Primos, LTE e Outras Histórias

Semana Olímpica 2019
Rafael Filipe - rafaelfilipedoss@gmail.com

O objetivo desse material é apresentar algumas ideias recentes que tem aparecido nos problemas de Teoria dos Números envolvendo principalmente a análise de potências de primos nas divisões com inteiros. No decorrer do artigo utilizaremos a seguinte notação: sejam p, n inteiros. O símbolo $\nu_p(n)$ indica a maior potência de p que divide n. Em geral utilizamos p primo.

1 Primeiros passos

O primeiro exemplo não é nada trivial, mas é um excelente exemplo de como "arrumar a casa", ou seja, organizar bem as variáveis do problema, já pode ser um grande passo pra solucionar os problemas.

Exemplo 1 (PFB) Prove que para quaisquer inteiros $a_1, a_2, ..., a_n$ o número

$$\prod_{1\leq i<j\leq n} \frac{a_i - a_j}{i-j}$$

é um inteiro.

Solução:

Tomemos um primo p qualquer. Vamos provar que o expoente de p no numerador é sempre maior ou igual ao expoente do numerador. Para isso, dada uma potência de p qualquer, digamos p^k vamos mostrar que o conjunto das diferenças $a_i - a_j, 1 \leq i < j \leq n$ possui uma quantidade de múltiplos de p^k maior ou igual a quantidade de múltiplos de p^k em no conjunto das diferenças $i - j, 1 \leq i < j \leq n$.

Primeiramente, vamos calcular a quantidade de múltiplos de p^k, a qual denotaremos por N_k, no numerador. Sejam $x_0, x_1, ..., x_{p^k-1}$ a quantidade de números que deixam restos $0, 1, ..., p^k - 1$, respectivamente, na divisão por p^k. Não é difícil verificar que

$$N_k = \binom{x_0}{2} + \binom{x_1}{2} + \binom{x_2}{2} + ... + \binom{x_{p^k-1}}{2}.$$

Agora, vamos calcular a quantidade de múltiplos de p^k, a qual denotaremos por D_k, no denominador. Aplicando a Divisão Euclidiana de n por p^k, seja $n = p^k q + r$, com $0 \leq r < p^k$. Veja que temos exatamente $q + 1$ números que deixam resto $1, 2, ..., r$ na divisão por p^k e q números que deixam resto $r + 1, ..., p^k - 1, 0$. Portanto, temos que

$$D_k = r \times \binom{q+1}{2} + (p^k - r) \times \binom{q}{2}.$$

Portanto, queremos mostrar que

$$\binom{x_0}{2} + \binom{x_1}{2} + \binom{x_2}{2} + ... + \binom{x_{p^k-1}}{2} \geq r \times \binom{q+1}{2} + (p^k - r) \times \binom{q}{2},$$

em que $x_0 + x_1 + ... + x_{p^k-1} = n$. Suponha que $(x_0, x_1, ..., x_{p^k-1})$ é a p^k-upla que minimiza N_k (que certamente existe, já que o número de soluções inteiras não negativas de $x_0 + x_1 + ... + x_{p^k-1} = n$ é finito). Veja que se existem índices i, j tais que $x_j - x_i > 1$ e $x_j, x_i \geq 2$, então temos que

$$\binom{x_i}{2} + \binom{x_j}{2} > \binom{x_i + 1}{2} + \binom{x_j - 1}{2} \iff x_j - x_i > 1,$$

e então, trocando (x_i, x_j) por $(x_i + 1, x_j - 1)$ diminuímos o valor de N_k, o que contradiz a minimalidade da p^k-upla escolhida. Portanto, para quaisquer $i, j \in \{0, 1, 2, ..., p^k - 1\}$, temos $x_j - x_i \leq 1$. Isso significa que,

se $x_{i_0} < x_{i_1} < ... < x_{i_{p^k-1}}$ é a ordenação dos x_i's em ordem crescente, então existe um natural t tal que $x_{i_0} = x_{i_1} = ... = x_{i_{t-1}} = a$ e $x_{i_t} = ...x_{i_{p^k-1}} = a+1$. Portanto, temos que

$$N_k = t \times \binom{a}{2} + (p^k - t)\binom{a+1}{2}.$$

Mas temos que $t \times a + (p^k - t) \times (a+1) = n \Rightarrow n = p^k a + (p^k - t)$, donde, pela unicidade do quociente e resto na Divisão Euclidiana, obtemos $a = q$ e $p^k - t = r \Rightarrow t = p^k - r$, obtendo assim o mínimo desejado.

