Três VIPs da Teoria dos Números

É claro, "VIP" significa "**V**ery **I**mportant **P**roblems". Os problemas discutidos aqui, além de suas variações, são bastante comuns em Olimpíadas de Matemática e costumam ser resolvidos com técnicas bem definidas.

As duas primeiras partes tratam de problemas de divisibilidade; a terceira e última parte é sobre problemas de expoente.

1. Problemas de divisibilidade

Os problemas de divisibilidade vêm desde o primeiro problema de todas as IMOs (veja o problema 2) e ainda estão presentes (até o momento, sua última aparição na IMO foi em 2003; 2007 se contarmos a próxima parte).

Utilizaremos a seguinte terminologia para simplificar as coisas: quando $a \mid b$ diremos que a é o *divisor* e b é o *múltiplo*.

A resolução desses problemas pode geralmente ser feita com o seguinte procedimento:

Problemas de divisibilidade 1

Passo 1 Reduza o grau do múltiplo usando combinação linear;

Passo 2 Quando o grau do múltiplo é menor do que o grau do divisor, aplique a propriedade $d \mid a \implies |d| \le |a|$ ou $a = 0$ e encontre um limitante superior (pequeno, se possível) para algumas variáveis;

Passo 3 Estude os casos obtidos e, se necessário, aplique os passos 1 e 2 novamente.

Isso vai ficar mais claro após vermos o nosso primeiro exemplo, que é o problema 4 da IMO 1998:

Exemplo 1.1.

Determine todos os pares (x, y) de inteiros positivos tais que $x^2y + x + y$ é divisível por $xy^2 + y + 7$.

Resolução

Primeiro, note que o grau de ambos o divisor e o múltiplo é 3. Vamos então reduzir o grau do múltiplo, utilizando combinação linear. A ideia é cancelar os termos com grau máximo multiplicando o divisor e o múltiplo por números convenientes. Como $xy^2 + y + 7 \mid x^2y + x + y$ os termos de grau máximo são xy^2 e x^2y, multiplixamos o divisor por $-x$ e o múltiplo por y:

$$xy^2 + y + 7 \mid (x^2y + x + y) \cdot y + (xy^2 + y + 7) \cdot (-x) \iff xy^2 + y + 7 \mid y^2 - 7x$$

Já conseguimos um múltiplo com grau menor do que o divisor (2 contra 3). Se não conseguíssemos, a ideia seria continuar com o mesmo procedimento. Isso é essencialmente o Passo 1.

Vamos agora ao Passo 2. Como $d \mid a \implies |d| \le |a|$ or $a = 0$,

$$xy^2 + y + 7 \mid y^2 - 7x \implies xy^2 + y + 7 \le |y^2 - 7x| \text{ ou } y^2 - 7x = 0$$

Temos três casos:

Primeiro caso: $y^2 - 7x = 0$. Temos $x = 7k^2$ e $y = 7k$, $k \in Z_+^*$, e é fácil verificar que $(7k^2, 7k)$ forma uma família de soluções.

Segundo caso: $y^2 - 7x > 0 \implies |y^2 - 7x| = y^2 - 7x$. Não há soluções nesse caso, pois $x \ge 1$ e $y + 7 > 0$, de modo que $xy^2 + y + 7 > y^2 > y^2 - 7x$, absurdo.

Terceiro caso: $y^2 - 7x < 0 \implies |y^2 - 7x| = 7x - y^2$. A desigualdade é equivalente a $(7 - y^2)x \ge y^2 + y + 7$, que implica $7 - y^2 > 0$, ou seja, $y = 1$ ou $y = 2$. Em todo caso temos um problema de divisibilidade de uma variável só: para $y = 1$, temos $x + 8 \mid 7x - 1$, assim $x + 8 \mid 7x - 1 - 7(x + 8) \iff x + 8 \mid 57 \implies x = 11$ ou $x = 49$. Ambos $(11, 1)$ e $(49, 1)$ soluções; para $y = 2$, temos $4x + 9 \mid 7x - 4$ e o leitor deve verificar que não há soluções nesse caso.

