Elementos de Teoria dos Números (2020.3) - Prova 2

Prof. Ricardo Bortolotti

1. a) Determine se 5 é resíduo quadrático módulo 103.

   b) Quais são os primos p para os quais 5 é resíduo quadrático?

   Solução:

   a) Pela Lei da Reciprocidade Quadrática:

$$\left(\frac{5}{103}\right)\left(\frac{103}{5}\right) = (-1)^{2\cdot 51} = 1.$$

   Então $\left(\frac{5}{103}\right) = \left(\frac{103}{5}\right) = \left(\frac{3}{5}\right)$. E notamos que é -1 porque os resíduos quadráticos módulo 5 são $1^2 = 1$ e $2^2 = 4 \equiv -1 \pmod 5$.

   b) Pela Lei da Reciprocidade Quadrática:

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{2\cdot \frac{p-1}{2}} = 1.$$

   Então $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. E, como vimos, os resíduos quadráticos módulo 5 são os inteiros da forma $5k+1$ e $5k+4$.

   Portanto, a resposta são os números primos da forma $5k \pm 1$.

2. Seja p um primo ímpar, prove que se g é uma raiz primitiva módulo p então

$$g^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

   Solução: Note que $g^{p-1} \equiv 1 \pmod p$. E como g é raiz primitiva: $\operatorname{ord}_p g = \Phi(p) = p-1$.

   Denotando $x = g^{\frac{p-1}{2}}$, temos $x^2 = g^{p-1} \equiv 1 \pmod p$.

$$\Rightarrow p|x^2 - 1 = (x-1)(x+1) \Rightarrow p|x-1 \text{ ou } p|x+1.$$

   Afirmamos que não pode ocorrer $p|x-1$. Se isso ocorresse, teríamos $g^{\frac{p-1}{2}} = x \equiv 1 \pmod p$, mas isto implicaria que $\operatorname{ord}_p g \leq \frac{p-1}{2}$, o que não é o caso.

   Então $p|x+1$, isso implica que $-1 \equiv x = g^{\frac{p-1}{2}} \pmod p$, e segue o resultado.

3. Seja p um primo ímpar, considere o primo de Mersenne $M_p = 2^p - 1$ e q um divisor primo de M_p.

   a) Prove que 2 tem ordem p módulo q.

   b) Usando o item anterior, conclua que $2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$.

   c) Usando o item anterior, conclua que 2 é resíduo quadrático módulo q e que $q \equiv \pm 1 \pmod 8$.

   Solução:

   a) $q|2^p - 1 \Rightarrow 2^p \equiv 1 \pmod{q}$.

   Seja $k = \text{ord}_q 2$, por propriedade da ordem: $k|p$.

   Como p é primo, temos $k = 1$ ou $k = p$. $k = 1$ não acontece pois 2^1 claramente não é 1 módulo q. Logo $k = p$.

   b) Pelo Teorema de Fermat, temos $2^{q-1} \equiv 1 \pmod{q}$. Logo, por propriedade da ordem: $p|q-1$.

   Como p é primo ímpar e $q-1$ é par, segue que $p|\frac{q-1}{2}$. Portanto $2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$.

   c) Pelo critério de Euler:

$$\left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \equiv 1 \pmod{q}.$$

   E vimos (por exemplo, no Teorema 5.10) que $\left(\frac{2}{q}\right) \equiv 1$ se e somente se $q \equiv \pm 1 \pmod 8$.

4. a) Encontre a fração contínua que representa o número $\sqrt{13}$.

   b) Determine qual o números representado pela fração contínua $[1, \overline{2, 3}] = [1, 2, 3, 2, 3, \cdots]$.

   c) Sabendo que $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \cdots]$, encontre os primeiros 6 convergentes desta fração contínua.

   Solução:

   a) Temos $a_1 = \lfloor \sqrt{13} \rfloor = 3$ e $x_1 = \frac{1}{\sqrt{13}-3} = \frac{\sqrt{13}+3}{4}$. Continuando:

   $a_2 = \lfloor \frac{\sqrt{13}+3}{4} \rfloor = 1$ e $x_2 = \frac{1}{\frac{\sqrt{13}+3}{4}-1} = \frac{1}{\frac{\sqrt{13}-1}{4}} = \frac{4}{\sqrt{13}-1} = \frac{4(\sqrt{13}+1)}{12} = \frac{\sqrt{13}+1}{3}$.

