Ordem

Semana Olímpica/2024

Prof. Armando Barbosa

Bento Gonçalves, 23 de janeiro de 2024

Material selecionado do livro laranja TN do Zero a IME/ITA/Cone Sul/EGMO.

1 Ordem e Raiz primitiva

Definição: Sendo a inteiro e m inteiro positivo tal que $mdc(a, m) = 1$, chama-se **ordem** de a módulo m ao **menor** inteiro positivo k tal que

$$a^k \equiv 1 \pmod{m}$$

Notação adotada: $\boxed{k = \text{ord}_m a}$.
Por exemplo:

1. a ordem de 9 módulo 10 é igual a 2, pois:

$$9^1 \equiv 9 \equiv -1 \pmod{10} \qquad 9^2 \equiv (-1)^2 \equiv 1 \pmod{10}$$

   Ou seja, $\text{ord}_{10}9 = 2$.

2. a ordem de 2 módulo 5 é igual a 4, pois:

$$2^1 \equiv 2 \pmod{5} \qquad 2^2 \equiv 4 \equiv -1 \pmod{5}$$
$$2^3 \equiv -2 \pmod{5} \qquad 2^4 \equiv -4 \equiv 1 \pmod{5}$$

   Ou seja, $\text{ord}_5 2 = 4$.

Aproveitemos para enunciar e provar um lema clássico e famoso de ordem, que nesta seção será referenciado como **lema famoso**:

Lema: Sejam m inteiro positivo e a inteiro tal que $mdc(a, m) = 1$. Seja $h = \text{ord}_m a$. Então, temos que:

$$a^k \equiv 1 \pmod{m} \Leftrightarrow h|k$$

Prova:

- Parte 1: $a^k \equiv 1 \pmod{m} \Rightarrow h|k$.
  Suponhamos que não, isto é, que h não divide k. Pelo algoritmo da divisão, temos que existem interios q (quociente) e r (resto) tais que

$$k = h \cdot q + r \quad 0 < r < h$$

Daí, temos que:

$$\begin{aligned} 1 \equiv a^k &\equiv a^{h\cdot q+r} \pmod m \\ &\equiv \left(a^h\right)^q \cdot a^r \pmod m \\ &\equiv 1^q \cdot a^r \pmod m \\ 1 &\equiv a^r \pmod m \end{aligned}$$

Notemos que o resultado encontrado é absurdo, pois $r < h = \text{ord}_m a$

- Parte 2: $a^k \equiv 1 \pmod m \Leftarrow h|k$.
  Seja q inteiro positivo tal que $k = h \cdot q$. Daí, temos que:

$$a^k \equiv \left(a^h\right)^q \equiv 1^q \equiv 1 \pmod m$$

■

Daí, por exemplo, pelo teorema de Euler, podemos concluir que: $\text{ord}_m a \mid \varphi(m)$.

Definição: Seja n inteiro positivo. Um inteiro g diz-se uma **raiz primitiva** módulo m se $mdc(g, n) = 1$ e a ordem de g módulo n é igual a $\varphi(n)$.

Por exemplo, 3 é uma raiz primitiva módulo 10, pois $\text{ord}_{10} 3 = 4 = \varphi(10)$.

Sobre raiz primitiva, existe um lema bem famoso, cujo enunciado está disposto a seguir e cuja prova foge ao escopo desse livro.

Lema: Apenas os números podem ser módulos 2, 4, p^k e $2p^k$ numa raiz primitiva, sendo p primo e k um inteiro positivo.

Normalmente, as soluções só envolvem saber da existência da raiz primitiva. No entanto, para fins didáticos, vejamos uma aplicação desse lema, para $p = 5$, provando que 2 é raiz primitiva módulo 5^k.

Problema 1 Prove que:

a) Para todo k inteiro, é válida a seguinte relação:

$$2^{4\cdot 5^{k-1}} \equiv 1 + 3 \cdot 5^k \pmod{5^{k+1}}$$

b) O número 2 é uma raíz primitiva módulo 5^n para todo n inteiro positivo.

Solução:

a) Resolvamos por indução.

Caso inicial: $k = 1$:

$$2^{4\cdot 5^0} \equiv 2^4 \equiv 1 + 3 \cdot 5 \pmod{5^2}$$

Ok!

