Congruências e Restos

Alessandro Machado

1 Introdução

1.1 Contextualização

Em *Teoria dos Números*, uma das principais ferramentas utilizadas para resolução de problemas é a divisibilidade e os restos de números por outros. Essa ideia é muito recorrente porque nem sempre a divisão de dois inteiros resulta em outro, ao contrário dos números reais. Então, essas ferramentas que veremos irão ajudar a determinar certas propriedades sobre tais números.

1.2 Esclarecimentos

Normalmente, ao trabalhar com divisibilidade, os inteiros negativos são análogos aos positivos, por isso que muitas vezes utilizamos a notação de "$|n|$" para indicar o módulo de n, permitindo trabalharmos com inteiros negativos e positivos de forma anágola, pois $|x| \geq 0 \ \forall \ x$. Isto é:

$$|x| = \begin{cases} x, & \text{se } x \geq 0 \\ -x, & \text{se } x < 0 \end{cases}$$

2 Definições

2.1 Algoritmo da Divisão

2.1.1 Inspiração

O <u>*Algoritmo da Divisão*</u> é apenas uma forma de reescrever um número inteiro em função de outro como uma "correção" da divisão. Também chamada de *"divisão euclidiana"*, em muitos casos é uma forma extremamente útil de reescrever números ganhando informações sobre eles.

2.1.2 Definição

Dado $a \in \mathbb{Z}$ e $b \in \mathbb{N}$, existem únicos $q, r \in \mathbb{Z}$ e $0 \leq r < b$ tal que:

$$a = qb + r$$

Note que é possível definirmos a *divisão euclidiana* para valores negativos de b, basta trocar a condição "$0 \leq r < b$" por "$0 \leq r < |b|$" e tal caso é análogo.

2.1.3 Demonstração

Primeiro provaremos que q e r de fato existem. Para isso demonstraremos o teorema a seguir:

- **Teorema de Eudoxius:** Dado $a \in \mathbb{Z}$ e $b \in \mathbb{N}$, existe q tal que $qb \leq a < (q+1)b$.

  Prova: Para isso, basta considerar a sequência:

$$\text{“}\ldots,\ -3b,\ -2b,\ -b,\ 0,\ b,\ 2b,\ 3b,\ \ldots\text{”}$$

  Note que todos os inteiros estão entre dois desses termos consecultivos ou é um deles, pois é possível particionar o conjunto dos inteiros em infinitos subconjuntos da forma $\{qb,\ qb+1,\ \ldots,\ (q+1)b-2,\ (q+1)b-1\}$ $\square$

Com isso, sabemos que $\forall\ a \in \mathbb{Z}$ existe $q \in \mathbb{Z}$ tal que $qb \leq a < (q+1)b \implies 0 = qb - qb \leq a - qb = r$ e $r = a - qb < (q+1)b - qb = b \implies 0 \leq r < b$, logo tais q e r existem.

Agora, suponha que tais q e r não sejam únicos. Ou seja, existem ao mínimo dois pares distintos $(q,\ r)$ para $a = qb + r$ com $0 \leq r < b$, sejam eles $(q_1,\ r_1)$ e $(q_2,\ r_2)$. Logo $a = q_1 b + r_1 = q_2 b + r_2$, perceba que a é irrelevante, pois não temos nenhuma informação sobre, então focaremos apenas em $q_1 b + r_1 = q_2 b + r_2 \implies q_1 b - q_2 b = r_2 - r_1 \implies b(q_1 - q_2) = r_2 - r_1$, mas $q_1 \neq q_2 \implies |q_1 - q_2| \geq 1 \implies |r_2 - r_1| = |b(q_2 - q_1)| \geq |b| = b$, mas $0 \leq r_1, r_2 < b$, portanto $|b - 0| = b > |r_2 - r_1| \geq b$, absurdo! Logo tal solução existe e é única ■

2.1.4 Exemplos

.....

Exemplo 1. Mostre que o quadrado de um número inteiro sempre deixa resto 0 ou 1 por 3.

