Math 4527 (Number Theory 2)

Lecture #30 of 37 $\sim$ April 1, 2021

Cubic Reciprocity

- The Equation $x^3 + y^3 = z^3$
- Arithmetic in $\mathcal{O}_{\sqrt{-3}}$
- The Cubic Residue Symbol
- Cubic Reciprocity

This material represents §8.3.3-8.3.4 from the course notes.

Some More Diophantine Equations, VII

We can, with a nontrivial amount of work, also establish the $n = 3$ case of Fermat's conjecture, which was first settled by Euler.

For convenience in organizing the proof, we first establish a lemma (which is itself another example of solving a Diophantine equation):

Lemma (Cubes of the Form $m^2 + 3n^2$)

Suppose that m, n are relatively prime integers of opposite parity. If $m^2 + 3n^2 = r^3$, then there exist positive integers a and b with $m = a^3 - 9ab^2$ and $n = 3a^2b - 3b^3$.

The expressions for m and n come from comparing coefficients in $m + n\sqrt{-3} = (a + b\sqrt{-3})^3$.

Some More Diophantine Equations, VIII

Proof:

- Let m, n be relatively prime, opposite parity, $m^2 + 3n^2 = r^3$.
- First, if $3|m$ so that $m = 3k$, then we obtain $9k^2 + 3n^2 = r^3$: this forces $3|r$, but then dividing by 3 shows that $n^3 = (r/3)^3 - 3k^2$ so that 3 would also divide n, which is impossible. Thus, $3 \nmid m$.
- Now factor the equation $m^2 + 3n^2 = r^3$ in $\mathcal{O}_{\sqrt{-3}}$ as $(m + n\sqrt{-3})(m - n\sqrt{-3}) = r^3$.
- Any common divisor of $m + n\sqrt{-3}$ and $m - n\sqrt{-3}$ must also divide $2m$ and $2n\sqrt{-3}$, and since m, n are relatively prime, this means the common divisor must divide $2\sqrt{-3}$.
- Since 2 and $\sqrt{-3}$ are irreducible in $\mathcal{O}_{\sqrt{-3}}$, we can see 2 does not divide $m + n\sqrt{-3}$ because m, n have opposite parities, and $\sqrt{-3}$ does not divide $m + n\sqrt{-3}$ because $3 \nmid m$.

Some More Diophantine Equations, IX

Proof (continued):

- So, $m + n\sqrt{-3}$ and $m - n\sqrt{-3}$ are relatively prime.
- Then since $\mathcal{O}_{\sqrt{-3}}$ is a UFD, we see that $m + n\sqrt{-3}$ must be a unit times a cube: say $m + n\sqrt{-3} = u \cdot (a + b\sqrt{-3})^3$. By negating, conjugating, and replacing $a + b\sqrt{-3}$ with an associate as necessary, we may assume $a, b \in \mathbb{Z}$ and that the unit u is either 1 or $\frac{-1+\sqrt{-3}}{2}$.
- However, if $m + n\sqrt{-3} = \frac{-1+\sqrt{-3}}{2} \cdot (a + b\sqrt{-3})^3$ then since m, n are integers, both a and b must be odd. But then $(-1 + \sqrt{-3})(a + b\sqrt{-3})$ has integer coefficients that are even, as does $(a + b\sqrt{-3})^2$, so the product $m + n\sqrt{-3}$ would have both m and n even, contrary to assumption.
- Therefore, we must have $m + n\sqrt{-3} = (a + b\sqrt{-3})^3 = (a^3 - 9ab^2) + (3a^2b - 3b^3)\sqrt{-3}$ and so $m = a^3 - 9ab^2$ and $n = 3a^2b - 3b^3$, as claimed.

Some More Diophantine Equations, X

We can now essentially give Euler's treatment of the $n = 3$ case of Fermat's equation:

Theorem (Euler's $p = 3$ Case of Fermat's Theorem)

There are no solutions to the Diophantine equation $x^3 + y^3 = z^3$ with $xyz \neq 0$.

As with the $n = 4$ case that we did a month and a half ago, the idea is to use a descent argument: by assuming there is a nontrivial solution, we will construct a smaller solution, which yields a contradiction if we assume that we start with the solution having the minimal possible $|z|$.

