HOMEWORK ASSIGNMENT #8 SOLUTIONS

(1) Let $p > 3$ be a prime. Let $r_1, \ldots, r_{\phi(p-1)}$ be the primitive roots mod p satisfying $1 < r_i < p$. Show that the product of all the r_i is congruent to $1 \mod p$.

Solution. We do this by showing that if g is a primitive root mod p, then g^{-1} is as well. Indeed, let g be primitive mod p. Suppose $(g^{-1})^d \equiv g^{-d} \equiv 1 \mod p$. Then $g^d \equiv 1 \mod p$ as well, so $(p-1) \mid d$, and therefore g^{-1} has order $p-1$ and is primitive mod p.

Since $p > 3$, we also have $g \not\equiv g^{-1} \mod p$, because $g \equiv g^{-1} \mod p$ implies $g^2 \equiv 1 \mod p$, or that g has order 2. Therefore in the list of primitive roots $r_1, \ldots, r_{\phi(p-1)}$, we can pair each root with its inverse, and this pairing partitions the primitive roots. When we multiply all the roots in this list together we get $1 \mod p$, because the product of each root with its inverse is $1 \mod p$. □

(2) Without using a calculator, determine whether 112 is a quadratic residue mod 659 or not. You may assume that 659 is a prime number.

Solution. We will calculate $\left(\frac{112}{659}\right)$. First, we factor $112 = 2^4 \cdot 7$. Since $\left(\frac{2}{659}\right)^4 = 1$, $\left(\frac{112}{659}\right) = \left(\frac{7}{659}\right)$. Since $659 \equiv 3 \mod 4, 7 \equiv 3 \mod 4$, quadratic reciprocity says $\left(\frac{7}{659}\right) = -\left(\frac{659}{7}\right) = -\left(\frac{1}{7}\right) = -1$, so 112 is not a quadratic residue mod 659. □

(3) If $p \equiv 1 \mod 4$ is a prime, show that

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

Solution. Notice that for $1 \leq k \leq (p-1)/2$, $k \equiv -(p-k) \mod p$. Therefore

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \left(\frac{p-1}{2}\right)! \cdot \left(\frac{-(p+1)}{2}\frac{-(p+3)}{2}\cdots(-(p-2))(-(p-1))\right) \mod p.$$

Notice that the last expression is, up to the $(p-1)/2$ negative signs appearing, the same as $(p-1)!$. Therefore

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

Since $p \equiv 1 \mod 4, (p-1)/2$ is even, so $(-1)^{(p-1)/2} = 1$, and Wilson's theorem says that $(p-1)! \equiv -1 \mod p$, as desired. □

(4) Recall that for an odd prime p, a product of quadratic non-residues is a quadratic residue, and that exactly half of the $p-1$ elements of U_p are quadratic residues. Show that for $n = 8$, neither of these properties holds: that is, the number of quadratic residues in U_8 is not half the size of U_8, and that a product of two quadratic non-residues in U_8 might not be a quadratic residue.

Solution. One immediately checks that the only quadratic residue of U_8 is $1 \mod 8$, so the quadratic residues are only $1/4$ the elements of U_8. Similarly, $3, 5 \mod 8$ are quadratic non-residues, but their product is $15 \equiv 7 \mod 8$, which is also a quadratic non-residue. □

(5) Let $p > 3$ be a prime. Show that the sum of the quadratic residues (between 1 and p) mod p is congruent to 0 mod p.

Solution. Notice that the quadratic residues mod p are given by $1^2, 2^2, \ldots, ((p-1)/2)^2 \mod p$: there are $(p-1)/2$ such numbers, and they are all distinct mod p, because if $i^2 \equiv j^2 \mod p$, then $p \mid (i-j)(i+j)$, and if $1 \leq i, j \leq (p-1)/2$, then this is only possible if $i = j$. Therefore the sum of the quadratic residues mod p is the same as the sum

$$1^2 + 2^2 + \ldots + \left(\frac{p-1}{2}\right)^2 \mod p,$$

and we calculate the sum of the first $(p-1)/2$ squares using the formula $1^2 + \ldots + n^2 = n(n+1)(2n+1)/6$:

$$1^2 + \ldots + \left(\frac{p-1}{2}\right)^2 = \frac{p-1}{2}\frac{p+1}{2}\frac{p}{6} = \frac{p(p-1)(p+1)}{24}.$$

On the one hand, this last expression is an integer, since it is the sum of integers. On the other hand, p divides this integer, because p appears in the numerator but not the denominator (since $p > 3$). Therefore, mod p this entire expression is 0, as desired. □

(6) Give a characterization of all primes p such that $1, 2, 3, 4, 5$ are all quadratic residues mod p. Your final answer should be in the form $p \equiv a_1, a_2, \ldots, a_r \mod n$ for various integers a_i and an integer n. Exhibit such a p. (For the last part, you can use a calculator to test for primality.)

