

É só fatorar. . . Será mesmo?

Neste pequeno artigo resolveremos o problema 2 da USAMO (USA Mathematical Olympiad) 2005:

Problema. Prove que o sistema

$$\begin{cases} x^6 + x^3 + x^3y + y = 147^{157} \\ x^3 + x^3y + y^2 + y + z^9 = 157^{147} \end{cases}$$

não tem solução em inteiros x, y, z .

Solução. No começo, podemos pensar que este é mais um problema simples na qual “é só fatorar”:

$$\begin{cases} x^6 + x^3 + x^3y + y = 147^{157} \\ x^3 + x^3y + y^2 + y + z^9 = 157^{147} \end{cases} \iff \begin{cases} (x^3 + 1)(x^3 + y) = 147^{157} \\ (x^3 + y)(1 + y) = 157^{147} - z^9 \end{cases}$$

Aí é só fatorar $147^{157} = 3^{157} \cdot 7^{314}$ e testar todos os $2 \cdot (157 + 1) \cdot (314 + 1)$ casos, certo?

Infelizmente, acho que na hora da prova não iríamos ter tempo para fazer isso. Então temos que dar um jeito de estudar menos casos.

Observe que $x^3 + 1$ é um divisor de $3^{157} \cdot 7^{314}$. Logo

$$x^3 + 1 = \pm 3^\alpha \cdot 7^\beta$$

Você poderia pensar no $x^3 + y$, mas isso não seria uma boa, considerando que $x^3 + y$ é linear em y e poderia assumir qualquer valor inteiro por causa disso. Além disso, $x^3 + 1$ tem só uma variável e o principal. . . fatora!

Assim, o principal no problema é resolver a equação diofantina

$$x^3 + 1 = \pm 3^\alpha \cdot 7^\beta \quad (*)$$

em que x é inteiro (positivo, negativo ou até quem sabe nulo!) e α e β são inteiros não negativos.

Podemos fatorar o primeiro membro de (*):

$$x^3 + 1 = \pm 3^\alpha \cdot 7^\beta \iff (x + 1)(x^2 - x + 1) = \pm 3^\alpha \cdot 7^\beta$$

Quando fatoramos em equações diofantinas, devemos calcular o mdc dos fatores, senão a equação fica ofendida! Vamos usar tanto esse fato que o chamaremos de

Lema. Seja x inteiro. Então $\text{mdc}(x + 1; x^2 - x + 1) = 1$ ou $\text{mdc}(x + 1; x^2 - x + 1) = 3$. Além disso, se 3 divide um dos números $x + 1$ ou $x^2 - x + 1$ então divide ambos, ou seja, 3 divide $x + 1$ se, e somente se, 3 divide $x^2 - x + 1$.

Demonstração. Seja $d = \text{mdc}(x + 1; x^2 - x + 1)$. Vendo $x + 1 \pmod d$, obtemos $x + 1 \equiv 0 \pmod d \iff x \equiv -1 \pmod d$. Vendo agora $x^2 - x + 1 \pmod d$, obtemos $x^2 - x + 1 \equiv 0 \pmod d \iff (-1)^2 - (-1) + 1 \equiv 0 \pmod d \iff 3 \equiv 0 \pmod d \iff d|3 \iff d = 1$ ou $d = 3$.

Vimos acima que se $x + 1$ é divisível por 3 então $x^2 - x + 1$ também é. Vejamos agora a recíproca. Mas isso é tão fácil quanto resolver equação do segundo grau!

$$\begin{aligned} x^2 - x + 1 \equiv 0 \pmod 3 &\iff 4x^2 - 4x + 4 \equiv 0 \pmod 3 \iff 4x^2 - 4x + 1 \equiv 0 \pmod 3 \\ &\iff (2x - 1)^2 \equiv 0 \pmod 3 \iff 2x - 1 \equiv 0 \pmod 3 \\ &\iff -x - 1 \equiv 0 \pmod 3 \iff x + 1 \equiv 0 \pmod 3 \end{aligned}$$

■

Agora, voltemos à equação (*), ou seja,

$$(x+1)(x^2-x+1) = \pm 3^\alpha \cdot 7^\beta$$

Logo $x+1 = \pm 3^{\alpha_1} \cdot 7^{\beta_1}$ e $x^2-x+1 = 3^{\alpha_2} \cdot 7^{\beta_2}$ (note que $x^2-x+1 = \frac{1}{4}((2x-1)^2+3) > 0$), sendo $\alpha_1, \beta_1, \alpha_2$ e β_2 inteiros não negativos.

