Lema do Levantamento do Expoente

27 de Abril de 2019

Resumo

Este pequeno artigo é uma forma de introdução ao clássico Lema do Levantamento do Expoente e às suas aplicações em problemas de olimpíadas.

Notação

Dado um primo p e um inteiro $n \neq 0$, representamos por $v_p(n)$ o expoente de p na factorização em primos de n. Assim, por exemplo, $v_3(54) = 3$, $v_5(10) = 1$ e $v_7(81) = 0$.

Introdução e motivação

Seja p um primo, e sejam a e b inteiros tais que $p \mid a - b$. Então, para qualquer inteiro positivo n,

$$p \mid a^n - b^n.$$

Isto não é surpreendente, nem difícil de ver porque é que é verdade; é imediato a partir de propriedades básicas de congruências ($a \equiv b \pmod{p} \Rightarrow a^n \equiv b^n \pmod{p}$) ou da famosa factorização $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$. Podemos dizer ainda mais: se $k = v_p(a-b) > 0$, então

$$p^k \mid a^n - b^n$$

para qualquer inteiro positivo n, e mais uma vez isto decorre de propriedades básicas das congruências ($a \equiv b \pmod{p^k} \Rightarrow a^n \equiv b^n \pmod{p^k}$). É natural questionar se é possível que $a^n - b^n$ seja divisível por uma potência maior de p; será possível que $p^{k+1} \mid a^n - b^n$? Agora, infelizmente, já não temos $a \equiv b \pmod{p^{k+1}}$; mas tal não impede que $a^n \equiv b^n \pmod{p^{k+1}}$. A resposta à nossa questão é afirmativa; como exemplo, observe-se que $v_3(4-1) = 1$ (ou seja, $4-1$ é divisível por 3 mas não por 3^2), e, por outro lado, $v_3(4^3 - 1^3) = 2$ (portanto, $4^3 - 1^3$ é divisível por 3^2). Esta divisibilidade, contudo, já não resulta trivialmente da congruência $4 \equiv 1 \pmod{3}$.

O Lema do Levantamento do Expoente responde de forma generalizada a esta questão, permitindo-nos saber em quanto é que $v_p(a^n - b^n)$ excede $v_p(a - b)$. Será especialmente útil em problemas devido ao facto de essa diferença $v_p(a^n - b^n) - v_p(a - b)$ não ser muito grande em comparação com n, como vamos ver. Passemos ao Lema.

1 O Lema

Teorema 1.1 (Lema do Levantamento do Expoente)**.** *Seja p um primo ímpar. Sejam a e b inteiros tais que $p \mid a-b$, mas p não divide nem a nem b. Então, para qualquer inteiro positivo n,*

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

Demonstração. A prova do Lema passa pela prova de dois casos particulares:

- Se p não divide n, então $v_p(a^n - b^n) = v_p(a-b)$.
- $v_p(a^p - b^p) = v_p(a-b) + 1$.

Depois de provarmos estes casos particulares, não é difícil ver como concluir a prova. Intuitivamente, provamos que cada primo diferente de p no expoente n não contribui nada para aumentar $v_p(a^n - b^n)$ em relação a $v_p(a-b)$; e cada factor p aumenta $v_p(a^n - b^n)$ em exactamente uma unidade, logo $v_p(a^n - b^n)$ é aumentado em exactamente $v_p(n)$. Veremos como formalizar isto de seguida, agora vamos à prova destes casos.

Comecemos pelo primeiro. Temos

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

pelo que, para provarmos que $v_p(a^n - b^n) = v_p(a-b)$, basta provar que $v_p(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) = 0$, ou seja, provar que p não divide $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}$. Mas, como $a \equiv b \pmod{p}$, temos $a^k b^{n-1-k} \equiv b^k b^{n-1-k} \equiv b^{n-1} \pmod{p}$ para $k = 0, \ldots, n-1$, e, portanto,

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

pelo que, já que n e b são ambos não divisíveis por p, $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}$ não é divisível por p, concluindo a prova do primeiro passo.

