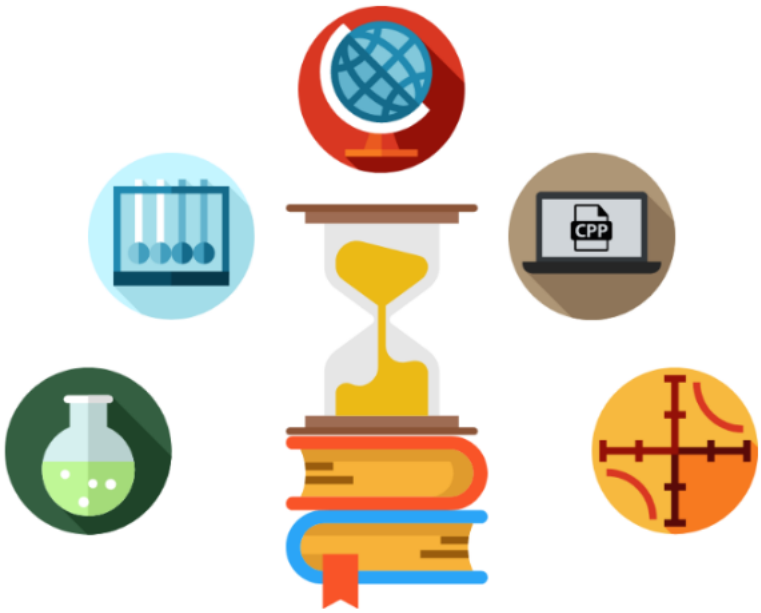
Valorização P-ádica

João Pedro de Almeida da Silva



1 Introdução

Esse material tem como objetivo o estudo dos expoentes máximos de um primo que divide um inteiro. Vamos começar a partir de novas definições que nos ajudarão a resolver problemas de teoria dos números.

2 Valorização p-ádica

2.1 Definição

Vamos definir como "V_p"de um certo $n \in \mathbb{Z}$ e p primo como o expoente da maior potência de p que divide n.

Ex.:

- $V_2(24) = 3$;
- $V_7(196) = 2$;
- $V_5(35) = 1$.

Para $n = 0$, dizemos que $V_p(0) = \infty$. Algo importante também é que, pelo teorema fundamental da aritmética, $n = p_1^{V_{p_1}(n)} p_2^{V_{p_2}(n)} ... p_k^{V_{p_k}(n)}$, então se dois inteiros positivos x, y são tais que $V_p(x) = V_p(y), \forall$ p primo, então $x = y$.

2.2 Propriedades de V_p

Considere x, y inteiros e p um primo. Abaixo, temos propriedades envolvendo x, y e p:

1°) Divisibilidade:

Temos que $x|y \Leftrightarrow V_p(x) \leq V_p(y)$.

2°) Produto:

Temos que $V_p(xy) = V_p(x) + V_p(y)$.

3°) Divisão:

Se $x|y$, então $V_p(\frac{y}{x}) = V_p(y) - V_p(x)$.

4°) Expoente:

Temos que $V_p(x^n) = nV_p(x)$, para n inteiro positivo.

5°) Soma:

Se $V_p(x) \neq V_p(y)$, então $V_p(x+y) = min\{V_p(x), V_p(y)\}$.

É interessante que antes de prosseguir, o leitor tente provar as propriedades. Abaixo, vemos como prová-las:

1°) Divisibilidade:

Suponha que $x|y$, com x,y inteiros, diferentes de 0, 1 ou -1. Veja que, se $V_p(x) > V_p(y)$, podemos escrever $x = p^{V_p(x)}x_0$ e $y = p^{V_p(y)}y_0$, então $p^{V_p(x)}x_0|p^{V_p(y)}y_0$, mas por $V_p(x) > V_p(y)$, então $p^{V_p(x)-V_p(y)}x_0|y_0$, onde $V_p(x) - V_p(y) > 0$, fazendo com que $p|y_0$, que é falso, pois y_0 são todos os fatores de y diferentes de p. Agora se $V_p(x) \leq V_p(y)$, para todo primo, podemos afirmar que $x|y$, pois se temos $2 = p_1 < p_2 < ...$ a sequência dos primos, $x = p_1^{V_{p_1}(x)}p_2^{V_{p_2}(x)}...$ e $y = p_1^{V_{p_1}(y)}p_2^{V_{p_2}(y)}...$, queremos $p_1^{V_{p_1}(x)}p_2^{V_{p_2}(x)}...|p_1^{V_{p_1}(y)}p_2^{V_{p_2}(y)}...$, mas por $V_p(x) \leq V_p(y)$, para todo primo, então $0 \leq V_p(y) - V_p(x)$, logo, queremos $1|p_1^{V_{p_1}(y)-V_{p_1}(x)}p_2^{V_{p_2}(y)-V_{p_2}(x)}...$, que é verdade, pois 1 divide qualquer número inteiro.

