AULA 14: **ARITMÉTICA** – APLICAÇÕES DE CONGRUÊNCIAS, ARITMÉTICA MODULAR.

-Exercícios:

I. $x^3 + 21y^2 + 5 = 0$
$X^3 + 21y^2 = -5$.
Para esta equação ter soluções inteiras $x^3 \equiv -5 \equiv 2 \pmod 7$.
Analisando todos os possíveis restos de x^3 por 7:
$x \equiv 0 \pmod 7 \rightarrow x^3 \equiv 0^3 \equiv 0 \pmod 7$
$x \equiv 1 \pmod 7 \rightarrow x^3 \equiv 1^3 \equiv 1 \pmod 7$
$x \equiv 2 \pmod 7 \rightarrow x^3 \equiv 2^3 \equiv 1 \pmod 7$
$x \equiv 3 \pmod 7 \rightarrow x^3 \equiv 3^3 \equiv 6 \pmod 7$
$x \equiv 4 \pmod 7 \rightarrow x^3 \equiv 4^3 \equiv 1 \pmod 7$
$x \equiv 5 \pmod 7 \rightarrow x^3 \equiv 5^3 \equiv 6 \pmod 7$
$x \equiv 6 \pmod 7 \rightarrow x^3 \equiv 6^3 \equiv 6 \pmod 7$.
Portanto x^3 não é congruente à 2 módulo 7 e a equação não tem soluções inteiras.

II. a) Sendo 'n' o número que será elevado ao quadrado, temos 8 possibilidades:
$n \equiv 0 \pmod 8 \rightarrow n^2 \equiv 0^2 \equiv 0 \pmod 8$
$n \equiv 1 \pmod 8 \rightarrow n^2 \equiv 1^2 \equiv 1 \pmod 8$
$n \equiv 2 \pmod 8 \rightarrow n^2 \equiv 2^2 \equiv 4 \pmod 8$
$n \equiv 3 \pmod 8 \rightarrow n^2 \equiv 3^2 \equiv 1 \pmod 8$
$n \equiv 4 \pmod 8 \rightarrow n^2 \equiv 4^2 \equiv 0 \pmod 8$
$n \equiv 5 \pmod 8 \rightarrow n^2 \equiv 5^2 \equiv 1 \pmod 8$
$n \equiv 6 \pmod 8 \rightarrow n^2 \equiv 6^2 \equiv 4 \pmod 8$
$n \equiv 7 \pmod 8 \rightarrow n^2 \equiv 7^2 \equiv 1 \pmod 8$.
Portanto n^2 só é congruente à 0, 1 ou 4 módulo 8.

b) $20 \equiv 4 \pmod 8$. Multiplicando ambos os lados da congruência por 10:
$200 \equiv 40 \equiv 0 \pmod 8$. Se continuarmos multiplicando por 10 sempre encontraremos um número congruente à 0 módulo 8. Assim:
$2 \equiv 2 \pmod 8$. Somando a primeira congruência acima:
$22 \equiv 6 \pmod 8$. Somando a segunda:

$222 \equiv 6 \pmod 8$. Procedendo desta forma concluímos que dos números da sequência, todos, à exceção do 2, são congruentes à 6 módulo 8 e pelo item anterior nenhum será um quadrado perfeito.

c) $3 \equiv 3 \pmod 8$ e $8 \equiv 0 \pmod 8$. Somando as duas congruências:
$11 \equiv 3 \pmod 8$. Adicionando sucessivamente a segunda congruência só encontraremos números congruentes à 3 módulo 8 e pelo item 'a' não haverá nenhum quadrado perfeito entre eles.

III. Na divisão por 100 são 100 restos possíveis, mas sendo 'n' um número natural qualquer:
$n \equiv 0 \pmod{10} \to n^2 \equiv 0^2 \equiv 0 \pmod{10}$
$n \equiv 1 \pmod{10} \to n^2 \equiv 1^2 \equiv 1 \pmod{10}$
$n \equiv 2 \pmod{10} \to n^2 \equiv 2^2 \equiv 4 \pmod{10}$
$n \equiv 3 \pmod{10} \to n^2 \equiv 3^2 \equiv 9 \pmod{10}$
$n \equiv 4 \pmod{10} \to n^2 \equiv 4^2 \equiv 6 \pmod{10}$
$n \equiv 5 \pmod{10} \to n^2 \equiv 5^2 \equiv 5 \pmod{10}$
$n \equiv 6 \pmod{10} \to n^2 \equiv 6^2 \equiv 6 \pmod{10}$
$n \equiv 7 \pmod{10} \to n^2 \equiv 7^2 \equiv 9 \pmod{10}$
$n \equiv 8 \pmod{10} \to n^2 \equiv 8^2 \equiv 4 \pmod{10}$
$n \equiv 9 \pmod{10} \to n^2 \equiv 9^2 \equiv 1 \pmod{10}$.
Portanto n^2 só é congruente à 0, 1, 4, 5, 6 ou 9 módulo 10 e estas são as únicas possibilidades para o algarismo das unidades do resto da divisão de um número por 100. Temos agora $6 \cdot 10 = 60$ restos possíveis.
Mas se 'n' for da forma $10x + 5$, seu quadrado será $100x^2 + 100x + 25$. Como os dois primeiros são múltiplos de 100, conclui-se que os algarismos das dezenas e unidades do quadrado de número terminado em 5 são respectivamente o 2 e o 5. Então temos agora como possíveis restos na divisão por 100, $5 \cdot 10 + 1 = 51$ números e pelo Princípio das Casas dos Pombos, entre 52 números quaisquer haverão pelo menos 2 com o mesmo resto na divisão por 100.