Math 3527 (Number Theory 1)

Lecture #32

Applications of Quadratic Reciprocity:

- Finding p For Which a is a Quadratic Residue
- Primes Dividing Quadratic Polynomials
- Berlekamp's Root-Finding Algorithm
- Solovay-Strassen Compositeness Test

This material represents §5.5 from the course notes.

Quadratic Reciprocity

In the last lecture, we discussed quadratic reciprocity for Legendre symbols and then generalized it to Jacobi symbols:

Theorem (Quadratic Reciprocity for Jacobi Symbols)

If $b = p_1 p_2 \cdots p_k$ is a product of odd primes and a is odd, then

1. $\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}$. *Equivalently,* $\left(\frac{-1}{b}\right)$ *is* $+1$ *if* $b \equiv 1 \pmod 4$ *and is* -1 *if* $b \equiv 3 \pmod 4$.
2. $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$. *Equivalently,* $\left(\frac{2}{b}\right)$ *is* $+1$ *if* $b \equiv 1, 7 \pmod 8$ *and is* -1 *if* $b \equiv 3, 5 \pmod 8$.
3. *If a and b are odd, relatively prime positive integers, then* $\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}$.

When Is a a QR Mod p?, I

Our first application of quadratic reciprocity is determining (given a particular value of a) for which primes p is a a quadratic residue.

- To outline the procedure, if we want to compute $\left(\frac{a}{p}\right)$ for a fixed a, first we find the prime factorization of $a = q_1 q_2 \cdots q_k$.
- Then since $\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_k}{p}\right)$, we just need to evaluate each individual Legendre symbol $\left(\frac{q_i}{p}\right)$.
- If there is a -1 or 2 term, we can handle those directly.
- For the odd prime terms, quadratic reciprocity converts the question to determining the Legendre symbol $\left(\frac{p}{q_i}\right)$.
- We can do this by listing all of the quadratic residues and nonresidues modulo q_i for each of the fixed values q_i.

When Is a a QR Mod p?, II

Example: When is 17 a quadratic residue modulo p?

When Is a a QR Mod p?, II

Example: When is 17 a quadratic residue modulo p?

- First, we observe that 17 is a quadratic residue modulo $p = 2$.
- For odd primes, since $17 \equiv 1 \pmod 4$, quadratic reciprocity says that $\left(\frac{17}{p}\right) = \left(\frac{p}{17}\right)$.
- But since the quadratic residues modulo 17 are $1, 2, 4, 8, 9, 13, 15, 16$, this means that $\left(\frac{p}{17}\right) = +1$ precisely when $p \equiv 1$, 2, 4, 8, 9, 13, 15, or 16 (mod 17).
- Thus, we conclude that 17 is a quadratic residue modulo p precisely when $p = 2$, or when $p \equiv 1$, 2, 4, 8, 9, 13, 15, or 16 (mod 17).

When Is a a QR Mod p?, III

Example: When is 3 a quadratic residue modulo p?

When Is a a QR Mod p?, III

Example: When is 3 a quadratic residue modulo p?

- First, we observe that 3 is a quadratic residue modulo $p = 2$.
- For odd primes, we want to find $\left(\frac{3}{p}\right)$ by using quadratic reciprocity to convert the question to one about $\left(\frac{3}{p}\right)$.
- However, the relationship between those two Legendre symbols will depend on the value of p mod 4.
- Specifically, if $p \equiv 1 \pmod 4$, then $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$, while if $p \equiv 3 \pmod 4$, then $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$.
- So we will look at the two possible cases $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$ separately.

When Is a a QR Mod p?, IV

Example (continued): When is 3 a quadratic residue modulo p?

- Note $\left(\frac{p}{3}\right)$ is $+1$ if $p \equiv 1 \pmod 3$, and -1 if $p \equiv 2 \pmod 3$.
- Therefore, if $p \equiv 1 \pmod 4$, then $\left(\frac{3}{p}\right) = +1$ only when $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$.
- Putting these congruences together yields $p \equiv 1 \pmod{12}$.
- In the other case where $p \equiv 3 \pmod 4$, we see that $\left(\frac{3}{p}\right) = +1$ only when $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$.
- Putting these congruences together yields $p \equiv 11 \pmod{12}$.
- Thus, we conclude that 3 is a quadratic residue modulo p precisely when $p = 2$, or when $p \equiv 1$ or $11 \pmod{12}$.

