Valorização p-ádica em inteiros e racionais

João Ferreira

Introdução.

Como afirma o Teorema Fundamental da Aritmética, todo número inteiro tem uma fatoração única em números primos. Isso nos leva à ideia de analisar um número a partir de seus fatores primos e é daí que surge a valorização p-ádica. Nesse material, iremos introduzir o conceito já conhecido por muitos como v_p e expandí-lo ao conjunto dos números racionais, um truque que tem sido muito útil em problemas recentes de grandes olimpíadas. Como o objetivo principal desse material é apresentar problemas com ideias diferentes e ensinar o leitor a aplicar os conceitos aprendidos, não incluiremos as demonstrações das propriedades básicas. É recomendado que você tente prová-las e, caso não consiga, visite as referências de Ana Paula e Davi Lopes.

Definição: Denotaremos por $v_p(n)$ o maior expoente k tal que $p^k \mid n$ (i.e. $p^{k+1} \nmid n$) para um inteiro qualquer n e um primo p. Como um abuso de notação, $v_p(0) = \infty$.

Propriedades básicas:

1. $v_p(ab) = v_p(a) + v_p(b)$;
2. $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$;
3. $v_p(a \pm b) \geq \min(v_p(a), v_p(b))$, com igualdade sempre que $v_p(a) \neq v_p(b)$;

   Para demonstrar as propriedades acima, escreva $a = p^\alpha x$ e $b = p^\beta y$ onde $p \nmid xy$ e desenvolva as expressões.
4. **Lifting The Exponent (LTE).** Seja p um primo ímpar tal que $p \nmid ab$.
   - $p \mid a - b \implies v_p(a^n - b^n) = v_p(a-b) + v_p(n)$;
   - $p \mid a + b$ e n ímpar $\implies v_p(a^n + b^n) = v_p(a+b) + v_p(n)$.

     Se $p = 2$ e $2 \nmid ab$, temos o seguinte:

- n ímpar $\implies v_2(a^n - b^n) = v_2(a-b)$;
- n par $\implies v_2(a^n - b^n) = v_2(a-b) + v_2(a+b) + v_2(n) - 1$.

Para provar o LTE, tente realizar uma indução em $v_p(n)$. O caso $a^n + b^n$ requer n ímpar para ser fatorado como $(a+b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1})$ e é imediato à partir da demonstração do caso $a^n - b^n$ (substitua b por $-b$).

No caso $p = 2$, escreva $n = 2^x y$ com $2 \nmid y$ e fatore a expressão utilizando sucessivas diferenças de quadrados. Em seguida, analise a divisibilidade de cada termo por 4, pois a maior parte deles não será divisível por 4 (por que?).

5. **Fórmula de Polignac/Legendre.**

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

Nesse caso, perceba que há $\left\lfloor \frac{n}{p} \right\rfloor$ múltiplos de p menores que n e que cada um contribui com uma unidade de cada lado da expressão. O argumento para as outras potências e p é semelhante. Por fim, perceba que a soma é infinita pois eventualmente $n < p^i \implies \left\lfloor \frac{n}{p^i} \right\rfloor = 0$.

Exemplos Resolvidos.

Agora que já temos todas as ferramentas, veremos como aplicar essas técnicas em problemas olímpicos recentes. É recomendado tentar resolver sozinho (a) antes de ler as soluções.

Exemplo 1 (USEMO 2020). Quais inteiros positivos podem ser expressos da forma

$$\frac{\text{mmc}(x,y) + \text{mmc}(y,z)}{\text{mmc}(x,z)}$$

com x, y e z inteiros positivos?

Solução. Note que conseguimos formar todos os pares fazendo $(x, y, z) = (t, t^2, t)$ pois a expressão se torna $\frac{2t^2}{t} = 2t$. Agora provaremos que nenhum ímpar pode ser expresso dessa forma.

Sejam $a = v_2(x)$, $b = v_2(y)$ e $c = v_2(z)$ e N a expressão do enunciado. Pela definição do mínimo múltiplo comum, $v_2(\text{mmc}(p,q)) = \max(v_2(p), v_2(q))$. Usaremos intensamente a **Propriedade 3** de maneira implícita. Tente entender onde e como!

Temos então três casos.

- $a \leq b$ e $c \leq b$.

  O v_2 do numerador de N se torna pelo menos $v_2(2^b+2^b) = b+1$, enquanto o do denominador é $\max(a, c)$. Dessa forma, $v_2(N) \geq b+1-max(a,c) > 0 \implies N$ é par.

- $a \geq b$ e $c \geq b$.

  Se $a \neq c$, $v_2(N) = \min(a, c) - \max(a,c) < 0 \implies N \notin \mathbb{Z}$. Se $a = c$, v_2 do numerador é maior que $a = c$ e portanto $v_2(N) > a - a = 0 \implies N$ é par.