Some More Diophantine Equations, XI

Proof:

- Assume $x, y, z \neq 0$ and suppose we have a solution to the equation with $|z|$ minimal.
- If two of x, y, z are divisible by a prime p then the third must be also, in which case we could divide x, y, z by p and obtain a smaller solution.
- Thus, without loss of generality, we may assume x, y, z are relatively prime, and so two are odd and the other is even.
- By rearranging and negating, suppose that x and y are odd and relatively prime. Set $x + y = 2p$ and $x - y = 2q$, so that $x = p + q$ and $y = p - q$, where p, q are necessarily relatively prime of opposite parity. We then obtain a factorization $z^3 = x^3 + y^3 = (x + y)(x^2 - xy + y^2) = 2p \cdot (p^2 + 3q^2)$.
- We now proceed in two cases: where $3 \nmid p$ and where $3|p$.

Some More Diophantine Equations, XII

Proof (Case $3 \nmid p$, Start):

- Suppose $3 \nmid p$. Since $p^2 + 3q^2$ is odd, any common divisor of $2p$ and $p^2 + 3q^2$ necessarily divides p and $p^2 + 3q^2$, hence also divides p and $3q^2$. Furthermore, since $3 \nmid p$ this means any common divisor of p and $3q^2$ divides both p and q^2, but these elements are relatively prime.
- Thus, $2p$ and $p^2 + 3q^2$ are relatively prime, so since their product is a cube, each must be a cube up to a unit factor in $\mathbb{Z}$, hence are actually cubes.
- By the lemma, we then have $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$ for some $a, b \in \mathbb{Z}$, and we also know $2p = 2a(a - 3b)(a + 3b)$ is a cube.

Some More Diophantine Equations, XIII

Proof (Case $3 \nmid p$, Finish):

- We have $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$ for some $a, b \in \mathbb{Z}$, and $2p = 2a(a - 3b)(a + 3b)$ is a cube.
- We see that $2a$, $a - 3b$, $a + 3b$ must be pairwise relatively prime, since any common divisor would necessarily divide $2a$ and $6b$ hence divide 6, but a cannot be divisible by 3 (since then p, q would both be divisible by 3) and a, b cannot have the same parity (since then both p, q would be even).
- Therefore, since their product is a cube in $\mathbb{Z}$, each of $2a$, $a - 3b$, and $a + 3b$ must be a cube in $\mathbb{Z}$. But then if $2a = z_1^3$, $a - 3b = x_1^3$, and $a + 3b = y_1^3$, we have $x_1^3 + y_1^3 = z_1^3$, and clearly we also have $0 < |z_1| < |a| < |r| < |z|$.
- We have therefore found a solution to the equation with a smaller value of z, which is a contradiction.

Some More Diophantine Equations, XIV

Proof (Case $3|p$, Start):

- The case $3|p$ is similar: write $p = 3s$ and note q, s are relatively prime of opposite parity with $z^3 = 18s \cdot (3s^2 + q^2)$.
- Since q cannot be divisible by 3 and $3s^2 + q^2$ is odd, any common divisor of $18s$ and $3s^2 + q^2$ must divide s and $3s^2 + q^2$ hence divides s and q^2, but these are relatively prime.
- Thus $18s$ and $3s^2 + q^2$ are relatively prime, so they are each cubes.
- By the lemma again, we have $q = a^3 - 9ab^2$ and $s = 3a^2b - 3b^3$, where $18s = 3^3 \cdot 2b(a-b)(a+b)$ is a perfect cube.

Some More Diophantine Equations, XV

Proof (Case $3|p$, Finish):

- We have $q = a^3 - 9ab^2$ and $s = 3a^2b - 3b^3$, where $18s = 3^3 \cdot 2b(a-b)(a+b)$ is a perfect cube.
- Like before, any common divisor of any pair of $2b$, $a-b$, $a+b$ must divide $2a$ and $2b$ hence divide 2, but a, b must have opposite parity since otherwise q, s would both be even.
- Thus, $2b$, $a-b$, and $a+b$ are all perfect cubes. But then if $a+b = z_1^3$, $a-b = x_1^3$, and $2b = y_1^3$, we have $x_1^3 + y_1^3 = z_1^3$, and clearly we also have $0 < |z_1| = |a+b| < |s| < |z|$.
- We have again found a solution to the equation with a smaller value of z, which is a contradiction. Since we have reached a contradiction in both cases, we are done.