□

Nota-se que apenas a contagem dos fatores já é uma ideia bastante interessante para a resolução de um problema desse tipo.

Muitos desses problemas de divisibilidade abordam alguns números mais interessantes, como números binomiais e fatoriais. O seguinte fato básico envolvendo esse tipo de número é o teorema mais importante envolvendo esses números.

Teorema 1.1. *Seja n um inteiro positivo e p um número primo. Então,*

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + ... = \frac{n - s_p(n)}{p-1},$$

em que $s_p(n)$ é a soma dos algarismos de n na base p.

Demonstração: A primeira igualdade é direto por uma simples contagem dos fatores. Para a segunda igualdade, seja $n = n_0 + n_1 p + n_2 p^2 + \cdots + n_r p^r$ a representação de n na base p. Temos que

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{\infty} \left\lfloor \frac{n_0 + n_1 p + n_2 p^2 + \cdots + n_r p^r}{p^k} \right\rfloor = \sum_{k=1}^{r} (n_k + n_{k+1} p + \cdots + n_r p^{r-k}) =$$

$$\sum_{k=1}^{r} \sum_{i=0}^{r-k} n_{k+i} p^i = \sum_{k=1}^{r} \sum_{i=0}^{k-1} n_k p^i = \sum_{k=1}^{r} n_k \sum_{i=0}^{k-1} p^i = \sum_{k=1}^{r} n_k \left(\frac{p^k - 1}{p-1} \right) =$$

$$= \frac{\sum_{k=1}^{r} n_k p^k - \sum_{k=1}^{r} n_k}{p-1} = \frac{(n - n_0) - (S_p(n) - n_0)}{p-1} = \frac{n - S_p(n)}{p-1}.$$

Uma generalização desse teorema é segue abaixo (o caso particular ocorre quando $m_1 = m_2 = ... = m_k = 1$):

Teorema 1.2. *(Teorema de Kummer) Seja p um número primo e n um inteiro positivo que se escreve na base p como $n = n_0 + n_1 p + n_2 p^2 + \cdots + n_r p^r$. Defina $S_p(n) = n_0 + n_1 + ... + n_r$. Sendo $m_1, m_2, \ldots, m_k$ inteiros não negativos tais que $m_1 + m_2 + \cdots + m_k = n$, então*

$$\nu_p\left(\binom{n}{m_1, \ldots, m_k} \right) = \frac{1}{p-1} \left(\sum_{i=1}^{k} S_p(m_i) - S_p(n) \right).$$

A demonstração do Teorema 2 é direta usando a fórmula do multinomial e o Teorema 1. Prossigamos com mais alguns exemplos.

Exemplo 2 (PFB) Sejam n um inteiro positivo. Mostre que:

$$n! \mid (2^n - 1)(2^n - 2)...(2^n - 2^{n-1}).$$

Solução:

Veja primeiramente $(2^n - 1)(2^n - 2)...(2^n - 2^{n-1}) = 2^{1+2+...+(n-1)}(2^n - 1)(2^{n-1} - 1)...(2-1)$. Agora, veja que se q é um primo qualquer, então

$$\nu_q((2^n - 1)(2^{n-1} - 1)...(2-1)) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{ord_{q^k}(2)} \right\rfloor \geq \sum_{k=1}^{\infty} \left\lfloor \frac{n}{\phi(q^k)} \right\rfloor \geq \sum_{k=1}^{\infty} \left\lfloor \frac{n}{q^k} \right\rfloor = \nu_q(n!),$$

já que $q^k > \phi(q^k) \geq ord_q^k(2)$ para todo $q^k \geq 2$. Para $q = 2$ temos que $n - S_2(n) < n < 1 + 2 + ... + (n-1)$, obtendo assim o resultado desejado.

