Lema do Levantamento do Expoente

Treinamento EGMO 2021
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

Muitos desses problemas de divisibilidade abordam alguns números mais interessantes, como números binomiais e fatoriais.

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

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

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

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

Exemplo 1 (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.

□

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 2 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 3 (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 4 (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 5 (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 6 (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.

□

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 7 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.

4 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. Calcule $\text{ord}_{2^k}(5)$ e $\text{ord}_{5^k}(2)$ para todo inteiro positivo k.
6. (PFB) Sejam a, b, c inteiros positivos tais que $c \mid a^c - b^c$. Mostrar que $c \mid \frac{a^c - b^c}{a-b}$.
7. (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.
8. (IMO 2019) Determine todos os pares (k, n) de inteiros positivos tais que
$$k! = (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1}).$$
9. (Turquia TST 2019) Seja $p > 2$ um número primo e $m > 1$ e n inteiros positivos tais que $\frac{m^{pn}-1}{m^n-1}$ é um número primo. Mostre que:
$$pn \mid (p-1)^n + 1.$$
10. Seja p um número primo. Determine todas as soluções da equação $a^p - 1 = p^k$ no conjunto dos inteiros positivos.
11. Determine todas as soluções de $(n-1)! + 1 = n^m$.
12. (Bulgária 1997) Para um inteiro positivo n, o número $3^n - 2^n$ é uma potência de primo. Mostre que n é primo.
13. (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.
14. (Shortlist 2006) Determine todas as soluções inteiras da equação
$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$
15. (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.
16. (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.

17. (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
$$f(d) \leq f(k) + f(m) - f(km) \leq 2f(d).$$

18. (Taiwan 1999) Determine todas as triplas (x, y, z) de inteiros positivos tais que $(x+1)^{y+1} + 1 = (x+2)^{z+1}$.

19. (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:
$$n! \mid a^n + 1.$$

20. (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 $a^b > \frac{3^n}{n}$.

21. (Shortlist 2017) UM número racional é chamado *pequeno* se ele tem uma quantidade finita de dígitos em sua representação decimal. Para um inteiro positivo m, dizemos que um inteiro positivo t é $m-$*tástico* se existe um número $c \in \{1, 2, 3, \ldots, 2017\}$ tal que $\frac{10^t-1}{c \cdot m}$ é pequeno, e tal que $\frac{10^k-1}{c \cdot m}$ não é pequeno para $1 \leq k < t$. Seja $S(m)$ o conjunto dos números $m-$*tásticos*. Considere $S(m)$ para $m = 1, 2, \ldots$. Qual é a maior quantidade de elementos em $S(m)$?

22. (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).

23. (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 $1 \leq i \leq k$.

24. (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
$$a + b = c \text{ e } c > k.rad(abc)?$$

25. (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 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.