Solution. First, 1 is a quadratic residue mod p for any prime p. We already proved that 2 is a quadratic residue mod p if and only if $p \equiv 1, 7 \mod 8$. We also know that 4 is a quadratic residue mod p for any $p > 2$, since $4 = 2^2$. (The reason we need $p > 2$ is because 4 is not relatively prime to 2, hence cannot be a quadratic residue mod 2.) So we are left with the cases of $3, 5$ mod p. We use quadratic reciprocity.

We first calculate when $\left(\frac{5}{p}\right) = 1$. First, we need $p \neq 5$, which in any case must be true if $\left(\frac{2}{p}\right) = 1$. Next, since $5 \equiv 1 \mod 4$, quadratic reciprocity says that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. But this is equal to 1 if and only if $p \equiv 1, 4 \mod 5$, because $1, 4$ are the only squares mod 5. Therefore 5 is a quadratic residue mod p if and only if $p \equiv 1, 4 \equiv \pm 1 \mod 5$.

Next we calculate when $\left(\frac{3}{p}\right) = 1$. Again, we need $p \neq 3$. We now have to separately consider two cases: when $p \equiv 1 \mod 4$ and when $p \equiv 3 \mod 4$. In the former, quadratic reciprocity tells us that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$, and this equals 1 exactly when $p \equiv 1 \mod 3$. Notice that $p \equiv 1 \mod 3, p \equiv 1 \mod 4$ is equivalent to $p \equiv 1$

mod 12. If $p \equiv 3 \mod 4$, then quadratic reciprocity tells us that $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 2 \mod 3$. One checks that $p \equiv 3 \mod 4, p \equiv 2 \mod 3$ is true if and only if $p \equiv 11 \mod 12$. So altogether, $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1, 11 \equiv \pm 1 \mod 12$.

So the end result is that $1, 2, 3, 4, 5$ are all quadratic residues mod p if and only if the following congruences are satisfied:

$$p \equiv \pm 1 \mod 8, p \equiv \pm 1 \mod 12, p \equiv \pm 1 \mod 5.$$

(Notice that we also have the condition $p \neq 2$ arising from the fact that 4 is a quadratic residue mod p, but this is automatically contained in any of these congruences.)

We first find an equivalent set of congruences to the first two congruences listed above. Since $8, 12$ are not coprime, we cannot quite use the Chinese Remainder Theorem, but the modification of the CRT given in the textbook when the moduli are not coprime tell us that we can find an equivalent set of congruences to mod $\text{lcm}(8, 12) = 24$. If $p \equiv \pm 1 \mod 8$, then $p \equiv 1, 7, 9, 15, 17, 23 \mod 24$, and of these six choices, the only ones that are $\equiv \pm 1 \mod 12$ are $1, 23 \mod 24$. So the first two congruences are equivalent to $p \equiv \pm 1 \mod 24$.

Therefore, we want to find p satisfying $p \equiv \pm 1 \mod 24, p \equiv \pm 1 \mod 5$. Since the moduli are coprime, the CRT tells us that there will be exactly four congruence classes mod 120 satisfying these two conditions. Since $p \equiv \pm 1 \mod 24$ implies $p \equiv \pm 1, 24 \pm 1, 48 \pm 1, 72 \pm 1, 96 \pm 1 \mod 120$, and the only of these ten classes mod 120 which are also congruent to $\pm 1 \mod 5$ are $1, 49, 71, 119$ mod 120, we see that the primes p which satisfy the original conditions of the problem are $p \equiv 1, 49, 71, 119$ mod 120.

There are actually infinitely many primes p which satisfy these congruence conditions, but $p = 241 \equiv 1 \mod 120$ works. Also, $p = 71 \equiv 71 \mod 120$ is also prime. □