Hipótese indutiva: Suponha que seja verdade para um inteiro t. Daí, temos que:

$$2^{4\cdot 5^{t-1}} \equiv 1 + 3 \cdot 5^t \pmod{5^{t+1}}$$

Passo indutivo: Da hipótese indutiva, temos que existe $k \in \mathbb{Z}$ tal que:

$$2^{4\cdot 5^{t-1}} = 5^{t+1} \cdot k + \left(1 + 3 \cdot 5^t\right)$$

Elevando tudo a quinta potência, podemos concluir que:

$$\begin{aligned}\left(2^{4\cdot 5^{t-1}}\right)^5 &= \left[5^{t+1}\cdot k+\left(1+3\cdot 5^t\right)\right]^5\\ &= \left(5^{t+1}\cdot k\right)^5+5\cdot\left(5^{t+1}\cdot k\right)^4\cdot\left(1+3\cdot 5^t\right)+10\cdot\left(5^{t+1}\cdot k\right)^3\cdot\left(1+3\cdot 5^t\right)^2\\ &+ 10\cdot\left(5^{t+1}\cdot k\right)^2\cdot\left(1+3\cdot 5^t\right)^3+5\cdot\left(5^{t+1}\cdot k\right)\cdot\left(1+3\cdot 5^t\right)^4+\left(1+3\cdot 5^t\right)^5\end{aligned}$$

Notemos que apenas o último termo da direita não tem fator 5^{t+2}. Com isso, temos que:

$$\begin{aligned}\left(2^{4\cdot 5^{t-1}}\right)^5 &\equiv \left(1+3\cdot 5^t\right)^5 \pmod{5^{t+2}}\\ 2^{4\cdot 5^t} &\equiv 1+\binom{5}{1}\cdot 3\cdot 5^t+\sum_{i=2}^{5}\left[\binom{5}{i}\cdot 1^{1-i}\cdot\left(3\cdot 5^t\right)^i\right] \pmod{5^{t+2}}\\ &\equiv 1+3\cdot 5^{t+1}+\sum_{i=2}^{5}\left[\binom{5}{i}\cdot\left(3\cdot 5^t\right)^i\right] \pmod{5^{t+2}}\end{aligned}$$

Daí, para todo $i=2,3,4,5$, temos que:

$$5^{t+2}\left|\binom{5}{i}\cdot\left(3\cdot 5^t\right)^{(5-i)}\right.$$

Dos três últimos resultados encontrados, podemos concluir que:

$$2^{4\cdot 5^t}\equiv 1+3\cdot 5^{t+1} \pmod{5^{t+2}}$$

Portanto, indução concluída! Item resolvido!

b) Resolvamos por indução.

Caso inicial: Provemos que 2 é uma raíz primitiva módulo 5:

$$\begin{aligned}2^1 &\equiv 2 \pmod 5\\ 2^2 &\equiv 4 \pmod 5\\ 2^3 &\equiv 3 \pmod 5\\ 2^4 &\equiv 1 \pmod 5\end{aligned}$$

Hipótese indutiva: Suponha que seja verdade para um inteiro t. Daí, temos que 2 é uma raiz primitiva módulo 5^t. Com isso, podemos concluir que:

$$\mathrm{ord}_{5^t}2=\phi(5^t)=4\cdot 5^{t-1}$$

Passo indutivo: Seja $x=\mathrm{ord}_{5^{t+1}}2$. Fazendo $m=5^{t+1}$ e $k=\phi(5^{t+1})=4\cdot 5^t$, podemos concluir, pelo lema famoso, que:

$$x|4\cdot 5^t$$

Além disso, temos que:

$$\begin{aligned}2^x &\equiv 1 \pmod{5^{t+1}}\\ 2^x &\equiv 1 \pmod{5^t}\end{aligned}$$

Então, pelo lema famoso, fazendo $m=5^t$ e $k=x$, temos que:

$$4\cdot 5^{t-1}\,|x$$

Das últimas duas conclusões encontradas, podemos concluir que há apenas dois casos possíveis:

Caso 1: $x = 4 \cdot 5^{t-1}$: Absurdo pelo item a;
Caso 2: $x = 4 \cdot 5^t = \phi(5^{t+1})$: Ok!

Portanto, indução concluída! Item resolvido! ■

Obs.: A questão original pede apenas para provar que 2 é uma raiz primitiva módulo 5^k, sendo k inteiro positivo. O item a é um lema que "surge naturalmente" no passo indutivo do item b, mais especificamente no caso 1. O que pretende-se dizer é que o item a não foi "tirado do nada", mas que tal item surgiu da necessidade de provar o item b.

É possível provar, analogamente, que 2 é raiz primitiva módulo 3^k, ficando isso como exercício para o leitor.

Seguindo nossos estudos, vejamos algumas questões resolvidas sobre ordem.

2 Questões resolvidas

Problema 2 Prove que não existe inteiro positivo $n > 1$ tal que $n \mid 2^n - 1$.

