

Polos Olímpicos de Treinamento Intensivo (POTI)  
Curso de Teoria dos Números - Nível 2

Aula 6 - Congruências II

Prof. Samuel Feitosa

*Arquivo Original<sup>1</sup>*

---

<sup>1</sup>**Documento:** "...gaia/educacional/matematica/pot2tn06/Aula06-CongruenciasII.pdf".

# Sumário

<b>1</b>	<b>Congruências II</b>	<b>1</b>
1.1	Problemas Propostos . . . . .	5
1.2	Dicas e Soluções . . . . .	6

## 1 Congruências II

Na aula de hoje, aprenderemos um dos teoremas mais importantes do curso: o “pequeno” teorema de Fermat. Começaremos relembrando um resultado da aula passada:

**Lema 1.** Se  $ka \equiv kb \pmod{m}$  e  $\text{mdc}(m, k) = 1$ , então  $a \equiv b \pmod{m}$ .

*Demonstração.* Como  $m|k(a - b)$  e  $\text{mdc}(m, k) = 1$ , segue que  $m|a - b$ .

**Teorema 2.** (Teorema de Fermat) Seja  $p$  um primo. Se  $p$  não divide  $a$  então

$$a^{p-1} \equiv 1 \pmod{p}.$$

Além disso, para todo inteiro  $a$ ,  $a^p \equiv a \pmod{p}$

*Demonstração.* Considere o conjunto de inteiros  $B = \{a, 2a, 3a, \dots, (p-1)a\}$  onde  $a$  é um inteiro satisfazendo  $\text{mdc}(a, p) = 1$ . Nenhum deles é divisível por  $p$  e quaisquer dois deles são incongruentes módulo  $p$ , em virtude do lema anterior. Assim, o conjunto dos restos dos elementos de  $B$  coincide com o conjunto dos restos não nulos na divisão por  $p$ , a saber,  $\{1, 2, 3, \dots, p-1\}$ . Portanto,

$$\begin{aligned} a \cdot 2a \cdot 3a \dots (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdot \dots (p-1) \pmod{p}, \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p}. \end{aligned}$$

Podemos cancelar o termo  $(p-1)!$  em ambos os lados pois  $\text{mdc}((p-1)!, p) = 1$ , concluindo assim a demonstração do teorema.

**Exemplo 3.** Prove que  $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$  é um inteiro para todo inteiro  $n$ .

Primeiramente note que  $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} = \frac{3n^5 + 5n^3 + 7n}{15}$ . Como  $\text{mdc}(3, 5) = 1$ , basta mostrarmos que o numerador é múltiplo de 3 e 5. Pelo teorema de Fermat:

$$\begin{aligned} 3n^5 + 5n^3 + 7n &\equiv 5n^3 + 7n \equiv 5n + 7n = 12n \equiv 0 \pmod{3}, \\ 3n^5 + 5n^3 + 7n &\equiv 3n^5 + 7n \equiv 3n + 7n = 10n \equiv 0 \pmod{5}. \end{aligned}$$

**Problema 4.** Mostre que  $n^7 \equiv n \pmod{42}$ ,  $\forall n \in \mathbb{N}$

Pelo teorema de Fermat,

$$\begin{aligned} n^7 &\equiv n \pmod{7} \\ n^7 &\equiv (n^3)^2 \cdot n \equiv n^2 \cdot n = n^3 \equiv n \pmod{3} \\ n^7 &\equiv (n^2)^3 \cdot n \equiv n^3 \cdot n = (n^2)^2 \equiv n^2 \equiv n \pmod{2} \end{aligned}$$

Como 2, 3 e 7 são primos entre si,  $n^7 \equiv n \pmod{2 \cdot 3 \cdot 7 = 42}$ .

**Exemplo 5.** (Bulgária 95) Encontre o número de inteiros  $n > 1$  para os quais o número  $a^{25} - a$  é divisível por  $n$  para cada inteiro  $a$ .

Se  $n$  satisfaz o enunciado,  $p^2$  ( $p$  primo) não pode dividi-lo, pois  $p^{25} - p$  não é divisível por  $p^2$ . Assim,  $n$  é múltiplo de primos diferentes. Os fatores primos de  $n$  são fatores de  $2^{25} - 2 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$ . Entretanto,  $n$  não é divisível por 17 e 241 pois  $3^{25} \equiv -3 \pmod{17}$  e  $3^{25} \equiv 32 \pmod{241}$ . Seguindo o exemplo anterior, podemos usar o teorema de Fermat para mostrar que  $a^{25} \equiv a \pmod{p}$  para  $p \in \{2, 3, 5, 7, 13\}$ . Portanto,  $n$  deve ser igual a um dos divisores de  $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$  diferente de 1. A quantidade de tais divisores é  $2^5 - 1 = 31$ .

