

## PROBLEMAS DE TEORIA DOS NÚMEROS: DIVISIBILIDADE, CONGRUÊNCIAS, TEOREMA DE EULER-FERMAT

Nestas notas, vamos abordar alguns problemas envolvendo divisibilidade, congruências e o Teorema de Euler.

O principal problema que motivo estas notas é o Problema 2 da segunda fase da OBM-U de 2017:

**Problema 1** (Problema 2 - OBMU 2017). *Fixados os inteiros positivos  $a$  e  $b$ , mostre que o conjunto dos divisores primos dos termos da sequência*

$$a_b = a \cdot 2017^n + b \cdot 2016^n$$

*é infinito.*

Ainda que motivados por este problema, vamos listar diversos fatos básicos de Teoria dos Números, incluindo definições, propriedades básicas e teoremas.

No que se segue,  $a, b, c, d, m, n, p, q, x, y$  são sempre inteiros.

### Definições.

- (1) Dizemos que  $d$  **divide**  $a$  (denotado por  $d|a$ ) se existe algum inteiro  $k$  tal que  $a = kd$ .
- (2) Dizemos que  $a \equiv b \pmod{m}$  ( $a$  é **congruente a  $b$  módulo  $m$** ) se  $m$  divide  $b - a$ .
- (3) O **maior divisor comum** entre  $a$  e  $b$  (denotado por  $(a, b)$ ) é o maior inteiro  $d$  que divide  $a$  e  $b$  ao mesmo tempo.
- (4) Dizemos que  $p$  é um **número primo** se os únicos inteiros positivos que dividem  $p$  são  $1$  e  $p$ .
- (5) Dizemos que  $a$  e  $b$  são **primos entre si** se o maior divisor comum entre  $a$  e  $b$  é igual a  $1$ .
- (6) A **função phi de Euler** é definida por  $\varphi(n) = \#\{a | 1 \leq a \leq n, (a, n) = 1\}$  (isto é,  $\varphi(n)$  é a quantidade de números menores que  $n$  que são primos entre si com  $n$ .  
Em particular, se  $p$  é primo, então  $\varphi(p) = p - 1$ .

### Propriedades.

- (1) Se  $d|a$  e  $d|b$ , então  $d|ax + by$  para todos inteiros  $x, y$ .
- (2) Se  $d|a$ , então  $|d| \leq |a|$ .
- (3) Se  $d|1$ , então  $d = 1$  ou  $d = -1$ .
- (4) Se  $d|ab$  e  $\text{mdc}(d, a) = 1$ , então  $d|b$ .
- (5) Se  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$ , então  $ax + cy \equiv bx + dy \pmod{m}$ , e  $ac \equiv bd \pmod{m}$  para todos inteiros  $x, y$ .
- (6) Se  $(c, m) = 1$  e  $ac \equiv bc \pmod{m}$ , então  $a \equiv b \pmod{m}$ .
- (7) Se  $a \equiv b \pmod{m_1}$ ,  $a \equiv b \pmod{m_2}$  e  $(m_1, m_2) = 1$ , então  $a \equiv b \pmod{m_1 m_2}$ .
- (8) Se  $(m, n) = 1$ , então  $\varphi(mn) = \varphi(m)\varphi(n)$ .
- (9) Se  $p$  é primo, então  $(a + b)^p \equiv a^p + b^p \pmod{p}$ .

**Exercício 1.** *Demonstre as propriedades acima.*

**Teoremas.**

- (1) (**Divisão euclídeana**) Dados  $a, b$  inteiros, existem únicos inteiros  $q, r$  tais que  $0 \leq r < |b|$  e  $a = bq + r$ .
- (2) (**Bézout**) Dados  $a, b$  inteiros e  $d = (a, b)$ , então existem inteiros  $x, y$  tais que  $d = ax + by$ .
- (3) (**Euclides**) Existem infinitos primos.
- (4) (**Teorema Fundamental da Aritmética**) Todo número natural  $n \geq 2$  pode ser escrito unicamente na forma

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

onde  $p_1, p_2, \dots, p_k$  são números primos distintos,  $k \geq 1$  e  $\alpha_i \geq 1$  para todo  $i$ .

- (5) (**Euler**) Se  $a$  e  $m$  são primos entre si, então  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .
- (6) (**Pequeno teorema de Fermat**) Se  $p$  é primo, então  $a^p \equiv 1 \pmod{p}$ .
- (7) (**Wilson**) Se  $p$  é primo, então  $(p-1)! \equiv -1 \pmod{p}$ .
- (8) (**Teorema chinês dos restos**) Se  $m_1, \dots, m_r$  são dois-a-dois primos entre si, então o sistema de equações

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv b_r \pmod{m_r}$$

admite solução, que é única módulo  $m_1 m_2 \cdots m_r$ .