Solução. Por *Algoritmo da Divisão*, escreva o número como $3a + b$, onde $0 \leq b < 3 \implies b \in \{0,\ 1,\ 2\}$. Logo o quadrado desse número será $(3a+b)^2 = 9a^2 + 6ab + b^2 = 3(3a^2 + 2ab) + b^2$. Agora basta testar os valores de b:

Caso 1. $(b = 0)$: Substituindo $(3a+b)^2 = 3(3a^2 + 2a \cdot 0) + 0$ que, por definição deixa resto 0 por 3.

Caso 2. ($b = 1$): Substituindo $(3a+b)^2 = 3(3a^2+2a\cdot 1)+1)$ que, por definição deixa resto 1 por 3.

Caso 3. ($b = 2$): Por fim $(3a+b)^2 = 3(3a^2+2a\cdot 2)+4 = 3(3a^2+4a+1)+1$ que também deixa resto 1 por 3.

Ou seja, o quadrado de um número inteiro sempre deixa resto 0 ou 1 por 3.

.....

Exemplo 2. Seja S um conjunto infinito de inteiros não-negativos tal que, se $x, y \in S$ então $|x-y| \in S$. Seja d o menor elemento positivo de S. Prove que $S = \{kd \mid k \geq 0\}$.

Solução. Suponha que exista $x \in S$ tal que x não seja múltiplo de d, ou seja, por *Algoritmo da Divisão* podemos escrever $x = qd+r$, onde $q \in \mathbb{Z}_+$, pois $x \in \mathbb{Z}_+^*$ e $d > r \in \mathbb{Z}_+^*$ porque x não é múltiplo de d. Mas temos que $d, x \in S \implies |x-d| = |(qd+r)-d| = (q-1)d+r \in S$.

Agora, se $q \geq 2$, repita esse processo, pois $(q-1)d+r \geq d+r > d$, sabemos que $d, (q-1)d+r \in S \implies |((q-1)d+r)-d| = (q-2)d+r \in S$. Faça esse processo até que obtenha que $|(d+r)-d| = r \in S$ mas, partindo da suposição que x não é múltiplo de d, temos que $r > 0$, porém $r < d$, absurdo! Porque tomamos d para ser o menor inteiro positivo em S. Logo, a nossa suposição é falsa, portanto se $x \in S$, então x é da forma $kd, k \in \mathbb{Z}_+$.

Agora, basta provar que todo múltiplo de d está em S. Suponha que existe $k \in \mathbb{Z}_+^*$ tal que $kd \notin S$. Note que S possui infinitos elementos, ou seja, para todo natural $m \notin S$ existe $M \in S$ tal que $M > m$. Seja $M = Nd$ e $m = nd$, note que $d, M \in S \implies |M-d| = |Nd-d| = (N-1)d \in S \implies |(N-1)d-d| = (N-2)d \in S \implies \cdots \implies 2d \in S$, e como $M > m \implies N > n \implies n \in \{1,\ 2,\ \ldots,\ N\} \implies nd = m \in \{d,\ 2d,\ \ldots,\ Nd\} \subset S \implies m \in S$, absurdo! Logo todo múltiplo de d está em S e todo elemento de S é múltiplo de d, portanto $S = \{kd \mid k \geq 0\}$.

2.2 Divisibilidade

2.2.1 Inspiração

A <u>*divisibilidade*</u>, como dita anteriormente em "**1.1**", é um jeito de obter informações adicionais sobre os inteiros, uma vez que a divisão entre dois inteiros nem sempre é inteira.

2.2.2 Definição

Dados $a, b \in \mathbb{Z}$ com $a \neq 0$, denotamos por $a|b$ como "a divide b" $\iff \frac{b}{a} \in \mathbb{Z}$

2.2.3 Propriedades

1. $1|a$, $b|0$ e $b|b$ $\forall\ a, b \in \mathbb{Z}, b \neq 0$;
2. $a|b \iff \exists\ k \in \mathbb{Z}$ tal que $b = ak$;
3. Se $a|b$ e $b|c \implies a|c$;
4. Se $a|b \implies \frac{b}{a}|b$;
5. Se $a|b$ e $c|d \implies ac|bd$;
6. $a|b \iff ac|bc, c \in \mathbb{Z}^*$;
7. Se $a|b$ e $a|c \implies a|b \pm c$;
8. Se $a|b$ e $a|c \implies a|bx \pm cy\ \forall\ x, y \in \mathbb{Z}$;
9. Se $a|b$ e $b \neq 0 \implies |a| \leq |b|$;
10. Se $a|b$ e $b|a \implies |a| = |b|$;