When Is a a QR Mod p?, V

Example: When is 6 a quadratic residue modulo p?

When Is a a QR Mod p?, V

Example: When is 6 a quadratic residue modulo p?

- We want to compute $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{3}{p}\right)$, for $p \neq 2, 3$.
- From the previous example, $\left(\frac{3}{p}\right) = +1$ when $p \equiv 1$ or $11 \pmod{12}$, and $\left(\frac{3}{p}\right) = -1$ when $p \equiv 5$ or $7 \pmod{12}$.
- From our basic evaluations, $\left(\frac{2}{p}\right) = +1$ when $p \equiv 1$ or $7 \pmod{8}$, and $\left(\frac{2}{p}\right) = -1$ when $p \equiv 3$ or $5 \pmod{8}$.

When Is a a QR Mod p?, VI

Example (continued): When is 6 a quadratic residue modulo p?

- Thus, $\left(\frac{6}{p}\right) = +1$ in the following cases:
- Case 1: $\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right) = +1$. This requires $p \equiv 1, 11 \pmod{12}$ and $p \equiv 1, 7 \pmod{8}$. Solving these simultaneous congruences yields $p \equiv 1, 23 \pmod{24}$.
- Case 2: $\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right) = -1$. This requires $p \equiv 5, 7 \pmod{12}$ and $p \equiv 3, 5 \pmod{8}$. Solving these simultaneous congruences yields $p \equiv 5, 19 \pmod{24}$.
- Therefore, 6 is a quadratic residue modulo p precisely when $p \equiv 1, 5, 19, 23 \pmod{24}$.

Primes Dividing Quadratics, I

Our second application is to characterize the prime numbers that can divide the values taken by a quadratic polynomial.

- This should be unexpected, because polynomials can combine addition and multiplication in arbitrary ways.
- There is no especially compelling reason, a priori, to think that the primes dividing the values of, say, the polynomial $q(x) = x^2 + x + 7$, should have any identifiable structure at all: for all we know, the set of primes dividing an integer of the form $n^2 + n + 7$ could be totally arbitrary.

Primes Dividing Quadratics, II

Example: Characterize the primes dividing an integer of the form $n^2 + n + 7$, for n an integer.

Primes Dividing Quadratics, II

Example: Characterize the primes dividing an integer of the form $n^2 + n + 7$, for n an integer.

- It is not hard to see that $n^2 + n + 7$ is always odd, so 2 is never a divisor.
- Now suppose that p is an odd prime and that $n^2 + n + 7 \equiv 0 \pmod{p}$.
- We multiply by 4 and complete the square to obtain $(2n + 1)^2 \equiv -27 \pmod{p}$.
- Since p is odd, there will be a solution for n if and only if -27 is a square modulo p. If $p = 3$, this clearly holds, so now assume $p \geq 5$.

Primes Dividing Quadratics, III

Example (continued): Characterize the primes dividing an integer of the form $n^2 + n + 7$, for n an integer.

- We compute $\left(\frac{-27}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right)^3 = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right)$.
- Since $\left(\frac{-1}{p}\right) = +1$ for $p \equiv 1 \pmod 4$ and $\left(\frac{3}{p}\right) = +1$ when $p \equiv 1$ or $11 \pmod{12}$, we can see that $\left(\frac{-3}{p}\right) = +1$ precisely when $p \equiv 1 \pmod 6$.
- Thus, by the above, we conclude that a prime p divides an integer of the form $n^2 + n + 7$ either when $p = 3$ or when $p \equiv 1 \pmod 6$.

Primes Dividing Quadratics, IV

Example: Characterize the primes dividing an integer of the form $n^2 + 2n + 6$, for n an integer.

Primes Dividing Quadratics, IV

Example: Characterize the primes dividing an integer of the form $n^2 + 2n + 6$, for n an integer.

