Math 4527 (Number Theory 2)

Lecture #31 of 37 $\sim$ April 5, 2021

Cubic and Quartic Reciprocity

- Cubic Reciprocity
- Arithmetic in $\mathbb{Z}[i]$
- The Quartic Residue Symbol
- Quartic Reciprocity

This material represents §8.3.4-8.3.5 from the course notes.

The Cubic Residue Symbol

Recall our definition of our cubic residue symbol:

Definition

If π is a prime element of $\mathcal{O}_{\sqrt{-3}}$ and $N(\pi) \neq 3$, we define the cubic residue symbol $\left[\frac{\alpha}{\pi}\right]_3 \in \{0, 1, \omega, \omega^2\}$ to be 0 if $\pi | \alpha$, and otherwise to be the unique value among $\{1, \omega, \omega^2\}$ satisfying $\left[\frac{\alpha}{\pi}\right]_3 \equiv \alpha^{(N(\pi)-1)/3} \pmod{\pi}$.

The cubic residue symbol detects cubes, much as the Legendre symbol detects squares.

Cubic Reciprocity, I

Here is the statement of cubic reciprocity:

Theorem (Cubic Reciprocity in $\mathcal{O}_{\sqrt{-3}}$)

If π and λ are both primary primes in $\mathcal{O}_{\sqrt{-3}}$ with different norms (i.e., with π, λ both congruent to 2 modulo 3, and with $N(\pi) \neq N(\lambda)$), then $\left[\frac{\pi}{\lambda}\right]_3 = \left[\frac{\lambda}{\pi}\right]_3$.

Some aspects of this result were mentioned by Euler and Gauss, and results that are essentially equivalent to this one are implied by some results in Gauss's papers, but the first proof is due to Eisenstein: indeed, the ring $\mathcal{O}_{\sqrt{-3}}$ is occasionally known as the Eisenstein integers for this reason.

Cubic Reciprocity, II

The proof is relatively involved and is typically broken into three cases: when π and λ are both integer primes, when one is an integer prime, and when both are complex.

- The first case is trivial, since if p is an integer then $\left[\frac{p}{\lambda}\right]_3 = 1$ regardless of the value of λ, as we showed earlier.
- The second case requires proving that $\left[\frac{\lambda}{p}\right]_3 = 1$ if p is a prime integer and λ is a prime element, since $\left[\frac{p}{\lambda}\right]_3 = 1$ as noted above.
- The third case is the most difficult.

Cubic Reciprocity, III

Example: Verify cubic reciprocity for $\pi = \dfrac{7+3\sqrt{-3}}{2} = 5+3\omega$ and $\lambda = 2+3\sqrt{-3} = 5+6\omega$ in $\mathcal{O}_{\sqrt{-3}}$.

Cubic Reciprocity, III

Example: Verify cubic reciprocity for $\pi = \dfrac{7+3\sqrt{-3}}{2} = 5+3\omega$ and $\lambda = 2+3\sqrt{-3} = 5+6\omega$ in $\mathcal{O}_{\sqrt{-3}}$.

- We have $N(\pi) = 19$ and $N(\lambda) = 31$.
- By definition we have
$$\left[\frac{\lambda}{\pi}\right]_3 \equiv \lambda^{(N(\pi)-1)/3} \equiv (5+6\omega)^6 \equiv \omega^2 \pmod{\pi}.$$
- By definition we also have
$$\left[\frac{\pi}{\lambda}\right]_3 \equiv \lambda^{(N(\lambda)-1)/3} \equiv (5+3\omega)^{10} \equiv \omega^2 \pmod{\lambda}.$$
- Thus, we see $\left[\dfrac{\lambda}{\pi}\right]_3 = \left[\dfrac{\pi}{\lambda}\right]_3$, precisely as dictated by cubic reciprocity.

Cubic Reciprocity, IV

The general approach to most proofs of cubic reciprocity involves manipulation of Gauss sums.

Definition

A multiplicative character on $\mathbb{F}_p$ is a function $\chi : \mathbb{F}_p^\times \to \mathbb{C}$ such that $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{F}_p^\times$.

Equivalently, a multiplicative character is a group homomorphism from $\mathbb{F}_p^\times$ to $\mathbb{C}$. The Legendre symbol and the cubic residue symbol are both examples of multiplicative characters.

