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

$$D = \mathbb{Z}[\omega]$$

and the cubic reciprocity law.

Contents

1. D is the full integer ring

Consider the field

$$F = \mathbb{Q}(\omega) = \mathbb{Q}[\omega],$$

the second equality holding because for nonzero $a, b \in \mathbb{Q}$, the multiplicative inverse of $a + b\omega$ is $(a + b\omega^2)/(a^2 - ab + b^2)$; here the denominator cannot be 0 because it is $(a - b/2)^2 + 3(b/2)^2 = \frac{1}{4}((2a - b)^2 + 3b^2)$.

The ring D lies in the field F. Each element of D is an algebraic integer, because such an element $a+b\omega$ with $a, b \in \mathbb{Z}$ satisfies the monic polynomial $x^2-(2a-b)x+(a^2-ab+b^2)$ whose coefficients lie in $\mathbb{Z}$ because its coefficients a and b do. We show that conversely, every algebraic integer in F lies in D, so that $D = F \cap \overline{\mathbb{Z}}$. That is, we show that for $a, b \in \mathbb{Q}$, if $2a - b$ and $a^2 - ab + b^2$ lie in $\mathbb{Z}$ then so do a, b. The conditions are $2a - b \in \mathbb{Z}$ and $(2a - b)^2 + 3b^2 \in 4\mathbb{Z}$. Immediately, $3b^2 \in \mathbb{Z}$, from which $b \in \mathbb{Z}$. If b is even then $3b^2 \equiv_4 0$ and so the condition $(2a - b)^2 + 3b^2 \in 4\mathbb{Z}$ makes $2a-b$ even, making $2a$ an even integer and so $a \in \mathbb{Z}$. If b is odd then $3b^2 \equiv_4 3$ and so the condition $(2a - b)^2 + 3b^2 \in 4\mathbb{Z}$ makes $2a - b$ odd, again making $2a$ an even integer and so again $a \in \mathbb{Z}$. This completes the argument.

2. Unique factorization

The ring D is Euclidean with norm function

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

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

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

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 $\tilde{e}_i = e_i$.

3. Units

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

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

Indeed, $\implies$ is immediate because if $uv = 1$ in D then $Nu\,Nv = N(uv) = N(1) = 1$ in $\mathbb{Z}_{\geq 1}$; $\impliedby$ is also immediate because if $u\overline{u} = 1$ then u has inverse $\overline{u}$. Here and throughout we use the fact that beyond being a ring, D is closed under complex conjugation. The equivalence shows that

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

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

4. Irreducibles (nonzero primes)

Let $\pi \in D$ be irreducible. Then $\pi \mid \pi\overline{\pi} = N\pi \in \mathbb{Z}_{>1}$. Thus (because 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. Because πD is a prime ideal of D, $\pi D \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, nonzero because it contains $\pi\overline{\pi}$. Thus $\pi D \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime p. Because $p\mathbb{Z} \subset \pi D$, 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.

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

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

5. Factorization of rational primes

Because 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

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

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

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

There are three possibilities.

- p **splits**: $g=2$, $e_1=f_1=1$, $e_2=f_2=1$. Here we have $p=u\pi_1\pi_2$ where $N\pi_1=N\pi_2=p$, so that in fact
$$p=\pi\overline{\pi} \quad \text{and } \pi,\ \overline{\pi} \text{ are nonassociate.}$$
- 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
$$p=\pi\overline{\pi} \quad \text{and } \pi,\ \overline{\pi} \text{ are associate.}$$

Note that in the first possibility, $e_1=e_2$, and so we may as well just call it e, and similarly for f. So in all three cases the formula $\sum_{i=1}^{g}e_if_i=2$ simplifies to

$$efg=2.$$

A prime p splits when $g=2$, is inert when $f=2$, and ramifies when $e=2$.