- Observe that 2 is a divisor when $n = 0$, so we may now restrict our attention to odd primes p.
- Completing the square yields $(n+1)^2 \equiv -5 \pmod{p}$, which is equivalent to saying -5 is a quadratic residue modulo p. Clearly this has a solution when $p = 5$, so also assume $p \neq 5$.
- Then, to characterize these values we want to determine when $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{5}{p}\right)$ is equal to $+1$.

Primes Dividing Quadratics, V

Example (continued): Characterize the primes dividing an integer of the form $n^2 + 2n + 6$, for n an integer.

- By quadratic reciprocity, we see $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, so $\left(\frac{5}{p}\right) = +1$ for $p \equiv 1, 4 \pmod 5$ and $\left(\frac{5}{p}\right) \equiv -1$ for $p \equiv 2, 3 \pmod 5$.
- Also, $\left(\frac{-1}{p}\right) = +1$ precisely when $p \equiv 1 \pmod 4$.
- Then, by combining the appropriate cases with the Chinese remainder theorem, we see $\left(\frac{-5}{p}\right) = +1$ precisely when $p \equiv 1, 3, 7, 9 \pmod{20}$.
- Thus, the prime p divides an integer of the form $n^2 + n + 7$ either when $p = 2$ or $p = 5$ or when $p \equiv 1, 3, 7, 9 \pmod{20}$.

Berlekamp's Root-Finding, I

Our third application of our results is to describe a fast root-finding algorithm for polynomials modulo p.

- So let $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be an element of $\mathbb{F}_p[x]$: we would like to describe a method for calculating a root of $q(x)$ in $\mathbb{F}_p$, if there is one.
- As a starting point, we will consider the case where $q(x)$ factors completely into linear terms (so that there are no irreducible factors of degree greater than 1).
- So suppose that $q(x) = (x - r_1)(x - r_2)\cdots(x - r_n)$ in $\mathbb{F}_p[x]$.
- We can detect if one of the r_i is equal to zero (then q will have constant term 0), and also if any of the r_i are equal (then q will have a common factor with its derivative q').
- So now also assume that all of the r_i are distinct and nonzero.

Berlekamp's Root-Finding, II

We have $q(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$ with distinct $r_i \neq 0$.

- By Euler's criterion in $\mathbb{F}_p$, $r^{(p-1)/2} \equiv \left(\frac{r}{p}\right) \bmod p$.
- This tells us that the roots of $x^{(p-1)/2} - 1$ in $\mathbb{F}_p$ are precisely the quadratic residues, while the roots of $x^{(p-1)/2} + 1$ in $\mathbb{F}_p$ are precisely the quadratic nonresidues.
- Thus, the greatest common divisor of $x^{(p-1)/2} - 1$ with $q(x)$ will be equal to the product of all the terms $x - r_i$ where r_i is a quadratic residue.
- Likewise, the greatest common divisor of $x^{(p-1)/2} + 1$ with $q(x)$ will be equal to the product of all the terms $x - r_i$ where r_i is a quadratic nonresidue.
- This means that at least one root is a quadratic residue, and another is a quadratic nonresidue, then we will obtain a partial factorization of $q(x)$.

Berlekamp's Root-Finding, III

The argument we gave can give us a partial factorization. The next insight is that we can repeat this procedure:

- Specifically, we perform the same calculation with $q(x - a)$ for an arbitrary $a \in \mathbb{F}_p$.
- This will work because the roots of this polynomial are simply the values $a + r_1, \ldots, a + r_n$.
- Since a can be arbitrary, and half of the residue classes modulo p are quadratic residues, we would expect to obtain at least one quadratic residue and one nonresidue with probability roughly $1 - 2/2^n$, which is always at least $1/2$ when $n \geq 2$.
- Thus, if there are at least two roots of this polynomial, we expect to find a partial factorization with probability at least $1/2$ for each attempt.
- By iteratively applying this method for each factor, we can quickly calculate the polynomial's full list of roots.

Berlekamp's Root-Finding, IV

Here is a more formal description of this method:

Algorithm (Berlekamp's Root-Finding Algorithm)

Let $q(x) \in \mathbb{F}_p[x]$ and suppose that $q(x) = (x - r_1) \cdots (x - r_n)$ for some distinct $r_i \in \mathbb{F}_p$.