□

O exemplo a seguir trabalha um pouco com somatórios módulo primo. É bastante importante saber lidar com esse tipo de soma, principalmente quando envolve "frações" (inversos), pois isso pode evitar perda de tempo em passos intermediários de alguns problemas.

Exemplo 3 (Teorema de Wolstenholme) Seja $p > 3$ um número primo. Então o numerador do número

$$1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p-1}$$

é divisível por p^2.

Solução:

Considere o polinômio $Q(x) = (x-1)(x-2)...(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + ... + a_2x^2 + a_1x + a_0$. Veja que vale

$$1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p-1} = \frac{-a_1}{(p-1)!}.$$

Portanto, basta mostrarmos que $a_1 \equiv 0 \pmod{p^2}$. Olhemos $Q(p) \pmod{p^3}$. Temos que

$$Q(p) \equiv a_2p^2 + a_1p + a_0 \pmod{p^3}.$$

Mas $Q(p) = (p-1)! = a_0$, de modo que $a_2p^2 + a_1p \equiv 0 \pmod{p^3} \iff a_2p + a_1 \equiv 0 \pmod{p^2}$. Basta mostrar então que $a_2 \equiv 0 \pmod{p}$. Mas veja que

$$a_2 = (p-1)! \sum_{i<j} \frac{1}{ij} = \frac{(p-1)!}{2} \left[\left(\sum \frac{1}{i} \right)^2 - \sum \frac{1}{i^2} \right].$$

Mas temos que os inversos de $1, 2, ..., p-1$ são exatamente os números $1, 2, ..., p-1$ em alguma ordem, assim como os inversos de $1^2, 2^2, ..., (p-1)^2$ são exatamente os números $1^2, 2^2, ..., (p-1)^2$ em alguma ordem. Portanto, temos que

$$\frac{(p-1)!}{2} \left[\left(\sum \frac{1}{i} \right)^2 - \sum \frac{1}{i^2} \right] \equiv \frac{(p-1)!}{2} \left[\left(\sum i \right)^2 - \sum i^2 \right] \equiv$$

$$\equiv \frac{(p-1)!}{2} \left[\left(\frac{(p-1)p}{2} \right)^2 - \frac{(p-1)p(2p-1)}{6} \right] \equiv 0 \pmod{p}.$$

Agora, alguns problemas para praticar.

Problemas

1. (Shortlist 2007) Para cada inteiro $k \geq 2$, prove que 2^{3k} divide o número

$$\binom{2^{k+1}}{2^k} - \binom{2^k}{2^{k-1}}$$

mas 2^{3k+1} não.

2. (Shortlist 2012) Determine todos os inteiros $m \geq 2$ tais que todo n com $\frac{m}{3} \leq n \leq \frac{m}{2}$ divide o coeficiente binomial $\binom{n}{m-2n}$.

3. (Grécia TST 2017) Prove que o número $A = \frac{(4n)!}{(2n)!n!}$ é um inteiro divisível por 2^{n+1}, em que n é um inteiro positivo.

4. (IMO 2015) Determine todos os inteiros positivos (a, b, c) tais que

$$ab - c, \quad bc - a, \quad ca - b$$

são todos potências de 2.

5. Demonstrar que se $p > 3$ é primo, então $p^3 | \binom{2p}{p} - 2$.

6. Demonstre que para todo número primo $p > 3$, o número $\binom{np}{p} - n$ é divisível por p^{3+r} onde p^r é a maior potência de p que divide n.

7. (Tuymaada) Prove que a equação
$$\frac{1}{10^n} = \frac{1}{n_1!} + \frac{1}{n_2!} + ... + \frac{1}{n_k!}$$
não possui solução inteira com $1 \leq n_1 < ... < n_k$.

8. (Ibero 2005) Sejam m e n inteiros tais que
$$\frac{1}{1^p} + \frac{1}{2^p} + ... + \frac{1}{(p-1)^p} = \frac{m}{n}.$$
Prove que p^3 divide m.

9. (Shortlist 2011) Seja p um primo ímpar. Para cada a, defina $S_a = \sum_{k=1}^{p-1} \frac{a^k}{k}$. Prove que p divide o numerador de $S_3 + S_4 - 3S_2$.

