No Pain, No Brain - Levantamento de Expoentes

23ª Semana Olímpica – Natal, RN

Prof. Davi Lopes – Nível 2

1. Introdução

Muitos problemas olímpicos de Teoria dos Números envolvem fatores primos de determinadas expressões, e fazer tal decomposição pode ser uma tarefa bem trabalhosa e árdua. Nesse material, veremos algumas técnicas que permitem facilitar e muito nosso trabalho nessas questões. Porém, é muito importante que você leia as demonstrações dos resultados mostrados aqui, e entenda bem os artifícios usados, uma vez que a sistemática delas é bem parecida com a sistemática de muitos problemas de olimpíada sobre o tema.

Pode ser que esse processo seja um tanto duro, e que o leitor se sinta tentado a apenas aplicar as fórmulas, mas é como os marombeiros da matemática dizem: No Pain, no Brain (na verdade eles não dizem isso não, eu acabei de inventar isso! kkkkk). Vamos erguer nossa cabeça, levantar nosso astral, e encarar essas demonstrações pesadas, para que os exercícios fiquem bem leves e que nosso monstrão matemático saia da jaula. Birl!

No que segue, para cada número real x, denotamos $\lfloor x \rfloor$ como a parte inteira de x, ou seja, o maior inteiro menor ou igual a x (por exemplo, $\lfloor 5{,}67 \rfloor = 5, \lfloor \pi \rfloor = 3, \lfloor 4 \rfloor = 4, \lfloor -2 \rfloor = -2$ e $\lfloor -4{,}5 \rfloor = -5$), e para cada inteiro positivo n, e cada número primo p, denotamos $v_p(n)$ como sendo o maior expoente t tal que p^t divide n (por exemplo, $v_2(2^4.3^8) = 4$, $v_3(2^4.3^8) = 4$ e $v_5(2^4.3^8) = 0$).

2. Levantando Expoentes em Fatoriais

A primeira fórmula que veremos aqui é uma ferramenta excelente para lidar com fatoriais e binomiais. Vamos conhece-la?

Fórmula de Polignac: Seja n um inteiro positivo e p um número primo. Então:

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Onde calculamos a soma até o ponto onde as parcelas são iguais a zero.

Demonstração: A prova da fórmula é, essencialmente, uma contagem. Para tanto, precisamos saber quantos múltiplos de certo número existem num determinado intervalo. Ou seja:

Lema: Dados inteiros positivos a e b, existem $\left\lfloor \frac{a}{b} \right\rfloor$ múltiplos de b dentre os números de 1 até a.

Prova: Fazendo a divisão euclidiana de a por b, existe um inteiro não negativo q e um inteiro $0 \leq r < b$ tal que $a = qb + r$. Assim, os múltiplos de b de 1 até a são $b, 2b, \dots, qb$, ou seja, q números ao todo. Como $0 \leq \frac{r}{b} < 1$, temos $\frac{a}{b} = \frac{qb+r}{b} = q + \frac{r}{b}$, donde $q \leq \frac{a}{b} < q + 1$, ou seja, $q = \left\lfloor \frac{a}{b} \right\rfloor$, finalizando a demonstração do lema.

Agora, vamos à demonstração da fórmula. A ideia aqui é contar quantos números, de 1 a n, possuem expoente p^1, p^2, etc, em sua fatoração em primos, pois $v_p(n!)$ nada mais é do que a soma de todos esses expoentes.

Observe que, para α inteiro positivo, a quantidade de inteiros positivos de 1 a n que possuem p^α na sua fatoração em primos, é $\left\lfloor \frac{n}{p^\alpha} \right\rfloor - \left\lfloor \frac{n}{p^{\alpha+1}} \right\rfloor$, pois $\left\lfloor \frac{n}{p^\alpha} \right\rfloor$ é a quantidade de múltiplos de p^α dentre os números 1 até n. Porém, devemos descontar os múltiplos de $p^{\alpha+1}$, pois os expoentes em p deles são maiores que α, logo não devem ser contados, e por isso subtraímos $\left\lfloor \frac{n}{p^{\alpha+1}} \right\rfloor$. Portanto:

$$v_p(n!) = 1.\left(\left\lfloor \frac{n}{p^1} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor\right) + 2.\left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor\right) + 3.\left(\left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^4} \right\rfloor\right) + \cdots =$$

$$= \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor (2-1) + \left\lfloor \frac{n}{p^3} \right\rfloor (3-2) + \left\lfloor \frac{n}{p^4} \right\rfloor (4-3) + \cdots = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Finalizando a demonstração ■

Um exemplo onde podemos aplicar essa fórmula é a questão 4 do primeiro TM^2.

Exemplo 1 (TM²/2019): Um inteiro positivo n é chamado bonitinho quando existe um inteiro positivo m tal que $m!$ termina em exatamente n zeros.

(a) Determine se 2019 é bonitinho.

(b) Quantos inteiros positivos menores que 2019 são bonitinhos?

Solução: (a) Note que a quantidade de zeros na representação decimal em $m!$ é exatamente $v_5(m!)$ (demonstre isso!), de modo que 2019 é bonitinho se, e somente se, existe um inteiro positivo m tal que:

$$\left\lfloor \frac{m}{5} \right\rfloor + \left\lfloor \frac{m}{25} \right\rfloor + \left\lfloor \frac{m}{125} \right\rfloor + \cdots = 2019$$

Vamos tentar um chute inicial, ignorando a parte inteira. È verdade, não podemos simplesmente tirar essa parte inteira, mas fazemos isso para ter uma ideia de quem é, aproximadamente o número m.

$$2019 = \frac{m}{5} + \frac{m}{25} + \frac{m}{125} + \frac{m}{625} + \frac{m}{3125}$$

Não olhamos a próxima potência de 5, pois se $m \geq 5^6$, então $\frac{m}{5} \geq 5^5 = 3125 > 2019$. Daí:

$$2019 = \frac{781m}{3125} \Rightarrow m = \frac{2019.3125}{781} = 8078{,}585\ldots$$

Como as partes inteiras são menores ou iguais que as frações, temos que testar inteiros positivos maiores ou iguais a $8078{,}585\ldots$, ou seja, vamos testar $m \geq 8079$.