- *Choose a random $a \in \mathbb{F}_p$ and compute the gcd of $q(x - a)$ with $x^{(p-1)/2} - 1$ and $x^{(p-1)/2} + 1$ in $\mathbb{F}_p[x]$.*
- *If one of these gcds is a constant, choose a different value of a and start over.*
- *Otherwise, if both gcds have positive degree, then each gcd gives a nontrivial factor of $q(x)$.*
- *Repeat the factorization procedure on each gcd, until the full factorization of $q(x)$ is found.*

Berlekamp's Root-Finding, V

We make a few more remarks about this algorithm:

- The first step in the Euclidean algorithm's gcd calculation can be performed efficiently using successive squaring modulo $q(x - a)$: explicitly, to find the remainder upon dividing $x^{(p-1)/2}$ by $q(x - a)$, we use successive squaring (of powers of x) modulo $q(x - a)$.
- As we noted above, the probability of failure on any given attempt should be (heuristically) roughly $2^{-(n-1)}$, which means that even in the worst case for a polynomial of degree 2, we have a 50% chance of success on each attempt.
- Overall, this algorithm can be implemented in $O(n^2 \log p)$ time. For large n, then, it is still fairly slow, but if n is small and p is large, it is much more efficient than a brute-force search for the roots.

Berlekamp's Root-Finding, VI

As a specific application, Berlekamp's method is quite efficient for computing square roots modulo p for arbitrary primes p.

- During our analysis of the Rabin cryptosystem, we showed that if $p \equiv 3 \pmod 4$, then $a^{(p+1)/4}$ is a square root of a modulo p, so in this case there is a simple formula for computing square roots.
- However, if $p \equiv 1 \pmod 4$ there is not such a nice formula, and so Berlekamp's method is a viable alternative.
- We will also mention, in particular, that using $a = 0$ will never work for computing square roots modulo p if $p \equiv 1 \pmod 4$, since the two square roots will always be both quadratic residues or both quadratic nonresidues because -1 is a quadratic residue modulo p.

Berlekamp's Root-Finding, VII

Example: Find the roots of $x^2 \equiv 3 \pmod{13}$.

Berlekamp's Root-Finding, VII

Example: Find the roots of $x^2 \equiv 3 \pmod{13}$.

- First, we can compute $\left(\frac{3}{13}\right) = +1$ (either via Euler's criterion or by using quadratic reciprocity), so 3 does have square roots modulo 13.
- To compute them we let $q(x) = x^2 - 3$ modulo $p = 13$, and use Berlekamp's algorithm.
- As noted previously, $a = 0$ will not work, so we try $a = 1$: then $q(x - a) = x^2 - 2x - 2$.
- Using successive squaring, we can calculate $x^{(p-1)/2} = x^6 \equiv 3x + 10 \pmod{13}$.

Berlekamp's Root-Finding, VIII

Example: Find the roots of $x^2 \equiv 3 \pmod{13}$.

- This means $x^{(p-1)/2} - 1 \equiv 3x + 9 \pmod{13}$, and so the first step of the Euclidean algorithm reads $x^{(p-1)/2} \equiv [\text{quotient}] \cdot q(x-a) + (3x+9)$.
- Performing the next step shows that $3x + 9$ does indeed divide $x^2 - 2x - 2$ modulo 13 (the quotient is $9x + 7$).
- Solving for the first root (i.e., solving $3n + 9 \equiv 0 \pmod{13}$) yields $n \equiv -3 \equiv 10 \pmod{13}$.
- This means $n = 10$ is a root of $q(x-1)$, and therefore $n - 1 = 9$ is a root of the original polynomial $q(x)$.
- Indeed, we can check that $9^2 \equiv 3 \pmod{13}$. Therefore, the two roots are $r \equiv \boxed{\pm 9} \pmod{13}$.

Berlekamp's Root-Finding, IX

Example: Find the roots of $x^2 \equiv 11 \pmod{2017}$.

Berlekamp's Root-Finding, IX

Example: Find the roots of $x^2 \equiv 11 \pmod{2017}$.

