MA 553, Teoria Aritmética dos Números
Terceira lista de exercícios
Segundo semestre de 2019

1. Encontrar os primos $p > 2$ tais que $\left(\frac{360}{p}\right) = 1$.

2. Calcular os símbolos de Legendre $\left(\frac{237}{1009}\right)$, $\left(\frac{3}{1009}\right)$, $\left(\frac{1007}{1009}\right)$, $\left(\frac{44}{103}\right)$, $\left(\frac{2019}{1019}\right)$, $\left(\frac{-60}{1019}\right)$.

3. Calcular os símbolos de Jacobi $\left[\frac{32}{635}\right]$, $\left[\frac{429}{565}\right]$, $\left[\frac{86}{181}\right]$, $\left[\frac{77}{2019}\right]$.

4. Seja $A = \{1, 2, \ldots, p-1\}$ onde p é primo positivo. Calcular $\sum_{a=1}^{p-1}(\frac{a^2}{p})$ para $p > 2$ e $\sum_{a=3}^{p-1}(\frac{a}{p})$ para $p > 3$.

5. Seja p um primo ímpar. Denotamos $s(a,p) = \sum_{n=1}^{p}\left(\frac{n(n+a}{p}\right)$. (Aqui assumimos que se p divide b, o símbolo de Legendre $(\frac{b}{p}) = 0$.)
a) Mostrar que $s(0,p) = p-1$.
b) Mostrar que $\sum_{a=1}^{p} s(a,p) = 0$.
c) Se p não divide a, mostrar que $s(a,p) = s(1,p)$.
d) Se p não divide a, mostrar que $s(a,p) = -1$.

6. Calcular para qual p primo positivo a congruência $f(x) \equiv 0 \pmod{p}$ tem solução onde $f(x) = x^2 + x + 1$; $f(x) = (x^2-6)(x^2-5)$.

7. Seja p um número primo impar. Então 3 não é residuo quadrático módulo p se e somente se $p \equiv \pm 5 \pmod{12}$.

8. Se p é número primo positivo usando o fato que existe raiz primitiva calcular o número de raizes primitivas. Calcular todas raizes primitivas módulo p para $p = 11$.

9. Mostrar que se a é uma raiz primitiva módulo um primo $p = 4k+1$ então $-a$ também é uma raiz primitiva.

10. Mostrar que para primo $p > 2$ e inteiro $a > 1$ todos os divisores primos impares de $a^p + 1$ são divisores de $a+1$ ou são da forma $2np+1$.

11. Sejam a e m dois números naturais e $(a,m) = 1$. Sejam $a^k \equiv 1 \pmod{m}$ e $a^t \not\equiv 1 \pmod{m}$ para todo $t \in [1, k-1]$, então indicamos $k = |a|$ a ordem de a módulo m. Demonstrar que se $|a| = k$, então $|a^r| = \dfrac{k}{(r,k)}$ onde (r,k) é o maior divisor comum de r e k.

12. Mostrar que se n ínteiro positivo então 2 é raiz primitiva módulo 5^n. (Dica: Indução por n. Se $k_n = |2|_{5^n}$, suponha $k_n = 4 \cdot 5^{n-1}$ e $k_{n+1} \neq 4 \cdot 5^n$. Mas k_{n+1} divide $4 \cdot 5^n$, $2^{k_{n+1}} \equiv 1 \pmod{5^{n+1}}$ e $2^{k_{n+1}} \equiv 1 \pmod{5^n}$, donde k_n divide k_{n+1}. Segue $k_{n+1} = 4 \cdot 5^{n-1}$. Pela indução $2^{4 \cdot 5^{n-2}} \equiv -1 \pmod{5^n}$ e $2^{4 \cdot 5^{n-2}} \equiv 1 \pmod{5^{n-1}}$, $2^{4 \cdot 5^{n-2}} = 5n - 1t + 1$ onde t é coprimo com 5. De $2^{4 \cdot 5^{n-1}} - 1 = (2^{4 \cdot 5^{n-2}})^5 - 1$ mostre que 5^{n+1} não divide $2^{4 \cdot 5^{n-1}} - 1$, absurdo.)