LISTA DE EXERCÍCIOS DE TEORIA DOS NÚMEROS

HEMAR GODINHO
DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDADE DE BRASÍLIA

1. Ordem, Raiz Primitiva e Índice

(1) Seja $p = 29$ e considere $E(29) = \{1, 2, 3, \ldots, 26, 27, 28\}$.
   (a) Encontre todas as raízes primitivas módulo 29.
   (b) Para cada divisor positivo de $\phi(29)$ determine T_d, o conjunto de todos os elementos de $E(29)$ de ordem d.
   (c) Verifique que $\sum_d \phi(d) = \phi(29)$, onde a soma percorre todos os divisores positivos de $\phi(29)$.
   (d) Escolha uma raíz primitiva g módulo 29 e determine o índice de todos os elementos de $E(29)$ na base g.

(2) Utilizando os métodos e teoremas descritos nas videoaulas, mostre que a congruência $3x^{35} \equiv 7 \pmod{29}$ tem solução e determine todas as suas soluções.

(3) Utilize o algoritmo descrito nas videoaulas para determinar uma raiz primitiva módulo 421.

(4) Use a teoria apresentada nas videoaulas para determinar uma raiz primitiva g_n módulo 17^n para todo $n \in \mathbb{N}$.

(5) Seja p um primo ímpar. Mostre que se g_1 e g_2 são raizes primitivas módulo p então $g_1 - g_2$ não é raiz primitiva módulo p.

(6) Seja p um primo tal que $p \equiv 1 \pmod 4$. Mostre que se g é raiz primitiva módulo p então $-g$ também é raiz primitiva módulo p. Verifique isso para $p = 17$.

(7) Sejam $a, b, p \in \mathbb{N}$ tais que p é um primo ímpar e $a \equiv b^2 \pmod p$. Mostre que a não é uma raiz primitiva módulo p.

Departamento de Matemática, Universidade de Brasília, Brasília-DF, Brasil