Introdução à Teoria dos Números
Aula de Problemas 6.

1. Aplicar o algoritmo da divisão aos polinómios com coeficientes em $\mathbb{Z}_5$ $f(x) = x^5 - x$ e $g(x) = 2x^3 + x + 4$.

2. 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 $x^3 + 2x^2 + 5x + 6 \equiv 0 \mod 11$.

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

4. Mostrar que se p é primo ímpar então

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

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

5. 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

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

6. 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.

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

8. Mostrar que $3^8 \equiv -1 \mod 17$. Justificar porque é que podemos concluir que 3 é raiz primitiva de 17.