P = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \ldots$$

A soma acima é conhecida como *série harmônica*, e é possível provar que tal soma é maior que qualquer número real. Portanto, P não pode ser nenhum número real positivo, contradizendo a hipótese de que a quantidade de números primos é finita.

Assim, sabemos dizer que existem infinitos números primos, no entanto pouco temos a dizer ainda sobre sua distribuição. Várias conjecturas relativamente simples sobre números primos permanecem em aberto até hoje.

Um resultado relativamente fácil de se provar diz respeito a podermos encontrar primos consecutivos "tão distantes entre si quanto se desejar".

Proposição 4.2. Dado um inteiro positivo n, existem n inteiros positivos consecutivos que são todos compostos.

Demonstração. Fixemos a sequência de números inteiros dada por:

$$(n+1)!+2, (n+1)!+3, \ldots (n+1)!+(n+1)$$

Para todo m inteiro com $2 \leq m \leq n+1$, temos que $m|(n+1)!$. Logo $m|(n+1)!+m$. Como existem n números na sequência considerada, obtemos pelo menos n inteiros consecutivos que são todos compostos.

■

Problemas Propostos

Os problemas estão classificados por nível de dificuldade:

●	▲	♦	★
Fácil	Médio	Difícil	Desafio

Definição 1. Dado $n \in \mathbb{N}$, denotaremos por $\sigma(n)$ a soma de todos os divisores de n. Denotaremos também por $\sigma_0(n)$ a soma de todos os divisores próprios de n.

Definição 2. Diremos que $n \in \mathbb{N}$ é um número perfeito se satisfaz a seguinte igualdade $\sigma(n) = 2n$.

Obs. Se n é perfeito, então $\sigma_0(n) = n$. Como $\sigma_0(n) = \sigma(n) - n$ isto implica que $\sigma(n) = 2n$.

Afirmação 1. Seja $n \in \mathbb{N}$, com $n \geq 2$, cuja fatoração prima é dada por $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$. Então

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdots \frac{p_r^{\alpha_r+1}-1}{p_r-1}$$

1. ● O número $M_n = 2^n - 1$, com $n \geq 1$ é chamado de *n-ésimo* número de Mersenne.

   Mostre que se $M_n = 2^n - 1$ é primo, então n é primo.

2. ● Prove por Indução os itens da Proposição 1.

3. ● Seja $n \in \mathbb{Z}$, $n > 1$. Mostre que se $n|(n-1)!$, então n é composto.

4. ● Provar que, se $a \neq b$, existem infinitos positivos n tais que $a + n$ e $b + n$ sejam relativamente primos.

5. ▲ Mostre que três ímpares positivos consecutivos não podem ser todos primos, com exceção de 3, 5 e 7.

6. ▲ Demonstrar que existem infinitos primos da forma $4n + 3, n \in \mathbb{N}$.

7. ▲ Seja $\{p_1, \ldots, p_n\}$ um conjunto de primos positivos distintos. Seja A o produto de quaisquer r destes primos, e B o quociente:

$$B = \frac{p_1 \cdots p_n}{A}$$

   - Provar que p_k divide A ou B, mas não ambos
   - Provar que $A + B$ tem um divisor primo $p \notin \{p_1 \ldots p_n\}$
   - Deduzir, desse argumento, a existência de infinitos números primos.

8. ▲ Para cada inteiro $n \geq 1$ seja p_n o n-ésimo número primo positivo. Prove que o inteiro $p_1 p_2 \ldots p_n + 1$ não é um quadrado perfeito.

9. ♦ Prove que, se $2^m + 1$ é primo para algum $m > 0$, então m é uma potência de 2.

10. ♦ Mostre que todo número de Fermat é igual ao produto de seus anteriores somado a 2, ou seja, que $F_n = F_0 \cdot \ldots \cdot F_{n-1} + 2$.

11. ♦ Mostre a seguinte equivalência na prova formulada por Euler para a existência de infinitos números primos:

$$\left(\frac{1}{1-\frac{1}{2}}\right)\left(\frac{1}{1-\frac{1}{3}}\right)\cdots\left(\frac{1}{1-\frac{1}{p}}\right)\cdots = 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\cdots$$

12. ♦ Seja M um conjunto de 1537 inteiros positivos sem divisores primos maiores que 27. Mostre que:

    - Qualquer subconjunto de 513 números contém dois cujo produto é um quadrado perfeito.
    - M contém um subconjunto de quatro números cujo produto é uma quarta potência.

13. ♦ (IMO 2011) Considere um polinômio $P(x) = (x + d_1)(x + d_2)\ldots(x + d_9)$, com $d_1, d_2, \ldots d_9$ números inteiros distintos. Prove que existe um inteiro N tal que, para todos os inteiros $x > N$, o número $P(x)$ é divisível por um número primo maior que 20.

14. ★Seja $n \in \mathbb{N}$. Então, n é primo se, e somente se, $\sigma(n) = n+1$.

15. ★ Dado $n \in \mathbb{N}$ natural, denotaremos por $\sigma(N)$ a soma de todos os divisores de n. Denotaremos tambem por $\sigma_0(n)$ a soma de todos os divisores próprios de n.

    Seja $n \in \mathbb{N}$ composto tal que $n = ab$, com $(a, b) = 1$. Então, $\sigma(n) = \sigma(a)\sigma(b)$.

16. ★ Um natural da forma $n = 2^{p-1}(2^p - 1)$ é perfeito quando $2^p - 1$ é um primo de Mersenne.

Aula 5

Equações Diofantinas

Recebem o nome de *equações diofantinas* quaisquer equações polinomiais (tipicamente com duas ou mais incógnitas) com coeficientes inteiros, tendo em vista encontrar apenas suas soluções inteiras. Historicamente, o nome é uma referência a Diofanto de Alexandria, matemático grego do século III d.C., cuja principal obra, *Arithmetica*, é uma coletânea de equações determinadas e indeterminadas para as quais são encontradas as soluções numéricas. Dos treze livros originais dessa obra, apenas seis foram preservados em grego e presumivelmente outros quatro em tradução árabe. Mais propriamente, Diofanto de Alexandria se ocupou de estudar soluções racionais positivas em suas equações, no entanto, pelas estratégias algébricas que desenvolveu, tradicionalmente se vincula seu nome aos problemas relacionados com números inteiros.

Entre as equações diofantinas mais elementares estão as equações lineares a duas variáveis, que serão o objeto central de estudo dessa aula.

Equações diofantinas lineares a duas variáveis

Denominamos *equações diofantinas lineares a duas variáveis* as equações do tipo:

$$ax + by = c$$

em que x, y são as incógnitas e $a, b \in \mathbb{Z}$ não são simultaneamente nulos. Consideramos uma solução particular da equação um par da forma $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ tal que torne verdadeira a igualdade:

$$ax_0 + by_0 = c$$

Primeiro, precisamos considerar as condições de existência de alguma solução. Pelo Teorema de Bachet-Bézout que estudamos anteriormente, sabemos que, se $d = mdc(a, b)$, então existe solução inteira para a equação:

$$ax + by = d$$

De fato, podemos depreender disso as condições necessárias e suficientes para a existência de soluções de uma equação diofantina.

Proposição 5.1. Uma equação diofantina linear da forma $ax+by = c$ admite solução se, e somente se, $d = mdc(a, b)$ divide c.