2.2.4 Demonstrações

1. Note que $\frac{a}{1} = a \in \mathbb{Z}$, que $\frac{0}{b} = 0 \in \mathbb{Z}$ e que $\frac{b}{b} = 1 \in \mathbb{Z}$;
2. $a|b \iff \frac{b}{a} = k \in \mathbb{Z} \iff b = ak$;
3. De "2." temos que $a|b \implies b = ak \implies a = \frac{b}{k}$ e $b|c \implies c = bl \implies \frac{c}{a} = \frac{bl}{\frac{b}{k}} = lk \in \mathbb{Z} \implies a|c$;
4. $a|b \implies \frac{b}{a} \in \mathbb{Z}$, mas $\frac{b}{a}|b \iff \frac{b}{\frac{b}{a}} = a \in \mathbb{Z}$;
5. $a|b \implies \frac{b}{a} = k \in \mathbb{Z}$ e $c|d \implies \frac{d}{c} = l \in \mathbb{Z} \implies \frac{bd}{ac} = \frac{b}{a} \cdot \frac{d}{c} = kl \in \mathbb{Z} \implies ac|bd$;
6. $a|b \iff \frac{b}{a} = \frac{bc}{ac} \in \mathbb{Z}$;
7. $a|b \implies \frac{b}{a} = k \in \mathbb{Z}$ e $a|c \implies \frac{c}{a} = l \in \mathbb{Z}$, logo $a|b \pm c \iff \frac{b \pm c}{a} = \frac{b}{a} \pm \frac{c}{a} = k + l \in \mathbb{Z}$;
8. Como $a|b$ e $a|c$, de "5." sabemos que $a|bx$ e $a|cy$ (pois $x|x$ e $y|y$), mas de "7." sabemos que $a|bx \pm cy$;
9. De "2." sabemos que $b = ak, k \in \mathbb{Z}$ mas $b \neq 0 \implies k \neq 0 \implies |k| \geq 1 \implies |b| = |ak| = |a||k| \geq |a|$;
10. De "9." temos que como $a|b$, então $|a| \leq |b|$, mas como $b|a$ obtemos que $|b| \leq |a| \implies |a| = |b|$;

2.2.5 Exemplos

. . . . . .

Exemplo 1. Ache todos os inteiros positivos n tal que $2n+3|n^5+3n^2+7$.

Solução. Utilizaremos uma ideia muito comum em problemas de divisibilidade com polinômios. Queremos chegar que $2n+3|c$ onde "c" é uma constante, pois saberemos todas as soluções (os divisores de c).

Então iremos reduzir o grau de "n^5+3n^2+7" e iterar esse processo até chegarmos em grau 0 (constante). Para isso, usaremos as propriedades "5." e "8." de **2.2.3**. Temos que $2n+3|n^5+3n^2+7 \implies 2n+3|2(n^5+3n^2+7) = 2n^5+6n^2+14$ e $2n+3|2n+3 \implies 2n+3|n^4(2n+3) = 2n^5+3n^4 \implies 2n+3|(2n^5+6n^2+14)-(2n^5+3n^4) = -3n^4+6n^2+14$, agora temos que $2n+3$ divide um polinômio de grau 4.

Continuando esse processo, $2n+3|-3n^4+6n^2+14$ e $2n+3|2n+3 \implies 2n+3|2(-3n^4+6n^2+14)+3n^3(2n+3) = 9n^3+12n^2+28 \implies 2n+3|2(9n^3+12n^2+28)-9n^2(2n+3) = -3n^2+56 \implies 2n+3|2(-3n^2+56)+3n(2n+3) = 9n+112$ e, por fim $2n+3|9n+112 \implies 2n+3|2(9n+112) = 18n+224$ mas, $2n+3|2n+3 \implies 2n+3|9(2n+3) = 18n+27 \implies 2n+3|(18n+224)-(18n+27) = 197$. Porém 197 é primo, logo seus divisores positivos são 1 e 197. Logo $2n+3 = 1$ ou $2n+3 = 197$, sendo que se $2n+3 = 1 \implies n = -1$, mas n é inteiro positivo, absurdo! E se $2n+3 = 197 \implies n = 97$, portanto o único inteiro positivo n que satisfaz o enunciado é 97.