Definition

If χ is a multiplicative character on $\mathbb{F}_p$, we define the Gauss sum

$$g_a(\chi) = \sum_{t=1}^{p-1} \chi(t) e^{2\pi i a t/p} \in \mathbb{C}$$

Cubic Reciprocity, V

Definition

If χ is a multiplicative character on $\mathbb{F}_p$, we define the Gauss sum

$$g_a(\chi) = \sum_{t=1}^{p-1} \chi(t) e^{2\pi i a t/p} \in \mathbb{C}$$

- The values of the Gauss sum $g_a(\chi)$ are essentially the discrete Fourier transform of the function $\chi(t)$.
- Thus, the values of the Gauss sum completely encode all of the information that is contained in the values of the function $\chi(t)$, and we may convert back and forth between the values of $g_a(\chi)$ and the values $\chi(t)$.
- As such, if we can compute the value of the Gauss sum for a character, then it essentially uniquely determines the value of the character.

Cubic Reciprocity, VI

Thus, to prove cubic reciprocity, the idea is to consider the Gauss sums for the cubic character $\chi_\pi(t) = \left[\frac{t}{\pi}\right]_3$ on $\mathbb{F}_p$, where $p = \pi\overline{\pi}$.

Using the definitions, one may prove various identities involving the Gauss sums:

1. For any character χ, we have $g_a(\chi) = \chi(a)^{-1} g_1(\chi)$.
2. For any character $\chi \neq 1$, we have $g_1(\chi)\overline{g_1(\chi)} = p$.
3. For the cubic residue character χ_π, we have $g_1(\chi_\pi)^3 = p\pi$.

By suitably manipulating these identities, we can then show that $\chi_\lambda(\pi) = \chi_\pi(\lambda)$ for all primary primes λ and π, which establishes cubic reciprocity.

- We will illustrate by working through the second case of the proof (the third case is more difficult but can be done using a similar method).

Cubic Reciprocity, VII

Proof (Second Case of Cubic Reciprocity):

- Suppose $q \equiv 2 \pmod 3$ is an integer prime and π is a non-integral prime of $\mathcal{O}_{\sqrt{-3}}$, with $\pi\overline{\pi} = p$ that is 1 mod 3.
- Take the $(q^2-1)/3$ power of the Gauss-sum identity $g_1(\chi_\pi)^3 = p\pi$ to obtain
  $g_1(\chi_\pi)^{q^2-1} \equiv (p\pi)^{(q^2-1)/3} \equiv \chi_q(p\pi) = \chi_q(\pi) \pmod q$
  because χ_q is multiplicative and $\chi_q(p) = 1$ as we showed.
- Thus, $g_1(\chi_\pi)^{q^2} \equiv \chi_q(\pi) g_1(\chi_\pi) \pmod q$.

Cubic Reciprocity, VII

Proof (continued):

- Since $q^2 \equiv 1 \pmod 3$ and the value $\chi_\pi(t)$ is zero or a cube root of unity, we have $\chi_\pi(t)^{q^2} = \chi_\pi(t)$ for all t.
- Also, the qth-power map is additive mod q, so

$$\begin{aligned} g_1(\chi_\pi)^{q^2} &= \left[\sum_{t=0}^{p-1} \chi_\pi(t) e^{2\pi i t/p}\right]^{q^2} \\ &\equiv \sum_{t=0}^{p-1} \chi_\pi(t)^{q^2} e^{2\pi i q^2 t/p} \pmod q \\ &= \sum_{t=0}^{p-1} \chi_\pi(t) e^{2\pi i q^2 t/p} = g_{q^2}(\chi_\pi) \\ &= \chi_\pi(q^{-2}) g_1(\chi_\pi) = \chi_\pi(q) g_1(\chi_\pi) \end{aligned}$$

via the Gauss-sum identity $g_a(\chi) = \chi(a)^{-1} g_1(\chi)$.