**Exemplo 6.** Prove que para cada primo  $p$ , a diferença

$$111 \dots 11222 \dots 22333 \dots 33 \dots 888 \dots 88999 \dots 99 - 123456789$$

(onde cada dígito está escrito exatamente  $p$  vezes) é múltiplo de  $p$ .

Uma boa maneira de associar os números do problema com o teorema de Fermat é perceber que:

$$\underbrace{111 \dots 11}_{p \text{ uns}} = \frac{10^p - 1}{9}.$$

Assim, podemos escrever o número  $S = 111 \dots 11222 \dots 22333 \dots 33 \dots 888 \dots 88999 \dots 99$  como:

$$\begin{aligned} S &= \frac{10^p - 1}{9} \cdot 10^{8p} + 2 \cdot \frac{10^p - 1}{9} \cdot 10^{7p} + \dots + 9 \cdot \frac{10^p - 1}{9} \\ 9S &= (10^p - 1) \cdot 10^{8p} + 2 \cdot (10^p - 1) \cdot 10^{7p} + \dots + 9 \cdot (10^p - 1) \end{aligned}$$

Para  $p = 2$  ou  $p = 3$ , o resultado do enunciado segue dos critérios de divisibilidade por 2 e 3. Podemos então nos concentrar no caso  $p > 3$ . Nesse caso, é suficiente mostrarmos que  $9(S - 123456789)$  é divisível por  $p$  pois  $\text{mdc}(p, 9) = 1$ . Pelo teorema de Fermat:

$$\begin{aligned} 9S &= (10^p - 1) \cdot 10^{8p} + 2 \cdot (10^p - 1) \cdot 10^{7p} + \dots + 9 \cdot (10^p - 1) \\ &\equiv (10 - 1) \cdot 10^8 + 2 \cdot (10 - 1) \cdot 10^7 + \dots + 9 \cdot (10 - 1) \pmod{p} \\ &\equiv 9 \cdot 123456789 \pmod{p}. \end{aligned}$$

**Exemplo 7.** Dado um primo  $p$ , prove que existem infinitos naturais  $n$  tais que  $p$  divide  $2^n - n$ .

Se  $p = 2$ ,  $n$  pode ser qualquer número par. Suponha que  $p > 2$ . Considere  $(p-1)^{2k}$ , pelo teorema de Fermat temos:

$$2^{(p-1)^{2k}} \equiv (2^{p-1})^{(p-1)^{2k-1}} \equiv 1^{(p-1)^{2k-1}} = 1 \equiv (p-1)^{2k} \pmod{p}.$$

Assim, para qualquer  $k$ ,  $n = (p-1)^{2k}$  satisfaz o problema.

**Lema 8.** Se  $\text{mdc}(a, m) = 1$  então existe um inteiro  $x$  tal que

$$ax \equiv 1 \pmod{m}.$$

Tal  $x$  é único módulo  $m$ . Se  $\text{mdc}(a, m) > 1$  então não existe tal  $x$ .

*Demonstração.* Pelo teorema de Bachet-Bézout, existem inteiros  $x$  e  $y$  tais que  $ax + my = 1$ . Analisando essa congruência módulo  $m$ , obtemos  $ax \equiv 1 \pmod{m}$ . Se  $y$  é outro inteiro que satisfaz a congruência, temos  $ax \equiv ay \pmod{m}$ . Pelo primeiro lema,  $x \equiv y \pmod{m}$ . Se  $d = \text{mdc}(a, m) > 1$ , não podemos ter  $d|m$  e  $m|ax - 1$  pois  $d \nmid ax - 1$ .

**Teorema 9.** (Teorema de Wilson) Se  $p$  é primo, então

$$(p-1)! \equiv -1 \pmod{p}$$

*Demonstração.* Em virtude do lema anterior, para cada  $a \in \{2, 3, \dots, p-2\}$ , existe um resto  $x \in \{0, 1, 2, \dots, p-1\}$  tal que  $ax \equiv 1 \pmod{p}$ . Se  $x = 1$  ou  $x = p-1$ , teríamos  $a = 1$  ou  $p-1$ . Além disso, não podemos ter  $a = x$  pois os únicos restos que satisfazem  $a^2 \equiv 1 \pmod{p}$  são 1 e  $p-1$  (Veja o problema 20). Com isso, podemos agrupar os números de  $\{2, 3, \dots, p-2\}$  em pares onde o produto deixa resto 1 por  $p$ , o que nos permite concluir que o produto de todos eles também deixa resto 1 por  $p$ . Logo,

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

**Exemplo 10.** (Estônia 2000) Prove que não é possível dividir qualquer conjunto de 18 inteiros consecutivos em dois conjuntos disjuntos  $A$  e  $B$  tais que o produto dos elementos de  $A$  seja igual ao produto dos elementos de  $B$ .