10. Encontrar todos os inteiros positivos a, b, c tais que $(2^a - 1)(3^b - 1) = c!$.

2 Lema do Levantamento do Expoente

Quando falamos de divisibilidade e análise de potências de primo, talvez este seja o teorema mais importante. Vamos começar enunciando o lema:

Teorema 2.1. ***(Lema do Levantamento do Expoente - LTE)*** *Seja p um primo ímpar e a, b inteiros positivos distintos não divisíveis por p. Então, se $p|a-b$, então*
$$\nu_p(a^n - b^n) = \nu_p(a-b) + \nu_p(n).$$
Se n é ímpar e $p|a+b$, com $a+b \neq 0$, vale que
$$\nu_p(a^n + b^n) = \nu_p(a+b) + \nu_p(n).$$
Se $p = 2$, a melhor maneira de analisar é fatorando, de modo que omitiremos aqui a fórmula para esse caso.

A demonstração é por indução em $\nu_p(n)$ e ficará a cargo do leitor.

Vejamos agora algumas aplicações desse teorema.

Exemplo 4 Seja k um inteiro positivo. Determine todos os inteiros positivos n tais que $3^k \mid 2^n - 1$.

Solução:

Veja primeiramente que n é par, pois caso contrário teríamos $2^n - 1 \equiv (-1)^n - 1 \equiv 1 \pmod 3$, um absurdo. Logo, $n = 2t$, $t \in \mathbb{N}$. Portanto, queremos achar todos os t tais que $3^k \mid 4^t - 1$. Como $3^1 \mid\mid 4 - 1$, pelo Lema do Levanamento do Expoente temos $\nu_3(t) + 1 \geq k \Rightarrow \nu_3(t) \geq k - 1$. Portanto, $n = 2t = 2.3^{k-1}a$, $a \in \mathbb{N}$.

Exemplo 5 (Irlanda 1996) Seja p um número primo e a e n inteiros positivos. Prove que se
$$2^p + 3^p = a^n,$$
então $n = 1$.

Solução:

Suponha p primo ímpar (se $p = 2$ o resultado é imediato). Veja que $5 \mid\mid 3 + 2$. Portanto, pelo Lema do Levantamento do Expoente, temos que $\nu_5(2^p + 3^p) = 1 + \nu_5(p)$. Mas se $5 \mid 2^p + 3^p$, então $5 \mid a^n \Rightarrow 5 \mid a \Rightarrow 5^n \mid a^n \Rightarrow 5^n \mid 2^p + 3^p \Rightarrow n \leq 1 + \nu_5(p)$. Logo, $n = 1$ ou $n = 2$ e $p = 5$. Mas se $p = 5$, temos $a^n = 275$, que não é quadrado, absurdo! Portanto, $n = 1$.

Exemplo 6 (IMO 1990) Determine todos os inteiros $n > 1$ tais que

$$\frac{2^n + 1}{n^2}$$

é um inteiro.

Solução:

O primeiro grande fato a ser utilizado é o Teorema Fundamental da Aritmética. Seja então $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ a fatoração em primos de n, com $p_1 < p_2 < ... < p_k$ e $\alpha_1, \alpha_2, ..., \alpha_k > 0$. Evidentemente, n é ímpar e por isso $p_1, ..., p_k$ são todos ímpares. Temos que $2^n \equiv -1 \pmod{p_1} \Rightarrow 2^{2n} \equiv 1 \pmod{p_1}$. Temos também que, pelo Pequeno Teorema de Fermat, vale $2^{p_1 - 1} \equiv 1 \pmod{p_1}$.

Sabemos que $\text{mdc}(a^\ell - 1, a^k - 1) = a^{\text{mdc}(\ell,k)} - 1$. Então, $2^{\text{mdc}(2n, p_1 - 1)} \equiv 1 \pmod{p_1}$.

Mas os fatores primos de $p_1 - 1$ são menores que p_1 e como os fatores primos de n são maiores ou iguais a p_1, temos que $\text{mdc}(2n, p_1 - 1) = 2$ e, portanto, $2^2 \equiv 1 \pmod{p_1} \Rightarrow p_1 = 3$.

