Duke Math Meet 2013-14

Power Round

Quadratic Residues and Prime Numbers

For integers a and b, we write $a \mid b$ to indicate that a evenly divides b, and $a \nmid b$ to indicate that a does not divide b. (For example, $2 \mid 4$ and $4 \nmid 2$.)

Let p be a prime number. An integer a is called a **quadratic residue modulo** p if there exists an integer x with $p \mid x^2 - a$. For example, if we take $p = 5$, then 0, 1, and 4 are quadratic residues modulo 5, as $5 \mid 0^2 - 0 = 1^2 - 1 = 2^2 - 4$.

1. a. (1 point.) Explain why for every integer x, there must be an integer k such that x is equal to one of $5k$, $5k + 1$, $5k + 2$, $5k + 3$, or $5k + 4$.

   b. (1 point.) Explain why every integer of the form $5k$, $5k + 1$, or $5k + 4$ is a quadratic residue modulo 5.

   c. (2 points.) Using part (a), show that 2 and 3 are not quadratic residues modulo 5. Explain why every number of the form $5k + 2$ or $5k + 3$ is not a quadratic residue modulo 5.

Given p and a as above, we write

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } p \nmid a; \\ 0 & \text{if } p \mid a \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p. \end{cases}$$

This notation is commonly called the *Legendre symbol.* **Do not confuse this with the fraction a/p!**[1]

2. a. (1 point.) Compute $\left(\frac{2}{5}\right)$ and $\left(\frac{2}{7}\right)$.

   b. (1 point.) Explain why $\left(\frac{a^2}{p}\right) = 1$ for all primes p and integers a with $p \nmid a$.

   c. (2 points.) Show that if $p \mid a - b$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

[1]Yeah, this notation isn't the best. Unfortunately, it's traditional.

3. (3 points.) Suppose that $p > 2$. Explain why exactly $(p+1)/2$ of the numbers $\{0, 1, 2, \cdots, p-1\}$ are quadratic residues modulo p. (Hint: if a is a quadratic residue, factor the polynomial $x^2 - a$.)

4. (4 points.) Using the result of question 3, show that for any prime number p there must exist positive integers a, b with $p \mid a^2 + b^2 + 1$.

A celebrated theorem of Euler gives a somewhat convenient way to calculate Legendre symbols:

Euler's Criterion. *Let $p > 2$ be a prime, and let a be an integer. Then*

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

To see how to use this to compute Legendre symbols, let's calculate $\left(\frac{2}{3}\right)$. We know that $\left(\frac{2}{3}\right) - 2^1$ must be divisible by 3. As $\left(\frac{2}{3}\right)$ must be 1 or -1, it follows that $\left(\frac{2}{3}\right) = -1$. Hence 2 is not a quadratic residue modulo 3.

5. (3 points.) Show that $\left(\frac{-1}{p}\right) = 1$ if $p = 2$ or p is of the form $4k+1$ and $\left(\frac{-1}{p}\right) = -1$ if p is of the form $4k+3$.

6. (5 points.) Show that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

7. (6 points.) Let p be a prime of the form $4k+3$. Using the above results, show that if there exist integers a, b with $p \mid a^2 + b^2$, then $p \mid a$ and $p \mid b$. (Hint: how are $\left(\frac{-1}{p}\right)$ and $\left(\frac{-b^2}{p}\right)$ related?)

The second famous theorem concerning the Legendre symbol is generally credited to Gauss, and is known as the law of quadratic reciprocity:

Quadratic Reciprocity. *Let $p \neq q$ be odd prime numbers. Then*

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

This theorem can be extended to the case $q = 2$ and p odd, in which case it gives

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

8. (6 points.) Calculate, with explanation, $\left(\frac{42}{2017}\right)$

9. (7 points.) Show that if p is a prime and n is an integer with $p \mid n^2 + n + 1$, then either $p = 3$ or $p = 6k + 1$ for some positive integer k. (Hint: multiply by 4.)

10. (8 points.) Let k be an integer, and suppose that p is an odd prime with $p \mid 5k^2 + 1$. Show that the tens digit of p must be even. (Hint: what must $\left(\frac{-5}{p}\right)$ be?)