SEMANA OLÍMPICA 2021

• Levanta o expoente, princesa, senão a valorização p-ádica cai! •

Profª Ana Paula Chaves
apchaves@ufg.br
https://sites.google.com/ufg.br/apchaves

Resumo

Existem diversos resultados e tópicos em Teoria dos Números, que são recorrentes em diversas olimpíadas de Matemática, tanto a nível nacional quanto internacional. Um deles é o *Lema do Levantamento do Expoente*, ou simplesmente *LTE* (sigla em inglês). Nesse texto, vamos discorrer sobre esse resultado e aplicá-lo na resolução de alguns problemas de olimpíada. Ao final, deixamos alguns problemas propostos, para deleite do(a) leitor(a).

INTRODUÇÃO

Especialmente ao longo da última década, um resultado sobre o maior expoente de um primo que divide a diferença entre duas potências n-ésimas, tornou-se conhecido na comunidade olímpica como *Lema do Levantamento do Expoente*, abreviado por sua sigla em inglês *LTE*[1].

Tome p um número primo e sejam a e b inteiros, de modo que $p \mid a-b$. Então, sabemos de imediato (usando congruência, por exemplo), que $p \mid a^n - b^n$, para todo $n \in \mathbb{N}$. Mais ainda, se m é a maior potência de p que divide $a-b$ (teremos uma notação especial para essa potência depois), então pela fatoração $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$, também sabemos que $p^m \mid a^n - b^n$. A pergunta é: Será que $a^n - b^n$ pode ser divisível por uma potência de p maior que m? Caso a resposta seja positiva, qual passa a ser a maior potência de p que divide $a^n - b^n$? O *Lema do Levantamento do Expoente* responde à essas duas perguntas de forma bastante imediata, e possui versões inclusive para a soma de potências $a^n + b^b$.

Na primeira seção desse texto, passamos brevemente pelo background necessário para o bom entendimento e manuseio do LTE, falando um pouco sobre *valorização p-ádica*, seus resultados mais básicos e sugerindo alguns problemas. Na segunda parte, enunciamos e demonstramos a versão principal do LTE, estabelecendo os seus corolários, e propomos alguns problemas de "aquecimento". Na

[1] Lifting the Exponent

última seção, de *Problemas Propostos*, o leitor encontrará diversos desafios para praticar as técnicas e resultados encontrados no texto.

1. Valorização p-ádica

Antes de passarmos ao resultado principal dessas notas, é necessário um pequeno *background* para que o mesmo possa ser utilizado com mais desenvoltura, onde aproveitamos a oportunidade para enunciar alguns resultados básicos sobre *valorização p-ádica*, que definimos a seguir.

Definição 1. Sejam p um número primo e $a \in \mathbb{N}$. Denominamos por *valorização p-ádica de a*, a maior potência de p que divide a. A notação utilizada é $v_p(a)$.

Exemplo 1. Temos:

- $30 = 2 \cdot 3 \cdot 5$, então $v_2(30) = 1$;
- $400 = 2^4 \cdot 5^2$, então $v_5(400) = 2$;
- $1120 = 2^5 \cdot 5 \cdot 7$, então $v_3(1120) = 0$;

Observação 1. Também podemos definir a valorização p-ádica para um número racional a/b, como

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

Os dois fatos abaixo são essenciais, e suas demonstrações são deixadas como um leve exercício, apenas para “alongar"as mãos. :)

Teorema 1. Sejam p um número primo e $a, b \in \mathbb{Z}$. Então:

(i) $v_p(ab) = v_p(a) + v_p(b)$;

(ii) Se $v_p(a) > v_p(b)$, então $v_p(a+b) = v_p(b)$;

Para ilustrar uma primeira aplicação do conceito, passamos ao seguinte problema.

Problema 1.1. Mostre que $\displaystyle\sum_{i=1}^{n} \frac{1}{i}$ não é inteiro, para $n \geq 2$.