As soluções são então $(11, 1)$, $(49, 1)$ e $(7k^2, 7k)$, $k \in Z_+^*$.

A principal razão pela qual essa abordagem costuma funcionar bem é na verdade o Passo 2, que nos permite limitar uma variável. Polinômios com grau maior tendem a ser muito maiores do que polinômios com grau menor, então se o divisor é um polinômio com grau maior do que o do múltiplo normalmente é possível obter um limitante superior para alguma variável.

Em alguns problemas, nem sempre esse limitante é fácil de se obter. Nessas horas,

1.1. A diferença faz a diferença

O próximo exemplo é o Problema 2 da IMO 2003.

Exemplo 1.2.

Determine todos os pares de inteiros positivos (a, b) tais que $\frac{a^2}{2ab^2 - b^3 + 1}$ é um inteiro positivo.

Resolução

Note que o grau do divisor já é maior do que o grau do múltiplo. Infelizmente, isso não resolve o problema, porque o divisor ainda pode ser pequeno: se $b = 2a$ ele é igual a 1! O que nos leva à nossa primeira família infinita de soluções: $(n, 2n)$, n inteiro positivo.

Suponha então que $b \ne 2a$. Então $2a > b$, pois a^2 e $2ab^2 - b^3 + 1 = b^2(2a - b) + 1$ são ambos positivos. Em vez de nos perguntarmos o tempo todo “estamos utilizamos a desigualdade $2a > b$?”, o fazemos *automaticamente* com a substituição $k = 2a - b > 0$.

Essa substituição parece boba, mas faz o problema ficar bem mais fácil: obtemos $\frac{a^2}{2ab^2 - b^3 + 1} = \frac{(b+k)^2}{4(b^2k+1)}$ e obtemos um problema com o qual estamos mais acostumados.

Mas o problema requer ainda um pouco mais de trabalho. Primeiro separe o caso $b = 1$, que nos leva à nossa segunda família infinita de soluções $(2n, 1)$, n inteiro positivo (substitua $b = 1$ diretamente no problema original para verificar!). Suponha então que $b \ge 2$. Temos $4(b^2k + 1) \le (b + k)^2$, que nos dá a estimativa $k \ge 4b^2 - 2b$. Essa estimativa não parece muito interessante, então procuremos outra. Você pode provar (tente!) que $b^2k + 1 \mid b^4 - 2b - k$ e o Passo 2 nos dá nossa terceira família infinita de soluções $(8n^4 - n, 2n)$, n inteiro positivo e, caso contrário, outra estimativa $k \le b^2 - 2$. Isso implica $b^2 - 2 \ge 4b^2 - 2b$, absurdo.

Então as soluções são $(n, 2n)$, $(2n, 1)$, $(8n^4 - n, 2n)$, n inteiro positivo.

Observação: Essas estimativas polinomiais não foram questão de sorte. Você precisa fazer algumas divisões de polinômios e fazer algumas estimativas. Algumas são bastante fracas, como $b^2 - 4 \ge 0$, por exemplo.

Exercícios

01. E se $\frac{a^2}{2ab^2 - b^3 + 1}$ pudesse ser inteiro qualquer? Resolva o problema nesse caso.

02. Seja n inteiro. Prove que a fração $\frac{21n+4}{14n+3}$ é irredutível.

Observação: Esse é o primeiro problema na primeira IMO, e é só uma aplicação direta de combinação linear.

03. (Problema 1, IMO 1992) Encontre todos os inteiros a, b, c, $1 < a < b < c$, tais que $(a-1)(b-1)(c-1)$ é um divisor $abc - 1$.

Dica: Faça $x = a - 1$, $y = b - 1$, $z = c - 1$.

