Math 3527 (Number Theory 1)

Lecture #30

Quadratic Residues and Legendre Symbols:

- Quadratic Congruences
- Quadratic Residues and Nonresidues
- Legendre Symbols

This material represents §5.2 from the course notes.

Quadratic Congruences, I

In the last lecture, we discussed general polynomial congruences. We now narrow our focus to quadratic congruences mod m. By using the methods from last lecture, we may essentially reduce this problem to solving quadratic congruences modulo p where p is a prime.

- So let $f(x) = ax^2 + bx + c$, and consider the general quadratic congruence $f(x) \equiv 0 \pmod{p}$.
- If $p = 2$ then this congruence is easy to solve, so we can also assume p is odd.
- If $a \equiv 0 \pmod{p}$, then the congruence $f(x) \equiv 0 \pmod{p}$ reduces to a linear congruence, which we can easily solve.
- So we can also assume $a \not\equiv 0 \pmod{p}$: then a is invertible modulo p.

Quadratic Congruences, II

Now that we have handled the troublesome cases, we can solve the quadratic equation the usual way by completing the square.

- Explicitly, with $f(x) = ax^2 + bx + c$, we can write $4af(x) = (2ax + b)^2 + (4ac - b^2)$.
- Since $4a$ is invertible modulo p, the congruence $f(x) \equiv 0 \pmod{p}$ is equivalent to $(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$.
- Solving for x then amounts to finding all solutions to $y^2 \equiv D \pmod{p}$, where $y = 2ax + b$ and $D = b^2 - 4ac$.
- This is merely the quadratic formula: $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ (the hard part is computing the square root).

Quadratic Residues, I

We would like first like to determine whether the congruence $y^2 \equiv D \pmod{p}$ has a solution at all.

Definition

If a is a unit modulo m, we say a is a quadratic residue modulo m if there is some b such that $b^2 \equiv a \pmod{m}$. If there is no such b, then we say a is a quadratic nonresidue modulo m.

It is a matter of taste whether to include nonunits in the definition of quadratic residues/nonresidues. We will only consider units.

By definition, $y^2 \equiv D \pmod{p}$ has a solution for y precisely when D is a quadratic residue modulo p (or when $D = 0$).

Quadratic Residues, II

Examples:

- Modulo 3, there is one quadratic residue 1 and one quadratic nonresidue 2.
- Modulo 5, the quadratic residues are 1 and 4, while the quadratic nonresidues are 2 and 3.
- Modulo 13, the quadratic residues are 1, 4, 9, 3, 12, and 10, while the quadratic nonresidues are 2, 5, 6, 7, 8, and 11.
- Modulo 21, the quadratic residues are 1, 4, and 16, while the quadratic nonresidues are 2, 5, 8, 10, 11, 13, 17, 19, and 20.
- Modulo 25, the quadratic residues are 1, 6, 11, 16, 21, 4, 9, 14, 19, and 24, while the quadratic nonresidues are 2, 7, 12, 17, 22, 3, 8, 13, 18, and 23.

Quadratic Residues, III

Here are some of the basic properties of quadratic residues:

Proposition (Properties of Quadratic Residues)

Let p be an odd prime. Then the following hold:

1. *A unit a is a quadratic residue modulo p^d for $d \geq 1$ if and only if a is a quadratic residue modulo p.*
2. *If m is any odd positive integer, then a unit a is a quadratic residue modulo m if and only if a is a quadratic residue modulo p for each prime p dividing m.*
3. *The quadratic residues modulo p are $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$. Hence, half of the invertible residue classes modulo p are quadratic residues (the other half are nonresidues).*
4. *If u is a primitive root modulo p, then a is a quadratic residue modulo p if and only if $a \equiv u^{2k} \pmod{p}$ for some integer k.*

Quadratic Residues, IV

Proofs:

1. A unit a is a quadratic residue modulo p^d for $d \geq 1$ if and only if a is a quadratic residue modulo p.
   - Proof: Clearly, if there exists a b such that $a \equiv b^2 \pmod{p^d}$ then $a \equiv b^2 \pmod{p}$, so the forward direction is trivial.
   - For the other direction, suppose a is a unit and there exists some b with $a \equiv b^2 \pmod{p}$.
   - For $q(x) = x^2 - a$, we then want to apply Hensel's lemma to lift the solution $x \equiv b \pmod{p}$ of the congruence $q(x) \equiv 0 \pmod{p}$ to a solution modulo p^d.
   - We can do this as long as $q'(b) \not\equiv 0 \pmod{p}$: but $q'(b) = 2b$, and this is nonzero because $b \not\equiv 0 \pmod{p}$ and p is odd.