Solução: Seja p o <u>menor</u> primo que divide n. Daí, temos que:

$$p \mid n \Big| 2^n - 1 \Rightarrow p \mid 2^n - 1 \Rightarrow 2^n \equiv 1 \pmod{p}$$

Pelo teorema de Fermat, podemos concluir que:

$$2^{p-1} \equiv 1 \pmod{p}$$

Seja $d = \text{ord}_p 2$. Daí, pelo lema clássico demonstrado e pelas propriedades de mdc, temos que:

$$\begin{cases} d \mid n \\ d \mid p-1 \end{cases} \Rightarrow d \mid mdc(n, p-1)$$

Como p é o menor primo que divide n, então não há fator primo entre n e $p-1$, pois para todo primo $q \mid p-1$, temos que $q \nmid n$, pela minimalidade de p.

Com isso, podemos concluir que: $d = 1$, que gera um absurdo! ■

Problema 3 *(Romênia/TST - 2019)* Seja $k \geqslant 2$ e $n_1, n_2, \cdots, n_k$ inteiros positivos que satisfazem:

$$n_2 \mid 2^{n_1} - 1 \quad ; \quad n_3 \mid 2^{n_2} - 1 \quad \cdots \quad n_k \mid 2^{n_{k-1}} - 1; \quad n_1 \mid 2^{n_k} - 1$$

Prove que $n_1 = n_2 = \cdots = n_k = 1$.

Solução: Seja $M = mmc\,(n_1, n_2, \cdots, n_k)$. Pelo algebrismo de produtos notáveis, temos que:

$$m \mid n \Rightarrow a^m - 1 \mid a^n - 1$$

Daí, usando isso e propriedade de mmc, temos que:

$$\begin{aligned} n_2 \mid 2^{n_1} - 1 \Big| 2^M - 1 \\ n_3 \mid 2^{n_2} - 1 \Big| 2^M - 1 \\ \vdots \qquad\qquad \Rightarrow M \mid 2^M - 1 \\ n_k \mid 2^{n_{k-1}} - 1 \Big| 2^M - 1 \\ n_1 \mid 2^{n_k} - 1 \Big| 2^M - 1 \end{aligned}$$

Pela solução anterior, temos que: $\boxed{M = 1}$. E, portanto, segue que: $n_1 = n_2 = \cdots = n_k = 1$. ■

Problema 4 *(Sérvia/2010)* Uma tabela $n \times n$ totalmente preenchida com números $1, 2, \cdots, n^2$ é chamada *sérvia* se todos os produtos de n números escritos em n quadradinhos *espalhados* deixam o mesmo resto na divisão por $n^2 + 1$. Existe uma tabela sérvia para

a) $n = 8$?

b) $n = 10$?

Obs.: n quadradinhos são ditos espalhados se não há quaisquer dois deles na mesma linha ou mesma coluna.

Solução:

a) Suponha que existe. Daí, o produto dos números dos 8 quadradinhos espalhados deixam resto $r \pmod{65}$, sendo $65 = 5 \cdot 13$. Como algum dos números é múltiplo de 13, então $13 \mid r$. Por outro lado, como há apenas 4 múltiplos de 13, pegando 8 conjuntos de 8 quadradinhos espalhados, disjuntos dois a dois, é possível, pelo P.C.P., tomar algum conjunto que não tenha múltiplo de 13. Então, para este caso, não há tabela sérvia.

b) Provemos que existe. Para $n = 10$, temos que $10^2 + 1 = 101$ que é número primo. Daí, existe uma raiz primitiva $g \pmod{101}$.

Analisemos a tabela:

$$a_{i,j} \equiv g^{10i+j} \pmod{101} \qquad \forall 0 \leqslant i, j \leqslant 9$$

Pela definição de raiz primitiva, cada número de 1 a 100 foi usado exatamente uma vez. Além disso, tomemos 10 quadradinhos espalhados: $a_{0,p(0)}$, $a_{1,p(1)}$, $\cdots$, $a_{9,p(9)}$, sendo $p(0)$, $p(1)$, $\cdots$, $p(9)$ uma permutação de 0 a 9 e, então, $p(0) + p(1) + \cdots + p(9) = 0 + 1 + \cdots + 9 = 45$.

Então, temos o seguinte produto de 10 quadradinhos espalhados:

$$\prod_{i=0}^{9} a_{i,p(i)} \equiv g^{p(0)} \cdot g^{10+p(1)} \cdots g^{90+p(9)} \equiv g^{450+45} \equiv g^{495} \pmod{101}$$

não importando o modo de escolha de tais 10 quadradinhos espalhados, de forma que fica comprovada a existência da tabela sérvia para este caso. ■

Problema 5 *(Belarus/TST -2019)* Para $n > 1$, prove que $2^{n-1} + 1$ não é divisível por n.

