Listas de Teoria dos Números

Aluno: Henrique Lima Cardoso

February 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`.

0.1 Notação

Até agora encontrei os seguintes usos de notação não convencional:

- $x \equiv \{a_1, a_2, \dots\} \pmod c$ - significa que x é congruente a um elemento do conjunto $\{a_i\}$.
- $x \equiv \frac{a}{b} \pmod m$ - significa que $x \equiv ab^{-1} \pmod m$.
- Se $\sum_{n \geqslant 1} a_n$ é uma série de termos positivos, denoto $\sum_{n \geqslant 1} a_n < \infty$ se a série converge.

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

$$2abc - ab - bc - ca = xbc + yca + zab$$
$$2abc = (x + 1)bc + (y + 1)ca + (z + 1)ab$$

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:

$$x_0 + ra > -1$$
$$y_0 + sb > -1$$
$$z_0 + tc > -1$$
$$r + s + t = 0$$

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

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

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. 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. **(a)** Como 1 é sempre resíduo quadrático, sabemos que $s\geqslant 2$. Notamos que, pela propriedade multiplicativa dos símbolos de Legendre, para todo $1\leqslant k\leqslant(s-1)$, vale que

$$\left(\frac{ks}{p}\right)=\left(\frac{k}{p}\right)\left(\frac{s}{p}\right)=1\cdot -1=-1.$$

Isto é, nenhum dos números $\{s,2s,\dots(s-1)s\}$ são resíduos quadráticos. Como p é um primo ímpar, temos que ao menos $(p-1)/2$ elementos de $\mathbb{Z}_p$ não são resíduos quadráticos, logo $p>s$. Suponha que $p<s(s-1)$, então existe $1\leqslant k<(s-1)$ tal que

$$sk<p<s(k+1).$$

Isso é, $s(k+1)=p+r$ onde $0<r<s$ e temos $s(k+1)\equiv r\pmod p$. Portanto $-1=\left(\frac{s(k+1)}{p}\right)=\left(\frac{r}{p}\right)=1$, absurdo. □

Proof. **(b)** Segue muito similarmente da letra anterior. Note que como $p>5$, se $s=2$, $p>2\cdot 2^2-2=6$, já que o próximo primo ímpar é 7. Podemos supor que $\left(\frac{2}{p}\right)=1$ e $s>2$. Já que temos $\left(\frac{-1}{p}\right)=1$, sabemos que para todo $1\leqslant k\leqslant(s-1)$,

$$\left(\frac{-2sk}{p}\right)=\left(\frac{2sk}{p}\right)=-1.$$

Agora suponha que $p<2s^2-s$ ou, posto de forma mais instrutiva, $p<2s(s-1)+s$. Então existe $1\leqslant k\leqslant(s-1)$ tal que

$$p\in(2sk-s,2sk+s).$$

Note que como p é um primo maior que s, ele não pode estar nas bordas destes intervalos (que são múltiplas de s). Se vale que $2sk - s < p < 2sk$, então $2sk = p + r$ onde $0 < r < s$, logo $-1 = \left(\frac{2ks}{p}\right) = \left(\frac{r}{p}\right) = 1$, o que é absurdo. Se por outro lado, vale que $2sk < p < 2sk + s$, então podemos escrever $2sk = p - r$ onde $0 < r < s$ e $2sk \equiv -r \pmod{p}$, teríamos $-1 = \left(\frac{2ks}{p}\right) = \left(\frac{-r}{p}\right) = 1$, absurdo também. □

A seguinte definição será útil para os próximos dois problemas.

Definition 1.1. Dado p primo e $n \neq 0$ inteiro,

$$\nu_p(n) = \max\{\alpha \in \mathbb{N} : p^\alpha \mid n\}$$

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. **(a)** Considere o caso particular $\nu_p(a-1) = \alpha > 0$ e $\nu_p(n) = \beta = 0$, queremos mostrar que $\nu_p(a^n - 1) = \alpha$, temos

$$a^n - 1 = (a-1) \cdot \left(\sum_{j=0}^{n-1} a^j \right)$$

$$\nu_p(a^n - 1) = \nu_p(a-1) + \nu_p\left(\sum_{j=0}^{n-1} a^j \right) = \alpha + \nu_p\left(\sum_{j=0}^{n-1} a^j \right)$$

então basta mostrar que $\nu_p\left(\sum_{j=0}^{n-1} a^j \right) = 0$. Verificamos que, como $\nu_p(a-1) > 0$, $p \mid (a-1)$, ou seja $a \equiv 1 \pmod{p}$. Mas então

$$\sum_{j=0}^{n-1} a^j \equiv \sum_{j=0}^{n-1} 1 \equiv n \not\equiv 0 \pmod{p},$$

ou seja $p \nmid \sum_{j=0}^{n-1} a^j$ e $\nu_p\left(\sum_{j=0}^{n-1} a^j \right) = 0$.

Vamos provar indutivamente para $n = p^\beta$, $\beta \geqslant 1$, o caso base principal é $n = p$. Queremos mostrar que $\nu_p(a^p - 1) = \nu_p(a-1) + 1$, ou seja, como antes, que $\nu_p\left(\sum_{j=0}^{p-1} a^j \right) = 1$. Como $\nu_p(a-1) = \alpha$, escrevemos $a = p^\alpha s + 1$ com $(p, s) = 1$. O somatório se traduz como $\left(\sum_{j=0}^{p-1} (p^\alpha s + 1)^j \right)$. Se $\alpha \geqslant 2$, segue que

$$\sum_{j=0}^{p-1} (p^\alpha s + 1)^j \equiv \sum_{j=0}^{p-1} 1 \equiv p \pmod{p^2}$$

logo $p \mid \sum_{j=0}^{p-1} (p^\alpha s + 1)^j$, mas p^2 não, e portanto $\nu_p\left(\sum_{j=0}^{p-1} a^j \right) = 1$. Se $\alpha = 1$, temos

$$\sum_{j=0}^{p-1} (ps + 1)^j \equiv \sum_{j=0}^{p-1} (1 + jps) \equiv p + ps \cdot (p(p-1)/2) \equiv p \pmod{p^2}$$

e o resultado segue também.

Para o passo indutivo, suponha que o resultado vale para $\beta \geqslant 1$ e seja $n = p^{\beta+1}$. Então,

$$a^n - 1 = a^{p^{\beta+1}} - 1 = (a^p)^{p^\beta} - 1,$$

por indução com os parâmetros $(a = a^p)$ e $(n = p^\beta)$, temos

$$\nu_p(a^n - 1) = \nu_p(a^p - 1) + \nu_p(p^\beta) = \nu_p(a-1) + 1 + \beta = \nu_p(a-1) + \nu_p(p^{\beta+1}),$$

o que prova a afirmação.

Já temos o suficiente para o caso geral, suponha que $\nu_p(a-1) = \alpha \geqslant 1$ e $\nu_p(n) = \beta$, de onde $n = p^\beta \cdot k$ com $(p,k) = 1$. Então

$$a^n - 1 = (a^{p^\beta})^k - 1 = (a^{p^\beta} - 1) \cdot \left(\sum_{j=0}^{k-1} (a^{p^\beta})^j \right),$$

já sabemos que $\nu_p((a^{p^\beta} - 1)) = \alpha + \beta$, então basta mostrar que o somatório não é divisivel por p. Notamos, pelo teorema de Fermat, que para qualquer $\beta \geqslant 1$,

$$a^{p^\beta} = (a^p)^{p^{\beta-1}} \equiv a^{p^{\beta-1}} \pmod p,$$

ou seja $a^{p^\beta} \equiv a \pmod p$, mas $a \equiv 1 \pmod p$ pois $\nu_p(a-1) \geqslant 1$. No somatório, isso se traduz como

$$\sum_{j=0}^{k-1} (a^{p^\beta})^j \equiv \sum_{j=0}^{k-1} 1 \equiv k \not\equiv 0 \pmod p,$$

pois $(k,p) = 1$. Isto finaliza a demonstração. $\square$

A prova do segundo item é quase que idêntica a do primeiro, só fazemos uso da outra fatoração usual. Serei um pouco mais sucinto.

Proof. **(b)** Caso $\nu_p(n) = \beta = 0$ e $\nu_p(a+1) = \alpha \geqslant 1$. Escrevemos

$$a^n + 1 = (a+1) \cdot \left(\sum_{j=0}^{n-1} (-1)^j a^j \right) \Rightarrow \nu_p(a^n + 1) = \alpha + \nu_p\left(\sum_{j=0}^{n-1} (-1)^j a^j \right)$$

como $\alpha \geqslant 1$, $a \equiv -1 \pmod p$, ou seja

$$\sum_{j=0}^{n-1} (-1)^j a^j \equiv \sum_{j=0}^{n-1} (-1)^{2j} \equiv n \not\equiv 0 \pmod p$$

e portanto $\nu_p\big(\sum_{j=0}^{n-1} (-1)^j a^j \big) = 0$.

Caso $n = p$, $\nu_p(a+1) = \alpha \geqslant 1$. Como no caso anterior, basta mostrar que $\nu_p\big(\sum_{j=0}^{p-1} (-1)^j a^j \big) = 1$. Escrevemos $a = p^\alpha s - 1$ com $(p,s) = 1$. Substituindo no somatório,

$$\sum_{j=0}^{p-1} (-1)^j a^j = \sum_{j=0}^{p-1} (-p^\alpha s + 1)^j \equiv p + p^\alpha s \cdot (p(p-1)/2) \equiv p + p^{\alpha+1}(p-1)/2 \pmod{p^{2\alpha}}$$

como $\alpha \geqslant 1$ e p é ímpar, tomando a última equivalência módulo p^2 vemos que $\big(\sum_{j=0}^{p-1} (-1)^j a^j \big) \equiv p \pmod{p^2}$, e isso nos dá o resultado que queríamos.

Caso $n = p^{\beta+1}$ com $\beta \geqslant 1$, $\nu_p(a+1) = \alpha \geqslant 1$. Exatamente como antes, suponha, por indução, que o resultado é válido para $n = p^\beta$, segue que

$$\nu_p(a^n + 1) = \nu_p\left((a^p)^{p^\beta} + 1 \right) = \nu_p(a^p + 1) + \nu_p(p^\beta) = \alpha + 1 + \beta.$$

onde usamos o caso anterior da prova na última igualdade.