Demonstração. Seja (x_0, y_0) uma solução de $ax + by = c$. Nesse caso, temos que $d|a \implies d|ax_0$ e $d|b \implies d|by_0$, e, portanto, $d|ax_0 + by_0 = c$.

Reciprocamente, suponhamos que $d|c$. Logo, existe $c' \in \mathbb{Z}$ tal que $c = dc'$. Pelo Teorema de Bachet-Bézout, sabemos que existem inteiros r, s tais que $ar + bs = d$. Multiplicando ambos os lados da equação por c', obtemos:

$$a(c'r) + b(c's) = (ar + bs)c' = dc' = c$$

Logo, o par $(c'r, c's)$ é uma solução para a equação diofantina inicial. ■

Caso a equação diofantina linear tenha solução, podemos obter uma solução particular simplesmente a partir da solução de $ax+by = mdc(a, b)$. Porém, essa solução não é única para a nossa equação diofantina. De fato, quando tal equação admite alguma solução, as soluções são infinitas. O próximo resultado que apresentamos é uma descrição dessa família de soluções.

Proposição 5.2. Seja $ax + by = c$ uma equação diofantina linear, com $d = mdc(a, b)$ dividindo c. Se (x_0, y_0) é uma solução particular, então toda outra solução é da forma:

$$\left(x_0 + \frac{b}{d} \cdot t, y_0 - \frac{a}{d} \cdot t\right), t \in \mathbb{Z}$$

Além disso, para todo $t \in \mathbb{Z}$, os pares da forma acima são soluções.

Demonstração. Seja (x', y') uma solução qualquer. Então:

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

Rearranjando os termos dos dois extremos da equação, obtemos:

$$a(x_0 - x') = -b(y_0 - y') \tag{5.1}$$

Como d é máximo divisor comum de a e b, existem a' e b' inteiros tais que $a = da', b = db'$. Além disso, temos que $mdc(a', b') = 1$. Assim podemos reescrever (1) como:

$$a'd(x_0 - x') = -b'd(y_0 - y')$$

Então, cancelando d em ambos os lados da equação, temos que:

$$a'(x_0 - x') = -b'(y_0 - y') \tag{5.2}$$

Como a', b' são coprimos, se segue que $a'|(y_0 - y')$ e $b'|(x_0 - x')$. Portanto, existem inteiros u, t tais que $(x_0 - x') = b'u, (y_0 - y') = a't$. Fazendo as devidas substituições em (2):

$$a'b'u = -b'a't \tag{5.3}$$

Cancelando $a'b'$ em ambos os lados, concluímos que $u = -t$, e, consequentemente $x' = x_0 + b't, y' = y_0 - a't$. Como $b' = b/d, a' = a/d$, a solução é exatamente da forma enunciada.

A prova de que para qualquer $t \in \mathbb{Z}$ o par $(x_0 + (b/d)t, y_0 - (a/d)t)$ é solução será deixada como exercício. ■

Exemplo 5.1. Encontre as soluções de $56x + 72y = 40$.

Inicialmente, calculando o máximo divisor comum dos coeficientes acompanhando as incógnitas, obtemos $mdc(56, 72) = 8$, e $8|40$, portanto existem soluções.

Resolvendo $56r + 72s = 8$ pelo Algoritmo de Euclides, obtemos $r = 4, s = -3$. Como $c' = 40/8 = 5$, nossa solução particular é dada por $x_0 = rc' = 4 \cdot 5 = 20$ e $y_0 = sc' = (-3) \cdot 5 = -15$. Por fim, temos que $a/d = 56/8 = 7, b/d = 72/8 = 9$, o que nos leva à forma geral:

$$x = 20 + 9t, y = -15 - 7t, t \in \mathbb{Z}$$

A Proposição 2 garante que quando $ax + by = c$ admite uma solução inteira, existe uma quantidade infinita de soluções para a equação. Porém, em algumas situações, como alguns contextos de mundo real, queremos considerar apenas soluções não-negativas, isto é, soluções (x, y) em que simultaneamente $x \geq 0, y \geq 0$. Tais soluções nem sempre existem (como você pode verificar no Exemplo 1).

Exemplo 5.2. Suponha que um certo produto é vendido apenas em sacos de 7kg ou 15kg. É possível fazer uma compra de exatamente 125kg?

Nosso problema pode ser expresso na forma da equação diofantina:

$$15x + 7y = 125$$

No entanto, pela natureza do problema, somos forçados a considerar apenas as soluções não-negativas da equação. Começamos resolvendo de modo usal, verificando que $mdc(7, 15) = 1$ obviamente divide 125. Também é fácil verificar que $r = 1, s = -2$ é solução de $15r + 7s = 1$, o que nos fornece a solução particular:

$$x_0 = 1 \cdot 125 = 125$$
$$y_0 = (-2) \cdot 125 = -250$$

Por sua vez a solução geral é da forma:

$$\begin{aligned} x &= 125 + 7t \\ y &= -250 - 15t, t \in \mathbb{Z} \end{aligned}$$

Assim, para obter uma solução não-negativa, precisamos encontrar $t \in \mathbb{Z}$ satisfazendo simultaneamente as duas inequações:

$$\begin{cases} 125 + 7t \geq 0 \\ -250 - 15t \geq 0 \end{cases}$$

Da primeira inequação, resulta que $t \geq -17$, da segunda, que $t \leq -17$. Considerando essas condições, $t = -17$ fornece a única solução não-negativa, da qual obtemos $x = 6, y = 5$. Portanto, o único modo de comprar 125kg do produto nas condições do problema é comprando 6 pacotes de 15kg e 5 pacotes de 7kg.

Como vimos no último exemplo, algumas aplicações de equações diofantinas lineares a situações cotidianas exigem uma restrição das soluções aos inteiros não-negativos. Isso nos leva naturalmente à questão: como determinar quando existe pelo menos uma solução não-negativa para a equação?

Em geral, dados $a, b > 0$ tais que $mdc(a, b) = 1$, sabemos que a equação diofantina $ax + by = c$ tem solução para todo $c \in \mathbb{Z}$. Sejam r, s tais que $ar + bs = 1$. Sabemos que a solução geral de $ax + by = c$ é da forma $x = rc + bt, y = sc - at$. Para avaliar se existe uma solução não-negativa, precisamos satisfazer simultaneamente as seguintes equações:

$$\begin{cases} rc + bt \geq 0 \\ sc - at \geq 0 \end{cases}$$

Destas inequações, obtemos: $(sc)/a \geq t \geq (-rc)/b$. Isto significa que uma solução não-negativa existe se, e somente se, existe algum inteiro entre $(sc)/a$ e $(-rc)/b$. Note que para c suficientemente

grande, sempre conseguimos garantir a existência de algum inteiro nesse intervalo, e, consequentemente, de uma solução não-negativa.

Vamos definir a função $g(a, b) = N$ como o maior inteiro positivo para o qual a equação $ax + by = N$ *não tem* solução não-negativa. O problema de determinar $g(a, b)$ é conhecido como o *Problema do Troco de Frobenius* (ou *Problema das Moedas de Frobenius*) para duas incógnitas. De modo geral, supondo que tenhamos moedas que valem $a_1, \ldots, a_n$ centavos, com $mdc(a_1, \ldots, a_n) = 1$, o problema consiste em determinar o maior valor que não pode ser pago exatamente utilizando apenas essas moedas.

