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 $5k+4$.
   Solution. Using division with remainder, we can write $x = 5k + r$, where $0 \leq r \leq 4$. Thus we have x in the desired form.

   b. (1 point.) Explain why every integer of the form $5k$, $5k+1$, or $5k+4$ is a quadratic residue modulo 5.
   Solution. For $a = 5k$ we may take $x = 0$ in the definition of a quadratic residue; we then have $5 \mid x^2 - a = -5k$ as desired.
   For $a = 5k+1$ we may take $x = 1$, as we obtain $5 \mid 1-(5k+1) = -5k$. Similarly for $a = 5k+4$ we may take $x = 2$.

   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.
   Solution. We show that 2 is not a quadratic residue modulo 5 by contradiction. Suppose there exists x such that $5 \mid x^2 - 2$. Write $x = 5k + r$, so that $x^2 = 25k^2 + 10kr + r^2 = 5(5k^2 + 2kr) + r^2$. Then we must have $5 \mid 5(5k^2+2kr) + r^2 - 2$, so that $5 \mid r^2 - 2$. But we only have 5 possibilities for r, none of which work: 5 does not divide -2, -1, 2, 7, or 14. Hence 2 cannot be a quadratic residue modulo 5. An analogous argument shows that 3 is not a quadratic residue modulo 5 either.
   As $5 \mid x^2 - a$ iff $5 \mid x^2 - (a+5k)$, replacing 2 by $2+5k$ or 3 by $3+5k$ in the above arguments doesn't change their validity. Hence no number of the form $5k+2$ or $5k+3$ is 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 $\left(\frac{2}{7}\right)$.

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

Solution. By 1(c), we know that 2 is not a quadratic residue modulo 5. Hence $\left(\frac{2}{5}\right) = -1$.
We have $7 \mid 3^2 - 2$, so 2 is a quadratic residue modulo 7. Hence $\left(\frac{2}{7}\right) = 1$.

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

Solution. Taking $x = a$ in the definition of a quadratic residue, we have $p \mid a^2 - a^2 = 0$ for all primes p and integers a. Hence a^2 is always a quadratic residue modulo p; if we further assume that $p \nmid a$ then $\left(\frac{a^2}{p}\right) = 1$.

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

Solution. Suppose that $\left(\frac{a}{p}\right) = 1$. Then a is a quadratic residue modulo p, so there exists x with $p \mid x^2 - a$. Hence $p \mid (x^2 - a) + (a - b) = x^2 - b$, so b is a quadratic residue modulo p. Furthermore, if $p \nmid a$ and $p \mid a - b$, then $p \nmid b$, so $\left(\frac{b}{p}\right) = 1$.
If $\left(\frac{a}{p}\right) = 0$, then $p \mid a$. Hence $p \mid a + (b - a) = b$, so $\left(\frac{b}{p}\right) = 0$.
If $\left(\frac{a}{p}\right) = -1$, then there does not exist x with $p \mid x^2 - a$. If there existed x' with $p \mid x^2 - b$, then we would have $p \mid (x^2 - b) + (b - a) = x^2 - a$, a contradiction. Hence b is not a quadratic residue modulo p, and so $\left(\frac{b}{p}\right) = -1$.

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 $x^2 - a$.)

Solution. Consider the pairs $(0, 0), (1, 1), \cdots, (x, \overline{x^2}), \cdots, (p - 1, 1)$, where $\overline{x^2}$ is the unique number between 0 and $p - 1$ such that $p \mid x^2 - \overline{x^2}$. For example, as $p \mid (p - 1)^2 - 1 = p^2 - 2p$, we have $\overline{(p - 1)^2} = 1$.

Then the number of quadratic residues among $\{0, 1, 2, \cdots, p - 1\}$ is clearly the number of distinct second elements among all these pairs. Clearly $\overline{x^2} = \overline{(p - x)^2}$, as $(p - x)^2 = p^2 - 2px + x^2$. Hence 1 and $p - 1$ have the same second element, and similarly for $2, p - 2$ and so on. There are $(p - 1)/2$ of these pairs, and all of them have nonzero second element, as if $p \mid x^2$ then $p \mid x$.

Now we claim that no other pairs have equal second element. For if $x \neq y$ have equal second elements $\overline{x^2}, \overline{y^2}$, then $p \mid 0 = \overline{x^2} - \overline{y^2}$. Hence $p \mid x^2 - y^2 = (x - y)(x + y)$, and thus either $p \mid x - y$ or $p \mid x + y$. Note that as $x, y \in \{0, \cdots, p - 1\}$ we have $0 < |x - y| < p$ and thus $p \nmid x - y$. Hence $p \mid x + y$, and thus $y = p - x$. So no other pairs have equal second elements. Throwing in the second element of zero from the pair $(0, 0)$ does not give us any more collisions, as noted above, and hence there are $(p - 1)/2 + 1 = (p + 1)/2$ quadratic residues among $\{0, 1, 2, \cdots, p - 1\}$.

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

Solution. If $p = 2$ the result is clear: take a even and b odd.

Now if $p > 2$, then exactly $(p + 1)/2$ elements of the set $\{0, 1, 2, \cdots, p - 1\}$ are quadratic residues. The map $x \mapsto p - 1 - x$ maps this set to itself bijectively, and hence by the pigeonhole principle there exists c such that c and $p-1-c$ are quadratic residues. Thus there exist integers a, b such that $p \mid a^2 - c$ and $p \mid b^2 - (p - 1 - c)$.

Hence we have

$$p \mid (a^2 - c) + (b^2 - p + 1 + c) = a^2 + b^2 + 1 - p,$$

and hence $p \mid a^2 + b^2 + 1$. We may clearly take a, b to be positive.

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 $4k + 3$.