$$\left\lfloor\frac{8079}{5}\right\rfloor + \left\lfloor\frac{8079}{25}\right\rfloor + \left\lfloor\frac{8079}{125}\right\rfloor + \left\lfloor\frac{8079}{625}\right\rfloor + \left\lfloor\frac{8079}{3125}\right\rfloor = 1615 + 323 + 64 + 12 + 2 = 2016$$

Perto! Será que vamos ter que subir o valor de m um a um? Não! Na verdade, basta variar m nos múltiplos de 5, pois são apenas nos múltiplos de 5 que $v_5(m!)$ vai aumentar. Vamos testar $m = 8080{,}8085{,}8090, \ldots$

$$\left\lfloor\frac{8080}{5}\right\rfloor + \left\lfloor\frac{8080}{25}\right\rfloor + \left\lfloor\frac{8080}{125}\right\rfloor + \left\lfloor\frac{8080}{625}\right\rfloor + \left\lfloor\frac{8080}{3125}\right\rfloor = 1616 + 323 + 64 + 12 + 2 = 2017$$

$$\left\lfloor\frac{8085}{5}\right\rfloor + \left\lfloor\frac{8085}{25}\right\rfloor + \left\lfloor\frac{8085}{125}\right\rfloor + \left\lfloor\frac{8085}{625}\right\rfloor + \left\lfloor\frac{8085}{3125}\right\rfloor = 1617 + 323 + 64 + 12 + 2 = 2018$$

$$\left\lfloor\frac{8090}{5}\right\rfloor + \left\lfloor\frac{8090}{25}\right\rfloor + \left\lfloor\frac{8090}{125}\right\rfloor + \left\lfloor\frac{8090}{625}\right\rfloor + \left\lfloor\frac{8090}{3125}\right\rfloor = 1618 + 323 + 64 + 12 + 2 = 2019$$

Assim, 2019 é bonitinho. Note que a conta parece gingante, mas uma vez que a gente fez a conta inicial, a coisa não fica tão difícil a partir daí, pois para mudar as partes inteiras com denominador 25, 125, etc, m deveria ser múltiplo de 25, o que não foi o caso nos testes. Por isso, só mudamos a parte inteira com denominador 5, de um em um.

(b) Observe que, para cada número bonitinho n, existem exatamente 5 inteiros positivos m tais que $v_5(m!) = n$: $5k, 5k+1, 5k+2, 5k+3, 5k+4$, onde k é um inteiro positivo tal que $5k$ é o primeiro múltiplo de 5 tal que $v_5\big((5k)!\big) = n$. Logo, se x é o número de números bonitinhos entre 1 e 2018, $5x = 8089 - 5 + 1$, pois dentre $5!, 6!, \ldots, 8089!$, cada número bonitinho aparece 5 vezes (não contamos $8090!$, pois ele tem 2019 zeros, por (a)). Logo, $x = 1617$ é a quantidade pedida de números bonitinhos ■

Estudar os expoentes em p é uma tarefa que é possível fazer não apenas em fatoriais, mas em binômias também.

Teorema de Kummer: se p é um primo, então $v_p\left(\binom{n}{k}\right)$ é igual ao número de "vai uns", na representação da base p, da soma $k + (n-k)$.

Demonstração: Para demonstrar esse teorema, vamos demonstrar primeiro uma versão alternativa da Fórmula de Polignac.

Lema:

$$v_p(n!) = \frac{n - s_p(n)}{p-1}$$

Onde $s_p(n)$ é a soma dos algarismos de n, quando escrito na base p.

Prova do Lema: Escreva n na base p como $n = (c_x c_{x-1} \dots c_2 c_1)_p$, onde os algarismos $c_1, c_2, \dots, c_x$ são tais que $0 \leq c_i \leq p-1$, para todo $i = 1,2, \dots, x$. Assim, se $\theta \geq x$ é um inteiro positivo, temos:

$$n = c_x p^{x-1} + c_{x-1} p^{x-2} + \cdots + c_2 p + c_1 \leq$$

$$\leq (p-1)p^{x-1} + (p-1)p^{x-2} + \cdots + (p-1)p + (p-1) =$$

$$= (p^x - p^{x-1}) + (p^{x-1} - p^{x-2}) + \cdots + (p^2 - p) + (p-1) = p^x - 1 < p^x \leq p^\theta$$

Logo, $n < p^\theta$, donde $\left\lfloor \frac{n}{p^\theta} \right\rfloor = 0$. Agora, para $\theta < x$, temos:

$$\frac{n}{p^\theta} = \frac{c_x p^{x-1} + c_{x-1} p^{x-2} + \cdots + c_2 p + c_1}{p^\theta} =$$

$$c_x p^{x-1-\theta} + \cdots + c_{\theta+2} p + c_{\theta+1} + \frac{c_\theta p^{\theta-1} + c_{\theta-1} p^{\theta-2} + \cdots + c_2 p + c_1}{p^\theta}$$

De modo semelhante ao que fizemos antes, pode-se provar que:

$$c_\theta p^{\theta-1} + c_{\theta-1} p^{\theta-2} + \cdots + c_2 p + c_1 < p^\theta \Rightarrow$$

$$\Rightarrow 0 \leq \frac{c_\theta p^{\theta-1} + c_{\theta-1} p^{\theta-2} + \cdots + c_2 p + c_1}{p^\theta} < 1$$

E daí $\left\lfloor \frac{n}{p^\theta} \right\rfloor = c_x p^{x-1-\theta} + \cdots + c_{\theta+2} p + c_{\theta+1}$. Portanto, pela fórmula de Polignac:

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^{x-1}} \right\rfloor =$$

$$= (c_x p^{x-2} + \cdots + c_3 p + c_2) + (c_x p^{x-3} + \cdots + c_4 p + c_3) + \cdots + (c_x) =$$

$$= c_x(p^{x-2} + \cdots + p + 1) + c_{x-1}(p^{x-3} + \cdots + p + 1) + \cdots + c_3(p+1) + c_2$$

Usando que $p^m + p^{m-1} + \cdots + p + 1 = \frac{p^{m+1}-1}{p-1}$ (soma dos termos de uma PG), temos:

$$v_p(n!) = c_x \left(\frac{p^{x-1} - 1}{p-1} \right) + c_{x-1} \left(\frac{p^{x-2} - 1}{p-1} \right) + \cdots + c_2 \left(\frac{p-1}{p-1} \right) + c_1 \left(\frac{1-1}{p-1} \right) =$$

$$= \frac{(c_x p^{x-1} + c_{x-1}p^{x-2} + \cdots + c_2 p + c_1) - (c_x + c_{x-1} + \cdots + c_2 + c_1)}{p-1} = \frac{n - s_p(n)}{p-1}$$

E o lema está demonstrado.