Para o caso de duas incógnitas, é conhecida uma solução explícita, expressa na seguinte fórmula, descoberta por James Joseph Sylvester em 1882:

$$g(a, b) = ab - a - b$$

Para o caso $n = 3$ também se conhece uma solução explícita, porém inviável para o cálculo manual. Para $n \geq 4$, ainda não se conhecem soluções explícitas do problema de Frobenius, embora sejam conhecidas algumas estimativas de limite superior.

Equações Diofantinas não Lineares

Em algumas equações diofantinas, encontramos potências das incógnitas e eventualmente produto entre incógnitas diferentes. Estes casos em geral exigem variadas estratégias de resolução. Uma das mais comuns consiste conseguir isolar uma constante k que possa ser escrita como produto de parcelas inteiras dadas pelas incógnitas, como no exemplo a seguir:

Exemplo 5.3. Sejam p e q dois números primos distintos. Encontre as soluções inteiras positivas da equação:

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{pq}$$

Neste caso, o problema equivale a determinar as soluções estritamente positivas de:

$$xpq + ypq = xy$$

Note que a equação diofantina acima é não-linear, uma vez que temos o produto entre as duas incógnitas na equação. Porém, neste caso, podemos reescrever a equação das seguintes maneiras:

$$\begin{aligned} 0 &= xy - xpq - ypq \\ p^2q^2 &= xy - xpq - ypq + (p^2q^2) \\ p^2q^2 &= (x - pq)(y - pq) \end{aligned}$$

Note que agora nós conseguimos escrever p^2q^2 como produto constante das parcelas inteiras $(x - pq)$ e $(y - pq)$. Como p^2q^2 tem exatamente 9 divisores positivos, basta encontrarmos as soluções do sistema:

$$\begin{cases} x - pq = d \\ y - pq = \frac{p^2q^2}{d} \end{cases}$$

em que $d \in \{1, p, q, p^2, pq, q^2, p^2q, pq^2, p^2q^2\}$, o que nos dá as soluções:

$(pq + 1, pq(pq + 1))$	$(p(q + 1), pq(q + 1))$	$(q(p + 1), pq(p + 1))$
$(p(p + q), q(p + q))$	$(2pq, 2pq)$	$(q(p + q), p(p + q))$
$(pq(p + 1), q(p + 1))$	$(pq(q + 1), p(q + 1))$	$(pq(pq + 1), pq + 1)$

Problemas Propostos

Os problemas estão classificados por nível de dificuldade:

●	▲	♦	★
Fácil	Médio	Difícil	Desafio

1. ● Encontre a solução geral das seguintes equações diofantinas:

   - 2x + 3y = 9

- 8x + 7y = 3
- -26x + 39y = 65
- 12x + 27y = 33

2. ● Determinar, quando existem, as soluções não-negativas das equações diofantinas:

   - 123x + 360y = 99
   - 30x + 17y = 300

3. ● Para cada $c \in \{12, 13, \ldots, 18\}$ calcule uma solução não-negativa da equação diofantina $7x+3y = c$. Conclua que para todo $N \geq 12$, a equação diofantina $7x + 3y = N$ admite uma solução não-negativa

4. ● Encontre frações de denominadores 11 e 13 respectivamente, cuja soma seja $\frac{67}{143}$.

5. ● Determine todas as maneiras de escrever 270 como soma entre um múltiplo positivo de 9 e um múltiplo positivo de 11.

6. ● Escreva o número 100 como soma de dois números positivos tais que um deles seja múltiplo de 7 e o outro múltiplo de 11.

7. ▲ Conclua a demonstração da Proposição 2.

8. ▲ Determine o menor inteiro positivo que tem resto 9 na divisão por 37 e resto 15 na divisão por 52.

9. ▲ Uma loja de discos compra exemplares de um determinado CD e exemplares de um determinado DVD. Se cada CD sai por R$12,00 e cada DVD por R$20,00, qual o maior número de unidades que a loja pode comprar com R$860,00? Quantos DVDs e quantos CDs?

10. ▲ Uma certa quantidade de maçãs é dividida em 37 montes de igual número. Após serem retiradas 17 frutas, as restantes são acondicionadas em 79 caixas, cada uma com a mesma

quantidade. Quantas maçãs foram colocadas em cada caixa? Quantas havia em cada monte?

11. ▲ Encontre todos os inteiros estritamente positivos com a seguinte propriedade: fornecem resto 6 quando divididos por 11 e resto 3 quando divididos por 7.

12. ▲ Somando-se um certo númeor $6x$ com um certo numero $9y$, obtém-se 126. Se x e y forem trocados, obtém-se a soma 114. Determine os valores de x e y.

13. ♦ Prove que a equação diofantina linear a três incógnitas, dada por $a_1x + a_2y + a_3z = b$, onde a_1, a_2, a_3 são inteiros não-nulos, tem solução se, e somente se, $d = mdc(a_1, a_2, a_3)$ divide b

14. ♦ Encontre uma solução para equação diofantina abaixo:

$$21x + 33y + 77z = 1$$

15. ♦ Sejam $a, b > 0$ tais que $mdc(a, b) = 1$. Prove que $ax - by = c$ tem infinitas soluções positivas.

16. ♦ Um pescador tenta pescar um cardume jogando diversas redes na água. Se cair exatamente um peixe em cada rede, salvam-se ainda n peixes. Se caírem n peixes em cada rede, sobram n redes vazias. Quantas são as redes? Quantos são os peixes?

17. ♦ Qual o menor valor de c para o qual a equação $9x + 13y = c$ tem pelo menos duas soluções estritamente positivas, isto é $x > 0$ e $y > 0$?

18. ♦ (KöMaL) Sejam p, q números primos distintos. Determine os pares de inteiros positivos (x, y) que satisfazem a equação:

$$\frac{p}{x} + \frac{q}{y} = 1$$

19. ★ Sejam a e b inteiros positivos tais que $mdc(a, b) = 1$.

- Prove que, para todo $N > ab-a-b$, a equação diofantina $ax + by = N$ tem solução não negativa.
- Prove que não existe solução não negativa para $ax+by = ab - a - b$.

Deduza dos itens acima a fórmula de Sylvester.

20. ★ Seja k um primo. Prove que a equação $x^4 + 4y^4 = k$ tem solução inteira se, e somente se, $k = 5$. Nesse caso, determinar suas soluções.

Aula 6

Congruências

Congruências

Definição 6.1. Seja R uma relação no conjunto X. Diremos que R é uma relação de equivalência se as seguintes propriedades forem satisfeitas:

(i) (Propriedade reflexiva) xRx, para todo $x \in X$;

(ii) (Propriedade simétrica) Se xRy, então yRx;

(iii) (Propriedade transitiva) Se xRy e yRz, então xRz.

No nosso contexto, iremos escrever a relação de equivalência R por $\equiv$. Observe que a classe de equivalência de um certo elemento x em X é um subconjunto de X. E iremos defini-lo do seguinte modo:

$$\overline{x} = \{y \in X | x \equiv y\}$$

Ou seja, no conjunto $\overline{x}$ teremos todos os elementos de X que se relacionam com x.