Veja que, do Lema, concluímos que $\alpha_1 = 0 \iff \alpha_2 = 0$ e, além disso, $\beta_1 = 0$ ou $\beta_2 = 0$, pois se ambos os expoentes β_1 e β_2 forem positivos então 7 seria um dos fatores de $\text{mdc}(x+1; x^2-x+1)$, absurdo. Além disso, se $\alpha_1 > 0$ (ou $\alpha_2 > 0$) então $\alpha_1 = 1$ ou $\alpha_2 = 1$ pois, caso contrário, 9 dividiria $\text{mdc}(x+1; x^2-x+1)$, absurdo.

Suponha primeiro que α_1 e β_1 são ambos não nulos. Logo $\alpha_2 > 0$ e $\beta_2 = 0$.

Se $\alpha_1 \geq 2$, $\alpha_2 = 1$ e, portanto, $x^2-x+1 = 3 \iff x = -1$ ou $x = 2$. $x = -1$ é o mesmo que $x+1 = 0$, o que não é possível. $x = 2$ é equivalente a $x+1 = 3$, absurdo já que supomos que $\beta_1 > 0$.

Logo $\alpha_1 = 1$ e, portanto, $x+1 = \pm 3 \cdot 7^{\beta_1}$ e $x^2-x+1 = 3^{\alpha_2}$. Mas aí, sendo $a = 7^{\beta_1}$, $x = 3a - 1 \iff x^3 = 27a^3 - 27a^2 + 9a - 1 \iff x^3 + 1 = 9(3a^3 - 3a^2 + 1)$. Como $3a^3 - 3a^2 + 1$ não é divisível por 3, a maior potência de 3 que divide x^2-x+1 é 3^2 , ou seja, $\alpha_2 = 2$. Portanto, $x^2-x+1 = 9$, o que é impossível para x inteiro.

Desta forma, não é possível que α_1 e β_1 sejam ambos não nulos. Resta-nos, então, dois casos: $\alpha_1 = 0$ e $\beta_1 = 0$.

- *Primeiro caso:* $\alpha_1 = 0$ e $\beta_1 = 0$. Neste caso, $x+1 = \pm 1$ e, portanto, $x = 0$ ou $x = -2$. Veja que, para esses valores de x , x^3+1 é da forma $3^\alpha \cdot 7^\beta$.
- *Segundo caso:* $\alpha_1 = 0$ e $\beta_1 > 0$. Aqui temos $x+1 = \pm 7^{\beta_1}$, $\alpha_2 = 0$ e $\beta_2 = 0$, ou seja, $x^2-x+1 = 1 \iff x = 1$ ou $x = 0$. Nenhum desses valores de x satisfaz $x+1$ ser uma potência de 7 maior que 1.
- *Terceiro caso:* $\alpha_1 > 0$ e $\beta_1 = 0$. Temos $x+1 = \pm 3^{\alpha_1}$, $\alpha_2 > 0$ e $\beta_2 \geq 0$. Além disso, $\alpha_1 = 1$ ou $\alpha_2 = 1$.

Se $\alpha_1 = 1$, $x+1 = \pm 3$, ou seja, $x = 2$ ou $x = -4$. Novamente, para esses valores de x , x^3+1 é da forma $3^\alpha \cdot 7^\beta$.

Se $\alpha_2 = 1$, $x+1 = \pm 3^{\alpha_1}$ e $x^2-x+1 = 3 \cdot 7^{\beta_2}$. Logo $x = \pm 3^{\alpha_1} - 1$ e $x^2-x+1 = (\pm 3^{\alpha_1} - 1)^2 - (\pm 3^{\alpha_1} - 1) + 1 = 3^{2\alpha_1} \mp 3^{\alpha_1+1} + 3$. Logo $x^2-x+1 = 3 \cdot 7^{\beta_2} \iff 3^{2\alpha_1} \mp 3^{\alpha_1+1} + 3 = 3 \cdot 7^{\beta_2} \iff 3^{\alpha_1}(3^{\alpha_1-1} \mp 1) = 7^{\beta_2} - 1$.

