

MATH 361: NUMBER THEORY — TWELFTH LECTURE

Let

$$\omega = \zeta_3 = e^{2\pi i/3} = \frac{-1 + \sqrt{-3}}{2}.$$

The subjects of this lecture are the arithmetic of the ring

$$D = \mathbf{Z}[\omega],$$

and the cubic reciprocity law.

1. UNIQUE FACTORIZATION

The ring D is Euclidean with norm function

$$N : D \longrightarrow \mathbf{Z}_{\geq 0}, \quad Nz = z\bar{z}, \quad N(a + b\omega) = a^2 - ab + b^2.$$

Hence D is a PID and consequently a UFD. That is, every nonzero $z \in D$ takes the form

$$z = u \prod_{i=1}^g \pi_i^{e_i}, \quad u \in D^\times, \text{ each } \pi_i \text{ irreducible, each } e_i \in \mathbf{Z}^+,$$

and if also $z = \tilde{u} \prod_{i=1}^{\tilde{g}} \tilde{\pi}_i^{\tilde{e}_i}$ then $\tilde{g} = g$ and after indexing we may take each $\tilde{\pi}_i = u_i \pi_i$ with $u_i \in D^\times$ (that is, $\tilde{\pi}_i$ and π_i are *associate*) and $\tilde{e}_i = e_i$.

2. UNITS

Only 0_D has norm 0. For any nonzero $u \in D$, we have the equivalence

$$u \in D^\times \iff Nu = 1.$$

(\iff is immediate since if $u\bar{u} = 1$ then u has inverse \bar{u} ; \implies is also immediate since if $u \in D^\times$ then $Nu = (Nu^{-1})^{-1}$ is both a positive integer and a reciprocal positive integer, so it is 1.) The equivalence shows that

$$D^\times = \{\pm 1, \pm\omega, \pm\omega^2\} = \langle \zeta_6 \rangle.$$

Structurally, $D^\times \cong \mathbf{Z}/6\mathbf{Z}$, with generators $\zeta_6 = -\omega^2$ and $\zeta_6^{-1} = -\omega$.

3. IRREDUCIBLES (NONZERO PRIMES)

Let $\pi \in D$ be irreducible. Then $\pi \mid \pi\bar{\pi} = N\pi \in \mathbf{Z}_{>1}$. Thus (since π is prime) $\pi \mid p$ for at least one rational prime p . If also $\pi \mid q$ for a different rational prime q then consequently $\pi \mid 1$, a false statement. So in fact

$$\pi \mid p \quad \text{for a unique rational prime } p.$$

(The result just displayed can also be established by working with ideals, as follows. Since πD is a prime ideal of D , $\pi D \cap \mathbf{Z}$ is a prime ideal of \mathbf{Z} , nonzero since it contains $\pi\bar{\pi}$. Thus $\pi D \cap \mathbf{Z} = p\mathbf{Z}$ for some rational prime p . Since $p\mathbf{Z} \subset \pi D$, also $pD \subset \pi D$, showing that $\pi \mid p$. If also $\pi \mid q$ for a different rational prime q then consequently $qD \subset \pi D$ and thus $1 \in \pi D$, leading to the false statement that π is a unit.)

Note: If $\bar{\pi} \mid q$ then $\pi \mid \bar{q} = q$, showing that $q = p$. Thus $N\pi = \pi\bar{\pi}$ is a power of p . Let the letter f denote the relevant power. That is, define f by the formula

$$\boxed{N\pi = p^f.}$$

4. FACTORIZATION OF RATIONAL PRIMES

Since each irreducible π is a factor of a unique rational prime p , the question now is how rational primes factor in D . The factorization of any rational prime p is

$$p = u \prod_{i=1}^g \pi_i^{e_i}, \quad u \in D^\times, N\pi_i = p^{f_i} \text{ for each } i.$$

It follows that

$$p^2 = Np = N \left(u \prod_{i=1}^g \pi_i^{e_i} \right) = 1 \cdot \prod_{i=1}^g (p^{f_i})^{e_i} = \prod_{i=1}^g p^{e_i f_i} = p^{\sum_{i=1}^g e_i f_i}.$$

Therefore, the positive integers e_i , f_i , and g satisfy the relation

$$\sum_{i=1}^g e_i f_i = 2.$$

There are three possibilities.

- p **splits**: $g = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$. Here we have $p = u\pi_1\pi_2$ where $N\pi_1 = N\pi_2 = p$, so that in fact

$$p = \pi\bar{\pi} \quad \text{and } \pi, \bar{\pi} \text{ are nonassociate.}$$

- p is **inert**: $g = 1$, $e = 1$, $f = 2$. Here we have $p = u\pi$ where $N\pi = p^2$, so that

$$p \text{ is irreducible in } D.$$

- p **ramifies**: $g = 1$, $e = 2$, $f = 1$. Here we have $p = u\pi^2$ where $N\pi = p$, so that

$$p = \pi\bar{\pi} \quad \text{and } \pi, \bar{\pi} \text{ are associate.}$$

The next question is: *Which rational primes p split, which are inert, and which ramify?*

- *The prime $p = 3$ ramifies.* Specifically,

$$3 = -\omega^2\lambda^2 \quad \text{where } \boxed{\lambda = 1 - \omega}.$$

This was a homework problem. To see where the factorization comes from, set $X = 1$ in the relation $X^2 + X + 1 = (X - \omega^2)(X - \omega)$ to get

$$3 = (1 - \omega^2)(1 - \omega) = (1 + \omega)(1 - \omega)^2 = -\omega^2\lambda^2.$$

- *The prime $p = 3$ is the only prime that ramifies.* If p ramifies then $p = \pi\bar{\pi}$ with $\pi/\bar{\pi} \in D^\times$. After replacing π by $\omega\pi$ or $\omega^2\pi$ if necessary, we may assume that $\pi/\bar{\pi} = \pm 1$, and hence $\pi^2 = \pm p$. Let $\pi = a + b\omega$ (with $b \neq 0$), so that $\pi^2 = (a^2 - b^2) + (2ab - b^2)\omega$. Since $\pi^2 = \pm p$ and $b \neq 0$, necessarily $b = 2a$. Thus $N\pi = a^2 - ab + b^2$ equals $3a^2$. Thus $p = 3$, and furthermore $\pi = \pm(1 + 2\omega) = \pm\omega(\omega^2 + 2) = \pm\omega(1 - \omega) = \pm\omega\lambda$.