Solução: Considere a seguinte fatoração de n em fatores primos: $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, com $p_1 < p_2 < \cdots < p_k$ e, por paridade, $p_1 > 2$.

Para todo $1 \leqslant j \leqslant k$, seja $d_j = \operatorname{ord}_{p_j^{\alpha_j}} 2$. Seja $n - 1 = 2^{\beta} \cdot I_{n-1}$, onde I_{n-1} é ímpar, (ou, em outras palavras, seja $\beta = v_2(n-1)$). Daí, pelo lema famoso da ordem, temos que:

$$\begin{cases} 2^{n-1} \equiv -1 \pmod{n} \Rightarrow d_j \nmid n-1 \\ 2^{2(n-1)} \equiv 1 \pmod{n} \Rightarrow d_j \mid 2(n-1) \end{cases} \Rightarrow \boxed{d_j = 2^{\beta+1} \cdot I_j} \text{ onde } I_j \text{ é ímpar.}$$

Pelo teorema de Euler e pelo lema famoso de ordem, podemos concluir que:

$$d_j \mid \varphi\left(p_j^{\alpha_j}\right) = p_j^{\alpha_j}(p_j - 1) \Rightarrow \boxed{p_j \equiv 1 \pmod{2^{\beta+1}}} \quad \forall 1 \leqslant j \leqslant k$$

Fazendo um produto telescópico de 1 a k, temos que:

$$n = \prod_{j=1}^{k} p_j^{\alpha_j} \equiv 1 \pmod{2^{\beta+1}} \Rightarrow 2^{\beta+1} \mid n-1$$

chegando a um absurdo com a consideração inicial que $n - 1 = 2^{\beta} \cdot I_{n-1}$, onde I_{n-1} é ímpar, (ou, em outras palavras, que $\beta = v_2(n-1)$). ■

Problema 6 *(Belarus/TST - 2019)* Em duas caixas, são colocadas, no total, 1019 bolas de forma que não há caixa sem bola. Em cada minuto, Sofia escolhe a caixa com quantidade par de bolas e passa a metade delas para a outra caixa. Prove que, para cada k inteiro positivo, com $1 \leqslant k \leqslant 2018$, há um momento em que existe uma caixa com exatamente k bolas.

Solução: Sejam a_i, b_i as quantidades de bolas em cada caixa no minuto i, após Sofia ter movimentado elas. Sejam a_0 e b_0 as quantidades iniciais de bola. Daí, temos que a soma das quantidades de bolas é invariante. Isto é:

$$a_i + b_i = 2019$$

Suponhamos que, em algum momento, b_i seja par. Nesse caso, olhando para a invariância já citada, podemos concluir que:

$$\begin{cases} a_{i+1} = a_i + \frac{b_i}{2} \Rightarrow 2a_{i+1} = 2a_i + b_i \Rightarrow \boxed{2a_{i+1} - a_i = 1019} \\ b_{i+1} = \frac{b_i}{2} \Rightarrow \boxed{2b_{i+1} = b_i} \end{cases}$$

Se o a_i for o par, podemos fazer uma análise análoga. Desse modo, através de indução ou produto telescópico, temos que:

$$\begin{cases} a_i \equiv 2^j \cdot a_{i+j} \pmod{1019} \\ b_i \equiv 2^j \cdot a_{i+j} \pmod{1019} \end{cases} \tag{1}$$

Além disso, sabemos que:

$$\begin{aligned} 1019 \text{ é primo} &\Rightarrow 2^{1018} \equiv 1 \pmod{1019} \Rightarrow \text{ord}_2 1019 \mid 1018 \\ \frac{1018}{2} = 509 \text{ é primo} &\Rightarrow \text{ord}_2 1019 = \{1, 2, 509, 1018\} \\ 2^1 - 1 < 1019 \text{ e } 2^2 - 1 < 1019 &\Rightarrow \boxed{\text{ord}_2 1019 = 509 \text{ ou } 1018} \end{aligned}$$

Temos, agora, o suficiente para concluir pois:

Caso 1: Se $\text{ord}_2 1019 = 1018$

Por $j = 0$ em (1), temos que, em cada caixa, em algum momento, terá k bolas, para todo $1 \leqslant k \leqslant 1018$, pois, nesse caso, teríamos que o conjunto $\left\{2^1, 2^2, \cdots, 2^{1018}\right\}$ formaria um sistema completo de resíduos (mod 1019) e, sendo 1019 primo, temos que os elementos iniciais são tais que:

$$mdc\,(1019, a_0) = (1019, b_0) = 1$$

e, por consequência, os conjuntos $\left\{2^1 \cdot a_0, 2^2 \cdot a_0, \cdots, 2^{1018} \cdot a_0\right\}$ e $\left\{2^1 \cdot b_0, 2^2 \cdot b_0, \cdots, 2^{1018} \cdot b_0\right\}$, também, formam um sistema completo de resíduos.