. . . . . .

Exemplo 2. *(AIME 1986)* Qual é o maior inteiro n tal que $n+10$ divide n^3+100.

Solução. Note que podemos fatorar soma de cubos "$a^3+b^3 = (a+b)(a^2-ab+b^2)$", e no enunciado temos n^3+100, isso é, um cubo mais uma constante. O que nos motiva a escrevermos $n^3+10^3 = (n+10)(n^2-10n+10^2)$ e como $n+10|n+10 \implies n+10|(n+10)(n^2-10n+10^2) = n^3+10^3$ mas, como $n+10|n^3+100 \implies n+10|(n^3+1000)-(n^3+100) = 900$, sendo que $|n+10| \leq 900$ então a solução máxima seria quando $n+10 = 900 \implies n = 890$.

. . . . . .

Exemplo 3. *(Olimpíada de Maio 2006)* Encontre todos os naturais a e b tais que $a|b+1$ e $b|a+1$.

Solução. Perceba que o enunciado é simétrico em a e b, então suponha que $a \leq b$ sem perda de generalidade. Temos que $b|a+1 \implies |b| \leq |a+1|$, mas como $a, b \in \mathbb{N} \implies a \leq b \leq a+1$. Logo temos 2 casos, $b = a$ ou $b = a+1$.

Caso 1. $a = b \implies a|a+1$, mas $a|a \implies a|a+1-a = 1 \implies a = b = 1$.

Caso 2. $b = a+1 \implies a|a+2$ e $b|b$, mas "$b|b$" é sempre verdade, logo precisamos analisar apenas $a|a+2$, sendo que $a|a \implies a|2 \implies a \in \{1,\ 2\}$. Portanto os pares $(a,\ b)$ satisfazendo o caso 2 são: $(1,\ 2)$ e $(2,\ 3)$. Mas assumimos que a era o menor, logo todos

os pares $(a,\ b)$ são: $(1,\ 1)$, $(1,\ 2)$, $(2,\ 3)$, $(2,\ 1)$ e $(3,\ 2)$.

. . . . . .

Exemplo 4. *(Olimpíada de Leningrado 1989)* Seja $a \in \mathbb{Z}_{>1}$ e b tal que $b|a^2+1$. Prove que se $b-a>0$, então $b-a>\sqrt{a}$.

Solução. Perceba que as únicas condições dadas sobre b é que $b|a^2+1$ e que $b-a>0$, então, para tentar usar melhor o fato de que $b-a>0$, tome $q=b-a \implies q \in \mathbb{N}$. Reescrevendo "$b|a^2+1$" como $a+q|a^2+1$, sendo que $(a-q)(a+q)=a^2-q^2 \implies a+q|(a^2+1)-(a^2-q^2)=q^2+1 \implies a+q \leq q^2+1 \implies a+1 \leq a+q \leq q^2+1 \implies a \leq q^2 \implies q \geq \sqrt{a}$, pois $q \geq 1$. Sendo que a igualdade só ocorre quando $q=1 \implies b=a+1 \implies a+1|a^2+1$, sendo que $(a-1)(a+1)=a^2-1 \implies a+1|(a^2+1)-(a^2-1)=2 \implies a+1 \leq 2 \implies a \leq 1$, absurdo! Portanto a igualdade não pode acontecer, logo $b-a>\sqrt{a}$.

. . . . . .

Exemplo 5. *(OBM 2021)* Uma tripla de inteiros $(a,\ b,\ c)$ é chamada de *miranha* se:

- a divide $bc+1$
- b divide $ca+1$
- c divide $ab+1$

Determine todas as triplas *miranhas*.