- *If $p \equiv 1 \pmod{3}$ then p splits.* Indeed, the character group $\widehat{\mathbf{F}_p^\times}$ contains an element χ of order 3. Note that $\chi(\mathbf{F}_p^\times) \subset D^\times$. Let $\pi = J(\chi, \chi) \in D$. By the table of Jacobi sum values, $N\pi = p$. So p is not inert. Nor does it ramify, so the remaining possibility is that it splits.
- *If $p \equiv 2 \pmod{3}$ then p is inert.* We show this by contraposition. If p is not inert then $p = N\pi$ for some π , i.e., $p = a^2 - ab + b^2$ for some a and b . So $4p = (2a - b)^2 + 3b^2$ for some a and b , so that p is a square modulo 3. Thus $p \not\equiv 2 \pmod{3}$. Note:

From now on we use the symbol q to denote a $2 \pmod{3}$ prime.

In sum, we have shown that the Legendre symbol $(\cdot/3)$ describes factorization in D ,

$$\begin{aligned} p \text{ splits} &\iff (p/3) = 1, \\ p \text{ is inert} &\iff (p/3) = -1, \\ p \text{ ramifies} &\iff (p/3) = 0. \end{aligned}$$

5. CANONICAL REPRESENTATIVE OF EACH ASSOCIATE CLASSES

Each irreducible in D is one of six associates. We now specify one associate from each class of six.

As before, we specify $\lambda = 1 - \omega$ among the irreducibles that divide 3.

For any rational prime $p \neq 3$, each divisor π of p has a so-called **primary associate**, meaning the associate π' such that

$$\pi' \equiv 2 \pmod{3}.$$

That is,

$$\pi' = a + b\omega, \quad a \equiv 2 \pmod{3}, \quad b \equiv 0 \pmod{3}.$$

Indeed, if π divides a rational prime $q \equiv 2 \pmod{3}$ then its primary associate is simply q . Otherwise, π divides a rational prime $p \equiv 1 \pmod{3}$ and $N\pi = p$. The first part of the proof of 9.3.5 in Ireland and Rosen shows that π has a primary associate. (It may help to modify the wording after (a)–(f) to say, *we may assume (after replacing $a + b\omega$ by an associate if necessary) that $3 \nmid a \dots$*) In both cases, the second part of the proof of Ireland and Rosen 9.3.5 shows that the primary associate is unique.

Given a rational prime $p \equiv 1 \pmod{3}$, to find a primary prime π lying over p , proceed as follows. We know that $\pi = a + b\omega$ where $a \equiv 2 \pmod{3}$ and $b \equiv 0 \pmod{3}$, and we want to find a and b . Since $p = N\pi = a^2 - ab + b^2$, it follows that $4p = (2a - b)^2 + 3b^2$. The procedure is to find A and B such that $4p = A^2 + 27B^2$ and $A \equiv 1 \pmod{3}$ (note that A and B must have the same parity; also note that we have two choices for B , leading to the two primary primes π and $\bar{\pi}$ lying over p) and then set $b = 3B$ (which has the same parity as B , hence the same parity as A , and independently of the parity we have $A + b \equiv 4 \pmod{6}$), and finally $a = (A + b)/2$, which is $2 \pmod{3}$. Note that this is exactly the procedure described in Gauss's Theorem about the solution-count of the equation $x^3 + y^3 = 1$ modulo p .

For example, let $p = 103$, so that $4p = 412$. The values $27B^2$ are 27, 108, 243, 432, \dots . Since $412 - 243 = 169$, we have $A = 13$ and $B = \pm 3$. Thus $b = \pm 9$ and then $a = (A + b)/2$ is correspondingly 11 or 2. In sum, the primary primes lying over $p = 103$ are $\{\pi, \bar{\pi}\} = \{11 + 9\omega, 2 - 9\omega\}$.

6. THE RESIDUE FIELD $D/\pi D$

For each irreducible $\pi \in D$, the ideal πD is maximal, and so the quotient ring $D/\pi D$ is a field. The fact that πD is maximal follows from π being irreducible since for any ideal gD of D ,

$$\pi D \subset gD \implies g \mid \pi \implies g \sim \pi \text{ or } g \in D^\times \implies gD = \pi D \text{ or } gD = D.$$

The fact that the quotient of a commutative ring with 1 by a maximal ideal yields a field is a basic fact of algebra, essentially a rephrasing of the definition of maximal ideal. Indeed, let R be such a ring and let M be a maximal ideal of R ; if $a + M \neq M$ in R/M then $(a, M) = R$, so $ar + m = 1$ for some $r \in R$ and $m \in M$, and thus $(a + M)(r + M) = 1 + M$, i.e., $a + M$ is invertible in R/M .

Also, we can show that $D/\pi D$ is a field by using the special circumstance of the Euclidean property of D : If $z \in D - \pi D$ then $(z, \pi) = 1$, and so $xz + y\pi = 1$ for some $x, y \in D$, showing that $xz = 1 \pmod{\pi}$.

