GABARITO P2 - ALGEBRA I / 1º sem. 2012

ex1) Determine o menor inteiro positivo que satisfaz o sistema: $\begin{cases} 2x \equiv 1 \bmod 5 \\ 3x \equiv 2 \bmod 7 \\ 5x \equiv 7 \bmod 11. \end{cases}$

Primeiramente, como 5, 7 e 11 são primos entre si e $mdc(2,5) = mdc(3,7) = mdc(5,11) = 1$, então este sistema de congruências lineares terá solução.

Começamos assim, simplificando o sistema:

$\Rightarrow 2x \equiv 1 \bmod 5$ | $\Rightarrow 3x \equiv 2 \bmod 7$ | $\Rightarrow 5x \equiv 7 \bmod 11$

$\cdot 3 \Leftrightarrow 6x \equiv 3 \bmod 5$ | $\cdot 5 \Leftrightarrow 15x \equiv 10 \bmod 7$ | $\cdot 9 \Leftrightarrow 45x \equiv 63 \bmod 11$

Resto $\Leftrightarrow x \equiv 3 \bmod 5$ | Resto $\Leftrightarrow x \equiv 3 \bmod 7$ | Resto $\Leftrightarrow x \equiv 8 \bmod 11$

$\therefore$ Logo $\begin{cases} 2x \equiv 1 \bmod 5 \\ 3x \equiv 2 \bmod 7 \\ 5x \equiv 7 \bmod 11 \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \bmod 5 \ (i) \\ x \equiv 3 \bmod 7 \ (ii) \\ x \equiv 8 \bmod 11 \ (iii) \end{cases}$

De (i), ficamos com $x = 3 + 5t$, $t \in \mathbb{Z}$

$\Rightarrow$ (i) em (ii), ficamos: $3 + 5t \equiv 3 \bmod 7$

$(-3) \Leftrightarrow 5t \equiv 0 \bmod 7$

$\cdot 3 \Leftrightarrow 15t \equiv 0 \bmod 7$

Resto $\Leftrightarrow t \equiv 0 \bmod 7$, $\Leftrightarrow t = 7k$, $k \in \mathbb{Z}$

$\therefore$ Logo $x = 3 + 5t = 3 + 5(7k) = 3 + 35k$ (iv)

$\Rightarrow$ (iv) em (iii), ficamos: $3 + 35k \equiv 8 \bmod 11$

$\Leftrightarrow 35k \equiv 5 \bmod 11$

Resto $\Leftrightarrow 2k \equiv 5 \bmod 11$

$\cdot 6 \Leftrightarrow 12k \equiv 30 \bmod 11$

Resto $\Leftrightarrow k \equiv 8 \bmod 11$, $\Leftrightarrow k = 8 + 11k'$, $k' \in \mathbb{Z}$.

, Portanto $x = 3 + 35k = 3 + 35(8 + 11k')$

$\Leftrightarrow x = 283 + 385k'$, $k' \in \mathbb{Z}$.

, Logo o menor inteiro positivo que satisfaz o sistema será $k' = 0$, ou seja, $\boxed{x = 283}$ //

Ex2) Mostrar que se p é um primo ímpar, então $p \mid 2(p-3)! + 1$.

Como p é primo e maior que 2, pelo Teorema de Wilson, temos: $(p-1)! \equiv -1 \bmod p$

$\Leftrightarrow p \mid (p-1)! + 1$

, mas $(p-1)! = (p-1)(p-2)(p-3)!$, isto pois $p > 2$.

$\Leftrightarrow (p-1)! = (p^2 - 2p - p + 2)(p-3)!$

$\Leftrightarrow (p-1)! = p(p-3) + 2(p-3)!$ (i)

, Logo como p divide qualquer combinação linear de si mesmo, (Verifique!), então $p \mid p(p-3)$ (ii)

, Sendo assim, por Wilson: $p \mid (p-1)! + 1$

(i) $\Rightarrow p \mid p(p-3) + 2(p-3)! + 1$

, como $p \mid p(p-3)$ (ii), então

Segue que: $\boxed{p \mid 2(p-3)! + 1}$ //

OBS:

Propriedades usadas:

Se $p \mid p$, então $p \mid ap$ //

Se $p \mid a+b$ e $p \mid a$, então $p \mid b$ //

(Verifiquem!)

Ex3) Encontrar o dígito das unidades de $2^{70}+3^{70}$ quando expresso na base 13.

Note que encontrar o dígito das unidades por uma base é equivalente a determinar o resto de sua divisão pela base em questão.