Solução. $a|bc+1$, $b|ca+1$ e $c|ab+1 \implies abc|(ab+1)(bc+1)(ca+1)=a^2b^2c^2+a^2bc+ab^2c+abc^2+ab+bc+ca+1$ mas, $abc|abc(abc+a+b+c)=a^2b^2c^2+a^2bc+ab^2c+abc^2 \implies abc|ab+bc+ca+1 \implies abc \leq ab+bc+ca+1 \implies 1 \leq \frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{abc}$. Porém, se $a,b,c \geq 4 \implies \frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{abc} \leq \frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{64}<1$. Logo, assumindo sem perda de generalidade que $a \geq b \geq c \implies c \leq 3$.

Caso 1. $(c=3)$ $3ab|ab+3b+3a+1 \leq 3ab+1$, mas $\frac{ab+3b+3a+1}{3ab} \leq \frac{3ab+1}{3ab}<2 \implies \frac{ab+3b+3a+1}{3ab}=1 \implies ab+3b+3a+1=3ab \implies 3a+1=2ab-3b=b(2a-3) \geq 3(2a-3) \implies 3a+1 \geq 6a-9 \implies 3a \leq 10 \implies a<4 \implies (a,\ b,\ c)=(3,\ 3,\ 3)$ absurdo, basta testar!

Caso 2. $(c=2)$ Como $c>1 \implies a,b>1 \implies a \neq b$, pois se $a=b \implies a|2a+1 \implies a|(2a+1)-2a=1 \implies a=1$, absurdo!. E como $a|2b+1 \implies a \leq 2b+1<2a$, pois $a \geq b+1$. Então $a=2b+1$, porém $b|2a+1=2(2b+1)+1=4b+3 \implies b|(4b+3)-4b=3 \implies b=3 \implies a=7$ e, de fato $(a,\ b,\ c)=(7,\ 3,\ 2)$ funciona.

Caso 3. $(c=1)$ Portanto $a|b+1$ e $b|a+1$, então, como vimos no "**Exemplo 3.**", as soluções são os pares $(a,\ b)$: $(1,\ 1)$, $(2,\ 1)$ e $(3,\ 2)$. O que gera as triplas $(a,\ b,\ c)$: $(1,\ 1,\ 1)$, $(2,\ 1,\ 1)$ e $(3,\ 2,\ 1)$.

Portanto as triplas *miranha* são: (7, 3, 2), (1, 1, 1), (2, 1, 1) e (3, 2, 1) e suas permutações.

2.3 Congruência

2.3.1 Inspiração

A *Congruência* é uma notação baseada em divisibilidade que permite-nos usarmos de forma mais clara e direta, é uma forma de "igualdade de restos". Tal notação se assemelha muito com a igualdade "=".

2.3.2 Definição

Dados $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$, dizemos que $a \equiv b \pmod{m} \iff m|a-b$. Perceba que podemos definir congruência para $m \in \mathbb{Z}_-^*$, mas isso é análogo, pois $m|a-b \iff -m|a-b$. Então, por convenção sempre assumimos que $m > 0$, pois $\frac{x}{0}$ é indefinido e $m|a-b \iff -m|a-b$.

2.3.3 Propriedades

1. $a \equiv a \pmod{m}$;
2. $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$;
3. $a \equiv b \pmod{m} \iff a = q_1 m + r, b = q_2 m + r, q_1, q_2 \in \mathbb{Z}, m > r \in \mathbb{Z}_+$;
4. Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$;
5. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \implies a + c \equiv b + d \pmod{m}$;
6. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$;
7. Se $a \equiv b \pmod{m}$ e $n|m \implies a \equiv b \pmod{n}$;
8. Se $a \equiv b \pmod{m} \implies a^n \equiv b^n \pmod{m}$;

2.3.4 Demonstrações

1. $m|0 = a - a \implies a \equiv a \pmod{m}$;
2. $m|a-b \iff m|b-a$;
3. Primeiro provaremos a ida. Escreva $a = q_1 m + r_1$ e $b = q_2 m + r_2$ com $m > r_1, r_2 \in \mathbb{Z}_+$ e $r_1 \neq r_2$, logo $a \equiv b \pmod{m} \iff m|a-b = (q_1 m + r_1) - (q_2 m + r_2) = (q_1 - q_2)m + (r_1 - r_2)$, sendo que $m|(q_1 - q_2)m \implies m|r_1 - r_2$, mas como