Agora estamos prontos para demonstrar nosso teorema. Pelo lema, temos que:

$$v_p\left(\binom{n}{k}\right) = v_p\left(\frac{n!}{k!\,(n-k)!}\right) = v_p(n!) - v_p(k!) - v_p\big((n-k)!\big) =$$

$$= \frac{n - s_p(n)}{p-1} - \frac{k - s_p(k)}{p-1} - \frac{(n-k) - s_p(n-k)}{p-1} = \frac{s_p(k) + s_p(n-k) - s_p(n)}{p-1}$$

Agora, vamos olhar a soma, na base p, a soma $k + (n-k)$, algarismo a algarismo. Escrevendo os números $k = (a_x a_{x-1} \ldots a_2 a_1)_p$, $n-k = (b_x b_{x-1} \ldots b_2 b_1)_p$, $n = (c_x c_{x-1} \ldots c_2 c_1)_p$ na base p, de modo que todos eles possuam a mesma quantidade de algarismos (possivelmente com zeros à esquerda). Para $i = 1,2,\ldots,x$, seja $\varepsilon_i = 1$, se há um vai-um na i −ésima posição, e 0, caso contrário. Logo, podemos representar a soma $k + (n-k)$ na base p assim:

$$\begin{array}{cccccc} (\varepsilon_x) & (\varepsilon_{x-1}) & (\varepsilon_{x-2}) & \ldots & (\varepsilon_1) & \\ a_x & a_{x-1} & \cdots & a_2 & a_1 & \\ b_x & b_{x-1} & \cdots & b_2 & b_1 & \oplus \\ \hline c_x & c_{x-1} & \ldots & c_2 & c_1 & \end{array}$$

Daí, note que $a_1 + b_1 = c_1$, se não há vai-um, e $c_1 + p$, se há vai-um na primeira posição, podemos dizer que $a_1 + b_1 = c_1 + \varepsilon_1 p$. De modo semelhante, $\varepsilon_1 + a_2 + b_2 = c_2$, se não há vai-um, e $c_2 + p$, se há vai-um na segunda posição, podemos dizer que $\varepsilon_1 + a_2 + b_2 = c_2 + \varepsilon_2 p$. Continuando assim, temos:

$$a_1 + b_1 = c_1 + \varepsilon_1 p$$

$$\varepsilon_1 + a_2 + b_2 = c_2 + \varepsilon_2 p$$

$$\varepsilon_2 + a_3 + b_3 = c_3 + \varepsilon_3 p$$

...

$$\varepsilon_{x-2} + a_{x-1} + b_{x-1} = c_{x-1} + \varepsilon_{x-1} p$$

$$\varepsilon_{x-1} + a_x + b_x = c_x$$

Onde na última igualdade usamos que $\varepsilon_x = 0$. Somando membro a membro:

$$(\varepsilon_1 + \cdots + \varepsilon_{x-1}) + (a_1 + \cdots + a_x) + (b_1 + \cdots + b_x) = (c_1 + \cdots + c_x) + (\varepsilon_1 + \cdots + \varepsilon_{x-1})p$$

Como $\varepsilon_1 + \cdots + \varepsilon_{x-1} = T$ é a quantidade de vai-uns na soma $k + (n-k)$ na base p, e além disso, $a_1 + \cdots + a_x = s_p(k)$, $b_1 + \cdots + b_x = s_p(n-k)$, $c_1 + \cdots + c_x = s_p(n)$, vem:

$$T + s_p(k) + s_p(n-k) = s_p(n) + Tp \Rightarrow \frac{s_p(k) + s_p(n-k) - s_p(n)}{p-1} = T$$

E assim o Teorema de Kummer está demonstrado ■

Que tal vermos uma aplicaçãozinha básica desse teorema?

Exemplo 2: Determine todos os inteiros positivos n tais que $\binom{2n}{n}$ é múltiplo de 4.

Solução: Pelo Teorema de Kummer, $v_2\left(\binom{2n}{n}\right)$ é o número de vai-uns na soma $n + n$. Observe que, nessa soma, a quantidade de vai-uns é exatamente a quantidade de 1's na representação binária de n (prove isso!), de modo que $v_2\left(\binom{2n}{n}\right) \geq 2$ (ou seja, $\binom{2n}{n}$ é múltiplo de 4) se, e somente se, n tem pelo menos 2 algarismos 1 na base binária, ou seja, n não é uma potência de 2. Portanto, $\binom{2n}{n}$ é múltiplo de 4 se, e somente se, n não é uma potência de 2 ■

3. Lifting The Exponent Lemma (Vulgo LTE)

A seguir, veremos um dos resultados mais importantes sobre levantamentos de expoentes em Teoria dos Números, e que possui muitos problemas na qual sua aplicação facilita imensamente a solução deles. Vejamos o:

Lema do Levantamento do Expoente – LTE: Seja p um primo e a, b inteiros distintos, nenhum dos quais é divisível por p. Seja ainda n um inteiro positivo.

(i) Se p é ímpar e $p|a-b$, então $v_p(a^n - b^n) = v_p(a-b) + v_p(n)$.
(ii) Se p é ímpar, n é ímpar e $p|a+b$, então $v_p(a^n + b^n) = v_p(a+b) + v_p(n)$.
(iii)Se $p = 2$, n é ímpar e $2|a-b$, então $v_2(a^n - b^n) = v_2(a-b)$.
(iv)Se $p = 2$, n é ímpar e $2|a-b$, então $v_2(a^n + b^n) = v_2(a+b)$.
(v) Se $p = 2$, n é par e $2|a-b$, então $v_2(a^n - b^n) = v_2(a+b) + v_2(a-b) + v_2(n) - 1$.

Demonstração: (i) Extraia todos os fatores primos p de n, de modo que podemos escrever $n = p^k m$, onde m é um inteiro positivo não divisível por p e k é um inteiro não negativo. Para demonstrar isso, faremos indução em k.