Caso $n = p^\beta k$ com $(k,p)=1$ e $\beta \geqslant 1$, $\nu_p(a+1) = \alpha \geqslant 1$. Escrevemos (como no item anterior),

$$a^n + 1 = (a^{p^\beta} + 1) \cdot \left(\sum_{j=0}^{k-1} (-a^{p^\beta})^j \right).$$

Pelo caso indutivo, já sabemos que $\nu_p(a^{p^\beta}+1) = \alpha+\beta$, basta mostrar que $\sum_{j=0}^{k-1}(-a^{p^\beta})^j \not\equiv 0 \pmod p$. Mas, pela mesma observação de antes, se $\beta \geqslant 1$, $a^{p^\beta} \equiv a \pmod p$ e, como $a \equiv -1 \pmod p$, temos

$$\sum_{j=0}^{k-1}(-a^{p^\beta})^j \equiv \sum_{j=0}^{k-1}(-1\cdot -1)^j \equiv k \not\equiv 0 \pmod p.$$

O que completa a demosntração. □

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 $0 \leqslant j < 2^{k-2}$, únicamente determinados, tais que $a \equiv \varepsilon_j \cdot 5^j \pmod{2^k}$.

Proof. **(a)** Vamos provar por indução em k. O resultado é claro para $k=2$ pois $5 \equiv 1 \pmod 4$. Suponha que vale para $k \geqslant 2$, vamos provar para $k+1$. Isto é, queremos mostrar que $t = \mathrm{ord}_{2^{k+1}} 5 = 2^{k-1}$, sabemos que

$$\mathrm{ord}_{2^k} 5 \mid t = \mathrm{ord}_{2^{k+1}} 5 \mid \varphi(2^{k+1}) = 2^k \Rightarrow t \in \{2^{k-2}, 2^{k-1}, 2^k\}.$$

Como 5 não é raiz primitiva módulo 4, não pode ser raiz primitiva módulo 2^k para $k \geqslant 2$. Logo $t \in \{2^{k-2}, 2^{k-1}\}$ e basta mostrar que $5^{2^{k-2}} \not\equiv 1 \pmod{2^{k+1}}$. Para isso, vamos calcular $\nu_2(5^{2^{k-2}} - 1)$. Vamos usar uma fatoração esperta, repetindo o fato que $x^2 - 1 = (x+1)(x-1)$, temos

$$(5^{2^{k-2}} - 1) = (5^{2^{k-3}} + 1)(5^{2^{k-4}} + 1)\dots(5^2+1)(5+1)(5-1) = 4 \cdot \prod_{j=0}^{k-3}(5^{2^j}+1). \tag{2}$$

Como $5 \equiv 1 \pmod 4$, para qualquer número par s, $5^s \equiv 1 \pmod 4$ e portanto $5^s + 1 \equiv 2 \pmod 4$. Em particular, $\nu_2(5^s+1) = 1$. Usando esse fato na expressão acima, temos

$$\nu_2(5^{2^{k-2}} - 1) = \nu_2(4) + \sum_{j=0}^{k-3} \nu_2(5^{2^j}+1) = 2 + k - 2 = k.$$

Portanto $2^{k+1} \nmid 5^{2^{k-2}} - 1$, ou seja $5^{2^{k-2}} \not\equiv 1 \pmod{2^{k+1}}$. □

Proof. **(b)** Essa prova é um belo problema de contagem. Note que como $5 \equiv 1 \pmod 4$, para todo k, $5^k \equiv 1 \pmod 4$. No entanto, para $k \geqslant 2$, há exatamente $2^k/4$ classes de equivalência módulo 2^k que são congruentes a 1 módulo 4. Como $\mathrm{ord}_{2^k} 5 = 2^{k-2} = 2^k/4$, segue que

$$\{\bar{5}^k \pmod{2^k} : 0 \leqslant k \leqslant \mathrm{ord}_{2^k} 5 = 2^{k-2}\} = \{\bar{a} \pmod{2^k} : a \equiv 1 \pmod 4\}.$$

Particularmente, se $a \equiv 1 \pmod 4$, então existe um único $0 \leqslant j \leqslant 2^{k-2}$ tal que $5^j \equiv a \pmod{2^k}$. Caso $a \equiv -1 \pmod 4$, então existe um único $0 \leqslant j \leqslant 2^{k-2}$ tal que $5^k \equiv -a \pmod{2^k}$, logo $a \equiv -5^j \pmod{2^k}$. Note que os pares (ε_j, j) estão únicamente determinados pois, se $\varepsilon_i \neq \varepsilon_j$ então $\varepsilon_i 5^i \not\equiv \varepsilon_j 5^j \pmod 4$ e se $\varepsilon_i = \varepsilon_j$, então $5^i \equiv 5^j$, mas $0 \leqslant i \neq j < \mathrm{ord}_{2^k} 5$ o que é absurdo. □

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. Esse problema é cabuloso e não fui capaz de resolvê-lo sozinho, nem mesmo com dicas - a solução escrita aqui segue a da revista Eureka.

Note que a questão se resume a achar o menor $n > 0$ tal que existe k satisfazendo

$$n^k \equiv \sum_{j=0}^{2025} 10^j \equiv \frac{10^{2026}-1}{9} \equiv -1 \cdot 9^{-1} \pmod{10^{2026}},$$

equivalentemente, usando o Teorema Chinês dos Restos,

$$n^k \equiv -9^{-1} \pmod{2^{2026}}$$
$$n^k \equiv -9^{-1} \pmod{5^{2026}}.$$

A ideia da prova é inicialmente restringir n, fazemos isso olhando para congruências simples. Vamos olhar módulo potências de 2. Como n^k deve terminar com 1, temos que n tem que ser ímpar. Olhando a primeira congruência módulo 8, temos

$$n^k \equiv -1 \pmod 8,$$

mas como todo número ímpar ao quadrado é 1 módulo 8, devemos ter que $n \equiv -1 \pmod 8$ e $k \equiv 1 \pmod 2$ ou seja $k = 2l+1$. Olhando módulo 16, segue que n é congruente a 7 ou 15. Mas, se n fosse $\overline{15}$, teríamos $15^{2l+1} \equiv -1 \equiv -9^{-1} \pmod{16}$, o que é absurdo pois $-1 \cdot -9 \equiv 9 \not\equiv 1 \pmod{16}$. Portanto $n \equiv 7 \pmod{16}$ e essa é nossa primeira congruência de importância.

Olhando módulo 5, vemos que $n^{2l+1} \equiv -(-1)^{-1} \equiv 1 \pmod 5$, logo $n \equiv 1 \pmod 5$. Isso segue, pois $-1^{2l+1} \equiv -1$ e $-3^{2l+1} \equiv 2^{2l+1} \in \{-2, 2\}$ portanto nem 2 e nem 3 podem são tais que elevados a um ímpar dão $-1 \pmod 5$).

Sabemos então que $n \equiv 1 \pmod 5$ e que $n \equiv 7 \pmod{16}$, resolvendo o sistema, temos que $n \equiv 71 \pmod{80}$ e aqui devemos fazer um salto de fé e sonhar que 71 seja solução.

Vamos tentar cálcular $t_5 := \mathrm{ord}_{5^{2026}} 71$ usando o problema anterior. Notamos que $t_5 \mid \varphi(5^{2026}) = 4 \cdot 5^{2025}$. Uma boa estratégia é entender o valor de $\nu_5(71^s - 1)$, se este for maior ou igual a 2026 temos que $71^s \equiv 1 \pmod{5^{2026}}$. Pelo primeiro item do exercício anterior [1.3], temos

$$\nu_5(71^s - 1) = \nu_5(s) + \nu_5(71-1) = \nu_5(s) + 1,$$

portanto, se $s = 5^{2025}$, vemos que

$$\nu_5(71^{5^{2025}} - 1) = 2026 \Rightarrow 71^{5^{2025}} \equiv 1 \pmod{5^{2026}},$$

mas, crucialmente, se $s = 5^x$ com $x < 2025$, então $\nu_5(71^{5^x} - 1) = x + 1 < 2026$, e portanto $t_5 \neq 5^x$. Isso significa que temos $t_5 = 5^{2025}$.

Para calcular $t_2 := \mathrm{ord}_{2^{2026}} 71$ usaremos a mesma fatoração que no exercício anterior [2]. Como $t_2 \mid \varphi(2^{2026}) = 2^{2025}$, t_2 é da forma 2^x para algum $x \geqslant 1$. Vamos calcular $\nu_2(71^{2^x} - 1)$ usando a fatoração. Note que

$$(71^{2^x} - 1) = (71-1) \cdot \prod_{j=0}^{x-1} (71^{2^j} + 1) = (71-1) \cdot (71+1) \cdot \prod_{j=1}^{x-1} (71^{2^j} + 1)$$
$$\nu_2(71^{2^x} - 1) = \nu_2(70) + \nu(72) + \sum_{j=1}^{x-1} \nu_2(71^{2^x} + 1)$$

Como $71 \equiv -1 \pmod 8$, para qualquer $x \geqslant 1$ vale que $71^{2^x} = (-1^2)^{2^{x-1}} \equiv 1 \pmod 8$, ou seja $71^{2^x}+1 \equiv 2 \pmod 8$. Portanto $\nu_2(71^{2^j}+1) = 1$. Substituindo na equação acima temos:

$$\nu_2(71^{2^x}-1) = 1+3+x-1 = x+3.$$

Assim como antes, segue que $71^{2^{2023}} \equiv 1 \pmod{2^{2026}}$, mas $71^{2^x} \not\equiv 1 \pmod{2^{2026}}$ para qualquer $x \leqslant 2022$. Logo sabemos que $t_2 = 2^{2023}$.

Agora estamos quase prontos. Como $71 \equiv 1 \pmod 5$, $t_5 = 5^{2025}$ e há exatamente 5^{2025} números $0 \leqslant m < 5^{2026}$ com $m \equiv 1 \pmod 5$, segue que para cada um deles, existe $0 \leqslant s < t_5$ com $71^s \equiv m \pmod{5^{2025}}$. Em particular, como $\frac{-1}{9} \equiv 1 \pmod 5$, segue que existe $0 \leqslant k_5 < t_5$ com

$$71^{k_5} \equiv -(9)^{-1} \pmod{5^{2026}}.$$

Da mesma forma, $71 \equiv 7 \pmod{16}$, portanto $71^x \equiv \{1,7\} \pmod{16}$. Mas existem exatamente 2^{2023} números $0 \leqslant m < 2^{2026}$ com $m \equiv \{1,7\} \pmod{16}$, portanto para cada um deles existe um único $0 \leqslant s < t_2$ com $71^s \equiv m \pmod{2^{2026}}$. Em particular, como $-1 \equiv 7 \cdot 9 \pmod{16}$, segue que $\frac{-1}{9} \equiv 7 \pmod{16}$ e existe $0 \leqslant k_2 < t_2$ com

$$71^{k_2} \equiv -(9)^{-1} \pmod{2^{2026}}.$$

Como $(t_2, t_5) = (2^{2023}, 5^{2025}) = 1$, pelo teorema chinês dos restos, existe $k > 0$ natural grande satisfazendo

$$\begin{aligned} 71^k &> 10^{2027} \\ k &\equiv k_2 \pmod{t_2} \\ k &\equiv k_5 \pmod{t_5} \end{aligned}$$

E por fim (graças a deus),

$$\begin{aligned} 71^k &= 71^{k_2+q\cdot t_2} \equiv -9^{-1} \pmod{2^{2026}} \\ 71^k &= 71^{k_5+r\cdot t_5} \equiv -9^{-1} \pmod{5^{2026}} \\ 71^k &\equiv \frac{10^{2026}-1}{9} \equiv \underbrace{111\ldots1}_{2026} \pmod{10^{2026}} \end{aligned}$$

Portanto, $n = 71$.