Arithmetic in $\mathcal{O}_{\sqrt{-3}}$, I

As our next application of our study of the quadratic integer rings, we can develop cubic reciprocity using properties of the ring $\mathcal{O}_{\sqrt{-3}}$.

Proposition (Arithmetic in $\mathcal{O}_{\sqrt{-3}}$)

Let π be a prime of $R = \mathcal{O}_{\sqrt{-3}}$ and let $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathcal{O}_{\sqrt{-3}}$ denote a nonreal cube root of unity. 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 $\sqrt{-3}$, the elements 1, ω, and ω^2 are distinct modulo π, and $N(\pi) - 1$ is divisible by 3.*

Arithmetic in $\mathcal{O}_{\sqrt{-3}}$, II

1. The quotient ring $R/(\pi)$ is a finite field with $N(\pi)$ elements.

Proof:

- We showed earlier that R/I is finite for any $I \neq 0$, and it is a field because (π) is prime hence maximal.
- For the statement about the cardinality, if π is associate to $\sqrt{-3}$ then clearly $R/(\pi)$ has 3 residue classes (represented by 0, 1, and 2) and $N(\pi) = 3$.
- If π is associate to a rational prime $p \equiv 2 \pmod 3$ then $R/(p)$ has p^2 elements (per the calculation above) and $N(\pi) = p^2$.
- Finally, if π is one of the two conjugate factors of a rational prime $p \equiv 1 \pmod 3$, then $R/(p) \cong R/(\pi) \times R/(\overline{\pi})$ and since both $R/(\pi)$ and $R/(\overline{\pi})$ are fields (and thus have cardinality greater than 1) and $R/(p)$ has cardinality p^2, we must have $\#(R/(\pi)) = \#(R/(\overline{\pi})) = p = N(\pi)$.

Arithmetic in $\mathcal{O}_{\sqrt{-3}}$, III

2. For any nonzero residue class α modulo π, we have $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.

Proof:

- As shown in (1), the quotient ring $R/(\pi)$ is a finite field with $N(\pi)$ elements. The multiplicative group of this finite field then has $N(\pi) - 1$ elements.
- Hence by Lagrange's theorem, any element in this group (i.e., any nonzero residue class) $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$, as claimed.

Note that this is a generalization of Euler's theorem for $\mathbb{Z}/m\mathbb{Z}$, which says $a^{\varphi m} \equiv 1 \pmod{m}$ for any a relatively prime to m.

Arithmetic in $\mathcal{O}_{\sqrt{-3}}$, IV

3. If π is not associate to $\sqrt{-3}$, the elements 1, ω, and ω^2 are distinct modulo π, and $N(\pi) - 1$ is divisible by 3.

Proof:

- Suppose that $1 \equiv \omega$, $1 \equiv \omega^2$, or $\omega \equiv \omega^2 \pmod{\pi}$.
- Then π necessarily has a nontrivial gcd with $(1 - \omega)(1 - \omega^2) = 3$, so since π is irreducible, it must be an irreducible factor of 3, hence associate to $\sqrt{-3}$.
- Taking the contrapositive shows that if π is not associate to $\sqrt{-3}$, the elements 1, ω, and ω^2 are distinct modulo π.
- The second statement then follows by Lagrange's theorem, since $\{1, \omega, \omega^2\}$ is a subgroup of order 3 of the multiplicative group of residues modulo π. (Alternatively, we could verify it directly using our characterization of the primes in $\mathcal{O}_{\sqrt{-3}}$.)

The Cubic Residue Symbol, I

The idea now is that we can define a cubic residue symbol that will detect cubes modulo π, in a similar way to how we define the quadratic residue symbol modulo p that detects squares.

- For the quadratic residue symbol, the idea is to observe that $a^{p-1} - 1 \equiv 0 \pmod{p}$ by Euler's theorem.
- Thus, when p is odd, we may use the factorization $z^2 - 1 = (z-1)(z+1)$ to factor this expression as $(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \pmod{p}$.
- This tells us that $a^{(p-1)/2} \equiv 1$ or $-1 \pmod{p}$.
- Furthermore, the elements with $a^{(p-1)/2} \equiv 1 \pmod{p}$ will precisely be the squares modulo p: this is exactly the content of Euler's criterion for the Legendre symbol, which says that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

The Cubic Residue Symbol, II

Let's run through the analogous procedure inside $\mathcal{O}_{\sqrt{-3}}/(\pi)$.

