Quadratic residues and quadratic nonresidues

Kyle Miller

Feb 17, 2017

A number a is called a *quadratic residue*, modulo p, if it is the square of some other number, modulo p. That is to say, a is a quadratic residue if there is a b such that $a \equiv b^2 \pmod{p}$. A number is called a *quadratic nonresidue* if it is not a quadratic residue.[1]

In one discussion section on Wednesday, I described how to use primitive roots to prove the following fact:

Theorem 1. *If p is an odd prime, then there are exactly $\frac{p-1}{2}$ nonzero quadratic residues (and $\frac{p-1}{2}$ quadratic nonresidues).*

For sake of the other discussion, and because primitive roots are a topic of the course, I'll give the primitive root argument later, but the purpose of this note is to explain another argument that doesn't make use of primitive roots that I came up with last night.

Another way to define a quadratic residue is that a number a is a quadratic residue if it has a square root. That is to say, a is a quadratic residue if $x^2 \equiv a \pmod{p}$ has a solution, or equivalently if $x^2 - a$ has a root modulo p.

Fact: every nonzero number a modulo p has either zero or two distinct square roots. Suppose a had a square root b. Then $x^2 - a \equiv (x-b)(x+b) \pmod{p}$ is a factorization of the polynomial. The equation $(x-b)(x+b) \equiv 0 \pmod{p}$, since p is prime, is equivalent to saying $x - b \equiv 0 \pmod{p}$ or $x + b \equiv 0 \pmod{p}$, so the only roots to $x^2 - a$ are $x \equiv \pm b \pmod{p}$. We know $b \not\equiv -b \pmod{p}$ since if $b \equiv -b \pmod{p}$, then $2b \equiv 0 \pmod{p}$, and since $\gcd(2,p) = 1$, $b \equiv 0 \pmod{p}$, but $b \not\equiv 0 \pmod{p}$ since $0 \not\equiv a \equiv b^2 \pmod{p}$.

So every nonzero quadratic residue has exactly two square roots, and (by definition) every nonzero number squares to a quadratic residue. This implies that half of the nonzero numbers, modulo p, are quadratic residues, which is to say there are $\frac{p-1}{2}$ quadratic residues.

More specifically, we know that $b^2 \equiv (-b)^2 \pmod{p}$, so the numbers $1, \dots, \frac{p-1}{2}$ represent all of the nonzero quadratic residues. We know that they represent distinct quadratic residues since the only time $x^2 \equiv y^2 \pmod{p}$ is when $x \equiv \pm y \pmod{p}$, and the numbers in the list $1, \dots, \frac{p-1}{2}$ are not negatives of each other.

Since there are $p - 1$ nonzero numbers, that leaves $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ quadratic nonresidues.

1 With primitive roots

A *primitive root*, modulo p, is a number α with the property that the list $\alpha, \alpha^2, \alpha^3, \dots$ contains all the numbers $1, 2, \dots, p-1$ (modulo p).

The equation $x^2 \equiv a \pmod{p}$ can be rewritten as $(\alpha^k)^2 \equiv \alpha^n \pmod{p}$, where n is chosen so that $a \equiv \alpha^n \pmod{p}$, and where k is the unknown. The congruence is equivalent to $\alpha^{2k} \equiv \alpha^n \pmod{p}$, and by Fermat's little theorem it is equivalent to $2k \equiv n \pmod{p-1}$, since $\alpha \not\equiv 0 \pmod{p}$. A homework problem concerns congruences like this, and it says the solutions satisfy $k \equiv \frac{n}{2} \pmod{\frac{p-1}{2}}$ since $\gcd(p-1, 2) = 2$. The fraction $\frac{n}{2}$ might not be an integer, and in that case the solution is not satisfiable. Otherwise, this gives the value of k modulo $\frac{p-1}{2}$, so there are exactly two solutions modulo $p-1$: $\frac{n}{2}$ and $\frac{n}{2} + \frac{p-1}{2}$. (Going back to the $x \equiv \alpha^k \pmod{p}$, then x is $\alpha^{n/2}$ or $\alpha^{n/2}\alpha^{(p-1)/2}$, where $\alpha^{(p-1)/2} \equiv -1 \pmod{p}$ since when squared it is 1.)