Suponha, por absurdo, que existam tais conjuntos. Considere o primo  $p = 19$ . Como o produto dos elementos de  $A$  é igual ao produto dos elementos de  $B$ , se um dos conjuntos contém um múltiplo de 19, o outro necessariamente também conterá. Como entre 18 inteiros consecutivos não existem dois múltiplos de 19, nenhum dos conjuntos do problema contém tais números. Seja  $x$  o resto na divisão por 19 do produto dos elementos de  $A$ . Calculemos então o resto na divisão por 19 do produto de todos os 18 inteiros consecutivos:

$$\begin{aligned} x \cdot x &\equiv n(n+1)(n+2)(n+3)\dots(n+17) \\ &\equiv 1 \cdot 2 \cdot 3 \dots 18 \\ &\equiv -1 \pmod{19} \text{ (Pelo teorema de Wilson)}. \end{aligned}$$

Como  $x^2 \equiv -1 \pmod{19}$ ,  $x^{18} \equiv (-1)^9 \equiv 1 \pmod{19}$ . Isso contraria o teorema de Fermat e obtemos um absurdo.

**Definição 11.** Um conjunto  $S$  é chamado de sistema completo de resíduos módulo  $n$ , denotado abreviadamente por **scr**, se para cada  $0 \leq i \leq n-1$ , existe um elemento de  $s \in S$  tal que  $i \equiv s \pmod{n}$ . Para qualquer  $a$ , o conjunto  $\{a, a+1, a+2, \dots, a+(n-1)\}$  é um exemplo de **scr**.

**Exemplo 12.** Se  $\text{mdc}(m, s) = 1$ , mostre que  $\{t, t+s, t+2s, \dots, t+(m-1)s\}$  é um **scr**.

Pelo primeiro lema, se  $t+is \equiv t+js \pmod{m}$ , temos  $is \equiv js \pmod{m}$  e  $i \equiv j \pmod{m}$ . Como  $i, j \in \{0, 1, \dots, m-1\}$ ,  $i = j$ . Isso nos diz que temos  $m$  inteiros que deixam restos distintos na divisão por  $m$ . Como existem exatamente  $m$  restos na divisão por  $m$ , o conjunto é um **scr**.

**Exemplo 13.** Seja  $m$  um inteiro positivo par. Suponha que  $\{a_1, a_2, \dots, a_m\}$  e  $\{b_1, b_2, \dots, b_m\}$  são dois sistemas completos de resíduos módulo  $m$ . Prove que

$$S = \{a_1 + b_1, a_2 + b_2, \dots, a_m + b_m\}$$

não é um sistema completo de resíduos.

Suponha que  $S$  seja um **scr**, então:

$$\begin{aligned} 1 + 2 + \dots + m &\equiv (a_1 + b_1) + (a_2 + b_2) + \dots + (a_m + b_m) \pmod{m} \\ &\equiv (a_1 + a_2 + \dots + a_m) + (b_1 + b_2 + \dots + b_m) \\ &\equiv 2(1 + 2 + \dots + m) \\ &\equiv 2(1 + 2 + \dots + m) \end{aligned}$$

Isso implica que  $m \mid \frac{m(m+1)}{2}$ , ou seja,  $\frac{m+1}{2}$  é inteiro. Um absurdo pois  $m$  é par.

**Exemplo 14.** (Polônia 1997) Prove que a sequência  $a_n$  definida por  $a_1 = 1$  e

$$a_n = a_{n-1} + a_{\lfloor \frac{n}{2} \rfloor}$$

contém infinitos termos divisíveis por 7.

