O PROBLEMA 6 DA IMO DE 1990 E O LEMA DE HENSEL

RICARDO BORTOLOTTI

O objetivo deste texto é resolver o Problema 6 da IMO de 1990:

Problema 1 (P6 - IMO 1990)**.** *Determine todos os inteiros positivos n para os quais*

$$\frac{2^n+1}{n^2}$$

é inteiro.

As ferramentas necessária para a resolução deste problema serão:

(1) **Teorema Fundamental da Aritmética:** Todo inteiro $n \geq 2$ pode ser escrito unicamente na forma

$$\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}},$$

aonde $p_1 < p_2 < \cdots < p_k$ são primos e $\alpha_1, \alpha_2, \cdots, \alpha_k \geq 1$.

(2) **Teorema de Fermat:** Se p é primo e não divide a, então

$$\boxed{a^{p-1} \equiv 1 (\mathrm{mod}\, p)}.$$

(3) **Fórmula do binômio de Newton:** $\boxed{(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}}$.

(4) **Teorema de Bézout:** Seja $d = \mathrm{mdc}(a,b)$, então existem inteiros x_1 e y_1 tais que $d = ax_1 + by_1$.

(5) Uma consequência do Teorema de Bézout: se $a^x \equiv 1(\mathrm{mod}\, m)$ e $a^y \equiv 1(\mathrm{mod}\, m)$, então $a^{\mathrm{mdc}(x,y)} \equiv (a^x)^{x_1}(a^y)^{y_1} \equiv 1(\mathrm{mod}\, m)$.

1. Um problema mais simples

Vamos começar com um Problema mais simples:

Problema 2. *Determine todos os inteiros positivos n para os quais*

$$\frac{2^n-1}{n}$$

é inteiro.

Solução do Problema 2: Como $n = 1$ é uma resposta, vamos supor que $n \geq 2$.
Utilizando o Teorema Fundamental da Aritmética, escrevemos n na forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.
Claramente n deve ser um número ímpar, pois $2^n - 1$ é ímpar.

Supondo que $\frac{2^n-1}{n}$ é inteiro, e como 2 não divide n, então

$$2^n \equiv 1(\mathrm{mod}\, n). \tag{1}$$

Utilizando o Teorema de Fermat, temos algo mais sobre p_1 (o menor fator primo de n):

$$2^{p_1-1} \equiv 1(\mathrm{mod}\, p_1). \tag{2}$$

Juntando (1) e (2), podemos utiliar a consequência do teorema de Bézout para concluir:

$$2^{\mathrm{mdc}(n,p_1-1)} \equiv 1(\mathrm{mod}\, p_1) \tag{3}$$

Porém p_1 é o menor fator de n!!! Isto significa que $p_1 - 1$ não tem nenhum divisor em comum com n, portanto $\mathrm{mdc}(n, p_1 - 1) = 1$. Logo, (3) se torna:

$$2^1 \equiv 1(\mathrm{mod}\, p_1) \quad \Leftrightarrow \quad p_1|2^1 - 1 = 1.$$

Então $p_1|1 \Rightarrow p_1 = 1$, o que é impossível. Portanto, a única solução para este problema é $n = 1$.

2. Resolução do Problema 1

Nesta Seção, vamos agora resolver o Problema 1, descrevendo em cada subseção um passo importante.

2.1. **Começar de forma idêntica ao problema anterior:** Como $n = 1$ é solução, supomos que $n \geq 2$.

Utilizando o Teorema Fundamental da Aritmética, escrevemos n na forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, com $p_1 < p_2 < \cdots < p_k$.

Devemos notar que n deve ser um número ímpar, pois $2^n + 1$ é ímpar, isso significa que $p_1 \geq 3$.

Supondo que $\frac{2^n+1}{n^2}$ é inteiro, e como 2 não divide n, então

$$2^n \equiv -1(\mathrm{mod}\, n^2). \tag{4}$$

Vamos utilizar o Teorema de Fermat para concluirmos algo mais sobre p_1 (o menor fator primo de n):

$$2^{p_1-1} \equiv 1(\mathrm{mod}\, p_1). \tag{5}$$

Até aqui tudo igual, porém agora não podemos usar a consequência do teorema de Bézout pois o lado direito de (4) não é 1. Mas elevando (4) ao quadrado, obtemos: $2^{2n} \equiv 1(\mathrm{mod}\, n^2) \Rightarrow n^2|2^{2n} - 1 \Rightarrow p_1|2^{2n} - 1$ e portanto:

$$2^{2n} \equiv 1(\mathrm{mod}\, p_1) \tag{6}$$

Agora sim, juntando (6) e (5) e utilizando a consequência do teorema de Bézout, concluimos:

$$2^{\mathrm{mdc}(2n,p_1-1)} \equiv 1(\mathrm{mod}\, p_1) \tag{7}$$

2.2. **Concluír que $p_1 = 3$:** Novamente, p_1 é o menor fator de n. Isto significa que $p_1 - 1$ não tem nenhum divisor em comum com n, mas pode dividir 2.