Proposição 6.1. Seja X um conjunto e considere $\equiv$ uma relação de equivalência em X. Se x,$y \in X$, então as afirmações abaixo são equivalentes:

(i) $x \equiv y$

(ii) $\overline{x} = \overline{y}$

(iii) $x \in \overline{y}$

Demonstração. (i) $\Longrightarrow$ (ii)

Hipótese: $x \equiv y$

Desejamos mostrar que $\overline{x} = \overline{y}$, para isso basta verificarmos que $\overline{x} \subset \overline{y}$.

De fato, dado $z \in \overline{x} \implies z \equiv x$. Por hipótese, temos que $x \equiv y$. E pela propriedade transitiva, segue que $z \equiv y$, o que implica $z \in \overline{y}$. Ou seja, $\overline{x} \subset \overline{y}$.

De maneira análoga, decorre que $\overline{y} \subset \overline{x}$.

(ii) $\Longrightarrow$ (iii)

Hipótese: $\overline{x} = \overline{y}$

Pela propriedade reflexiva temos que $x \in \overline{x}$, como $\overline{x} = \overline{y}$ decorre imediatamente que $x \in \overline{y}$.

(iii) $\Longrightarrow$ (i)

Hipótese: $x \in \overline{y}$

Segue da definição de equivalência.

As demais implicações são imediatas e deixaremos como exercício para o leitor. ■

Definição 6.2. Dado um inteiro m positivo fixo. Dizemos que os

inteiros a e b são **congruentes** módulo m, se $m|(a-b)$.

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

Consideremos alguns exemplos. $191 \equiv 58 \pmod{7}$ pois $191 - 58 = 133 = 7 \cdot 19$, porém 8 e 3 não são congruentes módulo 2 pois $8 - 3 = 5$ e 2 não divide 5.

Como veremos na proposição seguinte, a congruência é uma relação de equivalência e, portanto, assume as propriedades vistas na Definição 1: reflexiva, simétrica e transitiva.

Proposição 6.2. A relação de congruência módulo m é uma relação de equivalência em $\mathbb{Z}$.

Demonstração. É imediato que $a \equiv a \pmod{m}$ e que, se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

Resta provar que, se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$. De fato, temos que $m|(a-b)$ e $m|(b-c)$, logo, pelas propriedades de divisibilidade, $m|((a-b)+(b-c))$, o que equivale a afirmar $m|(a-c)$, e, portanto $a \equiv c \pmod{m}$. ■

A relação de congruência possui muitas propriedades boas com relação a somas, produtos e potências. Tais propriedades são dadas pelo seguinte teorema.

Teorema 6.1. Se $x \equiv y \pmod{m}$ e $z \equiv w \pmod{m}$. Então:

(i) $x + z \equiv y + w \pmod{m}$

(ii) $x - z \equiv y - w \pmod{m}$

(iii) $kx \equiv ky \pmod{m}$, $\forall k \in \mathbb{Z}$

(iv) $xz \equiv yw \pmod{m}$

(v) $x^k \equiv y^k \pmod{m}$, $\forall k \in \mathbb{N}$

Demonstração. (i) Por hipótese, temos que $x \equiv y \pmod{m} \Leftrightarrow m|x-y$ e $z \equiv w \pmod{m} \Leftrightarrow m|z-w$. Pelas propriedades de divisibilidade, segue que $m|(x-y)+(z-w) = (x+z)-(y+w)$. Por definição de congruência módulo m, segue que $x+z \equiv y+w \pmod{m}$.

(ii) Observe que $z \equiv w \pmod{m} \Leftrightarrow m|z-w \implies m|(-1)(z-w) = w-z$

Como $m|x-y$, decorre que $m|(x-y)+(w-z) = (x-z)+(w-y) = (x-z)+(-1)(y-w) = (x-z)-(y-w) \Leftrightarrow x-z \equiv y-w \pmod{m}$

(iii) Note que $x \equiv y \pmod{m} \Leftrightarrow m|x-y \implies m|k(x-y)$, com $k \in \mathbb{Z} \implies m|kx-ky \Leftrightarrow kx \equiv ky \pmod{m}$.

(iv) Como $x \equiv y \pmod{m} \Leftrightarrow m|x-y \Leftrightarrow \exists q_1 \in \mathbb{Z}$, tal que $x-y = mq_1 \implies x = mq_1 + y$. Da mesma forma, temos que $z = mq_2 + w$, com $q_2 \in \mathbb{Z}$.

Logo, $xz = (mq_1+y)(mq_2+w) = m^2q_1q_2+mq_1w+ymq_2+yw = yw + m(mq_1q_2 + q_1w + yq_2)$

$\implies xz = yw+m(mq_1q_2+q_1w+yq_2)$, com $(mq_1q_2+q_1w+yq_2) \in \mathbb{Z}$.

E, portanto, $m|xz-yw \Leftrightarrow xz \equiv yw \pmod{m}$.

(v) A prova deste item será feita por indução em k.

Para $k = 2$, basta usar o item (iv) tomando $z = x$ e $w = y$. Dessa forma temos que $x^2 \equiv y^2 \pmod{m}$, verificando assim o primeiro passo da indução.

Agora, suponha que vale para algum $n \in \mathbb{N}$ e vejamos que vale também para $n+1$.

De fato, pela hipótese de indução temos que $x^n \equiv y^n \pmod{m}$ e além disso sabemos que $x \equiv y \pmod{m}$. Usando novamente o item (iv) nessas duas últimas congruências, decorre que:

$$x^n x \equiv y^n y \pmod{m} \Leftrightarrow x^{n+1} \equiv y^{n+1} \pmod{m}$$

■

Este último teorema essencialmente nos diz que a congruência módulo m é compatível com as operaçãoes em $\mathbb{Z}$.

Uma outra caracterização para a noção de congruências é dado pela seguinte propriedade:

Proposição 6.3. Dado m um inteiro fixo. Dois inteiros x,y são congruente módulo m se, e somente se, eles possuem como resto o mesmo inteiro quando dividmos por m.

Demonstração. Dados

$x = mq_1 + r_1$, com $0 \leq r_1 < m$

$y = mq_2 + r_2$, com $0 \leq r_2 < m$

Então, $x - y = m(q_1 - q_2) + (r_1 - r_2)$. Assim, $m|x-y \Leftrightarrow m|r_1 - r_2$.

Como $0 \leq r_1 < m$ e $0 \leq r_2 < m$, segue que $0 \leq |r_1 - r_2| < m$. E, portanto, $m|r_1 - r_2$ se, e somente se, $r_1 - r_2 = 0$. Ou seja, apenas se $r_1 = r_2$. ■

Calcular dígitos e restos de divisão, em geral, é facilitado pelas propriedades de congruência, como ilustramos com os próximos exemplos.

Exemplo 6.1. Calcule os restos de 4^{100} por 3 e 4^{100} por 5.

Como $4 \equiv 1 \pmod 3$ segue que $4^{100} \equiv 1^{100} = 1 \pmod 3$.

Logo, $4^{100} - 1 = 3k$ e portanto $4^{100} = 3k + 1$ e o resto é 1.

Do mesmo modo $4 \equiv -1 \pmod 5$, ou seja $4^{100} \equiv (-1)^{100} = 1 \pmod 5$ e o resto também é 1.

