NÚMEROS INTEIROS E CRIPTOGRAFIA – UFRJ

GABARITO 7: EQUAÇÃO DE PELL MODULAR

1. 2 é resíduo quadrático relativamente a 7 e 17 e 3 é resíduo quadrático relativamente a 11 e 13. Para descobrir isto liste todos os quadrados módulo o primo e verifique se 2 ou 3 aparece entre eles. Lembre-se que, como
$$(n-a)^2 \equiv (-a)^2 \pmod{n}$$
basta listar os quadrados dos números menores que $(n-1)/2$.

2. O único resíduo quadrático módulo 5 é 4, módulo 7 temos 2 e 4 e módulo 11 temos $3, 4, 5, 9$. Esta questão é resolvida usando a mesma estratégia que a anterior.

3. Se a e b são resíduos quadráticos módulo p, então existem inteiros a_1 e b_1 tais que
$$a \equiv a_1^2 \pmod{p} \quad \text{e} \quad b \equiv b_1^2 \pmod{p},$$
de modo que
$$ab \equiv a_1^2 \cdot b_1^2 \equiv (a_1 b_1)^2 \pmod{p}$$
também é resíduo quadrático módulo p. Na a letra (b) temos que
$$a \equiv a_1^2 \pmod{p} \quad \text{e} \quad ab \equiv 1 \pmod{p},$$
donde
$$(a_1)^2 b \equiv 1 \pmod{p}.$$
Em particular, a_1 é inversível módulo p. Se a_1' for o inverso de a_1 módulo p, então, multiplicando esta última congruência por $(a_1')^2$, obtemos
$$b \equiv (a_1')^2 \cdot (a_1)^2 b \equiv (a_1')^2 \pmod{p}$$
de modo que b também é resíduo quadrático módulo p.

4. Usando o método explicado nas notas de aula, temos que
$$\mathcal{P}(3,5) = [[\overline{4},\overline{0}],[\overline{3},\overline{4}],[\overline{3},\overline{1}],[\overline{2},\overline{4}],[\overline{2},\overline{1}],[\overline{1},\overline{0}]];$$
$$\mathcal{P}(4,5) = [[\overline{4},\overline{0}],[\overline{1},\overline{0}],[\overline{0},\overline{4}],[\overline{0},\overline{1}]];$$
$$\mathcal{P}(3,7) = [[\overline{6},\overline{0}],[\overline{5},\overline{6}],[\overline{5},\overline{1}],[\overline{2},\overline{6}],[\overline{2},\overline{1}],[\overline{1},\overline{0}],[\overline{0},\overline{4}],[\overline{0},\overline{3}]];$$
$$\mathcal{P}(4,7) = [[\overline{6},\overline{0}],[\overline{4},\overline{4}],[\overline{4},\overline{3}],[\overline{3},\overline{4}],[\overline{3},\overline{3}],[\overline{1},\overline{0}]].$$

5. Como $P = [\overline{8}, \overline{2}]$ e $Q = [\overline{7}, \overline{4}]$, temos que
$$P^{-1} = [\overline{8}, -\overline{2}] = [\overline{8}, \overline{15}]$$
donde
$$S = P^{-1} \otimes Q = [\overline{8}, \overline{15}] \otimes [\overline{7}, \overline{4}] = [\overline{15}, \overline{1}]$$

6. Os geradores de $\mathcal{P}(3,5)$ são $[\overline{3}, \overline{4}]$ e $[\overline{3}, \overline{1}]$, geradores de $\mathcal{P}(4,5)$ são $[\overline{0}, \overline{4}]$ e $[\overline{0}, \overline{1}]]$, geradores de $\mathcal{P}(3,7)$ são
$$[\overline{5}, \overline{6}], [\overline{5}, \overline{1}], [\overline{2}, \overline{6}] \quad \text{e} \quad [\overline{2}, \overline{1}]$$
e os geradores de $\mathcal{P}(3,5)$ são $[\overline{4}, \overline{4}]$ e $[\overline{4}, \overline{3}]$.