04. (Problema 4, IMO 1994) Encontre todos os pares ordenados (m, n) em que m e n são inteiros positivos tais que $\frac{n^3+1}{mn-1}$ é um inteiro.

05. Encontre todos os inteiros que podem ser expresso unicamente na forma $\frac{x^2+y}{xy+1}$, x e y inteiros positivos.

06. (APMO) Encontre todos os inteiros positivos m e n tais que $\frac{m^2+n}{n^2-m}$ e $\frac{n^2+m}{m^2-n}$ são ambos inteiros.

Você deve estar se perguntando: "E se eu não conseguir aplicar o Passo 2?" Então você deve estar enfrentando

2. Problemas com root-flipping

Nesse caso, geralmente temos infinitas soluções. Uma ideia é reduzir todas as soluções a um conjunto finito (e preferivelmente pequeno) de soluções finitas usando equações do segundo grau.

O próximo exemplo é da IMO 2007.

Exemplo 2.1.

Sejam a e b inteiros positivos. Prove que se $4ab - 1$ divide $(4a^2 - 1)^2$, então $a = b$.

Resolução

Quando você sabe que está lidando com problemas de root-flipping? Uma evidência é quando o máximo que você consegue ao reduzir o grau do múltiplo é obter $4ab - 1 \mid (a-b)^2$. O que fazer?

Root-flipping

Passo 1 Seja $k = \frac{\text{múltiplo}}{\text{divisor}}$. Reescreva essa equação como uma equação de segundo grau em uma das variáveis.

Passo 2 Seja (a_0, b_0) uma solução minimal (a_0 minimal, b_0 minimal, $a_0 + b_0$ minimal, o que fizer as contas mais fáceis). Encontre outra solução usando soma e/ou produto da equação do segundo grau (isso é o "root-flipping").

Passo 3 Use o fato de que (a_0, b_0) é minimal para obter uma desigualdade.

Passo 4 Encontre os possíveis valores de (a_0, b_0) usando a desigualdade ou obtenha uma contradição.

Como usual, esse procedimento fica mais claro após vê-lo em ação. Seja $k = \frac{(a-b)^2}{4ab-1}$. Então $a^2 - (4kb + 2b)a + (b^2 + k) = 0$ $(*)$ (esse é o Passo 1). Note que todas as soluções (a, b) do problema original satisfaz $(*)$ para algum inteiro k.

Seja (a_0, b_0) uma solução minimal. O que vai ser minimal vai ser decidio mais tarde (não dá para prever as contas agora). Sejam a_0 e a_1 as raízes de $(*)$. Então $a_0 + a_1 = 4kb_0 + 2b_0$ e $a_0 \cdot a_1 = b_0^2 + k$. Vamos trabalhar com $a_1 = \frac{b_0^2+k}{a_0}$ (na verdade, trabalhar com a outra relação dá o mesmo resultado). Note que $a_1 = 4kb_0 + 2b_0 - a_0$ é inteiro positivo. Esse é o Passo 2.

Agora estamos prontos para decidir o que vai ser minimal e, além disso, considerando a simetria do problema, qual dos números a_0 e b_0 é maior. Como estamos lidando com a_1 e a_0, é natural considerarmos

a_0 minimal, assim $a_1 \geq a_0 \iff b_0^2 + k \geq a_0^2$. Mas podemos supor também, ser perda de genaralidade, que $a_0 > b_0$ e temos $k \geq a_0^2 - b_0^2$. Esse é o Passo 3.

E agora vamos ao Passo 4. Lembre que $k = \frac{(a_0-b_0)^2}{4a_0b_0-1}$. Substituindo e cancelando $a_0 - b_0$ obtemos $\frac{a_0-b_0}{4a_0b_0-1} \geq a_0 + b_0$, que é uma contradição, pois $\frac{a_0-b_0}{4a_0b_0-1} \leq a_0 - b_0 < a_0 + b_0$. Então não podíamos ter $a_0 > b_0$ nem cancelado $a_0 - b_0$, porque na verdade $a_0 = b_0$. Logo $k = 0$ e, portanto, $a = b$.