2°) Produto:

Para provar, basta fazer $x = p^{V_p(x)}x_0$ e $y = p^{V_p(y)}y_0$, pois assim, temos que $V_p(xy) = V_p(p^{V_p(x)}x_0p^{V_p(y)}y_0) = V_p(p^{V_p(x)+V_p(y)}x_0y_0) = V_p(x) + V_p(y)$, como queríamos.

3°) Divisão:

Usando que $x|y$, temos que $V_p(x) \leq V_p(y)$, $\forall$ p primo. Assim, como $x = p_1^{V_{p_1}(x)}p_2^{V_{p_2}(x)}...$ e $y = p_1^{V_{p_1}(y)}p_2^{V_{p_2}(y)}...$, para $2 = p_1 < p_2 < ...$ a sequência dos primos, temos que $V_p(\frac{y}{x}) = V_p(\frac{p_1^{V_{p_1}(y)}p_2^{V_{p_2}(y)}...}{p_1^{V_{p_1}(x)}p_2^{V_{p_2}(x)}...}) = V_p(p_1^{V_{p_1}(y)-V_{p_1}(x)}p_2^{V_{p_2}(y)-V_{p_2}(x)}...) = V_p(y) - V_p(x)$, $\forall$ p primo.

4°) Expoente:

Escrevendo $x = p^{V_p(x)}T$, temos que $V_p(x^n) = V_p((p^{V_p(x)}T)^n) = V_p(p^{V_p(x)n}T^n) = V_p(x)n$, como queríamos.

5°) Soma: Como $V_p(x) \neq V_p(y)$, sem perda de generalidade, assuma que $V_p(x) > V_p(y)$, fazendo com que $\min\{V_p(x), V_p(y)\} = V_p(y)$. Temos que $x = p^{V_p(x)}x_0$ e $y = p^{V_p(y)}y_0$, $V_p(x+y) = V_p(p^{V_p(x)}x_0 + p^{V_p(y)}y_0) = V_p(p^{V_p(y)}(y_0 + p^{V_p(x)-V_p(y)}x_0))$, como p não divide y_0, então p não divide $y_0 + p^{V_p(x)-V_p(y)}x_0$, fazendo com que $V_p(p^{V_p(y)}(y_0 + p^{V_p(x)-V_p(y)}x_0)) = V_p(p^{V_p(y)}) = V_p(y) = \min\{V_p(x), V_p(y)\} = V_p(y)$, como queríamos.

Problema 1. Quantos números n menores que 2024 são tais que, para todo p primo, se $p|n$, então p^2 divide n, mas p^3 não divide n.

Solução. Veja que, se $p|n$, então, pelo enunciado, $V_p(n) \geq 2$, mas também $V_p(n) < 3$, isso é, os n's que procuramos são os quadrados perfeitos que não tem nenhum primo com $V_p(n) \geq 4$. Para calcular a quantidade de números que satisfazem isso, vamos separar em alguns casos:

1°) Se n tem apenas um fator primo:

Temos que $n = p^2$, com p primo, e como $45^2 > 2024$, então todo $p < 45$ satisfaz, que são 13 primos.

2°) Se n tem dois fatores primos distintos:

Temos que $n = p^2q^2$, com p, q primos. Queremos $n < 45^2$, então precisamos que pq seja menor que 45, que ocorre quando $pq = 2\cdot3, 2\cdot5, 2\cdot7, 2\cdot11, 2\cdot13, 2\cdot17, 2\cdot19, 3\cdot5, 3\cdot7, 3\cdot11, 3\cdot13, 5\cdot7$, chegando em 12 soluções.