□

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 $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \ldots \left(\frac{a}{p_k}\right)^{\alpha_k}$ se $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ 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. **(1)** Note que se $a \equiv b \pmod{n}$, então $a \equiv b \pmod{p_j}$ para todo $1 \leqslant j \leqslant k$. Pela propriedade usual do símbolo de Legendre, $\left(\frac{a}{p_j}\right) = \left(\frac{b}{p_j}\right)$ para todo j e, portanto,

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{\alpha_j} = \prod_{j=1}^{r} \left(\frac{b}{p_j}\right)^{\alpha_j} = \left(\frac{b}{n}\right).$$

(2) Se $(a, n) \neq 1$, então existe algum primo p_i tal que $p_i \mid a$, portanto $\left(\frac{a}{p_i}\right) = 0$ e

$$\prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{\alpha_j} = 0.$$

Por outro lado, se $(a, n) = 1$, então para todos os primos p_i, temos que $p_i \nmid a$ e temos $\left(\frac{a}{p_i}\right) \in \{-1, 1\}$. Portanto

$$\prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{\alpha_j} \in \{-1, 1\}.$$

(3) Basta abrir a conta e usar a propriedade dos símbolos usuais de Legendre,

$$\left(\frac{ab}{n}\right) = \prod_{j=1}^{r} \left(\frac{ab}{p_j}\right)^{\alpha_j} = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{\alpha_j} \left(\frac{b}{p_j}\right)^{\alpha_j} = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{\alpha_j} \prod_{j=1}^{r} \left(\frac{b}{p_j}\right)^{\alpha_j} = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

(4) Sejam $q_1 \dots q_r$ os primos que dividem n ou m. Escrevemos $n = q_1^{\alpha_1} \dots q_r^{\alpha_r}$ e $m = q_1^{\beta_1} \dots q_r^{\beta_r}$ onde os α_i e β_j podem potencialmente ser 0. Temos

$$nm = q_1^{\alpha_1+\beta_1} \dots q_r^{\alpha_r+\beta_r}$$

e logo

$$\left(\frac{a}{nm}\right) = \prod_{j=1}^{r} \left(\frac{a}{q_j}\right)^{\alpha_j+\beta_j} = \prod_{j=1}^{r} \left(\frac{a}{q_j}\right)^{\alpha_j} \prod_{j=1}^{r} \left(\frac{a}{q_j}\right)^{\beta_j}.$$

Agora notamos que se $q_j \nmid n$, então $\alpha_j = 0$ e se $q_i \nmid m$, então $\beta_i = 0$, então os produtórios acima se expressam como

$$\left(\frac{a}{nm}\right) = \prod_{q_j \mid n} \left(\frac{a}{q_j}\right)^{\alpha_j} \prod_{q_i \mid m} \left(\frac{a}{q_i}\right)^{\beta_i} = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right).$$

(5) Esse é mais interessante, vamos usar reciprocidade quadrática e as propriedades anteriores. Primeiramente, note que por **(2)**, a fórmula é válida se $(m, n) \neq 1$, já que tanto $\left(\frac{m}{n}\right) = 0$ quanto $\left(\frac{n}{m}\right) = 0$. Podemos supor então que $(m, n) = 1$. Outro caso de interesse é que se $a^2 \mid m$, então $m = a^2 m'$ e por **(3)**, $\left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right)$. Já que o mesmo vale para o "denominador" do símbolo de Legendre, podemos supor ainda mais que m e n são livres de quadrados. Ou seja, podemos considerar (ad hoc) que suas fatorações são $n = p_1 \dots p_l \cdot r_1 \dots r_k$ e $m = q_1 \dots q_t \cdot s_1 \dots s_h$ onde os $p_i \equiv q_j \equiv 1 \pmod{4}$, os $r_i \equiv s_j \equiv 3 \pmod{4}$ e os primos das fatorações são todos distintos.

Após todas nossas suposições, temos (usando a propriedade **(3)** e **(4)** várias vezes)

$$\left(\frac{m}{n}\right) = \left(\frac{q_1 \dots q_t \cdot s_1 \dots s_h}{p_1 \dots p_l \cdot r_1 \dots r_k}\right) = \left(\frac{q_1 \dots q_t}{p_1 \dots p_l}\right)\left(\frac{s_1 \dots s_h}{p_1 \dots p_l}\right)\left(\frac{q_1 \dots q_t}{r_1 \dots r_k}\right)\left(\frac{s_1 \dots s_h}{r_1 \dots r_k}\right),$$

ou seja,

$$\left(\frac{m}{n}\right) = \prod_{(q_i,p_j)} \left(\frac{q_i}{p_j}\right) \cdot \prod_{(s_i,p_j)} \left(\frac{s_i}{p_j}\right) \cdot \prod_{(q_i,r_j)} \left(\frac{q_i}{r_j}\right) \cdot \prod_{(s_i,r_j)} \left(\frac{s_i}{r_j}\right).$$

Pela lei da reciprocidade quadrática, se h é um primo com $h \equiv 1 \pmod 4$ e g é outro primo qualquer, então $\left(\frac{h}{g}\right) = \left(\frac{g}{h}\right)$ e se ambos g e h forem congruentes a 3 módulo 4, então $\left(\frac{h}{g}\right) = -\left(\frac{g}{h}\right)$. Podemos usar isso na expressão acima para obter

$$\left(\frac{m}{n}\right) = \prod_{(q_i,p_j)} \left(\frac{p_j}{q_i}\right) \cdot \prod_{(s_i,p_j)} \left(\frac{p_j}{s_i}\right) \cdot \prod_{(q_i,r_j)} \left(\frac{r_j}{q_i}\right) \prod_{(s_i,r_j)} -\left(\frac{r_j}{s_i}\right),$$

de forma que (juntando os produtórios)

$$\left(\frac{m}{n}\right) = (-1)^{kh}\left(\frac{n}{m}\right).$$

Para o resultado, basta mostrar que $kh \equiv (n-1)/2 \cdot (m-1)/2 \pmod 2$ (note que são inteiros uma vez que n e m são ímpares). Vamos olhar para n e m módulo 4, observamos que

$$n \equiv p_1 \dots p_l \cdot r_1 \dots r_k \equiv r_1 \dots r_k \equiv 3^k \equiv \left\{\begin{matrix} 1 & \text{se } k \equiv 0 & \text{mod } 2 \\ 3 & \text{se } k \equiv 1 & \text{mod } 2 \end{matrix}\right\} \pmod 4$$

o resultado análogo segue para m e h. Disso já obtemos que se h ou k forem pares, então n ou m são 1 módulo 4, portanto $(n-1)/2$ ou $(m-1)/2$ é par e $hk \equiv 0 \equiv (n-1)/2 \cdot (m-1)/2 \pmod 2$. Se ambos h e k forem ímpares, então $n \equiv m \equiv 3 \pmod 4$, logo $(n-1)/2$ e $(m-1)/2$ são ímpares e $hk \equiv 1 \equiv (n-1)/2 \cdot (m-1)/2 \pmod 2$ concluindo a demonstração.

(6) Vamos fazer uma análise semelhante a **(5)**. Pelo observado anteriormente, podemos supor que n é livre de quadrados e se escreve $n = p_1 \dots p_l \cdot r_1 \dots r_k$ com os $p_i \equiv 1 \pmod 4$ e $r_i \equiv 3 \pmod 4$. Abrindo o símbolo de Jacobi, temos então

$$\left(\frac{-1}{n}\right) = \prod_{p_i} \left(\frac{-1}{p_i}\right) \prod_{r_j} \left(\frac{-1}{r_j}\right).$$

Como $\left(\frac{-1}{x}\right) = 1$ se x é primo e $x \equiv 1 \pmod 4$ e $\left(\frac{-1}{x}\right) = -1$ se x for um primo com $x \equiv 3 \pmod 4$, segue que

$$\left(\frac{-1}{n}\right) = (-1)^k$$

ou seja, para mostrar a igualdade, basta veriricar que $k \equiv (n-1)/2 \pmod 2$ e já fizemos isso na prova da propriedade anterior.

(7) Seguindo a mesma ideia, vamos fatorar n de maneira esperta. Vimos que, sem perda de generalidade, podemos supor n livre de quadrados, então escrevemos a fatoração prima de n como

$$n = (p_1^+ p_2^+ \dots p_l^+) \cdot (p_1^- p_2^- \dots p_k^-) \cdot (q_1^+ q_2^+ \dots q_r^+) \cdot (q_1^- q_2^- \dots q_s^-)$$

onde cada $p_i^+ \equiv 1 \pmod 8$, $p_i^- \equiv -1 \pmod 8$, $q_i^+ \equiv 3 \pmod 8$ e $q_i^- \equiv -3 \pmod 8$. Usando a propriedade **(4)**, temos

$$\left(\frac{2}{n}\right) = \prod_{p_i^+} \left(\frac{2}{p_i^+}\right) \cdot \prod_{p_i^-} \left(\frac{2}{p_i^-}\right) \cdot \prod_{q_i^+} \left(\frac{2}{q_i^+}\right) \cdot \prod_{q_i^-} \left(\frac{2}{q_i^-}\right).$$

Por reciprocidade quadrática, sabemos que para todo i vale $\left(\frac{2}{p_i^+}\right) = \left(\frac{2}{p_i^-}\right) = 1$ e $\left(\frac{2}{q_i^+}\right) = \left(\frac{2}{q_i^-}\right) = -1$, portanto, a equação acima reduz-se para

$$\left(\frac{2}{n}\right) = (-1)^{r+s}.$$

Para finalizar a demonstração, basta mostrar que $r+s \equiv (n^2-1)/8 \pmod 2$ ou, equivalentemente, desejamos mostrar

$$r + s \equiv 0 \pmod 2 \iff n \equiv \{-1, 1\} \pmod 8 \quad \text{e} \quad r + s \equiv 1 \pmod 2 \iff n \equiv \{-3, 3\} \pmod 8.$$

Notamos primeiramente que

$$n = (p_1^+ p_2^+ \dots p_l^+) \cdot (p_1^- p_2^- \dots p_k^-) \cdot (q_1^+ q_2^+ \dots q_r^+) \cdot (q_1^- q_2^- \dots q_s^-) \equiv (1)^l \cdot (-1)^k \cdot (3)^r \cdot (-3)^s \pmod 8,$$

ou seja, $n \equiv \varepsilon \cdot (3)^r \cdot (-3)^s \pmod 8$ onde $\varepsilon \in \{-1, 1\}$. Agora para a análise de casos. Se $r+s$ for par, então ou r e s são pares onde $n \equiv \varepsilon \cdot 1 \cdot 1 \in \{-1, 1\} \pmod 8$ ou r e s são ímpares e temos $n \equiv \varepsilon \cdot 3 \cdot -3 \equiv -\varepsilon \in \{-1, 1\} \pmod 8$. Se, por outro lado, $r+s$ for ímpar, então ou r é ímpar e s é par onde $n \equiv \varepsilon \cdot 3 \cdot 1 \in \{3, -3\} \pmod 8$ ou r é par e s é ímpar, onde também temos $n \equiv \varepsilon \cdot 1 \cdot -3 \in \{3, -3\} \pmod 8$. O que conclui a demonstração. $\square$

2 Lista 2 - 26/01/2026

Problem 2.1. Sejam $a, n \in \mathbb{N}^*$ e considere a sequência (x_k) definida por $x_1 = a, x_{k+1} = a^{x_k}$ para todo $k \in \mathbb{N}$. Demonstre que existe $N \in \mathbb{N}$ tal que $x_{k+1} \equiv x_k \pmod n$ para todo $k \geqslant N$.