Agora, temos que $3|2 + 1$. Então, $\nu_3(2^n + 1) = \nu_3(2 + 1) + \nu_3(n) = \nu_3(n) + 1 = \alpha_1 + 1$. Mas como $n^2|2^n + 1$, temos que $2\alpha_1 \leq \alpha_1 + 1 \Rightarrow \alpha_1 \leq 1 \Rightarrow \alpha_1 = 1$.

Repetindo o procedimento para p_2, dessa vez, podemos afirmar que $\text{mdc}(2n, p_2 - 1)$ divide $2p_1 = 6$. Portanto, $2^6 \equiv 1 \pmod{p_2} \Rightarrow 63 \equiv 0 \pmod{p_2}$ e por isso $p_2 = 3$ ou $p_2 = 7$. Como $p_2 > p_1 = 3$, segue que $p_2 = 7$. Mas repare que se $n = 3t$, com t inteiro ímpar, então $2^{3t} + 1 \equiv 8^t + 1 \equiv 2 \pmod{7}$, absurdo! Portanto, isso nos mostra que p_2 não pode existir.

Portanto, a única solução é $n = 3$.

□

Exemplo 7 (Shortlist 2000) Determine todas as triplas de inteiros positivos (a, m, n) tais que $a^m + 1 \mid (a + 1)^n$.

Solução:

Seja p um primo que divide $a^m + 1$. Então, p divide $a + 1$. Portanto, $a^m + 1 \equiv (-1)^m + 1 \pmod{p}$. Se $m = 2t$, temos que $p = 2$ e portanto $a^{2t} + 1 = 2^k$. Mas é fácil ver que $4 \nmid a^{2t} + 1$, de modo que $k = 1 \Rightarrow a = 1$. Nesse caso temos a solução $(a, m, n) = (1, m, n)$.

Suponha m ímpar e $a > 1$. Sendo p um divisor de $a^m + 1$, pelo Lema do Levantamento do Expoente, temos que

$$\nu_p(a + 1) + \nu_p(m) = \nu_p(a^m + 1) \Rightarrow \nu_p(m) = \nu_p\left(\frac{a^m + 1}{a + 1}\right).$$

Mas temos que todo primo que divide $a^m + 1$ divide $a + 1$. Mas então, necessariamente devemos ter

$$\frac{a^m + 1}{a + 1} \mid m,$$

donde $a^m + 1 \leq m(a + 1)$.

Se $a > 2$, não é difícil mostrar por indução que para $m \geq 2$ temos $a^m + 1 > m(a + 1)$ e, portanto, não há solução. Então, $m = 1$, obtendo assim a solução $(a, m, n) = (a, 1, n)$, $a > 2$.

Se $a = 2$, podemos mostrar por indução que $2^m + 1 > 3m$ para $m \geq 4$. Temos $m = 1$ ou $m = 3$ (m é ímpar), obtendo assim as soluções $(a, m, n) = (2, 1, n)$ e $(a, m, n) = (2, 3, n)$, $n \geq 2$.

Portanto, as soluções são $(1, m, n), (a, 1, n)$ e, para $k \geq 2$, $(a, m, n) = (2, 3, k)$.

□

Exemplo 8 (CIIM 2014) Sejam n um inteiro positivo e p um primo ímpar. Mostre que:

$$(p - 1)^n . n! \mid (p^n - 1)(p^n - p)...(p^n - p^{n-1}).$$

Solução:

Veja primeiramente $(p^n - 1)(p^n - p)...(p^n - p^{n-1}) = p^{1+2+...+(n-1)}(p^n - 1)(p^{n-1} - 1)...(p - 1)$. Agora, veja que se q é um primo qualquer diferente de p e que não divide $p - 1$, então

$$\nu_q((p^n - 1)(p^{n-1} - 1)...(p - 1)) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{ord_{q^k}(p)} \right\rfloor \geq \sum_{k=1}^{\infty} \left\lfloor \frac{n}{\phi(q^k)} \right\rfloor \geq \sum_{k=1}^{\infty} \left\lfloor \frac{n}{q^k} \right\rfloor = \nu_q(n!),$$

já que $q^k > \phi(q^k) \geq ord_q^k(p)$ para todo $q^k \geq 2$. Para $q = p$ temos que $\frac{n-S_p(n)}{p-1} < n < 1 + 2 + ... + (n-1)$. Resta analisar quando q divide $p-1$. Temos que se $q^\alpha \mid\mid p-1$, então $\nu_q((p-1)^n.n!) = n\alpha + \sum_{k=1}^{\infty} \left\lfloor \frac{n}{q^k} \right\rfloor$.