Exemplo 6.2. Encontre o último algarismo de $3^{70} + 7^{70}$.

Sabemos que $3^4 = 81 \equiv 1 \pmod{10}$ e $70 = 4 \cdot 17 + 2$. Assim,

$$3^{70} = 3^{4 \cdot 17} \cdot 3^2 \equiv 1 \cdot 3^2 = 9 \pmod{10}.$$

Além disso $7^2 = 49 \equiv -1 \pmod{10}$, logo como $70 = 2 \cdot 35$ temos

$$7^{70} = (7^2)^{35} \equiv (-1)^{35} = -1 \pmod{10}.$$

Assim $3^{70} + 7^{70} \equiv 9 - 1 = 8 (\mathrm{mod}\, 10)$ e portanto o último algarismo de $3^{70} + 7^{70}$ é 8.

Um teorema muito útil para resolver exercicios é o seguinte:

Teorema 6.2. Seja n um número inteiro e denote por $d(n)$ a soma dos algarismos de n. Então

$$n \equiv d(n) (\mathrm{mod}\, 9)$$

Problemas Propostos

Os problemas estão classificados por nível de dificuldade:

●	▲	♦	★
Fácil	Médio	Difícil	Desafio

1. ● Prove o critério de divisibilidade por 3.

2. ● Mostre que:

$$x \equiv y (\mathrm{mod}\, m) \Leftrightarrow x + k \equiv y + k (\mathrm{mod}\, m), \forall k \in \mathbb{Z}$$

3. ● Mostre que a relação de congruência módulo m é uma relação de equivalência em $\mathbb{Z}$.

4. ● Prove que $20^{15} - 1$ é divisível por 11.31.61

5. ● Sejam x,$y \in \mathbb{Z}$ com a relação de equivalência módulo m, mostre que:
$$\overline{x} \neq \overline{y} \implies \overline{x} \cap \overline{y} = \{\}$$

6. ▲ Sejam x,y e z inteiros arbitrários e m um inteiro fixo.

   Mostre que: se $\text{mdc}(z, m) = 1$, então $xz \equiv yz (\text{mod}\, m) \implies x \equiv y (\text{mod}\, m)$

7. ▲ Calcule o resto de $34 \cdot 35 \cdot 36 \cdot 37 + 5! - 423$ por 6.

8. ▲ Calcule o resto de 5^{60} por 26.

9. ▲ Calcule o resto de 4^{100} por 7.

10. ▲ Prove que $2222^{5555} + 5555^{2222}$ é divisível por 7.

11. ▲ Prove que $n^5 + 4n$ é divisível por 5 para todo inteiro n.

12. ▲ Prove que $11^{n+2} + 12^{2n+1}$ é divísivel por 133 para qualquer n natural.

13. ◆ Prove o critério de divisibilidade por 11.

14. ◆ Prove que não existem inteiros $x_1, \ldots, x_{14}$ tais que:
$$x_1^4 + \ldots + x_{14}^4 = 1599$$

15. ◆ Escreva uma única congruência que é equivalente à um par de congruências $x \equiv 1 (\text{mod}\, 4)$ e $x \equiv 2 (\text{mod}\, 3)$.

16. ◆ Mostre que se n divide um número de Fibonacci, então divide uma infinidade.

17. ♦ Mostre que o quadrado de um inteiro é da forma $3k$ ou $3k+1$.

18. ♦ Prove que $3x^2 + 2 = y^2$ não tem solução em $\mathbb{Z}$.

19. ★ **Afirmação de Fermat:** Todo número na forma $F_n = 2^{2^n} + 1$ é primo.

    Prove que a afirmação é falsa para $n = 5$.

    Dica: Euler provou que F_5 é divisível por 641.

20. ★ Seja $d(n)$ a soma dos dígitos de n. Suponha que $n + d(n) + d(d(n)) = 1995$. Quais os possíveis restos da divisão de n por 9?

Aula 7

Teorema Chinês do Resto

Teorema Chinês do Resto Sejam n_1,n_2,n_3,$\cdots$,n_k números inteiros positivos tais que $\text{mdc}(n_i, n_j) = 1$, para $i \neq j$, e sejam $a_1.a_2$,a_3,$\cdots$,a_k inteiros arbitrários. Então, o sistema de congruências lineares

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ x \equiv a_3 \pmod{n_3} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

admite solução, que é única módulo $n = n_1 n_2 n_3 \cdots n_k$.

Demonstração. Considerando $n = n_1 n_2 n_3 \cdots n_k$, tome $N_i = \frac{n}{n_i}$.

Observe que $N_i = n_1 n_2 n_3 \cdots n_{i-1} n_{i+1} \cdots n_k$, ou seja, N_i é o produto de todos os inteiros n_1,n_2,n_3,$\cdots$,n_k, omitindo o próprio n_i.

Pela hipótese do teorema, temos que os esses n_j são relativamente primos com n_i. E, portanto, têm-se que $\text{mdc}(N_i, n_i) = 1$.

Dessa forma, conseguimos determinar os inteiros r_i,s_i tais que

$$r_i N_i + s_i n_i = 1 \tag{7.1}$$

com $1 \leq i \leq k$.

Iremos mostrar que

$$x_0 = a_1 r_1 N_1 + a_2 r_2 N_2 + \cdots + a_k r_k N_k$$

é uma solução para o sistema dado.

De fato, observe primeiramente que se $i \neq j$, temos que

$$N_j = n_1 n_2 n_3 \cdots n_i \cdots n_{j-1} n_{j+1} \cdots n_k \equiv 0 \pmod{n_i}$$

pois n_i é um dos fatores de N_j.

Segue imediatamente pelas propriedades de congruência que

$$a_j r_j N_j \equiv 0 \pmod{n_i}$$

O que acaba implicando

$$x_0 = a_1 r_1 N_1 + a_2 r_2 N_2 + \cdots + a_i r_i N_i + \cdots + a_k r_k N_k \equiv a_i r_i N_i \pmod{n_i}$$

$$\implies x_0 \equiv a_i r_i N_i \pmod{n_i} \tag{7.2}$$

Voltando na equação (1), note que

$s_i n_i = 1 - r_i N_i \implies n_i | 1 - r_i N_i \implies n_i | (-1)(1 - r_i N_i) \Leftrightarrow n_i | r_i N_i - 1$.

Pela definição de congruência, segue que

$$r_i N_i \equiv 1 \pmod{n_i} \tag{7.3}$$

Substituindo a congruência (3) em (2), decorre que

$$x_0 \equiv a_i \pmod{n_i}$$

E, portanto, x_0 é solução da equação $x \equiv a_i \pmod{n_i}$ para cada i, consequentemente, é uma solução do sistema.

Agora, basta verificarmos que essa solução é única.

Para isso, considere $\overline{x}$ solução do sistema. Ou seja, $\overline{x} \equiv a_i \pmod{n_i}$, para cada $1 \leq i \leq k$. Também temos x_0 solução, ou seja, $x_0 \equiv a_i \pmod{n_i}$.