Caso 2: Se $\text{ord}_2 1019 = 509$

Pela invariância da soma, temos que: $a_0 \equiv -b_0 \pmod{1019}$. Daí, com essa relação e por $j = 0$ em (1), vamos mostrar que apenas uma das caixas, em algum momento, terá k bolas, para todo $1 \leqslant k \leqslant 1018$. Para isso, comecemos do fato que 1019 é primo e isso implica em:

$$mdc\,(1019, a_0) = (1019, b_0) = 1$$

Daí, caso não aconteça o que afirmamos no começo desse caso, então teríamos que existe m, n inteiros positivos, com $0 \leqslant m, n \leqslant 508$, tais que:

$$\begin{aligned} & & a_m \equiv b_n \pmod{1019} \\ j = 0 \text{ em (1)} &\Rightarrow & 2^m a_0 \equiv 2^n b_0 \pmod{1019} \\ b_0 \equiv -a_0 \pmod{1019} &\Rightarrow & 2^m a_0 + 2^n a_0 \equiv 0 \pmod{1019} \end{aligned}$$

Suponhamos, s.p.g., $m \geqslant n$. Daí, como $mdc\,(1019, a_0) = 1$, podemos concluir que:

$$1019 \mid a_0\left(2^m + 2^n\right) \Rightarrow 1019 \mid 2^n\left(2^{m-n} + 1\right) \Rightarrow 1019 \mid 2^{m-n} + 1$$

Com isso, se $\text{ord}_2 1019 = 509$, então temos que $509 \nmid m-n$ e $509 \mid 2(m-n)$. Esses fatos são contraditórios com $0 \leqslant m, n \leqslant 508$, pois dessa última relação, teríamos que: $-508 \leqslant m - n \leqslant 508$.

■

Problema 7 *(Hong Kong/TST - 2023)* Seja n um inteiro positivo. Sendo p um número primo tal que:

$$p \mid 5^{4n} - 5^{3n} + 5^{2n} - 5^n + 1$$

mostre que $p \equiv 1 \pmod 4$.

Solução: de Levi Magalhães Pereira Castello Branco

Vamos resolver, inicialmente, o caso n par.

$$5^{5n} + 1 = \left(5^{4n} - 5^{3n} + 5^{2n} - 5^n + 1\right)(5^n + 1)$$
$$\Rightarrow p \mid 5^{5n} + 1 \Rightarrow 5^{5n} \equiv -1 \pmod p$$
$$\Rightarrow \boxed{\left(5^{\frac{5n}{2}}\right)^2 \equiv -1 \pmod p} \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow \boxed{p \equiv 1 \pmod 4}$$

Falta, então, o caso n ímpar. Inicialmente, conforme vimos no desenvolvimento algébrico acima, temos que:

$$5^{5n} \equiv -1 \pmod p \Rightarrow \left(5^{\frac{5n+1}{2}}\right)^2 \equiv -5 \pmod p \Rightarrow \boxed{\left(\frac{-5}{p}\right) = 1} \quad (I)$$

Daí, a partir de $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)$, falta provar que $\left(\frac{5}{p}\right) = 1$. Pela lei de reciprocidade quadrática, sabemos que isso é equivalente a provar que: $\left(\frac{p}{5}\right) = 1$. Provemos isso.

Precisaremos de dois resultados. O primeiro é imediato, a partir do lema conhecido:

$$p \mid 5^{5n} + 1 \Rightarrow 5^{5n} \equiv -1 \pmod p \Rightarrow 5^{10n} \equiv 1 \pmod p$$
$$\Rightarrow \boxed{\text{ord}_p 5 \mid 10n} \qquad (II)$$

Vamos para o segundo. Comecemos provando que $p \nmid 5^{2n} - 1$. Dividamos esse caso em dois, usando a condição do enunciado:

$$\text{Se } p \mid 5^n - 1 \Rightarrow \begin{cases} p \mid 5^{4n} - 5^{3n} \\ p \mid 5^{2n} - 5^n \end{cases} \Rightarrow p \mid 5^{4n} - 5^{3n} + 5^{2n} - 5^n$$

$$\begin{cases} p \mid 5^{4n} - 5^{3n} + 5^{2n} - 5^n \\ p \mid 5^{4n} - 5^{3n} + 5^{2n} - 5^n + 1 \end{cases} \Rightarrow p \mid 1 \Rightarrow \text{ Absurdo!}$$