$r_1 \neq r_2 \implies r_1 - r_2 \neq 0 \implies m \leq |r_1 - r_2| < |m - 0| = m$, abusurdo! Logo $r_1 = r_2$ e a volta é clara, pois $a = q_1 m + r, b = q_2 m + r \implies a \equiv b \pmod{m} \iff m | a - b = (q_1 m + r) - (q_2 m + r) = (q_1 - q_2)m$, o que é verdade;

4. $a \equiv b \pmod{m} \implies m | a - b$ e $b \equiv c \pmod{m} \implies m | b - c$, subtraindo as divisibilidades obtemos que $m | (a + b) - (b + c) = a - c \implies a \equiv c \pmod{m}$;

5. $a \equiv b \pmod{m} \implies m | a - b$ e $c \equiv d \pmod{m} \implies m | c - d$, somando ambas divisibilidades obtemos que $m | (a - b) + (c - d) = (a + c) - (b + d) \implies a + c \equiv b + d \pmod{m}$;

6. $a \equiv b \pmod{m} \implies m | a - b \implies m | c(a - b)$ e $c \equiv d \pmod{m} \implies m | c - d \implies m | b(c - d)$, somando ambas divisibilidades obtemos que $m | c(a - b) + b(c - d) = ac - bd \implies ac \equiv bd \pmod{m}$;

7. $a \equiv b \pmod{m} \implies m | a - b$ e $n | m | a - b \implies n | a - b \implies a \equiv b \pmod{n}$;

8. $a \equiv b \pmod{m} \implies m | a - b \implies m | (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) = a^n - b^n \implies a^n \equiv b^n \pmod{m}$;

2.4 Exemplos

. . . . . .

Exemplo 1. *(OBM 1998, 1ª fase)* Qual é o dígito das unidades do número 3^{1998}?

Solução. Reescreva $3^{1998} = (3^2)^{\frac{1998}{2}} = 9^{999}$. Note que analisar o dígito das unidades é o mesmo que olhar módulo 10, pois $\overline{(d_n d_{n-1} \ldots d_1 d_0)}_{10} = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + 10 d_1 + d_0 = 10(d_n 10^{n-1} + d_{n-1} 10^{n-2} + \cdots + d_1) + d_0 \equiv d_0 \pmod{10}$, logo queremos saber quanto é $9^{999} \pmod{10}$, sendo que usando a propriedade "6." de **2.3.3**, $9 \equiv -1 \pmod{10} \implies 9^{999} \equiv (-1)^{999} = -1 \equiv 9 \pmod{10}$, logo o dígito das unidades do número 3^{1998} é 9.

. . . . . .

Exemplo 2. Ache todos os pares de inteiros positivos $(a,\ b)$ tal que $3^a + 7 = 2^b$.

Solução. Se $b = 1$ temos que $3^a + 7 = 2 \implies 3^a = -5$, absurdo! Portanto $b \geq 2 \implies 2^b \equiv 0 \pmod{4} \implies 3^a + 7 = 2^b \equiv 0 \pmod{4}$, mas $7 \equiv 3 \equiv -1 \pmod{4} \implies 3^a + 7 \equiv (-1)^a - 1 \equiv 0 \pmod{4} \implies (-1)^a \equiv 1 \pmod{4}$ logo a é par, pois $(-1)^{2k} = ((-1)^2)^k = 1^k = 1$ e $(-1)^{2k+1} = (-1)^{2k}(-1) = -1$. Analogamente, analisando módulo 3 temos que $2^b = 3^a + 7 \equiv 1 \pmod{3}$, sendo que $2 \equiv -1 \pmod{3} \implies 2^b \equiv$