- First, we can compute $\left(\frac{11}{2017}\right) = +1$ (either via Euler's criterion or by using quadratic reciprocity), so 11 does have square roots modulo the prime 2017.
- To compute them we let $q(x) = x^2 - 11$ modulo $p = 2017$.
- As noted above, $a = 0$ will not work, so we try $a = 1$, so that $q(x - a) = x^2 - 2x - 10$.
- Using successive squaring, we can calculate $x^{(p-1)/2} = x^{1008} \equiv 307x + 1710 \pmod{2017}$.

Berlekamp's Root-Finding, X

Example: Find the roots of $x^2 \equiv 11 \pmod{2017}$.

- This means $x^{(p-1)/2} - 1 \equiv 307x + 1709 \pmod{2017}$, and so the first step of the Euclidean algorithm reads $x^{(p-1)/2} \equiv [\text{quotient}] \cdot q(x-a) + (307x + 1709)$.
- Performing the next step shows that $307x + 1709$ does indeed divide $x^2 - 2x - 10$ modulo 2017 (the quotient is $1360x + 668$).
- Solving for the first root (i.e., solving $307n + 1709 \equiv 0 \pmod{2017}$) yields $n \equiv 1361 \pmod{2017}$.
- This means $n = 1361$ is a root of $q(x-1)$, and therefore $n - 1 = 1360$ is a root of the original polynomial $q(x)$.
- Indeed, we can check that $1360^2 \equiv 11 \pmod{2017}$. Therefore, the two roots are $r \equiv \boxed{\pm 1360} \pmod{2017}$.

Berlekamp's Root-Finding, XI

Although we have quoted this result for polynomials $q(x)$ that factor as a product of linear terms, we can in fact reduce the general problem of finding roots for arbitrary polynomials in $\mathbb{F}_p[x]$ to this case.

- Explicitly, first we remove any repeated irreducible factors from q using its derivative, and then we apply the factorization algorithm above to the greatest common divisor of $q(x)$ and $x^p - x$.
- Since $x^p - x$ is the polynomial whose roots are all the elements of $\mathbb{F}_p$, the greatest common divisor of $q(x)$ and $x^p - x$ will be the product of all the linear terms in the factorization of $q(x)$, which is the factor of $q(x)$ that contains all its roots.
- Thus, to find roots of $q(x)$, we need only find the roots of the greatest common divisor of $q(x)$ and $x^p - x$, and we can do this using the algorithm described above.

Solovay-Strassen, I

Our fourth and final application of quadratic reciprocity is to give another compositeness test. Here is the basic idea:

- By Euler's criterion, if p is prime then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$.
- Initially, we used this test to give a method for computing the Legendre symbol $\left(\frac{a}{p}\right)$.
- But we also have another way to compute this symbol, namely, by evaluating the Jacobi symbol $\left(\frac{a}{p}\right)$ using the "flip and reduce" procedure provided by quadratic reciprocity.
- If we then compare the results of these two methods, we see that if $a^{(p-1)/2} \not\equiv \left(\frac{a}{p}\right)$ modulo p, then p is not prime.

Solovay-Strassen, II

This is precisely the idea of the Solovay-Strassen test:

Test (Solovay-Strassen)

If m is an odd integer such that $a^{(m-1)/2} \not\equiv \left(\frac{a}{m}\right)$ modulo m, then m is composite.

We remark that in order for the test to be useful, we need to calculate the Jacobi symbol $\left(\frac{a}{m}\right)$ using quadratic reciprocity. Thus, we will want to select a to be an odd residue class that is greater than 1.

Solovay-Strassen, III

This compositeness test was developed by Solovay and Strassen in 1978 (thereby slightly predating our version of Miller-Rabin).

- Like with the Fermat and Miller-Rabin tests, this is a compositeness test only: each individual application for a single value of a can only produce the results "m is composite" or "no result".
- In practice, the Solovay-Strassen test is used probabilistically, like with the Miller-Rabin test: we apply the test many times to the integer m, and if it passes sufficiently many times, we say m is probably prime.
- It can be shown that any given residue has at least a $1/2$ probability of showing that m is composite, so the probability that a composite integer m can pass the test k times with randomly-chosen residues a is at most $1/2^k$.

Solovay-Strassen, IV

Example: Use Solovay-Strassen to decide whether 561 is prime. (Note that 561 is a Carmichael number, and passes the Fermat test for every residue class.)