Observation 2.1. Note que, se $a > 1$, a sequência (x_k) é estritamente crescente já que $x_{k+1} = a^{x_k} \geqslant 2^{x_k} > x_k$ e tende para infinito.

Proof. Caso $a = 1$, então o resultado segue pois $x_k = 1$ para todo k. Vamos provar os outros casos por indução em n.

Caso $a \neq 1$. Para $n = 1$ é óbvio, uma vez que $x_k \equiv 0 \pmod 1$ para todo k independente de a. Seja $n > 1$ e suponha que vale para todo $m < n$ i.e. existe N_m tal que se $k \geqslant N_m$, então $x_{k+1} \equiv x_k \pmod m$. Fatorando n, podemos supor que

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

com os p_i sendo primos distintos. Pelo Teorema Chinês dos Restos, o problema se resume a mostrar que existe N tal que para todo $k \geqslant N$, vale para todo i,

$$x_{k+1} \equiv x_k \pmod{p_i^{\alpha_i}}.$$

Vamos encontrar um N_i para cada p_i e tomar $N = \max\{N_i : 1 \leqslant i \leqslant r\}$. Se $(a, p_i) = p_i$, temos $a = p_i q$ e basta que $x_k \geqslant \alpha_i$ para $x_{k+1} = a^{x_k} = (p_i \cdot q)^{x_k} \equiv 0 \pmod{p_i^{\alpha_i}}$. Como $x_k \to \infty$, existe N_i satisfazendo $x_k \equiv 0 \pmod{p_i^{\alpha_i}}$ para todo $k \geqslant N_i$. Por outro lado, se $(a, p_j) = 1$, podemos usar indutivamente o resultado para $m = \varphi(p_j^{\alpha_j}) < n$ de onde segue que existe M_j tal que

$$x_{k+1} \equiv x_k \pmod{m = \varphi(p_j^{\alpha_j})} \quad \forall k \geqslant M_j,$$

portanto

$$x_{k+2} = a^{x_{k+1}} = a^{m \cdot t + x_k} \equiv a^{x_k} = x_{k+1} \pmod{p_j^{\alpha_j}} \quad \forall k \geqslant M_j$$

e portanto, podemos tomar $N_j = M_j + 1$. Tomando N o máximo dos N_i, segue que

$$\forall k \geqslant N, \forall 1 \leqslant i \leqslant r \quad x_{k+1} \equiv x_k \pmod{p_i^{\alpha_i}}$$

e, por fim,

$$x_{k+1} \equiv x_k \pmod n \quad \forall k \geqslant N$$

□

Problem 2.2.
(a) Seja $F_n = 2^{2^n} + 1$ o n-ésimo número de Fermat. Prove que todo fator primo de F_n é da forma $k \cdot 2^{n+1}$.

(b) Prove que, se $n \geqslant 2$, então todo fator primo de F_n é da forma $k \cdot 2^{n+2} + 1$.

(c) Mostre que $2^{2^5} + 1$ é composto.

Proof. Vamos fazer o item (a) e (b) simultâneamente. Note que, se $p \mid F_n$, então p é ímpar e

$$2^{2^n} \equiv -1 \pmod p \quad \wedge \quad 2^{2^{n+1}} \equiv 1 \pmod p,$$

logo $t := \mathrm{ord}_p 2 \mid 2^{n+1}$, i.e $t := 2^q$ com $1 \leqslant q \leqslant 2^{n+1}$. Agora usamos um truque já visto [2], escrevemos

$$2^{2^n} + 1 = 2^{2^n} - 1 + 2 = \prod_{m=0}^{n-1} (2^{2^m} + 1) + 2. \tag{3}$$

Vamos provar que $q = n+1$. Se $q \leqslant n$, sabemos do fato que $(2^{2^{q-1}})^2 \equiv 1 \pmod p$ e $2^{2^{q-1}} \not\equiv 1 \pmod p$ que $2^{2^{q-1}} \equiv -1 \pmod p$ e, portanto, tomando [3] módulo p, achamos

$$\prod_{m=0}^{n-1} (2^{2^m} + 1) + 2 \equiv 0 + 2 \not\equiv 0 \pmod p$$

absurdo, pois, por hipótese, $p \mid F_n$. Portanto $q = n+1$ e temos $t = 2^{n+1}$, logo $t = 2^{n+1} \mid \varphi(p) = p-1$ e segue a letra **(a)**, $p = k \cdot 2^{n+1} + 1$. Para a letra **(b)**, basta perceber que, caso $n \geqslant 2$, então, pela letra (a), $p \equiv 1 \pmod 8$, ou seja $(\frac{2}{p}) = 1$, logo $2^{(p-1)/2} \equiv 1 \pmod p$ e segue (da mesma forma que antes) que $t = 2^{n+1} \mid (p-1)/2$, ou seja $p = k \cdot 2^{n+2} + 1$.

Para a parte (c), usamos (b) e torcemos que achemos um fator rapidamente. Fazendo as continhas vemos que $k = 5$ funciona. Isso é

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$$

onde $641 = 5 \cdot (2^7) + 1$. Essas contas foram feitas nesse script que está no github. ☐

Problem 2.3. Seja $\alpha = [a_0; a_1, a_2, \dots]$ um número real.

(a) Prove que, se $\text{ord}\alpha > 2$ então existe $\lambda > 1$ tal que para infinitos inteiros positivos n, temos $a_n \geqslant \lambda^n$.

(b) Prove que $\text{ord}\alpha \geqslant 1 + \exp(\limsup_{n\to\infty} \frac{\log\log(a_n+1)}{n})$.

(c) Prove que para todo $c \geqslant 2$, existe $\alpha \in \mathbb{R}$ tal que $\text{ord}\alpha = 1 + \exp(\limsup_{n\to\infty} \frac{\log\log(a_n+1)}{n}) = c$.

(d) Determine $\text{ord}\alpha$ se $a_n = 2^n, \forall n \geqslant 0$.

Proof. **(a)** Note que, como $q_n = a_n q_{n-1} + q_{n-2} \geqslant 2q_{n-2}$, segue (por indução) que $q_n \geqslant C2^{n/2}$ para alguma constante positiva C. Portanto, para $1 < \gamma < \sqrt{2}$ e n suficientemente grande, vale que $q_n \geqslant \gamma^n$ (na verdade, no pior caso, q_n cresce como a sequência de Fibonacci). Portanto, se $\text{ord}\alpha > 2$, segue que

$$\text{ord}\alpha - 2 = \limsup_{n\to\infty} \frac{\log a_{n+1}}{\log q_n} > \varepsilon > 0$$

para algum $\varepsilon > 0$ e

$$\limsup_{n\to\infty} \frac{\log a_{n+1}}{\log(\gamma^n)} \geqslant \limsup_{n\to\infty} \frac{\log a_{n+1}}{\log q_n} > \varepsilon$$

$$\limsup_{n\to\infty} \frac{\log a_{n+1}}{n \log \gamma} > \varepsilon$$

i.e, existe sequência infinita (n_j) tal que

$$\frac{\log a_{n_j+1}}{n_j \log \gamma} > \varepsilon \quad \text{e} \quad a_{n_j+1} > (\gamma^\varepsilon)^{n_j}.$$

Como $\gamma^\varepsilon > 1$, tomando $1 < \beta < \gamma^\varepsilon$, segue que para n_j suficientemente grande,

$$a_{n_j+1} > (\gamma^\varepsilon)^{n_j} > \beta^{n_j+1},$$

finalizando a questão.

(b) Suponha, por absurdo, que $\text{ord}\alpha < 1 + \exp(\limsup_{n\to\infty} \frac{\log\log(a_n+1)}{n})$, então existem $\gamma, \gamma' \in \mathbb{R}$ tal que

$$2 + \limsup_{n\to\infty} \frac{\log a_{n+1}}{\log q_n} < \gamma' < \gamma < 1 + \exp(\limsup_{n\to\infty} \frac{\log\log(a_n+1)}{n}). \tag{4}$$

Da primeira desigualdade e da propriedade do $\limsup$ segue que existe $N \in \mathbb{N}$ tal que para todo $n \geqslant N$

$$\frac{\log a_{n+1}}{\log q_n} < \gamma' - 2 \quad \text{e} \quad \log a_{n+1} < (\gamma' - 2) \log q_n,$$

como $q_{n+1} = a_{n+1} q_n + q_{n-1} < 2a_{n+1} q_n$, segue que, para todo $n \geqslant N$

$$\log q_{n+1} < \log 2 + \log a_{n+1} + \log q_n \leqslant \log(2) + (\gamma' - 1) \log q_n$$

Resolvendo a recorrência até N, temos para $n > N$,

$$\log q_n < \log 2 \cdot \left(\sum_{m=0}^{n-N-1} (\gamma' - 1)^m \right) + (\gamma' - 1)^{n-N} \log q_N$$

ou seja, existe alguma constante positiva $K \in \mathbb{R}$, tal que, para todo n maior que N,

$$\log q_n < K(\gamma' - 1)^n.$$

Pela segunda desigualdade de [4], segue que existe sequência (n_j) infinita, tal que para todo j vale

$$\exp\left(\frac{\log\log(a_{n_j} + 1)}{n_j} \right) > \gamma - 1$$

portanto

$$\log(a_{n_j} + 1) > (\gamma - 1)^{n_j},$$

pela concavidade do log,

$$\log a_{n_j} + 1 > \log a_{n_j} + \frac{1}{a_{n_j}} > \log(a_{n_j} + 1) > (\gamma - 1)^{n_j}$$

e sendo bem gastosos e supondo n_j suficientemente grande,

$$\log a_{n_j} > \frac{(\gamma - 1)^{n_j}}{2}.$$

Agora vamos calcular um lowerbound para $\operatorname{ord}\alpha$ usando essa sequência, segue que

$$\operatorname{ord}\alpha > 2 + \lim_{j \to \infty} \frac{\log a_{n_j}}{\log q_{n_j - 1}} > 2 + \lim_{n_j \to \infty} \frac{(\gamma - 1)^{n_j}}{2K(\gamma' - 1)^{n_j - 1}} = \infty.$$

o que é absurdo (na verdade provamos que deve ser que $\operatorname{ord}\alpha = \infty$, de onde a desigualdade segue trivialmente).