3°) Se n tem três fatores primos distintos:

Se um dos fatores é maior ou igual a 11, então $n \geq 11^2 3^2 2^2 = 66^2 > 45^2 > 2024$. Portanto, para esse caso, as únicas soluções são $n = 2^2 3^2 7^2$ e $2^2 3^2 5^2$, totalizando duas soluções.

4°) Se n tem quatro ou mais fatores primos distintos:

Veja que $n \geq 2^2 3^2 5^2 7^2 = 210^2 > 45^2 > 2024$, então n não pode ter quatro ou mais fatores primos distintos.

Logo, concluímos que a quantidade de n's é $13 + 12 + 2 = 27$.

2.3 Trabalhando com V_p em fatoriais

Vamos começar falando sobre a fórmula de Polignac:

Fórmula de Polignac:

Seja n um inteiro e p um primo. Temos que:

$V_p(n!) = \sum \left\lfloor \frac{n}{p^i} \right\rfloor = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$

Prova:

Para resolver, precisaremos do seguinte lema:

Lema 1. Sejam $k, n \in \mathbb{Z}_+^*$. A quantidade de múltiplos de k de 1 até n é dada por $\left\lfloor \frac{n}{k} \right\rfloor$.

A prova do lema fica a cargo do leitor. Veja que, a fórmula parece que soma os divisores de

$p, p^2, p^3, \ldots$ de 1 até n, e de fato, vamos mostrar que é isso que ela faz. Temos $V_p(n!) = V_p(1\cdot 2\cdot 3\ldots\cdot(n-1)\cdot n) = V_p(p\cdot 2p\cdot 3p\ldots\cdot(\lfloor\frac{n}{p}\rfloor p))$, que são todos os múltiplos de p menores ou iguais a n. Como todos tem um fator p, podemos escrever o produto $V_p(p\cdot 2p\cdot 3p\ldots\cdot(\lfloor\frac{n}{p}\rfloor p))$ como $V_p(1\cdot 2\cdot 3\ldots\cdot(\lfloor\frac{n}{p}\rfloor)) + \lfloor\frac{n}{p}\rfloor$. Agora, temos que os fatores p que sobraram em $V_p(1\cdot 2\cdot 3\ldots\cdot(\lfloor\frac{n}{p}\rfloor))$ foram apenas os de p^2 em $n!$, então temos $V_p(1\cdot 2\cdot 3\ldots\cdot(\lfloor\frac{n}{p}\rfloor)) + \lfloor\frac{n}{p}\rfloor = V_p(1\cdot 2\ldots\cdot\lfloor\frac{\lfloor\frac{n}{p}\rfloor}{p}\rfloor) + \lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor$. Podemos fazer tal passo infinitas vezes, de forma que chegamos exatamente na fórmula de Polignac que foi apresentada.

Problema 2. (OPEMAT/2021) Qual o dígito da posição 2020 de 8095! (Contando da direita para esquerda)?

Solução. Perceba que muitos dos algarismos da direira de 8095! são 0's, devido a grande quantidade de fatores 2 e 5. Para contar quantos 0's são, basta analisar o V_5, pois com certeza o fator 2 aparece mais que o 5 em 8095!. Assim, temos que $V_5(8095!) = \lfloor\frac{8095}{5}\rfloor + \lfloor\frac{8095}{25}\rfloor + \lfloor\frac{8095}{125}\rfloor + \lfloor\frac{8095}{625}\rfloor + \lfloor\frac{8095}{3125}\rfloor = 1619 + 323 + 64 + 12 + 2 = 2020$. Assim, o 2020 dígito é 0.

Problema 3. Seja $N = \frac{3995!}{995!}$. Ache a maior potência de 3 que divide N.