- From the proposition, if π is not associate to $\sqrt{-3}$, then $N(\pi) - 1$ is divisible by 3 and $\alpha^{N(\pi)-1} - 1 \equiv 0 \pmod{\pi}$.
- Then we may use the factorization $z^3 - 1 = (z-1)(z-\omega)(z-\omega^2)$ to factor the expression as $(\alpha^{(N(\pi)-1)/3} - 1)(\alpha^{(N(\pi)-1)/3} - \omega)(\alpha^{(N(\pi)-1)/3} - \omega^2) \equiv 0 \pmod{\pi}$.
- Thus, since $\mathcal{O}_{\sqrt{-3}}/(\pi)$ is an integral domain, this means $\alpha^{(N(\pi)-1)/3}$ is congruent to one of 1, ω, ω^2 modulo π.
- Furthermore (as we will show in a moment) the cubes modulo π are precisely the elements with $\alpha^{(N(\pi)-1)/3} \equiv 1 \pmod{\pi}$.

The Cubic Residue Symbol, III

We take the content of this calculation as the 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 $\left[\frac{\alpha}{\pi}\right]_3 \equiv \alpha^{(N(\pi)-1)/3} \pmod{\pi}$.

We showed in the proposition that $1, \omega, \omega^2$ are distinct modulo π, and we showed on the last slide that $\alpha^{(N(\pi)-1)/3}$ is always congruent to one of $1, \omega, \omega^2$ whenever π does not divide α, so the cubic residue symbol is well-defined.

The Cubic Residue Symbol, IV

Here are some properties of the cubic residue symbol:

Proposition (Properties of Cubic Residues)

Let π be a prime element of $\mathcal{O}_{\sqrt{-3}}$ with $N(\pi) \neq 3$, and let $\alpha, \beta \in \mathcal{O}_{\sqrt{-3}}$. Then the following hold:

1. *If $\alpha \equiv \beta \pmod{\pi}$ then $\left[\frac{\alpha}{\pi}\right]_3 = \left[\frac{\beta}{\pi}\right]_3$.*
2. *The cubic residue symbol is multiplicative: $\left[\frac{\alpha\beta}{\pi}\right]_3 = \left[\frac{\alpha}{\pi}\right]_3 \left[\frac{\beta}{\pi}\right]_3$.*
3. *We have $\left[\frac{\overline{\alpha}}{\pi}\right]_3 = \overline{\left[\frac{\alpha}{\pi}\right]_3} = \left[\frac{\alpha}{\pi}\right]_3^2 = \left[\frac{\alpha^2}{\pi}\right]_3$.*
4. *If n is an integer not divisible by π, then $\left[\frac{n}{\pi}\right]_3 = 1$.*
5. *If u is a primitive root modulo π, then $\left[\frac{u}{\pi}\right]_3$ is either ω or ω^2.*
6. *The cubic residue symbol detects cubes: if $\alpha \neq 0 \bmod \pi$, then $\left[\frac{\alpha}{\pi}\right]_3 = 1$ if and only if α is a cubic residue modulo π (which is to say, $\alpha \equiv \beta^3 \pmod{\pi}$ for some β).*

The Cubic Residue Symbol, V

1. If $\alpha \equiv \beta \pmod{\pi}$ then $\left[\frac{\alpha}{\pi}\right]_3 = \left[\frac{\beta}{\pi}\right]_3$.

Proof:

- By definition we have
$$\left[\frac{\alpha}{\pi}\right]_3 \equiv \alpha^{(N(\pi)-1)/3} \equiv \beta^{(N(\pi)-1)/3} \equiv \left[\frac{\beta}{\pi}\right]_3 \pmod{\pi}.$$
- But since the elements $0, 1, \omega, \omega^2$ are distinct modulo π, this congruence actually implies equality: $\left[\frac{\alpha\beta}{\pi}\right]_3 = \left[\frac{\alpha}{\pi}\right]_3 \left[\frac{\beta}{\pi}\right]_3$.