Exercícios

07. (Problema 6, IMO 1988) Sejam a e b inteiros positivos tais que $ab + 1$ divide $a^2 + b^2$. Prove que $\frac{a^2+b^2}{ab+1}$ é um quadrado perfeito.

Observação: Ninguém do comitê seletor de problemas da IMO daquele ano resolveu o problema. Ainda assim, alguns alunos resolveram o problema durante a prova.

08. Sejam a e b inteiros positivos tais que $\frac{a^2+b^2+1}{ab}$ é inteiro. Prove esse inteiro é 3.

09. (Romênia, Teste de Seleção) Sejam a e b inteiros positivos tais que $ab \neq 1$. Encontre todos os valores inteiros de $f(a, b) = \frac{a^2+ab+b^2}{ab-1}$.

10. (Brasil, 1996) Prove que a equação $x^2 + y^2 + z^2 = 3xyz$ tem infinitas soluções inteiras.

11. Seja m inteiro positivo. Mostre que existem infinitos pares (a, b) de inteiros positivos tais que a divide $b^2 + m$ e b divide $a^2 + m$.

12. (IMO Shortlist, 2002) Existe um inteiro positivo m tal que a equação $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{abc} = \frac{m}{a+b+c}$ é satisfeita por infinitos inteiros positivos a, b, c?

13. (EUA, Teste de Seleção 2009) Encontre todos os pares de inteiros positivos (m, n) tais que $mn - 1$ divide $(n^2 - n + 1)^2$.

Até agora só resolvemos problemas de divisibilidade envolvendo polinômios. Mas o que fazer se a variável estiver no expoente?

3. Problemas de expoente

Se uma variável está no expoente, geralmente utilizamos o pequeno teorema de Fermat, ordem e lema de Hensel.

Pequeno teorema de Fermat. *Se p é primo e a não é múltiplo de p então $a^{p-1} \equiv 1 \pmod{p}$.*

Demonstração

É um caso particular do teorema de Euler-Fermat. ∎

Definição 3.1. *Sejam a e m inteiros primos entre si. A ordem de a módulo m, denotado por $\operatorname{ord}_m a$, é o menor inteiro positivo d tal que $a^d \equiv 1 \pmod{m}$.*

Propriedade da ordem (o menor divide). $a^x \equiv a^y \pmod{m} \iff x \equiv y \pmod{\operatorname{ord}_m a}$. *Em particular,* $a^t \equiv 1 \pmod{m} \iff \operatorname{ord}_m a \mid t$.

Demonstração

Divida t por $\operatorname{ord}_m a$, ou seja, $t = q \cdot \operatorname{ord}_m a + r$, $0 \leq r < \operatorname{ord}_m a$. Então $a^t = (a^{\operatorname{ord}_m a})^q a^r \equiv 1 \pmod{m} \implies a^r \equiv 1 \pmod{m}$. Como $\operatorname{ord}_a m$ é mínimo e $r < \operatorname{ord}_m a$, então r deve ser zero. Isso prova o caso particular. O caso geral pode ser reduzido a esse caso: $a^x \equiv a^y \pmod{m} \iff a^{x-y} \equiv 1 \pmod{m}$. ∎

Corolário. $\text{ord}_m a \mid \phi(m)$. *Em particular, se p é primo,* $\text{ord}_p a \mid p-1$.

Demonstração

Basta utilizar o último fato e o teorema de Euler-Fermat. ∎

Definição 3.2. *Dizemos que p^α divide exatamente m e denotamos por $p^\alpha \parallel m$ o fato de que m tem exatamente α fatores primos p.*

O próximo teorema nos diz que se sabemos quantos fatores p primo $a \pm 1$ e n têm então sabemos quantos fatores p o número $a^n \pm 1$ tem. E não são muitos!