Temos também que $ord_{q^k}(p) = 1$ para $k = 1, 2, ..., \alpha$ e, para $\alpha + i$, vale por LTE que $\nu_q(p^{ord_{q^{\alpha+i}}(p)} - 1) = \nu_q(p-1) + \nu_q(ord_{q^{\alpha+i}}(p))$, donde $ord_{q^{\alpha+i}}(p) = q^i$. Portanto, temos que

$$\nu_q((p^n-1)(p^n-p)...(p^n-p^{n-1})) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{ord_{q^k}(p)} \right\rfloor = n\alpha + \sum_{k=1}^{\infty} \left\lfloor \frac{n}{ord_{q^{\alpha+k}}(p)} \right\rfloor = n\alpha + \sum_{k=1}^{\infty} \left\lfloor \frac{n}{q^k} \right\rfloor = \nu_q((p-1)^n.n!),$$

o que conclui a demonstração.

□

Mais problemas para exercitar.

Problemas

1. (Shortlist 1991) Determine o maior k tal que
$$1991^k \mid 1990^{1991^{1992}} + 1992^{1991^{1990}}.$$
2. Prove que o número $a^{a-1} - 1$ nunca é livre de quadrados para qualquer inteiro $a > 2$.
3. (Unesco 1995) Sejam a, n inteiros positivos e p um primo ímpar tal que $a^p \equiv 1 \pmod{p^n}$. Prove que $a \equiv 1 \pmod{p^{n-1}}$.
4. (Iran 2008) Mostre que os únicos valores inteiros positivos de a para os quais $4(a^n + 1)$ é um cubo perfeito para todo inteiro positivo n é 1.
5. (PFB) Sejam a, b, c inteiros positivos tais que $c \mid a^c - b^c$. Mostrar que $c \mid \frac{a^c - b^c}{a-b}$.
6. (Rússia 1996) Sejam x, y, p, n, k tais que n é ímpar e p é um primo ímpar. Prove que se $x^n + y^n = p^k$, então n é uma potência de p.
7. Seja p um número primo. Determine todas as soluções da equação $a^p - 1 = p^k$ no conjunto dos inteiros positivos.
8. Determine todas as soluções de $(n-1)! + 1 = n^m$.
9. (Bulgária 1997) Para um inteiro positivo n, o número $3^n - 2^n$ é uma potência de primo. Mostre que n é primo.
10. (PFB) Sejam a, b racionais positivos tais que para infinitos valores inteiros positivos de n, o número $a^n - b^n$ é um inteiro positivo. Prove que a e b são ambos inteiros.
11. (Shortlist 1997) Sejam m, n, b inteiros posivitos com $m \neq n$ e $b > 1$. Mostre que se os divisores primos dos números $b^n - 1$ e $b^m - 1$ são os mesmos, então $b + 1$ é uma potência de 2.
12. (Shortlist 2014) Determine todas as triplas (p, x, y) consistindo de um primo p e dois inteiros positivos x e y tais que $x^{p-1} + y$ and $x + y^{p-1}$ são todos potências de p.
13. (China 2018) Seja n um inteiro positivo. Denote por A_n o conjunto dos primos p tais que existem inteiros positivos a, b para os quais
$$\frac{a+b}{p} \text{ e } \frac{a^n + b^n}{p^2}$$
são ambos inteiros relativamente primos com p. Se A_n é finito, seja $f(n)$ o valor de $|A_n|$.
a) Prove que A_n é finito se, e somente se, $n \neq 2$.
b) Sejam m, k inteiros positivos ímpares e seja d o mdc deles. Mostre que
$$f(d) \leq f(k) + f(m) - f(km) \leq 2f(d).$$
14. (Taiwan 1999) Determine todas as triplas (x, y, z) de inteiros positivos tais que $(x+1)^{y+1} + 1 = (x+2)^{z+1}$.