O que concluímos é que $\mathrm{mdc}(2n, p_1 - 1) = 1$ ou 2. Logo, (7) se torna:

$$2^1 \equiv 1(\mathrm{mod}\, p_1) \quad \text{ou} \quad 2^2 \equiv 1(\mathrm{mod}\, p_1).$$

No primeiro caso, $p_1|2^1 - 1 = 1 \Rightarrow p_1 = 1$, o que é impossível. Portanto, devemos ter $p_1|2^2 - 1 = 3 \Rightarrow p_1 = 3$.

2.3. **Concluír que $\alpha_1 = 1$:** Até aqui chegamos com idéias similares às da resolução do Problema 2. O passo seguinte consiste em descobrir algo sobre o expoente α_1.

Podemos escrever, alternativamente, $n = 3^{\alpha_1} l$, aonde $\mathrm{mdc}(6, l) = 1$.

A condição do enunciado equivale a: existe algum inteiro q tal que

$$2^{3^{\alpha_1} l} = 3^{2\alpha_1} l^2 q - 1. \tag{8}$$

Neste passo, investigaremos qual é o maior expoente β com a propriedade de que $2^{3^\beta l}$ divide $3^{2\alpha_1} l^2 q - 1$.

Lema 1. *Considere l fixado tal que $\mathrm{mdc}(6, l) = 1$. Seja $\beta(m)$ o maior inteiro β tal que 3^β divide $2^{3^m l} + 1$, então $\beta(m+1) = 1 + \beta(m)$. Em particular, $\beta(m) = 1 + m$.*

Prova do Lema 1: Fixado m, seja q tal que $2^{3^m l} = 3^{\beta(m)} q - 1$ e q não é múltiplo de 3. Então, pelo binômio de Newton (lembra que dissémos na primeira página que o utilizaríamos?):

$$\begin{aligned} 2^{3^{m+1} l} &= (3^{\beta(m)} q - 1)^3 \\ &= 3^{3\beta(m)} q^3 - 3 \cdot 3^{2\beta(m)} q^2 + 3 \cdot 3^{\beta(m)} q - 1 \\ &= 3^{\beta(m)+1} (3^{2\beta(m)-1} q^3 - 3^{\beta(m)} q^2 + q) - 1 \\ &= 3^{\beta(m)+1} \tilde{q} - 1, \end{aligned}$$

aonde $\tilde{q} = 3^{2\beta(m)-1} q^3 - 3^{\beta(m)} q^2 + q \equiv q (\mathrm{mod}\, 3)$ não é múltiplo de 3. Portanto $\beta(m+1) = \beta(m) + 1$.

O resultado final segue por indução em m. Para $m = 1$, podemos ver que $2^{3l} + 1 = 8^l + 1 \equiv 8 + 1 \equiv 0 (\mathrm{mod}\, 3^2)$ e $2^{3l} + 1 = 8^l + 1 \equiv 9 (\mathrm{mod}\, 3^3)$. Portanto $\beta(1) = 2$ e a relação $\beta(m+1) = \beta(m) + 1$ implica $\beta(m) = 1 + m$. □

Aplicando o Lema 1 para a equação (8), do fato que $3^{2\alpha_1}$ divide $2^{3^{\alpha_1} l} + 1$, concluímos que

$$2\alpha_1 \leq \beta(\alpha_1) = \alpha_1 + 1, \tag{9}$$

o que implica que $\alpha_1 \leq 1$ e, portanto, $\alpha_1 = 1$. (lembre-se de que todos os α_j são maiores ou iguais a 1).

Note que $n = 3$ é também uma solução do problema.

2.4. **Concluír que $p_2 = 7$:** Já sabemos que $n = 1$ e $n = 3$ são soluções do problema. Vamos supor que n é outra solução que admite um segundo fator primo além de $p_1 = 3$.

Então $n = 3 p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Vamos repetir os passos anteriores agora para calcular p_2 e estimar α_2.