Agora temos que resolver esta outra equação diofantina:

$$3^{\alpha_1}(3^{\alpha_1-1} \mp 1) = 7^{\beta_2} - 1 \tag{**}$$

Neste caso utilizamos o

Lema de Hensel. *Seja p um primo ímpar, a um inteiro e n um inteiro positivo. Sejam α e β inteiros não negativos, com $\alpha > 0$.*

- Se a maior potência de p que divide n é p^β e a maior potência de p que divide $a-1$ é p^α (atenção, p deve dividir $a-1$! Mas note que p não precisa dividir n), então a maior potência de p que divide $a^n - 1$ é $p^{\alpha+\beta}$.*
- Se n é ímpar, a maior potência de p que divide n é p^β e a maior potência de p que divide $a+1$ é p^α (as mesmas condições sobre os expoentes α e β do item (i) devem valer), então a maior potência de p que divide $a^n + 1$ é $p^{\alpha+\beta}$.*

Vejamos como aplicá-lo no problema.

Seja 3^γ a maior potência de 3 que divide β_2 . Como a maior potência de 3 que divide $7-1$ é 3, aplicando o Lema de Hensel para $a = 7$, $p = 3$, $n = \beta_2$, $\alpha = 1$ e $\beta = \gamma$, obtemos que a maior potência de 3 que divide

$7^{\beta_2} - 1$ é $\gamma + 1$. Mas, de (**), a maior potência de 3 que divide $7^{\beta_2} - 1$ é 3^{α_1} , logo $\gamma + 1 = \alpha_1 \iff \gamma = \alpha_1 - 1$. Logo $3^{\alpha_1 - 1}$ divide β_2 e, portanto, $\beta_2 \geq 3^{\alpha_1 - 1}$. Sendo $w = 3^{\alpha_1 - 1}$, temos

$$3^{\alpha_1} (3^{\alpha_1 - 1} \mp 1) = 7^{\beta_2} - 1 \geq 7^{3^{\alpha_1 - 1}} - 1 \implies 3w(w \mp 1) \geq 7^w - 1$$

Mas note que a exponencial $7^w - 1$ cresce bem mais que o polinômio $3w(w - 1)$. De fato, uma simples indução mostra que $7^w - 1 > 3w(w + 1) \geq 3w(w \mp 1)$ para $w \geq 2$: $7^{w+1} - 1 - 3(w + 1)((w + 1) + 1) = (7^w - 1) - 3w(w + 1) + 6(7^w - 1 - w)$. Por hipótese, $7^w - 1 - 3w(w + 1) > 0$ e, além disso, $7^w - 1 - w > (7^w - 1) - 3w(w + 1) > 0$. Logo se a desigualdade $7^w - 1 > 3w(w + 1)$ é válida então a mesma desigualdade vale para valores maiores de w . Como, em particular, vale para $w = 2$, acabou.

Logo $w = 1 \iff 3^{\alpha_1 - 1} = 1 \iff \alpha_1 = 1$, que já estudamos.

As aplicações do Lema de Hensel geralmente seguem esse *script*: primeiro, aplicamos o teorema e depois chegamos a alguma desigualdade que limita algum dos expoentes, chegando a um número normalmente bem finito de casos.

Você deve estar se perguntando como é a demonstração do Lema de Hensel. Vamos demonstrá-lo nesse caso particular ($a = 7, p = 3$). A prova do Lema em si não é muito diferente do que se segue.

Primeiro, seja $\beta_2 = 3^\gamma \cdot t$, sendo que 3 não divide t . Utilizaremos a fatoração $x^t - 1 = (x - 1)(x^{t-1} + x^{t-2} + \dots + x + 1)$ para $x = 7^{3^\gamma}$:

$$7^{\beta_2} - 1 = (7^{3^\gamma})^t - 1 = (7^{3^\gamma} - 1)((7^{3^\gamma})^{t-1} + (7^{3^\gamma})^{t-2} + \dots + 7^{3^\gamma} + 1)$$