A congruência $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} \equiv n \cdot b^{n-1} \pmod{p}$ permite-nos concluir ainda mais; se n é divisível por p, então $n \cdot b^{n-1}$ é divisível por p, logo

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

é divisível por p, e, portanto, $v_p(a^n - b^n) > v_p(a-b)$. Na verdade, um erro ingénuo poderia levar-nos a concluir a prova observando que $v_p(n \cdot b^{n-1}) = v_p(n)$, já que p não divide b, e portanto $v_p(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) = v_p(n)$, de onde o Lema resulta. No entanto, esta "prova" está errada: a "igualdade" $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} \equiv n \cdot b^{n-1}$ só é necessariamente válida

módulo p, e pode ser falsa módulo p^2, p^3, etc. Analisando igualdades módulo p, podemos decidir se $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}$ é, ou não, divisível por p; mas não podemos concluir nada sobre o seu v_p, se este for positivo.

Vamos então provar o segundo caso. Como

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

devemos provar que $a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}$ é divisível por p, mas não por p^2. A primeira parte pode ser provada usando a ideia anterior; temos $a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \equiv p \cdot b^{p-1} \pmod{p}$, logo esta p divide esta soma. A segunda parte equivale a $a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}$ não ser divisível por p^2; vamos assim calcular esta soma módulo p^2 e provar que é diferente de 0. Como $p \mid a - b$, podemos escever $a = b + mp$, onde $m \in \mathbb{Z}$.

Cada parcela da soma é da forma $a^k b^{p-1-k}$. Observe-se que

$$a^k = (b+mp)^k = \sum_{i=0}^{k} \binom{k}{i} b^i (mp)^{k-i}$$

pelo Binómio de Newton. No entanto, quase todos estes termos são 0 módulo p^2; na verdade, tal acontece sempre que $k - i \geq 2$. Assim, para calcular esta soma módulo p^2, basta-nos considerar os termos obtidos com $i = k-1$ e com $i = k$. Obtemos assim

$$a^k \equiv \binom{k}{k-1} b^{k-1} \cdot mp + \binom{k}{k} b^k \equiv b^k + kmp \cdot b^{k-1} \pmod{p^2}.$$

Logo,

$$a^k b^{p-1-k} \equiv (b^k + kmp \cdot b^{k-1}) b^{p-1-k} \equiv b^{p-1} + kmp \cdot b^{p-2} \pmod{p^2}.$$

Então,

$$\begin{aligned}
\sum_{k=0}^{p-1} a^k b^{p-1-k} &\equiv \sum_{k=0}^{p-1} b^{p-1} + kmp \cdot b^{p-2} \\
&\equiv p \cdot b^{p-1} + \sum_{k=0}^{p-1} kmp \cdot b^{p-2} \\
&\equiv p \cdot b^{p-1} + \frac{p(p-1)}{2} mp \cdot b^{p-2} \\
&\equiv p \cdot b^{p-1} \pmod{p^2}
\end{aligned}$$

já que $\frac{p(p-1)}{2} mp \cdot b^{p-2} = p^2 \cdot \frac{p-1}{2} \cdot m \cdot b^{p-2}$ é divisível por p^2. E isto completa a prova do segundo caso particular, já que $p \cdot b^{p-1}$ não é divisível por p^2, uma vez que b não é divisível por p.

Veremos agora como terminar a prova do Lema usando estes casos particulares. Escrevemos $n = l \cdot p^k$, onde p não divide l. Então

$$\begin{aligned} v_p(a^n - b^n) &= v_p(a^{l \cdot p^k} - b^{l \cdot p^k}) \\ &= v_p((a^{l \cdot p^{k-1}})^p - (b^{l \cdot p^{k-1}})^p) = v_p(a^{l \cdot p^{k-1}} - b^{a \cdot p^{k-1}}) + 1 \\ &= v_p(a^{l \cdot p^{k-2}} - b^{l \cdot p^{k-2}}) + 2 \\ &\dots \\ &= v_p(a^l - b^l) + k = v_p(a-b) + v_p(n). \end{aligned}$$

E isto termina a demonstração.