De forma ao similar ao passo em que concluímos (5), (6) e (7), temos pelo Teorema de Fermat:

$$2^{p_2 - 1} \equiv 1 (\mathrm{mod}\, p_2). \tag{10}$$

Pela condição $n^2 | 2^n + 1$, segue:

$$2^{2n} \equiv 1 (\mathrm{mod}\, p_2). \tag{11}$$

Juntando (10) e (11), temos:

$$2^{\mathrm{mdc}(p_2 - 1, 2n)} \equiv 1 (\mathrm{mod}\, p_2). \tag{12}$$

Agora temos que analisar quais são os possíveis valores de $\mathrm{mdc}(p_2 - 1, 2n)$, lembrando que p_2 é o segundo menor fator primo de n. Como $p_2 - 1$ é menor que p_2, os fatores em comum

que $p_2 - 1$ pode ter em comum com $2n$ são 2 e $p_1 = 3$, portanto $\text{mdc}(p_2 - 1, 2n)$ pode ser igual a 1, 2, 3 ou 6. Então:

$$2^1 \equiv 1(\text{mod}\, p_2) \quad \text{ou} \quad 2^2 \equiv 1(\text{mod}\, p_2) \quad \text{ou} \quad 2^3 \equiv 1(\text{mod}\, p_2) \quad \text{ou} \quad 2^6 \equiv 1(\text{mod}\, p_2) \tag{13}$$

No primero caso, $p_2|2^1 - 1 = 2- = 1$, o que é impossível. No segundo caso, $p_2|2^2 - 1 = 4-1 = 3$, o que também é impossível pois $p_2 > p_1 = 3$. No terceiro caso, $p_2|2^3-1 = 8-1 = 7$ e segue que $p_2 = 7$. No quarto caso, $p_2|2^6 - 1 = 64 - 1 = 63 = 3^2 \cdot 7$, do fato de que p_2 é primo e maior que 3 segue que $p_2 = 7$. Portanto $p_2 = 7$.

2.5. **As únicas soluções são $n = 1$ e $n = 3$:** Agora poderíamos proceder para calcular os possíveis valores de α_2, porém ao analisar $2^n + 1(\text{mod}\, 7)$ já garantimos que é impossível termos $p_2 = 7$.

De fato, temos $7|n^2|2^n + 1$ implica que $2^n \equiv -1(\text{mod}\, 7)$. Mas as potências 2^n módulo 7 sempre valem 1 ou 4:

$$2^1 \equiv 1(\text{mod}\, 7) \quad , \quad 2^2 \equiv 4(\text{mod}\, 7) \quad \text{e} \quad 2^3 \equiv 1(\text{mod}\, 7), \cdots, \tag{14}$$

isto é, $2^{2n+1} \equiv 1$ e $2^{2n} \equiv 4(\text{mod}\, 7)$.

Portanto é impossível haver o segundo petor primo além de $p_1 = 3$ e, com isso, descobrimos que apenas $n = 1$ e $n = 3$ satisfazem as condições do enunciado.

3. Lema de Hensel

Para finalizar este texto, comentamos que o passo crucial na solução foi utilizar o Lema 1 para estimar α_1. Este Lema é uma versão particular do chamado Lema de Hensel, que enunciamos abaixo (compare os 2 enunciados e chegue a essa conclusão).

Notação 1. *Seja p um número primo e b um inteiro qualquer, denotamos $p^\alpha \| b$ se $p^\alpha | b$ e $p^{\alpha+1} \not| b$. Isto é, α é a maior potência de p com a propriedade $p^\alpha | b$.*

Lema 2 (Lema de Hensel)**.** *Sejam p um número primo e $\alpha > 0$.*
a) Se n é ímpar, $p^\alpha \| a + 1$ e $p^\beta \| n$, então $p^{\alpha+\beta} \| a^n + 1$.
b) Se $p^\alpha \| a - 1$ e $p^\beta \| n$, então $p^{\alpha+\beta} \| a^n - 1$.

Demonstração:
a) A demonstração será feita por indução em β.
Caso inicial: ($\beta = 0$) Neste caso, p não divide n. Fatorando $a^n + 1$:

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

Como $p^\alpha \| a+1$, basta verificarmos que p não divide $a^{n-1} - a^{n-2} + \cdots - a + 1$. Mas $a \equiv -1(mod p)$ (lembre-se que $\alpha > 0$!), daonde segue que

$$a^{n-1} - a^{n-2} + \cdots - a + 1 \equiv 1 - 1 + \cdots - 1 + 1 \equiv 1(mod p.$$

Logo $p^\alpha \| a^n - 1$.
Passo indutivo: Suponha o resultado válido para $\beta = k$ e $p^{k+1} \| n$. Queremos concluir que $p^{\alpha+k+1} \| a^n + 1$.

