Listas de Teoria dos Números

Aluno: Henrique Lima Cardoso

January 13, 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/medida`.

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.

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 $p > 2s^2 - s$.

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 $a^n + 1$.

Problem 1.4. (a) Prove que $\mathrm{ord}_{2^k} 5 = 2^{k-2}$, 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 $a \equiv \varepsilon_j \cdot 5^j \mod 2^k$.

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?

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.