□

1.1 Alguma reflexão sobre a prova

Terminada a prova, é essencial colocar uma questão importante em artigos olímpicos: o que deve ser memorizado desta prova? Essencialmente é importante saber quais são as etapas essenciais ($v_p(a^n - b^n) = v_p(a-b)$ se p não divide n e $v_p(a^p - b^p) = v_p(a-b) + 1$) e saber como concluir a prova tendo provado estas; também é importante ter consciência da importância da congruência $a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1} \equiv n \cdot b^{n-1} \pmod{p}$ na prova; esta faz não parecer surpreendente que $v_p(a^n - b^n) - v_p(a-b)$ esteja relacionado com $v_p(n)$. Os detalhes técnicos de cada uma das etapas não necessitam de ser memorizados, mas é desejável que o leitor tenha alguma confiança em como seria capaz de os completar se necessitasse. Além do interesse que estes factos e ideias possam ter por si só, os factos úteis em problemas olímpicos são úteis não só nos problemas em que se aplicam, mas também pelas motivações que possam ser despertadas pelas ideias por detrás deles.

É também importante destacar o facto (embora tal se torne mais claro nos exemplos que se seguirão) de que o grande poder do Lema está na desigualdade $v_p(a^n - b^n) \leq v_p(a-b) + v_p(n)$. De facto, utilizando $a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1} \equiv n \cdot b^{n-1} \pmod{p}$ é fácil provar, sob as hipóteses do Lema, que $v_p(a^p - b^p) \geq v_p(a-b) + 1$, e usando as ideias finais da prova obtemos facilmente $v_p(a^n - b^n) \geq v_p(a-b) + v_p(n)$. A desigualdade contrária, que foi a que ocupou mais linhas da prova, é o motivo do poder deste Lema; diz-nos que $v_p(a^n - b^n)$ *não excede muito* $v_p(a-b)$ (excede em $v_p(n)$, e $v_p(n) \leq \log_p(n)$, que é "pequeno"). Estes pensamentos tornar-se-ão mais claros nos exemplos.

1.2 O caso $p = 2$

No enunciado do Lema impusemos que $p \neq 2$. De facto, isto foi essencial na nossa prova: utilizámos o facto de o número

$$p^2 \cdot \frac{p-1}{2} \cdot m \cdot b^{p-2}$$

ser divisível por p^2, que resulta do facto de $\frac{p-1}{2}$ ser um inteiro. Quando $p = 2$, temos um resultado semelhante:

Teorema 1.2 (Lema do Levantamento do Expoente para primos pares)**.** *Sejam a e b inteiros ímpares e n um inteiro positivo. Então,*

- *Se n é ímpar, $v_2(a^n - b^n) = v_2(a - b)$.*
- *Se n é par, $v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1$.*

Demonstração. Para o caso n ímpar, a prova anterior do caso em que n não é divisível por p adequa-se perfeitamente para este caso. Suponhamos agora que n é par e seja $n = m \cdot 2^k$, onde k é um inteiro positivo e m é ímpar. Então,

$$a^n - b^n = a^{m\cdot 2^k} - b^{m\cdot 2^k} = (a^m - b^m)(a^m + b^m)(a^{m\cdot 2} + b^{m\cdot 2})(a^{m\cdot 4} + b^{m\cdot 4}) \cdots (a^{m\cdot 2^{k-1}} + b^{m\cdot 2^{k-1}}).$$

Cada um dos factores $a^{m\cdot 2}+b^{m\cdot 2}, \ldots, a^{m\cdot 2^{k-1}}+b^{m\cdot 2^{k-1}}$ é a soma de dois quadrados perfeitos ímpares. Ora, se x e y são ímpares, temos $x^2, y^2 \equiv 1 \pmod 4$, logo $x^2 + y^2 \equiv 2 \pmod 4$. Assim, cada um destes factores é divisível por 2 mas não por 4, pelo que contribui em exactamente 1 para $v_2(a^n - b^n)$. Por fim, temos $v_2(a^m - b^m) = v_2(a - b)$, já que 2 não divide m, e $v_2(a^m + b^m) = v_2(a^m - (-b)^m) = v_2(a - (-b)) = v_2(a + b)$. Logo,

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

como pretendido. □

Note-se que um dos números $v_2(a - b)$ e $v_2(a + b)$ é igual a 1; de facto, estes números são ambos pares, e não podem ser ambos divisíveis por 4 (tal implicaria $4 \mid (a + b) + (a - b) = 2a$, pelo que $2 \mid a$, o que é uma contradição). Assim, temos $v_2(a^n - b^n) = v_2(a - b) + v_2(n)$ ou $v_2(a^n - b^n) = v_2(a + b) + v_2(n)$ para todo o n.