Da propriedade transitiva de congruências, segue que $\overline{x} \equiv x_0 \pmod{n_i}$, isto é, $n_i | \overline{x} - x_0$, para cada $1 \leq i \leq k$. Comos os inteiros $n_1, n_2, n_3, \cdots, n_k$ são relativamente primos entre si, temos que $n_1 n_2 \cdots n_k | (\overline{x} - x_0)$, o que implica

$$\overline{x} \equiv x_0 \pmod{n}.$$

■

Exemplo 7.1. Resolva o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Solução:

Na forma como esta distribuída no Teorema Chinês do Restos, temos que:

$n = 3 \cdot 5 \cdot 7 = 105$

$a_1 = 2$, $a_2 = 3$ e $a_3 = 2$

$n_1 = 3$, $n_2 = 5$ e $n_3 = 7$

$\Longrightarrow N_1 = \frac{n}{n_1} = \frac{3 \cdot 5 \cdot 7}{3} = 5 \cdot 7 = 35$

$\Longrightarrow N_2 = \frac{n}{n_2} = \frac{3 \cdot 5 \cdot 7}{5} = 3 \cdot 7 = 21$

$\Longrightarrow N_3 = \frac{n}{n_3} = \frac{3 \cdot 5 \cdot 7}{7} = 3 \cdot 5 = 15$

Na demonstração do teorema, em algum momento nos deparamos com a seguinte congruência:

$$r_i N_i \equiv 1 \pmod{n_i}$$

.

No caso $i = 1$, devemos encontrar r_1,s_1 tais que:

$$r_1 \cdot N_1 + s_1 \cdot n_1 = 1 \Leftrightarrow r_1 \cdot 35 + s_1 \cdot 3 = 1$$

Para determinar os valores r_1 e s_1 iremos usar o método visto na aula 2. Primeiro, fazemos divisões sucessivas usando o Algoritmo de Euclides:

$35 = 3 \cdot 11 + 2$

$3 = 2 \cdot 1 + 1$

Em seguida isolamos os restos:

$$2 = 35 - 3 \cdot 11 \tag{7.4}$$

$$1 = 3 - 2 \tag{7.5}$$

Substituindo a equação (4) em (5), decorre que:

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

$\implies (-1)\cdot 35+12\cdot 3=1$

E, portanto, $r_1=-1$ e $s_1=12$.

Agora observando a congruência $r_2N_2 \equiv 1(\mathrm{mod}\, n_2)$, desejamos encontrar inteiros r_2 e s_2 tais que

$$r_2\cdot 21+s_2\cdot 5=1$$

Note que, $21=5\cdot 4+1 \implies 1\cdot 21+(-4)\cdot 5=1$

Assim, $r_2=1$ e $s_2=4$.

Enfim, considerando a congruência $r_3N_3 \equiv 1(\mathrm{mod}\, n_3)$, temos que:

$$r_3\cdot 15+s_3\cdot 7=1$$

Onde, $15=7\cdot 2+1 \implies 1\cdot 15+(-2)\cdot 7=1$.

Logo, $r_3=1$ e $s_3=-2$.

Como vimos na demonstração do teorema, x_0 é solução do sistema dado, onde

$$x_0=a_1r_1N_1+a_2r_2N_2+a_3r_3N_3=2\cdot(-1)\cdot 35+3\cdot 1\cdot 21+2\cdot 1\cdot 15=23$$

$\implies x_0=23$.

De fato x_0 é solução do sistema dado, pois:

$$x_0=23=21+2\equiv 0+2\equiv 2\ (\mathrm{mod}\, 3)$$

$x_0 = 23 = 20 + 3 \equiv 0 + 3 \equiv 3 \pmod 5$

$x_0 = 23 = 21 + 2 \equiv 0 + 2 \equiv 2 \pmod 7$

É fácil verificar que $\overline{x} = 233$ também é uma solução do sistema, logo

$$\overline{x} \equiv x_0 \pmod{105}.$$

Problemas Propostos

Os problemas estão classificados por nível de dificuldade:

●	▲	♦	★
Fácil	Médio	Difícil	Desafio

1. ● Resolva o sistema de congruências lineares dado a seguir:

$$\begin{cases} x \equiv 2 \pmod 2 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

2. ● Resolva o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv -1 \pmod 4 \\ x \equiv 2 \pmod 6). \end{cases}$$

3. ● Verifique que o seguinte sistema não possui solução:

$$\begin{cases} x \equiv 8 \pmod{12} \\ x \equiv 6 \pmod 9) \end{cases}$$

Por que isso não contradiz o Teorema Chinês do Resto?

4. ● Mostre que o seguinte sistema não possui solução.

$$\begin{cases} x \equiv -1 \pmod 4 \\ x \equiv 2 \pmod 6 \end{cases}$$

5. ▲ Resolva o seguinte sistema linear e determine a sua menor solução positiva:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

6. ▲ Resolva de maneira análoga ao último exercício com o seguinte sistema linear:

$$\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod 7 \end{cases}$$

7. ▲ Usando congruências, resolva as seguintes equações diofantinas:

   - $4x + 51y = 9$
   - $12x + 25y = 331$

8. ▲ Determine todos os números naturais menores que 1000 que possuem como restos 9, na divisão por 37, e 15, na divisão por 52.

9. ▲ Ache x inteiro que satisfaça simultaneamente as congruências:

$$\begin{cases} x \equiv 2 \pmod 5 \\ 3x \equiv 1 \pmod 8 \end{cases}$$

10. ▲ Encontre uma solução geral do seguinte sistema de congruências lineares:

$$\begin{cases} 6x \equiv 2 \pmod 4 \\ 2x \equiv 1 \pmod 3 \\ 4x \equiv 2 \pmod 7 \end{cases}$$

11. ♦ Encontre o menor $a > 100$ tal que $2|a$, $3|(a+1)$, $4|(a+2)$, $5|(a+3)$ e $6|(a+4)$.

12. ♦ Um certo inteiro n é tal que tem restos 1 e 7 na divisão por 15 e 21 respectivamente. Qual seu resto na divisão por 35?

13. ♦Determine todas as soluções da congruência linear $3x - 7y \equiv 11 \pmod{11}$.

14. ♦ Resolva a congruência linear $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$.

15. ★ Prove que as congruências $x \equiv a \pmod n$ e $x \equiv b \pmod m$ possuem uma solução em comum se, e somente se, $\text{mdc}(m,n)|(a-b)$.

16. ★ Suponha que $\text{mdc}(m,n) = 1$ e prove que a solução do item anterior é única módulo $\text{mmc}(m,n)$.

Aula 8

Pequeno Teorema de Fermat

No ano de 1640, Pierre de Fermat afirmou em correspondência que, se um número a não divisível por um primo p, então p divide $a^{p-1} - 1$. Como aconteceu com várias afirmações de Fermat, não se conhece uma prova apresentada por ele próprio. Esse resultado, que posteriormente ficou conhecido como o Pequeno Teorema de Fermat, pode ser formulado em linguagem de aritmética modular da seguinte maneira:

Teorema 8.1 (Pequeno Teorema de Fermat)**.** Sejam p um número primo e a um inteiro não divisível por p. Então:

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

Demonstração. Inicialmente, vamos observar o seguinte conjunto:

$$A = \{a, 2a, 3a, \ldots, (p-1)a\}.$$

Se tomamos quaisquer dois elementos desse conjunto, temos que eles *não* são congruentes entre si módulo p. Se tivermos $xa \equiv ya(mod\ p)$, para $1 \leq x, y \leq p-1$, como $mdc(a, p) = 1$, podemos cancelar a os dois lados da congruência , e obtemos $x \equiv y (\mathrm{mod}\ p)$.