Recall that $\pi D \cap \mathbf{Z} = p\mathbf{Z}$ where $\pi \mid p$. It follows that the composition

$$\mathbf{Z} \longrightarrow D \longrightarrow D/\pi D$$

induces an injection

$$\mathbf{Z}/p\mathbf{Z} \hookrightarrow D/\pi D.$$

We view the injection as a containment, i.e., we identify $\mathbf{Z}/p\mathbf{Z}$ with its image in $D/\pi D$.

Now assume that π is primary.

- If $\pi = q = 2 \pmod{3}$ then

$$D/qD \cong \{x + y\omega : x, y \in \{0, \dots, q-1\}\}$$

and so

$$|D/\pi D| = |D/qD| = q^2 = Nq = N\pi.$$

- If $\pi = \lambda = 1 - \omega$ then for any $x, y \in \mathbf{Z}$, $x + y\omega \equiv_\lambda x + y \equiv_\lambda x + y \pmod{3}$, and so we have an injection

$$D/\lambda D \hookrightarrow \mathbf{Z}/3\mathbf{Z}.$$

Along with the opposite injection from before, this shows that

$$D/\lambda D \cong \mathbf{Z}/3\mathbf{Z}$$

and so

$$|D/\lambda D| = |\mathbf{Z}/3\mathbf{Z}| = 3 = N\lambda.$$

- If $\pi \mid p$ where $p = 1 \pmod{3}$ then $\pi = a + b\omega$ with $p = a^2 - ab + b^2$. Note that $p \nmid b$, because otherwise $\pi \mid b$ and so also $\pi \mid \pi - b\omega = a$ since $a = \pi - b\omega$, so that $p \mid a$ and thus $p \mid a + b\omega = \pi$, contradicting the fact that p splits in D .

Now for any $x + y\omega \in D$, let $c = yb^{-1} \pmod{p}$, so that $p \mid y - bc$. Then the difference $x + y\omega - c\pi = x + y\omega - c(a + b\omega)$ takes the form $x' + py'\omega$. Consequently, $x + y\omega = x' \pmod{\pi D}$ where $x' \in \mathbf{Z}$. We may further translate x' freely by multiples of p , so that as in the ramified case, $D/\pi D \hookrightarrow \mathbf{Z}/p\mathbf{Z}$ and thus

$$D/\pi D \cong \mathbf{Z}/p\mathbf{Z}$$

and

$$|D/\pi D| = |\mathbf{Z}/p\mathbf{Z}| = p = N\pi.$$

In sum,

$$\boxed{|D/\pi D| = N\pi = p^f \text{ in all cases.}}$$

The formula $\sum_{i=1}^g e_i f_i = 2$ shows that for any rational prime p , the *decomposition* (the number g of nonassociate irreducible factors of p), the *ramification* (the powers e_i of the factors in the factorization of p), and the *inertia* (the dimension of $D/\pi D$ over $\mathbf{Z}/p\mathbf{Z}$) always sum to 2, the dimension of $\mathbf{Q}(\omega)$ as a vectors space over \mathbf{Q} .

7. THE CUBIC CHARACTER

Continuing to work in D , let π be a primary prime, $\pi \neq \lambda$. (Recall that $\lambda = 1 - \omega$ divides 3.) We want a cubic character modulo π ,

$$\chi_\pi : (D/\pi D)^\times \longrightarrow \{1, \omega, \omega^2\},$$

akin to the quadratic character $(\cdot/p) : (\mathbf{Z}/p\mathbf{Z})^\times \longrightarrow \{\pm 1\}$.

To define χ_π , first note that $(D/\pi D)^\times$ is cyclic of order $N\pi - 1$. If $\pi \equiv 1 \pmod 3$ then $N\pi - 1 \equiv 0 \pmod 3$, while if $\pi \equiv 2 \pmod 3$ then $N\pi - 1 \equiv 1 \pmod 3$. Thus $N\pi - 1 \equiv 0 \pmod 3$ in all cases. Consequently $3 \mid |(D/\pi D)^\times|$, and so $(D/\pi D)^\times$ contains three cube roots of unity. Specifically, they are $\{1, g^{(N\pi-1)/3}, g^{2(N\pi-1)/3}\}$ where g generates $(D/\pi D)^\times$. Next we establish that:

These three cube roots of unity are $\{1 + \pi D, \omega + \pi D, \omega^2 + \pi D\}$.

Since each of $1, \omega, \omega^2$ cubes to 1 in D , certainly the three elements in the display cube to 1 in $D/\pi D$. What needs to be shown is that they are distinct. But indeed they are, because $1 - \omega = \lambda$ and $\omega - \omega^2 = \omega\lambda$ and $1 - \omega^2 = (1 + \omega)(1 - \omega)$ are all associates of λ , and so they are not divisible by π .

For all $a \in D - \pi D$, the relation

$$a^{N\pi-1} = 1 \pmod \pi$$

shows that

$$a^{(N\pi-1)/3} + \pi D \in \{1 + \pi D, \omega + \pi D, \omega^2 + \pi D\}.$$

Now we can define the cubic character.