Solovay-Strassen, IV

Example: Use Solovay-Strassen to decide whether 561 is prime. (Note that 561 is a Carmichael number, and passes the Fermat test for every residue class.)

- We try $a = 5$: we have $5^{(m-1)/2} \equiv 5^{280} \equiv 67 \pmod{561}$, whereas $\left(\frac{5}{561}\right) = \left(\frac{561}{5}\right) = \left(\frac{1}{5}\right) = 1$.
- Since these are unequal, we conclude that 561 is composite.
- As usual with our compositeness tests, we don't obtain any information about the factorization of 561; all we know is that it is composite.

Solovay-Strassen, V

Example: Use Solovay-Strassen with $a = 137$ to decide whether 35113 is prime.

Solovay-Strassen, V

Example: Use Solovay-Strassen with $a = 137$ to decide whether 35113 is prime.

- With $m = 35113$, we have $137^{(m-1)/2} \equiv 137^{17556} \equiv 1 \pmod{2701}$.
- Also, we have $\left(\frac{137}{35113}\right) = \left(\frac{35113}{137}\right) = \left(\frac{41}{137}\right) = \left(\frac{137}{41}\right) = \left(\frac{14}{41}\right) = \left(\frac{2}{41}\right) \cdot \left(\frac{7}{41}\right) = +1 \cdot \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1.$
- Since these are unequal, we conclude that 35113 is composite.

Generalizations of Quadratic Reciprocity, I

To close out this lecture, we will briefly mention a few tidbits about some generalizations of quadratic reciprocity.

Generalizations of Quadratic Reciprocity, I

To close out this lecture, we will briefly mention a few tidbits about some generalizations of quadratic reciprocity.

If you have been following the structure of the course so far, here is what we did:

- We studied factorization and modular arithmetic over the integers.
- Then we studied factorization and modular arithmetic in residue rings of $\mathbb{Z}[i]$ and $\mathbb{F}_p[x]$.
- Now we have finished studying quadratic residues and quadratic reciprocity in $\mathbb{Z}/m\mathbb{Z}$.
- The natural next step is then to study quadratic residues and quadratic reciprocity in residue rings of $\mathbb{Z}[i]$ and $\mathbb{F}_p[x]$.

Generalizations of Quadratic Reciprocity, II

There are several possible ways to generalize quadratic reciprocity:

- One natural avenue for generalization is to seek a version of the Legendre symbol that detects when a given element is a square modulo a prime, in more general rings.
- Another avenue is to generalize to higher degree: to seek a version of the Legendre symbol that detects when a given element is a cube, fourth power, etc., modulo a prime.
- There are generalizations in each of these directions, and although we do not have the tools to discuss many of them, the program of finding and classifying these various "reciprocity laws" motivated much of the development of algebraic number theory in the early 20th century.

Generalizations of Quadratic Reciprocity, III

Here are the generalizations that we discuss in §5.6:

- In §5.6.1, we discuss how to define quadratic residues and a general quadratic residue symbol for an arbitrary Euclidean domain. Then we generalize Euler's criterion.
- In §5.6.2, we prove quadratic reciprocity over $\mathbb{Z}[i]$.
- In §5.6.3, we describe an extension of quadratic reciprocity over $\mathbb{Z}[i]$ called "quartic reciprocity", so named because it detects 4th powers.
- Finally, §5.6.4, we discuss quadratic reciprocity over $\mathbb{F}_p[x]$ and also a much more general version known as dth-power reciprocity.

Summary

We discussed several applications of quadratic reciprocity:

- Characterizing the primes p for which a is a quadratic residue modulo p
- Characterizing primes dividing values of a quadratic polynomial
- Berlekamp's factorization algorithm
- The Solovay-Strassen primality test.

We gave a brief overview of some generalizations of quadratic reciprocity.

It's The End, For Real!

We're now at the end of the course (except of course for the final).

I hope you enjoyed learning number theory with me this semester as much as I enjoyed teaching it. It is a subject near and dear to me (I am, after all, a number theorist!) and I hope you will take away at least a bit of appreciation for the subject.

If you did in fact enjoy the course, I would greatly appreciate it if you took the time to fill out the TRACE evaluations and mention that fact.

Thanks, and good luck on the final!