

Elementos de Teoria dos Números (2020.3) - Lista 6  
Prof. Ricardo Bortolotti

**Capítulo 6 (Raízes Primitivas)**

1. Encontre uma raiz primitiva módulo: 5, 6, 10, 11, 18, 19.
2. Mostre que se  $m$  é inteiro positivo,  $a$  é inteiro com  $(a, m) = 1$  e  $\text{ord}_m a = m - 1$ , então  $m$  é primo.
3. Mostre que os divisores primos ímpares de  $n^2 + 1$  são da forma  $4k + 1$ .
4. Mostre que se  $m$  divide  $n$  e  $a$  é raiz primitiva módulo  $n$ , então  $a$  é raiz primitiva módulo  $m$ .
5. Mostre que 2 é raiz primitiva módulo 25. Conclua que 2 é raiz primitiva módulo  $5^k$  para todo  $k \geq 1$ .
6. Sendo  $p > 2$  primo e  $a > 1$  um inteiro, mostre que os divisores primos ímpares da  $a^p + 1$  são divisores de  $a + 1$  ou são da forma  $2np + 1$ .
7. Mostrar que se  $a$  é uma raiz primitiva módulo  $p$  (primo) com  $p \equiv 1 \pmod{4}$ , então  $-a$  também é raiz primitiva.
8. Mostrar que se  $a$  é resíduo quadrático módulo  $p$  (primo ímpar), então  $a$  não é raiz primitiva módulo  $p$ .