Cubic Reciprocity, VIII

Proof (continued):

- So, we have now computed two different expressions for the power $g_1(\chi_\pi)^{q^2}$ modulo q: they are

$$\begin{aligned} g_1(\chi_\pi)^{q^2} &\equiv \chi_q(\pi) g_1(\chi_\pi) \pmod{q} \\ g_1(\chi_\pi)^{q^2} &\equiv \chi_\pi(q) g_1(\chi_\pi) \pmod{q} \end{aligned}$$

- Multiplying both sides by $\overline{g_1(\chi_\pi)}$ and using the Gauss-sum identity $g_1(\chi_\pi)\overline{g_1(\chi_\pi)} = p$ then yields

$$\chi_q(\pi) p \equiv \chi_\pi(q) p \pmod{q}.$$

- So, since p is invertible modulo q, we may cancel it to deduce that $\chi_q(\pi) \equiv \chi_\pi(q) \pmod{q}$.
- At last, this congruence implies the equality $\chi_q(\pi) = \chi_\pi(q)$, which is exactly cubic reciprocity in this case.

Cubic Reciprocity, IX

We can use cubic reciprocity to calculate the cubic residue symbol $\left[\frac{\alpha}{\pi}\right]_3$, after we find the prime factorization of the element α, using the same "flip-and-invert" procedure we use for evaluating Legendre symbols.

- Explicitly, if we write $\alpha = u \cdot (1-\omega)^k \lambda_1 \lambda_2 \cdots \lambda_n$ where the λ_i are primary primes, then we only need to compute the cubic residue symbols $\left[\frac{u}{\pi}\right]_3$, $\left[\frac{1-\omega}{\pi}\right]_3$, and $\left[\frac{\lambda_i}{\pi}\right]_3$.

Cubic Reciprocity, X

It remains to compute the residue symbols $\left[\frac{u}{\pi}\right]_3$ and $\left[\frac{1-\omega}{\pi}\right]_3$.

- The residue symbol $\left[\frac{u}{\pi}\right]_3$ we can compute using the definition since $u = \pm\omega^k$ and $\left[\frac{\omega}{\pi}\right]_3 = \omega^{(N(\pi)-1)/3}$, so $\left[\frac{\omega}{\pi}\right]_3 = 1$, ω, or ω^2 when $N(\pi) \equiv 1$, 4, or 7 modulo 9 (respectively), and $\left[\frac{-1}{\pi}\right]_3 = 1$.
- The residue symbol $\left[\frac{1-\omega}{\pi}\right]_3$ is more difficult to compute, but its value can be shown to be equal to $\omega^{2(p+1)/3}$ if $\pi = p$ is an integer prime, and it is equal to $\omega^{2(a+1)/3}$ if $\pi = a + b\omega$ is a primary prime.

Arithmetic in $\mathbb{Z}[i]$, I

We close with a brief discussion of quartic reciprocity, which (in analogy with quadratic and cubic reciprocity) gives a reciprocity law involving fourth powers.

- The values of the quartic residue symbol will be fourth roots of unity, just as the values of the cubic residue symbol are cube roots of unity, so we will work in the ring $\mathbb{Z}[i]$.
- Other than having to change a few things to accommodate the fact that we now have four values for the residue symbol, quartic reciprocity is quite similar to quadratic and cubic reciprocity.

Arithmetic in $\mathbb{Z}[i]$, II

First, some properties of arithmetic in $\mathbb{Z}[i]$:

Proposition (Arithmetic in $\mathbb{Z}[i]$)

Let π be a prime of $R = \mathbb{Z}[i]$. Then the following are true:

1. *The quotient ring $R/(\pi)$ is a finite field with $N(\pi)$ elements.*
2. *For any nonzero residue class α modulo π, we have $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.*
3. *If π is not associate to $1+i$, the elements 1, i, -1, and $-i$ are distinct modulo π, and $N(\pi) - 1$ is divisible by 4.*

Arithmetic in $\mathbb{Z}[i]$, II

1. The quotient ring $R/(\pi)$ is a finite field with $N(\pi)$ elements.
2. For any nonzero residue class α modulo π, we have $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.

Proofs:

- These results hold for any prime element π in any quadratic integer ring.

---

3. If π is not associate to $1+i$, the elements 1, i, -1, and $-i$ are distinct modulo π, and $N(\pi)-1$ is divisible by 4.

Proof:

- If any of 1, i, -1, $-i$ are equivalent modulo π, then π must have a common factor with $(1+i)(1-i)=2$, which it cannot.
- The second statement follows from Lagrange's theorem applied to the subgroup $\{1, i, -1, -i\}$ of residues modulo π.

Arithmetic in $\mathbb{Z}[i]$, III

Now we can define the quartic residue symbol by looking at a factorization, just as with the quadratic and cubic residue symbols.