$(-1)^b \equiv 1 \pmod 3$, então b também é par. Reescrevendo $a = 2a_0$ e $b = 2b_0$ pois ambos são pares, temos que $3^{2a_0} + 7 = 2^{2b_0} \implies (2^{b_0})^2 - (3^{a_0})^2 = 7$, sendo que por diferença de quadrados $(2^{b_0})^2 - (3^{a_0})^2 = (2^{b_0} + 3^{a_0})(2^{b_0} - 3^{a_0}) = 7$, mas 7 é primo, ou seja:

$$\begin{cases} 2^{b_0} + 3^{a_0} = 7 \\ 2^{b_0} - 3^{a_0} = 1 \end{cases}$$

Pois $2^{b_0} + 3^{a_0} > 2^{b_0} - 3^{a_0}$ e $(2^{b_0} + 3^{a_0}) \in \mathbb{N}$. Somando ambas equações descobrimos que $2^{b_0} + 2^{b_0} = 7 + 1 \implies 2^{b_0+1} = 8 = 2^3 \implies b_0 + 1 = 3 \implies b_0 = 2$. Substituindo b_0 em uma das equações, chegamos que $2^2 + 3^{a_0} = 7 \implies 3^{a_0} = 3 \implies a_0 = 1$, mas $a = 2a_0 = 2$ e $b = 2b_0 = 4$, portanto a única solução é $(a,\ b) = (2,\ 4)$.

. . . . . .

Exemplo 3. Prove que para todo natural n a expressão $n^5 - n$ é múltipla de 5.

Solução. Para isso, iremos analisar módulo 5, pois assim poderemos apenas testar os restos por 5 no lugar de n, que são 5 possibilidades:

Caso 1. ($n \equiv 0 \pmod 5$): $n^5 - n \equiv 0^5 - 0 = 0 \pmod 5 \implies 5|n^5 - n$.

Caso 2. ($n \equiv 1 \pmod 5$): $n^5 - n \equiv 1^5 - 1 = 0 \pmod 5 \implies 5|n^5 - n$.

Caso 3. ($n \equiv 2 \pmod 5$): $n^5 - n \equiv 2^5 - 2 = 30 \equiv 0 \pmod 5 \implies 5|n^5 - n$.

Caso 4. ($n \equiv 3 \pmod 5$): $n^5 - n \equiv 3^5 - 3 = 240 \equiv 0 \pmod 5 \implies 5|n^5 - n$.

Caso 5. ($n \equiv 4 \pmod 5$): $n^5 - n \equiv 4^5 - 4 = 1020 \equiv 0 \pmod 5 \implies 5|n^5 - n$.

Logo, independentemente do resto de n por 5, $5|n^5 - n$, portanto $5|n^5 - n$ para todo n natural.

. . . . . .

Exemplo 4. Prove que $13^{29} + 29^{13}$ é divisível por 21.

Solução. Para isso perceba que $21 = 3 \cdot 7$ e como 3 e 7 são primos distintos, basta provar que $13^{29} + 29^{13}$ é múltiplo de 3 e de 7. Sendo que $13^{29} + 29^{13} \equiv 1^{29} + (-1)^{13} \equiv 1 - 1 \equiv 0 \pmod 3$ e $13^{29} + 29^{13} \equiv (-1)^{29} + 1^{13} \equiv -1 + 1 \equiv 0 \pmod 7$. Logo $13^{29} + 29^{13}$ é múltiplo de 3 e 7, portanto também é múltiplo de 21.

. . . . . .

Exemplo 5. *(OBM 2007, 3ª fase)* Prove que não existem soluções inteiras e positivas para a equação $3^m + 3^n + 1 = t^2$.

Solução. Note que $3^2 = 9 \equiv 1 \pmod 8$, logo $3^{2k} \equiv 1 \pmod 8 \implies 3^{2k+1} \equiv 3 \pmod 8$, ou seja, 3^n só pode ser 1 ou 3 módulo 8. Perceba também que:

$$\begin{cases} t \equiv 0 \pmod 8 \implies t^2 \equiv 0 \pmod 8 \\ t \equiv 1 \pmod 8 \implies t^2 \equiv 1 \pmod 8 \\ t \equiv 2 \pmod 8 \implies t^2 \equiv 4 \pmod 8 \\ t \equiv 3 \pmod 8 \implies t^2 \equiv 1 \pmod 8 \\ t \equiv 4 \pmod 8 \implies t^2 \equiv 0 \pmod 8 \\ t \equiv 5 \pmod 8 \implies t^2 \equiv 1 \pmod 8 \\ t \equiv 6 \pmod 8 \implies t^2 \equiv 4 \pmod 8 \\ t \equiv 7 \pmod 8 \implies t^2 \equiv 1 \pmod 8 \end{cases}$$

Portanto t^2 só pode ser 0,1 ou 4 módulo 8.