Solução. O problema se resume a achar $V_3(N)$. Temos que $V_3(N) = V_3(\frac{3995!}{995!}) = V_3(3995!) - V_3(995!)$. Utilizando Polignac, temos $V_3(3995!) - V_3(995!) = \lfloor\frac{3995}{3}\rfloor + \lfloor\frac{3995}{9}\rfloor + \lfloor\frac{3995}{27}\rfloor + \lfloor\frac{3995}{81}\rfloor + \lfloor\frac{3995}{243}\rfloor + \lfloor\frac{3995}{729}\rfloor + \lfloor\frac{3995}{2187}\rfloor - \lfloor\frac{995}{3}\rfloor - \lfloor\frac{995}{9}\rfloor - \lfloor\frac{995}{27}\rfloor - \lfloor\frac{995}{81}\rfloor - \lfloor\frac{995}{243}\rfloor - \lfloor\frac{995}{729}\rfloor = 1331 + 443 + 147 + 49 + 16 + 5 + 1 - 331 - 110 - 36 - 12 - 4 - 1 = 1498$. Logo, a maior potência de 3 que divide N é 3^{1498}.

Também existe uma outra fórmula que calcula o $V_p(n!)$:

Teorema:
Defina como $S_p(n)$ a soma dos algarismos de $n \in \mathbb{Z}_+^*$ na base p, com p primo. Temos que: $V_p(n!) = \frac{n - S_p(n)}{p-1}$.

Prova:

Na base p, temos que $n = (a_x a_{x-1}\ldots a_1 a_0)_p$, onde $0 \le a_i \le p-1$, $\forall\ i = 0,1,2,\ldots,x$. Por Polignac, sabemos que $V_p(n!) = \lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor + \lfloor\frac{n}{p^3}\rfloor + \ldots$, e como $n = a_x p^x + \ldots + a_1 p^1 + a_0$, temos $V_p(n!) = \lfloor\frac{a_x p^x + \ldots + a_1 p^1 + a_0}{p}\rfloor + \lfloor\frac{a_x p^x + \ldots + a_1 p^1 + a_0}{p^2}\rfloor + \lfloor\frac{a_x p^x + \ldots + a_1 p^1 + a_0}{p^3}\rfloor + \ldots$, onde podemos escrever como $(a_x p^{x-1} + \ldots + a_1 p^0 + \lfloor\frac{a_0}{p}\rfloor) + (a_x p^{x-2} + \ldots + a_2 p^0 + \lfloor\frac{a_1 p^1 + a_0}{p^2}\rfloor) + (a_x p^{x-3} + \ldots + a_3 p^0 + \lfloor\frac{a_2 p^2 + a_1 p^1 + a_0}{p^3}\rfloor) + \ldots$. Perceba que toda parte que tem $\frac{a_i p^i + a_{i-1} p^{i-1} + \ldots + a_0}{p^{i+1}}$, para $i = 0,1,2,\ldots$, é 0, pois o valor máximo que pode assumir é quando $a_i = a_{i-1} = \ldots = a_1 = a_0 = p-1$, que ainda assim é tal que $(p-1)(p^i + \ldots + p^0) = p^{i+1} - 1 \le p^{i+1}$. Logo, temos que $V_p(n!) = \lfloor\frac{a_x p^x + \ldots + a_1 p^1 + a_0}{p}\rfloor + \lfloor\frac{a_x p^x + \ldots + a_1 p^1 + a_0}{p^2}\rfloor + \lfloor\frac{a_x p^x + \ldots + a_1 p^1 + a_0}{p^3}\rfloor + \ldots =$

$(a_x p^{x-1}+...+a_1 p^0+\lfloor \frac{a_0}{p} \rfloor)+(a_x p^{x-2}+...+a_2 p^0+\lfloor \frac{a_1 p^1+a_0}{p^2} \rfloor)+(a_x p^{x-3}+...+a_3 p^0+\lfloor \frac{a_2 p^2+a_1 p^1+a_0}{p^3} \rfloor)+... =$ $(a_x p^{x-1}+...+a_1 p^0)+(a_x p^{x-2}+...+a_2 p^0)+(a_x p^{x-3}+...+a_3 p^0)+...$, que pondo os a_i's em evidência, temos $a_x(p^{x-1}+p^{x-2}+...+p^1+p^0)+a_{x-1}(p^{x-2}+...+p^0)+...+a_2(p^1+p^0)+a_1 = a_x(\frac{p^x-1}{p-1})+a_{x-1}(\frac{p^{x-1}-1}{p-1})+...+a_2(\frac{p^2-1}{p-1})+a_1(\frac{p-1}{p-1}) = \frac{(a_x p^x+...+a_1 p+a_0)-(a_x+...+a_1+a_0)}{p-1} = \frac{n-S_p(n)}{p-1}$, como queríamos.