- If π is a prime element of odd norm in $\mathbb{Z}[i]$ and $\pi \nmid \alpha$, then since $N(\pi) - 1$ is divisible by 4, we can factor the expression $\alpha^{N(\pi)-1} - 1 \equiv 0$ in $\mathbb{Z}[i]/\pi$ as $(\alpha^{(N(\pi)-1)/4} - 1) \cdot (\alpha^{(N(\pi)-1)/4} + 1) \cdot (\alpha^{(N(\pi)-1)/4} + i) \cdot (\alpha^{(N(\pi)-1)/4} - i) \equiv 0 \pmod{\pi}$.
- Since $\mathbb{Z}[i]/(\pi)$ is an integral domain, this means $\alpha^{(N(\pi)-1)/4}$ is equivalent to one of 1, -1, i, $-i$ modulo π.

Arithmetic in $\mathbb{Z}[i]$, IV

Now we can define the quartic residue symbol:

Definition

If π is a prime element of $\mathbb{Z}[i]$ and $N(\pi) \neq 2$, we define the quartic residue symbol $\left[\frac{\alpha}{\pi}\right]_4 \in \{0, 1, i, -1, -i\}$ to be 0 if $\pi | \alpha$, and otherwise to be the unique value among $\{1, i, -1, -i\}$ satisfying $\left[\frac{\alpha}{\pi}\right]_4 \equiv \alpha^{(N(\pi)-1)/4} \pmod{\pi}$.

Examples:

1. $\left[\frac{1+i}{3}\right]_4 \equiv (1+i)^2 \equiv -i \pmod{3}$, so $\left[\frac{1+i}{3}\right]_4 = -i$.
2. $\left[\frac{2+i}{4+i}\right]_4 \equiv (2+i)^4 \equiv -1 \pmod{4+i}$, so $\left[\frac{2+i}{4+i}\right]_4 = -1$.

Arithmetic in $\mathbb{Z}[i]$, V

The quartic residue symbol the same properties as the cubic residue symbol:

Proposition (Properties of Quartic Residues, I)

Let π be a prime element of $\mathbb{Z}[i]$ and $N(\pi) \neq 2$ and let $\alpha, \beta \in \mathbb{Z}[i]$. Then the following hold:

1. *If $\alpha \equiv \beta \pmod{\pi}$ then* $\left[\frac{\alpha}{\pi}\right]_4 = \left[\frac{\beta}{\pi}\right]_4$.
2. *The symbol is multiplicative:* $\left[\frac{\alpha\beta}{\pi}\right]_4 = \left[\frac{\alpha}{\pi}\right]_4 \left[\frac{\beta}{\pi}\right]_4$.
3. *We have* $\left[\frac{\overline{\alpha}}{\pi}\right]_4 = \overline{\left[\frac{\alpha}{\pi}\right]_4} = \left[\frac{\alpha}{\pi}\right]_4^3 = \left[\frac{\alpha^3}{\pi}\right]_4$.
4. *If n is an integer not divisible by π, then* $\left[\frac{n}{\pi}\right]_4 = 1$ *or* -1.

Proofs: These are straightforward.

Arithmetic in $\mathbb{Z}[i]$, VI

The quartic residue symbol has most of the same properties as the cubic residue symbol:

Proposition (Properties of Quartic Residues, II)

Let π be a prime element of $\mathbb{Z}[i]$ and $N(\pi) \neq 2$ and let $\alpha, \beta \in \mathbb{Z}[i]$. Then the following hold:

5. *If u is a primitive root modulo π (i.e., an element of order $N(\pi) - 1$ modulo π), then $\left[\frac{u}{\pi}\right]_4$ is either i or $-i$.*
6. *The quartic residue symbol detects fourth powers and squares: if $\alpha \neq 0 \bmod \pi$, then $\left[\frac{\alpha}{\pi}\right]_4 = 1$ if and only if α is a quartic residue modulo π (which is to say, $\alpha \equiv \beta^4 \pmod{\pi}$ for some β), and $\left[\frac{\alpha}{\pi}\right]_4 = -1$ if and only if α is a quadratic residue that is not a quartic residue.*

Arithmetic in $\mathbb{Z}[i]$, VII

5. If u is a primitive root modulo π (i.e., an element of order $N(\pi)-1$ modulo π), then $\left[\frac{u}{\pi}\right]_4$ is either i or $-i$.

