Introdução à Teoria dos Números

Exame - 26/02/2022

Atenção: justifique cuidadosamente todas as respostas
O exame consiste nas perguntas 1., 2., 3., 4. e 5. e uma das perguntas 6. e 7.

1. a) (3 valores) Determinar as soluções da equação modular

$$234x \equiv 54 \mod 315.$$

b) (2 valores) Determinar, para cada $d \in \{1, 3, 5\}$, para quantos valores de $1 \leq m \leq 315$ a equação modular

$$mx \equiv 54 \mod 315$$

tem exactamente d soluções.

2. (2 valores) Sabendo que $d = m.d.c.(a, b)$ determinar o valor de $m.d.c.(ab, a^2 + b^2)$.

3. (3 valores) Determinar os algarismos das unidades e das dezenas de 19^{82}.

4. (3 valores) Sabendo que 3 é raiz primitiva módulo 31 e que $3^{10} \equiv -6 \mod 31$, determinar os $0 < x < 31$ que são solução da equação

$$27x^{33} + 1 \equiv 0 \mod 31.$$

5. Seja p um primo ímpar e a e b duas raizes primitivas módulo p.

a) (2 valores) Calcular $a^{\frac{p-1}{2}}$ e justificar se ab pode ser raiz primitiva módulo p.

b) (2 valores) Determinar, em função de p, o número de pares de inteiros $0 \leq t < p-1$, $0 \leq s < p-1$ para os quais $a^t b^s$ é raiz primitiva módulo p.

6. (3 valores) Mostrar que a equação

$$(x^2-2)(x^2-3)(x^2-6) \equiv 0 \mod p$$

tem solução para todo o primo p.
Sugestão: Aplicar o Critério de Euler.

7. (3 valores) Mostrar que a equação modular $x^2 + x + 1 \equiv 0 \mod p$, onde p é primo, tem duas soluções distintas se e só se $p \equiv 1 \mod 3$.
Sugestão: $(x-1)(x^2+x+1) = x^3 - 1$.