Para **(c)**, se $c = 2$ basta tomar $a_n = 1$ e o resultado segue. Caso $c > 2$, queremos $a_n \in \mathbb{Z}$ tal que

$$1 + \exp(\lim_{n \to \infty} \frac{\log\log(a_n + 1)}{n}) = c$$

desenvolvendo, uma alternativa seria

$$a_n + 1 = \exp\exp(n \log(c - 1)).$$

Para facilitar as contas, vamos tomar $\alpha = [0; a_1, a_2, \dots]$ para a_n sendo

$$a_n = \lceil \exp\exp(n \log(c - 1)) \rceil \in \mathbb{N}^*$$

e veremos que $\text{ord}\alpha = c$. Já sabemos que

$$\begin{aligned}\text{ord}\alpha &\geqslant 1 + \exp(\limsup_{n\to\infty} \frac{\log\log(a_n+1)}{n}) \\ &\geqslant 1 + \exp(\limsup_{n\to\infty} \frac{\log\log(\exp\exp(n\log(c-1)))}{n}) \\ &\geqslant 1 + \exp(\limsup_{n\to\infty} \log(c-1)) = c\end{aligned}$$

Para a outra desigualdade, lembramos que

$$q_n = a_n q_{n-1} + q_{n-2} \geqslant a_n q_{n-1}$$

e portanto, por indução

$$\log q_n \geqslant \sum_{j=1}^{n} \log a_j$$

substituindo nossos valores e usando a soma da progressão aritmética, temos

$$\log q_n \geqslant \sum_{j=1}^{n} \exp(j\log(c-1)) = \frac{\exp((n+1)\log(c-1)) - \exp(\log(c-1))}{\exp(\log(c-1)) - 1} = \frac{(c-1)^{n+1} - (c-1)}{c-2}.$$

Temos também que (para n suficientemente grande)

$$\log a_{n+1} \leqslant \log(2\exp\exp((n+1)\log(c-1))) = \log(2) + \exp(n\log(c-1)) = \log(2) + (c-1)^{n+1}$$

Logo,

$$\text{ord}\alpha = 2 + \limsup_{n\to\infty} \frac{\log a_{n+1}}{q_n} \leqslant 2 + \limsup_{n\to\infty} \frac{(c-2)((c-1)^{n+1} + \log(2))}{(c-1)^{n+1} - (c-1)} = 2 + c - 2 = c.$$

(d) Basta usar o que já conhecemos. De $q_n = a_n q_{n-1} + q_{n-2}$, temos

$$\sum_{i=1}^{n} \log a_n \leqslant q_n \leqslant \sum_{i=1}^{n} \log(a_n+1) \leqslant \sum_{i=1}^{n} \log(a_n+1) \leqslant \sum_{i=1}^{n} \log(a_n) + \frac{1}{a_n}$$

portanto, se $a_n = 2^n$, segue

$$\frac{n(n-1)\log 2}{2} = \log 2\left(\sum_{i=1}^{n} i\right) \leqslant \log q_n \leqslant \log 2\left(\sum_{i=1}^{n} i\right) + 1 = \frac{n(n-1)\log 2}{2} + 1$$

ou seja $\log q_n = \Theta(n^2)$, substituindo na fórmula de $\text{ord}\alpha$, vemos

$$\text{ord}\alpha = 2 + \limsup_{n\to\infty} \frac{\log a_{n+1}}{\log q_n} = 2 + \limsup_{n\to\infty} \frac{(n+1)\log 2}{\Theta(n^2)} = 2.$$

□

Problem 2.4. Seja $\alpha = [a_0; a_1, a_2 \ldots] \in \mathbb{R}$. Prove que, se $q_n \leqslant q < q_{n+1}$, $(p,q) = 1$ e $p/q \neq p_n/q_n$ então vale $|p/q - \alpha| < 1/q^2$ se e somente se vale uma das seguintes condições:

(i) $\alpha_{n+1} \geqslant 2$, $p/q = (p_{n+1} - p_n)/(q_{n+1} - q_n)$ e $a_{n+1} + \beta_{n+1} - 2 < \alpha_{n+2}$ ou

(ii) $\alpha_{n+1} \geqslant 2$, $p/q = (p_n + p_{n-1})/(q_n + q_{n-1})$ e $(\alpha_{n+1} - 2)\beta_{n+1} < 1$.

Proof. **RESOLUÇÃO INCOMPLETA.** Vou fazer só a volta que envolve somente manipulações feias. Suponha que vale (i), notamos primeiramente que

$$pq_{n+1} - qp_{n+1} = p_{n+1}q_{n+1} - p_n q_{n+1} - q_{n+1}p_{n+1} + q_n p_{n+1} = q_n p_{n+1} - p_n q_{n+1} = (-1)^n$$

logo $(p,q) = 1$ e $p/q \neq p_n/q_n$. Temos também que

$$q_n \leqslant (a_{n+1} - 1)q_n \leqslant (a_{n+1} - 1)q_n + q_{n-1} = q = q_{n+1} - q_n < q_{n+1}$$

já que $a_{n+1} \geqslant 2$. Para estimar o erro da aproximação, notamos

$$\begin{aligned}
\left|\alpha - \frac{p}{q}\right| \leqslant \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| + \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p}{q}\right| &= \frac{1}{(\alpha_{n+2} + \beta_{n+2})q_{n+1}^2} + \frac{|pq_{n+1} - qp_{n+1}|}{qq_{n+1}} \\
&= \frac{1}{(\alpha_{n+2} + \beta_{n+2})q_{n+1}^2} + \frac{1}{qq_{n+1}} = \frac{q + q_{n+1}(\alpha_{n+2} + \beta_{n+2})}{q(\alpha_{n+2} + \beta_{n+2})q_{n+1}^2} \\
&= \frac{q + q_{n+1}\alpha_{n+2} + q_n}{q(\alpha_{n+2} + \beta_{n+2})q_{n+1}^2} = \frac{\alpha_{n+2} + 1}{q(\alpha_{n+2} + \beta n + 2)q_{n+1}}
\end{aligned}$$

agora, essa última expressão é menor que $1/q^2$ se e só se

$$\begin{aligned}
\frac{\alpha_{n+2} + 1}{(\alpha_{n+2} + \beta_{n+2})q_{n+1}} &< \frac{1}{q} \\
q\alpha_{n+2} + q &< q_{n+1}\alpha_{n+2} + q_n \\
q_{n+1} &< q_n(\alpha_{n+2} + 2) \\
a_{n+1} + \beta_{n+1} &\leqslant \alpha_{n+2} + 2
\end{aligned}$$

o que finaliza a primeira parte.

Agora vamos supor que vale (ii). Notamos que $q_n \leqslant q_n + q_{n-1} = q < a_{n+1}q_n + q_{n-1} = q_{n+1}$, pois $\alpha_{n+1} \geqslant 2$. Além disso, temos

$$\frac{p}{q} - \frac{p_n}{q_n} = \frac{p_n q_n + q_n p_{n-1} - p_n q_n - q_{n-1}p_n}{qq_n} = \frac{(-1)^n}{qq_n},$$

portanto, $(p,q) = 1$ (por causa do numerador) e $p/q \neq p_n/q_n$. É sabido que, sob essas condições, $p/q \notin [p_n/q_n, p_{n+1}/q_{n+1}]$ e que para n par, $p_n/q_n < \alpha \leqslant p_{n+1}/q_{n+1}$ e para n ímpar vale a desigualdade oposta, $p_{n+1}/q_{n+1} \leqslant \alpha < p_n/q_n$, a partir disso e da equação anterior, temos que

$$p_n/q_n < \alpha < p/q \text{ se } n \text{ par} \quad \text{e} \quad p/q < \alpha < p_n/q_n \text{ se } n \text{ ímpar.}$$

De qualquer maneira, vale que

$$\begin{aligned}
\left|\alpha - \frac{p}{q}\right| = \left|\frac{p}{q} - \frac{p_n}{q_n}\right| - \left|\alpha - \frac{p_n}{q_n}\right| &= \frac{1}{qq_n} - \frac{1}{(\alpha_{n+1} + \beta_{n+1})q_n^2} \\
&= \frac{q_n(\alpha_{n+1} + \beta_{n+1}) - q}{q(\alpha_{n+1} + \beta_{n+1})q_n^2} = \frac{q_n\alpha_{n+1} + q_{n-1} - q_n - q_{n-1}}{q(\alpha_{n+1} + \beta_{n+1})q_n^2} \\
&= \frac{(\alpha_{n+1} - 1)}{q(\alpha_{n+1} + \beta_{n+1})q_n}
\end{aligned}$$

então, para a afirmação, basta mostrar que sob nossas condições,

$$\frac{\alpha_{n+1} - 1}{(\alpha_{n+1} + \beta_{n+1})q_n} < \frac{1}{q}$$

□

ou equivalentemente

$$\begin{aligned} q\alpha_{n+1} - q &< (\alpha_{n+1} + \beta_{n+1})q_n \\ q_{n-1}\alpha_{n+1} - q_n - q_{n-1} &< q_{n-1} \\ (\alpha_{n+1} - 2) &< \frac{q_n}{q_{n-1}} = \frac{1}{\beta_{n+1}} \end{aligned}$$

como queríamos mostrar.

Problem 2.5. Prove que se a e b são inteiros positivos tais que $4ab - 1 \mid (4a^2 - 1)^2$, então $a = b$.

Proof. Primeiramente, notamos que, sendo $(4ab - 1, b) = 1$, então

$$\begin{aligned} 4ab - 1 \mid (4a^2 - 1)^2 &\iff 4ab - 1 \mid (4a^2 - 1)^2 \cdot b^2 \\ &\iff 4ab - 1 \mid (4a^2 b - b)^2 \\ &\iff 4ab - 1 \mid (a - b)^2 \\ &\iff \exists k \in \mathbb{N}, (a - b)^2 = (4ab - 1)k \end{aligned}$$

e portanto o problema é simétrico em relação as variáveis a, b. Suponha, sem perda de generalidade, que existe solução (a, b) com $a > b$ e a mínimo. Segue que existe $k \in \mathbb{N}$ tal que

$$(a - b)^2 = (4ab - 1)k \quad \text{ou seja} \quad a^2 - (2b + 4bk)a + b^2 + k = 0,$$

note que a é solução de $p(x) = x^2 - (2b + 4bk)x + b^2 + k = 0$. Sabemos que existe outra solução a', tal que $p(a') = 0$ e

(i) $a' + a = 2b + 4bk$

(ii) $a' \cdot a = b^2 + k$

Agora, segue de (i) que $a' \in \mathbb{Z}$ e segue de (ii) que $a' = \frac{b^2+k}{a} > 0$, logo $a' \in \mathbb{N}$. Como $p(a') = 0$, segue que (a', b) é solução também. Sendo $k = (a - b)^2/(4ab - 1)$, segue que

$$a' = \frac{b^2 + \frac{(a-b)^2}{(4ab-1)}}{a} < b + \frac{a^2}{3a^2} = b + \frac{1}{3}$$

portanto, $a' \leqslant b$. Agora, se $a' = b$, então, por (i) $b \mid a$ e por (ii) $b \mid k$, logo $(a/b, 1)$ é uma soulução menor o que é absurdo. Se $a' < b$, temos que (b, a') é uma solução menor e também temos absurdo. $\square$

Problem 2.6. Demonstre que $2x^2 - 219y^2 = -1$ não tem soluções inteiras, mas $2x^2 - 219y^2 \equiv -1 \pmod{m}$ tem soluções para todo inteiro positivo m.