Como $p^k \| n/p$, pela hipótese de indução, temos que $p^{\alpha+k} | a^{n/p} + 1$. Logo existe q tal que $\text{mdc}(q,p) = 1$ e $a^{n/p} = p^{\alpha+k}q - 1$. Elevando à p-ésima potência:

$$\begin{aligned} a^n = (a^{n/p})^p &= (p^{\alpha+k}q - 1)^p \\ &= p^{p(\alpha+k)}q^p - \binom{p}{1}p^{(p-1)(\alpha+k)}q^{p-1} + \cdots - \binom{p}{p-2}p^{2(\alpha+k)}q^2 + \binom{p}{1}p^{\alpha+k}q - 1 \\ &= p^{\alpha+k+1}\Big[p\Big(p^{(p-1)(\alpha+k)+1}q^p - \cdots - \binom{p}{p-2}p^{\alpha+k-1}q^2\Big) + q\Big] - 1 \\ &= p^{\alpha+k+1}\tilde{q} - 1, \end{aligned}$$

aonde, usando que $p|\binom{p}{j}$, concluímpos que $\tilde{q} \equiv q(mod p)$, implicando que p não divide $\tilde{q}$, daonde segue que $p^{\alpha+k+1} \| a^n + 1$.

b) Análogo ao item anterior.

4. Problemas propostos

Finalizamos propondo alguns problemas para o leitor. Para a maioria dos problemas abaixo, a dica é a mesma: utilize o lema de Hensel para encontra a maior potência de p que divide uma expressão do tipo $a^n \pm 1$.

Problema 3. *Sejam p um primo ímpar e a e b inteiros não divisíveis por p tais que $p|a-b$. Mostre que $p^k|a^n - b^n$ se e somente se $p^k|n(a-b)$.*

Problema 4. *Sejam $k \geq 2$ e $n_1, n_2, \cdots, n_k \geq 1$ inteiros que satisfazem*

$$n_2|2^{n_1} - 1 \quad , \quad n_3|2^{n_2} - 1 \quad , \quad \cdots n_2|2^{n_1} - 1 \quad , \quad n_k|2^{n_{k-1}} - 1 \quad \text{e} \quad n_1|2^{n_k} - 1.$$

Demonstre que $n_1 = n_2 = n \cdots = n_k = 1$.

Problema 5. *Encontre todos os inteiros não-negativos x e y tais que*

$$7^y - 1 = 2 \cdot 3^x.$$

Problema 6 (China-2005)**.** *Encontre todos os inteiros não-negativos x, y, z e w tais que*

$$2^x \cdot 3^y - 5^z \cdot 7^w = 1.$$

Problema 7 (APMO-1997)**.** *Encontrar um n inteiro com $100 \leq n \leq 1997$ tal que n divide $2^n + 2$.*

Problema 8 (IMO-2000)**.** *Existe um inteiro positivo n com exatamente 2000 divisores primos tal que $2^n + 1$ é múltiplo de n?*

Problema 9 (IMO-1999)**.** *Encontre todos os pares (n,p) onde n é inteiro positivo, p é primo, $n \leq 2p$ e*

$$(p-1)^n + 1 \text{ é divisível por } n^{p-1}.$$

Problema 10 (Banco IMO-2000)**.** *Encontre todos os inteiros positivos a, m e n tais que $a^m + 1$ divide $(a+1)^n$.*

Problema 11. *Sejam $a > 1$, $m \neq n$ inteiros positivos tais que $a^m - 1$ e $a^n - 1$ tem os mesmos fatores primos. Prove que $a + 1$ é uma potência de 2.*

Referências

Nas duas primeiras referências é possível encontrar a solução para o Problema 6 da IMO de 1990, assim como um estudo mais amplo sobre o Lema de Hensel. As duas útlimas correspondem a dois livros brasileiros que são ótimas referências para um estudo de teoria dos números:

(1) Shine, C. Y. - Três VIPs da Teoria dos Números - disponível em http://cyshine.webs.com/tres-vip.pdf.
(2) Shine, C. Y. - 21 Aulas de Matemática Olímpica, Coleção Olimpíadas de Matemática, IMPA, 2009.
(3) Brochero, F.; Moreira, C.G.; Saldanha, N.; Tengan, E. - Teoria dos números um passeio pelo mundo inteiro com primos e outros números familiares, Projeto Euclides, IMPA, 2010.
(4) Santos, J. P. O. - Introdução à Teoria dos Números, Coleção Matemática Universitária, IMPA, 2017.