$$\text{Se } p \mid 5^n + 1 \Rightarrow \begin{cases} p \mid 5^{4n} + 5^{3n} \\ p \mid -2 \cdot 5^{3n} - 2 \cdot 5^{2n} \\ p \mid 3 \cdot 5^{2n} + 3 \cdot 5^n \\ p \mid -4 \cdot 5^n - 4 \end{cases} \Rightarrow p \mid 5^{4n} - 5^{3n} + 5^{2n} - 5^n - 4$$

$$\begin{cases} p \mid 5^{4n} - 5^{3n} + 5^{2n} - 5^n - 4 \\ p \mid 5^{4n} - 5^{3n} + 5^{2n} - 5^n + 1 \end{cases} \Rightarrow p \mid 5 \Rightarrow p = 5$$

$$\Rightarrow \text{ Absurdo, pois } \begin{cases} 5 \mid 5^{4n} - 5^{3n} + 5^{2n} - 5^n \\ 5 \mid 5^{4n} - 5^{3n} + 5^{2n} - 5^n + 1 \end{cases} \Rightarrow 5 \mid 1$$

Daí, lembrando que, pelo lema famoso e o teorema de Fermat, temos que: $\text{ord}_p 5 \mid p-1$, podemos concluir que:

$$p \nmid 5^{2n} - 1 \Rightarrow \text{ord}_p 5 \nmid 2n \Rightarrow$$

$$\begin{cases} \text{ord}_p 5 \nmid 2n \\ (II) : \text{ord}_p 5 \mid 10n \end{cases} \Rightarrow 5 \mid \text{ord}_p 5 \big| p-1 \Rightarrow$$

$$p \equiv 1 \pmod 5 \Rightarrow \left(\frac{p}{5}\right) = 1 \Rightarrow$$

$$\left(\frac{p}{5}\right)\left(\frac{5}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{5-1}{2}\right)} = 1 \Rightarrow \left(\frac{5}{p}\right) = 1 \Rightarrow$$

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) \overset{(I)}{\Longrightarrow} \left(\frac{-1}{p}\right) = 1 \Rightarrow \boxed{p \equiv 1 \pmod 4}$$

■

Problema 8 *(China/TST - 2009)* Encontre todos os pares de números primos p, q tais que $pq \mid 5^p + 5^q$.

Solução: de Caio Harley Constâncio Neves

Obs.: Nesta solução, adotaremos a notação $v_2(x)$ para denotar a maior potência de 2 que divide x.

Suponhamos, sem perda de generalidade, que $p \leqslant q$. Inicialmente, façamos alguns casos:

Caso 1: Se $p = 2$, temos que: $2q \mid 5^q + 25$

- Se $q = 2$, não há solução, pois $4 \nmid 150$.
- Se $q = 5$, há solução, pois $10 \mid 5^5 + 25$, geranado a solução $\boxed{(p,q) = (2,5)}$.
- Se $q \neq 2$ e $q \neq 5$, pelo teorema de Fermat, podemos concluir que:

$$\begin{cases} q \mid 5^{q-1} - 1 \\ 2 \mid 5^{q-1} - 1 \end{cases} \Rightarrow 2q \mid 5^{q-1} - 1 \big| 5^q - 5$$

$$\Rightarrow \begin{cases} 2q \mid 5^q + 25 \\ 2q \mid 5^q - 5 \end{cases} \Rightarrow 2q \mid 30$$

gerando a solução $\boxed{(p,q) = (2,3)}$.

Caso 2: Se $p = 3$, temos que: $3q \mid 5^q + 5^3 = 5^q + 125 \big| 3 \cdot 5^q + 375$ Por outro lado, pelo teorema de Fermat, podemos concluir que:

$$q \mid 5^{q-1} - 1 \Rightarrow 3q \mid 3 \cdot 5^{q-1} - 3 \big| 3 \cdot 5^q - 15$$

Subtraindo as duas últimas relações encontradas, temos que: $3q \mid 390$. Os casos $q = 5$ e $q = 13$ não geram solução. Em particular, apresentemos o teste de $q = 13$ (o caso $q = 5$ é análogo): $13 \cdot 3 \mid 5^{13} + 125$ fato contraditório com: $5^{13} + 125 \equiv (-1)^{13} + (-1) \equiv -2 \pmod 3$

Caso 3: Se $p = 5$, temos que: $5q \mid 5^q + 5^5 = 5^q + 3125$

- Se $q = 5$, temos a solução $\boxed{(p,q) = (5,5)}$.

- Se $q \neq 5$, pelo teorema de Fermat, podemos concluir que:

$$q \mid 5^{q-1} - 1 \Rightarrow 5q \mid 5^q - 5$$

Subtraindo as duas últimas relações encontradas, temos que: $5q \mid 3130$. O caso $q = 313$ gera a solução $\boxed{(p, q) = (5, 313)}$.