Proof. Para a primeira parte, suponha que existe solução $(x_0, y_0) \in \mathbb{N}^2$ com x_0 mínimo. Seguindo a dica, notamos que $(x_1, y_1) = (|293x_0 - 3066y_0|, |-28x_0 + 293y_0|)$, pois

$$\begin{gathered} 2(293x_0 - 3066y_0)^2 - 219(-28x_0 + 293y_0)^2 = \\ [2(293)^2 - 219(28)^2]x_0^2 - [219(293)^2 - 2(3066)^2]y_0^2 + [219(2(28)(293)) - 2(2(293)(3066))]x_0y_0 = \\ 2x_0^2 - 219y_0^2 = -1 \end{gathered}$$

(óbviamente). Agora, segue de x_0 ser minimal que $x_0 \leqslant x_1$ e portanto,

$$x_0 \leqslant 293x_0 - 3066y_0 \quad \vee \quad x_0 \leqslant 3066y_0 - 293x_0$$

que é equivalente a

$$x_0 \geqslant \frac{3066}{292}y_0 \quad \vee \quad x_0 \leqslant \frac{3066}{294}y_0$$

mas verificamos que para $2x_0^2 - 219y_0^2 = -1$, devemos ter

$$x_0^2 - \frac{219}{2}y_0^2 + \frac{1}{2} = 0$$

ou seja, como estamos tomando x_0 positivo,

$$\sqrt{\frac{218}{2}}y_0 < x_0 = \sqrt{\frac{219y_0^2 - 1}{2}} < \sqrt{\frac{219}{2}}y_0$$

mas, usando uma calculadora,

$$(10.42...)y_0 = \frac{3066}{294}y_0 < 10.4402y_0 < \sqrt{\frac{218}{2}}y_0 < x_0 < \sqrt{\frac{219}{2}}y_0 < 10.4643y_0 < \frac{3066}{292}y_0 = 10.5y_0$$

absurdo.

Para a segunda parte (mostrar que admite solução módulo m), vamos separar em casos.

Caso m primo: se $m = 2$, então $(0, 1)$ é solução; se $m = 3$, então $(1, 0)$ é solução; se $m = 73$, $(6, 1)$ é solução. Se m é qualquer outro primo, então $(m, 2) = 1$ e $(m, 219) = 1$ e portanto queremos achar soluções módulo m para

$$2x^2 \equiv 219y^2 - 1 \pmod{m}.$$

Agora note que se definimos a função $f : \mathbb{Z}_m \to \mathbb{Z}_m$ dada por $f(x) = 2x^2 \pmod{m}$, segue, como há exatamente $(m-1)/2$ resíduos quadráticos, que $|f(\mathbb{Z}_m)| = (p+1)/2$. Da mesma forma, definindo $g : \mathbb{Z}_m \to \mathbb{Z}_m$ dada por $g(y) = 219y^2 - 1$, temos $|g(\mathbb{Z}_m)| = (p+1)/2$. Pelo principio da casa dos pombos, existe $(x, y) \in (\mathbb{Z}_m)^2$ tal que $f(x) = g(y)$ e portanto solução $\pmod{m}$.

Caso $m = p^\alpha$ para p primo e $\alpha > 1$: seguindo a ideia do Joseph, vamos tentar provar por indução em α. Seja (x, y) solução para

$$2x^2 - 219y^2 + 1 \equiv 0 \pmod{p^\alpha} \quad \text{ou seja} \quad 2x^2 - 219y^2 + 1 = kp^\alpha$$

Se $k \equiv 0 \pmod{p}$, já temos o resultado. Podemos supor que $k \not\equiv 0 \pmod{p}$. Vamos olhar para as soluções $\pmod{p^\alpha}$ dadas por $(x + ap^\alpha, y + bp^\alpha)$ para $a, b \in \mathbb{Z}$, note que

$$\begin{aligned}
2(x + ap^\alpha)^2 - 219(y + bp^\alpha)^2 + 1 &\equiv (2x^2 - 219y^2 + 1) + (4xap^\alpha - 437ybp^\alpha) \pmod{p^{\alpha+1}} \\
&\equiv kp^\alpha + p^\alpha(4xa - 438yb) \pmod{p^{\alpha+1}} \\
&\equiv p^\alpha(k + 4xa - 438yb) \pmod{p^{\alpha+1}}
\end{aligned}$$

então basta que $k + 4xa - 438yb \equiv 0 \pmod{p}$. Se $(4x, p) = 1$, então independente do valor de b e k, sempre conseguimos achar a que satisfaz a equação. Se $(4x, p) = p$, ou $p = 2$ ou $p \mid x$. Se $p \mid x$,

$$219y^2 \equiv 2x^2 - 219y^2 \equiv -1 \pmod{p}$$

e portanto $(p, y) = 1$, donde segue que sempre podemos escolher b a fim de satisfazer a equação. Caso $p = 2$ e $\alpha = 2$, então $(1, 1)$ é solução, se $\alpha \geqslant 3$, buscamos soluções levemente diferentes. Olhemos para $(x + a2^{\alpha-1}, y + b2^{\alpha-1})$ com $a, b \in \mathbb{Z}$. Repetindo a conta anterior, temos

$$\begin{aligned}
2(x + a2^{\alpha-1})^2 - 219(y + b2^{\alpha-1})^2 + 1 &\equiv (2x^2 - 219y^2 + 1) + ax2^{\alpha+1} + a^2 2^{2\alpha-1} - 219yb2^\alpha - 219b^2 2^{2\alpha-2} \\
&\equiv 2^\alpha(k - 219yb) \pmod{2^{\alpha+1}}
\end{aligned}$$

mas já estamos supondo k ímpar e $y \equiv 1 \pmod 2$ pois $2x^2 - 219y^2 \equiv 1 \pmod 2$. Portanto $k - 219y \equiv 0 \pmod 2$ e tomando $b = 1$ temos solução.

Agora moralmente terminamos, pois para $m = p^\alpha$ com p primo sempre conseguimos solução e basta usar o Teorema Chinês dos Restos. Se $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ com os p_j primos distintos, então, para cada i, encontramos solução

$$2x_i^2 - 219y_i^2 \equiv -1 \pmod{p_i^{\alpha_i}}$$

aplicando o TCM nos sistemas

$$x \equiv x_i \pmod{p_i^{\alpha_i}} \quad \wedge \quad y \equiv y_i \pmod{p_i^{\alpha_i}} \quad \forall 1 \leqslant i \leqslant n$$

encontramos $x \in \mathbb{Z}_m$ e $y \in \mathbb{Z}_m$ tal que

$$2x^2 - 219y^2 \equiv -1 \pmod m$$

$\square$

3 Lista 3 - 09/02/2026

Problem 3.1. Uma pulseira é formada por pedras coloridas, de mesmo tamanho, pregadas em volta de um círculo de modo a ficarem igualmente espaçadas. Duas pulseiras são consideradas iguais se, e somente se, suas configurações de pedras coincidem por uma rotação. Se há pedras disponíveis de $k \geqslant 1$ cores distintas, mostre que o número de pulseiras diferentes possíveis com n pedras é dado pela expressão

$$\frac{1}{n} \sum_{d|n} \varphi(d) \cdot k^{n/d}$$

Precisaremos de uma ferramenta famosa para contagens desse tipo.

Lemma 3.1. (Burnside) Seja $G \curvearrowright X$ uma ação de um grupo finito G sob um conjunto finito X. Dado $g \in G$, denotamos $N(g) = \{x \in X \mid g \cdot x = x\}$, i.e. os elementos fixados por g. Então vale a seguinte igualdade

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |N(g)|.$$

A prova desse lema envolve somente contagem e o teorema de Lagrange. Se necessário, provarei, ele em um apêndice. Agora podemos dar seguimento ao problema.

Proof. (do Exercício) Conseguimos encaixar precisamente o contexto dado no problema nas condições do Lema. Definimos $X = [k]^n$ os vetores com n entradas e coordenadas em $\{1, 2 \dots k\}$ e seja G o grupo das rotações das pulseiras, podemos tomar $G \cong (\mathbb{Z}_n, +)$. Dada $r \in G$ rotação e $\vec{x} = (x[1], x[2], \dots x[n]) \in X$ vetor de pedras coloridas, definimos a ação

$$(r \cdot \vec{x})[(i + r)] = x[i]$$

onde os índices são tomados módulo n. Por exemplo, se $n = 3$, $k = 3$, $\vec{x} = (1, 2, 3)$ e $r = \bar{2}$, temos $r \cdot \vec{x} = (2, 3, 1)$, rodamos as entradas do vetor em duas posições para a direita.