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

- *The prime $p=3$ ramifies.* Specifically, recalling that $\omega=\zeta_3=e^{2\pi i/3}\in D^\times$,
$$3=-\omega^2\lambda^2 \quad \text{where } \boxed{\lambda=1-\omega}.$$
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 $p=\pi\overline{\pi}$ with $\overline{\pi}\in D^\times\pi$. After replacing π by $\omega\pi$ or $\omega^2\pi$ if necessary, we may assume that $\overline{\pi}=\pm\pi$ (i.e., $\overline{\pi}=\pm\omega^j\pi \implies \overline{\omega^{2j}\pi}=\omega^j\cdot\pm\omega^j\pi=\pm\omega^{2j}\pi$), and hence $\pi^2=\pm p$. Let $\pi=a+b\omega$ (with $b\neq 0$), so that $\pi^2=(a^2-b^2)+(2ab-b^2)\omega$. Because $\pi^2=\pm p$ and $b\neq 0$, necessarily $b=2a$. Thus $N\pi=a^2-ab+b^2$ equals $3a^2$. Consequently $p=3$, and furthermore $\pi=\pm(1+2\omega)=\pm\omega(\omega^2+2)=\pm\omega(1-\omega)=\pm\omega\lambda$.
- *If $p=1 \bmod 3$ then p splits.* Indeed, the character group $\widehat{\mathbb{F}_p^\times}$ contains an element χ of order 3. Note that $\chi(\mathbb{F}_p^\times)\subset D^\times$. 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 $p=2 \bmod 3$ 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 $p\neq 2 \bmod 3$. Note:

From now on we use the symbol q to denote a 2 mod 3 *prime.*

In sum, we have shown that the Legendre symbol $(p/3)$ describes factorization in D: p splits, is inert, or ramifies as $(p/3)$ equals 1, -1, or 0. Equivalently, by the laws of quadratic reciprocity,

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

6. Factorization via ideals

To see again how a rational prime p decomposes in D, consider the quotient ring D/pD. Because $D = \mathbb{Z}[\omega]$ and the polynomial of ω is $X^2 + X + 1$, we have

$$D/pD \approx \mathbb{Z}[X]/\langle p, X^2 + X + 1\rangle \approx \mathbb{F}_p[X]/\langle X^2 + X + 1\rangle.$$

The polynomial $X^2 + X + 1$ has discriminant -3. For odd primes $p = 2 \bmod 3$ the Legendre symbol $(-3/p) = (3^*/p) = (p/3)$ is -1, and so the polynomial is irreducible modulo p. Also the polynomial is irreducible modulo 2. Thus D/pD is a field of order p^2 for all primes $p = 2 \bmod 3$, showing that such p remain prime in D.

For primes $p = 1 \bmod 3$, the Legendre symbol $(-3/p)$ is 1, and so the polynomial factors as $X^2 + X + 1 = (X - \alpha)(X - \beta)$ modulo p with α and β distinct modulo p. Thus

$$\mathbb{F}_p[X]/\langle X^2 + X + 1\rangle \approx \mathbb{F}_p[X]/\langle X - \alpha\rangle \times \mathbb{F}_p[X]/\langle X - \beta\rangle, \quad p = 1 \bmod 3.$$

Here it is relevant that α and β are distinct modulo p, so that the sum $\langle X - \alpha\rangle + \langle X - \beta\rangle$ contains $\alpha - \beta$, which is invertible in $\mathbb{F}_p$, making the sum all of $\mathbb{F}_p[X]$. The previous display shows that D/pD is not a field but rather is the product of two fields of order p, and hence p decomposes. The surjection from D/pD to $\mathbb{F}_p[X]/\langle X - \alpha\rangle$ gives an isomorphism $D/\langle p, \omega - \alpha\rangle \approx \mathbb{F}_p[X]/\langle X - \alpha\rangle$ and similarly for β, and so

$$D/pD \approx D/\langle p, \omega - \alpha\rangle \times D/\langle p, \omega - \beta\rangle, \quad p = 1 \bmod 3.$$

By the Sun Ze theorem, $\langle p\rangle$ factors as the product of $\langle p, \omega - \alpha\rangle$ and $\langle p, \omega - \alpha\rangle$.