Proof:

- We cannot have $u^{(N(\pi)-1)/2} \equiv 1 \pmod{\pi}$ since this would imply u has order at most $(N(\pi)-1)/2$.

---

6. The quartic residue symbol detects fourth powers and squares: if $\alpha \neq 0 \bmod \pi$, then $\left[\frac{\alpha}{\pi}\right]_4 = 1$ if and only if α is a quartic residue modulo π, and $\left[\frac{\alpha}{\pi}\right]_4 = -1$ if and only if α is a quadratic residue that is not a quartic residue.

Proof:

- By (5), if $\alpha = u^k$ then $\left[\frac{\alpha}{\pi}\right]_4 = (\pm i)^k$, which equals $+1$ if k is a multiple of 4 and equals -1 if k is even and not a multiple of 4. These are equivalent to saying α is a quartic residue, and a quadratic residue that is not a quartic residue, respectively.

Arithmetic in $\mathbb{Z}[i]$, VIII

Example: Determine whether $3+3i$, $6-i$, and 6 are quartic residues and whether they are quadratic residues modulo $\pi = 7+2i$ inside $\mathbb{Z}[i]$.

Arithmetic in $\mathbb{Z}[i]$, VIII

Example: Determine whether $3+3i$, $6-i$, and 6 are quartic residues and whether they are quadratic residues modulo $\pi = 7+2i$ inside $\mathbb{Z}[i]$.

- Since $N(\pi) = 53$, for $3+3i$ we must calculate the quartic residue symbol $\left[\frac{3+3i}{7+2i}\right]_4 \equiv (3+3i)^{(53-1)/4} \equiv (3+3i)^{13} \equiv -i \pmod{7+2i}$. Thus, $\left[\frac{3+3i}{7+2i}\right]_4 = -i$ and so $3+3i$ is not a quartic or quadratic residue modulo $7+2i$.
- Similarly, we have $\left[\frac{6-i}{7+2i}\right]_4 \equiv (6-i)^{13} \equiv 1 \pmod{7+2i}$ so $6-i$ is a quartic and quadratic residue mod $7+2i$.
- Finally, $\left[\frac{6}{7+2i}\right]_4 \equiv (6)^{13} \equiv -1 \pmod{7+2i}$ so 6 is a quadratic but not a quartic residue modulo $7+2i$.

Arithmetic in $\mathbb{Z}[i]$, IX

Example: Determine whether 2, 3, and $2 + i$ are quartic residues modulo $2 + 3i$, and also whether they are quadratic residues.

Arithmetic in $\mathbb{Z}[i]$, IX

Example: Determine whether 2, 3, and $2+i$ are quartic residues modulo $2+3i$, and also whether they are quadratic residues.

- We compute $\left[\frac{2}{2+3i}\right]_4 \equiv 2^3 \equiv i \pmod{\pi}$. Since this is not 1 or -1, 2 is not a quadratic residue or quartic residue modulo $2+3i$.
- Also, $\left[\frac{3}{2+3i}\right]_4 \equiv 3^3 \equiv 1 \pmod{\pi}$, which means 3 is a quartic residue (and also a quadratic residue) modulo $2+3i$.
- Finally, $\left[\frac{2+i}{2+3i}\right]_4 \equiv (2+i)^3 \equiv -1 \pmod{\pi}$, which means $2+i$ is a quadratic residue but not a quartic residue modulo $2+3i$.

Arithmetic in $\mathbb{Z}[i]$, X

We can define a similar notion of a primary prime for $\mathbb{Z}[i]$:

Definition

A prime element $\pi \in \mathbb{Z}[i]$ is primary if it is congruent to 1 modulo $2 + 2i$.

Examples:

- The primes -3, -7, and $3 + 2i$ are primary, while 11 and $2 + i$ are not.

As with the primary elements in $\mathcal{O}_{\sqrt{-3}}$, for all primes except the primes associate to $1 + i$ of norm 2, exactly one associate will be primary.

Arithmetic in $\mathbb{Z}[i]$, XI

We can now state quartic reciprocity:

Theorem (Quartic Reciprocity in $\mathbb{Z}[i]$)

If π and λ are distinct primes in $\mathbb{Z}[i]$ congruent to 1 modulo $2+2i$, then $\left[\frac{\pi}{\lambda}\right]_4 = \left[\frac{\lambda}{\pi}\right]_4 \cdot (-1)^{\frac{N(\pi)-1}{4}\cdot\frac{N(\lambda)-1}{4}}$.