Lema de Hensel. *Seja p primo ímpar, a inteiro, n inteiro positivo. Se $p^\alpha \parallel a-1$, $\alpha > 0$ e $p^\beta \parallel n$ então $p^{\alpha+\beta} \parallel a^n - 1$. Além disso, se n é ímpar, $p^\alpha \parallel a+1$, $\alpha > 0$ e $p^\beta \parallel n$ então $p^{\alpha+\beta} \parallel a^n+1$.*

Demonstração

Indução em β, utilizando o binômio de Newton (faça as contas!). ∎

Note que esse lema nos diz que $a^n \pm 1$ tem tantos fatores p quanto $(a \pm 1)n$. Isso é propício para diminuir mdc, obter desigualdades...

Problemas com expoentes podem ser resolvidos com o seguinte "algoritmo":

Problemas com expoentes

Passo 1 Fatore o expoente n em primos, digamos $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, com $p_1 < p_2 < \cdots < p_k$.

Passo 2 Faça $i = 1$.

Passo 3 *(Ordem e progresso)* Encontre p_i, usando o teorema de Fermat e ordem.

Passo 4 Encontre α_i, usando o lema de Hensel.

Passo 5 Se encontramos uma contradição em algum dos dois passos anteriores, terminamos. Caso contrário, faça $i = i+1$ e volte ao Passo 3. Se for o caso, prove que é possível continuar indefinidamente por indução.

Começamos com esse problema da IMO 1990, que na época foi considerado uma grande inovação.

Exemplo 3.1.

Encontre todos os inteiros positivos n tais que $\frac{2^n+1}{n^2}$ é inteiro.

Resolução

Note primeiro que $n = 1$ é uma solução. Suponha agora que $n > 1$. Seja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, com $p_1 < p_2 < \cdots < p_k$.

Encontremos p_1. Note que como $n^2 \mid 2^n + 1$, $p_1 \mid 2^n + 1 \iff 2^n \equiv -1 \pmod{p_1} \implies 2^{2n} \equiv 1 \pmod{p_1}$. Seja $d_1 = \text{ord}_{p_1} 2$. Então $d_1 \mid 2n$, d_1 não divide n e $d_1 \mid p_1 - 1$. Logo $d_1 \mid \text{mdc}(2n, p_1 - 1)$. Mas note que $p_1 - 1$ é menor do que qualquer fator primo de n, de modo que não pode ter divisores comuns com n. Portanto $\text{mdc}(2n, p_1 - 1) \mid 2$, e temos $d_1 \mid 2 \implies 2^2 \equiv 1 \pmod{p_1} \implies p_1 = 3$.

Agora vamos ao lema de Hensel. Coom $3 \parallel 2+1$ e $3^{\alpha_1} \parallel n$, pelo lema de Hensel $3^{1+\alpha_1} \parallel 2^n + 1$. Mas $3^{2\alpha} \parallel n^2$, logo $2\alpha_1 \le 1 + \alpha_1 \implies \alpha_1 = 1$.

Nenhuma contradição, então encontremos p_2. Novamente, $2^n \equiv -1 \pmod{p_2}$ e $2^{2n} \equiv 1 \pmod{p_2}$. Seja $n_2 = n/3 = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ e $d_2 = \operatorname{ord}_{p_2} 2$. Logo $d_2 \mid 6n_2$, d_2 não divide $3n_2$ e $d_2 \mid p_2 - 1$. Como todos os divisores primos de n_2 são maiores do que $p_2 - 1$, $d_2 \mid 6$ e d_2 não divide 3. Portanto $2^6 \equiv 1 \pmod{p_2} \implies p_2 = 7$. Isso é uma contradição porque $d_2 = \operatorname{ord}_7 2 = 3$ e d_2 não divide 3.

Portanto não há p_2 (e primos maiores também), e as únicas soluções são $n = 1$ e $n = 3$.