- Sem perda de generalidade, $a \leq b \leq c$.

  No numerador, temos algo maior ou igual à $\min(b, c)$. Já no denominador, temos c. Se $b < c$, há a igualdade de v_2 no numerador e, portanto, $v_2(N) = b - c < 0 \implies N \notin \mathbb{Z}$. Caso contrário, no numerador temos algo maior que $b = c$ e no denominador temos c. Consequentemente, N é par.

Dessa forma, concluímos que se N é inteiro, N é par, c.q.d.

Exemplo 2 (IMO 2019). Encontre todos os pares (k, n) de inteiros positivos tais que

$$k! = (2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1}).$$

Solução. Aqui, LE denota o lado esquerdo da equação e LD o lado direito. Começaremos analisando o v_2 dos dois lados da equação.

$$v_2(k!) = \sum_{i \geq 1} \left\lfloor \frac{k}{2^i} \right\rfloor < \sum_{i \geq 1} \frac{k}{2^i} = k \left(\frac{1}{2} + \frac{1}{4} + \dots \right) = k.$$

Temos também $v_2(2^n - 2^i) = i$ para todo $i = 1, 2, \dots, n-1$. Portanto $v_2(LD) = 1 + 2 + \dots + n - 1 = \frac{(n-1)n}{2}$. Assim concluímos que

$$k > v_2(LE) = v_2(LD) = \frac{(n-1)n}{2}.$$

Agora olharemos para o v_3. Note que queremos uma cota invertida entre k e n.

$$v_3(k!) = \sum_{i \geq 1} \left\lfloor \frac{k}{3^i} \right\rfloor \geq \frac{k-2}{3}.$$

Para calcularmos o v_3 do lado direito devemos tomar alguns cuidados. Note que $3 \mid 2^n - 2^i \iff n \equiv i \pmod 2$. Dividiremos então em dois casos.

- $n = 2t$.

  Olhemos para um fator de índice par: $2^n - 2^{2i} = 2^{2i}(2^{2(t-i)} - 1)$. Não podemos aplicar LTE diretamente, pois $3 \nmid 2 - 1$. Entretanto, $2^{2(t-i)} - 1 = 4^{t-i} - 1^{t-i}$ e $3 \mid 4 - 1 \implies v_3(4^{t-i} - 1) = v_3(3) + v_3(t-i)$.

  Somando tudo, temos

  $v_3(LE) = (1+1+\cdots+1) + v_3(t) + v_3(t-1) + \ldots v_3(1) = t + v_3(t!) < t + \frac{t}{2} = \frac{3n}{4}$.

- $n = 2t + 1$.

  Similarmente ao caso anterior, $2^{2t+1} - 2^{2i+1} = 2^{2i+1}(2^{2(t-i)} - 1) = 2^{2i+1}(4^{t-i} - 1)$. Portanto o v_3 de cada fator desse é $1 + v_3(t-i)$. Somando,

  $v_3(LD) = (1+1+\cdots+1) + v_3(t) + v_3(t-1) + \ldots v_3(1) = t + v_3(t!) < t + \frac{t}{2} = \frac{3(n-1)}{4}$.

Em ambos os casos, não passa de $\frac{3n}{4}$. Assim,

$$\frac{k-2}{3} \leq v_2(LE) = v_2(LD) < \frac{3n}{4}.$$

Então
$$\frac{9n}{4} + 2 > k > \frac{(n-1)n}{2} \implies 2n^2 - 11n - 8 < 0$$
que é falso para todo $n \geq 7$. Resta testar os casos pequenos.

- $(2^1 - 1) = 1! \implies$ (1,1) é solução.
- $3 \cdot 2 = 3! \implies (2, 3)$ é solução.
- $7 \cdot 6 \cdot 4$ não é um fatorial.
- $15 \cdot 14 \cdot 12 \cdot 8$ não é um fatorial.
- $31 \cdot 30 \cdot 28 \cdot 24 \cdot 16$ não é um fatorial.
- $63 \cdot 62 \cdot 60 \cdot 56 \cdot 48 \cdot 32$ não é um fatorial.

As únicas soluções são (1,1) e $(2, 3)$.

Expansão aos racionais.

Como talvez tenha notado, no **Exemplo 1**, não nos preocupamos com o fato de N ser inteiro ou não para analisarmos seu v_2. De fato, todas as propriedades que enunciamos valem para racionais, considerando que $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$, isto é, admitindo valores negativos ao v_p. Os exemplos a seguir ilustram isso.