   $a_3 = \lfloor \frac{\sqrt{13}+1}{3} \rfloor = 1$ e $x_3 = \frac{1}{(\frac{\sqrt{13}+1}{3})-1} = \frac{3}{\sqrt{13}-2} = \frac{3(\sqrt{13}+2)}{9} = \frac{\sqrt{13}+2}{3}$.

   $a_4 = \lfloor \frac{\sqrt{13}+2}{3} \rfloor = 1$ e $x_4 = \frac{1}{\frac{\sqrt{13}+2}{3}-1} = \frac{1}{\frac{\sqrt{13}-1}{3}} = \frac{3}{\sqrt{13}-1} = \frac{3(\sqrt{13}+1)}{12} = \frac{\sqrt{13}+1}{4}$.

   $a_5 = \lfloor \frac{\sqrt{13}+1}{4} \rfloor = 1$ e $x_5 = \frac{1}{(\frac{\sqrt{13}+1}{4})-1} = \frac{1}{\frac{\sqrt{13}-3}{4}} = \frac{4(\sqrt{13}+3)}{4} = \sqrt{13}+3$.

   $a_6 = \lfloor \sqrt{13}+3 \rfloor = 6$ e $x_6 = \frac{1}{(\sqrt{13}+3)-6} = \frac{\sqrt{13}+3}{4} = x_1$.

Como $x_6 = x_1$, de agora em diante a sequência vai repetir: $a_7 = a_2 = 1$, $a_8 = a_3 = 1$, $a_9 = a_4 = 1$, $a_{10} = a_5 = 1$, $a_{11} = a_6 = 6$, etc. Portanto

$$\sqrt{13} = [3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, \cdots] = [3, \overline{1, 1, 1, 1, 6}].$$

b) Chamando o período de y, temos: $[1, \overline{2, 3}] = 1 + \frac{1}{y}$, onde y satisfaz:

$$y = 2 + \frac{1}{3 + \frac{1}{y}} = 2 + \frac{1}{\frac{3y+1}{y}} = 2 + \frac{y}{3y+1} = \frac{6y + 1 + y}{3y + 1}$$

$$\Rightarrow 3y^2 + y = 6y + 1 + y \Rightarrow 3y^2 - 6y - 1 = 0 \Rightarrow y = \frac{6 \pm \sqrt{36 + 12}}{6} = 1 + \frac{2\sqrt{3}}{3}.$$

Obs: descartamos a raiz negativa porque y é positivo.

c) Vamos calcular através da relação: $p_i = a_i p_{i-1} + p_{i-2}$ e $q_i = a_i q_{i-1} + q_{i-2}$ $\forall i \geq 3$.
Da expansão $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \cdots]$, temos $a_1 = 2$, $a_2 = 1$, $a_3 = 2$, $a_4 = 1$, $a_5 = 1$, $a_6 = 4$. Também temos $p_1 = a_1 = 2$, $p_2 = a_1 a_2 + 1 = 3$, $q_1 = 1$, $q_2 = a_2 = 1$, logo:

$$p_3 = 2 \cdot 3 + 2 = 8 \text{ e } q_3 = 2 \cdot 1 + 1 = 3 \Rightarrow c_3 = \frac{8}{3},$$

$$p_4 = 1 \cdot 8 + 3 = 11 \text{ e } q_4 = 1 \cdot 3 + 1 = 4 \Rightarrow c_4 = \frac{11}{4},$$

$$p_5 = 1 \cdot 11 + 8 = 19 \text{ e } q_5 = 1 \cdot 4 + 3 = 7 \Rightarrow c_5 = \frac{19}{7},$$

$$p_6 = 4 \cdot 19 + 11 = 87 \text{ e } q_6 = 4 \cdot 7 + 4 = 32 \Rightarrow c_6 = \frac{87}{32}.$$