Como já dissemos antes, se não calcularmos o mdc das parcelas, a equação fica ofendida! Assim, seja $D = \text{mdc}(x - 1; x^{t-1} + x^{t-2} + \dots + x + 1)$, com $x = 7^{3^\gamma}$. Vendo $x - 1 \pmod D$ temos $x \equiv 1 \pmod D$. Logo $x^{t-1} + x^{t-2} + \dots + x + 1 \equiv 0 \pmod D \iff \underbrace{1 + 1 + \dots + 1}_{t \text{ uns}} \equiv 0 \pmod D \iff t \equiv 0 \pmod D$, ou

seja, D divide t . Note que esse resultado não depende do valor de x (desde que seja inteiro, é claro!), então, você pode guardar:

Fato. *Seja x inteiro e $D = \text{mdc}(x - 1; x^{t-1} + x^{t-2} + \dots + x + 1)$. Então D divide t .*

Na nossa demonstração, o que interessa é que 3 não divide t e, portanto, não divide D . Em outras palavras, todos os fatores 3 estão em $7^{3^\gamma} - 1$.

Agora vamos provar que $7^{3^\gamma} - 1$ tem $\gamma + 1$ fatores 3 por indução em γ : a base $\gamma = 0, 1$ é óbvia. Agora, note que $7^{3^{\gamma+1}} - 1 = (7^{3^\gamma})^3 - 1 = (7^{3^\gamma} - 1)((7^{3^\gamma})^2 + 7^{3^\gamma} + 1)$. Mas $\text{mdc}(x - 1; x^2 + x + 1) = 3$ para todo x inteiro, em particular para $x = 7^{3^\gamma}$. Logo a maior potência de 3 que divide $(7^{3^\gamma})^2 + 7^{3^\gamma} + 1$ é 3 e, pela hipótese de indução, a maior potência de 3 que divide $7^{3^\gamma} - 1$ é $\gamma + 1$. Assim, o passo indutivo está provado e a indução também.

Enfim, chegamos à solução de (*): $x = -2; x = 0; x = 2; x = -4$. Assim, $x^3 + 1$ só tem fatores primos 3 e 7 para esses valores de x .

Agora é só testar no sistema original. Da primeira equação encontramos y ; substituímos na segunda e provamos que não existe z .

- $x = -2 \iff x^3 + 1 = -7$.

$$\begin{cases} (x^3 + 1)(x^3 + y) = 147^{157} = 3^{157} \cdot 7^{314} \\ (x^3 + y)(1 + y) = 157^{147} - z^9 \end{cases} \iff \begin{cases} y = 8 - 3^{157} \cdot 7^{313} \\ -3^{157} \cdot 7^{313}(9 - 3^{157} \cdot 7^{313}) = 157^{147} - z^9 \end{cases}$$

Vendo $\pmod{157}$ (e observando que 157 é primo e, portanto, $a^{156} \equiv 1 \pmod{157}$ para a não divisível por 157), obtemos

$$\begin{aligned} & -3^{156} \cdot 3 \cdot 7^{2 \cdot 156} \cdot 7(9 - 3^{156} \cdot 3 \cdot 7^{2 \cdot 156} \cdot 7) \equiv -z^9 \pmod{157} \\ \iff & 3 \cdot 7(9 - 3 \cdot 7) \equiv z^9 \pmod{157} \\ \iff & -252 \equiv z^9 \pmod{157} \\ \iff & z^9 \equiv 62 \pmod{157} \end{aligned}$$

Notando que $156 = 3 \cdot 52$, elevando a 52 obtemos no lado esquerdo $z^{3 \cdot 156} \equiv 1 \pmod{157}$. Logo

$$62^{52} \equiv 1 \pmod{157}$$

Veamos se isso é verdade. Se não for, não há soluções nesse caso.

$$\begin{aligned} 62^2 &= 62 \cdot 3 \cdot 20 + 62 \cdot 2 \equiv 29 \cdot 20 - 33 \equiv -48 - 33 \equiv -81 \pmod{157} \\ \implies 62^{52} &\equiv (-3^4)^{26} \pmod{157} \\ \implies 62^{52} &\equiv 3^{104} \pmod{157} \end{aligned}$$

Logo $62^{52} \equiv 1 \pmod{157} \iff 3^{104} \equiv 1 \pmod{157} \iff 3^{156-104} = 3^{52} \equiv 1 \pmod{157}$. Vamos lá!