Agora, façamos o caso geral: $7 \leqslant p \leqslant q$.
Do enunciado, temos que:

$$pq \mid 5^p \left(1 + 5^{q-p}\right) \Rightarrow \begin{cases} 5^{q-p} \equiv -1 \pmod{p} \\ 5^{2(q-p)} \equiv 1 \pmod{p} \end{cases} \Rightarrow \boxed{v_2\left(\text{ord}_p 5\right) = v_2(q-p) + 1} \tag{2}$$

Por outro lado, pelo teorema de Fermat, temos que:

$$p \mid 5^q + 5^p \Rightarrow 5^q + 5 \equiv 0 \pmod{p} \Rightarrow 5^{q-1} \equiv -1 \pmod{p}$$

Analogamente ao feito em (2), podemos concluir que:

$$v_2\left(\text{ord}_p 5\right) = v_2(q-1) + 1$$

Aplicando isso a (2), temos que: $v_2(q-p) = v_2(q-1)$.
De forma análoga a tudo que foi feito, mas para $\pmod{q}$, podemos concluir que: $v_2(q-p) = v_2(p-1)$.
As duas últimas conclusões geram um absurdo pois, sendo $\alpha = v_2(p-1) = v_2(q-1)$, podemos concluir que:

$$q - p = (q-1) - (p-1) = 2^\alpha \cdot (I_q - I_p) \Rightarrow v_2(q-p) > \alpha$$

pois I_q e I_p são ímpares e, por isso, a diferença entre eles é par. ■

Encerremos essa seção em grande estilo, apresentando uma solução que será tema da próxima seção: Equações Diofantinas. Vale ressaltar que a ideia da solução seguinte está melhor descrita e que a questão a seguir está como desafio em alguma subseção da próxima seção.

Problema 9 *(Cone Sul/TST - 2015)* Ache todos os inteiros positivos x e y para os quais a equação a seguir é verdadeira:

$$3^x - 5^y = 2$$

Solução: Testando os casos iniciais até $x < 4$, temos a solução: $\boxed{(x, y) = (3, 2)}$. Vejamos se há outras soluções:

$$3^x - 5^y = 3^3 - 5^2 \Rightarrow 3^3\left(3^{x-3} - 1\right) = 5^2\left(5^{y-2} - 1\right)$$

Daí, temos que: $5^2 \left\| 3^{x-3} - 1 \right.$.
Calculemos $\text{ord}_{5^3} 3$, sempre lembrando do lema famoso:

$$\begin{aligned}
&\text{(Euler) } 3^{\phi(125)} \equiv 3^{100} \equiv 1 \pmod{125} \\
&3^{50} \equiv \left(3^5\right)^{10} \equiv (-7)^{10} \equiv \left(7^5\right)^2 \equiv \left(7 \cdot 7^4\right)^2 \equiv (7 \cdot 26)^2 \equiv 57^2 \equiv -1 \pmod{125} \\
&3^{20} \equiv \left(3^5\right)^4 \equiv (-7)^4 \equiv 7^4 \equiv 26 \pmod{125} \\
&\Rightarrow \begin{cases} \text{ord}_{5^3} 3 \mid 100 \\ \text{ord}_{5^3} 3 \nmid 50 \\ \text{ord}_{5^3} 3 \nmid 20 \end{cases} \Rightarrow \boxed{\text{ord}_{5^3} 3 = 100}
\end{aligned}$$

Portanto, 100 não pode dividir $x - 3$, pois caso isso ocorra, teremos 5 dividindo $5^{y-2} - 1$, pela relação inicial encontrada.

Agora, para facilitar, organizemos os resultados encontrados em fatos:

Fato 1: $20 \mid x-3$

Prova: 5^b sempre termina em 25, para $b > 2$, na base decimal, ou seja, $5^b \equiv 25 \pmod{100}$. Com algumas contas e lembrando que 3^a para terminar em 7 precisa ser da forma $4K+3$, temos que (para facilitar as contas, basta pegar o número formado pela dezena e unidade e multiplicar por 81, ou por -19):

$$3^3 \equiv 27 \pmod{100} \qquad 3^7 \equiv -13 \pmod{100}$$
$$3^{11} \equiv 47 \pmod{100} \qquad 3^{15} \equiv 7 \pmod{100}$$
$$3^{19} \equiv -33 \pmod{100} \qquad \boxed{3^{23} \equiv 27 \pmod{100}}$$

Fato 2: $20 \mid y-2$

Prova: Consequência dos dois resultados a seguir:

(a) $5 \mid y-2$: basta analisar 3^x e $5^y \pmod{11}$ e aplicar o fato 1 (o período é 5, nos dois casos)
(b) $4 \mid y-2$: basta analisar 3^x e $5^y \pmod{16}$ e aplicar o fato 1 (o período é 4, nos dois casos)

Nosso objetivo agora é provar que de $20 \mid x-3$ podemos chegar a $100 \mid x-3$ e, assim, provar que não há solução maior que $(x, y) = (3, 2)$.

