Solutions to homework #8

1. Let $p > 3$ be a prime. Prove that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 11 \mod 12 \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \mod 12 \end{cases}$$

in two different ways:

(i) using quadratic reciprocity

(ii) directly using Gauss lemma

Solution: (i) Using quadratic reciprocity: If $p \equiv 1 \mod 4$, then

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 3 \\ -1 & \text{if } p \equiv 2 \mod 3 \end{cases}$$

If $p \equiv 3 \mod 4$, then

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 2 \mod 3 \\ -1 & \text{if } p \equiv 1 \mod 3 \end{cases}$$

Thus, $\left(\frac{3}{p}\right) = 1 \iff$ either

(i) $p \equiv 1 \mod 4$ and $p \equiv 1 \mod 3$ or

(ii) $p \equiv 3 \mod 4$ and $p \equiv 2 \mod 3$

Clearly, (i) is equivalent to $p \equiv 1 \mod 12$ and (ii) is equivalent to $p \equiv 11 \mod 12$.
Thus, $\left(\frac{3}{p}\right) = 1 \iff p \equiv 1, 11 \mod 12$, and $\left(\frac{3}{p}\right) = -1$ in the remaining cases, that is, $\iff p \equiv 5, 7 \mod 12$.
(ii) Using Gauss lemma: this is done by considering four cases. All cases are similar, so we will do just one of them: $p = 12k + 5$. In the notations from class we have $P = \{1, 2, \ldots, 6k+2\}$, $3P = \{3, \ldots, 6k, 6k+3, \ldots, 12k+3, 12k+6, \ldots, 18k+6\}$ and

$$\overline{3P} = \{\underbrace{3, \ldots, 6k}_{\text{group } I}, \underbrace{-(6k+2), \ldots, -2}_{\text{group } II}, \underbrace{1, \ldots, 6k+1}_{\text{group } III}\}.$$

Elements in groups I and III lie in P and elements in group II lie N. Hence, $|\overline{3P} \cap N|$ is the number of elements in group II, which equals $(6k+2-2)/3+1 = 2k+1$. This number is odd, so by Gauss lemma $\left(\frac{3}{p}\right) = -1$.

2. Let q be an odd prime, and set $N = q$ if $q \equiv 1 \mod 4$ and $N = 4q$ if $q \equiv 3 \mod 4$. Prove that if p is an odd prime different from q, then the Legendre symbol $\left(\frac{q}{p}\right)$ is completely determined by the congruence class of p mod N. In other words, prove that there exist integers $a_1, \ldots, a_t$ and $b_1, \ldots, b_s$ depending only on q such that

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv a_1, \ldots, \text{ or } a_t \mod N \\ -1 & \text{if } p \equiv b_1, \ldots, \text{ or } b_s \mod N \end{cases}$$

Solution: By definition, to prove that $\left(\frac{q}{p}\right)$ is completely determined by $[p]_N$, we need to show the following:

Let p_1 and p_2 be primes such that $p_1 \equiv p_2 \mod N$. Then $\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_2}\right)$.
We consider the cases $q \equiv 1 \mod 4$ and $q \equiv 3 \mod 4$ separately.
Case 1: $q \equiv 1 \mod 4$. Then

$$\left(\frac{q}{p_1}\right) = \left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right) = \left(\frac{q}{p_2}\right)$$

where the first and third equalities hold by quadratic reciprocity and the second holds since $p_1 \equiv p_2 \mod q$.

Case 2: $q \equiv 3 \mod 4$. Then

$$\left(\frac{q}{p_1}\right) = (-1)^{\frac{p_1-1}{2}\frac{q-1}{2}} \left(\frac{p_1}{q}\right) \tag{1}$$

$$\left(\frac{q}{p_2}\right) = (-1)^{\frac{p_2-1}{2}\frac{q-1}{2}} \left(\frac{p_2}{q}\right). \tag{2}$$

We are given that $p_1 \equiv p_2 \mod 4q$, so $p_1 \equiv p_2 \mod q$ and $p_1 \equiv p_2 \mod 4$. The first congruence implies that $(\frac{p_1}{q}) = (\frac{p_2}{q})$. The second congruence implies that $\frac{p_1-1}{2}\frac{q-1}{2} - \frac{p_2-1}{2}\frac{q-1}{2} = \frac{p_1-p_2}{2}\frac{q-1}{2}$ is even, whence $(-1)^{\frac{p_1-1}{2}\frac{q-1}{2}} = (-1)^{\frac{p_2-1}{2}\frac{q-1}{2}}$. Therefore, (1) and (2) implies that $\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_2}\right)$.

3. Let p be an odd prime, let $a \in \mathbb{Z}$ be coprime to p, and let $k \geq 1$ be an integer. Use the lifting method to prove that a is a quadratic residue mod $p^k \iff a$ is a quadratic residue mod p. Note that a completely different (group-theoretic) proof of this fact is given in the book (Theorem 7.13)

Solution: The forward implication is obvious. Conversely, suppose that a is a quadratic residue mod p. This means that $gcd(a, p) = 1$ and the

congruence $x^2 \equiv a \mod p$ has a solution x_0. Then $gcd(a, p^k) = 1$ as well. Let $f(x) = x^2 - a$. Then $f'(x_0) = 2x_0$ is not divisible by p since p is odd and $p \nmid a = x^2$. Therefore, by the lifting theorem, x_0 lifts to a solution to $x^2 \equiv a \mod p^k$. Hence a is a quadratic residue mod p^k.

4. Let Q_n be the group of quadratic residues mod n (in this problem we think of quadratic residues as elements of U_n, not as integers, which is the convention that the book uses).

(a) Let n be an odd integer. Prove that $|Q_n| = \frac{\phi(n)}{2^k}$ where k is the number of distinct prime divisors of n.

(b) Prove that Q_{105} is a cyclic group of order 6.

(c) Find a generator for Q_{105}.

Solution: (a) Let $n = p_1^{a_1} \dots p_k^{a_k}$ be the prime factorization of n. By Theorem 7.15 (book) we have $Q_n \cong Q_{p_1^{a_1}} \times \dots \times Q_{p_k^{a_k}}$, and by Lemma 7.3 (book) we have $|Q_{p_i^{a_i}}| = \frac{\phi(p_i^{a_i})}{2}$ for each i. Hence

$$|Q_n| = \prod_{i=1}^{k} \frac{\phi(p_i^{a_i})}{2} = \frac{\prod \phi(p_i^{a_i})}{2^k} = \frac{\phi(n)}{2^k}.$$

(b) Using theorems quoted above, $Q_{105} \cong Q_3 \times Q_5 \times Q_7$ is a direct product of cyclic groups of orders $1 = \frac{3-1}{2}$, $2 = \frac{5-1}{2}$ and $3 = \frac{7-1}{2}$. Since $1, 2$ and 3 are pairwise coprime, this direct product is also cyclic (this is a standard fact in group theory which follows, for instance, from the ring-theoretic form of CRT).

(c) To find a generator of Q_{105}, we can take any generators $[u]_3$ of Q_3, $[v]_5$ of Q_5 and $[w]_7$ of Q_7, and then find x such that $x \equiv u \mod 3$, $x \equiv v \mod 5$ and $x \equiv w \mod 7$. Then $[x]_{105}$ is a generator of Q_{105}.
For instance, we can take $u = 1$, $v = w = 4$, which gives $x = 4$.