$$\begin{aligned} 3^6 &= 729 \equiv -56 \pmod{157} \implies 3^{12} \equiv 56^2 \pmod{157} \\ \iff 3^{12} &\equiv 56 \cdot 3 \cdot 18 + 56 \cdot 2 \equiv 11 \cdot 18 - 45 \equiv -4 \pmod{157} \\ \implies 3^{48} &\equiv 256 \pmod{157} \iff 3^{52} \equiv -58 \cdot 81 \pmod{157} \\ \iff 3^{52} &\equiv -58 \cdot 3 \cdot 27 \equiv -17 \cdot 27 \equiv -17 \cdot 9 \cdot 3 \equiv -(-4) \cdot 3 \equiv 12 \pmod{157} \end{aligned}$$

Logo $3^{52} \equiv 12 \pmod{157}$ e, portanto, não há soluções nesse caso.

- $x = 2 \iff x^3 + 1 = 9$.

$$\left| \begin{array}{l} (x^3 + 1)(x^3 + y) = 147^{157} = 3^{157} \cdot 7^{314} \\ (x^3 + y)(1 + y) = 157^{147} - z^9 \end{array} \right. \iff \left| \begin{array}{l} y = 3^{155} \cdot 7^{314} - 8 \\ 3^{155} \cdot 7^{314}(3^{155} \cdot 7^{314} - 7) = 157^{147} - z^9 \end{array} \right.$$

Vendo mód 157:

$$\begin{aligned} 3^{156-1} \cdot 7^{2 \cdot 156+2}(3^{156-1} \cdot 7^{2 \cdot 156+2} - 7) &\equiv -z^9 \pmod{157} \\ \iff 3^{-1} \cdot 7^2(3^{-1} \cdot 7^2 - 7) &\equiv -z^9 \pmod{157} \\ \iff -52 \cdot 7 \cdot 7(-52 \cdot 7 \cdot 7 - 7) &\equiv -z^9 \pmod{157} \\ \iff 364 \cdot 7(-364 \cdot 7 - 7) &\equiv z^9 \pmod{157} \\ \iff 50 \cdot 7(-50 \cdot 7 - 7) &\equiv -z^9 \pmod{157} \\ \iff 350 \cdot 357 &\equiv -z^9 \pmod{157} \\ \iff 36 \cdot 43 &\equiv -z^9 \pmod{157} \\ \iff 22 &\equiv z^9 \pmod{157} \end{aligned}$$

Elevando a 52,

$$22^{52} \equiv 1 \pmod{157}$$

Vamos lá!

$$\begin{aligned} 22^2 &= 484 \equiv 13 \pmod{157} \implies 22^4 \equiv 169 \equiv 12 \pmod{157} \\ \implies 22^8 &\equiv 144 \equiv -13 \pmod{157} \iff 22^8 \equiv -22^2 \pmod{157} \\ \iff 22^6 &\equiv -1 \pmod{157} \implies 22^{48} \equiv 1 \pmod{157} \\ \iff 22^{52} &\equiv 22^4 \equiv 12 \pmod{157} \end{aligned}$$

De novo, não temos soluções nesse caso.

- $x = -4 \iff x^3 + 1 = -63$.

$$\left| \begin{array}{l} (x^3 + 1)(x^3 + y) = 147^{157} = 3^{157} \cdot 7^{314} \\ (x^3 + y)(1 + y) = 157^{147} - z^9 \end{array} \right. \iff \left| \begin{array}{l} y = 8 - 3^{155} \cdot 7^{313} \\ -3^{155} \cdot 7^{313}(9 - 3^{155} \cdot 7^{313}) = 157^{147} - z^9 \end{array} \right.$$

Vendo mód 157:

$$\begin{aligned}
 & -3^{156-1} \cdot 7^{2 \cdot 156+1} (9 - 3^{156-1} \cdot 7^{2 \cdot 156+1}) \equiv -z^9 \pmod{157} \\
 \iff & -3^{-1} \cdot 7(9 - 3^{-1} \cdot 7) \equiv -z^9 \pmod{157} \\
 \iff & 52 \cdot 7(9 + 52 \cdot 7) \equiv -z^9 \pmod{157} \\
 \iff & 364(9 + 364) \equiv -z^9 \pmod{157} \\
 \iff & 50 \cdot 59 \equiv -z^9 \pmod{157} \\
 \iff & 33 \equiv z^9 \pmod{157}
 \end{aligned}$$