Problema 4. Prove que $V_p(\binom{n}{k})$ é $\frac{S_p(k)+S_p(n-k)-S_p(n)}{p-1}$, com $n,k \in \mathbb{Z}_+^*$ e p primo.

Solução. Veja que $V_p(\binom{n}{k}) = V_p(\frac{n!}{k!(n-k)!}) = V_p(n!)-V_p(k!)-V_p((n-k)!) = \frac{n-S_p(n)}{p-1}-\frac{k-S_p(k)}{p-1}-\frac{(n-k)-S_p(n-k)}{p-1} = \frac{S_p(k)+S_p(n-k)-S_p(n)}{p-1}$, chegando no desejado.

Problema 5. Ache todos os n's ,$n \in \mathbb{Z}_+^*$, tal que $2^{n-1}|n!$.

Solução. Queremos achar os n's tal que $V_2(2^{n-1}) \leq V_2(n!)$, isso é, $n-1 \leq n-S_2(n)$, então precisamos $S_2(n) \leq 1$. Mas, veja que $1 \leq S_2(n)$, pois é necessário que n tenha pelo menos um algarismo na base 2, assumindo que ele seja diferente de 0. Assim, queremos que $1 \leq S_2(n) \leq 1$, ou seja, $S_2(n) = 1$, que ocorre apenas quando n é uma potência de 2. Vamos conferir se $2^{n-1}|n!$ quando $n = 2^r$, com $r \in \mathbb{Z}_+^*$. Precisamos que $2^{2^r-1}|2^r!$, que de fato ocorre, pois $2^r-1 \leq 2^r-S_2(2^r) = 2^r-1$.

3 Lifting The Exponent (LTE)

Nesse seção, veremos um pouco sobre levantamentos no expoente, o famoso "LTE", e alguns problemas que ficam muito mais fáceis com sua aplicação.

Lema do levantemento do expoente/LTE:
Sejam a,b inteiros, $p>2$ primo e n um inteiro positivo. Temos as seguintes propriedades:

- Se a,b são coprimos com p e $p|a-b$, então $V_p(a^n-b^n) = V_p(a-b)+V_p(n)$;
- Se a,b são coprimos com p, n é ímpar e $p|a+b$, então $V_p(a^n+b^n) = V_p(a+b)+V_p(n)$.

Prova: Vamos começar provando a primeira propriedade do LTE. Escreva n como $p^{V_p(n)}T$. Vamos fazer um prova por indução no $V_p(n)$.

1°) Caso inicial:
Se $V_p(n) = 0$, basta ver que $a^n-b^n = (a-b)(a^{n-1}+...+b^{n-1})$, e como $a \equiv b\ mod.p$, então $(a^{n-1}+...+b^{n-1}) \equiv a^{n-1}+a^{n-1}+...+a^{n-1} \equiv na^{n-1}\ mod.p$, que não é congruente a 0 $mod.p$, então $V_p((a^{n-1}+$

$\ldots + b^{n-1})) = 0$, fazendo com que $V_p(a^n - b^n) = V_p((a-b)(a^{n-1} + \ldots + b^{n-1})) = V_p(a-b) + 0 = V_p(a-b) + V_p(n)$, concluindo o caso inicial.

2°) Hipótese de indução:

Assuma válido para $V_p(n) = x$ que $V_p(a^n - b^n) = V_p(a-b) + V_p(n)$ e tentaremos mostrar que se $V_p(n) = x+1$, então $V_p(a^{np} - b^{np}) = V_p(a-b) + V_p(n) + 1$.

