Homework 6
(The Legendre symobol and Gauss's Lemma.)
Due Friday, November 8 at 11:30am in class.

Note: Be sure to justify your answers. No credit will be given for answers without work/justification. In addition, all written homework assignments should be neat and well-organized; **this assignment has only one part and can be submitted as a single packet**.

(1) Find $\left(\frac{a}{11}\right)$ for each $a \in \mathbb{Z}$.

$$\left(\frac{a}{11}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{11} \\ 1 & \text{if } a \equiv 1, 3, 4, 5, 9 \pmod{11} \\ -1 & \text{if } a \equiv 2, 6, 7, 8, 10 \pmod{11} \end{cases}$$

(2) Let p be an odd prime and $[g]$ and $[h]$ be primitive roots mod p.
(a) Show that $[g], [h] \notin Q_p$.

Proof. Suppose towards a contradiction that $[g] \in Q_p$. Then there is an $[a] \in U_p$ such that $a^2 \equiv g \pmod{p}$. But then

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p}.$$

Since the order of a primitive root mod p is $p-1$, we have reached a contradiction. Similarly, $[h] \notin Q_p$. □

(b) Show that $[gh] \in Q_p$.

Proof. We have that

$$\left(\frac{gh}{p}\right) = \left(\frac{g}{p}\right) \cdot \left(\frac{h}{p}\right) = (-1)(-1) = 1.$$

Thus $[gh] \in Q_p$. □

(3) Let p be an odd prime. Show that

$$[-50] \in Q_p \text{ if and only if } p \equiv 1 \text{ or } 3 \pmod{8}.$$

Proof. If $p = 5$, then it is clear that $[-50] = [0] \notin Q_p$. So assume $p \neq 5$. We have that

$$\begin{aligned} [-50] \in Q_p \text{ iff } & \left(\frac{-50}{p}\right) = 1 \\ \text{iff } & \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)^2 = 1 \\ \text{iff } & \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1 \\ \text{iff } & \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \pm 1 \\ \text{iff } & p \equiv 1 \pmod{4} \text{ and } p \equiv \pm 1 \pmod{8} \\ & \text{OR } p \equiv 3 \pmod{4} \text{ and } p \equiv \pm 3 \pmod{8} \\ \text{iff } & p \equiv 1 \pmod{8} \text{ OR } p \equiv 3 \pmod{8} \end{aligned}$$

□

(4) Suppose that q is a prime number such that $q \equiv 1 \pmod 4$ and suppose that the number $p = 2q + 1$ is also a prime number. Show that $[2]$ is a primitive root mod p.

Proof. Suppose that q is a prime number such that $q \equiv 1 \pmod 4$ and suppose that the number $p = 2q + 1$ is also a prime number. Then note that $\phi(p) = p - 1 = 2q$. So the only prime divisors of $\phi(p)$ are 2 and q. We have that

$$2^{\phi(p)/q} = 2^2 = 4 \not\equiv 1 \pmod p$$

since $p = 2q + 1 \geq 2(5) + 1 = 11$. We need to show that

$$2^{\phi(p)/2} = 2^q \not\equiv 1 \pmod p.$$

Euler's Criterion tells us that

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

So we just need to compute $\left(\frac{2}{p}\right)$. Since $q \equiv 1 \pmod 4$, we have that $q = 4k+1$ for some k and so

$$p = 2(4k + 1) + 1 = 8k + 3 \equiv 3 \pmod 8.$$

Since $p \not\equiv \pm 1 \pmod 8$, we know that $[2] \notin Q_p$. So $\left(\frac{2}{p}\right) = -1$. Thus

$$2^{\phi(p)/2} \equiv -1 \not\equiv 1 \pmod p.$$

Therefore, $[2]$ is a primitive root mod p. □

(5) (a) Use Euler's Criterion to determine if $[5]$ is a quadratic residue mod 23.
We have that

$$\left(\frac{5}{23}\right) \equiv 5^{11} \equiv (5^2)^5 \cdot 5 \equiv 2^5 \cdot 5 \equiv 9 \cdot 5 \equiv 45 \equiv -1 \pmod{23}.$$

So $[5]$ is not a quadratic residue mod 23.

(b) Use Gauss's Lemma to determine if $[5]$ is a quadratic residue mod 23. We have that

$$P = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

and

$$N = \{-1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11\}.$$

So

$$\begin{aligned} 5P &= \{5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55\} \\ &= \{5, 10, -8, -3, 2, 7, -11, -6, -1, 4, 9\}. \end{aligned}$$

Thus

$$5P \cap N = \{-8, -3, -11, -6, -1\}$$

and so $\mu = |5p \cap N| = 5$. So by Gauss's Lemma,

$$\left(\frac{5}{23}\right) = (-1)^\mu = (-1)^5 = -1.$$

So $[5]$ is not a quadratic residue mod 23.