Elevando a 52,

$$33^{52} \equiv 1 \pmod{157}$$

Vamos ver se isso é verdade mesmo: primeiro note que $33^{52} = 3^{52} \cdot 11^{52}$ e que já sabemos que $3^{52} \equiv 12$ (mód. 157). Assim, basta calcular 11^{52} mód 157.

$$\begin{aligned}
 11^2 & \equiv -36 \pmod{157} \implies 11^4 \equiv 36^2 = 36 \cdot 4 \cdot 9 \equiv (-13) \cdot 9 \equiv 40 \pmod{157} \\
 \implies 11^8 & \equiv 1600 \equiv 30 \pmod{157} \implies 11^{16} \equiv 900 \equiv -42 \pmod{157} \\
 \implies 11^{32} & \equiv 42^2 = 42 \cdot 40 + 42 \cdot 2 \equiv 1680 + 84 \equiv 110 - 73 \equiv 37 \pmod{157} \\
 \implies 11^{48} & = 11^{32} \cdot 11^{16} \equiv 37 \cdot (-42) \equiv -37 \cdot 40 - 37 \cdot 2 \equiv 90 - 74 \equiv 16 \pmod{157} \\
 \implies 11^{52} & = 11^{48} \cdot 11^4 \equiv 16 \cdot 40 = 640 \equiv 12 \pmod{157}
 \end{aligned}$$

Novamente, não há soluções.

- $x = 0 \iff x^3 + 1 = 1$. Nesse caso, obtemos $y = 147^{157} - 1$ e $y(y+1) = 157^{147} - z^9 \iff (147^{157} - 1)147^{157} = 157^{147} - z^9 \implies (147 - 1)147 \equiv -z^9 \pmod{157} \iff z^9 \equiv 47 \pmod{157} \implies 47^{52} \equiv 1 \pmod{157}$.

Vamos fazer mais uma vez as contas! Algo que pode ajudar é que $47^{52} \equiv (-110)^{52} \equiv 11^{52} \cdot 10^{52}$ (mód. 157) e que sabemos que $11^{52} \equiv 12$ (mód. 157). Falta, então, calcular 10^{52} mód 157.

$$10^3 \equiv -58 \pmod{157} \iff 10^4 \equiv -580 \equiv 48 \pmod{157} \iff 10^5 \equiv 480 \equiv 9 \equiv 3^2 \pmod{157}$$

Já calculamos algumas potências de 3 mód 157! Entre elas, $3^{12} \equiv -4$ (mód. 157):

$$\begin{aligned}
 10^{30} & \equiv 3^{12} \equiv -4 \pmod{157} \implies 10^{45} = 10^{30} \cdot (10^5)^3 \equiv -4 \cdot 3^6 \equiv -4 \cdot (-56) \equiv 67 \pmod{157} \\
 \implies 10^{50} & = 10^{45} \cdot 10^5 \equiv 67 \cdot 9 = 603 \equiv -25 \pmod{157} \\
 \implies 10^{52} & \equiv -250 \cdot 10 \equiv 64 \cdot 10 \equiv 12 \pmod{157}
 \end{aligned}$$

De novo, nenhuma solução.

Assim, o sistema dado não tem soluções inteiras. ■

O problema também admite uma solução mais curta. Vamos apresentá-las e depois fazemos alguns comentários sobre as duas soluções.

Solução alternativa. No sistema

$$\begin{cases} x^6 + x^3 + x^3y + y = 147^{157} \\ x^3 + x^3y + y^2 + y + z^9 = 157^{147} \end{cases}$$

o que aparece mais são números ao cubo. Então pode ser interessante ver algum módulo primo com poucos resíduos cúbicos.

O fato é que os primos com “poucos” resíduos cúbicos são os da forma $3k + 1$. Depois vamos ver por quê.