1.3 Algumas dicas finais

Concluiremos a secção com algumas observações finais. Em primeiro lugar, se n é ímpar é possível utilizar o Lema do Levantamento do Expoente com soma ao invés de diferença, pois

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

Em segundo lugar, um aviso MUITO IMPORTANTE: **a hipótese $p \mid a - b$ é essencial!** Se p não divide $a - b$, o Lema não é necessariamente verdadeiro, e uma solução baseada nesse pressuposto está completamente errada.

2 Os problemas

Vamos agora mostrar exemplos de aplicação do Lema. O primeiro é um exemplo bastante simples que mostra, de certa forma, como rodear a necessidade de $p \mid a-b$ na utilização do Lema.

Problema 1. Seja k um inteiro positivo. Para que inteiros positivos n é que 2^n-1 é divisível por 5^k?

Solução. A condição dada é equivalente a $v_5(2^n-1) \geq k$, e a primeira tentação é utilizar imediatamente o Lema do Levantamento do Expoente: $v_5(2^n-1^n) = v_5(2-1)+v_5(n) = v_5(n)$. No entanto, a aplicação não está correcta, pois 5 não divide $2-1$! Como podemos então recorrer ao Lema do Levantamento do Expoente?

Estamos exclusivamente interessados em inteiros positivos n tais que 2^n-1 é divisível por 5. Para que inteiros positivos n é que tal acontece? O menor tal inteiro positivo n é 4; e, como tal, as potências de 2, módulo 5, repetem-se de 4 em 4 (4 é a *ordem* de 2 módulo 5). Assim, 5 divide 2^n-1 se e só se 4 divide n. Então podemos escrever $n=4m$; mas, precisamente pelo motivo que nos levou ao 4, temos $5 \mid 2^4-1$, e agora temos todas as condições necessárias:

$$v_5(2^n-1) = v_5(2^{4m}-1) = v_5((2^4)^m-1^m) = v_5(2^4-1)+v_5(m) = 1+v_5(m).$$

Logo, $5^k \mid 2^n-1$ se e só se $1+v_5(m) \geq k$, ou seja, se e só se $v_5(m) \geq k-1$, que equivale a 5^{k-1} dividir m. Assim, os inteiros positivos n que verificam o enunciado são os da forma $n = 4 \cdot 5^{k-1} \cdot t$, com $t \in \mathbb{Z}^+$. Isto conclui o problema. □

Mencionámos anteriormente a importância do facto de $v_p(a^n-b^n)$ exceder $v_p(a-b)$ em "apenas" $v_p(n)$. Os próximos dois exemplos mostram o poder do Lema do Levantamento do Expoente para estabelecer desigualdades altamente restritivas.

Problema 2. Encontrar todos os pares (m,n) de inteiros positivos tais que

$$14 \cdot 3^m = 5^n + 1.$$

Solução. Temos $v_3(5^n+1) = v_3(5+1)+v_3(n) = 1+v_3(n)$. É claro que tal acontece unicamente se n for ímpar, e por momentos isso pode parecer um obstáculo intransponível na nossa abordagem. Mas não é, pois se n é par temos $5^n+1 \equiv (-1)^n+1 \equiv 2 \pmod 3$, e portanto 5^n+1 não é divisível por 3. Logo, n é ímpar e podemos utilizar o Lema do Levantamento do Expoente para 5^n+1 sem obstáculos.