Quadratic Residues, IV

2. If m is any odd positive integer, then a unit a is a quadratic residue modulo m if and only if a is a quadratic residue modulo p for each prime p dividing m.
   - Proof: By the Chinese Remainder Theorem, there is a solution to $x^2 \equiv a \pmod{m}$ if and only if there is a solution to $x^2 \equiv a \pmod{p^d}$ for each prime power p^d appearing in the prime factorization of m.
   - But by (1), there is a solution to $x^2 \equiv a \pmod{p^d}$ if and only if there is a solution to $x^2 \equiv a \pmod{p}$.
   - In other words, a is a quadratic residue modulo m if and only if a is a quadratic residue modulo p for each prime p dividing m, as claimed.

Quadratic Residues, V

3. The quadratic residues modulo p are 1^2, 2^2, ... , $(\frac{p-1}{2})^2$. Hence, half of the invertible residue classes modulo p are quadratic residues (the other half are nonresidues).
   - Proof: If p is prime, then $p|(a^2 - b^2)$ implies $p|(a - b)$ or $p|(a + b)$: thus, $a^2 \equiv b^2 \pmod{p}$ is equivalent to $a \equiv \pm b \pmod{p}$.
   - We conclude that 1^2, 2^2, ... , $(\frac{p-1}{2})^2$ are distinct modulo p.
   - The other squares $(\frac{p+1}{2})^2$, ... , $(p-1)^2$ are equivalent to these in reverse order, since $k^2 \equiv (p-k)^2 \pmod{p}$.

Examples:
The quadratic residues mod 11 are 1^2, 2^2, 3^2, 4^2, 5^2 (1, 4, 9, 5, 3).
The quadratic residues mod 13 are 1^2, 2^2, 3^2, 4^2, 5^2, 6^2.

Quadratic Residues, VI

4. If u is a primitive root modulo p, then a is a quadratic residue modulo p if and only if $a \equiv u^{2k} \pmod{p}$ for some integer k.
   - Proof: Clearly, if $a \equiv u^{2k} \pmod{p}$ then $a \equiv (u^k)^2$ is a quadratic residue.
   - Conversely, suppose a is a quadratic residue, with $a \equiv b^2 \pmod{p}$. Then because u is a primitive root, we can write $b \equiv u^k \pmod{p}$ for some k: then $a \equiv b^2 \equiv u^{2k} \pmod{p}$, as required.

This says the quadratic residues are the even powers of the primitive root while the quadratic nonresidues are the odd powers.

Example: 2 is a primitive root mod 11, and the quadratic residues mod 11 are $2^2 \equiv 4$, $2^4 \equiv 5$, $2^6 \equiv 9$, $2^8 \equiv 3$, and $2^{10} \equiv 1$.

Quadratic Residues, VII

The items in the proposition allow us to write down the quadratic residues modulo p using various descriptions.

Our next goal is to find an efficient way to decide whether a given residue class a modulo p is a quadratic residue or a quadratic nonresidue.

Legendre Symbols, I

We now introduce notation that will help us distinguish between quadratic residues and quadratic nonresidues:

Definition

If p is an odd prime, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be $+1$ if a is a quadratic residue, -1 if a is a quadratic nonresidue, and 0 if p divides a.

The notation for the Legendre symbol is somewhat unfortunate, since it is the same as that for a standard fraction. When appropriate, we may write $\left(\frac{a}{p}\right)_L$ to emphasize that we are referring to a Legendre symbol rather than a fraction.

Legendre Symbols, II

Examples:

- We have $\left(\frac{2}{7}\right) = +1$, $\left(\frac{3}{7}\right) = -1$, and $\left(\frac{0}{7}\right) = 0$, since 2 is a quadratic residue and 3 is a quadratic nonresidue modulo 7.
- We have $\left(\frac{3}{13}\right) = \left(\frac{-3}{13}\right) = +1$, and $\left(\frac{2}{13}\right) = 1$, since 3 and -3 are quadratic residues modulo 13, while 2 is not.
- We have $\left(\frac{16}{17}\right) = \left(\frac{13^2}{17}\right) = +1$ since both $16 = 4^2$ and 13^2 are quadratic residues modulo 17.

Legendre Symbols, III

We now give an easy way to calculate the Legendre symbol.

Theorem (Euler's Criterion)

If p is an odd prime, then for any residue class a, it is true that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Euler's criterion gives a very efficient way to compute any Legendre symbol, because we can very rapidly evaluate $a^{(p-1)/2}$ modulo p using successive squaring.

