1 Problemas para a aula de 05/11

- Notando que $7^2 \equiv 5 \mod 11$, determinar, sem ser por tentativa e erro, quais as soluções de

$$x^{12} + 3x^{11} + 5 \equiv 0 \mod 11$$

- Determinar (sem esforço...) a única solução da equação

$$47x^{120} + 7x^{100} + 54x^{20} + 25x + 2 \equiv 0 \mod 101$$

- Verificando que

$x^{11}-x \equiv (x^3+2x^2+5x+6)(x^8-2x^7-x^6+6x^5+3x^4+3x^3-2x^2+4x+6)+2x^2-3$

determinar se existem e quais são as soluções de $x^3 + 2x^2 + 5x + 6 \equiv 0 \mod 11$.

- Se g é raiz primitiva de p, para que valores de k é que g^k também é raiz primitiva?

- Sabendo que 5 é uma raiz primitiva de 47 e que $5^{16} \equiv 17 \mod 47$, determinar as soluções da equação "exponencial"

$$25^x \equiv 17 \mod 47$$

- Se p é um primo ímpar, para quantos $a \in \mathbb{Z}_{/p}$ é que

$$x^2 \equiv a \mod p$$

tem solução?
Sugestão: Seja g uma raiz primitiva de p e $g^k \equiv a$. Estudar a existência de solução em função da paridade de k.

- Mostrar que se p é primo ímpar então

$$x^2 \equiv -1 \mod p$$

tem solução se e só se $p \equiv 1 \mod 4$.

- Mostrar que existem infinitos primos congruentes com 1 módulo 4.

  Sugestão: Dados primos $p_1, p_2, \cdots, p_k$ congruentes com 1 módulo 4, considerar os factores primos de

  $$(p_1 p_2 \cdots p_k)^2 + 1$$

- Mostrar que se p e q são primos ímpares diferentes e a é primo com pq,

  $$a^{\phi(pq)/2} \equiv 1 \mod pq.$$

  Concluir que pq não tem raizes primitivas.

- Usar o critério de Euler para determinar quais das seguintes equações têm solução e qual o seu número

  a) $x^{12} \equiv 16 \mod 17$;

  b) $x^{20} \equiv 13 \mod 17$;

  c) $x^{48} \equiv 9 \mod 17$;

  d) $x^{11} \equiv 9 \mod 17$;

- Mostrar que $3^8 \equiv -1 \mod 17$. Justificar porque é que podemos concluir que 3 é raiz primitiva de 17.
  Usar uma lista das classes de congruência de $3^i \mod 17$ para encontrar as soluções do problema anterior.

- 3 é raiz primitiva módulo 31 e $3^{12} \equiv 8 \mod 31$. Determinar as soluções de

  $$x^4 \equiv 8 \mod 31.$$