7. Como 1541 não é primo, não podemos afirmar que $x^2 - 4y^2 \equiv 1 \pmod{1541}$ tem 1540 soluções. Mas podemos adaptar o mesmo método usado para contar as soluções usado no caso do módulo primo, porque 4 é obviamente um resíduo quadrático módulo 1541. Para isto, fatoramos $x^2 - 4y^2$, o que nos dá
$$(x - 2y)(x + 2y) \equiv x^2 - 4y^2 \equiv 1 \pmod{1541}.$$
Mas isto significa que $x - 2y$ tem que ser inversível módulo 1541 e $x + 2y$ tem que ser seu inverso. Portanto, devemos ter
$$x - 2y = \overline{a} \in U(1541)$$
donde
$$x + 2y = \overline{a}'$$
em que $\overline{a}'$ é o inverso de $\overline{a}$ em $U(1541)$. Mas o sistema
$$x - \overline{2}y = \overline{a}$$
$$x + \overline{2}y = \overline{a}'$$
nos dá
$$\overline{2}x = \overline{a} + \overline{a}' \quad \text{e} \quad \overline{4}y = \overline{a}' - \overline{a}.$$
Como 2 e 4 são inversíveis módulo 1541, podemos concluir que o sistema acima *sempre tem uma única solução*. Logo, haverá uma solução da equação $x^2 - 4y^2 \equiv 1 \pmod{1541}$ para cada escolha
$$x - 2y = \overline{a} \in U(1541)$$
Mas $\#U(1541 = \phi(1541) = 1452$, de modo que o argumento acima mostra que $x^2 - 4y^2 \equiv 1 \pmod{1541}$ tem 1452 soluções. O mesmo argumento mostra que se n é ímpar então $x^2 - 4y^2 \equiv 1 \pmod{n}$ tem $\phi(n)$ soluções.

8. Como $\overline{2} = \overline{60}^2$, temos que 2 é resíduo quadrático módulo 257, de modo que $\mathcal{P}(2, 97)$ tem $257 - 1 = 256 = 2^8$ elementos. Logo, pelo teorema de Lagrange combinado com o lema chave, a ordem de P tem que dividir 2^8. Em particular, a ordem de P tem que ser uma potência de 2. Como foi dado no problema que $P^{64} = [\overline{0}, \overline{34}]$, sabemos que a ordem de P não pode ser uma potência de 2 menor ou igual a que 2^6. Mas,

$$P^{128} = (P^{64})^2 = [\overline{256}, \overline{0}] = [\overline{-1}, \overline{0}]$$

cujo quadrado é o elemento neutro. Portanto, P tem ordem 2^8, já que nenhuma potência de P com expoente da forma 2^k e $k < 8$ é igual a $[\overline{1}, \overline{0}]$. Para fazer o item (b), basta notar que, como P tem ordem $256 = 8 \cdot 32$ então P^{32} tem que ter ordem 8. De fato, se r for a ordem de P^{32}, então

$$(P^{32})^r = P^{32r} = [\overline{1}, \overline{0}];$$

de modo que, pelo lema chave, a ordem de P tem que dividir $32r$. Mas o menor r para o qual 256 divide $32r$ é $r = 8$. Portanto, para completar a questão, basta achar as coordenadas de P^{32}. Mas, Em vez de calcular P^{32} diretamente, prefiro usar o fato de que

$$P^{64} = (P^{32})^2.$$

Supondo que $P^{32} = [\overline{a}, \overline{b}]$, teremos que

$$[\overline{0}, \overline{34}] = P^{64} = (P^{32})^2 = [\overline{a^2 + 2b^2}, \overline{2ab}],$$

donde

$$\overline{a^2 + 2b^2} = \overline{0} \text{ e } \overline{2ab} = \overline{34}.$$

Mas $P^3 2$ é solução de $x^2 - \overline{2}y^2 = \overline{1}$, de modo que

$$\overline{a^2 - 2b^2} = \overline{1}.$$

Subtraindo esta última igualdade de $\overline{a^2 + 2b^2} = \overline{1}$, obtemos

$$\overline{4b^2} = \overline{-1} = \overline{256};$$

donde $\overline{b^2} = \overline{64}$, que nos dá $\overline{b} = \overline{8}$. Logo, de $\overline{2ab} = \overline{34}$ obtemos $\overline{16a} = \overline{34}$; isto é, $\overline{8a} = \overline{17}$. Mas $\overline{8}$ tem inverso $\overline{225}$ de modo que

$$a = \overline{225} \cdot \overline{17} = \overline{227}.$$

Assim, $Q = [\overline{227}, \overline{8}]$.

Como $P^2 = [\overline{31}, \overline{134}]$, efetuando o cálculo acima obtemos

$$P^{32} = [\overline{253}, \overline{176}] \otimes [\overline{31}, \overline{134}] = [\overline{140}, \overline{26}]$$

Se você encontrar algum erro no gabarito, por favor comunique ao professor através do endereço `collier@dcc.ufrj.br`. Qualquer dúvida entre em contato com os monitores via Facebook. As aulas de monitoria serão nas segundas-feiras 13h-15h