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. Because we know all the w_i, $gcd(|w_i - w_j|, n) = p$ or q.
   $gcd(|1234 - 39593|, 189209) = 431 \implies 189209 = 431 \cdot 439 \implies p = 431,\ q = 439.$
   $v_1 = 85780^{((431+1)/4)} \mod 189209 = 28292$, $v_2 = 431 - 85780^{((431+1)/4)} \mod 189209 = 161348$,
   $v_3 = 85780^{((439+1)/4)} \mod 189209 = 133509$, $v_4 = 439 - 85780^{((439+1)/4)} \mod 189209 = 56139$

3. In Z_{17} 3,5,7 are not quadratic residues. $15^{(17-1)/2} = 15^8 = 21^8 = 35^8 = 1 \mod p$, $105^8 = -1 \mod p \implies$
   15,21,35 are quadratic residues.
   According to the theorem on p. 17 of the Appendix, 105 cannot be a quadratic residue.
   $3 = g^k$, $5 = g^l$, $7 = g^j$, k, l, j are odd. $105 = 3 \cdot 5 \cdot 7 = g^{(k+l+j)}$, $(k + l + j)$ is odd.

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 $a^2 = b^2 \mod p$, $1 \le a \le b \le \frac{p-1}{2}$.
   $p | a^2 - b^2 = (a + b)(a - b) \implies p|(a + b) \vee p|(a - b)$. The first one is impossible because of the constrains for a, b. The second one can only hold for $a - b = 0 \implies a = b$.

7. $w_1 = 100 \cdot 4^{-42} = 122 \mod 503$
   $w_2 = 457 \cdot 299^{-42} = 30 \mod 503$

8. (a)
   $$\bar{p}(n) = \frac{n!\binom{365}{n}}{365^n},\ p = 1 - \bar{p}$$
   $\bar{p}(45) = 0.0590241 \implies p(45) = 0.9409759$

   (b) $\bar{p}(31) = 0.2695, \bar{p}(32) = 0.2466 \implies$ There must be at least 32 people.