For $p = 3$, the Legendre symbol $(-3/p)$ is 0 and the polynomial factors as $X^2 + X + 1 = (X - 1)^2$ modulo 3. Thus

$$\mathbb{F}_p[X]/\langle X^2 + X + 1\rangle = \mathbb{F}_p[X]/\langle (X - 1)^2\rangle, \quad p = 3.$$

Here we get $\langle 3\rangle = \langle 3, \omega - 1\rangle^2 = \langle \lambda\rangle^2$ in D, as before.

7. Canonical representative of each associate class

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

$$\pi' = 2 \bmod 3.$$

That is,

$$\pi' = a + b\omega, \quad a = 2 \bmod 3, \ b = 0 \bmod 3.$$

Indeed, if π divides a rational prime $q = 2 \bmod 3$ then its primary associate is simply q. Otherwise, π divides a rational prime $p = 1 \bmod 3$ and $N\pi = p$. To show that the prime $\pi = a + b\omega$ has a unique primary associate, note that altogether its associates are

$$\pm(a + b\omega), \qquad \pm(b + (b - a)\omega), \qquad \pm((a - b) + a\omega).$$

The relation $a^2 - ab + b^2 = p = 1 \bmod 3$ says that not both of a and b are 0 mod 3, and also that $ab \neq -1 \bmod 3$. If $a = 0 \bmod 3$ then one of the third pair in the previous display is primary, and no other; if $b = 0 \bmod 3$ then one of the first pair is primary, and no other; if $ab = 1 \bmod 3$ then one of the second pair is primary, and no other.

Given a rational prime $p = 1 \bmod 3$, to find a primary prime π lying over p, proceed as follows. We know that $\pi = a + b\omega$ where $a = 2 \bmod 3$ and $b = 0 \bmod 3$, and we want to find a and b. Because $p = N\pi = a^2 - ab + b^2$, 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 $A = 1 \bmod 3$ (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 $\overline{\pi}$ lying over p) and then set $b = 3B$. Note that b has the same parity as A. Finally, set $a = (A + b)/2$, which is 2 mod 3 because $2a = A + b = 1 \bmod 3$. All of this is exactly the procedure described in Gauss's Theorem about the solution-count of the equation $x^3 + y^3 = 1$ modulo p. Repeating,

$$4p = A^2 + 27B^2, \text{ with } A = 1 \bmod 3 \text{ and two choices of } B,$$
$$b = 3B \text{ and then } a = \frac{A + b}{2}, \text{ producing two pairs } (a, b).$$

For example, let $p = 103$, so that $4p = 412$. The values $27B^2$ through 412 are $27, 108, 243$, and $412 - 27 = 385$ and $412 - 108 = 304$ are nonsquares. But $412 - 243 = 169$, so we have $A = 13$ and $B = \pm 3$. Thus $b = \pm 9$ and then $a = (A + b)/2$ is correspondingly 11 or 2. Thus the primary primes lying over $p = 103$ are $\{\pi, \overline{\pi}\} = \{11 + 9\omega, 2 - 9\omega\}$. These are visibly primary, and it is easy to check that their product is 103.

8. 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 because 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 $xz = 1 \bmod \pi$.

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

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

induces an injection

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

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

Now assume that π is primary.

- If $\pi = q = 2 \bmod 3$ then

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

and so

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

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

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

Along with the opposite injection from before, this shows that

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

and so

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

- If $\pi \mid p$ where $p = 1 \bmod 3$ then $\pi = a + b\omega$ with $p = a^2 - ab + b^2$. Note that $p \nmid b$, because otherwise the previous equality shows that also $p \mid a$ and then $p \mid a + b\omega = \pi$, contradicting the fact that p splits in D. Because $p \nmid b$, there exists $c \in \mathbb{Z}$ such that $cb = 1 \bmod p$, and so $\omega \equiv_\pi cb\omega$. Because $\pi = a + b\omega$, this gives $\omega \equiv_\pi -ca$, and thus $\pi = a + b\omega \equiv_\pi a(1 - bc) \in \mathbb{Z}$. We may further translate $a(1 - bc)$ freely by multiples of p, so that as in the ramified case, $D/\pi D \hookrightarrow \mathbb{Z}/p\mathbb{Z}$ and thus