Como x, y são possíveis restos distintos da divisão por p, suas classes de congruência são necessariamente iguais, logo $x = y$. Também temos que nenhum elemento de A é congruente a 0 módulo p, pois para $xa \in A$, tanto x quanto a são relativamente primos a p.

Assim sendo, para alguma reordenação $x_1, x_2, \ldots, x_{p-1}$ dos inteiros $1, 2, \ldots, p-1$, encontramos as seguintes congruências:

$$\begin{aligned} a &\equiv x_1 (mod\ p) \\ 2a &\equiv x_2 (mod\ p) \\ &\vdots \\ (p-1)a &\equiv x_{p-1} (mod\ p). \end{aligned}$$

A partir disso, podemos simplesmente multiplicar todos os elementos de cada lado, e a congruência se mantém. Como todos os números entre 1 e $p-1$ ocorrem em cada lado, o resultado da nossa multiplicação será:

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

Por fim, como $(p-1)!$ é um produto de números coprimos com p, esse fatorial pode ser cancelado em ambos os lados da congruência. Isso nos dá o resultado:

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

■

Como consequência imediata desse teorema, é fácil verificar o seguinte resultado.

Corolário 8.1. Sejam p um número primo e a um inteiro qualquer. Então:

$$a^p \equiv a (\mathrm{mod}\, p)$$

O Pequeno Teorema de Fermat é bastante útil para provar alguns resultados envolvendo divisibilidade, como nos exemplos a seguir:

Exemplo 8.1. Seja a um número inteiro qualquer. Então a^{n+4} tem o mesmo algarismo das unidades que a^n.

De fato, basta mostrar que a^5 tem o mesmo algarismo das unidades que a, ou, na forma de congruências $a^5 \equiv a(\mathrm{mod}\, 10)$. Mostraremos que a congruência vale para cada um dos fatores primos de 10.

A congruência $a^5 \equiv a(\mathrm{mod}\, 5)$ se segue imediatamente do Corolário. Por sua vez, como a^5 e a são ou ambos ímpares ou ambos pares, sua diferença é par, e portanto $a^5 \equiv a(\mathrm{mod}\, 2)$. Como $mdc(2, 5) = 1$, segue-se que $a^5 \equiv a(\mathrm{mod}\, 10)$.

Exemplo 8.2. Sejam a e b inteiros, e p um número primo. Então, tem-se que:

$$(a + b)^p \equiv a^p + b^p(\mathrm{mod}\, p)$$

De fato, aplicando o Pequeno Teorema de Fermat primeiro em $(a + b)$ e depois em a e b individualmente, obtemos:

$$(a + b)^p \equiv a + b \equiv a^p + b^p(\mathrm{mod}\, p)$$

A primeira prova publicada do Pequeno Teorema de Fermat se deve a Euler, que posteriormente generalizou o resultado para qualquer número natural. Contudo, antes de apresentar tal generalização, será necessário definir uma função sobre os números naturais, chamada *função totiente de Euler* ou ainda *função phi de Euler*.

Definição 8.1 (Função Totiente de Euler)**.** A função $\phi : \mathbb{N}^* \to \mathbb{N}^*$ que associa cada inteiro positivo n à quantidade de números menores ou iguais a n que são coprimos com ele é denominada **Função Totiente de Euler**

Assim, por exemplo, $\phi(8) = 4$, pois ao listarmos os números de 1 a 8, encontramos precisamente 4 números coprimos com relação a 8: $1, 3, 5$ e 7.

Para qualquer número primo p, podemos constatar facilmente que $\phi(p) = p - 1$, pois de 1 a p, temos que apenas precisamente p não é coprimo consigo próprio. Também podemos calcular o valor de $\phi(p^k)$ para qualquer potência k. De fato, como $mdc(p, n) \neq 1 \iff$

$p|n$, basta contar a quantidade de múltiplos de p entre 1 e p^k, que é dada por exatamente p^{k-1} números. Logo $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

A proposição seguinte, que enunciaremos aqui sem demonstrar, permite generalizar $\phi(n)$ para qualquer inteiro positivo n

Proposição 8.1. Se m e n são inteiros positivos e $mdc(m,n) = 1$, então:

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n)$$

Exemplo 8.3. Vamos supor $m = 4, n = 5$. Queremos calcular $\phi(20)$. Podemos verificar que $\phi(4) = 2, \phi(5) = 4$, logo $\phi(20) = \phi(4) \cdot \phi(5) = 8$. De fato, podemos verificar o resultado dispondo os números em uma tabela $m \times n$:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20

Retirando os números sublinhados, que não são coprimos com 20, obtemos exatamente 8 números: $1, 3, 7, 9, 11, 13, 17$ e 19.

Definida a função totiente de Euler, estamos prontos para enunciar o Teorema de Euler, que é a generalização do Pequeno Teorema de Fermat para os números naturais:

Teorema 8.2 (Teorema de Euler)**.** Sejam $m > 1$ e $a \in \mathbb{Z}$ tal que $mdc(a,m) = 1$. Então:

$$a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$$

.

Demonstração. Sejam $s_1, \ldots, s_{\phi(m)}$ os inteiros de 1 a m que são relativamente primos a m. Dividindo cada $a \cdot s_i$ por m, podemos escrever:

$$a \cdot s_i = m \cdot q_i + r_i, 0 \leq 1 r_i < m$$

Se existisse algum primo p divisor comum de m e r_i, teríamos que $p|a \cdot s_i$. Então teríamos $p|a$ ou $p|s_i$, o que contradiz a hipótese $mdc(a,m) = 1$ bem como $mdc(s_i,m) = 1$. Logo, para cada $i, 1 \leq i \leq \phi(m)$ temos que $mdc(r_i,m) = 1$.

Mostremos agora que, para cada $i \neq j, r_i \neq r_j$. Supondo $i \neq j$ e $r_i = r_j$, teríamos $a \cdot s_i - m \cdot q_i = a \cdot s_j - m \cdot q_j$, o que implica $a(s_i - s_j) = m(q_i - q_j)$. Como $mdc(a,m) = 1$ temos que $m|(s_i - s_j)$, mas como $1 \leq s_i, s_j \leq m$, a única possibilidade seria $s_i = s_j$, contradição.

Portanto, a menos reordenação, os conjuntos $\{s_1, \ldots, s_{\phi(m)}\}$ e $\{r_1, \ldots, r_{\phi(m)}\}$ são iguais. Assim, se multiplicarmos todas as congruências $a \cdot s_i \equiv r_i (\mathrm{mod}\, m)$, obtemos:

$$a^{\phi(m)} \cdot s_i \cdot \ldots \cdot s_{\phi(m)} \equiv r_1 \cdot \ldots \cdot r_{\phi(m)} (\mathrm{mod}\, m)$$

Como os produtos $s_i \cdot \ldots \cdot s_{\phi(m)}$ e $r_1 \cdot \ldots \cdot r_{\phi(m)}$ são iguais, e m é relativamente primo a cada r_i, temos que $mdc(m, r_1 \cdot \ldots \cdot r_{\phi(m)}) = 1$. Assim sendo, podemos cancelar este produto em ambos os lados da congruência, e disso obtemos o resultado:

$$a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$$

.