Definition 7.1. Let $\pi \in D$ be a primary prime, $\pi \neq \lambda$. The **cubic character modulo π** is

$$\chi_\pi : (D/\pi D)^\times \longrightarrow \{1, \omega, \omega^2\},$$

defined by the condition

$$\chi_\pi(\alpha) = a^{(N\pi-1)/3} \pmod \pi \quad \text{for any } a \in D \text{ such that } \alpha = a + \pi D.$$

The formula for χ_π can be rewritten in various ways. For example,

$$\chi_\pi(\alpha) + \pi D = \alpha^{(N\pi-1)/3}, \quad \chi_\pi(\alpha) \in \{1, \omega, \omega^2\},$$

or

$$\chi_\pi(a + \pi D) = a^{(N\pi-1)/3} \pmod \pi, \quad \chi_\pi(a + \pi D) \in \{1, \omega, \omega^2\}.$$

In practice, after one has some experience working in this environment, one adopts notation that is less fussy about distinguishing elements a of $D - \pi D$ from their equivalence classes $\alpha = a + \pi D$ in $(D/\pi D)^\times$. In fact, one often refers to the composite map

$$D - \pi D \longrightarrow (D/\pi D)^\times \xrightarrow{\chi_\pi} \{1, \omega, \omega^2\}$$

as χ_π also. This version of χ_π is defined by the condition

$$\chi_\pi(a) = a^{(N\pi-1)/3} \pmod \pi, \quad \chi_\pi(a) \in \{1, \omega, \omega^2\}.$$

The various cubic character formulas are all analogous to Euler's identity

$$(a/p) = a^{(p-1)/2} \pmod p \quad \text{for } a \in \mathbf{Z} \text{ such that } p \nmid a,$$

but now the same idea is being used to *define* the cubic character. Note that since $a \in \mathbf{Z}$ here, it is the last version of the cubic character formula that most closely parallels Euler's identity.

Proposition 7.2 (Properties of the Cubic Character). *Let $\pi \in D$ be a primary prime, $\pi \neq \lambda$. Then*

(a) *For all $\alpha \in D - \pi D$,*

$$\chi_\pi(\alpha) = 1 \iff \alpha \text{ is a cube modulo } \pi.$$

(b) *For all $\alpha, \beta \in D - \pi D$,*

$$\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta).$$

That is, χ_π is a homomorphism.

(c) *For all $\alpha \in D - \pi D$,*

$$\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha^2) = \chi_{\overline{\pi}}(\overline{\alpha}).$$

(d) *If $\pi = q = 2 \pmod 3$ then for all $\alpha \in D - \pi D$,*

$$\overline{\chi_\pi(\alpha)} = \chi_\pi(\overline{\alpha}),$$

and so in particular,

$$\chi_\pi(n) = 1 \quad \text{for all } n \in \mathbf{Z} - q\mathbf{Z}.$$

Proof. (a) Let g generate $(D/\pi D)^\times$. For any $\alpha \in D - \pi D$, let $\alpha + \pi D = g^e$ and compute that

$$\begin{aligned} \chi_\pi(\alpha) = 1 &\iff \alpha^{(N\pi-1)/3} = 1 \pmod \pi \\ &\iff g^{e(N\pi-1)/3} = 1 \\ &\iff N\pi - 1 \mid e(N\pi - 1)/3 \\ &\iff 3 \mid e \\ &\iff \alpha \text{ is a cube modulo } \pi. \end{aligned}$$

(b) For any $\alpha, \beta \in D - \pi D$, compute, working modulo π , that

$$\chi_\pi(\alpha\beta) = (\alpha\beta)^{(N\pi-1)/3} = \alpha^{(N\pi-1)/3}\beta^{(N\pi-1)/3} = \chi_\pi(\alpha)\chi_\pi(\beta).$$

Since the values at the beginning and the end of the display agree modulo π and both lie in $\{1, \omega, \omega^2\}$, they are truly equal.

(c) For any $\alpha \in D - \pi D$, compute that

$$\begin{aligned} \overline{\chi_\pi(\alpha)} &= \chi_\pi(\alpha)^2 \quad \text{since } \chi_\pi(\alpha) \in \{1, \omega, \omega^2\} \\ &= \chi_\pi(\alpha^2) \quad \text{since } \chi_\pi \text{ is a homomorphism.} \end{aligned}$$

Compute also, working modulo π , that

$$\overline{\chi_\pi(\alpha)} = \overline{\alpha^{(N\pi-1)/3}} = \overline{\alpha}^{(N\pi-1)/3} = \chi_{\overline{\pi}}(\overline{\alpha}),$$

and since the values at the beginning and the end of the display agree modulo π and both lie in $\{1, \omega, \omega^2\}$, they are truly equal.

(d) The first part of (d) follows from (c), and the second part of (d) follows from the first. The second part of (d) is clear anyway since $3 \nmid |(\mathbf{Z}/q\mathbf{Z})^\times| = q - 1$, and so the cubing map is an automorphism of $(\mathbf{Z}/q\mathbf{Z})^\times$. \square

8. CUBIC RECIPROCITY

Theorem 8.1 (Cubic Reciprocity). *The main law of cubic reciprocity is:*

Let π and π' be primary primes in D , neither of them λ . Assume that $N\pi \neq N\pi'$, so that π and π' lie over different rational primes p and p' , neither of them 3. Then

$$\chi_\pi(\pi') = \chi_{\pi'}(\pi).$$

The auxiliary laws of cubic reciprocity are:

$$\chi_\pi(\lambda) = \omega^{2m} \quad \text{where } \pi = 3m - 1 + b\omega$$

and

$$\chi_\pi(-1) = 1$$

and

$$\chi_\pi(\omega) = \begin{cases} 1 & \text{if } N\pi = 1 \pmod{9}, \\ \omega & \text{if } N\pi = 4 \pmod{9}, \\ \omega^2 & \text{if } N\pi = 7 \pmod{9}. \end{cases}$$

The first auxiliary law is exercises 9.24–9.26 in Ireland and Rosen. The second auxiliary law holds because -1 is a cube. The third auxiliary law follows from the definition $\chi_\pi(\omega) = \omega^{(N\pi-1)/3}$.