Ver mód 7 não dá certo (tente e veja por si mesmo!). Mas ver mód 13 funciona bem. A tabela a seguir mostra os resíduos cúbicos mód 13:

$$\begin{array}{cccccccc} x \text{ mód } 13 & 0 & \pm 1 & \pm 2 & \pm 3 & \pm 4 & \pm 5 & \pm 6 \\ x^3 \text{ mód } 13 & 0 & \pm 1 & \pm 8 & \pm 1 & \mp 1 & \pm 8 & \pm 8 \end{array}$$

Como no problema o x só aparece ao cubo, podemos encontrar y mód 13 na primeira equação e substituir na segunda. Temos $147 \equiv 4 \pmod{13} \implies 147^6 \equiv 2^{12} \equiv 1 \pmod{13} \implies 147^{156} \equiv 1 \pmod{13} \iff 147^{157} \equiv 4 \pmod{13}$ e $157 \equiv 1 \pmod{13} \implies 157^{147} \equiv 1 \pmod{13}$. Assim, vendo mód 13 o sistema fica

$$\left| \begin{array}{l} (x^3 + 1)(x^3 + y) \equiv 4 \pmod{13} \\ (x^3 + y)(1 + y) \equiv 1 - z^9 \pmod{13} \end{array} \right. \iff \left| \begin{array}{l} (x^3 + 1)(x^3 + y) \equiv 4 \pmod{13} \\ z^9 \equiv 1 - (x^3 + y)(1 + y) \pmod{13} \end{array} \right.$$

Já vemos, por exemplo, que $x^3 \not\equiv -1 \pmod{13}$. Vamos testar os outros quatro casos ($x^3 \equiv 0, 1, 5, 8 \pmod{13}$):

$$\begin{array}{ccc} x^3 \text{ mód } 13 & (x^3 + y) \equiv 4(x^3 + 1)^{-1} \pmod{13} & z^9 \equiv 1 - (x^3 + y)(1 + y) \pmod{13} \\ 0 & 0 + y \equiv 4 \cdot 1^{-1} \equiv 4 & z^9 \equiv 1 - 4 \cdot (1 + 4) \equiv 11 \\ 1 & 1 + y \equiv 4 \cdot 2^{-1} \equiv 2 & z^9 \equiv 1 - 2 \cdot (1 + 1) \equiv 10 \\ 5 & 5 + y \equiv 4 \cdot 6^{-1} \equiv 5 & z^9 \equiv 1 - 5 \cdot (1 + 0) \equiv 9 \\ 8 & 8 + y \equiv 4 \cdot 9^{-1} \equiv -1 & z^9 \equiv 1 - (-1) \cdot (1 + 4) \equiv 6 \end{array}$$

Nenhum dos números 6, 9, 10, 11 é resíduo cúbico de 13 e portanto $z^9 = (z^3)^3 \equiv 6, 9, 10, 11 \pmod{13}$ não tem solução. Logo o sistema não tem solução. ■

Agora, vamos explicar por que os primos com “poucos” resíduos são os da forma $3k + 1$.

Lema. *Seja p um primo maior que 3. Então*

- *Se $p \equiv -1 \pmod{3}$ então todo resíduo é resíduo cúbico, ou seja, p admite p resíduos cúbicos.*
- *Se $p \equiv 1 \pmod{3}$ então p admite $\frac{p-1}{3} + 1$ resíduos cúbicos.*

A demonstração desse lema é baseado no seguinte fato:

Fato. *Seja p primo ímpar e a inteiro não divisível por p . A congruência $x^3 \equiv a^3 \pmod{p}$ tem*

- *1 solução se $p \equiv -1 \pmod{3}$;*
- *3 soluções se $p \equiv 1 \pmod{3}$.*

Vamos provar esse fato: primeiro, temos

$$\begin{aligned} x^3 \equiv a^3 \pmod{p} &\iff x^3 - a^3 \equiv 0 \pmod{p} \\ &\iff (x - a)(x^2 + ax + a^2) \equiv 0 \pmod{p} \\ &\iff x \equiv a \pmod{p} \text{ ou } x^2 + ax + a^2 \equiv 0 \pmod{p} \end{aligned}$$

Já temos uma solução, $x \equiv a \pmod{p}$. Estudemos a congruência quadrática.

$$x^2 + ax + a^2 \equiv 0 \pmod{p} \iff 4x^2 + 4ax + 4a^2 \equiv 0 \pmod{p} \iff (2x + a)^2 \equiv -3a^2 \pmod{p}$$