Notamos que as classes em $|X/G|$ são exatamente as pulseiras em que estamos interessados em contar. Aplicando o lema, teriamos

$$\#\{\text{pulseiras}\} = \frac{1}{n} \sum_{r \in \mathbb{Z}_n} \#\{\text{vetores fixados por } r\}$$

Então basta calcular quantos vetores são fixados por cada rotação $r \in Z_n$. Se $r \cdot x = x$, segue que para todo $i \in \mathbb{Z}_n$, $x[i + r] = x[i]$, consequentemente, para todo $a \in \mathbb{Z}$ e portanto para todo $a \in \mathbb{Z}_n$

$$x[i + ar] = x[i]$$

onde novamente aqui as somas nos índices são tomadas módulo n. Isso é, se fixarmos a cor de $x[i]$, fixamos a cor de todos os índices $\{i + ar \pmod n) \mid a \in \mathbb{Z}_n\}$. Mas, se $d = (r, n)$,

$$|\{i + ar \pmod n \mid a \in \mathbb{Z}_n\}| = |\{ar \pmod n \mid a \in \mathbb{Z}_n\}| = \frac{n}{d}$$

Portanto, fixando um elemento, determinamos n/d outros. Como a pulseira tem n elementos, podemos fazer d escolhas entre as k cores. Logo $|N(r)| = k^d$. Substituindo no Lema,

$$\#\{\text{pulseiras}\} = \frac{1}{n} \sum_{r=0}^{n-1} k^{(r,n)} = \frac{1}{n} \sum_{d|n} \varphi(d) k^{n/d}$$

onde a última igualdade segue do fato que

$$\sum_{i=1}^{n} k^{(r,n)} = \sum_{i=1}^{n}\sum_{d|n} \mathbb{1}[d=(i,n)]k^d = \sum_{d|n} k^d \cdot \left(\sum_{i=1}^{n} \mathbb{1}[(i,n)=d]\right) = \sum_{d|n} k^d \varphi(n/d)$$

□

Proof. (Segunda prova mais fácil) □

Problem 3.2. Dadas duas funções $f, g : \mathbb{N}^* \to \mathbb{C}$, definimos a convolução de Dirichlet $f * g : \mathbb{N}^* \to \mathbb{C}$ de f e g por

$$f * g(n) := \sum_{d|n} f(d)g(n/d) = \sum_{d_1 d_2 = n} f(d_1)g(d_2) \tag{5}$$

(a) Prove que, se $s \in \mathbb{C}$ e as séries $\sum_{n\geqslant 1} \frac{f(n)}{n^s}$ e $\sum_{n\geqslant 1} \frac{g(n)}{n^s}$ convergem absolutamente, então

$$\sum_{n\geqslant 1} \frac{f(n)}{n^s} \cdot \sum_{n\geqslant 1} \frac{g(n)}{n^s} = \sum_{n\geqslant 1} \frac{(f*g)(n)}{n^s}$$

Proof. Como as séries convergem absolutamente, o produto converge absolutamente e podemos reordenar os índices de qualquer forma (contanto que apareçam todos). Portanto,

$$\sum_{n\geqslant 1} \frac{f(n)}{n^s} \cdot \sum_{m\geqslant 1} \frac{g(m)}{n^s} = \sum_{n,m\geqslant 1} \frac{f(n)g(m)}{(nm)^s} = \sum_{n\geqslant 1} \frac{1}{n^s} \cdot \left(\sum_{d_1 d_2 = n} f(d_1)g(d_2) \right) = \sum_{n\geqslant 1} \frac{(f*g)(n)}{n^s}.$$

□

(b) Prove que para quaisquer funções $f, g, h : \mathbb{N}^* \to \mathbb{C}$, temos $f * g = g * f$ e $f * (g * h) = (f * g) * h$ (comutatividade e associatividade), e que a função $I : \mathbb{N}^* \to \mathbb{C}$ dada por

$$I(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases}$$

é o elemento neutro da operação $*$.

Proof. A comutatividade segue diretamente da involução nos índices $d \to n/d$, segue que

$$f * g(n) = \sum_{d|n} f(d)g(n/d) = \sum_{d'|n} f(n/d')g(d') = g * f(n).$$

Associatividade é vista melhor da segunda forma,

$$f * (g * h)(n) = \sum_{d_1 x = n} f(d_1)(g * h)(x) = \sum_{d_1 x = n} \sum_{d_2 d_3 = x} f(d_1)g(d_2)h(d_3) = \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3)$$

da mesma forma,

$$(f * g) * h(n) = \sum_{x d_3 = n} (f * g)(x)g(d_3) = \sum_{x d_3 = n} \sum_{d_1 d_2 = x} f(d_1)g(d_2)h(d_3) = \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3)$$

Por fim, para todo $n \in \mathbb{N}^*$,

$$(I * f)(n) = \sum_{d|n} I(d)f(n/d) = f(n)$$

logo, $I * f = f$. □

(c) Prove que se f e g são multiplicativas, então $f * g$ é multiplicativa.

Proof. Sejam $n, m \in \mathbb{N}^*$ com $(n,m) = 1$, então $(f * g)(nm) = \sum_{dd'=nm} f(d)g(d')$. Escrevendo $d = (d,n) \cdot (d,m) = d_n d_m$ e $d' = (d',n)(d',m) = d'_n d'_m$, como $dd' = nm$, devemos ter que $(d_n, d_m) = (d'_n, d'_m) = 1$, $d_n d'_n = n$ e $d_m d'_m = m$. Logo,

$$\begin{aligned}(f * g)(nm) &= \sum_{\substack{(d_n d'_n = n)\\(d_m d'_m = m)}} f(d_n d_m) g(d'_n d'_m) = \sum_{\substack{(d_n d'_n = n)\\(d_m d'_m = m)}} f(d_n) f(d_m) g(d'_n) g(d'_m)\\ &= \Bigg(\sum_{(d_n d'_n = n)} f(d_n) g(d'_n)\Bigg)\Bigg(\sum_{(d_m d'_m = m)} f(d_m) g(d'_m)\Bigg) = (f * g)(n) \cdot (f * g)(m)\end{aligned}$$

□

(d) Prove que, se $f : \mathbb{N}^* \to \mathbb{C}$ é tal que $f(1) \neq 0$, então existe uma única função $g : \mathbb{N}^* \to \mathbb{C}$ tal que $f * g = I$, a qual é dada recursivamente por $g(1) = 1/f(1)$ e, para $n > 1$

$$g(n) = \frac{-1}{f(1)} \sum_{d|n, d \neq n} f(n/d) g(d).$$

Proof. A condição $(f * g)(1) = I(1) = 1$ determina únicamente que $g(1) = 1/f(1)$. Para $n > 1$, basta notar que deveríamos ter

$$0 = I(n) = (f * g)(n) = \sum_{d|n} g(d) f(n/d) \iff f(1) g(n) = -\sum_{d|n, d \neq n} f(n/d) g(d)$$

o que implica a fórmula. □

(e) Prove que, se f é multiplicativa então a função $f^{(-1)} = g$ definida no item anterior é multiplicativa.

Proof. Primeiramente, como f é multiplicativa, $f(1) = 1 = g(1)$ (não pode ser 0 senão não teria inversa). Vamos provar por indução em n que para todo $ab = n$ com $(a,b) = 1$, vale $g(n) = g(a)g(b)$ e portanto que g é multiplicativa. O resultado segue para $n = 1$, suponha que vale para todo $m < n$ e seja $n = ab$ com $(a,b) = 1$. Segue que

$$g(ab) = -\sum_{\substack{d|ab\\ d \neq ab}} g(d) f(ab/d) = -\sum_{\substack{d_a|a, d_b|b\\ d_a d_b \neq ab}} g(d_a d_b) f\Big(\frac{ab}{d_a d_b}\Big) \tag{6}$$

$$= -\sum_{\substack{d_a|a, d_b|b\\ d_a d_b \neq ab}} g(d_a) g(d_b) f\Big(\frac{a}{d_a}\Big) f\Big(\frac{b}{d_b}\Big) \tag{7}$$

$$= -\Bigg[\Bigg(\sum_{d_a|a} g(d_a) f(a/d_a)\Bigg)\Bigg(\sum_{d_a|a} g(d_a) f(a/d_a)\Bigg) - g(a) f(1) g(b) f(1)\Bigg] \tag{8}$$

Agora, segue da fórmula do item anterior que

$$\sum_{d_a|a} g(d_a) f(a/d_a) = g(a) f(1) + \sum_{d_a|a, d_a \neq a} g(d_a) f(a/d_a) = g(a) f(1) - f(1) g(a) = 0,$$

portanto [8] se torna

$$-[0 - g(a) g(b) f(1)^2] = g(a) g(b)$$

pois $f(1) = 1$. □

Problem 3.3. Prove que, se $\alpha > 2$, então

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^\alpha} = \sum_{n=1}^{\infty} \frac{1}{n^{\alpha-1}} \Big/ \sum_{n=1}^{\infty} \frac{1}{n^\alpha}.$$

Proof. Como $\alpha > 2$ e $1 \leqslant \varphi(n) \leqslant n$, todos os somatórios são absolutamente convergentes. Basta mostrar que

$$\left(\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^\alpha}\right)\left(\sum_{n=1}^{\infty} \frac{1}{n^\alpha}\right) = \sum_{n=1}^{\infty} \frac{1}{n^{\alpha-1}}.$$

Mas usando a equação [5] de (3.a) com $f(n) = \varphi(n)$ e $g(n) = 1$, temos

$$\left(\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^\alpha}\right)\left(\sum_{n=1}^{\infty} \frac{1}{n^\alpha}\right) = \sum_{n=1}^{\infty} \frac{(f * g)(n)}{n^\alpha} =$$
$$= \sum_{n=1}^{\infty} \frac{1}{n^\alpha} \sum_{d \mid n} \varphi(d) = \sum_{n=1}^{\infty} \frac{n}{n^\alpha} = \sum_{n=1}^{\infty} \frac{1}{n^{\alpha-1}}$$

onde usamos o fato de que para todo $n \in \mathbb{N}^*$, vale que

$$\sum_{d \mid n} \varphi(d) = n.$$

□

Problem 3.4. Mostre que o conjunto

$$\left\{ \frac{\varphi(n)}{n} \;\middle|\; n \in \mathbb{N}^* \right\}$$

é denso em $[0, 1]$.

Precisaremos de um Lema fácil.

Lemma 3.2. Seja $\sum_{n=1}^{\infty} a_n = \infty$ uma série divergente de termos positivos com $a_n \to 0$, então o conjunto

$$M = \left\{ \sum_{n \in A} a_n \mid A \subset \mathbb{N}, |A| < \infty \right\}$$

é denso em $(0, \infty)$ e portanto em $[0, \infty)$.

Proof. Dados quaisquer $x > 0$ e $\varepsilon > 0$, queremos encontrar um ponto de M em $(x - \varepsilon, x + \varepsilon)$. Como $a_n \to 0$, existe N tal que $\forall m \geqslant N$, $a_m < \min(\varepsilon, x)$. Como $a_N < x$, $\sum_{n \geqslant N} a_n = \infty$ e os a_n são positivos, segue que existe um índice mínimo $j > N$ tal que

$$x + \varepsilon < \sum_{n=N}^{j+1} a_n$$

e portanto,

$$x + \varepsilon > \sum_{n=N}^{j} a_n = \left(\sum_{n=N}^{j+1} a_n\right) - a_{j+1} \geqslant (x + \varepsilon) - \varepsilon = x$$

ou seja, se $A = \{n \mid N \leqslant n \leqslant j\}$, segue que $\sum_{n \in A} a_n \in (x - \varepsilon, x + \varepsilon)$. □

Agora podemos dar seguimento à solução do problema.