**Exercício 2.** Consultando qualquer livro de teoria dos números, demonstre os teoremas acima.

## 1. EXERCÍCIOS (NÃO TÃO OLÍMPICOS)

**Exercício 3.** Prove que  $20^{15} - 1$  é um múltiplo de 31.

**Exercício 4.** Mostre que a equação  $x^3 - 117y^3 = 5$  não possui soluções inteiras.

**Exercício 5.** Encontre os últimos dígitos de  $3^{2018}$  na representação decimal.

**Exercício 6.** Encontre todos os inteiros positivos  $n$  tais que  $2n^2 + 1 | n^3 + 9n - 17$ .

Dica:  $|2n^2 + 1| \leq |n^3 + 9n - 17|$  só é válido para poucos valores de  $n$ , pois o polinômio de grau 3 cresce mais rápido que o polinômio de grau 2.

**Exercício 7.** Determine todos os inteiros  $x, y$  tais que  $13x + 5y = 1$ .

**Exercício 8.** Mostre que  $2^{15} - 1$  e  $2^{10} + 1$  são primos entre si.

**Exercício 9.** *Mostre que não existe um inteiro  $m$  tal que  $103|m^3 - 2$ .*

**Exercício 10.** *Mostre que  $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$  não é um inteiro se  $n > 1$ .*

## 2. PROBLEMAS COM EXPOENTE $n$ E O TEOREMA DE EULER

Agora sim, vamos nos focar no tipo de problema que estamos interessados, que são aqueles com expoente  $n$  e que podem ser abordados utilizando o Teorema de Euler.

**Problema 2** (P4 - IMO 2005). *Consideremos a sequência infinita  $a_1, a_2, \dots$  definida por*

$$a_n = 2^n + 3^n + 6^n - 1$$

*para todos  $n \geq 1$ . Determine todos os inteiros positivos que são primos entre si com todos os termos da sequência.*

*Dica: Sabemos o valor de  $a_p \pmod{p}$ . Que tal investigar  $a_{p-1}$  ou  $a_{p-2} \pmod{p}$ ?*

**Problema 3** (P2 - OBMU 2017). *Fixados os inteiros positivos  $a$  e  $b$ , mostre que o conjunto dos divisores primos dos termos da sequência  $a_b = a \cdot 2017^n + b \cdot 2016^n$  é infinito.*

**Problema 4.** *Seja  $n > 1$ , prove que  $n$  não divide  $2^n - 1$ .*

*Dica: considere o menor fator primo  $q$  de  $n$ .*

**Problema 5.** *Seja  $n > 1$ , prove que  $n$  não divide  $3^n - 2^n$ .*

*Dica: considere o menor fator primo  $q$  de  $n$ .*

O seguinte problema também está intimamente relacionado com os teoremas de Wilson e o teorema de Euler.

**Problema 6** (2016 - Problema 3, 2a fase). *Seja  $k \geq 1$  um inteiro. Definimos a sequência  $(a_n)_{n \geq 0}$  por  $a_0 = 0$ ,  $a_1 = 1$  e*

$$a_{n+1} = ka_n + a_{n-1}$$

*para  $n = 1, 2, \dots$ . Seja  $p$  um número primo ímpar. Denote por  $m(p)$  o menor inteiro positivo  $i$  tal que  $p|a_i$ . Denote por  $T(p)$  o menor inteiro positivo tal que para qualquer natural  $j$  temos  $p|a_{j+T(p)} - a_j$ .*

*i) Mostre que  $T(p) \leq m(p)(p-1)$ .*

*ii) Se  $T(p) = m(p)(p-1)$ , mostre que*

$$\prod_{1 \leq j \leq T(p)-1, j \neq 0 \pmod{m(p)}} a_j \equiv (-1)^{m(p)-1} \pmod{p}.$$

## 3. PROBLEMAS DIVERSOS DE TEORIA DOS NÚMEROS

**Problema 7** (IMO 1959). *Mostre que a fração  $\frac{21n+4}{14n+3}$  é irredutível para todo inteiro positivo  $n$ .*

**Problema 8.** *Mostre que existe um inteiro positivo  $n$  tal que  $2^n$  tenha mais de duas mil casas decimais e tenha entre suas 2000 últimas casas decimais 1000 zeros consecutivos.*

*Dica: olhe para os números  $2^{\varphi(5^{2000})}$  e  $2^{2000+\varphi(5^{2000})}$ .*

**Problema 9** (OBM 1991). *Mostre que existe um número da forma  $199 \cdots 991$ , com mais de dois dígitos 9, que é múltiplo de 1991.*

**Problema 10** (OBM 1998). *Determine todos os primos que são a soma e a diferença de dois primos.*

**Problema 11** (OBM). *Encontre todas as soluções da equação  $n^a + n^b = n^c$ , para  $n, a, b$  e  $c$  estritamente positivos.*

**Problema 12.** *Prove que para todo  $n$ , existem  $n$  inteiros consecutivos nenhum dos quais é uma potência de primo.*