Achamos que esse material não estaria completo sem um exemplo em que o "algoritmo" continue indefinidamente (e é por isso que "algoritmo" está entre aspas). O próximo problema, da IMO 2000, é um exemplo disso.

Exemplo 3.2.

Existe um inteiro positivo n tal que n tem exatamente 2000 divisores primos e n divide $2^n + 1$?

Resolução

Seja (novamente) $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, com $p_1 < p_2 < \cdots < p_k$.

Exatamente como no exemplo anterior, encontramos $p_1 = 3$. Mas agora o divisor é n em vez de n^2, então podemos escolher α_1 **qualquer**. Isso é indicativo que a resposta ao problema deve ser *sim*, então vamos tentar encontrar valores possíveis para p_2, p_3, ..., p_{2000}.

Nesse caso, indução geralmente vai bem, como em muitos outros problemas de Teoria dos Números. Suponha que já encontramos m fatores primos,isto é, suponha que já encontramos $n_m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ tal que $n_m \mid 2^{n_m} + 1$. Vamos encontrar p_{m+1}.

Como? Basta seguir o nosso "algoritmo"! Primeiro, vamos provar que é possível encontrar p_{m+1}. Primeiro vamos ver **onde** procurar esse primo. Temos, como usual, $p_{m+1} \mid 2^{n_{m+1}} + 1 \iff 2^{n_{m+1}} \equiv -1 \pmod{p_{m+1}} \implies 2^{2n_{m+1}} \equiv 1 \pmod{p_{m+1}}$. Seja $d_{m+1} = \operatorname{ord}_{p_{m+1}} 2$. Então $d_{m+1} \mid 2n_{m+1}$, $d_{m+1} \mid p_{m+1} - 1$ mas d_{m+1} não divide n_{m+1}. Novamente, como $n_{m+1} = p_{m+1}^{\alpha_{m+1}} n_m$, temos na verdade $d_{m+1} \mid 2n_m$ e que d_{m+1} não divide n_m. Então $2^{2n_m} \equiv 1 \pmod{p_{m+1}} \iff (2^{n_m})^2 \equiv 1 \pmod{p_{m+1}} \iff 2^{n_m} \equiv \pm 1 \pmod{p_{m+1}}$ (é por isso que trabalhar módulo primo é muito melhor! Isso não vale para compostos). Mas $2^{n_m} \not\equiv 1 \pmod{p_{m+1}}$ (caso contrário, d_{m+1} dividiria n_m), então $2^{n_m} \equiv -1 \pmod{p_{m+1}}$. Logo p_{m+1} deve dividir $2^{n_m} + 1$. Como p_{m+1} não divide n_m, concluímos que p_{m+1} divide... $\frac{2^{n_m}+1}{n_m}$! E tem mais: **qualquer** divisor primo de $\frac{2^{n_m}+1}{n_m}$ funciona. Por quê? Note que p_{m+1} e n_m dividem $2^{n_m}+1$; como $\operatorname{mdc}(p_{m+1}, n_m) = 1$, $n_m p_{m+1}$ divide $2^{n_m} + 1$, que divide $(2^{n_m})^{p_{m+1}} + 1 = 2^{n_m p_{m+1}} + 1$. Então, nosso próximo divisor primo pode ser qualquer divisor primo de $\frac{2^{n_m}+1}{n_m}$! Legal, não? Vamos ver de novo o exemplo anterior, a título de ilustração: encontrar p_2 tornou-se impossível no momento que encontramos que $\alpha_1 = 1$: $\frac{2^3+1}{3} = 3$ não tem novos primos!