O caso $k = 0$ é consequência da fatoração:

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

Como $p|a-b$, temos $a \equiv b \ (mod\ p)$, donde $= a^t b^{n-1-t} \equiv a^t a^{n-1-t} \equiv a^{n-1} \ (mod\ p)$ e daí:

$$a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} \equiv \underbrace{a^{n-1} + a^{n-1} + \cdots + a^{n-1}}_{n\ vezes} \equiv na^{n-1} \ (mod\ p)$$

E como na^{n-1} não é divisível por p (pois $n = m$ e a não são), temos que, em (1), o fator $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}$ não contribui com fator p, donde:

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

Finalizando o caso inicial. Agora, supondo que, se $v_p(n) = t$, então é válido que $v_p(a^n - b^n) = v_p(a-b) = v_p(a-b) + v_p(n)$, temos que provar que essa fórmula vale para $v_p(n) = t+1$. Para tanto, deixe $n = p^{t+1}m$, onde m não divide p. Com isso:

$$a^n - b^n = \left(a^{p^t m}\right)^p - \left(b^{p^t m}\right)^p = (x-y)(x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1}) \ (2)$$

Onde $x = a^{p^t m}$ e $y = b^{p^t m}$. Observe que, por hipótese de indução:

$$v_p(x-y) = v_p\left(a^{p^t m} - b^{p^t m}\right) = v_p(a-b) + v_p(p^t m) = v_p(a-b) + t$$

Agora, provemos que $v_p(x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1}) = 1$. A ideia é estudar essa expressão módulo p^2 e usar binômio de Newton. Para tanto, como $p|x-y$ (pois $x - y = a^{p^t m} - b^{p^t m}$ tem fator $(a-b)$, que é divisível por p), existe um inteiro s tal que $x = ps + y$. Assim, para todo inteiro $0 \leq t \leq p-1$:

$$x^t y^{p-1-t} = (ps+y)^t y^{p-1-t} =$$

$$= \left(\binom{t}{t} p^t s^t y^0 + \binom{t}{t-1} p^{t-1} s^{t-1} y^1 + \cdots + \binom{t}{2} p^2 s^2 y^{t-2} + \binom{t}{1} psy^{t-1} + \binom{t}{0} y^t\right) y^{p-1-t} \equiv$$

$$\equiv (0 + 0 + \cdots + 0 + tpsy^{t-1} + y^t) y^{p-t-1} \equiv (tps + y) y^{p-2} \ (mod\ p^2)$$

Portanto:

$$x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \equiv$$

$$\equiv \big((p-1)ps + y\big)y^{p-2} + \big((p-2)ps + y\big)y^{p-2} + \cdots + (ps+y)y^{p-2} + (y)y^{p-2} \equiv$$

$$\equiv \Big(\big((p-1) + (p-2) + \cdots + 2 + 1\big)ps + py\Big)y^{p-2} \equiv \left(\left(\frac{p(p-1)}{2}\right)ps + py\right)y^{p-2} \equiv$$

$$\equiv \underbrace{\left(\frac{p-1}{2}\right)}_{\in \mathbb{Z}\ (p\ \acute{i}mpar)} p^2 s y^{p-2} + p y^{p-1} \equiv 0 + p y^{p-1} \equiv p y^{p-1}\ (mod\ p^2)$$

Logo, como p divide py^{p-1}, mas p^2 não divide py^{p-1}, temos que $v_p(x^{p-1} + \cdots + y^{p-1}) = 1$. Finalmente, (2) implica:

$$v_p(a^n - b^n) = v_p(x - y) + v_p(x^{p-1} + \cdots + y^{p-1}) = v_p(a - b) + t + 1 = v_p(a - b) + v_p(n)$$

E o resultado segue por indução.

(ii) A demonstração é análoga a (i) e é deixada como exercício (a necessidade de n ser ímpar é que, se n for par, $a^n + b^n$ não tem como ser fatorado de maneira direta).

(iii) Note que, como $p = 2$ não divide a e b, então a, b são ímpares. Pela fatoração:

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 \ldots + ab^{n-2} + b^{n-1})$$

Temos que, como cada número da forma $a^k b^{n-1-k}$, $0 \leq k \leq n - 1$, é ímpar, a soma $a^{n-1} + a^{n-2}b + a^{n-3}b^2 \ldots + ab^{n-2} + b^{n-1}$ é uma soma de n parcelas ímpares, logo é ímpar, pois n é ímpar. Daí, tal parcela não contribui em nada com o expoente, donde $v_2(a^n - b^n) = v_2(a - b)$.

(iv) A demonstração é análoga a (iii) e é deixada como exercício.

(v) Escreva $n = 2^k m$, onde m é um inteiro ímpar (ou seja, extraímos todos os fatores 2, obtendo o fator 2^k). Com isso, $v_2(n) = k \geq 1$ (pois n é par), e também:

$$a^n - b^n = a^{2^k m} - b^{2^k m} = (a^m)^{2^k} - (b^m)^{2^k} =$$

$$\left((a^m)^{2^{k-1}} + (b^m)^{2^{k-1}}\right)\left((a^m)^{2^{k-2}} + (b^m)^{2^{k-2}}\right) \ldots ((a^m)^2 + (b^m)^2)(a^m + b^m)(a^m - b^m)\ (*)$$

Como a, b são ímpares e usando o fato de que $x^2 \equiv 1(mod\ 4)$, para todo x ímpar, temos que $(a^m)^2, (b^m)^2 \equiv 1(mod\ 4)$, ou seja, para todo $1 \leq t \leq k - 1$:

$$(a^m)^{2^t} + (b^m)^{2^t} \equiv ((a^m)^2)^{2^{t-1}} + ((b^m)^2)^{2^{t-1}} \equiv 1^{2^{t-1}} + 1^{2^{t-1}} \equiv 1 + 1 \equiv 2(mod\ 4)$$

Isso significa que cada um dos $k - 1$ fatores $(a^m)^{2^t} + (b^m)^{2^t}$ é divisível por 2, mas não por 4, ou seja, cada um deles contribui com apenas uma potência de 2. Logo, $v_2(A) = k - 1$, onde:

$$A = \left((a^m)^{2^{k-1}} + (b^m)^{2^{k-1}}\right)\left((a^m)^{2^{k-2}} + (b^m)^{2^{k-2}}\right) \ldots ((a^m)^2 + (b^m)^2)$$

Finalmente, de $(*)$ resulta que:

$$v_2(a^n - b^n) = v_2\big(A(a^m + b^m)(a^m - b^m)\big) = v_2(A) + v_2(a^m + b^m) + v_2(a^m - b^m)$$

Como $v_2(A) = k - 1 = v_2(n) - 1$, e, por (iii), (iv), e do fato de m ser ímpar, podemos escrever $v_2(a^m + b^m) = v_2(a + b)$, $v_2(a^m - b^m) = v_2(a - b)$. Substituindo, temos:

$$v_2(a^n - b^n) = v_2(a + b) + v_2(a - b) + v_2(n) - 1$$

Finalizando a demonstração do LTE ■

O LTE é destruidor pelo fato de que, uma vez conhecido os fatores primos de uma expressão da forma $a^n \pm 1$, o valor de n cresce de modo exponencial à medida que $a^n \pm 1$ também cresce, o que permite-nos limitar bastante o valor de n. Ficou meio confuso, né? Nada melhor do que um exemplo para você entender melhor.