15. (Shortlist 2005) Determine todos os inteiros positivos n tais que existe um único a tal que $0 \leq a < n!$ e vale a seguinte propriedade:
$$n! \mid a^n + 1.$$

16. (China TST 2009) Sejam $a > b > 1$ um inteiro positivo, com b um inteiro ímpar, e n um inteiro positivo. Se $b^n \mid a^n - 1$, mostre que $a^b > \frac{3^n}{n}$.

3 Construindo Exemplos

Há problemas de Teoria dos Números em que não se vê diretamente como aplicar algumas técnicas diretamente. Porém, pode ser interessante utilizá-las para construir "números espertos", que satisfaçam alguma propriedade desejada.

Exemplo 9 Seja $k > 1$ um inteiro. Mostre que existem infinitos inteiros positivos n tais que
$$n \mid 1^n + 2^n + ... + k^n.$$

Solução:

Vamos utilitar o LTE para construir os inteiros n desejados. Se k é par, veja que
$$1^n + 2^n + ... + k^n = (1^n + k^n) + (2^n + (k-1)^n) + ... + ((k/2)^n + (k/2+1)^n).$$

Seja q um primo divisor de $k+1$. Tomando $n = q^a$, pelo LTE, temos que $q^a \mid (k+1-i)^{q^a} + i^{q^a}$.

Se k é ímpar seja q um divisor primo de k. Veja que
$$1^n + 2^n + ... + k^n = (1^n + (k-1)^n) + (2^n + (k-2)^n) + ... + ((k-1)/2-1)^n + ((k-1)/2)^n) + k^n.$$
Tomando $n = q^a$, temos novamente pelo LTE que $q^a \mid (k-i)^{q^a} + i^{q^a}$ e temos também que $q^a \mid k^n$.

Variando a nos inteiros positivos, obtemos infinitos n, como desejado.

□

Problemas

1. (Shortlist 2014) Seja $n > 1$ um inteiro. Prove que infinitos termos da sequência $(a_k)_{k \geq 1}$, definida por
$$a_k = \left\lfloor \frac{n^k}{k} \right\rfloor,$$
são ímpares. (Dado um número real x, $\lfloor x \rfloor$ denota o maior inteiro que não excede x).

2. (Shortlist 2007) Para um primo p e um inteiro n, seja $\nu_p(n)$ o expoente de p na fatoração em primos de $n!$. Dado $d \in \mathbb{N}$ e $\{p_1, p_2, \ldots, p_k\}$ um conjunto de k, mostre que existem infinitos inteiros positivos n tais que $d \mid \nu_{p_i}(n)$ for all $1 \leq i \leq k$.

3. (Treinamento IMO 2014) Seja k um inteiro positivo fixado. O radical de um número natural n, denotado por $rad(n)$ é o porduto de todos os divisores primos de n, cada primo sendo considerado só uma vez. Por exemplo, $rad(120) = 2.3.5 = 30$. Existe uma terna de inteiros positivos primos entre si, a, b e c tais que
$$a + b = c \text{ e } c > k.rad(abc)?$$

4. (Iran 2017) Seja n um inteiro positivo. Prove que existe um inteiro positivo m tal que
$$7^n \mid 3^m + 5^m - 1$$

5. (IMO 2003) Seja p um inteiro positivo. Prove que existe um primo q tal que para todo inteiro positivo n, o número $n^p - p$ não é divisível por q.

6. (RMM 2012) Seja $f(n) = 2^n + 1$. Prove que há infinitos n tais que $n \nmid f(n)$ mas $n \mid f(f(n))$.

7. (USA TST 2019) Seja $\mathbb{Z}/n\mathbb{Z}$ o conjunto dos inteiros módulo n (então $\mathbb{Z}/n\mathbb{Z}$ tem n elementos). Determine todos os inteiros positivos n para os quais existe uma função bijetora $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, tais que as 101 funções
$$g(x), \quad g(x) + x, \quad g(x) + 2x, \quad \ldots, \quad g(x) + 100x$$
sejam todas bijeções em $\mathbb{Z}/n\mathbb{Z}$.