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

and

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

The second and third bullets just above can be gathered into a single argument, as follows. In both cases, $p = \pi\pi'$ where π and π' are nonassociate, and so if we believe that the Sun Ze theorem works for D as it works for $\mathbb{Z}$ then

$$D/pD \cong D/\pi D \times D/\pi' D.$$

Because $|D/pD| = p^2$ and $D/\pi D$ and $D/\pi' D$ are nontrivial, $|D/\pi D| = p$. Regardless of which argument is used, the results gather together to give

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

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 $\mathbb{Z}/p\mathbb{Z}$) always sum to 2, the dimension of $\mathbb{Q}(\omega)$ as a vector space over $\mathbb{Q}$.

9. 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 $(\cdot/p) : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}$.

To define χ_π, first note that $(D/\pi D)^\times$ is cyclic of order $N\pi - 1$. If $\pi \mid p$ where $p = 1 \bmod 3$ then $N\pi = p = 1 \bmod 3$, while if $\pi = q = 2 \bmod 3$ then $N\pi = q^2 = 1 \bmod 3$. Thus $N\pi = 1 \bmod 3$ 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 $\{1 + \pi D, \omega + \pi D, \omega^2 + \pi D\}$.

Because each of 1, ω, ω^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 $1 - \omega^2 = (1+\omega)(1-\omega) = -\omega^2\lambda$ are all associates of λ, and so they are not divisible by π.

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

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

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 9.1. *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

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

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

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

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

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

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

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

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

For example, take $p = 7 = 1 \bmod 3$. To factor p in D, note that the relations $28 = A^2 + 27B^2$, $A = 1 \bmod 3$ have solutions $(A, B) = (1, \pm 1)$, giving $b = 3B = \pm 3$ and then $a = (A \pm b)/2 = 2, -1$. Thus

$$7 = \pi\overline{\pi}, \quad \pi = 2 + 3\omega, \ \overline{\pi} = -1 - 3\omega,$$

and we can confirm the factorization of 7 directly now that we have it. To compute χ_π, note that in $D/\pi D$ we have the relations $3\omega = -2$ and $7 = 0$, giving $\omega = -3$, and $D/\pi D \approx \mathbb{Z}/7\mathbb{Z}$. Because $(\mathbb{Z}/7\mathbb{Z})^\times$ is generated by $3 + 7\mathbb{Z}$, the character χ_π is entirely determined by the observation that $3^{(7-1)/3} = 9 = \omega^2 \bmod \pi D$. That is,

$$\chi_\pi(3^e + 7\mathbb{Z}) = \omega^{2e}, \quad e = 0, \dots, 5.$$

One can check that similarly

$$\chi_{\overline{\pi}}(3^e + 7\mathbb{Z}) = \omega^e, \quad e = 0, \dots, 5.$$

Thus $\chi_{\overline{\pi}} = \overline{\chi_\pi}$ on $\mathbb{Z} - 7\mathbb{Z}$. However, $\chi_{\overline{\pi}}$ and $\overline{\chi_\pi}$ are not equal on all of $D - \pi D$, as we can see by computing that $\chi_{\overline{\pi}}(\omega) = \omega^2$ while $\overline{\chi_\pi}(\omega) = \omega$. Instead, $\chi_{\overline{\pi}}(\overline{\omega}) = \chi_{\overline{\pi}}(\omega^2) = \omega^4 = \omega$ does match $\overline{\chi_\pi(\omega)}$. Part (c) of the next proposition confirms this.

Proposition 9.2 (Properties of the Cubic Character)**.** *Let $\pi \in D$ be a primary prime, $\pi \neq \lambda$. Then*

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

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

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

$$\chi_\pi(ab) = \chi_\pi(a)\chi_\pi(b).$$

That is, χ_π is multiplicative.