Exemplo 3: Ache todos os valores inteiros positivos (a, b, c) tais que $5^a - 3^b = c^2$.

Solução: Antes de aplicar LTE, vamos usar propriedades básicas de teoria dos números para desenrolar o que pudermos sobre a, b, c. Inicialmente, analisando módulo 3, temos que:

$$c^2 \equiv 5^a - 3^b \equiv (-1)^a \ (mod\ 3)$$

E como $c^2 \equiv 0\ ou\ 1\ (mod\ 3)$, $(-1)^a \equiv 1\ (mod\ 3)$, donde a é par ($a = 2a_0, a_0 \in \mathbb{N}$). Logo:

$$3^b = 5^a - c^2 = (5^{a_0})^2 - c^2 = (5^{a_0} + c)(5^{a_0} - c)$$

E como tal expressão é uma potência de 3, cada parênteses é uma potência de 3. Assim, existem inteiros não negativos α, β, com $5^{a_0} + c = 3^\alpha$, $5^{a_0} + c = 3^\beta$ e $\alpha > \beta$ (pois $5^{a_0} + c > 5^{a_0} - c$). Somando tais igualdades, obtemos:

$$2.5^{a_0} = 3^\alpha + 3^\beta = 3^\beta\left(3^{\alpha-\beta} + 1\right)$$

Se $\beta \geq 1$, o lado direito dessa expressão é múltiplo de 3, mas o lado esquerdo não, absurdo. Logo, $\beta = 0$ e assim $2.5^{a_0} = 3^\alpha + 1$. Olhando módulo 5, vemos que $3^\alpha \equiv -1\ (mod\ 5)$, e como as potências de 3 módulo 5 se repetem de 4 em 4, é fácil concluir que $\alpha \equiv 2\ (mod\ 4)$, ou seja $\alpha = 2m$, m ímpar. Portanto:

$$2.5^{a_0} = 3^{2m} + 1 \Rightarrow 10.5^{a_0 - 1} = 9^m + 1\ (*)$$

Se $a_0 = 1$, então $10 = 9^m + 1 \Rightarrow m = 1 \Rightarrow \alpha = 2 \Rightarrow 3^\alpha = 9 = 5^{a_0} + c = 5 + c \Rightarrow c = 4$. Voltando à equação original, $5^2 - 3^b = 4^2 \Rightarrow b = 2 \Rightarrow (a, b, c) = (2,2,4)$ é uma solução.

Suponha que $a_0 \geq 2$. De $(*)$, como m é ímpar e $5|9 + 1$, temos, por LTE $a_0 = v_5(2.5^{a_0}) = v_5(9^m + 1) = v_5(9 + 1) + v_5(m) = 1 + v_5(m) \Rightarrow v_5(m) = a_0 - 1$, donde $m \geq 5^{a_0 - 1}$. Portanto, se $x = 5^{a_0 - 1}$, essa desigualdade, combinado com $(*)$, implica:

$$10x = 10.5^{a_0 - 1} = 9^m + 1 \geq 9^{5^{a_0 - 1}} + 1 = 9^x + 1 > 9^x \Rightarrow \frac{9^x}{x} < 10$$

Mas $a_0 \geq 2$ implica $x \geq 5$, e pode-se provar facilmente por indução que $\frac{9^x}{x} > 10$ para $x \geq 2$. Assim, esse caso não gera nenhuma solução, e portanto a única resposta é $(a, b, c) = (2,2,4)$ ■

O LTE também pode ser usado para "gerar" primos novos. A questão a seguir ilustra isso.

Exemplo 4 (IMO/2000): Existe um natural n tal que n possui exatamente 2000 fatores primos e $n|2^n + 1$?

Solução: Incrivelmente, existe sim, e não é só para 2000 fatores primos, mas para qualquer quantidade! De fato, vamos tentar provar por indução em $k \in \mathbb{N}$ que existe um inteiro positivo n_k tal que n_k tenha exatamente k fatores primos e $n_k|2^{n_k} + 1$. A ideia é fazer com que $2^{n_k} + 1$ tenha um fator primo a mais que n_k, e usar esse fator primo para construir n_{k+1}. A princípio, podemos tentar pegar $n_1 = 3$, mas ele não serve, pois $2^3 + 1 = 3^2$ não tem um fator primo novo. Vamos tentar o próximo n_1 ímpar (afinal, os n_k's devem ser ímpares para usarmos LTE), que é $n_1 = 9$. Ele serve, pois $2^9 + 1 = 513 = 3^3.19$.

Defina então $n_1 = 9$ e faça $n_2 = 9.19$. Note que, por LTE:

$$v_3(2^{n_2} + 1) = v_3(2 + 1) + v_3(n_2) = 1 + 2 = 3$$

$$v_{19}(2^{n_2} + 1) = v_{19}((2^9)^{19} + 1) = v_{19}(2^9 + 1) + v_{19}(19) = 1 + 1 = 2$$

Logo, $2^{9.19} + 1 = 3^3.19^2.M_2$, onde M_2 é um inteiro positivo sem fatores 3 e 19. Como, obviamente, $2^{3^2.19} + 1 > 2^{3^2.19} > (3^2.19)^2$ (aqui, estamos usando a clássica desigualdade $2^T > T^2$, para $T > 4$) e $(3^2.19)^2 > 3^3.19^2$, segue que $M_2 > 1$, ou seja, M_2 tem um fator primo diferente, digamos p_3.

Tá vendo como esses caras novos aparecem? Eles meio que são as "sobras" dos levantamentos do expoentes. Vamos aproveitá-las para construir números com fatores ainda maiores! Mas primeiro, vamos reorganizar nossas ideias de maneira decente.