Some aspects of this result (like the other reciprocity laws) were conjectured by Euler, and most of it was known to Gauss; a proof essentially appears in some of his unpublished papers. The first published proof is due to Eisenstein.

Arithmetic in $\mathbb{Z}[i]$, XII

Example: Verify quartic reciprocity for $\pi = 3 + 2i$ and $\lambda = 5 - 4i$ in $\mathbb{Z}[i]$.

Arithmetic in $\mathbb{Z}[i]$, XII

Example: Verify quartic reciprocity for $\pi = 3 + 2i$ and $\lambda = 5 - 4i$ in $\mathbb{Z}[i]$.

- We have $N(\pi) = 13$ and $N(\lambda) = 41$.
- Then we have $\left[\dfrac{3+2i}{5-4i}\right]_4 \equiv (3+2i)^{(41-1)/4} \equiv (3+2i)^{10} \equiv i \pmod{5-4i}$, so $\left[\dfrac{3+2i}{5-4i}\right]_4 = i$.
- Likewise, $\left[\dfrac{5-4i}{3+2i}\right]_4 \equiv (5-4i)^{(13-1)/4} \equiv (5-4i)^3 \equiv i \pmod{3+2i}$, so $\left[\dfrac{5-4i}{3+2i}\right]_4 = i$ as well.
- Since $\dfrac{N(\pi)-1}{4} \cdot \dfrac{N(\lambda)-1}{4}$ is even, the result $\left[\dfrac{\pi}{\lambda}\right]_4 = \left[\dfrac{\lambda}{\pi}\right]_4$ is in accordance with quartic reciprocity.

Arithmetic in $\mathbb{Z}[i]$, XIII

Example: Verify quartic reciprocity for $\pi = 3 + 2i$ and $\lambda = 7 - 2i$ in $\mathbb{Z}[i]$.

Arithmetic in $\mathbb{Z}[i]$, XIII

Example: Verify quartic reciprocity for $\pi = 3 + 2i$ and $\lambda = 7 - 2i$ in $\mathbb{Z}[i]$.

- We have $N(\pi) = 13$ and $N(\lambda) = 53$.
- Then we have $\left[\dfrac{3+2i}{7-2i}\right]_4 \equiv (3+2i)^{(53-1)/4} \equiv (3+2i)^{13} \equiv 1 \pmod{7-2i}$, so $\left[\dfrac{3+2i}{7-2i}\right]_4 = 1$.
- Likewise, $\left[\dfrac{7-2i}{3+2i}\right]_4 \equiv (7-2i)^{(13-1)/4} \equiv (7-2i)^3 \equiv -1 \pmod{3+2i}$, so $\left[\dfrac{7-2i}{3+2i}\right]_4 = -1$.
- Since $\dfrac{N(\pi)-1}{4} \cdot \dfrac{N(\lambda)-1}{4}$ is odd, the result $\left[\dfrac{\pi}{\lambda}\right]_4 = -\left[\dfrac{\lambda}{\pi}\right]_4$ is in accordance with quartic reciprocity.

Arithmetic in $\mathbb{Z}[i]$, XIV

Like with cubic reciprocity, we can establish quartic reciprocity by manipulating the Gauss sums for the quartic character $\chi_\pi(t) = \left[\frac{t}{\pi}\right]_4$.

- Like with cubic reciprocity, the proof is relatively involved and is typically broken into three cases: when π and λ are both integer primes, when one is an integer prime, and when both are complex.
- The case where both primes are integers essentially amounts to quadratic reciprocity.
- We will establish the result in one special case, as an illustration, taking as given the Gauss-sum identities $g_a(\chi) = \chi(a)^{-1} g_1(\chi)$, $g_1(\chi_\pi)\overline{g_1(\chi_\pi)} = p$, and $g_1(\chi_\pi)^4 = \pi^3\overline{\pi}$.