Temos assim $m = 1+v_3(n)$. Logo, $5^n+1 = 14 \cdot 3^{1+v_3(n)} = 42 \cdot 3^{v_3(n)}$. Mas $3^{v_3(n)} \mid n$, logo $3^{v_3(n)} \leq n$, e, assim,

$$5^n+1 \leq 42n.$$

O núcleo da solução já acabou: a nossa intuição deverá dizer-nos agora que o lado esquerdo, sendo exponencial em n, não pode ser menor ou igual ao direito para n muito grande, uma vez que o lado direito é linear em n. De facto, $5^n + 1$ cresce muito mais depressa do que $42n$. É claro que precisamos de formalizar isto, e há várias formas de o fazer; podemos, por exemplo, utilizar indução em n para provar que, se $n \geq 4$, então $5^n + 1 > 42n$. O caso-base é trivial; e, se $5^n + 1 > 42n$,

$$5^{n+1} + 1 = 5 \cdot 5^n + 1 < 5(42n - 1) + 1 \geq 42(n + 1).$$

Logo, devemos ter $n \leq 3$. Verificando os casos $n = 1, 2, 3$, concluimos que a única solução do problema é $(m, n) = (2, 3)$. □

Analisaremos brevemente a solução anterior. Essencialmente obtivemos uma estimativa, utilizando o Lema do Levantamento do Expoente, para a maior potência de 3 que divide $5^n + 1$; provámos que essa potência de 3 não excede $3^{1+v_3(n)}$, que por sua vez é menor ou igual a $3n$. Ora, $3n$ é "muito pequeno" relativamente a $5^n + 1$; como tal, a potência de 3 não pode "preencher uma grande parte" da factorização em primos de $5^n + 1$. Por outro lado, queremos precisamente que $5^n + 1$ seja "quase" uma potência de 3, e isto resulta numa contradição para n suficientemente grande.

Formalizar esta ideia levou a $5^n + 1 \leq 42n$. A forma como provámos que isto é falso para n suficientemente grande é um aspecto relativamente irrelevante da solução; há muitas formas de o fazer, e como atrás se referiu, o núcleo da solução é a forma como obtivemos esta desigualdade; o importante a reter é a capacidade de intuir que esta desigualdade é muito restritiva (falha para quase todos os possíveis n), muito mais do que a formalização deste facto.

O próximo exemplo é bastante semelhante a este.

Problema 3 (MOP 2001)**.** Encontrar todos os quartetos (x, r, p, n) de inteiros positivos tais que p é primo, $n, r > 1$ e

$$x^n - 1 = p^r.$$

Solução. Inicialmente parece que não temos reunidas as condições para aplicar o Lema do Levantamento do Expoente; a primeira ideia é tentar estimar $v_p(x^n - 1)$, mas não nos é dado que $p \mid x - 1$! Na verdade, quase que é: temos

$$x - 1 \mid x^n - 1 = p^r.$$

Então $x - 1$ é uma potência de p. Isto, contudo, ainda não resolve o nosso obstáculo, pois é possível que $x - 1 = 1$. Vamos assim começar por resolver o caso em que $x - 1 = 1$, ou seja, em que $x = 2$.

Temos $p^r + 1 = 2^n$. Se r é par, p^r é um quadrado perfeito ímpar que, como tal, é congruente com 1 módulo 4; logo, $p^r + 1 \equiv 2 \pmod 4$. Assim, só podemos ter $n = 1$, contradição com o enunciado. Logo, r é ímpar. Assim, $p + 1 \mid p^r + 1 = 2^n$; logo $p + 1$ é uma potência de 2. Por outro lado, temos $v_2(p^r + 1) = v_2(p^r + 1^r) = v_2(p + 1)$, já que r é ímpar (pelo que vimos no caso $p = 2$

do Lema). Assim, como $p+1$ e p^r+1 são ambos potências de 2, temos $p+1 = p^r+1$, pelo que $r = 1$, contradição com o enunciado.

