Math 3110: Number Theory

Exploration 3: Quadratic equations

March 17, 2016

1 Quadratic residues

Suppose that p is a nonzero prime integer. We saw in the last exploration that -1 is a square in $\mathbb{F}_p$ if and only if p fails to be prime in $\mathbb{Z}[i]$. But how can we tell if -1 is a square in $\mathbb{F}_p$?

Definition 1. An element z of $\mathbb{F}_p$ is called a *quadratic residue* modulo p if there is some $x \in \mathbb{F}_p$ such that $x^2 = z$. More generally, if F is a finite field with q elements, we will call $z \in F$ a *quadratic residue* in F if there is some $x \in F$ such that $x^2 = z$.

Theorem 2 (Fermat's little theorem)**.** *If F is a finite field of size q and $a \in F^*$ then $a^{q-1} = 1$.*

Theorem 3. *If F is a field and $p(x)$ is a polynomial of degree d with coefficients in F then p has at most d roots in F.*

Question 4. Pick a few small fields and make a table of all of the quadratic residues and quadratic nonresidues in each one. How many quadratic residues are there? Can you conjecture a general pattern?

Question 5. Pick a field F of size q and an $x \in F$. Compute $x^{\frac{q-1}{2}}$. Do this for a few examples. Compare your answers to the results of the last question. Can you observe a pattern?

Theorem 6. *Let F be a finite field with an odd number of elements. Then an element $a \in F$ is a nonzero quadratic residue if and only if $a^{\frac{q-1}{2}} = 1$.*

Definition 7. For prime a and any integer a that is prime to p, we write:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$$

This is known as the *Legendre symbol*.

We have just learned that the Legendre symbol $\left(\frac{a}{p}\right)$ is always ± 1 and it is $+1$ when a is a quadratic residue modulo p and it is -1 when a is a quadratic nonresidue modulo p.

Theorem 8. *Suppose that p is an odd prime integer. Then -1 is a quadratic residue in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$.*

2 Quadratic reciprocity

Suppose that p, q, and r are nonzero prime integers. If $p \equiv q \pmod{r}$ then p is a quadratic residue modulo r if and only if q is a quadratic residue modulo r. But is there any relationship between whether r is a quadratic residue modulo p and whether r is a quadratic residue modulo q. We certainly don't have any reason yet to expect a relationship. But let's compute some data and see if we can make any observations:

Question 9. Choose $a \in \mathbb{F}_5^*$. Make a list of primes p such that $p \equiv a \pmod{5}$. For each p in your list, determine whether 5 is a quadratic residue modulo p. Do you observe any patterns? How do $\left(\frac{5}{p}\right)$ and $\left(\frac{5}{q}\right)$ compare when $p \equiv q \pmod{5}$? I suggest computing $\left(\frac{5}{p}\right)$ for all positive prime integers $p < 100$.

Question 10. Now make a list of $\left(\frac{p}{5}\right)$ for as many values of p as you computed $\left(\frac{5}{p}\right)$ in the last question. Notice anything?

Question 11. Make a conjecture about what is going on. Try replacing 5 by 11 and conducting the same experiments you did before. Does the pattern hold up?

Question 12. Choose $a \in \mathbb{F}_3^*$. Make a list of primes p such that $p \equiv a \pmod{3}$. For each p in your list, determine whether 3 is a quadratic residue modulo p. Do you observe any patterns? You might need even more data to see a pattern this time. It may help to compare $\left(\frac{3}{p}\right)$ and $\left(\frac{p}{3}\right)$, like you did before.

Question 13. If a pattern isn't starting to emerge, try multiplying $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right)$. See if you can find a pattern in these values.

Lemma 14. *Suppose that p is an odd prime. Then* $\left(\frac{p-1}{2}\right)!^2 = -\left(\frac{-1}{p}\right)$.

Question 15. Repeat your experiments with other small primes replacing 3, 5, and 11. Do you see the same patterns? New patterns? Make sure to look at 2!

Theorem 16 (Quadratic reciprocity)**.** *Suppose that p and q are odd prime integers. Then:*

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

Proof. This contains $(p-1)(q-1)$ elements. We are going to consider three different ways of picking a list of $\frac{(p-1)(q-1)}{2}$ elements such that for every α, either α or $-\alpha$ appears in the list. The first is to choose all elements of $(\mathbb{Z}/p\mathbb{Z})^*$ that can be represented as an integer between 0 and $\frac{p-1}{2}$ and choose the element of

$(\mathbb{Z}/q\mathbb{Z})^*$ arbitrarily. Taking the product of all of these elements, we get

$$\alpha = \prod_{\substack{0<k<\frac{p}{2} \\ 0<\ell<q}} (k \bmod p, \ell \bmod q) = \Big((\frac{p-1}{2})!^{q-1}, (q-1)!^{\frac{p-1}{2}} \Big)$$
$$= \big((-1)^{\frac{p-1}{2}\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}} \big)$$