3°) Passo indutivo:

Temos que $a^n - b^n = (a^{xT})^p - (b^{xT})^p = (a^{xT} - b^{xT})((a^{xT})^{p-1} + \ldots + (b^{xT})^{p-1})$, mas, pela hipótese, $V_p(a^{xT} - b^{xT}) = V_p(a-b) + V_p(n)$, então precisamos mostrar que $V_p(((a^{xT})^{p-1} + \ldots + (b^{xT})^{p-1})) = 1$. Primeiro, veja que p divide, pois como $a \equiv b \; mod.p$, então $(a^{xT})^{p-1} + \ldots + (b^{xT})^{p-1} \equiv 1+1+1+\ldots+1 \equiv p \; mod.p$. Assim, basta mostrar que p^2 não divide $((a^{xT})^{p-1} + \ldots + (b^{xT})^{p-1})$. Como $a \equiv b \; mod.p$, então $a^{xT} \equiv b^{xT} \; mod.p$, então podemos escrever a^{xT} como $pr + b^{xT}$, para algum $r \in \mathbb{Z}$. Pegando cada termo separadamente, temos $(a^{xT})^{p-1-k}(b^{xT})^k \equiv (pr + b^{xT})^{p-1-k}(b^{xT})^k \; mod.p^2$, que ao fazer o binômio de newton em $(pr + b^{xT})^{p-1-k}(b^{xT})^k$, concluimos que $(pr + b^{xT})^{p-1-k}(b^{xT})^k \equiv (krp + b^{xT})(b^{xT})^{p-2} \; mod.p^2$. Portanto, temos que $((a^{xT})^{p-1} + \ldots + (b^{xT})^{p-1}) \equiv ((p-1)rp + b^{xT})(b^{xT})^{p-2} + ((p-2)rp + b^{xT})(b^{xT})^{p-2} + \ldots + (1rp + b^{xT})(b^{xT})^{p-2} + (b^{xT})(b^{xT})^{p-2} \equiv ((\frac{(p-1)p}{2})pr(b^{xT})^{p-2}) + p(b^{xT})^{p-1} \; mod.p^2$, e como $p^2 | (\frac{(p-1)}{2})p^2 r(b^{xT})^{p-2})$, então $((\frac{(p-1)p}{2})pr(b^{xT})^{p-2}) + p(b^{xT})^{p-1} \equiv p(b^{xT})^{p-1} \; mod.p^2$, que, como p não divide b, então p^2 não divide $p(b^{xT})^{p-1}$. Logo, provamos que p^2 não divide $((a^{xT})^{p-1} + \ldots + (b^{xT})^{p-1})$, mas p divide, concluindo nossa passo indutivo e, consequentemente, a nossa indução.

A segunda propriedade fica a cargo do leitor, dado que a prova é análoga a que fizemos com indução.

Perceba que trabalhamos apenas com $p > 2$, mas o que acontece se $p = 2$?

Abaixo, temos 3 casos do LTE para $p = 2$:

Lema do levantamento do expoente para $p = 2$:

Sejam a, b inteiros ímpares e n um inteiro positivo. Temos as seguintes propriedades:

- Se n é ímpar e $2 | a-b$, então $V_2(a^n - b^n) = V_2(a-b)$;
- Se n é ímpar e $2 | a+b$, então $V_2(a^n + b^n) = V_2(a+b)$;
- Se n é par e $2 | a-b$, então $V_2(a^n - b^n) = V_2(a+b) + V_2(a-b) + V_2(n) - 1$.

Prova: Para os dois primeiros casos, basta fatorar, pois $a^n - b^n = (a-b)(a^{n-1} + \ldots + b^{n-1})$, mas por n ser ímpar, $(a^{n-1} + \ldots + b^{n-1})$ é ímpar, então $V_2(a^n - b^n) = V_2((a-b)(a^{n-1} + \ldots + b^{n-1})) = V_2(a-b)$. Também, $V_2(a^n + b^n) = V_2((a+b)(a^{n-1} - \ldots + b^{n-1})) = V_2(a+b)$.

Agora, vamos provar que para n par e $2 | a-b$, então $V_2(a^n - b^n) = V_2(a-b) + V_2(a+b) + V_2(n) - 1$.