Exemplo 3 (Teste Cone Sul 2023/Austria 2016). Sejam a, b e c inteiros positivos com $\text{mdc}(a,b,c) = 1$ e

$$\frac{ab}{c} + \frac{bc}{a} + \frac{ca}{b}$$

inteiro. Prove que abc é um quadrado perfeito.

Solução. A condição $\text{mdc}(a,b,c) = 1$ pode ser traduzida na notação de v_p como $\min(v_p(a), v_p(b), v_p(c)) = 0$.

Além disso, abc é um quadrado perfeito se, e somente se, $v_p(a) + v_p(b) + v_p(c)$ é par para todo primo p. Isso torna esse problema perfeito para usarmos as técnicas aprendidas.

Suponhamos por absurdo que abc não é um quadrado perfeito $\implies v_p(a) + v_p(b) + v_p(c) \equiv 1 \pmod 2$ para algum primo p. Como a expressão é simétrica, podemos supor, sem perda de generalidade, $v_p(a) \geq v_p(b) \geq v_p(c) \geq 0$ (todos são inteiros).

$$v_p\left(\frac{ab}{c}\right) = v_p(a) + v_p(b) - v_p(c) \geq v_p(a) + v_p(c) - v_p(c) \geq 0.$$

$$v_p\left(\frac{ca}{b}\right) = v_p(c) + v_p(a) - v_p(b) \geq v_p(c) + v_p(b) - v_p(b) \geq 0.$$

Então

$$v_p\left(\frac{ab}{c} + \frac{ca}{b}\right) \geq \min\left(v_p\left(\frac{ab}{c}\right), v_p\left(\frac{ca}{b}\right)\right) \geq 0.$$

Similarmente,

$$v_p\left(\frac{bc}{a} + \left(\frac{ab}{c} + \frac{ca}{b}\right)\right) \geq \min\left(v_p\left(\frac{bc}{a}\right), v_p\left(\frac{ab}{c} + \frac{ca}{b}\right)\right).$$

Se $v_p\left(\frac{bc}{a}\right) < 0$, ocorre a igualdade na desigualdade anterior e o v_p da expressão é negativo, ou seja, ela não é um número inteiro. Concluímos que $v_p\left(\frac{bc}{a}\right) \geq 0$.

Note agora que

$$v_p\left(\frac{bc}{a}\right) = v_p(b) + v_p(c) - v_p(a) \equiv v_p(a) + v_p(b) + v_p(c) \equiv 1 \pmod 2.$$

Por ser um inteiro não negativo e ímpar, temos $v_p(a) + v_p(c) - v_p(a) \geq v_p(b) + v_p(c) - v_p(a) \geq 1 \implies v_p(c) \geq 1$. Como $v_p(c)$ é o mínimo, chegamos numa contradição pois $\text{mdc}(a, b, c) = 1$. Assim, nossa suposição inicial era falsa e, de fato, abc é um quadrado perfeito.

Exemplo 4 (APMO 2017). Chamamos um número racional r de *poderoso* se ele pode ser expresso da forma $\dfrac{p^k}{q}$ com p e q inteiros positivos primos entre si e $k > 1$ inteiro. Sejam a, b e c racionais positivos tais que $abc = 1$. Suponha que existem inteiros positivos x, y e z tais que

$$a^x + b^y + c^z$$

é inteiro. Prove que a, b e c são poderosos.

Solução. $abc = 1 \iff v_p(a) + v_p(b) + v_p(c) = 0$ para todo primo p.

Um número r é poderoso se, e somente se, existe um inteiro $d > 1$ fixo tal que, para todo primo p que satisfaz $v_p(r) > 0$, $d \mid v_p(r)$.

Analisemos agora o fato de $a^x + b^y + c^z$ ser inteiro. Sem perda de generalidade, $v_p(a) \geq v_p(b) \geq v_p(c)$.

Se $v_p(c) \geq 0$, $v_p(a) = v_p(b) = v_p(c) = 0$ e podemos ignorar esse primo.

Considere então $v_p(c) < 0$. Se $v_p(b) \geq 0$, $v_p(a^x + b^y) \geq \min(xv_p(a), yv_p(b)) \geq 0$ e, ao somarmos esse número com c^z teremos $v_p((a^x + b^y) + c^z) = zv_p(c) < 0 \implies$ não é inteiro. Portanto $v_p(b) < 0$ e $v_p(a) > 0$ (por que?).

Além disso, se $v_p(b^y) \neq v_p(c^z)$, $v_p(b^y + c^z) < 0$, e daí $v_p(a^x + (b^y + c^z)) < 0$.