■

Exemplo 8.4. Encontre os últimos 2 dígitos de 3^{1000}.

Neste exemplo, como $\phi(100) = \phi(5^2) \cdot \phi(2^2) = 20 \cdot 2 = 40$, pelo Teorema de Euler $3^{40} \equiv 1 (\mathrm{mod}\, 100)$. Logo:

$$3^{1000} \equiv (3^{40})^{25} \equiv 1^{25} \equiv 1 (\mathrm{mod}\, 100)$$

Logo, os últimos dígitos são 01.

Problemas Propostos

Os problemas estão classificados por nível de dificuldade:

●	▲	♦	★
Fácil	Médio	Difícil	Desafio

1. ● Calcule x em cada congruência abaixo usando o Teorema de Euler:

   - $3^{1000} \equiv x (\mathrm{mod}\, 7)$
   - $7^{1000} \equiv x (\mathrm{mod}\, 54)$

2. ● Seja a um inteiro. Prove que:

   Se $mdc(a, 35) = 1$, então $a^{12} \equiv 1 (\mathrm{mod}\, 35)$.

3. ● Calcule $\phi(200), \phi(860), \phi(1001)$.

4. ● Sejam a e b inteiros e p um primo tal que $mdc(a, p) = 1$. Verifique que uma solução da congruência $ax \equiv b (\mathrm{mod}\, p)$ é dada por $x = a^{p-2}b$.

5. ▲ Seja $p > 2$ um número primo. Prove que $1^p + 2^p + \ldots + (p-1)^p \equiv 0 (\mathrm{mod}\, p)$.

6. ▲ Sejam a e n inteiros tais que $mdc(a, n) = mdc(a-1, n) = 1$. Prove que $1 + a + \ldots + a^{\phi(n)-1} \equiv 0 (\mathrm{mod}\, n)$.

7. ▲ Seja p um primo diferente de 2 e 5. Prove que p divide infinitos inteiros da sequência $1, 11, 111, 1111, \ldots$.

8. ▲ Se p é um primo ímpar, prove que $n^p \equiv n (\mathrm{mod}\, 2p)$ para todo inteiro n.

9. ▲ Se p é um primo ímpar e $p | m^p + n^p$, prove que $p^2 | m^p + n^p$.

10. ▲ Seja n um inteiro positivo ímpar em cuja decomposição canônica figuram r fatores primos distintos. Prove que $2^r | \phi(n)$.

11. ♦ Prove que, se $d|n$, então $\phi(d)|\phi(n)$.

12. ♦ Seja $m > 1$ e sejam $p_1, p_2 \ldots p_r$ os divisores primos distintos de m. Prove que:

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

13. ♦ Seja $n > 1$ e considere o número $N = (n!)^2 + 1$. Prove que existe algum número primo p da forma $4k + 1$ tal que $p|N$. Conclua disso que existem infinitos primos da forma $4k + 1$.

14. ♦ Encontre os últimos dois dígitos de $7^{7^{1000}}$.

15. ♦ Encontre o resto de

$$10^{10} + 10^{10^2} + \ldots + 10^{10^{10}}$$

na divisão por 7.

16. ♦ (Putnam, 1972) Mostre que, dado um primo ímpar p, existem infinitos inteiros n tais que $p|n \cdot 2^n + 1$.

17. ♦ (Olimpíada Polonesa de Matemática, 2003) Encontre todos os polinômios W com coeficientes inteiros satisfazendo a seguinte condição: para todo natural n, $2^n - 1$ é divisível por $W(n)$.

18. ♦ (IMO shortlist, 2006) Para certo $x \in (0, 1)$, seja $y \in (0, 1)$ um número cujo n-ésimo dígito após a vírgula é o 2^n-ésimo dígito de x após a vírgula. Mostre que, se x é racional, então y também é.

19. ★ (IMO, 1984) Encontre um par de inteiros positivos a e b tais que:

- $ab(a + b)$ não é divisível por 7.
- $(a + b)^7 - a^7 - b^7$ é divisível por 7^7.

20. ★ (USAMO, 1982) Prove que existe algum inteiro k tal que, para todo n, $k \cdot 2^n + 1$ é composto.

Referências Bibliográficas

Teoria de Números

Aula 1

1. MILIES, C. P.; COELHO, S. P. *Números, Uma Introdução à Matemática*. 3a Edição. São Paulo: Editora da Universidade de São Paulo, 2013.

2. COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, 2013.

Aula 2

1. MILIES, C. P.; COELHO, S. P. *Números, Uma Introdução à Matemática*. 3a Edição. São Paulo: Editora da Universidade de São Paulo, 2013.

2. COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, 2013.

Aula 3

1. MILIES, C. P.; COELHO, S. P. *Números, Uma Introdução à Matemática*. 3a Edição. São Paulo: Editora da Universidade de São Paulo, 2013.

2. TEOREMA FUNDAMENTAL DA ARITMÉTICA. Disponível em:
<http://www.dma.uem.br/kit/arquivos/arquivos_pdf/teoremafundamentalaritmetica.pdf>.
Acesso em: 15 fev. 2020.

3. CLUBES DE MATEMÁTICA DA OBMEP. Disponível em: <http://clubes.obmep.org.br/blog/tfa-problemas/>. Acesso em: 10 fev. 2020.

Aula 4

1. MILIES, C. P.; COELHO, S. P. *Números, Uma Introdução à Matemática*. 3a Edição. São Paulo: Editora da Universidade de São Paulo, 2013.

2. COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, 2013.

3. PRIMOS DE FERMAT, PRIMOS DE MERSENNE, NÚMEROS PERFEITOS E O FATORIAL. Disponível em: <https://www.ime.unicamp.br/ ftorres/ENSINO/MONOGRAFIAS/Maicon_TN17M2.pdf>. Acesso em: 20 fev. 2020.

Aula 5

1. MILIES, C. P.; COELHO, S. P. *Números, Uma Introdução à Matemática*. 3a Edição. São Paulo: Editora da Universidade de São Paulo, 2013.

2. DOMINGUES, H. H. *Fundamentos de Aritmética*. 2a Edição revista. Florianópolis: Editora da UFSC, 2017.

3. ANDRESCU, T.; ANDRICA, D. *An Introduction to Diophantine Equations*. Zalau: GIL Publishing House, 2002.

Aula 6

1. MILIES, C. P.; COELHO, S. P. *Números, Uma Introdução à Matemática*. 3a Edição. São Paulo: Editora da Universidade de São Paulo, 2013.

2. GONÇALVES, A. *Introdução à álgebra*. Rio de Janeiro: Editora do IMPA, 2017.

Aula 7

1. MILIES, C. P.; COELHO, S. P. *Números, Uma Introdução à Matemática*. 3a Edição. São Paulo: Editora da Universidade de São Paulo, 2013.

2. GONÇALVES, A. *Introdução à álgebra*. Rio de Janeiro: Editora do IMPA, 2017.

Aula 8

1. MILIES, C. P.; COELHO, S. P. *Números, Uma Introdução à Matemática*. 3a Edição. São Paulo: Editora da Universidade de São Paulo, 2013.

2. DOMINGUES, H. H. *Fundamentos de Aritmética*. 2a Edição revista. Florianópolis: Editora da UFSC, 2017.