Escreva n como $2^k I$, onde $k = V_2(n)$. Temos que $a^n - b^n = a^{2^k I} - b^{2^k I} = (a^I)^{2^k} - (b^I)^{2^k}$, então, fazendo diferença de dois quadrados, teremos $(a^I)^{2^k} - (b^I)^{2^k} = (a^{2^{k-1}I} + b^{2^{k-1}I})(a^{2^{k-2}I} + b^{2^{k-2}I})...(a^{2^1 I} + b^{2^1 I})(a^{2^0 I} + b^{2^0 I})(a^I - b^I)$. Veja que, já sabemos $V_2((a^I - b^I)(a^I + b^I))$, pois $V_2((a^I - b^I)(a^I + b^I)) = V_2((a^I - b^I)) + V_2((a^I + b^I)) = V_2(a-b) + V_2(a+b)$, pelas propriedades já provadas acima. Também, como x^2 deixa resto 1 por 4 quando x é ímpar, então $V_2(a^{2^i I} + b^{2^i I}) = 1$, para $i > 0$. Logo, $V_2((a^I)^{2^k} - (b^I)^{2^k}) = V_2((a^{2^{k-1}I} + b^{2^{k-1}I})(a^{2^{k-2}I} + b^{2^{k-2}I})...(a^{2^1 I} + b^{2^1 I})(a^{2^0 I} + b^{2^0 I})(a^I - b^I)) = V_2((a^{2^{k-1}I} + b^{2^{k-1}I})) + V_2((a^{2^{k-2}I} + b^{2^{k-2}I})) + ... + V_2((a^I + b^I)) + V_2(a^I - b^I) = 1 + 1 + ... + 1 + V_2(a+b) + V_2(a-b) = k - 1 + V_2(a+b) + V_2(a-b) = V_2(n) - 1 + V_2(a+b) + V_2(a-b)$, como queríamos demonstrar.

4 Problemas propostos

Problema 1. Prove que $\forall$ inteiro $n > 0$, $\frac{1}{n+1}\binom{2n}{n}$ é inteiro.

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

Problema 3. (TST Cone Sul/2013) Um inteiro positivo b é dito *maroto* se para todo inteiro positivo a, tal que $b^2 | a^5$, então $b | a^2$. Determine a quantidade de inteiros positivos *maroto* menores que 2013.

Problema 4. (IMO/1990) Determine todos os inteiros positivos n tal que $n^2 | 2^n + 1$.

Problema 5. Ache o menor inteiro positivo n tal que 3^{2024} é um divisor de $(n+1)(n+2)(n+3)...3n$.

Problema 6. (IMO Shortlist/2007) Sejam $b, n > 1$ inteiros. Suponha que para cada $k > 1$, $k \in \mathbb{Z}$, existe um inteiro a_k tal que $k | b - a_k^n$. Prove que $b = A^n$, para algum A inteiro.

Problema 7. (IMO/1999) Ache todos os pares de inteiros positivos (x, p) tal que p é um primo, $x \leq 2p$, e $x^{p-1} | (p-1)^x + 1$.

Problema 8. Determine os pares de inteiros positivos (m, n) tais que $(n-1)! + 1 = n^m$.

Problema 9. (TST Cone Sul/2024) Para inteiros positivos $n, k > 1$, defina $E_k(n)$ como o maior expoente r tal que k^r divide $n!$. Por exemplo, $E_9(12) = E_{10}(12) = 2$. Prove que existem infinitos n tais

que $E_{10}(n) > E_9(n)$ e infinitos m tais que $E_{10}(m) < E_9(m)$.

Problema 10. (TST Cone Sul/2023) Sejam a, b, c inteiros positivos com $mdc(a,b,c) = 1$ e $\frac{ab}{c} + \frac{bc}{a} + \frac{ac}{c}$ é inteiro. Prove que abc é quadrado perfeito.

Problema 11. (IMO Shortlist/2014) Ache todos os primos p e inteiros positivos (x,y) tais que $x^{p-1} + y$ e $y^{p-1} + x$ são ambos potências de p.

Problema 12. (CIIM/2014) Seja n um inteiro positivo e $p > 2$ um primo. Prove que: $n!(p-1)^n | (p^n - 1)(p^n - p)...(p^n - p^{n-1})$.

Problema 13. (China TST/2009) Sejam $a > b > 1$ inteiros positivos, com b ímpar e n um inteiro positivo. Se $b^n | a^n - 1$, mostre que $a^b > \frac{3^n}{n}$.

Bibliografia.

1. Modern olympiad number theory
(MONT)

2. Art of problem solving
(AOPS)

3. No pain, no brain-23° Semana Olímpica/Davi Lopes

4. Levanta o expoente, princesa, senão a valorização p-ádica cai!-24° Semana Olímpica/Ana Paula Chaves