A review of the proof of quadratic reciprocity will clarify the proof of cubic reciprocity. Let p and q be distinct odd primes. Recall the square of the Gauss sum for the quadratic character modulo p ,

$$\tau((\cdot/p))^2 = p^* \quad \text{where } p^* = (-1)^{(p-1)/2}p = (-1/p)p.$$

Compute, working modulo q in $\overline{\mathbf{Z}}$ and noting that $(\cdot/p)^q = (\cdot/p)$ since q is odd, that on the one hand,

$$\begin{aligned} \tau((\cdot/p))^{q+1} &= \tau((\cdot/p))\tau((\cdot/p))^q = \tau((\cdot/p)) \sum_{t \in \mathbf{F}_p^\times} (q^2t/p)^q \zeta_p^{qt} = \tau((\cdot/p))^2 (q/p) \\ &= p^*(q/p), \end{aligned}$$

and on the other, still working modulo q in $\overline{\mathbf{Z}}$,

$$\begin{aligned} \tau((\cdot/p))^{q+1} &= \tau((\cdot/p))^2 (\tau(\cdot/p))^2 (q-1)/2 = p^*(p^*)^{(q-1)/2} \\ &= p^*(p^*/q). \end{aligned}$$

So

$$p^*(p^*/q) = p^*(q/p) \pmod{q} \quad \text{in } \overline{\mathbf{Z}},$$

and therefore

$$p^*(p^*/q) = p^*(q/p) \pmod{q} \quad \text{in } \mathbf{Z},$$

and therefore, since p^* is invertible modulo q ,

$$(p^*/q) = (q/p) \pmod{q} \quad \text{in } \mathbf{Z},$$

and therefore

$$(p^*/q) = (q/p).$$

The crucial fact here was $\tau(\chi_p)^2 = p^*$.

To prepare for the proof of cubic reciprocity, we establish an analogous identity. Let $\pi \in D$ be a nonrational primary prime, so that $N\pi = p = 1 \pmod 3$. Consider the Jacobi sum

$$J = J(\chi_\pi, \chi_\pi) = \frac{\tau(\chi_\pi)^2}{\tau(\overline{\chi_\pi})} = \frac{\tau(\chi_\pi)^3}{\tau(\overline{\chi_\pi})\tau(\chi_\pi)} = \frac{\tau(\chi_\pi)^3}{\chi_\pi(-1)p} = \frac{\tau(\chi_\pi)^3}{p}.$$

Since the Gauss sum has norm p , the Jacobi sum has norm $N(J) = p$, and so J is associate to π . Furthermore, working modulo 3,

$$J = pJ = \tau(\chi_\pi)^3 = \sum_{t \in \mathbf{F}_p^\times} \chi_\pi(t)^3 \zeta_p^{3t} = \sum_{t \in \mathbf{F}_p^\times} \zeta_p^{3t} = -1 = 2.$$

That is, J is primary. Therefore $J = \pi$ and so

$$\boxed{\tau(\chi_\pi)^3 = p\pi.}$$

We now use the boxed relation to prove the main law of cubic reciprocity.

Proof. First consider the case where q and q' are distinct rational primes, both congruent to 2 modulo 3. Then by Proposition 7.2(d),

$$\chi_q(q') = 1 = \chi_{q'}(q).$$

Next consider the case where π and q are distinct primary primes in D . Thus $\pi \notin \mathbf{Z}$ and $N\pi = p = 1 \pmod 3$ and the cubic character χ_π is defined on $(D/\pi D)^\times \cong (\mathbf{Z}/p\mathbf{Z})^\times$, while on the other hand $q \in \mathbf{Z}$ and $q = 2 \pmod 3$. Recall that $\tau(\chi_\pi)^3 = p\pi$. Compute, working modulo q in $\overline{\mathbf{Z}}$ and noting that $\chi_\pi^{q^2} = \chi_\pi$ since $q^2 = 1 \pmod 3$, that on the one hand,

$$\begin{aligned} \tau(\chi_\pi)^{q^2+2} &= \tau(\chi_\pi)^2 \tau(\chi_\pi)^{q^2} = \tau(\chi_\pi)^2 \sum_{t \in \mathbf{F}_p^\times} \chi_\pi(q^3 t)^{q^2} \zeta_p^{q^2 t} = \tau(\chi_\pi)^3 \chi_\pi(q) \\ &= p\pi \chi_\pi(q), \end{aligned}$$

and on the other, still working modulo q in $\overline{\mathbf{Z}}$,

$$\begin{aligned} \tau(\chi_\pi)^{q^2+2} &= \tau(\chi_\pi)^3 (\tau(\chi_\pi)^3)^{(q^2-1)/3} = p\pi (p\pi)^{(q^2-1)/3} = p\pi \chi_q(p\pi) \\ &= p\pi \chi_q(\pi). \end{aligned}$$