Sendo assim, como 13 é primo e $MDC(2,13)=MDC(3,13)=1$, então por Fermat, temos:

$\Rightarrow 2^{12}\equiv 1 \mod 13$ e $\Rightarrow 3^{12}\equiv 1 \mod 13$

$()^5 \Leftrightarrow (2^{12})^5\equiv 1^5 \mod 13$ e $\Leftrightarrow (3^{12})^5\equiv 1^5 \mod 13$

$\Leftrightarrow 2^{60}\equiv 1 \mod 13$ e $\Leftrightarrow 3^{60}\equiv 1 \mod 13$

$\cdot 2^4 \Leftrightarrow 2^{64}\equiv 16 \mod 13$ e $\cdot 3^4 \Leftrightarrow 3^{64}\equiv 81 \mod 13$

Resto $\Leftrightarrow 2^{64}\equiv 3 \mod 13$ e Resto $\Leftrightarrow 3^{64}\equiv 3 \mod 13$

$\cdot 2^3 \Leftrightarrow 2^{67}\equiv 24 \mod 13$ e $\cdot 3^3 \Leftrightarrow 3^{67}\equiv 81 \mod 13$

Resto $\Leftrightarrow 2^{67}\equiv 11 \mod 13$ e Resto $\Leftrightarrow 3^{67}\equiv 3 \mod 13$

$\cdot 2^3 \Leftrightarrow 2^{70}\equiv 88 \mod 13$ e $\cdot 3^3 \Leftrightarrow 3^{70}\equiv 81 \mod 13$

Resto $\Leftrightarrow 2^{70}\equiv 10 \mod 13$ e Resto $\Leftrightarrow 3^{70}\equiv 3 \mod 13$

Logo somando os dois últimos, temos: $2^{70}+3^{70}\equiv 3+10 \mod 13$

$\Leftrightarrow 2^{70}+3^{70}\equiv 0 \mod 13$

ou seja, o resto da divisão de $2^{70}+3^{70}$ por 13 é **zero**.

EX4) Em $\mathbb{Z}_{14}$ determinar todos os elementos inversíveis junto com seus inversos.

Todos elementos inversíveis de $\mathbb{Z}_{14}$, serão: $\{1, 3, 5, 9, 11, 13\}$, ou seja, todos $\alpha \in \mathbb{Z}_{14}$, tal que $MDC(\alpha, 14) = 1$, onde $\alpha \neq 0$.

Seus inversos, serão:

$\overline{1} \cdot \overline{1} = \overline{1}$; $(\overline{1})$

$\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$; $(\overline{5})$

$\overline{5} \cdot \overline{3} = \overline{15} = \overline{1}$; $(\overline{3})$

$\overline{9} \cdot \overline{11} = \overline{99} = \overline{1}$; $(\overline{11})$

$\overline{11} \cdot \overline{9} = \overline{99} = \overline{1}$; $(\overline{9})$

$\overline{13} \cdot \overline{13} = \overline{169} = \overline{1}$; $(\overline{13})$ //

EX5) Mostrar em $\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)/\sim$ a operação de soma é bem definida.

Para mostra que a operação de soma está bem definida, basta mostrar que a definição da soma em $\mathbb{Q}$ independe dos representantes da classe de equivalência, isto é, sejam $\alpha, \alpha', \beta, \beta' \in \mathbb{Q}$, onde $\alpha = \frac{a}{b}$; $\alpha' = \frac{a'}{b'}$; $\beta = \frac{c}{d}$ e $\beta' = \frac{c'}{d'}$, com $a, b, c, d' \in \mathbb{Z}$ e $a', b', c', d' \in \mathbb{Z}^*$

se $\alpha = \alpha'$ e $\beta = \beta'$, então $\alpha + \beta = \alpha' + \beta'$.

Dem: Tome: $\alpha = \frac{a}{b} = \frac{a'}{b'} = \alpha'$ e $\beta = \frac{c}{d} = \frac{c'}{d'} = \beta'$

, Sendo assim, ficamos com: $\begin{cases} ab' = a'b \ (i) \\ cd' = dc' \ (ii) \end{cases}$

$\Leftrightarrow$ • (i) por dd' $\Rightarrow$ $ab'dd' = a'bdd'$

• (ii) por bb' $\Rightarrow$ $cd'bb' = dc'bb'$

$\oplus \Rightarrow ab'dd' + cd'bb' = a'bdd' + dc'bb'$

$\Leftrightarrow b'd'(ad+bc) = bd(a'd'+b'c')$

$\Leftrightarrow \dfrac{ad+bc}{bd} = \dfrac{a'd'+b'c'}{b'd'}$

$\underset{\text{SOMA}}{\overset{\text{def}}{\Leftrightarrow}}$ $\boxed{\alpha+\beta = \alpha'+\beta'}$ //

OBS: Note que $\dfrac{a}{b}+\dfrac{c}{d} \overset{\text{def}}{=} \dfrac{ad+bc}{bd}$ //

EX6) Determinar um sistema completo de resíduos módulo 11 que só tenha números ímpares. Pode achar o mesmo sistema módulo 4? Justifique.

Basta para cada $\alpha \in \mathbb{Z}_{11}$, onde $0 \leq \alpha < 11$ for da forma $\alpha = 2k$; $k \in \mathbb{Z}$, tomar seu representante ímpar, ficamos assim: $\{11, 1, 13, 3, 15, 5, 17, 7, 19, 9, 21\}$ //

, Note que: $\overline{11} = \overline{0}$; $\overline{13} = \overline{2}$; $\overline{15} = \overline{4}$; $\overline{17} = \overline{6}$; $\overline{19} = \overline{8}$ e $\overline{21} = \overline{10}$.

Sistema módulo 4:

Não; pois todo sistema completo de resíduos módulo 4, nunca teremos todos representantes ímpares, sempre teremos 2 pares. Note, um exemplo: $C = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, C é um S.C.R mod 4 mas note que todos elementos das classes de equivalência $\overline{0}$ e $\overline{2}$ serão sempre pares.