This is all to prove that there are either zero or two distinct square roots of a number, and then the same counting argument follows.

[1]The word *residue* is old and refers to the remainder after division. The value $b^2 \bmod p$ is a quadratic residue.

2 Finding quadratic nonresidues

It is extremely easy to find a nonzero quadratic residue: 1 is 1^2. However, it is less straightforward finding a nonresidue; a reason one might want to find one is that the algorithm for computing square roots modulo p requires finding some quadratic nonresidue. One way to find a nonresidue is to exhaustively list out all squares and take a number which is not in that list, but this is not efficient.

Suppose we had an efficient method of determining whether a particular number is a quadratic residue or not. By the fact that exactly half of the nonzero numbers modulo an odd prime are quadratic residues, we can perform a randomized algorithm: choose a random number, check if it's a residue. Since each attempt has a 50% chance of succeeding, we would expect the algorithm to take two steps on average to find one.

There is, in fact, an efficient method of determining whether a particular number is a quadratic residue or not, and that is using the *Legendre symbol*, which I will not discuss here.

3 Bonus: why is Fermat's little theorem true?

The proof which makes the theorem most obvious uses group theory, and in particular Lagrange's theorem. In this section I'll give a proof which is essentially using Lagrange's theorem, but I won't use any group theory language.

Theorem 2. *If $a \not\equiv 0 \pmod{p}$, then there is some integer $n \geq 1$ such that $a^n \equiv 1 \pmod{p}$.*

Proof. Consider the sequence $a^1, a^2, a^3, \ldots$. Since there are only finitely many numbers modulo p, by the Pigeonhole principle, there must be some numbers $n < m$ such that $a^n \equiv a^m \pmod{p}$. Since a has an inverse modulo p, a^n has an inverse modulo p, so $1 \equiv a^{m-n} \pmod{p}$. Thus, $m - n$ is the required number. □

Let the smallest positive n such that $a^n \equiv 1 \pmod{p}$ be called the *order* of a modulo p. Our goal is to prove that the order of a divides $p - 1$.

Let H_a be the set of powers of a modulo p, so $H_a = \{a^1, a^2, a^3, \ldots\}$. We have just shown that $|H_a|$ is the order of a. For $b \not\equiv 0 \pmod{p}$, let bH_a denote the set $\{ba^k : a^k \in H_a\}$. Since b has an inverse, multiplying by b is a bijection, so $|bH_a| = |H_a|$.

Fact: $a^\ell H_a = H_a$. This is because $a^\ell H_a \subseteq H_a$, and equality follows because they have the same size.

Fact: for any $b_1, b_2 \not\equiv 0 \pmod{p}$, then $b_1 H_a$ and $b_2 H_a$ are either disjoint sets or equal sets. Suppose $b_1 H_a$ and $b_2 H_a$ are not disjoint sets, which means they have an element in common, so $b_1 a^{k_1} = b_2 a^{k_2}$ for some k_1, k_2. Then $b_1 H_a = b_2 a^{k_2 - k_1} H_a = b_2 H_a$.

Fact: $\{bH_a : b \not\equiv 0 \pmod{p}\}$ is a *partition* of $1, 2, \ldots, p-1$. Every number $1 \leq b < p - 1$ is in at least one of these sets, in particular bH_a, and every number is in at most one since they are disjoint or equal.

Since every set bH_a is the same size, then $|H_a|$ divides $p - 1$. That is, $|H_a| m = p - 1$ for some $m \in \mathbb{Z}$. Thus, we have Fermat's little theorem:

Theorem 3. *If $a \not\equiv 0 \pmod{p}$ then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. $a^{p-1} \equiv a^{|H_a| m} \equiv (a^{|H_a|})^m \equiv 1^m \equiv 1 \pmod{p}$. □

If you want some words to look up: $1, \ldots, p-1$ are the elements of the *multiplicative group of* $\mathbb{Z}/p\mathbb{Z}$, H_a is the *cyclic subgroup generated by* a, and bH_a is a *coset*.