Homework #7. Solutions to selected problems.

1. Let p be an odd prime. Prove that $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0$.

Solution: By Lemma 7.3 from the book, precisely half of the integers in the interval $[1,p-1]$ are quadratic residues (while the other half are non-residues). Therefore in the sum $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)$ half of the terms are equal to 1 and half are equal to -1, so the sum is equal to 0.

Here is a slightly different solution. Let $s=\sum_{a=1}^{p-1}(\frac{a}{p})$. Since $(\frac{0}{p})=0$, we have $s=\sum_{a=0}^{p-1}(\frac{a}{p})$. Note that $s+p=\sum_{a=0}^{p-1}((\frac{a}{p})+1)$. Denote by $N(a)$ the number of reduced solutions to the congruence $x^2\equiv a \mod p$. As shown in class, $N(a)=(\frac{a}{p})+1$, so $s+p=\sum_{a=0}^{p-1}N(a)$.

On the other hand, each integer $x_0\in[0,p-1]$ arises as a reduced solution to $x^2\equiv a \mod p$ for unique $a\in[0,p-1]$ (namely $a=x_0^2 \mod p$). Therefore, $\sum_{a=0}^{p-1}N(a)$ is equal to the number of integers in $[0,p-1]$, that is, equal to p. So, $s+p=p$, whence $s=0$.

4. Let $a,b,c\in\mathbb{Z}$. Prove that for any prime p, the congruence $(x^2-ab)(x^2-ac)(x^2-bc)\equiv 0 \mod p$ has a solution.

Solution: Suppose that $(x^2-ab)(x^2-ac)(x^2-bc)\equiv 0 \mod p$ has no solutions. Then each of the congruences $(x^2-ab)\equiv 0 \mod p$, $(x^2-ac)\equiv 0 \mod p$ and $(x^2-bc)\equiv 0 \mod p$ has no solutions, which means that

$$\left(\frac{ab}{p}\right)=\left(\frac{ac}{p}\right)=\left(\frac{bc}{p}\right)=-1.$$

Multiplying these equalities together and using multiplicativity of the Legendre symbol in the numerator, we get $\left(\frac{a^2b^2c^2}{p}\right)=-1$. On the other hand, $(\frac{a^2b^2c^2}{p})=(\frac{abc}{p})^2\geq 0$, which is a contradiction.

5. The goal of this problem is to use Legendre symbols to prove that there are infinitely many primes of the form $8n+3, 8n+5$ and $8n+7$.

(a) Prove that there are infinitely many primes of the form $8n+5$.

(b) Now prove that there are infinitely many primes of the form $8n+7$.

(c) Finally prove that there are infinitely many primes of the form $8n+3$.

Solution: (a) Assume that there are only finitely many primes $p_1, \ldots, p_k$ of the form $8n + 5$, and let $m = 4(p_1 \ldots p_k)^2 + 1$. First note that since $z^2 \equiv 1 \mod 8$ for any odd z, we have $m \equiv 4 \cdot 1 + 1 = 5 \mod 8$.

Now let p be any prime divisor of m. Then p is odd (since m is odd) and $p \neq p_i$ for any i. Since m has the form $x^2 + 1$, the congruence $x^2 + 1 \equiv 0 \mod p$ has a solution, so $(\frac{-1}{p}) = 1$, and therefore (since p is odd), $p \equiv 1 \mod 4$.

Thus, all primes divisors of p are congruent to 1 mod 4, so congruent to 1 or 5 mod 8. If all prime divisors were congruent to 1 mod 8, then m itself would be congruent to 1 mod 8, which is not the case. Therefore, m has at least prime divisor of the form $8n + 5$ (different from $p_1, \ldots, p_k$), which is a contradiction.

(b) Again assume that there are only finitely many primes $p_1, \ldots, p_k$ of the form $8n + 7$, and let $m = (p_1 \ldots p_k)^2 - 2$. Then $m \equiv 1 - 2 \equiv 7 \mod 8$.

By the same argument as in (a), for each prime p dividing m we have $(\frac{2}{p}) = 1$, so $p \equiv 1$ or $7 \mod 8$.

As in (a), since m is congruent to 7 mod 8, it cannot be a product of primes of the form $8n + 1$, so m has a divisor of the form $8n + 7$ (different from $p_1, \ldots, p_k$), again a contradiction.

(c) We know that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \mod 8 \\ -1 & \text{if } p \equiv 3, 5 \mod 8 \end{cases} ; \quad \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 5 \mod 8 \\ -1 & \text{if } p \equiv 3, 7 \mod 8 \end{cases}$$

Multiplying these equalities, we get that

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3 \mod 8 \\ -1 & \text{if } p \equiv 5, 7 \mod 8 \end{cases} \qquad (***)$$

Now suppose that there are only finitely many primes $p_1, \ldots, p_k$ of the form $8n + 3$, and let $m = (p_1 \ldots p_k)^2 + 2$. Then $m \equiv 1 + 2 = 3 \mod 8$. As in (a) and (b), we first use (***) to prove that all prime divisors of m have the form $8n+1$ or $8n+3$ and then argue that at least one of those prime divisors has the form $8n + 3$.

6. Let p be an odd prime.

(a) Prove that $\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \mod p$ (this congruence will be used in the proof of quadratic reciprocity in class). **Hint:** write each expression as a product of $p - 1$ elements and show that after suitable reordering of factors, the i^{th} factor on the left is congruent mod p to the i^{th} factor on the right, for each i.

(b) Use (a) and Wilson's theorem to prove that if $p \equiv 3 \mod 4$, then $\left(\frac{p-1}{2}\right)! \equiv \pm 1 \mod p$.

Solution: Let $N = \left(\frac{p-1}{2}\right)!^2 = \prod_{i=1}^{\frac{p-1}{2}} i \cdot \prod_{j=1}^{\frac{p-1}{2}} j$. Let us subtract p from each factor in the second product $\prod_{j=1}^{\frac{p-1}{2}} j$. Then the resulting number N' will be congruent to N mod p. On the other hand,

$$N' = \prod_{i=1}^{\frac{p-1}{2}} i \cdot \prod_{j=-(p-1)}^{\frac{-(p+1)}{2}} j = \prod_{i=1}^{\frac{p-1}{2}} i \cdot (-1)^{\frac{p-1}{2}} \cdot \prod_{\frac{(p+1)}{2}}^{p-1} j = (-1)^{\frac{p-1}{2}} (p-1)!.$$

Thus, $\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p-1}{2}} (p-1)! \mod p$, as desired.

(b) By Wilson's theorem, $(p-1)! \equiv -1 \mod p$, so by (a) $\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}}$ mod p. If $p \equiv 3 \mod 4$, the right-hand side of this congruence is equal to 1. Since $x^2 \equiv 1 \mod p$ implies $x \equiv \pm 1 \mod p$, we conclude that $\left(\frac{p-1}{2}\right)! \equiv \pm 1$ mod p.