Para isso, falta provar que $25 \mid x-3$, uma vez que precisamos de outro fator 5 ao 20 para, então, chegar ao 100.

Para chegar a tal resultado, podemos olhar para os primos da forma $25K+1$, pois, nesse caso, aplicaríamos o teorema de Fermat e o lema famoso. Daí, surge o 101, pois 26, 51 e 76 não são primos.

Fato 3: $100 \mid x-3$

Prova: Analisemos 3^x e $5^y \pmod{101}$, usando os fatos 1 e 2:

$$3^{20} \equiv \left[\left(3^5\right)^2\right]^2 \equiv \left[(-60)^2\right]^2 \equiv (-36)^2 \equiv -17 \pmod{101}$$
$$3^3 \equiv 27 \pmod{101} \qquad 3^{23} \equiv 27 \cdot (-17) \equiv 46 \pmod{101}$$
$$3^{43} \equiv 46 \cdot (-17) \equiv 26 \pmod{101}$$
$$3^{63} \equiv 26 \cdot (-17) \equiv 63 \equiv -38 \pmod{101}$$
$$3^{83} \equiv (-38) \cdot (-17) \equiv 40 \pmod{101}$$
$$3^{103} \equiv 40 \cdot (-17) \equiv 27 \pmod{101}$$

$$5^{20} \equiv \left[\left(5^5\right)^2\right]^2 \equiv \left[(-6)^2\right]^2 \equiv 36^2 \equiv -17 \pmod{101}$$
$$5^2 \equiv 25 \pmod{101} \qquad 5^{22} \equiv 25 \cdot (-17) \equiv 80 \equiv -21 \pmod{101}$$
$$5^{42} \equiv (-21) \cdot (-17) \equiv 54 \pmod{101}$$
$$5^{62} \equiv 54 \cdot (-17) \equiv 92 \equiv -9 \pmod{101}$$
$$5^{82} \equiv (-9) \cdot (-17) \equiv 52 \pmod{101}$$
$$5^{102} \equiv 52 \cdot (-17) \equiv 25 \pmod{101}$$

Daí, pelos resultados acima, podemos concluir que:

$$3^x - 5^y \equiv 2 \pmod{101} \Leftrightarrow 100 \mid x-3$$

fato absurdo com o lema famoso, conforme relação inicial encontrada.

Portanto, solução única: $\boxed{(x, y) = (3, 2)}$. ■

2.1 Mais questões

Problema 10 Prove que:

a) Para todo k inteiro, é válida a seguinte relação:

$$2^{2\cdot 3^{k-1}} \equiv 1 + 3^k \pmod{3^{k+1}}$$

b) O número 2 é uma raíz primitiva $\pmod{3^n}$ para todo n inteiro positivo.

Problema 11 *(Coreia do Sul/2007)* Encontre todos os pares de primos (p, q) para os quais $pq \mid p^p + q^q + 1$.

Problema 12 *(Polônia/2016)* Sejam k, n inteiros positivos ímpares, maiores que 1. Prove que se existe um número natural a tal que $k \mid 2^a + 1$ e $n \mid 2^a - 1$, então não existe um número natural b que satisfaz $k \mid 2^b - 1$ e $n \mid 2^b + 1$.

Problema 13 Para todo n inteiro positivo, seja $X_n = 2^{2^n} + 1$. Prove que

$$3^{\frac{X_n - 1}{2}} \equiv -1 \pmod{X_n} \Rightarrow X_n \text{ é primo}$$

Problema 14 Mostre que não existem inteiros positivos d, a, n tais que $3 \leqslant d \leqslant 2^{n+1}$ e $d \mid a^{2^n} + 1$.

Problema 15 Prove que há uma potência de 2 cujos últimos 1000 algarismos são 1 ou 2.

Problema 16 *(Bósnia/TST-2014)* Encontre todos os inteiros não negativos x, y tais que:

$$2 \cdot 5^x - 7^y = 1$$

Problema 17 *(Turquia/TST - EGMO/2017)* Encontre todos os pares de números primos (p, q) para os quais os números

$$\frac{(2p^2 - 1)^q + 1}{p + q} \text{ e } \frac{(2q^2 - 1)^p + 1}{p + q}$$

são, ambos, inteiros.