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

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

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

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

and so in particular, still with $\pi = q = 2 \bmod 3$,

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

Proof. (a) First working additively, the kernel of the multiply-by-$(N\pi - 1)/3$ map on $\mathbb{Z}/(N\pi - 1)\mathbb{Z}$ is $\langle 3 + (N\pi - 1)\mathbb{Z}\rangle$. Now multiplicatively, the kernel of the raise-to-the-$(N\pi - 1)/3$ map on $(D/\pi D)^\times$ is $\langle g^3\rangle$, where g is a generator, and this kernel consists of the cubes.

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

$$\chi_\pi(ab) = (ab)^{(N\pi-1)/3} = a^{(N\pi-1)/3} b^{(N\pi-1)/3} = \chi_\pi(a)\chi_\pi(b).$$

Because 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 $a \in D - \pi D$, compute that

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

Compute also, working modulo $\overline{\pi}$ and noting that $N\pi = N\overline{\pi}$, that

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

and because the values at the beginning and the end of the display agree modulo $\overline{\pi}$ 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 because $3 \nmid |(\mathbb{Z}/q\mathbb{Z})^\times| = q-1$, and so the cubing map is an automorphism of $(\mathbb{Z}/q\mathbb{Z})^\times$, making each element of $(\mathbb{Z}/q\mathbb{Z})^\times$ a cube that χ_π therefore takes to 1. □

10. Cubic reciprocity

Theorem 10.1 (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*
>
> $$\boxed{\chi_\pi(\pi') = \chi_{\pi'}(\pi).}$$

The **auxiliary laws of cubic reciprocity** *are:*

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

and

$$\boxed{\chi_\pi(-1) = 1}$$

and

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

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

The main law here is analogous to the main law of quadratic reciprocity expressed as $(p^*/q) = (q/p)$. The first auxiliary law is analogous to the formula for the Legendre symbol $(2/p)$, but now λ is the anomalous prime rather than 2. The second and third auxiliary laws are analogous to the formula for the Legendre symbol $(-1/p)$, but now there are six units rather than two.

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 $\overline{\mathbb{Z}}$, that on the one hand,

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

and on the other, still working modulo q in $\overline{\mathbb{Z}}$, and noting that $(\cdot/p)^q = (\cdot/p)$ because q is odd,

$$\tau((\cdot/p))^{q+1} = \tau((\cdot/p))\tau((\cdot/p))^q = \tau((\cdot/p)) \sum_{t\in\mathbb{F}_p^\times} (q^2t/p)^q \zeta_p^{qt} = \tau((\cdot/p))^2(q/p)$$
$$= p^*(q/p).$$

So

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

and therefore

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

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

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

and therefore

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

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

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

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

Because the Gauss sum has norm p, the Jacobi sum has norm $N(J) = p$, and so J is associate to π or to $\overline{\pi}$. To show that J is associate to π, compute that modulo π,

$$J = \sum_{t=1}^{p-1} t^{(p-1)/3}(1-t)^{(p-1)/3} = \sum_{t=1}^{p-1} t^{(p-1)/3} \sum_{j=0}^{(p-1)/3} \binom{(p-1)/3}{j} (-t)^j$$
$$= \sum_{j=0}^{(p-1)/3} \binom{(p-1)/3}{j} (-1)^j \sum_{t=1}^{p-1} t^{(p-1)/3+j}.$$

Each inner sum at the end of the previous display is a nontrivial character sum of $(\mathbb{Z}/p\mathbb{Z})^\times$, showing that $J = 0 \bmod \pi D$, and so J is associate to π. Furthermore, working modulo 3,

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

That is, J is primary. Altogether we have shown that $J = \pi$, and so

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

This is analogous to an earlier result that we can find the square of the quadratic Gauss sum without too much difficulty, whereas finding the value of the quadratic Gauss sum itself was considerably harder. 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 9.2(d),

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

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

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

and on the other, still working modulo q in $\overline{\mathbb{Z}}$, and noting that $\chi_\pi^{q^2} = \chi_\pi$ because $q^2 = 1 \bmod 3$,