Legendre Symbols, IV

Proof:

- If $p|a$ then the result is trivial (since both sides are 0 mod p), so assume a is a unit and let u be a primitive root.
- If a is a quadratic residue, then by item (4) of our Proposition, we know that $a = u^{2k}$ for some integer k.
- Then $a^{(p-1)/2} \equiv (u^{2k})^{(p-1)/2} = (u^{p-1})^k \equiv 1^k = 1 = \left(\frac{a}{p}\right) \pmod{p}$, as required.
- If a is a quadratic nonresidue, then again by item (4) of the proposition above, we know $a = u^{2k+1}$ for some integer k.
- We observe that $u^{(p-1)/2} \equiv -1 \pmod{p}$, since its square is 1 but it cannot be 1 since u is a primitive root.
- Then $a^{(p-1)/2} \equiv (u^{2k+1})^{(p-1)/2} = (u^{p-1})^k \cdot u^{(p-1)/2} \equiv u^{(p-1)/2} \equiv -1 = \left(\frac{a}{p}\right) \pmod{p}$, again as required.

Legendre Symbols, V

Example: Calculate the Legendre symbol $\left(\frac{12}{17}\right)$.

- We simply compute $12^{(17-1)/2} \equiv 12^8 \equiv -1 \pmod{17}$.
- Thus, $\left(\frac{12}{17}\right) = -1$.

Legendre Symbols, V

Example: Calculate the Legendre symbol $\left(\frac{12}{17}\right)$.

- We simply compute $12^{(17-1)/2} \equiv 12^8 \equiv -1 \pmod{17}$.
- Thus, $\left(\frac{12}{17}\right) = -1$.

Example: Calculate the Legendre symbol $\left(\frac{13}{101}\right)$.

- We simply compute $13^{(101-1)/2} \equiv 13^{50} \equiv 1 \pmod{101}$.
- Thus, $\left(\frac{13}{101}\right) = 1$.

Legendre Symbols, V

Example: Calculate the Legendre symbol $\left(\frac{12}{17}\right)$.

- We simply compute $12^{(17-1)/2} \equiv 12^8 \equiv -1 \pmod{17}$.
- Thus, $\left(\frac{12}{17}\right) = -1$.

Example: Calculate the Legendre symbol $\left(\frac{13}{101}\right)$.

- We simply compute $13^{(101-1)/2} \equiv 13^{50} \equiv 1 \pmod{101}$.
- Thus, $\left(\frac{13}{101}\right) = 1$.

Example: Determine whether 14 is a quadratic residue modulo 23.

- We want to evaluate $\left(\frac{14}{23}\right)$. But by Euler's criterion this is $14^{(23-1)/2} \equiv 14^{11} \equiv -1 \pmod{23}$.
- This means 14 is a quadratic nonresidue modulo 23.

Legendre Symbols, VI

We can extend these calculations to determine the quadratic residues and nonresidues for other moduli:

Example: Determine whether 2 is a quadratic residue or nonresidue modulo 7^3.

Legendre Symbols, VI

We can extend these calculations to determine the quadratic residues and nonresidues for other moduli:

Example: Determine whether 2 is a quadratic residue or nonresidue modulo 7^3.

- Note that 7^3 is not prime, so we cannot use Euler's criterion directly. But because 7^3 is a prime power, we know that the quadratic residues modulo 7 are the same as the quadratic residues modulo 7^3.
- By Euler's criterion, $\left(\frac{2}{7}\right) \equiv 2^3 \equiv 1 \pmod 7$, so 2 is a quadratic residue modulo 7 hence also a quadratic residue modulo 7^3.

Legendre Symbols, VII

Example: Determine whether 112 is a quadratic residue or nonresidue modulo 675.

Legendre Symbols, VII

Example: Determine whether 112 is a quadratic residue or nonresidue modulo 675.

- Note that $675 = 3^3 5^2$, so by our results, 112 is a quadratic residue modulo 675 if and only if it is a quadratic residue modulo 3 and modulo 5.
- We have $\left(\frac{112}{3}\right) = \left(\frac{1}{3}\right) \equiv 1 \pmod 3$, so 112 is a quadratic residue modulo 3.
- However, $\left(\frac{112}{5}\right) = \left(\frac{2}{5}\right) \equiv 2^2 \equiv -1 \pmod 5$, so 112 is a quadratic nonresidue modulo 5.
- Therefore, 112 is a quadratic nonresidue modulo 675.

Legendre Symbols, VIII

Euler's criterion also yields an extremely useful corollary about the product of Legendre symbols:

Corollary (Multiplicativity of Legendre Symbols)

If p is a prime, then for any a and b, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Proof:

- Simply use Euler's criterion to write
$$\left(\frac{ab}{p}\right) = (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Equivalently, the product of two quadratic residues is a quadratic residue, the product of a quadratic residue and nonresidue is a nonresidue, and (much more unexpectedly) the product of two quadratic nonresidues is a quadratic residue.

Summary

We defined the quadratic residues (and nonresidues) and established some of their basic properties.

We defined the Legendre symbol, which allows us to detect quadratic residues and nonresidues

We proved Euler's criterion, which provides a method for calculating Legendre symbols efficiently.

Next lecture: Quadratic Reciprocity