É bastante recorrente em problemas de TN, termos que lidar com a valorização p-ádica de fatoriais. Para essa finalidade, o resultado a seguir é clássico e efetivo, como poderemos ver posteriormente em suas aplicações.

Teorema 2 (Fórmula de Polignac)**.** Para p um número primo e $n \in \mathbb{N}$, temos

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n - s_p(n)}{p-1},$$

onde $s_p(n)$ é a soma dos dígitos de n na base p.

Abaixo, temos alguns problemas onde aplicar a Fórmula de Polignac é uma jogada bem interessante. Tente!

Problema 1.2. Sem fazer uso de identidades binomiais, mostre que para todo n inteiro positivo, o número $\frac{1}{n+1}\binom{2n}{n}$ também é inteiro.

2. O Lema do Levantamento do Expoente

Entramos agora na nossa seção principal, onde primeiro enunciamos e demonstramos a versão principal do LTE, para então passar por seus corolários. Após tais resultados, vamos "atacar" os primeiros problemas onde será possível aplicar o Lema.

Teorema 3 (Lema do Levantamento do Expoente - LTE)**.** Sejam $p \in \mathbb{P} - \{2\}$ e $a, b \in \mathbb{N}$, tais que $p \nmid ab$. Então, se $p \mid a - b$, temos

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n).$$

Demonstração. Vamos proceder por indução em $v_p(n)$. Para o caso base, $v_p(n) = 0$, primeiro observe que

$$v_p(a^n - b^n) = v_p(a-b) + v_p(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}).$$

Como $a \equiv b \pmod{p}$, então

$$a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \equiv na^{n-1} \pmod{p},$$

e assim, como $(a,p) = (n,p) = 1$, então $p \nmid a^{n-1} + a^{n-2}b + \cdots + b^{n-1}$, donde concluímos que

$$v_p(a^n - b^n) = v_p(a-b),$$

como desejado. Ao invés de passar diretamente para o passo indutivo, vamos mostrar um "segundo" caso base, que vai nos ajudar a finalizar mais rápido a indução. Seja $v_p(n) = 1$, donde $n = pn_1$ e $p \nmid n_1$. Com isso, temos que,

$$v_p(a^{pn_1} - b^{pn_1}) = v_p((a^p)^{n_1} - (b^p)^{n_1}) = v_p(a^p - b^p),$$

onde a última igualdade é válida pelo “primeiro" caso base. Agora, como $p \mid a-b$, seja $a = b+kp$, para algum $k \in \mathbb{N}$. Assim, conseguimos,

$$(b+kp)^p - b^p = \binom{p}{1}(kp)b^{p-1} + \binom{p}{2}(kp)^2 b^{p-2} + \cdots + \binom{p}{p}(kp)^p.$$

Agora, usando que $p \mid \binom{p}{i}$, para todo $1 \leq i \leq p-1$, e também lembrando que $p \nmid b$, temos,

$$v_p((b+kp)^p - b^p) = v_p(kp^2) = 2 + v_p(k),$$

donde por $a-b = kp$, então $v_p(k) = v_p(a-b) - 1$, e substituindo acima, concluímos que

$$v_p((b+kp)^p - b^p) = v_p(a-b) + 1,$$

como queríamos. Agora estamos prontos para o nosso passo indutivo. Suponha que o Lema é válido para todo $v_p(n) = k$. Assim, tome m tal que $v_p(m) = k+1$, ou seja $m = m_1 p^{k+1}$, onde $p \nmid m_1$. Então, temos

$$\begin{aligned} v_p(a^m - b^m) &= v_p\left(a^{m_1 p^{k+1}} - b^{m_1 p^{k+1}}\right) \\ &= v_p\left((a^{p^k})^{pm_1} - (b^{p^k})^{pm_1}\right) \\ &= v_p\left(a^{p^k} - b^{p^k}\right) + 1 \\ &= v_p(a-b) + k + 1, \end{aligned}$$

onde a penúltima igualdade é consequência do nosso “segundo" caso base, e a última da hipótese de indução. Assim, finalizamos a demonstração. □

