Listas de Teoria dos Números

Aluno: Henrique Lima Cardoso

January 15, 2026

Contents

0 Introdução

Ao decorrer do curso, vou escrever minhas resoluções dos exercícios nesse arquivo. Tem alguns motivos para isso:

1. Posso reutilizar resultados passados.
2. Está tudo organizado se um futuro henrique quiser rever.

O código fonte pode ser encontrado em `https://github.com/hnrq104/tn`.

1 Lista 1 - 12/1/2026

Problem 1.1. Dados inteiros positivos a, b e c, dois a dois primos entre si, demonstre que $2abc-ab-bc-ca$ é o maior número inteiro que não pode expressar-se na forma $xbc + yca + zab$ com x, y e z inteiros não negativos.

Proof. Note que como $(b, c) = 1$, temos que $(ab, ac) = a$ e, portanto por Bachét-Bezout existe solução para $z'ab + y'ca = a$ com z', y' inteiros. Por sua vez, como $(a, bc) = 1$, existe solução para $ma + nbc = 1$ com m, n inteiros. Juntando as duas equações, encontramos $mz'ab + my'ca + nbc = 1$ que é solução para a equação $xbc + yca + zab = 1$ e, portanto, temos soluções para $xbc + yca + zab = k$ para qualquer inteiro k.

Vamos mostrar que $2abc - ab - bc - ca$ não pode ser escrito como $xbc + yca + zab$ para $x, y, z \in \mathbb{N}$. Suponha, que conseguimos, temos

$$\begin{aligned} 2abc - ab - bc - ca &= xbc + yca + zab \\ 2abc &= (x+1)bc + (y+1)ca + (z+1)ab \end{aligned}$$

tomando a segunda equação módulo a, achamos

$$0 \equiv (x+1)bc \pmod a \Rightarrow x + 1 \equiv 0 \pmod a$$

ou seja, $a \mid (x + 1)$. Como $x \geqslant 0$, devemos ter $(x + 1) \geqslant a$. Simetricamente (tomando módulo b e depois c), sabemos que $(y + 1) \geqslant b$ e $(z + 1) \geqslant c$. Mas já encontramos contradição, uma vez que essas desigualdades implicam

$$(x+1)bc + (y+1)ca + (z+1)ab \geqslant abc + bca + cab = 3abc > 2abc$$

Agora seja $n > 2abc - bc - ac - ab$, mostraremos que existe solução natural para $n = xbc + yac + zab$. Primeiro, vamos caracterizar as soluções inteiras, que existem pela observação anterior. Note que se (x, y, z) e (x', y', z') são soluções, então

$$(x - x')bc + (y - y')ac + (z - z')ab = 0 \tag{1}$$

tomando a equação módulo a, vemos que $(x - x') \equiv 0 \pmod a$ e portanto $x' = x + ra$ para algum $r \in \mathbb{Z}$. Simetricamente, vemos que $y' = y + sb$ e $z' = z + tc$ para $s, t \in \mathbb{Z}$. Portanto, [1] se expressa como

$$(ra)bc + (sb)ac + (tc)ab = (r + s + t)abc = 0 \iff (r + s + t) = 0$$

Ou seja, se (x_0, y_0, z_0) é uma solução inicial, todas as outras soluções são da forma $(x_0 + ra, y_0 + sb, z_0 + tc)$ onde $r + s + t = 0$, é fácil ver que qualquer qualquer tripla dessa forma também satisfaz a equação original. Nosso problema se resume então a encontrar soluções inteiras (r, s, t) para a seguinte série de relações:

$$\begin{aligned} x_0 + ra &> -1 \\ y_0 + sb &> -1 \\ z_0 + tc &> -1 \\ r + s + t &= 0 \end{aligned}$$

Isolando as variáveis e escrevendo t como $-(r + s)$, temos

$$\begin{aligned} -\frac{(x_0+1)}{a} &< r \\ -\frac{(y_0+1)}{b} &< s \\ r + s &< \frac{(z_0+1)}{c} \end{aligned}$$