We can do the same thing with p and q reversed:

$$\beta = \prod_{\substack{0<k<p-1 \\ 0<\ell<\frac{q}{2}}} (k \bmod p, \ell \bmod q)$$
$$= \big((-1)^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \big)$$

Or, we could take all pairs $(k \bmod p, k \bmod q)$ such that $0 < k < \frac{pq}{2}$. To compute this product, we take all numbers between 0 and $\frac{pq}{2}$, exclusive, cross out those that are divisible by p or by q, and then multiply all that are left together.

We do this differently modulo p and q. First we do it modulo p. Here is a table of all numbers between 0 and $\frac{pq}{2}$ (exclusive) with multiples of p crossed out:

$$\begin{array}{cccccccc}
1 & 2 & \cdots & \frac{p-1}{2} & \cdots & p-2 & p-1 & \cancel{p} \\
p+1 & p+2 & \cdots & p+\frac{p-1}{2} & \cdots & 2p-2 & 2p-1 & \cancel{2p} \\
2p+1 & 2p+2 & \cdots & 2p+\frac{p-1}{2} & \cdots & 3p-2 & 3p-1 & \cancel{3p} \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \vdots \\
\frac{q-3}{2}p+1 & \frac{q-3}{2}p+2 & \cdots & \frac{q-3}{2}p+\frac{p-1}{2} & \cdots & \frac{q-1}{2}p-2 & \frac{q-1}{2}p-1 & \cancel{\frac{q-1}{2}p} \\
\frac{q-1}{2}p+1 & \frac{q-1}{2}p+2 & \cdots & \frac{q-1}{2}p+\frac{p-1}{2} & & & &
\end{array}$$

If we reduce all of this modulo p and multiply them together, we get:

$$(p-1)!^{\frac{q-1}{2}}(\frac{p-1}{2})!$$

But we still need to cancel out all of the terms that are divisible by q. Here is a list of those terms, multiplied together:

$$q \times 2q \times 3q \times \ldots \times \frac{p-1}{2}q = \prod_{m=1}^{\frac{p-1}{2}} mq = (\frac{p-1}{2})!q^{\frac{p-1}{2}}$$

This gives us the first component in the calculation below. The second component is the same, but with p and q reversed:

$$\begin{aligned}
\gamma &= \prod_{0<k<\frac{pq}{2}} (k \bmod p, k \bmod q) \\
&= \left(\frac{(p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}{p^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}, \frac{(q-1)!^{\frac{p-1}{2}} \left(\frac{q-1}{2}\right)!}{q^{\frac{p-1}{2}} \left(\frac{q-1}{2}\right)!} \right) \\
&= \left(\frac{(-1)^{\frac{q-1}{2}}}{p^{\frac{q-1}{2}}}, \frac{(-1)^{\frac{p-1}{2}}}{q^{\frac{p-1}{2}}} \right)
\end{aligned}$$

But all of the terms in the product for α appear in the product for β, except maybe with a different sign. Therefore $\alpha = \pm\beta$. Likewise $\alpha = \pm\gamma$. Let's figure out exactly what the signs are:

$$\alpha/\beta = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

But we can also see by looking at the second components that:

$$q^{\frac{p-1}{2}} \gamma = \alpha$$

Likewise, the first components show us that:

$$p^{\frac{q-1}{2}} \gamma = \beta$$

Combining all three equations, we find that:

$$q^{\frac{p-1}{2}} = p^{\frac{q-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

This is the quadratic reciprocity formula. □

Theorem 17 (Quadratic reciprocity at 2)**.** *For any odd prime integer p:*

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

Proof. Consider the product:

$$\alpha = \prod_{k=1}^{\frac{p-1}{2}} 2k = 2^{\frac{p-1}{2}} (\frac{p-1}{2})!$$

We can rewrite this product another way:

$$\begin{aligned}
\alpha &= \prod_{0<k<\frac{p}{4}} 2k \prod_{\frac{p}{4}<k<\frac{p}{2}} 2k \\
&= \prod_{0<k<\frac{p}{4}} 2k \prod_{-\frac{p}{2}<k<0} -(p+1+2k) \\
&\equiv \prod_{0<k<\frac{p}{4}} 2k(-1-2k) \\
&= \prod_{k=1}^{\frac{p-1}{2}} (-1)^k k \\
&= (\frac{p-1}{2})!(-1)^{\frac{1}{2}\frac{p-1}{2}\frac{p+1}{2}}
\end{aligned}$$

If we put these together, we get:

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

□