Corolário 1. Sejam $p \in \mathbb{P} - \{2\}$, tal que $p \nmid ab$ mas $p \mid a-b$, e n um inteiro positivo ímpar, então

$$v_p(a^n + b^n) = v_p(a+b) + v_p(n)$$

Demonstração. Tente demonstrar esse fato, seguindo os mesmos passos da prova do Teorema 3. :) □

Teorema 4. Se $p = 2$ e n é par, então $4 \mid x \pm y \Rightarrow v_2(x^n - y^n) = v_2(x \pm y) + v_2(n)$

Demonstração. (Em Breve) □

Problema 2.1. Seja $k \in \mathbb{N}$. Encontre todos os $n \in \mathbb{N}$, tais que $3^k \mid 2^n - 1$.

Problema 2.2 (Irã 2008)**.** Mostre que o único $a \in \mathbb{N}$ para o qual $4(a^n+1)$ é um cubo para todo $n \in \mathbb{N}$, é $a = 1$.

Problema 2.3 (Irlanda 1996)**.** Seja $p \in \mathbb{P}$ e $a, n \in \mathbb{N}$. Prove que se $2^p + 3^p = a^n$, então $n = 1$.

3. Problemas Propostos

Problema 3.1 (Canada)**.** Encontre todos os inteiros positivos n tais que $2^{n-1} \mid n!$.

Problema 3.2. Encontre todos os inteiros positivos n tais que $n \mid (n-1)!$.

Problema 3.3 (USAMO)**.** Mostre que

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

é inteiro para todo par m, n de inteiros positivos.

Problema 3.4. Seja $k \in \mathbb{N}_{>1}$. Mostre que existem infinitos $n \in \mathbb{N}$, tais que

$$n \mid 1^n + 2^n + \cdots + k^n.$$

Problema 3.5. Encontre todos os $n \in \mathbb{N}$ para os quais existem x, y e $k \in \mathbb{N}$ tais que $(x, y) = 1, k > 1$ e

$$3^n = x^k + y^k.$$

Problema 3.6 (IMO 1990)**.** Determine todos os inteiros positivos n, tais que $\dfrac{2^n+1}{n^2}$ é inteiro.

Problema 3.7. Encontre todas as soluções da equação Diofantina

$$(n-1)! + 1 = n^m,$$

para n, m inteiros positivos.

Problema 3.8. Qual a maior potência k de 1991 para a qual

$$1991^k \mid 1991^{1991^{1992}} + 1992^{1991^{1990}}?$$

Problema 3.9. Sejam $p > 2013$ um número primo, e a, b inteiros positivos tais que $p \mid a+b$, mas $p^2 \nmid a+b$. Se $p^2 \mid a^{2013} + b^{2013}$, para quantos $n \leq 2013$ inteiros positivos, temos $p^n \mid a^{2013} + b^{2013}$?

Problema 3.10 (AMM)**.** Sejam a, b, c inteiros positivos tais que $c \mid a^c - b^c$. Mostre que

$$c \mid \frac{a^c - b^c}{a-b}$$

Problema 3.11 (IMO 1999)**.** Encontre todos os pares de inteiros positivos (x, p) tais que p é primo, $x \leq 2p$, e $x^{p-1} \mid (p-1)^x + 1$.

Problema 3.12 (Bulgária)**.** Mostre que se para n inteiro positivo, temos que $3^n - 2^n$ é uma potência de primo, então n é primo.

Problema 3.13 (China TST 2009)**.** Sejam $a > b > 1$ inteiros positivos, b um número ímpar e n um inteiro positivo. Se $b^n \mid a^n - 1$, mostre que $a^b > \dfrac{3^n}{n}$.