The Cubic Residue Symbol, VI

2. Cubic residue symbols are multiplicative: $\left[\frac{\alpha\beta}{\pi}\right]_3 = \left[\frac{\alpha}{\pi}\right]_3 \left[\frac{\beta}{\pi}\right]_3$.

Proof:

- By definition we have

$$\begin{aligned}\left[\frac{\alpha\beta}{\pi}\right]_3 &\equiv (\alpha\beta)^{(N(\pi)-1)/3} && \pmod{\pi}\\ &\equiv \alpha^{(N(\pi)-1)/3}\beta^{(N(\pi)-1)/3} && \pmod{\pi}\\ &\equiv \left[\frac{\alpha}{\pi}\right]_3 \left[\frac{\beta}{\pi}\right]_3 && \pmod{\pi}\end{aligned}$$

and just as in (1) this congruence implies equality.

The Cubic Residue Symbol, VII

3. We have $\left[\frac{\overline{\alpha}}{\pi}\right]_3 = \overline{\left[\frac{\alpha}{\pi}\right]_3} = \left[\frac{\alpha}{\pi}\right]_3^2 = \left[\frac{\alpha^2}{\pi}\right]_3$.

Proof:

- For the first equality we have $\left[\frac{\overline{\alpha}}{\pi}\right]_3 \equiv \overline{\alpha}^{(N(\pi)-1)/3} \equiv \overline{\alpha^{(N(\pi)-1)/3}} \equiv \overline{\left[\frac{\alpha}{\pi}\right]_3} \pmod{\pi}$ and again as above this congruence implies equality.
- For the second equality we note that each of the possible values $0, 1, \omega, \omega^2$ has the property that its square equals its complex conjugate.
- The third equality follows from multiplicativity of the cubic residue symbol.

The Cubic Residue Symbol, VIII

4. If n is an integer not divisible by π, then $\left[\frac{n}{\pi}\right]_3 = 1$.

Proof:

- By (3) we have $\overline{\left[\frac{n}{\pi}\right]_3} = \left[\frac{\overline{n}}{\pi}\right]_3 = \left[\frac{n}{\pi}\right]_3$ since n is real.
- Since $\left[\frac{n}{\pi}\right]_3 \neq 0$ the only possibility is that $\left[\frac{n}{\pi}\right]_3 = 1$.

The Cubic Residue Symbol, IX

Before I prove the next item, I will first show that $R/(\pi)$ always has a primitive root for any prime π.

Lemma (Multiplicative Groups of Finite Fields)

If G is a multiplicative subgroup of a field F, then G is a cyclic group. In particular, multiplicative groups of finite fields are cyclic.

Since $R/(\pi)$ is a finite field, the lemma implies that its multiplicative group is cyclic. A generator of this cyclic group is called a primitive root modulo π, just as in $\mathbb{Z}$ modulo m.

The Cubic Residue Symbol, X

Proof (of lemma):

- Let M be the maximal order among all elements in G; clearly $M \leq \#G$. If g has order M and h is any other element of order k, then if k does not divide M, there is some prime q which occurs to a higher power q^f in the factorization of k than the corresponding power q^e dividing M.
- Then $g^{q^f} \cdot h^{k/q^e}$ has order $M \cdot q^{f-e}$, which is impossible because this value is greater than M.
- Therefore, the order of every element divides M, so the polynomial $p(x) = x^M - 1$ has $\#G$ roots in $F[x]$.
- But by unique factorization in $F[x]$, this is impossible unless $M \geq \#G$, since a polynomial of degree M can have at most M roots in $F[x]$.
- Thus, $M = \#G$, so some element has order $\#G$ so G is cyclic.

The Cubic Residue Symbol, XI

5. If u is a primitive root modulo π (i.e., an element of order $N(\pi)-1$ modulo π), then $\left[\frac{u}{\pi}\right]_3$ is either ω or ω^2 (i.e., it cannot equal 1).

Proof:

- Observe that $\left[\frac{u}{\pi}\right]_3 = u^{(N(\pi)-1)/3}$ cannot be congruent to 1 modulo π since this would mean that the order of u would be at most $(N(\pi)-1)/3$, contradicting the assumption that its order is $N(\pi)-1$.
- Thus, since π cannot divide u, $\left[\frac{u}{\pi}\right]_3$ is either ω or ω^2, as claimed.