So

$$p\pi \chi_\pi(q) = p\pi \chi_q(\pi) \pmod q \quad \text{in } \overline{\mathbf{Z}},$$

and therefore

$$p\pi \chi_\pi(q) = p\pi \chi_q(\pi) \pmod q \quad \text{in } D,$$

and therefore, since $p\pi$ is invertible modulo q in D ,

$$\chi_\pi(q) = \chi_q(\pi) \pmod q \quad \text{in } D,$$

and therefore

$$\chi_\pi(q) = \chi_q(\pi).$$

Finally consider the case where π and π' are distinct primary primes in D . Thus $N\pi = p$ with $p = 1 \pmod 3$ and similarly for π' . Compute, working modulo π' in $\overline{\mathbf{Z}}$

and noting that $\chi_\pi^{p'} = \chi_\pi$ since $p' \equiv 1 \pmod 3$, that on the one hand,

$$\begin{aligned} \tau(\chi_\pi)^{p'+2} &= \tau(\chi_\pi)^2 \tau(\chi_\pi)^{p'} = \tau(\chi_\pi)^2 \sum_{t \in \mathbf{F}_p^\times} \chi_\pi(p'^3 t)^{p'} \zeta_p^{p' t} = \tau(\chi_\pi)^3 \chi_\pi(p'^2) \\ &= p\pi \chi_\pi(p'^2), \end{aligned}$$

and on the other, still working modulo π' in $\overline{\mathbf{Z}}$,

$$\begin{aligned} \tau(\chi_\pi)^{p'+2} &= \tau(\chi_\pi)^3 (\tau(\chi_\pi)^3)^{(p'-1)/3} = p\pi(p\pi)^{(N\pi'-1)/3} \\ &= p\pi \chi_{\pi'}(p\pi). \end{aligned}$$

So as twice before,

$$\chi_\pi(p'^2) = \chi_{\pi'}(p\pi).$$

By symmetry, also

$$\chi_\pi(p'\pi') = \chi_{\pi'}(p^2).$$

The product of the previous two left sides is the product of the previous two right sides, completing the proof of the third case,

$$\chi_\pi(\pi') = \chi_{\pi'}(\pi).$$

□

9. EXAMPLES

Recall the process to find a primary prime π lying over a given rational prime $p \equiv 1 \pmod 3$: Find A and B such that $4p = A^2 + 27B^2$ and $A \equiv 1 \pmod 3$, and then set $b = 3B$ and finally $a = (A + b)/2$. For instance,

$$\begin{aligned} 43 &= \pi\bar{\pi}, & \pi &= -1 + 6\omega, & \bar{\pi} &= -7 - 6\omega, & \mathbf{Z}/43\mathbf{Z} &\cong D/\pi D, \\ 37 &= \rho\bar{\rho}, & \rho &= -4 + 3\omega, & \bar{\rho} &= -7 - 3\omega, & \mathbf{Z}/37\mathbf{Z} &\cong D/\rho D, \\ 19 &= \sigma\bar{\sigma}, & \sigma &= 5 + 3\omega, & \bar{\sigma} &= 2 - 3\omega, & \mathbf{Z}/19\mathbf{Z} &\cong D/\sigma D, \\ 7 &= \tau\bar{\tau}, & \tau &= 2 + 3\omega, & \bar{\tau} &= -1 - 3\omega, & \mathbf{Z}/7\mathbf{Z} &\cong D/\tau D, \\ 103 &= \nu\bar{\nu}, & \nu &= 11 + 9\omega, & \bar{\nu} &= 2 - 9\omega, & \mathbf{Z}/103\mathbf{Z} &\cong D/\nu D. \end{aligned}$$

So, for example:

- *Is 19 a cube modulo 41?* Since $41 \equiv 2 \pmod 3$, *yes*: $3 \nmid 41 - 1$ and so the cubing map is an automorphism of $(\mathbf{Z}/41\mathbf{Z})^\times$. Alternatively, by Proposition 7.2(d), $\chi_{41}(19) = 1$.
- *Is 19 a cube modulo 43?* Since $\mathbf{Z}/43\mathbf{Z} \cong D/\pi D$, the question is whether $\chi_\pi(19) = 1$. Compute that

$$\begin{aligned} \chi_\pi(19) &= \chi_\pi(\sigma\bar{\sigma}) && \text{since } 19 = \sigma\bar{\sigma} \\ &= \chi_\pi(\sigma)\chi_\pi(\bar{\sigma}) && \text{since } \chi_\pi \text{ is a homomorphism} \\ &= \chi_\sigma(\pi)\chi_{\bar{\sigma}}(\pi) && \text{by cubic reciprocity} \\ &= \chi_\sigma(8)\chi_{\bar{\sigma}}(3) && \text{since } \pi \equiv 8 \pmod \sigma \text{ and } \pi \equiv 3 \pmod{\bar{\sigma}} \\ &= \chi_{\bar{\sigma}}(3) && \text{since } 8 \text{ is a cube} \\ &= \chi_{\bar{\sigma}}(-1)\chi_{\bar{\sigma}}(\omega)^2\chi_{\bar{\sigma}}(\lambda)^2 && \text{since } 3 = -\omega^2\lambda^2 \text{ and } \chi_{\bar{\sigma}} \text{ is a homomorphism.} \end{aligned}$$

The auxiliary laws give $\chi_{\bar{\sigma}}(-1) = 1$ and $\chi_{\bar{\sigma}}(\omega) = 1$ (since $N\bar{\sigma} = 19 = 1 \pmod{9}$). Also, $\chi_{\bar{\sigma}}(\lambda) = \omega^{2m}$ where $\bar{\sigma} = 3m - 1 + b\omega$. Since $\bar{\sigma} = 2 - 3\omega$ we have $m = 1$ and hence $\chi_{\bar{\sigma}}(\lambda) = \omega^2$. In sum,

$$\chi_{\pi}(19) = (\omega^2)^2 = \omega,$$

and so 19 is *not* a cube modulo 43.