Essa congruência tem solução se, e somente se, $-3a^2$ é resíduo quadrático de p , o que ocorre se, e somente se, -3 é resíduo quadrático de p . Para verificar quando isso acontece, utilizamos (sem demonstrar) a lei da reciprocidade quadrática:

Lei da reciprocidade quadrática. Defina o símbolo de Legendre por

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \text{ divide } a \\ 1 & \text{se } p \text{ não divide } a \text{ e } a \text{ é resíduo quadrático de } p \\ -1 & \text{caso contrário} \end{cases}$$

Então, sendo p e q primos,

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Queremos saber $\left(\frac{-3}{p}\right)$. Fazendo $q = 3$, obtemos

$$\left(\frac{p}{-3}\right) \cdot \left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{-3-1}{2}} = 1 \iff \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$$

Mas os resíduos quadráticos de 3 são 0 e 1. Logo se p é maior que 3

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \pmod{3} \\ -1 & \text{se } p \equiv -1 \pmod{3} \end{cases}$$

Deste modo, o fato está demonstrado. Poderíamos ter demonstrado uma (mas só essa!) mais facilmente: se $p \equiv -1 \pmod{3}$, $\frac{p-2}{3}$ é inteiro e

$$\begin{aligned} x^3 \equiv a^3 \pmod{p} &\implies (x^3)^{\frac{p-2}{3}} \equiv (a^3)^{\frac{p-2}{3}} \pmod{p} \\ &\iff x^{p-2} \equiv a^{p-2} \pmod{p} \\ &\iff x^{-1} \equiv a^{-1} \pmod{p} \\ &\iff x \equiv a \pmod{p} \end{aligned}$$

O resto da demonstração do lema é combinatória: para cada $k = 0, 1, 2, \dots, p-1$ seja A_k o número de soluções de $x^3 \equiv k \pmod{p}$. Sabemos que se $p \equiv 1 \pmod{3}$ então

$$|A_k| = \begin{cases} 1 & \text{se } k = 0 \\ 3 & \text{se } k \text{ é resíduo cúbico de } p \\ 0 & \text{caso contrário} \end{cases}$$

e se $p \equiv -1 \pmod{3}$ então

$$|A_k| = \begin{cases} 1 & \text{se } k = 0 \text{ ou } k \text{ é resíduo cúbico de } p \\ 0 & \text{caso contrário} \end{cases}$$

Observe que os conjuntos A_k 's são disjuntos e que todo x é raiz de alguma congruência do tipo $x^3 \equiv k \pmod{p}$ (é só tomar $k = x^3$!), logo $S = |A_0| + |A_1| + \dots + |A_{p-1}| = p$. Temos $A_0 = \{0\}$, então 0 é resíduo cúbico.

Seja n a quantidade de resíduos cúbicos de p . Se $p \equiv 1 \pmod{3}$, temos $S = 1 + 3n \iff n = \frac{p-1}{3}$ e se $p \equiv -1 \pmod{3}$, temos $S = 1 + n \iff n = p-1$ e a demonstração do fato está completa. ■

Comentários sobre as duas soluções. Há algumas considerações sobre o problema:

- (i) O expoente 9 em z^9 não é necessário. Poderia ser z^3 no lugar de z^9 .
- (ii) Podemos trocar 157^{147} por qualquer múltiplo de 157.

Comparando as soluções, sem dúvida a segunda solução é mais curta e envolve menos contas. Mas a primeira solução tem mais a dizer: além de provar (ii), o que a segunda solução não faz, nela também conseguimos um fato bastante interessante sobre números da forma $x^3 + 1$: eles consistem só em fatores primos 3 e 7 para poucos valores de x (quatro, para ser exato). Na verdade isso é razoavelmente esperado, dado que o mdc dos fatores $x+1$ e x^2-x+1 é pequeno: é de se esperar que os fatores primos de $x+1$ e x^2-x+1 sejam bem diferentes.

Isso pode levar a outras perguntas interessantes: seja X_k a quantidade de números inteiros x tais que $x^3 + 1$ tem exatamente k fatores primos distintos. X_k é finito ou infinito? E se trocarmos $x^3 + 1$ por $x^n - 1$, n inteiro positivo maior que 3?