**Problema 13** (IMO 1994). *Determine todos os pares de inteiros positivos  $m$  e  $n$  para os quais  $\frac{n^3+1}{mn+1}$  é inteiro.*

**Problema 14** (Problema 5, IMO-2006). *Seja  $P(x)$  um polinômio de grau  $n > 1$  com coeficientes inteiros e seja  $k$  um inteiro positivo. Considere o polinômio*

$$Q(x) = P(P(\cdots(P(P(x))\cdots))),$$

*em que  $P$  é aplicada  $k$  vezes. Prove que existem no máximo  $n$  inteiros  $t$  tais que  $Q(t) = t$ .*

**Problema 15** (Problema 6 da IMO-1988). *Prove que se  $a$  e  $b$  são inteiros positivos e  $\frac{a^2+b^2}{ab+1}$  é um inteiro, então  $\frac{a^2+b^2}{ab+1}$  é um quadrado perfeito.*

*Idéia: Sejam  $a_1 > b$  tais que  $a^2 - kab + (b^2 - k) = 0$  com a menor soma  $a_1 + b$  possível. O outro par de soluções  $(a_0, b)$  deve ter  $0 < a_0 < a_1$ , obtendo um absurdo.*

**Problema 16** (IMO-2007). *Prove que se  $a$  e  $b$  são inteiros positivos tais que  $4ab-1 \mid (4a^2-1)^2$ , então  $a = b$ .*

*Idéia: O mesmo truque usado no problema anterior.*

4. ALGUNS PROBLEMAS DE TEORIA DOS NÚMEROS NA OBM-U

**Problema 17** (2005 - Problema 6, 1a fase). *Prove que existem pelo menos 2005 potências 27-ésimas distintas (isto é, números da forma  $n^{27}$ , com  $n$  inteiro positivo), todas com exatamente 2005 algarismos, tais que qualquer uma pode ser obtida de qualquer outra a partir de uma permutação de seus algarismos.*

**Problema 18** (201? - Problema 6, 2a fase). *Prove que se  $10^{2n} + 8 \cdot 10^n + 1$  tem um fator primo da forma  $60k + 7$  então  $n$  e  $k$  são pares.*

**Problema 19** (Problema 4 - 2007, 1a fase). *Seja  $a$  um inteiro não-nulo. Prove que se  $a$  é uma  $n$ -ésima potência módulo  $4a^2$  (ou seja, existe algum  $b$  inteiro tal que  $a - b^n$  é um múltiplo de  $4a^2$ ), então  $a$  é uma  $n$ -ésima potência.*

**Problema 20** (Problema 4 - 2009, 1a fase). *Determine a quantidade de números inteiros positivos  $n$  menores ou iguais a  $31!$  tais que  $3^n + n$  é divisível por  $31$ .*

**Problema 21** (Problema 4 - 2012, 1a fase). *Sejam  $(x_n)$  e  $(y_n)$  duas sequências dadas por  $x_1 = 2$ ,  $y_1 = 2012$ ,  $x_{n+1} = 2^{x_n}$  e  $y_{n+1} = (y_n)!$  para todo  $n \geq 1$ . Determine o menor inteiro positivo  $k$  tal que  $x_k > y_{2012}$ .*

**Problema 22** (Problema 1 - 2013, 1a fase). *Seja  $P(x)$  um polinômio com coeficientes inteiros satisfazendo  $P(n) = n$  para todo inteiro  $n$  com  $1 \leq n \leq 6$  e  $P(0) = 2013$ . Determine quantos e quais são os possíveis valores de  $P(0)$ .*

**Problema 23** (OBM-U 2001 - Problema 2 - 1a fase). *Seja  $s(n)$  a soma dos algarismos de  $n$ . Assim, por exemplo,  $s(77) = 14$  e  $s(2001) = 3$ . Diga se existe um inteiro positivo  $n$  com  $s(n) = 10$  e  $s(n^2) = 100$ . Se não existir, demonstre este fato. Se existir, dê um exemplo.*

**Problema 24** (2016 - Problema 3, 2a fase). *Seja  $k \geq 1$  um inteiro. Definimos a sequência  $(a_n)_{n \geq 0}$  por  $a_0 = 0$ ,  $a_1 = 1$  e*

$$a_{n+1} = ka_n + a_{n-1}$$

*para  $n = 1, 2, \dots$ . Seja  $p$  um número primo ímpar. Denote por  $m(p)$  o menor inteiro positivo  $i$  tal que  $p|a_i$ . Denote por  $T(p)$  o menor inteiro positivo tal que para qualquer natural  $j$  temos  $p|a_{j+T(p)} - a_j$ .*

*i) Mostre que  $T(p) \leq m(p)(p - 1)$ .*

*ii) Se  $T(p) = m(p)(p - 1)$ , mostre que*

$$\prod_{1 \leq j \leq T(p) - 1, j \not\equiv 0 \pmod{m(p)}} a_j \equiv (-1)^{m(p)-1} \pmod{p}.$$