Logo $yv_p(b) = zv_p(c)$. Como queremos provar que um número fixo divide $v_p(a)$ (o único positivo), faz sentido buscarmos por divisores de $v_p(b) + v_p(c) = -v_p(a)$. Na expressão acima, não podemos afirmar que $y \mid v_p(c)$. Entretanto, $\frac{y}{\text{mdc}(y,z)} \mid v_p(c)$ e, analogamente, $\frac{z}{\text{mdc}(y,z)} \mid v_p(b)$. Temos então

$$\frac{v_p(b)}{\frac{z}{\text{mdc}(y,z)}} = \frac{v_p(c)}{\frac{y}{\text{mdc}(y,z)}} = \frac{v_p(b) + v_p(c)}{\frac{y+z}{\text{mdc}(y,z)}} \in \mathbb{Z},$$

o que implica que $\frac{y+z}{\text{mdc}(y,z)} \mid v_p(a)$. Como $\frac{y+z}{\text{mdc}(y,z)}$ não depende de p (é fixo), isso conclui a demonstração.

Problemas.

Os problemas estão aproximadamente em ordem de dificuldade. Entretanto, a dificuldade é muito relativa e que muitos deles são bem técnicos. Por isso, caso não consiga resolver um problema mesmo com as dicas da próxima seção, não deixe de tentar resolver os outros para consolidar o que aprendeu neste material.

Problema 1 (TM² 2019). Um inteiro positivo n é chamado de *bonitinho* quando existe um inteiro positivo m tal que $m!$ termina em exatamente n zeros na representação decimal.

a) Determine se 2019 é bonitinho.

b) Quantos inteiros positivos menores que 2019 são bonitinhos?

Problema 2 (APMO 2019). Seja m um inteiro positivo fixo. A sequência infinita $\{a_n\}_{n\geq 1}$ é definida da seguinte forma: a_1 é um inteiro positivo e, para todo inteiro $n \geq 1$,

$$a_{n+1} = \begin{cases} a_n^2 + 2^m & \text{se } a_n < 2^m \\ a_n/2 & \text{se } a_n \geq 2^m \end{cases}$$

Para cada m, determine todos os valores de a_1 tais que todo termo da sequência é um inteiro positivo.

Problema 3 (IMO 2018). Seja a_1, a_2, $\ldots$ uma sequência infinita de inteiros positivos. Suponha que existe um inteiro $N > 1$ tal que, para todo $n \geq N$, 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 inteiro. Prove que existe um inteiro positivo M tal que $a_m = a_{m+1}$ para todo $m \geq M$.

Problema 4 (IMO 2022). Encontre todas as triplas de inteiros positivos (a, b, p) tais que p é primo e

$$a^p = b! + p.$$

Problema 5 (ELMO 2017). Para cada inteiro $C > 1$, demonstre se existem ou não inteiros positivos a_1, a_2, $\ldots$, distintos dois a dois, tais que, para todo $k \geq 1$,

$$a_{k+1}^k \mid C^k a_1 a_2 \ldots a_k.$$

Problema 6 (IMO Shortlist 2021). Mostre que

$$n! = a^{n-1} + b^{n-1} + c^{n-1}$$

tem apenas finitas soluções nos inteiros positivos.

Dicas.

Problema 1. A quantidade de zeros na representação decimal de $m!$ é exatamente $v_5(m!)$.

Problema 2. Escreva $a_1 = 2^x y$ com $2 \nmid y$ e note o que acontece com y (parte ímpar) após cada operação.

Problema 3. Perceba que a diferença entre dois números consecutivos formados pela expressão também será inteira. Depois conclua que os fatores primos que dividem algum termo da sequência são finitos e brinque com v_ps usando o fato de que $v_p(a) = v_p(b)$ para todo primo p implica $a = b$.

Problema 4. Analise os casos em que $b < p$, $p \leq b < 2p$. Por que não é necessário $b \geq 2p$? Quando for conveniente, analise a expressão na forma $a^p - p = b!$ e utilize alguns LTEs e desigualdades das médias para cotar o tamanho dos números de cada lado.

Problema 5. Conjecture a resposta com casos pequenos. Depois, faça uma cota para $v_p(a_k)$ que lembre a média harmônica. Finalize com o princípio da casa dos pombos para algum k suficientemente grande.

Problema 6. Divida nos casos n ímpar (mais fácil) e n par. No caso par, faça estimativas para mostrar que $a + b \leq n$. Em seguida, analise o v_p das expressões $n! - c^{n-1}$ e $a^{n-1} + b^{n-1}$ para algum p ímpar que divide $a + b$. Conclua que $a + b$ é uma potência de 2, analise o v_2 e finalize o problema.

Referências.

`https://artofproblemsolving.com/`

Modern Olympiad Number Theory

Levanta o expoente, princesa, senão a valorização p-ádica cai! - Ana Paula Chaves

No Pain, No Brain - Levantamento de Expoentes - Davi Lopes