TJUSAMO 2011 – Number Theory 3

Mitchell Lee, Andre Kessler

1 Quadratic Residues

Given an odd prime p and an integer a, a is said to be a *quadratic residue* (or just *residue*) mod p if there is some b with $b^2 \equiv r \pmod{p}$. Many known results about quadratic residues come from the following result:

Theorem 1.1 (Primitive Root Theorem)**.** *Let p be a prime. Let g be called a* primitive root *mod p if $\{1, g, g^2, \cdots, g^{p-2}\} \equiv \{1, 2, \cdots, p-1\} \pmod{p}$.*
Then, for every prime p, there is a primitive root mod p.

If we square each of $1, g, g^2, \cdots, g^{p-2}$, we find that $1, g^2, g^4, \cdots, g^{p-3}$ are the nonzero quadratic residues mod p. In particular:

Corollary 1.2. *For any odd prime p, there are $\frac{p-1}{2}$ nonzero quadratic residues in mod p.*

In fact, we have the even stronger result:

Corollary 1.3. *For any odd prime p and $d|p-1$, there are $\frac{p-1}{d}$ nonzero d-th powers in mod p.*

What is $g^{\frac{p-1}{2}}$? First of all, we note that $g^{\frac{p-1}{2}}$ is not 1 mod p, because then 1 appears twice in the list $\{1, g, g^2, \cdots, g^{p-2}\}$. We also have

$$(g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \equiv g^{p-1} - 1 \equiv 0 \pmod{p},$$

so either $g^{\frac{p-1}{2}} - 1$ or $g^{\frac{p-1}{2}} + 1$ is 0 mod p. Since we have already established that $g^{\frac{p-1}{2}}$ is not 1 mod p, $g^{\frac{p-1}{2}} - 1$ is not divisible by p. Therefore, $g^{\frac{p-1}{2}} + 1$ is 0 mod p and

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Using this in conjunction with the previous result that $1, g^2, g^4, \cdots, g^{p-3}$ are the nonzero quadratic residues mod p, we get:

Theorem 1.4 (Euler's criterion)**.** *If p is an odd prime and a an integer, and*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a nonzero quadratic residue mod } p, \\ 0 & \text{if } a \text{ is zero mod } p, \\ -1 & \text{otherwise} \end{cases}$$

(pronounced "a on p") is the Legendre symbol,

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

In particular, putting $a = -1$, -1 is a quadratic residue mod p if and only if $p = 2$ or $p \equiv 1 \pmod{4}$. Additionally, this theorem implies that the product of two residues is a residue, the product of a (nonzero) residue and a nonresidue is a nonresidue, and the product of two nonresidues is a residue. The law of quadratic reciprocity is also worth mentioning: for all distinct odd primes p, q, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

2 Problems

Many of these problems do not involve any of the things discussed in this lecture; rather, they are meant as general number theory practice.

1. Let p be a prime, and let d be a positive integer. Find the number of dth powers mod p.

2. Let p be a prime. Find the number of primitive roots mod p.

3. Let d be a positive integer and let p be a prime. Find

$$1^d + 2^d + \cdots + (p-1)^d \pmod{p}.$$

4. Let p be a prime number and f an integer polynomial of degree d such that $f(0) = 0, f(1) = 1$ and $f(n)$ is congruent to 0 or 1 modulo p for every integer n. Prove that $d \geq p - 1$.

5. Let P be a polynomial that takes integers to integers. Prove that there are infinitely many primes p for which there exists an integer n with $p|P(n)$.

6. 2010 MOPpers are assigned numbers 1 through 2010. Each one is given a red slip and a blue slip of paper. Two positive integers, A and B, each less than or equal to 2010 are chosen. On the red slip of paper, each MOPper writes the remainder when the product of A and his or her number is divided by 2011. On the blue slip of paper, he or she writes the remainder when the product of B and his or her number is divided by 2011. The MOPpers may then perform either of the following two operations:

   - Each MOPper gives his or her red slip to the MOPper whose number is written on his or her blue slip.
   - Each MOPper gives his or her blue slip to the MOPper whose number is written on his or her red slip.

   Show that it is always possible to perform some number of these operations such that each MOPper is holding a red slip with his or her number written on it.

7. Let p be a prime. Find the number of pairs of positive integers (x, y) which satisfy $x^2 \equiv 1 + y^2 \pmod{p}$.

8. Let p be a prime. Find the number of pairs of positive integers (x, y) which satisfy $x^2 + y^2 \equiv 1 \pmod{p}$.

9. Prove that for each $n \geq 2$, there is a set S of n integers such that $(a-b)^2$ divides ab for every distinct $a, b \in S$.

10. a is a quadratic residue mod all primes p. Prove that a is a perfect square.

11. Let a, b be integers greater than 2. Prove that there exists a positive integer k and a finite sequence $n_1, n_2, \ldots, n_k$ of positive integers such that $n_1 = a$, $n_k = b$, and $n_i n_{i+1}$ is divisible by $n_i + n_{i+1}$ for each i $(1 \leq i < k)$.