The Cubic Residue Symbol, XII

6. The cubic residue symbol detects cubes: if $\alpha \neq 0 \bmod \pi$, then $\left[\frac{\alpha}{\pi}\right]_3 = 1$ if and only if α is a cubic residue modulo π (which is to say, $\alpha \equiv \beta^3 \pmod{\pi}$ for some β).

Proof:

- Let u be a primitive root modulo π and write $\alpha = u^k$ for some integer k. Then by (4), since $\left[\frac{\alpha}{\pi}\right]_3 = \left[\frac{u^k}{\pi}\right]_3 = \left[\frac{u}{\pi}\right]_3^k$, and $\left[\frac{u}{\pi}\right]_3$ is either ω or ω^2, we see that that $\left[\frac{\alpha}{\pi}\right]_3 = 1$ if and only if k is a multiple of 3.
- But this condition is easily seen to be equivalent to saying that α is a cubic residue: if $\alpha \equiv \beta^3$ then if $\beta = u^r$ we have $\alpha = u^{3r}$, and conversely if k is a multiple of 3 then $\alpha \equiv (u^{k/3})^3$.

The Cubic Residue Symbol, XIII

Example: Determine whether $2+\sqrt{-3}$ and $2\sqrt{-3}$ are cubic residues modulo $\pi = 5$ inside $\mathcal{O}_{\sqrt{-3}}$.

The Cubic Residue Symbol, XIII

Example: Determine whether $2+\sqrt{-3}$ and $2\sqrt{-3}$ are cubic residues modulo $\pi = 5$ inside $\mathcal{O}_{\sqrt{-3}}$.

- Since $N(\pi) = 25$, for $2+\sqrt{-3}$ we must calculate the cubic residue symbol $\left[\frac{2+\sqrt{-3}}{5}\right]_3 \equiv (2+\sqrt{-3})^{(25-1)/3} \equiv (2+\sqrt{-3})^8 \equiv 2+3\sqrt{-3} \pmod 5$.
- Since $\omega = \frac{-1+\sqrt{3}}{2} \equiv 2+3\sqrt{-3} \pmod 5$, we see $\left[\frac{2+\sqrt{-3}}{5}\right]_3 = \omega$, so $2+\sqrt{-3}$ is not a cubic residue mod 5.
- For $2\sqrt{-3}$ we calculate $\left[\frac{2\sqrt{-3}}{5}\right]_3 \equiv (2\sqrt{-3})^8 \equiv 1 \pmod 5$. Thus, $\left[\frac{2\sqrt{-3}}{5}\right]_3 = 1$ and so $2\sqrt{-3}$ is a cubic residue mod 5.

The Cubic Residue Symbol, XIV

In order to handle the situation of associates in $\mathcal{O}_{\sqrt{-3}}$, we select a unique associate for each prime:

Definition

If π is a prime in $\mathcal{O}_{\sqrt{-3}}$, we say π is primary if $\pi \equiv 2 \pmod 3$. Equivalently, if $\pi = a + b\omega$, then π is primary when $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$.

Examples:

- The primes 2 and $\dfrac{7 + 3\sqrt{-3}}{2} = 5 + 3\omega$ are primary.
- The prime $4 + \sqrt{-3} = 5 + 2\omega$ is not primary.

The Cubic Residue Symbol, XV

It is straightforward to see that if π is not associate to $\sqrt{-3}$, then exactly one associate of π is primary.

- Explicitly, if $\pi = a + b\omega$ then the associates of π are
  $\pi = a + b\omega$,
  $-\pi = (-a) + (-b)\omega$,
  $\omega\pi = (-b) + (a - b)\omega$,
  $-\omega\pi = b + (b - a)\omega$,
  $\omega^2\pi = (b - a) + (-a)\omega$, and
  $-\omega^2\pi = (a - b) + a\omega$.
- One may then check that exactly one of b, $a - b$, a is divisible by 3, so two of the associates will have ω-coefficient divisible by 3, and then exactly one will have its coefficient of 1 congruent to 2 modulo 3.

Cubic Reciprocity, I

We can now state cubic reciprocity in full:

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.

Summary

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

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

Next lecture: Quartic reciprocity.