Furthermore, we expect that $19 = g^{3k+1}$ for some k , where g generates $(\mathbf{Z}/43\mathbf{Z})^\times$. Note that $|(\mathbf{Z}/43\mathbf{Z})^\times| = 42 = 2 \cdot 3 \cdot 7$. To check whether $g = 2$ works as a generator, it suffices to check $2^{42/2} = 2^{21}$, $2^{42/3} = 2^{14}$, and $2^{42/7} = 2^6$ modulo 43. And fast exponentiation modulo 43 gives

$$\begin{aligned} (1, 2, 14) &\rightarrow (1, 4, 7) \rightarrow (4, 4, 6) \rightarrow (4, 16, 3) \\ &\rightarrow (21, 16, 2) \rightarrow (21, -2, 1) \rightarrow (\boxed{1}, -2, 0), \end{aligned}$$

so 2 is not a generator. Similarly, $g = 3$ is a generator. And indeed, another fast modular exponentiation shows that $3^{19} = 19 \pmod{43}$.

- *Is 22 a cube modulo 43?* The question is whether $\chi_{\pi}(22) = 1$. Compute, using the fact that $\pi \mid 43$ for the second equality and remembering that $\chi_{\pi}(-1) = 1$ for the third, that

$$\chi_{\pi}(22) = \chi_{\pi}(2)\chi_{\pi}(11) = \chi_{\pi}(2)\chi_{\pi}(-32) = \chi_{\pi}(2)^6 = 1.$$

So, *yes*, 22 is a cube modulo 43. Since $g = 3$ is a generator modulo 43, we can find the cube roots by using fast modular exponentiation to compute g^3, g^6, \dots , or we can just conduct an instant computer search. They are 19, 28, and 39.

But the calculation was rather flukish. To proceed conventionally, compute instead that

$$\begin{aligned} \chi_{\pi}(22) &= \chi_{\pi}(2)\chi_{\pi}(11) = \chi_2(\pi)\chi_{\pi}(11) \\ &= \chi_{\pi}(11) \quad \text{since } \pi = -1 + 6\omega = 1 \pmod{2}. \end{aligned}$$

But $11 - 2\omega^2\pi = 11 + 2\omega^2 - 12 = -3 - 2\omega = -\omega\bar{\tau}$, so now, quoting an auxiliary law and reducing π modulo $\bar{\tau}$ at the last step,

$$\chi_{\pi}(11) = \chi_{\pi}(-\omega\bar{\tau}) = \chi_{\pi}(\omega)\chi_{\bar{\tau}}(\pi) = \omega^2\chi_{\bar{\tau}}(-3).$$

Since $-3 = \omega^2\lambda^2$, we thus have, quoting the auxiliary laws,

$$\omega^2\chi_{\bar{\tau}}(-3) = \omega^2\chi_{\bar{\tau}}(\omega)^2\chi_{\bar{\tau}}(\lambda)^2 = \omega^2 \cdot \omega^4 \cdot 1^2 = 1.$$

And again the answer is *yes*.

- *Is 37 a cube modulo 103?* Recall that $103 = N\nu$ where $\nu = 11 + 9\omega$, and that $37 = \rho\bar{\rho}$ where $\rho = -4 + 3\omega$ and $\bar{\rho} = -7 - 3\omega$. The question is whether $\chi_{\nu}(37) = 1$. Compute first that

$$\chi_{\nu}(37) = \chi_{\nu}(\rho\bar{\rho}) = \chi_{\nu}(\rho)\chi_{\nu}(\bar{\rho}) = \chi_{\rho}(\nu)\chi_{\bar{\rho}}(\nu)$$

This is progress since $N\rho = 37 < 103 = N\nu$. Note that working modulo ρ ,

$$\nu = 11 + 9\omega = 11 + 12 = 23 = -14,$$

so that the first term in the product of character-values is

$$\begin{aligned}
 \chi_\rho(\nu) &= \chi_\rho(-1)\chi_\rho(2)\chi_\rho(7) \\
 &= 1 \cdot \chi_2(\rho)\chi_\rho(\tau\bar{\tau}) \\
 &= \chi_2(\omega)\chi_\rho(\tau)\chi_\rho(\bar{\tau}) \quad \text{since } \rho = \omega \pmod{2} \\
 &= \omega\chi_\tau(\rho)\chi_{\bar{\tau}}(\rho) \\
 &= \omega\chi_\tau(-6)\chi_{\bar{\tau}}(-5) \\
 &= \omega\chi_\tau(\omega^2 \cdot 2 \cdot \lambda^2)\chi_{\bar{\tau}}(2) \\
 &= \omega\chi_2(\tau\bar{\tau})(\omega^2)^2(\omega^2 m)^2 \quad \text{where } 2 = 3m - 1, \text{ so } m = 1 \\
 &= \omega\chi_2(7)\omega^8 \\
 &= 1.
 \end{aligned}$$

Similarly, since $\nu = 11 + 9\omega = 11 - 21 = -10 \pmod{\bar{\rho}}$, the second term is

$$\begin{aligned}
 \chi_{\bar{\rho}}(\nu) &= \chi_{\bar{\rho}}(-1 \cdot 2 \cdot 5) \\
 &= \chi_2(\bar{\rho})\chi_5(\bar{\rho}) \\
 &= \chi_2(-1 - \omega)\chi_5(-2(1 - \omega)) \\
 &= \chi_2(\omega)^2\chi_5(2)\chi_5(\lambda) \\
 &= \omega^2 \cdot 1 \cdot \omega^{2m} \quad \text{where } 5 = 3m - 1, \text{ so } m = 2 \\
 &= \omega^2\omega^4 \\
 &= 1.
 \end{aligned}$$

In sum, *yes*, 37 is a cube modulo 103. Indeed, 40, 77, and 89 cube to 37 modulo 103. Of these, 40 is particularly easy to check because $40^3 = 64000$.

10. FERMAT'S LAST THEOREM FOR $n = 3$

The *Descent Principle* rephrases the principle of mathematical induction.