Arithmetic in $\mathbb{Z}[i]$, XV

Proof (Second Case):

- Let q be a prime congruent to 3 modulo 4 (so that $-q$ is the primary element associate to q) and π be a non-integral primary prime with $\pi\overline{\pi} = p$.
- First, taking the $(q+1)/4$th power of the third Gauss-sum identity $g_1(\chi_\pi)^4 = \pi^3\overline{\pi}$ yields $g_1(\chi_\pi)^{q+1} = (\pi^3\overline{\pi})^{(q+1)/4}$.
- Since $\pi^q \equiv \overline{\pi} \pmod{q}$, as can be seen by taking the qth power of $(a+bi)^q$, we see that

$$\begin{aligned} g_1(\chi_\pi)^{q+1} &\equiv \pi^{(q+1)(q+3)/4} && \pmod{q} \\ &= \pi^{(q^2-1)/4}\pi^{q+1} \\ &\equiv \chi_q(\pi)\pi\overline{\pi} \equiv \chi_q(\pi)p && \pmod{q} \end{aligned}$$

by the definition of the quartic residue symbol.

Arithmetic in $\mathbb{Z}[i]$, XVI

Proof (Second Case, continued):

- Also note that $\chi_\pi(t)$ is a fourth root of unity, so since $q \equiv 3 \pmod 4$ the qth power is the same as the complex conjugate
- Since the qth-power map is additive mod q, we have

$$\begin{aligned} g_1(\chi_\pi)^q &\equiv \left[\sum_{t=1}^{p-1} \chi_\pi(t) e^{2\pi i t/p}\right]^q \pmod q \\ &\equiv \sum_{t=1}^{p-1} \chi_\pi(t)^q e^{2\pi i q t/p} \pmod q \\ &\equiv \sum_{t=1}^{p-1} \overline{\chi_\pi(t)} e^{2\pi i q t/p} \\ &\equiv g_q(\overline{\chi_\pi}) \pmod q. \end{aligned}$$

again by the definition of the Gauss sum.

Arithmetic in $\mathbb{Z}[i]$, XVII

Proof (Second Case, continued):

- But by the first Gauss-sum identity, we have $g_q(\overline{\chi_\pi}) = \overline{\chi_\pi(q)^{-1}} g_1(\overline{\chi_\pi}) = \chi_\pi(-q) g_1(\overline{\chi_\pi})$ since $\chi_\pi(q)$ is a root of unity.
- Putting all of this together yields $\chi_q(\pi)p \equiv g_1(\chi_\pi)^{q+1} \equiv \chi_\pi(-q) g_1(\chi_\pi) g_1(\overline{\chi_\pi}) \equiv \chi_\pi(-q)p \pmod{q}$ using the second Gauss-sum identity.
- Finally, cancelling the factor of p yields $\chi_\pi(-q) \equiv \chi_q(\pi) \pmod{q}$, and this congruence implies the equality $\chi_\pi(-q) = \chi_q(\pi)$, which is the statement of quartic reciprocity in this case.

Closing Remarks, I

We have now discussed quadratic, cubic, and quartic reciprocity laws.

- It is quite reasonable to wonder, then: what about for higher powers? Is there (for example) a quintic reciprocity law?
- The direct answer is: yes, such laws exist, but require more intricate arguments inside the cyclotomic extension $\mathbb{Z}[\zeta_p]$, where $\zeta_n = e^{2\pi i/n}$ is a primitive nth root of unity.
- For example, quintic reciprocity involves primes from the ring $\mathbb{Z}[\zeta_5]$. One proof of the classical version of quintic reciprocity relies on the geometry of the hyperelliptic curve $y^2 = x^5 + 1/4$.
- In fact, Eisenstein's original proofs for cubic and quartic reciprocity used elliptic functions, and these arguments can be reformulated to use elliptic curves.

Closing Remarks, II

There are many other classical questions that we have just scratched the surface of.

- For example, we established classifications of the integers that can be written in the form $a^2 + b^2$, $a^2 + 2b^2$, $a^2 + ab + b^2$, and $a^2 + 3b^2$.
- One may, more generally, ask about representations by arbitrary quadratic forms (i.e., arbitrary homogeneous quadratic polynomials in a, b) – this leads into quite deep directions, and answering this question in full requires developing class field theory.
- These various reciprocity laws we have discussed can be generalized and extended, as was done by Kummer (in establishing Kummer reciprocity), Hilbert (via his definition of the Hilbert symbol), and Artin (who formulated a very general law known as Artin reciprocity).

Summary

We outlined the proof of the cubic reciprocity law using properties of Gauss sums.

We developed the quartic residue symbol and established some of its properties.

We outlined the proof of the quartic reciprocity law using properties of Gauss sums.

Next lecture: The geometry of numbers.