Proof. (Do exercício) Escrevendo
$$\frac{\varphi(n)}{n}=\prod_{p|n}\left(1-\frac{1}{p}\right)$$
com os p primos. Vemos que o problema se resume a determinar se o conjunto
$$S=\left\{\prod_{p\in A}(1-\frac{1}{p})\ \mid\ A \text{ conjunto finito de primos}\right\}$$
é denso em $[0,1]$. Tomando $-\log$ (que é uma função contínua) em S, é equivalente também a verificar que
$$-\log(S)=\left\{\sum_{p\in A}-\log(1-\frac{1}{p})\ \mid\ A \text{ conjunto finito de primos}\right\}$$
é denso em $\mathbb{R}^+$. Mas, lembrando que $x-x^2/2\leqslant\log(1+x)\leqslant x$ para $x>1$, segue que
$$\sum_{p_n \text{ primo}}-\log(1-\frac{1}{p_n})\geqslant\sum_{p_n \text{ primo}}\frac{1}{p_n}=\infty$$
e que $0<-\log(1-\frac{1}{p_n})<\frac{1}{p_n}+\frac{1}{2p_n^2}\to 0$ quando $n\to\infty$. Portanto, pelo Lema anterior, $-\log(S)$ é denso em $[0,\infty)$, logo S é denso em $(0,1)$ e por consequência em $[0,1]$. $\square$

Problem 3.5. Seja $f:\mathbb{N}\to[0,\infty)$ uma função decrescente. Prove que a série
$$\sum_{p \text{ primo}} f(p)$$
converge se, e somente se, a série
$$\sum_{n=2}\frac{f(n)}{\log(n)}$$
converge. Em particular, mostre que $\sum_{p \text{ primo}}1/p=+\infty$, mas $\sum_{p \text{ primo}}1/(p\log(p))<\infty$ converge.

Tem um leminha útil para esse problema.

Lemma 3.3. Seja $f:[0,\infty)\to[0,\infty)$ uma função decrescente. Para toda constante $C>0$, $\sum_{n\geqslant 0}f(n)<\infty$ se, e somente se, $\sum_{n\geqslant 0}f(Cn)<\infty$.

Proof. Basta mostrar a ida, pois a recíproca é equivalente tomando $g(n)=f(Cn)$. Se $C\geqslant 1$, $f(n)\geqslant f(Cn)$ e
$$\sum_{n\geqslant 0}f(Cn)<\sum_{n\geqslant 0}f(n)<\infty.$$
Se $0<C<1$, tome $M\in\mathbb{N}$ tal que $1/M\leqslant C$, vale que
$$\sum_{n=0}^{\infty}f(Cn)\leqslant\sum_{n=0}^{\infty}f\left(\frac{n}{M}\right)=\sum_{k=0}^{\infty}\sum_{n=kM}^{(k+1)M-1}f\left(\frac{n}{M}\right)\leqslant\sum_{k=0}^{\infty}Mf(k)<\infty.$$
$\square$

Proof. (Do exercício) Pelo Teorema de Chebyshev, existem constantes $0<A<B$ tal que, se p_n é o n-ésimo primo, vale que
$$An\log n<p_n<Bn\log n,$$

portanto, se $\sum_{p_n} f(p_n) < \infty$, segue que

$$\sum_{n\geqslant 1} f(Bn\log n) \leqslant \sum_{n\geqslant 1} f(p_n) < \infty.$$

Pelo lema anterior, chamando $g(n) = f(Bn\log n)$, segue que para todo $C > 0$, $\sum_{n\geqslant 1} g(Cn) < \infty$. Em particular, tomando $C < \frac{A}{B}$, segue que para M grande o suficiente, se $n \geqslant M$, então $An\log n > CBn\log(Cn)$ e portanto,

$$\sum_{n\geqslant M} f(An\log n) \leqslant \sum_{n\geqslant M} f(CBn\log(n) + n\log(C/B)) \leqslant \sum_{n\geqslant 1} g(Cn) < \infty.$$

Na verdade, trocando A por qualquer constante positiva D, provamos que $\sum_{n\geqslant 1} f(Dn\log n) < \infty$. Portanto,

$$\sum_{p_n} f(p_n) < \infty \quad \iff \quad \sum_{n\geqslant 1} f(n\log n) < \infty.$$

Vamos mostrar que $\sum_{n\geqslant 1} f(n\log n) < \infty$ se, e somente se, $\sum_{n\geqslant 2} f(n)/\log n < \infty$. Chamando $w(n) = n\log(n)$, podemos escrever

$$\sum_{n=2}^{\infty} \frac{f(n)}{\log(n)} = C + \sum_{n=3}^{\infty} \sum_{m=\lfloor w(n)\rfloor}^{\lfloor w(n+1)\rfloor - 1} \frac{f(m)}{\log(m)}$$

para algum $C > 0$ que lida com os primeiros termos omitidos. Note que

$$w(n+1) - w(n) = (n+1)\log(n+1) - n\log(n) = \Theta(\log(n))$$

e

$$\log(w(n)) = \log(n\log(n)) = \log(n) + \log\log(n) = \Theta(\log(n)).$$

Segue que

$$\sum_{n=3}^{\infty} \sum_{m=\lfloor w(n)\rfloor}^{\lfloor w(n+1)\rfloor - 1} \frac{f(m)}{\log(m)} \leqslant \sum_{n=3}^{\infty} (w(n+1) - w(n)) \frac{f(w(n))}{\log(w(n))} = \sum_{n=3}^{\infty} \Theta(f(w(n))) < \infty$$

portanto $\sum_{n\geqslant 1} f(w(n)) < \infty$ implica $\sum_{n\geqslant 2} f(n)/\log(n) < \infty$ e da mesma forma,

$$\sum_{n=3}^{\infty} \sum_{m=\lfloor w(n)\rfloor}^{\lfloor w(n+1)\rfloor - 1} \frac{f(m)}{\log(m)} \geqslant \sum_{n=3}^{\infty} (w(n+1) - w(n) - 1) \frac{f(w(n+1))}{\log(w(n+1))} = \sum_{n=3}^{\infty} \Theta(f(w(n)))$$

e temos a volta, $\sum_{n\geqslant 2} f(n)/\log(n) < \infty \Rightarrow \sum_{n\geqslant 1} f(w(n)) < \infty$.

Para a segunda parte da questão, basta verificar que

$$\sum_{n\geqslant 2} \frac{1}{n\log n} = \infty \quad \text{e} \quad \sum_{n\geqslant 2} \frac{1}{n(\log n)^2} < \infty$$

mas segue do fato que

$$\sum_{n\geqslant 2}^{N} \frac{1}{n\log n} = \int_2^N \frac{dx}{x\log x} + O(1) = \log\log N + O(1) \to \infty.$$

Similarmente,

$$\sum_{n\geqslant 2}^{\infty} \frac{1}{n(\log n)^2} = \int_2^{\infty} \frac{dx}{x(\log x)^2} + O(1)$$

fazendo a substituição $u = \log x$, $du = \frac{dx}{x}$, segue

$$\int_2^\infty \frac{dx}{x(\log x)^2} + O(1) = \int_{\log(2)}^\infty \frac{du}{u^2} + O(1) < \infty$$

como queriámos mostrar. $\square$

Problem 3.6. Um número de Sierpinski é um número natural ímpar k tal que $2^n \cdot k + 1$ é composto para todo natural n. Prove que 78557 é um número de Sierpinski, e que existem infinitos números de Sierpinski a partir das congruências

$$\begin{aligned}
78557 \cdot 2^0 + 1 &\equiv 0 \pmod 3\\
78557 \cdot 2^1 + 1 &\equiv 0 \pmod 5\\
78557 \cdot 2^7 + 1 &\equiv 0 \pmod 7\\
78557 \cdot 2^{11} + 1 &\equiv 0 \pmod{13}\\
78557 \cdot 2^3 + 1 \equiv 78557 \cdot 2^{39} + 1 &\equiv 0 \pmod{73}\\
78557 \cdot 2^{15} + 1 &\equiv 0 \pmod{19}\\
78557 \cdot 2^{27} + 1 &\equiv 0 \pmod{37}.
\end{aligned}$$

Proof. Seja $k \in \mathbb{N}$, vamos mostrar que se k é um ímpar suficientemente grande que satisfaz as mesmas recorrências que 78557, então k é de Sierpinski.

Suponha que $k \cdot 2^n + 1$ é primo e $k > 73$, segue que $k \cdot 2^n + 1 \notin \{3, 5, 7, 13, 73, 19, 37\}$ e se $k \cdot 2^n + 1 \equiv 0$ módulo qualquer um desses primos, $k \cdot 2^n + 1$ seria composto.

Como $2^2 \equiv 1 \pmod 3$, se $n \equiv 0 \pmod 2$, então $k \cdot 2^n + 1 \equiv k \cdot 1 + 1 \equiv 0 \pmod 3$. Logo podemos supor que $n \equiv 1 \pmod 2$.

Como $2^4 \equiv 1 \pmod 5$, então se $n \equiv 1 \pmod 4$, segue que $k \cdot 2^n + 1 \equiv k \cdot 2^1 + 1 \equiv 0 \pmod 5$. Podemos supor que $n \equiv 3 \pmod 4$.

De $2^3 \equiv 1 \pmod 7$, segue que se $n \equiv 1 \pmod 3$, então $k \cdot 2^n + 1 \equiv k \cdot 2 + 1 \equiv k \cdot 2^7 + 1 \equiv 0 \pmod 7$. Portanto, temos que $n \equiv \{0, 2\} \pmod 3$. O que, junto com anterior, implica que $n \equiv \{3, 11\} \pmod{12}$.

Como $2^{12} \equiv 1 \pmod{13}$, se $n \equiv 11 \pmod{12}$, então $k \cdot 2^n + 1 \equiv k \cdot 2^{11} + 1 \equiv 0 \pmod{13}$, logo podemos supor $n \equiv 3 \pmod{12}$.

De $78557 \cdot 2^3 + 1 \equiv 78557 \cdot 2^{39} + 1 \pmod{73}$ e $(78557, 73) = 1$, segue que $2^{36} \equiv 1 \pmod{73}$ e, portanto, se $n \equiv 3 \pmod{36}$, então $k \cdot 2^n + 1 \equiv k \cdot 2^3 + 1 \equiv 0 \pmod{73}$. Ou seja, podemos supor $n \equiv \{15, 27\} \pmod{36}$.

Como $2^{18} \equiv 1 \pmod{19}$, então se $n \equiv 15 \pmod 1$8, temos $k \cdot 2^n + 1 \equiv k \cdot 2^{15} + 1 \equiv 0 \pmod{19}$. Ou seja, $n \not\equiv 15 \pmod{36}$ e devemos ter que $n \equiv 27 \pmod{36}$.

De $2^{36} \equiv 1 \pmod{37}$, se $n \equiv 27 \pmod{36}$, então $k \cdot 2^n + 1 \equiv k \cdot 2^{27} + 1 \equiv 0 \pmod{37}$. Mas isso é absurdo, já tinhamos restringido n para $27 \pmod{36}$.

Tomando $k \equiv 1 \pmod 2$, forçamos k a ser ímpar, pelo TCM, existem infinitas soluções para $k > 73$, todas elas de Sierpinski (inclusive 78557). $\square$