Vamos provar por indução em $k \geq 2$ que existe n_k com exatamente k fatores primos distintos $3 = p_1, p_2, \dots, p_k$, tal que:

$$n_k = 3^2.p_2^{\alpha_2}.p_3^{\alpha_3} \dots p_k^{\alpha_k}$$

$$2^{n_k} + 1 = 3^3.p_2^{2\alpha_2}.p_3^{2\alpha_3} \dots p_k^{2\alpha_k} p_{k+1}^{\alpha_{k+1}} R_{k+1}$$

Onde p_{k+1} é um primo que não aparece em n_k e R_{k+1} é um número não divisível pelos primos $p_1, \dots, p_{k+1}$. O caso inicial $k = 2$ foi feito acima ($n_2 = 3^2.19^1$). Supondo que isso vale para certo k, defina:

$$n_{k+1} = 3^2.p_2^{\alpha_2}.p_3^{\alpha_3} \dots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}} = n_k p_{k+1}^{\alpha_{k+1}}$$

Note que, para $i = 2, \dots, k$:

$$v_{p_i}(2^{n_{k+1}} + 1) = v_{p_i}\left((2^{n_k})^{p_{k+1}^{\alpha_{k+1}}} + 1\right) = v_{p_i}(2^{n_k} + 1) + v_{p_i}\left(p_{k+1}^{\alpha_{k+1}}\right) \overset{hipótese}{=} 2\alpha_i + 0 = 2\alpha_i$$

E, olhando o fator p_{k+1}:

$$v_{p_{k+1}}(2^{n_{k+1}} + 1) = v_{p_{k+1}}\left((2^{n_k})^{p_{k+1}^{\alpha_{k+1}}} + 1\right) = v_{p_{k+1}}(2^{n_k} + 1) + v_{p_{k+1}}\left(p_{k+1}^{\alpha_{k+1}}\right) \overset{hipótese}{=}$$

$$= \alpha_{k+1} + \alpha_{k+1} = 2\alpha_{k+1}$$

E olhando o fator 3:

$$v_3(2^{n_{k+1}} + 1) = v_3(2 + 1) + v_3(n_{k+1}) = 1 + 2 = 3$$

Logo, $2^{n_{k+1}} + 1 = 3^3 . p_2^{2\alpha_2} . p_3^{2\alpha_3} \dots p_k^{2\alpha_k} p_{k+1}^{2\alpha_{k+1}} M_{k+2}$, onde M_{k+2} é um inteiro positivo sem os fatores $p_1, \dots, p_{k+1}$. Para provarmos que $2^{n_{k+1}} + 1$ tem um novo fator primo além desses, precisamos provar que $M_{k+2} > 1$. Suponha o contrário, ou seja, $M_{k+2} = 1$. Assim:

$$2^{n_{k+1}} + 1 = 3^3 . p_2^{2\alpha_2} . p_3^{2\alpha_3} \dots p_k^{2\alpha_k} p_{k+1}^{2\alpha_{k+1}} < \left(3^2 . p_2^{\alpha_2} . p_3^{\alpha_3} \dots p_{k+1}^{\alpha_{k+1}}\right)^2 = (n_{k+1})^2$$

O que é absurdo, já que, para $N > 4$, $2^N > N^2$ (prove isso via indução!). Portanto, M_{k+2} possui um fator primo p_{k+2} distinto dos demais, e podemos escrever $M_{k+2} = p_{k+2}^{\alpha_{k+2}} R_{k+2}$, onde R_{k+2} não é divisível por $p_1, \dots, p_{k+2}$. Daí:

$$2^{n_{k+1}} + 1 = 3^3 . p_2^{2\alpha_2} . p_3^{2\alpha_3} \dots p_k^{2\alpha_k} p_{k+1}^{2\alpha_{k+1}} p_{k+2}^{\alpha_{k+2}} R_{k+2}$$

E a indução está completa ■

E para finalizar, que tal uma demonstração de força bruta nesse exercício, que mostra a explosão absurda nos expoentes e que também envolve a fórmula de Polignac? Só bora!

Exemplo 5: Determine todos os pares de inteiros positivos (m, n) tais que $(n-1)! + 1 = n^m$.

Solução: Vejamos alguns casos "chiquitos" para termos uma ideia do que fazer

- Se $n = 1$, então $(1-1)! + 1 = 1^m \Rightarrow 2 = 1^m$, absurdo.
- Se $n = 2$, então $(2-1)! + 1 = 2^m \Rightarrow 2 = 2^m \Rightarrow m = 1 \Rightarrow (m, n) = (1,2)$ é solução.
- Se $n = 3$, então $(3-1)! + 1 = 3^m \Rightarrow 3 = 3^m \Rightarrow m = 1 \Rightarrow (m, n) = (1,3)$ é solução.
- Se $n = 4$, então $(4-1)! + 1 = 4^m \Rightarrow 7 = 4^m$, absurdo.
- Se $n = 5$, então $(5-1)! + 1 = 5^m \Rightarrow 25 = 5^m \Rightarrow m = 2 \Rightarrow (m, n) = (2,5)$ é solução.

A partir dos casos $n \geq 6$, você verá que não haverão mais soluções, por isso omitimos esses testes aqui. Porém, devemos explicar porque não há mais soluções a partir daqui.

Suponha primeiro que n é composto. Isso implica que existe $2 \leq a \leq n-1$ tal que $a|n$. Como a aparece em $(n-1)!$, analisando a expressão original módulo a, vem $0 \equiv n^m = (n-1)! + 1 \equiv 0 + 1 \equiv 1\ (mod\ a)$, absurdo. Logo, $n = p$ é primo. Assim, nossa equação fica:

$$(p-1)! + 1 = p^m \Rightarrow (p-1)! = p^m - 1\ (*)$$

Suponha inicialmente que existe um primo ímpar q tal que $q|p-1$. Escrevamos $p - 1 = q^\alpha A$, onde A não é divisível por q (note que $v_q(p-1) = \alpha$). Veja que, por Polignac:

$$v_q\big((p-1)!\big) = \left\lfloor \frac{p-1}{q} \right\rfloor + \left\lfloor \frac{p-1}{q^2} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{q^\alpha} \right\rfloor + \cdots \geq \left\lfloor \frac{p-1}{q} \right\rfloor + \left\lfloor \frac{p-1}{q^2} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{q^\alpha} \right\rfloor =$$

$$= q^{\alpha-1}A + q^{\alpha-2}A + \cdots + A = A(q^{\alpha-1} + q^{\alpha-2} + \cdots + 1) \geq$$

$$\geq A(q + q + \cdots + q + 1) = A\big((\alpha-1)q + 1\big)$$

Aplicando LTE em $(*)$, temos:

$$\alpha + v_q(m) = v_q(p-1) + v_q(m) = v_q(p^m - 1) = v_q\big((p-1)!\big) \geq A\big((\alpha-1)q + 1\big)$$