Proposition 10.1 (Descent Principle). *Suppose that a subset T of \mathbf{Z}^+ satisfies the conditions*

- (a) $1 \notin T$,
- (b) *For all $n \in \mathbf{Z}^+$, $n + 1 \in T \implies n \in T$.*

Then $T = \emptyset$.

Indeed, the complement T^c is all of \mathbf{Z}^+ by the induction principle.

Proposition 10.2 (Fermat's Last Theorem for $n = 3$). *The equation*

$$(1) \quad x^3 + y^3 + z^3 = 0$$

has no solutions in $(\mathbf{Z} - \{0\})^3$.

Proof. We will work in the ring $D = \mathbf{Z}[\omega]$. Two results that we will cite are:

- $D/\lambda D \cong \mathbf{F}_3 \cong \{-1, 0, 1\}$,
- If $\alpha = \pm 1 \pmod{\lambda}$ then $\alpha^3 = \pm 1 \pmod{9}$.

Assume a solution of equation (1) in $(\mathbf{Z} - \{0\})^3$. We may assume that the solution is primitive, i.e., $\gcd(x, y, z) = 1$; and consequently we may assume that x , y , and z are pairwise coprime. Using the two bullets, inspect the equation modulo 9 to see

that $\lambda \mid xyz$, so that without loss of generality $\lambda \mid z$. Replace z by $\lambda^e z$ to see that the solution of (1) give us a solution (x, y, z, u, e) of the more general equation

$$(2) \quad x^3 + y^3 = u\lambda^{3e}z^3, \quad \text{where} \quad \begin{cases} x, y, z \in D - \{0\}, \\ x, y, z \text{ pairwise coprime,} \\ \lambda \nmid xyz, \\ u \in D^\times, \\ e \in \mathbf{Z}^+. \end{cases}$$

Consider the set of e -values that are possible in solutions of (2),

$$T = \{e \in \mathbf{Z}^+ : \text{there exists a solution } (x, y, z, u, e) \text{ of (2)}\}.$$

We will use the descent principle to show that $T = \emptyset$, and hence that (2) has no solutions.

The first part of the descent argument is to establish that $1 \notin T$. To do so, set $e = 1$ in (2) and reduce modulo 9,

$$\pm 1 \pm 1 = u\lambda^3 z^3 \pmod{9}.$$

The conditions $\pm 2 = u\lambda^3 z^3 \pmod{9}$ would force the false conditions $\pm 2 = 0 \pmod{\lambda}$, so they are impossible. The remaining possibility, $0 = u\lambda^3 z^3 \pmod{9}$, is false as well. Thus $e = 1$ is impossible.

For the second part of the descent argument, suppose that $e \in T$ (so that $e \geq 2$). We want to show that consequently $e - 1 \in T$. Factor the left side of (2) to get

$$(x + y)(x + \omega y)(x + \omega^2 y) = u\lambda^{3e}z^3.$$

The right side is divisible by λ^6 because $e \geq 2$, so some factor of the left side is divisible by λ^2 . We may replace y by ωy or $\omega^2 y$ (with no effect on y^3) to assume that in fact $\lambda^2 \mid x + y$. Now,

$$\begin{aligned} \gcd(x + y, x + \omega y) &\mid (x + y) - (x + \omega y) = \lambda y, \\ \gcd(x + y, x + \omega y) &\mid (x + y) - \omega^2(x + \omega y) = -\omega^2 \lambda x, \end{aligned}$$

and so

$$\gcd(x + y, x + \omega y) \mid \lambda.$$

On the other hand, since $\lambda \mid x + y$, also $\lambda \mid x + y - \lambda y = x + \omega y$, so in fact

$$\gcd(x + y, x + \omega y) = \lambda.$$

Similarly,

$$\gcd(x + y, x + \omega^2 y) = \lambda$$

and

$$\gcd(x + \omega y, x + \omega^2 y) = \lambda.$$

Now the factorization $(x + y)(x + \omega y)(x + \omega^2 y) = u\lambda^{3e}z^3$ shows that

$$\begin{aligned} 1 \cdot (x + y) &= u_3 \lambda^{3e-2} \tilde{z}^3, \\ \omega \cdot (x + \omega y) &= u_1 \lambda \tilde{x}^3, \\ \omega^2 \cdot (x + \omega^2 y) &= u_2 \lambda \tilde{y}^3, \end{aligned}$$

where \tilde{x} , \tilde{y} , and \tilde{z} are pairwise coprime and $\lambda \nmid \tilde{x}\tilde{y}\tilde{z}$. But adding the left sides of the previous display columnwise gives 0,

$$(1 + \omega + \omega^2)x + (1 + \omega^2 + \omega^4)y = 0.$$

Consequently the right sides sum to 0 as well,

$$u_1\lambda\tilde{x}^3 + u_2\lambda\tilde{y}^3 + u_3\lambda^{3e-2}\tilde{z}^3 = 0.$$

Cancel $u_1\lambda$ to get

$$\tilde{x}^3 + \tilde{u}_2\tilde{y}^3 + \tilde{u}_3\lambda^{3(e-1)}\tilde{z}^3 = 0.$$

Using the second bullet at the beginning of the proof, inspect modulo 3 to see that $\pm 1 \pm \tilde{u}_2 = 0 \pmod{3}$, so that $\tilde{u}_2 = \pm 1$. If $\tilde{u}_2 = -1$ then replace \tilde{y} by $-\tilde{y}$, so that in either case,

$$\tilde{x}^3 + \tilde{y}^3 + \tilde{u}_3\lambda^{3(e-1)}\tilde{z}^3 = 0.$$

Thus $e - 1 \in T$, completing the descent. □