E nessa hora, os pessimistas podem perguntar "ei, e se $\frac{2^{n_m}+1}{n_m}$ não tiver novos fatores primos?" Nós, os otimistas, respondemos primeiro que $\frac{2^{3^2}+1}{3^2} = 3 \cdot 19$. Na verdade, o fato de que podemos escolher **qualquer** α_1 no primeiro passo agora parece **crucial** para o problema. Então, vamos colocar esse fato na hipótese de indução (isso é frequente em induções: precisa de outro fato? Inclua-o na hipótese de indução!). Então agora temos que encontrar p_{m+1} E provar que podemos escolher α_{m+1} **qualquer**.

Como conseguir novos primos? Resposta: mdc pequeno! Coloque outro fator p_m em n_m, ou seja, considere $n_m \cdot p_m$. Da nossa (nova e estendida) hipótese de indução, $n_k p_k$ divide $2^{n_k p_k} + 1$ e podemos escolher qualquer divisor primo de $\frac{2^{n_k p_k}+1}{n_k p_k}$. Temos $\frac{2^{n_m p_m}+1}{2^{n_m}+1} = (2^{n_m})^{p_m-1} - (2^{n_m})^{p_m-2} + \cdots + 1 \equiv (-1)^{p_m-1} - (-1)^{p_m-2} + \cdots + 1 = p_m \pmod{2^{n_m}+1}$, então $\operatorname{mdc}(\frac{2^{n_m p_m}+1}{2^{n_m}+1}, 2^{n_m}+1)$ divide p_m e é pequeno comparado a $\frac{2^{n_m p_m}+1}{2^{n_m}+1}$ (faça as contas para verificar isso!). Então deve existir um primo novo entre os divisores de $\frac{2^{n_m p_m}+1}{2^{n_m}+1}$. Nenhum deles divide $n_m p_m$, então esse novo primo p_{m+1} também aparece em $\frac{2^{n_m p_m}+1}{n_m p_m}$.

Agora vamos provar que podemos escolher α_{m+1} qualquer. Isso é mais um trabalho para o nosso "algoritmo": como $p_{m+1}^t \parallel 2^{n_m} + 1$ para algum $t > 0$, pelo lema de Hensel $p_{m+1}^{\alpha_{m+1}+t} \parallel 2^{n_m p_{m+1}^{\alpha_{m+1}}} + 1$. Ou seja, se $n_{m+1} = n_m p_{m+1}^{\alpha_{m+1}}$ então $n_{m+1} \mid 2^{n_{m+1}} + 1$ para todo α_{m+1}. Faça $m = 2000$ e o problema terminou.

Exercícios

14. Seja $n > 1$ um inteiro. Prove que n não divide $2^n - 1$.

15. (IMO 1999, Problema 4) Encontre todos os pares de inteiros positivos (n, p) tais que p é primo, $n \leq 2p$ e n^{p-1} é um divisor de $(p-1)^n + 1$.

Observação: Na verdade você pode ignorar a condição $n \leq 2p$ e resolver o problema.

16. (IMO 2003, Problema 6) Seja p um número primo. Prove que existe um número primo q tal que, para todo inteiro n, o número $n^p - p$ não é divisível por q.

Dica: Tente encontrar q tal que $p^{\frac{q-1}{p}} \not\equiv 1 \pmod{q}$. Sendo mais específico: encontre q tal que $p = \operatorname{ord}_q p$ e $q \not\equiv 1 \pmod{p^2}$.

17. (IMO Shortlist, 1997) Sejam b, m, n inteiros positivos tais que $b > 1$ e $m \neq n$. Prove que se $b^m - 1$ e $b^n - 1$ têm os mesmos divisores primos então $b + 1$ é uma potência de 2.

18. (IMO Shortlist, 2000) Encontre todos os inteiros positivos a, m, n tais que $a^m + 1$ divide $(a+1)^n$.

Dica: Lema de Hensel em ação! Aliás, esse problema é brasileiro!

19. (IMO Shortlist, 2001) Seja $p > 3$ um primo. Mostre que existe um inteiro positivo $n < p - 1$ tal que $n^{p-1} - 1$ e $(n+1)^{p-1} - 1$ não são divisíveis por p^2.