AULA 11: **ARITMÉTICA** – CONGRUÊNCIAS, CRITÉRIOS DE DIVISIBILIDADE E RESTOS, CONGRUÊNCIAS E SOMAS, CONGRUÊNCIAS E PRODUTOS.

- Textos para estudo:

- Seções 4.1 a 4.4 da Apostila 1 da OBMEP, "Iniciação à Aritmética", A. Hefez.
  http://www.obmep.org.br/docs/apostila1.pdf

- Vídeo aulas do Portal da Matemática:

- Tópicos Adicionais:
  Módulo: "Aritmética dos Restos"
  http://matematica.obmep.org.br/index.php/modulo/ver?modulo=63

Vídeo aulas:
"Aritmética Modular",
"Cuidado! Cortes nem sempre valem em congruências. Classe inversa módulo n" e
"Caso em que vale a lei do corte".

- Exercícios:

I. Um inteiro é dito um *quadrado perfeito* quando ele é o quadrado de um inteiro. Usando congruências, encontre os possíveis algarismos das unidades de um quadrado perfeito.

II. Usando congruências, prove que $30^{99} + 61^{100}$ é divisível por 31.

III. Usando congruências, encontre o resto da divisão do número $10^{10} + 10^{100} + 10^{1000} + \cdots + 10^{10.000.000.000}$ por 7.

IV. **Problema 4.5.** Sejam a um número inteiro qualquer e m um inteiro maior do que 1. Suponha que r seja um número inteiro tal que $0 \leq r < m$ e $a \equiv r \bmod m$. Mostre que r é o resto da divisão de a por m.

SUGESTÃO: Utilize a unicidade da escrita no Algoritmo da Divisão.

V. **Problema 4.9.** Determine os restos da divisão por 4, 8, 25 e 125 dos números: 3 254, 12 736, 54 827, 33 875 435, 57 612 510.

VI. **Problema 4.13.** Sem efetuar as somas e subtrações indicadas, determine os restos da divisão por $2, 3, 4, 5, 8, 9, 10, 25$ e 125 do número $3\,534\,785 + 87\,538 - 9\,535\,832$.

VII. **Problema 4.16.** Sem efetuar as multiplicações indicadas, determine os restos da divisão por $2, 3, 4, 5, 8, 9, 10, 25$ e 125 do número $5\,327\,834^3 \times 3\,842\,536^2 \times 9\,369\,270\,001^{20}$.

Note que $2 \times 3 \equiv 2 \times 6 \bmod 6$, mas no entanto $3 \not\equiv 6 \bmod 6$. Portanto, no caso das congruências não vale um cancelamento análogo ao caso da igualdade.

VIII. **Problema 4.17.** Sejam a, b, c e m números inteiros e com $m > 1$. Mostre que se $a \times c \equiv b \times c \bmod m$ e se $\mathrm{mdc}(c, m) = 1$, então $a \equiv b \bmod m$.