Então $x \neq 2$, portanto já podemos supor que $p \mid x-1$ e podemos aplicar o Lema do Levantamento do Expoente. Temos

$$v_p(x^n - 1) = v_p(x-1) + v_p(n)$$

pelo que $r = v_p(x-1) + v_p(n)$. Mas $p^{v_p(x-1)+v_p(n)}$ é pequeno; $p^{v_p(x-1)+v_p(n)} = p^{v_p(x-1)} \cdot p^{v_p(n)} \leq n(x-1)$, já que $p^{v_p(x-1)} = x-1$ e $p^{v_p(n)}$ divide n. Novamente, tal como no exemplo anterior, obtivemos uma restrição forte baseada no facto de uma expressão da forma $a^n - b^n$ ser "quase" uma potência de um primo (na verdade, neste caso é mesmo uma potência de um primo): temos $x^n - 1 \leq n(x-1)$. Novamente devemos adivinhar que esta condição é altamente restritiva, já que o lado esquerdo tem aspecto de ser muito maior do que o direito. E, novamente, não é realmente importante como fazemos para provar tal coisa; em princípio qualquer tentativa vai funcionar. Uma possibilidade é observar que

$$x^n - 1 = (x-1)(x^{n-1} + \cdots + 1) \geq n(x-1)$$

e que, para a igualdade ocorrer, devemos ter $x = 1$, o que é impossível.

Assim, não existem soluções? Assim parece, mas $(x, r, p, n) = (3, 3, 2, 2)$ é claramente uma solução do problema! O que está mal, então? Esquecemo-nos de ver o caso em que $p = 2$, e de facto a nossa abordagem não funciona para esse caso. Se $p = 2$,

$$v_2(x^n - 1) = v_2(x-1) + v_2(x+1) + v_2(n) - 1$$

se n é par; mas n ímpar claramente não dá soluções, já que $v_2(x^n - 1) = v_2(x-1)$ nesse caso, e $x^n - 1$ e $x - 1$ são ambos potências de 2. Se $x - 1$ é divisível por 4, $v_2(x+1) = 1$ e temos $v_2(x^n - 1) = v_2(x-1) + v_2(n)$; a partir daqui, podemos mostrar de forma completamente análoga à do caso p ímpar que não há soluções. Assim, $x + 1$ é divisível por 4, pelo que $v_2(x-1) = 1$ e $v_2(x^n - 1) = v_2(x+1) + v_2(n)$. Portanto,

$$x^n - 1 = 2^{v_2(x+1)+v_2(n)} \leq n(x+1).$$

Estamos novamente perante uma desigualdade restritiva, portanto essencialmente podemos dar o problema por resolvido. Só precisamos de paciência; novamente, tudo o que tentarmos provavelmente funcionará, esta é apenas uma possível abordagem a esta parte final. Omitiremos desta vez as provas por indução das desigualdades do tipo exponencial $>$ linear.

Temos $x > 1$, e

$$x^n - 1 = (x-1)(x^{n-1} + \cdots + 1) \geq (x-1)(2^{n-1} + \cdots + 1) = (x-1)(2^n - 1)$$

mas é trivial verificar que se $x \geq 4$ então $\frac{x+1}{x-1} \leq \frac{5}{3}$, pelo que $2^n - 1 \leq \frac{5}{3}n$. Uma indução fácil mostra que não se verifica isto para $n \geq 3$. Assim, se $x \geq 4$ temos $n = 2$, e $x^2 - 1 \leq 2(x+1)$, o que é falso para $x \geq 4$.

Logo $x = 3$ ($x = 2$ é impossível pois $x^n - 1$ é uma potência de 2) e $3^n - 1 \leq 4n$, o que é falso se $n \geq 3$. Assim, $n = 2$, e obtemos a única solução $(x, r, p, n) = (3, 3, 2, 2)$. □

Concluimos com um exemplo final pouco relacionado com os anteriores.

Problema 4 (Irão 2008)**.** Seja a um inteiro positivo. Provar que se $4(a^n + 1)$ é um cubo perfeito para todo o inteiro positivo n, então $a = 1$.

Solução. Podemos reformular a condição do enunciado em termos de v_p's: queremos que $v_p(4(a^n + 1))$ seja múltiplo de 3 para todo o inteiro positivo n e todo o primo p. Isto equivale a que

- $v_p(a^n + 1) \equiv 0 \pmod 3$ se p é um primo diferente de 2;
- $v_2(a^n + 1) \equiv 1 \pmod 3$.