   Solution. Clearly $\left(\frac{-1}{2}\right) = 1$; now suppose $p > 2$. Then we have $p \mid \left(\frac{-1}{p}\right) - (-1)^{(p-1)/2}$. As $p > 2$ the only way that p can divide the difference of $\left(\frac{-1}{p}\right)$ and $(-1)^{(p-1)/2}$ is if they are equal to each other. Hence we have $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Thus if $p = 4k+1$ then $\left(\frac{-1}{p}\right) = (-1)^{2k} = 1$, and if $p = 4k+3$ then $\left(\frac{-1}{p}\right) = (-1)^{2k+1} = -1$.

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

   Solution. The statement is obvious for $p = 2$ - there are only 4 cases to check and they are all immediately clear. Now suppose $p > 3$.

   Then we have $p \mid \left(\frac{a}{p}\right) - a^{(p-1)/2}$, and hence $p \mid \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - a^{(p-1)/2}\left(\frac{b}{p}\right)$. Similarly, $p \mid \left(\frac{b}{p}\right) - b^{(p-1)/2}$, and hence $p \mid a^{(p-1)/2}\left(\frac{b}{p}\right) - a^{(p-1)/2}b^{(p-1)/2}$. Hence we have

$$p \mid \left[\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - a^{(p-1)/2}\left(\frac{b}{p}\right)\right] + \left[a^{(p-1)/2}\left(\frac{b}{p}\right) - a^{(p-1)/2}b^{(p-1)/2}\right] = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - (ab)^{(p-1)/2}.$$

   We also have $p \mid \left(\frac{ab}{p}\right) - (ab)^{(p-1)/2}$, and thus

$$p \mid \left[\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - (ab)^{(p-1)/2}\right] - \left[\left(\frac{ab}{p}\right) - (ab)^{(p-1)/2}\right] = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right).$$

   As $p > 2$ and as the two terms in the rightmost expression are equal to ± 1, they must be equal. Hence $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ as desired.

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?)

Solution. Suppose that $p \nmid a, b$; that is, $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right) \neq 0$. As $p \mid a^2 + b^2 = a^2 - (-b^2)$, we know that $-b^2$ is a quadratic residue modulo p, and so $\left(\frac{-b^2}{p}\right) = 1$. By above we have $\left(\frac{-b^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b^2}{p}\right)$. We have $\left(\frac{b^2}{p}\right) = 1$, and thus $\left(\frac{-1}{p}\right) = 1$, contradicting the hypothesis that $p = 4k + 3$. Hence it must be the case that $p \mid a, b$.

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, $\left(\frac{42}{2017}\right)$. *Solution.* We have

$$\left(\frac{42}{2017}\right) = \left(\frac{2}{2017}\right)\left(\frac{3}{2017}\right)\left(\frac{7}{2017}\right).$$

We have $16 \mid 2017 - 1$, and hence $16 \mid 2017^2 - 1$ so that $2 \mid (2017^2 - 1)/8$. Hence $\left(\frac{2}{2017}\right) = 1$ by the $q = 2$ case above.

Now we turn to the $\left(\frac{3}{2017}\right)$ term. As $8 \mid 2017 - 1$, by quadratic reciprocity we have $\left(\frac{3}{2017}\right)\left(\frac{2017}{3}\right) = 1$. As $\left(\frac{2017}{3}\right) = \left(\frac{1}{3}\right) = 1$ it follows that $\left(\frac{3}{2017}\right) = 1$.

Finally we calculate $\left(\frac{7}{2017}\right)$. We have similarly to the 3 case that $\left(\frac{7}{2017}\right)\left(\frac{2017}{7}\right) = 1$. As $2016 = 2100 - 84$, we have $\left(\frac{2017}{7}\right) = \left(\frac{1}{7}\right) = 1$. Hence $\left(\frac{7}{2017}\right) = 1$, and thus $\left(\frac{42}{2017}\right) = 1$.

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.)

Solution. Note that $n^2 + n + 1$ is odd for all n, and so $p \neq 2$. Now suppose $p > 3$.

Taking the hint, we have $p \mid 4n^2 + 4n + 4 = (2n + 1)^2 + 3$. Hence -3 is a quadratic residue modulo p. Hence we have

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{3}{p}\right).$$

By quadratic reciprocity we have $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{2(p-1)/4}$; as $\left(\frac{3}{p}\right) = \pm 1$ we have thus $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{(p-1)/2}$. Hence

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{2(p-1)/2} = \left(\frac{p}{3}\right)(-1)^{p-1} = \left(\frac{p}{3}\right),$$

and thus p is a quadratic residue modulo 3. Hence $p = 3j + 1$. As p must be odd, we must have $j = 2k$ even, and thus $p = 6k + 1$.

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?)

Solution. Note that if $p = 3$ then the hypothesis is trivially satisfied. Hence suppose $p > 5$.

Using the same trick as in the last problem, we have $p \mid 25k^2+5$, and thus $\left(\frac{-5}{p}\right) = 1$. We have $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)$, and thus as $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ we have by quadratic reciprocity that

$$1 = \left(\frac{-5}{p}\right) = (-1)^{(p-1)/2} \cdot \left(\frac{p}{5}\right)(-1)^{(p-1)} = (-1)^{(p-1)/2}\left(\frac{p}{5}\right).$$

Hence we have two cases: first, that $4 \mid p-1$ and $\left(\frac{p}{5}\right) = 1$, and second, that $2 \mid p-1$ but $4 \nmid p-1$ and $\left(\frac{5}{p}\right) = -1$. Note that $\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1$ and $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$.

Hence in the first case we have either $p = 20k+1$ or $p = 20k+9$, and in the second case we have either $p = 20k+3$ or $p = 20k+7$. Thus the tens digit of p must be odd, as desired.