Logo, $v_q(m) \geq A\big((\alpha-1)q + 1\big) - \alpha = (A(\alpha-1)q - 2\alpha) + \alpha + A$. Vejamos alguns casos:

Caso 1: Se $\alpha \geq 2$, então usando que $A \geq 1$, $q \geq 3$:

$$(A(\alpha-1)q - 2\alpha) + \alpha + A \geq (1.1.q - 4) + \alpha + A = q - 4 + \alpha + A > -1 + \alpha + A$$

Donde $v_q(m) \geq \alpha + A$. Assim, $m \geq q^{\alpha+A} = q^\alpha . \underbrace{q^A}_{q^A > A} \geq q^\alpha A = p - 1 \Rightarrow m \geq p$, e assim:

$$p^m - 1 = p^p - 1 > p^{p-1} = \underbrace{p.p \ldots .p.p}_{p-1\ fatores} > (p-1)(p-2) \ldots 2.1 = (p-1)!$$

O que é um absurdo (as desigualdades usadas aqui ficam como exercício para o leitor).

Caso 2: Se $\alpha \geq 1$, então $v_q(m) \geq A\big((\alpha-1)q + 1\big) - \alpha = A - 1$, donde $m \geq q^{A-1}$. Se $A \geq 3$, então $p^m - 1 \geq p^{q^{A-1}} - 1 = p^{q.q^{A-2}} - 1 \geq p^{q.3^{A-2}} - 1$, e como $3^{A-2} \geq A$ (mais um exercício para o leitor!), temos:

$$p^{q.3^{A-2}} - 1 \geq p^{qA} - 1 = p^{p-1} - 1 > (p-1)^{p-1} = (p-1)(p-1) \ldots (p-1)(p-1)$$

$$> (p-1)(p-2) \ldots 2.1 = (p-1)! \Rightarrow p^m - 1 > (p-1)!$$

O que é um absurdo. Se $A = 2$, então $p - 1 = 2q$, e assim, por LTE:

$$v_2(p^m - 1) = v_2(p-1) + v_2(p+1) + v_2(m) - 1 = v_2(p+1) + 1$$

Como:

$$v_2(p^m - 1) = v_2\big((p-1)!\big) = v_2\big((2q)!\big) = \left\lfloor \frac{2q}{2} \right\rfloor + \left\lfloor \frac{2q}{4} \right\rfloor + \cdots \geq$$

$$\geq \left\lfloor \frac{2q}{2} \right\rfloor + \left\lfloor \frac{2q}{4} \right\rfloor = q + \frac{q-1}{2} = \frac{3q-1}{2}$$

Vem:

$$v_2(p+1) + 1 \geq \frac{3q-1}{2} \Rightarrow v_2(p+1) \geq \frac{3q-3}{2} \geq q$$

Pois $q \geq 3$. Assim, $p + 1 \geq 2^q$, e como se pode provar por indução que $2^q > 2q + 2 = p + 1$ para $q > 3$ (exercício...), a única conclusão que chegamos é que $q = 3$, ou seja $p = 2.3 + 1 = 7$. Porém:

$$(7-1)! + 1 = 721 = 7.103 \neq 7^m$$

O que é um absurdo.

Ufa! Que trabalhão! Porém, ainda falta o caso em que não existe primo ímpar q tal que $q|p-1$, ou seja, $p - 1$ é uma potência de 2 (digamos 2^s). Assim, $p = 2^s + 1$. Para estudar esse caso, vamos levantar quem são os expoentes de 2. Força!

$$v_2\big((p-1)!\big) = v_2\big((2^s)!\big) = \left\lfloor \frac{2^s}{2} \right\rfloor + \left\lfloor \frac{2^s}{2^2} \right\rfloor + \cdots \left\lfloor \frac{2^s}{2^t} \right\rfloor = 2^{s-1} + 2^{s-2} + \cdots + 2 + 1 = 2^s - 1$$

Se m é ímpar, $v_2(p^m - 1) = v_2(p-1) = v_2(2^s) = s$, ou seja, $2^s - 1 = s$, e isso implica $s = 1$ (pois se $s > 1$, $2^s > s + 1$. Mais um exercício!). Com isso, $p = 2^1 + 1 = 3$, mas $n > 3$, e assim temos absurdo.

E se m é par:

$$v_2(p^m - 1) = v_2(p+1) + v_2(p-1) + v_2(m) - 1 =$$

$$= v_2(2^t + 2) + v_2(2^t) + v_2(m) - 1 = 1 + t + v_2(m) - 1 = t + v_2(m)$$

Assim, $v_2(m) = 2^s - s - 1$, e como, para $s \geq 3$, $2^s - s - 1 \geq s + 1$ (já sabe o que é, né? Rsrsrs...), vem:

$$v_2(m) \geq s + 1 \Rightarrow m \geq 2^{s+1} = 2(p-1) > p \Rightarrow (p-1)! = p^m - 1 > p^p - 1$$

E como vimos antes, isso resulta em um absurdo (veja a prova do caso 1). Assim, $s \leq 2$, o que implica $n = p \leq 2^2 + 1 = 5$, o que já estudamos antes.

Conclusão: $(m, n) = (1,2), (1,3), (2,5)$ ■

4. Problemas

4.1. Levantando Expoentes em Fatoriais - Problemas

Problema 1: Em quantos zeros $1000!$ termina em sua representação decimal?

Problema 2 (Argentina/1995): Seja $N = \frac{3995!}{995!}$. Ache a maior potência de 3 que divide *N*.

Problema 3: (a) Prove que o expoente da maior potência de *p* que divide $(p^k - 1)!$ é igual a:

$$\frac{p^k - (p-1)k - 1}{p-1}$$

(b) Determine a maior potência de 3 que divide $80!$ e a maior potência de 7 que divide $2400!$.