Uma maneira natural para mostrarmos que existem infinitos inteiros múltiplos de 7 na sequência é verificar que o aparecimento de um múltiplo de 7 acarreta o aparecimento de outro múltiplo na sequência com um índice maior. Suponha que  $a_k$  é múltiplo de 7. Seja  $a_{2k-1} = s$ . Então:

$$\begin{aligned} a_{2k-1} &= s \\ a_{2k} &= s + a_k \equiv s \pmod{7} \\ a_{2k+1} &= a_{2k} + a_k \equiv s \pmod{7} \end{aligned}$$

Ou seja, o aparecimento de um inteiro múltiplo de 7 implica no aparecimento de 3 inteiros com o mesmo resto por 7. Exploreemos essa ideia mais uma vez.

$$\begin{aligned} a_{4k-3} &= t \\ a_{4k-2} &\equiv t + a_{2k-1} \equiv t + s \pmod{7} \\ a_{4k-1} &\equiv t + s + a_{2k-1} \equiv t + 2s \pmod{7} \\ a_{4k} &\equiv t + 2s + a_{2k} \equiv t + 3s \pmod{7} \\ a_{4k+1} &\equiv t + 3s + a_{2k} \equiv t + 4s \pmod{7} \\ a_{4k+2} &\equiv t + 4s + a_{2k+1} \equiv t + 5s \pmod{7} \\ a_{4k+3} &\equiv t + 5s + a_{2k+2} \equiv t + 6s \pmod{7} \end{aligned}$$

Se  $s$  é múltiplo de 7, já teremos conseguido outro múltiplo de 7 na sequência. Em caso contrário, o conjunto  $\{t, t+s, t+2s, \dots, t+6s\}$  é um scr e conterá um múltiplo de 7.

**Exemplo 15.** Sejam  $x, y$  inteiros. Prove que  $3x^2 + 4y^2$  e  $4x^2 + 3y^2$  não podem ser ambos quadrados perfeitos.

Começemos com um lema bastante útil:

**Lema 16.** Seja  $p$  um número primo da forma  $4k+3$ . Então

$$p \mid m^2 + n^2 \iff p \mid m \text{ e } p \mid n.$$

Façamos inicialmente a primeira implicação. Se  $p \nmid m$ , então  $m^{p-1} \equiv 1 \pmod{p}$ , e daí temos as equivalências módulo  $p$

$$\begin{aligned} n^2 &\equiv -m^2 \\ \Rightarrow (nm^{p-2})^2 &\equiv -(m^{p-1})^2 \\ &\equiv -1 \\ \Rightarrow (nm^{p-2})^{p-1} &\equiv (-1)^{\frac{p-1}{2}} \\ &\equiv (-1)^{2k+1} \\ &\equiv -1, \end{aligned}$$

o que contraria o teorema de Fermat. Assim,  $p \mid m$  e  $p \mid n$ .

A recíproca é óbvia. Voltando ao problema, suponha que existam  $w, z$  inteiros positivos tais que

$$\begin{aligned} 3x^2 + 4y^2 &= w^2 & e \\ 4x^2 + 3y^2 &= z^2. \end{aligned}$$

Então  $7x^2 + 7y^2 = w^2 + z^2$  (\*). Afirmamos que a equação (\*) não possui solução. Para isso, seja  $S$  o conjunto formado pelas soluções inteiras  $(x, y, w, z)$  de (\*), e tome  $(a, b, c, d) \in S$  com  $c^2 + d^2$  mínimo. Pelo lema, temos que  $7|c$  e  $7|d$ , e daí  $c = 7c'$  e  $d = 7d'$ . Mas então  $a^2 + b^2 = 7c'^2 + 7d'^2 \Rightarrow (c', d', a, b) \in S$ , com

$$a^2 + b^2 < 7(a^2 + b^2) = c^2 + d^2,$$

o que contraria a minimalidade de  $(a, b, c, d)$ .

## 1.1 Problemas Propostos

**Problema 17.** Prove que se  $p$  é primo então

$$a^p \equiv b^p \pmod{p} \Rightarrow a^p \equiv b^p \pmod{p^2}$$

**Problema 18.** Encontre os restos das divisões de:

a)  $300^{3000} - 1$  por 1001

b)  $7^{120} - 1$  por 143

**Problema 19.** Encontre o resto de  $\underbrace{111 \dots 11}_{p-1 \text{ uns}}$  por  $p$ , onde  $p$  é um primo maior que 5.

**Problema 20.** Prove que se  $n$  é ímpar, então  $n^5 \equiv n \pmod{240}$ .

**Problema 21.** Sejam  $p$  e  $q$  primos distintos. Mostre que

i)  $(a + b)^p \equiv a^p + b^p \pmod{p}$

ii)  $p^q + q^p \equiv p + q \pmod{pq}$

iii)  $\lfloor \frac{p^q + p^q}{pq} \rfloor$  é par se  $p, q \neq 2$ .

