Číslo cvičení: 6
Jméno: Marek Bryša
UČO: 323771
Login: xbrysa1

1. $n = 11 \cdot 13 \implies$
   $w^2 = 56 \mod 11 \implies w_1 = 1,\, w_2 = 10 \mod 11$
   $w^2 = 56 \mod 13 \implies w_3 = 2,\, w_4 = 11 \mod 13$
   $w_1 = 11k + 1 = 13l + 2 \implies w_1 = 67$
   $w_2 = 11k + 10 = 13l + 2 \implies w_1 = 54$
   $w_3 = 11k + 1 = 13l + 11 \implies w_1 = 89$
   $w_4 = 11k + 10 = 13l + 1 \implies w_1 = 76$

2.

3. The only $p > 7$ such that none of 3,5,7 are its quadratic residues is 17.
   $15^{(17-1)/2} = 15^8 = 21^8 = 35^8 = 1 \mod p$, $105^8 = -1 \mod p \implies$
   15,21,35 are quadratic residues, 105 is not.

4. $y = q^x \mod p = 137565$, $a = q^r \mod p = 89804$, $b = y^r w \mod p = 7512 \implies$
   $c = (89804, 7512)$
   $w = b(a^x)^{-1} \mod p = 7512 \cdot 22233 \mod p = 15131$

5. $\lg_5 112 \mod 131$, $q = 5, y = 112, p = 131$, $m = 12$
   $L_1 = (1, 117, 65, 7, 33, 62, 49, 100, 41, 81, 45, 25)$
   $L_2 = (112, 101, 125, 25, 5, 1, 105, 21, 109, 48, 62, 91)$
   $25 \in L_1, L_2 \implies i = 3, j = 11 \implies x = 12 \cdot 11 + 3 = 135$

6. There are $\frac{p-1}{2}$ quadratic residues. They result from $1^2, 2^2, \ldots, (p-1)^2$.
   Since $a^2 = (-a)^2$, they form pairs $1^2 = (p-1), \ldots, (\frac{p-1}{2})^2 = (\frac{p+1}{2})^2 \mod p$.
   None of them are congruent $\mod p$. Let $a^2 = b^2 \mod p$, $1 \leq a \leq b \leq \frac{p-1}{2}$.
   $p | a^2 - b^2 = (a+b)(a-b) \implies p|(a+b) \vee p|(a-b)$. The first one is impossible because of the constrains for a, b. The second one can only hold for $a - b = 0 \implies a = b$.