É então natural utilizar o Lema do Levantamento do Expoente; só falta assegurar que temos as condições para tal. Se $a + 1$ tem um divisor primo $p \neq 2$, para qualquer n ímpar temos

$$v_p(a^n + 1) = v_p(a + 1) + v_p(n)$$

e $v_p(n)$ pode tomar qualquer valor; podemos assim escolher n de modo que 3 não divide $v_p(a + 1) + v_p(n)$, e o problema está resolvido neste caso.

Mas falta resolver o caso em que $a + 1$ não tem nenhum divisor primo ímpar, ou seja, em que $a + 1$ é uma potência de 2. A princípio parece que este caso será facilmente resolvido de maneira semelhante, analisando desta vez v_2. Mas infelizmente (ou não) não será tão fácil: se n é ímpar, temos $v_2(a^n + 1) = v_2(a + 1)$ (e isso apenas nos garante que $v_2(a + 1) \equiv 1 \pmod 3$, mas não podemos concluir nada variando o n) e se n é par não podemos aplicar o Lema do Levantamento do Expoente, mas temos $a^n + 1 \equiv 1 + 1 \equiv 2 \pmod 4$, pelo que $v_2(a^n + 1) = 1 \equiv 1 \pmod 3$. Então só concluímos que a é da forma $2^{3k+1} - 1$; mas se isto se verificar, teremos $v_2(a^n + 1) \equiv 1 \pmod 3$ para todo o n, e portanto o expoente de 2 não dará qualquer contradição. Para $a = 15$, por exemplo, $4(a^n + 1)$ tem sempre um expoente de 2 divisível por 3.

Então, para obtermos contradição quando $a \neq 1$, precisamos mesmo de utilizar os primos ímpares; mas como podemos calcular $v_p(a^n + 1)$ com o Lema do Levantamento do Expoente quando p é um primo ímpar que não divide $a + 1$? A ideia será muito semelhante à do nosso primeiro exemplo: se existir um primo ímpar p tal que $p \mid a^2 + 1$, temos

$$v_p(a^{2m} + 1) = v_p(a^2 + 1) + v_p(m)$$

para qualquer inteiro positivo ímpar m. E $v_p(m)$ pode tomar qualquer valor, logo podemos escolher m de modo que $v_p(a^2 + 1) + v_p(m)$ não seja divisível por 3! Claro que, novamente, esta abordagem só funciona se $a^2 + 1$ não for uma potência de 2; mas $a^2 + 1$ não é divisível por 4, logo, se $a^2 + 1$ é uma potência de 2, temos que $a^2 + 1 = 2$ e portanto $a = 1$. E isto conclui o problema. □

2.1 Problemas propostos

Problema 5. Sejam α e β reais positivos distintos tais que, para todo o inteiro positivo n, $\alpha^n - \beta^n$ é inteiro. Provar que α e β são ambos inteiros.

Problema 6. Encontrar todos os inteiros positivos a tais que

$$\frac{5^a + 1}{3^a}$$

é inteiro.

Problema 7 (Teste Delfos 2012)**.** Para que inteiros positivos n é que o número

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

é divisível por n^n?

Problema 8 (Ibero 2000)**.** Encontrar todas as soluções inteiras positivas (x, y, z) da equação

$$(x+1)^y - x^z = 1.$$

Problema 9 (IMO Shortlist 2000)**.** Encontrar todos os tripletos (a, m, n) de inteiros positivos tais que $a^m + 1$ divide $(a+1)^n$.

Problema 10 (IMO Shortlist 2005)**.** Encontrar todos os inteiros positivos n com a seguinte propriedade: existe um e apenas um inteiro a satisfazendo $0 \leq a < n!$ tal que $a^n + 1$ é divisível por $n!$.

Problema 11 (IMO Shortlist 2014)**.** Seja $n > 1$ um inteiro. Provar que existe uma infinidade de termos da sucessão $(a_k)_{k \geq 1}$, definida por

$$a_k = \left\lfloor \frac{n^k}{k} \right\rfloor,$$

que são ímpares.

Problema 12 (IMO Shortlist 2014)**.** Encontrar todos os tripletos (x, y, p) de inteiros positivos, tais que p é primo e ambos os números

$$x + y^{p-1}, x^{p-1} + y$$

são potências de p.