Problema 4: Analise se $\binom{1000}{500}$ é divisível por 7

Problema 5 (Canadá/85): Determine todos os inteiros positivos n tais que 2^{n-1} divide $n!$

Problema 6: Prove que, para todo natural n, $(n+1)(n+2)\ldots(2n)$ é divisível por 2^n.

Problema 7: Ache o menor natural n tal que 3^{2018} é um divisor de $(n+1)(n+2)\ldots 3n$.

Problema 8: Seja $B(m)$ o conjunto dos inteiros *r* tais que 2^r é um termo da representação na base 2 de *n*. Por exemplo, $B(100) = \{2,5,6\}$, pois $100 = 2^6 + 2^5 + 2^2$. Prove que $\binom{n}{k}$ é ímpar se, e somente se, $B(k) \subseteq B(n)$.

Problema 9: Mostre que $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ são todos pares se, e só se, n é potência de 2.

Problema 10 (Nórdica/98): Seja n um inteiro positivo. Prove que o número de $k \in \{0,1,2,\ldots,n\}$ para os quais $\binom{n}{k}$ é ímpar é uma potência de 2.

Problema 11: Se $n \geq 1$ e p é um primo, prove que:

(a) $\binom{2n}{n}$ é um inteiro par;

(b) Na fatoração de $\binom{2n}{n}$ o expoente de qualquer primo $n < p < 2n$ é igual a 1.

Problema 12: (a) Se *p* é primo, prove que $\binom{p}{i} \equiv 0\ (mod.p)$, para $1 \leq i \leq p-1$.

(b) Se *p* é primo, $k \in \mathbb{N}$, prove que $\binom{p^k}{i} \equiv 0\ (mod.p)$, para $1 \leq i \leq p^k - 1$.

Problema 13 (Índia/2000): Sejam *m, n* inteiros positivos tais que $m \leq \left(\frac{n}{2}\right)^2$ e todo divisor primo de *m* é menor ou igual a *n*. Prove que *m* divide $n!$.

Problema 14 (IMO/1972): Sejam *m, n* inteiros não-negativos. Prove que $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ é um inteiro.

Problema 15 (IMO/1972):Prove que $\binom{2n}{n}$ divide $mmc(1,2,\ldots,2n)$.

Problema 16 (Banco Ibero/1997): Ache todos os inteiros positivos *n* tais que o *n*-ésimo número de Catalão, $C_n = \frac{1}{n+1}\binom{2n}{n}$, é ímpar.

Problema 17: Sejam n, q inteiros positivos, com $n \geq 5$ e $2 \leq q \leq n$. Prove que $(q-1)$ divide $\left\lfloor \frac{(n-1)!}{q} \right\rfloor$.

4.2. Lifting The Exponent Lemma (Vulgo LTE) - Problemas

Problema 18: Seja k um inteiro positivo. Determine todos os inteiros positivos n tais que $3^k | 2^n - 1$.

Problema 19 (TST Balcânica Júnior – Romênia/2008): Seja $p \neq 3$ um primo, e inteiros a, b tais que $p|a+b$ e $p^2|a^3+b^3$. Prove que $p^2|a+b$ ou $p^3|a^3+b^3$.

Problema 20 (Irlanda/1996): Seja p primo e sejam a, n naturais. Prove que se $2^p + 3^p = a^n$, então $n = 1$.

Problema 21 (Rússia/1996): Determine todos os inteiros positivos n para os quais existem inteiros positivos x, y e k tais que $\mathrm{mdc}(x,y) = 1$, $k > 1$ e $3^n = x^k + y^k$.

Problema 22 (Rússia/1996): Sejam x, y, p, n, k inteiros positivos tais que n é ímpar e $p > 2$ é primo. Prove que se $x^n + y^n = p^k$, então n é uma potência de p.

Problema 23: Seja p um número primo. Resolva a equação $a^p - 1 = p^k$ no conjunto dos inteiros positivos.

Problema 24 (IMO/1990): Determine todos os inteiros positivos n tais que $n^2 | 2^n + 1$.

Problema 25: Determine todos os inteiros positivos n tais que n divide $2^{n-1} + 1$.

Problema 26 (MOSP/2001): Determine todas as quádruplas de inteiros positivos (x, r, p, n) tais que p é um número primo, n, r são maiores que 1 e $x^r - 1 = p^n$.

Problema 27 (Teste IMO – Romênia/1994): Seja n um inteiro positivo ímpar. Prove que:

$$((n-1)^n+1)^2 | n(n-1)^{(n-1)^n+1}+n$$

Problema 28: Determine todos os inteiros positivos n tais que 2^n divide 3^n-1.

Problema 29 (Teste IMO Romênia/2009): Sejam $a, n \geq 2$ inteiros, com a seguinte propriedade: existe um inteiro $k \geq 2$, tal que $n|(a-1)^k$. Mostre que $n|a^{n-1}+a^{n-2}+\cdots+a+1$.

Problema 30: Determine todos os inteiros positivos a tais que $3^n|5^n+1$.

Problema 31: Para algum número natural n, seja a o maior natural tal que 5^n-3^n é divisível por 2^a. Além disso, seja b o maior número natural tal que $2^b \leq n$. Prove que $a \leq b+3$.

Problema 32: Ache todas as triplas de inteiros não-negativos (x, y, z) tais que $2^x+3^y=z^2$.

Problema 33: Ache todos os valores inteiros positivos (a, b, c) tais que $5^a-3^b=c^2$.

Problema 34 (China TST/2009): Sejam $a > b > 1$ inteiros positivos, com b ímpar, e seja n um inteiro positivo. Se $b^n|a^n-1$, então prove que $a^b > 3^n/n$.

Problema 35: Sejam a, b inteiros positivos coprimos e $s > 0$ inteiro. Existe um inteiro positivo n tal que n possui exatamente s fatores primos distintos e $n|a^n+b^n$?

Problema 36 (Ibero/2000): Ache todos os $x, y, z > 1$ inteiros satisfazendo $(x+1)^y-x^z=1$.

Problema 37 (Banco IMO/2000): Determine todas as triplas de inteiros positivos (a, m, n) tais que a^m+1 divide $(a+1)^n$.

Problema 38 (CIIM/2014): Seja n um inteiro positivo e $p > 2$ um número primo. Prove que:

$$n!.(p-1)^n | (p^n-1)(p^n-p)(p^n-p^2)\ldots(p^n-p^{n-1})$$