As duas primeiras desigualdades, implicam que

$$-\left(\frac{(x_0+1)}{a}+\frac{(y_0+1)}{b}\right)<r+s<\frac{(z_0+1)}{c}$$

Notamos (seguindo a resolução do livro para um problema similar) que

$$\frac{(z_0+1)}{c}--\left(\frac{(x_0+1)}{a}+\frac{(y_0+1)}{b}\right)=\frac{(z_0+1)}{c}+\frac{(x_0+1)}{a}+\frac{(y_0+1)}{b}=\frac{n+bc+ac+ab}{abc}>2$$

pois $n>2abc-bc-ac-ab$. Segue que o intervalo $\left(-\frac{(x_0+1)}{a}-\frac{(y_0+1)}{b},\frac{(z_0+1)}{c}\right)$ tem ao menos dois inteiros. Particularmente, os números

$$\left\lceil-\frac{(x_0+1)}{a}-\frac{(y_0+1)}{b}\right\rceil \quad \text{e} \quad \left\lceil-\frac{(x_0+1)}{a}-\frac{(y_0+1)}{b}\right\rceil+1$$

pertencem ao intervalo. Tomando

$$r=\begin{cases}\lceil-(x_0+1)/a\rceil & \text{se } -(x_0+1)/a\notin\mathbb{Z}\\ \lceil-(x_0+1)/a\rceil+1 & \text{se } -(x_0+1)/a\in\mathbb{Z}\end{cases}$$

e s análoga, sendo

$$s=\begin{cases}\lceil-(y_0+1)/b\rceil & \text{se } -(y_0+1)/b\notin\mathbb{Z}\\ \lceil-(y_0+1)/b\rceil+1 & \text{se } -(y_0+1)/b\in\mathbb{Z}\end{cases}$$

achamos soluções (r,s,t) compatíveis com o sistema de desigualdades.

□

Problem 1.2. Seja p um número primo ímpar. Seja s o menor inteiro positivo que não é resíduo quadrático módulo p.

(a) Mostre que $p>s^2-s$.

(b) Suponha que $p>5$ e que -1 seja resíduo quadrático módulo p: mostre que $p>2s^2-s$.

Proof. □

Problem 1.3. Seja p um primo ímpar, a um inteiro e n um inteiro positivo. Sejam α e β inteiros negativos, com $\alpha>0$. Prove:

(a) Se p^β e p^α são as maiores potências de p que dividem n e $a-1$ respectivamente então $p^{\alpha+\beta}$ é a maior potência que divide a^n-1.

(b) Se n é ímpar e p^β e p^α são as maiores potências de p que dividem n e $a+1$ respectivamente então $p^{\alpha+\beta}$ é a maior potência de p que divide a^n+1.

Proof. □

Problem 1.4. (a) Prove que $\operatorname{ord}_{2^k}5=2^{k-2}$, para todo $k\geqslant 2$.

(b) Prove que se a é um inteiro ímpar e $k\geqslant 2$ então existem $\varepsilon_j\in\{-1,1\}$ e $j\in\mathbb{Z}$ com $0\leqslant j\leqslant 2^{k-2}$, únicamente determinados, tais que $a\equiv\varepsilon_j\cdot 5^j \mod 2^k$.

Proof. $\square$

Problem 1.5. Qual é o menor natural n para o qual existe k natural de modo que os 2026 últimos dígitos na representação decimal de n^k são iguais a 1?

Proof. $\square$

Problem 1.6. O símbolo de Legendre $\left(\frac{a}{p}\right)$ pode ser estendido para o símbolo de Jacobi $\left(\frac{a}{n}\right)$, que está definido para a inteiro arbitrário e n inteiro positivo ímpar por $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_k}\right)^{\alpha_k}$ se $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ é a fatoração prima de n (onde os $\left(\frac{a}{p_j}\right)$ são dados pelo símbolo de Legendre usual); temos $\left(\frac{a}{1}\right) = 1$ para todo inteiro a.

Prove as seguintes propriedades do símbolo de Jacobi, que podem ser usadas para calcular rapidametne símbolos de Legendre (e de Jacobi):

1. Se $a \equiv b \mod n$ então $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
2. $\left(\frac{a}{n}\right) = 0$ se $\gcd(a, n) \neq 1$ e $\left(\frac{a}{p}\right) \in \{-1, 1\}$ se $\gcd(a, n) = 1$.
3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$; em particular, $\left(\frac{a^2}{n}\right) \in 0, 1$.
4. $\left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$; em particular, $\left(\frac{a}{n^2}\right) \in 0, 1$.
5. Se m e n são positivos e ímpares, então $\left(\frac{m}{n}\right) = (-1)^{(m-1)/2 \cdot (n-1)/2}\left(\frac{n}{m}\right)$.
6. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
7. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$ se n é ímpar.

Proof. $\square$