4 Sequências e TN: olhando fatores primos

Agora vamos lidar com problemas um pouco não usuais. Aqui a ideia não é aplicar alguma técnica do assunto diretamente, mas analisar alguma espécie de "monovariante" em certas sequências, relacionada aos fatores primos dos elementos da sequência. Parece um pouco específico, mas é mais comum do que parece. Vejamos alguns exemplos:

Exemplo 10 (OBMU 2017) Fixados os inteiros positivos a e b, mostre que o conjunto dos divisores primos dos termos da sequência $a_n = a.2017^n + b.2016^n$ é infinito.

Solução:

Suponha que tal conjunto seja finito e sejam $\{p_1, p_2, ..., p_k\}$ estes primos. Não é difícil verificar que podemos supor a, b, 2016, 2017 dois a dois primos entre si (Por quê?).

Defina a sequência $n_\alpha = \phi(p_1^\alpha p_2^\alpha ... p_k^\alpha)$. Olhando para a sequência $(a_{n_\alpha})_{\alpha\in\mathbb{N}}$, temos que ela é claramente crescente e ilimitada.

Sejam $\theta_1, \theta_2, ..., \theta_k$ os expoentes de $p_1, p_2, ..., p_k$ em $a + b$, respectivamente. Veja que $a_{n_\alpha} \equiv a + b \pmod{p_i^\alpha}$.

Tome $\alpha > \theta_i$. Se $\nu_{p_i}(a_{n_\alpha}) > \theta_i$, temos que $a + b \equiv 0 \pmod{p_i^{\theta_i+1}}$, absurdo! Portanto, $\nu_{p_i}(a_{n_\alpha}) \leq \theta_i$ e então $a_{n_\alpha} \leq a + b$ para todo α, absurdo, já que a sequência $(a_{n_\alpha})_{\alpha\in\mathbb{N}}$ é ilimitada.

Portanto, o conjunto dos números primos que dividem tal sequência é infinito.

□

Problemas

1. (IMO 2018) Sejam a_1, a_2, ... uma sequência infinita de inteiros positivos. Suponha que existe um inteiro $N > 1$ tal que, para cada $n \geq N$, o número

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$$

é um inteiro. Prove que existe um inteiro positivo M tal que $a_m = a_{m+1}$ para todo $m \geq M$.

2. (TSTST 2018) Para quais inteiros positivos $b > 2$ existem infinitos inteiros positivos n tais que n^2 divide $b^n + 1$?

3. (Iran 2017) Seja n um inteiro positivo. Considere números primos $p_1, \ldots, p_k$. Seja $a_1, \ldots, a_m$ todos os inteiros positivos menores que n que não são divisíveis por p_i para todo $1 \leq i \leq n$. Prove que se $m \geq 2$ então

$$\frac{1}{a_1} + \cdots + \frac{1}{a_m}$$

não é inteiro.

4. (Shortlist 2012) Sejam x e y inteiros positivos. Se $x^{2^n} - 1$ é divisível por $2^n y + 1$ para todo inteiro positivo n, prove que $x = 1$.

5 Problemas Extras

1. (CIIM 2018) Seja m um inteiro ímpar e $\mathbb{Z}_m$ o anel de inteiros módulo m. Definimos uma relação de equivalência em $\mathbb{Z}_m$ dada por $x \sim y$ se existe um natural t tal que $y = 2^t x$. Determine todos os valores de m tais que o número de classes de equivalência é par.

2. (Erdos) Começando com um inteiro n_0, queremos construir uma sequência $n_0, n_1, n_2, ...$ tal que $\phi(n_i) = n_{i-1}$, para $i = 1, 2, ...$ Então isto é possível se, e somente se, n_0 é da forma $2^j 3^k$, e o mesmo acontecerá com todos os $n_i's$.

3. (Vjtech 2016) Determine todos os inteiros n tais que $\phi(n)$ divide $n^2 + 3$.

6 Referências

[1] BROCHERO, Fábio et al. Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro. 2011.

[2] ANDREESCU, Titu; DOSPINESCU, Gabriel. Problems from the Book. 2008.