Caso 1. (Ambos pares): $3^m \equiv 3^n \equiv 1 \pmod 8 \implies 3^m + 3^n + 1 \equiv 3 \equiv t^2 \pmod 8$, absurdo!

Caso 2. (Ambos ímpares): $3^m \equiv 3^n \equiv 3 \pmod 8 \implies 3^m + 3^n + 1 \equiv 7 \equiv t^2 \pmod 8$, absurdo!

Caso 3. (Um deles é par e o outro é ímpar): Assuma sem perder a generalidade que m é par e n é ímpar, logo temos que $3^m \equiv 1 \pmod 8$ e $3^n \equiv 3 \pmod 8 \implies 3^m + 3^n + 1 \equiv 5 \equiv t^2 \pmod 8$, absurdo!

Então não existem soluções inteiras e positivas para a equação $3^m + 3^n + 1 = t^2$.

---

3 Problemas

. . . . . .

- **Problema 1.** Ache todos os n naturais tal que $3n + 1 | 5n^4 + 2n - 3$.

  . . . . . .

- **Problema 2.** Prove que $7 | \overline{d_n d_{n-1} \dots d_1 d_0} \iff 7 | \overline{d_n d_{n-1} \dots d_1} - 2d_0$.

  . . . . . .

- **Problema 3.** Prove que $11 | \overline{d_n d_{n-1} \dots d_1 d_0} \iff 11 | (d_1 + d_3 + \dots) - (d_2 + d_4 + \dots)$.

  . . . . . .

- **Problema 4.** Ache o algarismo das unidades de 3^{102}.

  . . . . . .

- **Problema 5.** Ache o algarismo das unidades de $\underbrace{2023^{2023^{\cdot^{\cdot^{\cdot^{2023}}}}}}_{2023 \text{ vezes}}$.

. . . . . .

- **Problema 6.** Prove que $8|3^m + 7^m - 2$ para todo m natural.

. . . . . .

- **Problema 7.** Ache todas as soluções inteiras e positivas da equação $3^x + 4^y = 5^z$.

. . . . . .

- **Problema 8.** Resolva a equação para os inteiros positivos $3^x - 5^y = z^2$.

. . . . . .

- **Problema 9.** Uma quádrupla $(a,\ b,\ c,\ d)$ é dita *dobarulho* quando a,b e c são algarismos não nulos e d é um inteiro positivo tais que:

  1. $a \leq 8$;
  2. $d > 1$;
  3. d divide os seis números de três algarismos $\overline{abc}$, $\overline{bca}$, $\overline{cab}$, $\overline{(a+1)cb}$, $\overline{cb(a+1)}$ e $\overline{b(a+1)c}$;

  Determine todas as quádruplas *dobarulho*.

. . . . . .

- **Problema 10.** Determine todos os pares $(a,\ b)$ de inteiros positivos tais que $ab^2 + b + 7$ divide $a^2b + a + b$.

. . . . . .

4 Conclusão

Por mais que simples os conceitos vistos nesse material, eles são muito úteis e aparecem com muita frequência em problemas, principalmente quando combinados. Muitas vezes não é uma ideia muito difícil que resolve esse tipo de problema, mas sim uma junção de várias ideias simples.

Esses são conceitos essenciais para a base de *Teoria dos Números*, portanto sempre devemos mantê-los em mente. Conteúdos mais avançados são, na maioria dos casos, apenas aprofundamentos e junções dessas propriedades.

"A Matemática pura, é, à sua maneira, a poesia das ideias lógicas"
–Albert Eistein