**Problema 22.** Mostre que se  $p$  é primo e  $a^2 \equiv b^2 \pmod{p}$ , então  $a \equiv \pm b \pmod{p}$ .

**Problema 23.** Encontre os últimos três dígitos de  $7^{9999}$

**Problema 24.** Prove que  $20^{15} - 1$  é divisível por  $11 \cdot 31 \cdot 61$

**Problema 25.** Sejam  $\{a_1, a_2, \dots, a_{101}\}$  e  $\{b_1, b_2, \dots, b_{101}\}$  sistemas completos de resíduos módulo 101. Pode  $\{a_1 b_1, a_2 b_2, \dots, a_{101} b_{101}\}$  ser um sistema completo de resíduos módulo 101?

**Problema 26.** (Balcânica 2003) Existe um conjunto  $B$  de 4004 inteiros positivos tal que, para cada subconjunto  $A$  de  $B$  com 2003 elementos, a soma dos elementos em  $A$  não é divisível por 2003?

**Problema 27.** Para um inteiro ímpar  $n > 1$ , seja  $S$  o conjunto de inteiros  $x$ ,  $1 \leq x \leq n$ , tal que ambos  $x$  e  $x + 1$  são relativamente primos com  $n$ . Mostre que o produto de todos os elementos de  $S$  deixa resto 1 na divisão por  $n$ .

**Problema 28.** Sejam  $n$  um inteiro positivo maior que 1 e  $p$  um primo positivo tal que  $n$  divide  $p - 1$  e  $p$  divide  $n^3 - 1$ . Mostre que  $4p - 3$  é um quadrado perfeito.

## 1.2 Dicas e Soluções

17. Pelo teorema de Fermat,  $a \equiv a^p \equiv b^p \equiv b \pmod{p}$ . Assim,

$$\begin{aligned} a^{p-1} + a^{p-2}b + \dots + ab^{p-2} + b^{p-1} &\equiv a^{p-1} + a^{p-1} + \dots + a^{p-1} \\ &\equiv pa^{p-1} \\ &\equiv 0 \pmod{p} \end{aligned}$$

Como  $a - b \equiv 0 \pmod{p}$ , temos:

$$a^p - b^p = (a - b)(a^{p-1} + a^{p-2}b + \dots + ab^{p-2} + b^{p-1}) \equiv 0 \pmod{p^2}$$

19. Veja que:

$$\begin{aligned} \underbrace{111 \dots 11}_{p-1 \text{ uns}} &= \frac{999 \dots 99}{9} \\ &= \frac{10^{p-1} - 1}{9} \end{aligned}$$

Pelo teorema de Fermat, o numerador  $10^{p-1} - 1$  é divisível por  $p$  visto que  $p \neq 5$ . Além disso, usando que  $p \neq 2$  e  $3$ , segue que  $\frac{10^{p-1} - 1}{9}$  também é múltiplo de  $p$ .

20. Proceda como no exemplo 20.

21. i) Pelo teorema de Fermat:

$$\begin{aligned} (a + b)^p &\equiv a + b \\ &\equiv a^p + b^p \pmod{p}. \end{aligned}$$

ii) Pelo teorema de Fermat,

$$\begin{aligned} p^q + q^p &\equiv 0 + q \equiv p + q \pmod{p} \\ p^q + q^p &\equiv p + 0 \equiv p + q \pmod{q} \end{aligned}$$

22. Veja que  $(a - b)(a + b) \equiv 0 \pmod{p}$  e assim  $a - b \equiv 0 \pmod{p}$  ou  $a + b \equiv 0 \pmod{p}$ .

25. Suponha, por absurdo, que seja possível. Sejam  $a_i$  e  $b_j$  tais que  $a_i \equiv b_j \equiv 0 \pmod{101}$ . Se  $i \neq j$ , o conjunto  $\{a_1b_1, a_2b_2, \dots, a_{101}b_{101}\}$  teria dois inteiros com resto 0 na divisão por  $p$  e não poderia ser um **scr**. Suponha, sem perda de generalidade, que  $i = j = 101$ , então:

$$\begin{aligned} 100! &\equiv (a_1b_1)(a_2b_2) \dots (a_{100}b_{100}) \\ &\equiv (a_1a_2 \dots a_{100})(b_1b_2 \dots b_{100}) \\ &\equiv (100!)(100!) \\ &\equiv (100!)^2 \pmod{101} \end{aligned}$$

Assim,  $100! \equiv 1 \pmod{101}$ . Isso contradiz o teorema de Wilson.

26. Sim. Um exemplo de tal conjunto é a união de um conjunto de 2002 inteiros positivos que deixem resto 0 com outro conjunto composto por 2002 inteiros que deixem resto 1 por 2003.