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

So

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

and therefore

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

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

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

and therefore

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

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

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

and on the other, still working modulo π' in $\overline{\mathbb{Z}}$, and noting that $\chi_\pi^{p'} = \chi_\pi$ because $p' = 1 \bmod 3$,

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

So as twice before,

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

By symmetry, also

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

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

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

□

11. Examples

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

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

So, for example:

- *Is 19 a cube modulo 41?* Because $41 = 2 \bmod 3$, *yes*: $3 \nmid 41 - 1$ and so the cubing map is an automorphism of $(\mathbb{Z}/41\mathbb{Z})^\times$. Alternatively, by Proposition 9.2(d), $\chi_{41}(19) = 1$.
- *Is 19 a cube modulo 43?* Because $\mathbb{Z}/43\mathbb{Z} \cong D/\pi D$, the question is whether $\chi_\pi(19) = 1$. Compute that

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

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

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

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

We might expect $19 = g^{3k+1}$ for some k, where g generates $(\mathbb{Z}/43\mathbb{Z})^\times$. Note that $|(\mathbb{Z}/43\mathbb{Z})^\times| = 42 = 2 \cdot 3 \cdot 7$. Thus, to check whether $g = 2$ is a generator it suffices to check $2^{42/2} = 2^{21}$, $2^{42/3} = 2^{14}$, and $2^{42/7} = 2^6$ modulo 43. Fast exponentiation modulo 43 gives

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

so 2 is not a generator. Similarly, $g = 3$ *is* a generator. Another fast modular exponentiation shows that $19 = 3^{19} \bmod 43$, and the exponent 19 is indeed 1 mod 3. One can check that the next generator after 3 is $g = 5$, and $19 = 5^{31}$ and $31 = 1 \bmod 3$, and the next generator is $g = 12$, and $19 = 12^{37}$ and $37 = 1 \bmod 3$. However, the next generator after that is $g = 18$, and $19 = 18^5 \bmod 43$ and $5 = 2 \bmod 3$, so our possible expectation is wrong. In fact, of the $\phi(42) = 12$ generators g modulo 43, half are such that $19 = g^{3k+1} \bmod 43$ and the other half are such that $19 = g^{3k+2} \bmod 43$. In hindsight, the issue is that we could just as well have used $\overline{\pi}$ to determine

whether 19 is a cube modulo 43, but the value $\chi_{\overline{\pi}}(19) = \overline{\chi}_{\pi}(19) = \omega^2$ equally suggests that $19 = g^{3k+2}$ for generators g until we realize that the choice of generator matters.

- *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. Because 3 is a generator modulo 43, we can find the cube roots of 22 by using fast modular exponentiation to compute $3^3, 3^6, 3^9, \ldots$, 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

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

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

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

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

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

And again the answer is *yes.*

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

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

This is progress because $N\rho = 37 < 103 = N\nu$. 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

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

Similarly, because $\nu = 11 + 9\omega = 11 - 21 = -10 \bmod \overline{\rho}$, the second term is

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

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 $40^3 = 64000$.

12. Comment on Ireland and Rosen section 9.6

Our text shows that for any prime p,

$$p = x^2 + 27y^2 \iff p = 1 \bmod 3 \text{ and } (2/p)_3 = 1.$$

This equivalence can be viewed as a mechanism to check whether 2 is a cube modulo p for any given prime $p = 1 \bmod 3$. (If $p = 2 \bmod 3$ then cubing is an automorphism modulo p and so 2 is a cubic residue except when $p = 2$. And $2 = -1 = (-1)^3 \bmod 3$.) However, another perspective is that the equivalence says what primes p take the form $p = x^2 + 27y^2$, and that in some sense the answer depends only on congruence conditions where the modulus is related to p. The idea is that any such p equals 1 mod 3, and so it factors in $D = \mathbb{Z}[\omega]$ as $p = \pi\overline{\pi}$ with $\overline{\pi}$ not associate to π; the condition $(2/p)_3 = 1$ is $(2/\pi)_3 = 1$, which in turn is $(\pi/2)_3 = 1$ by cubic reciprocity, and this last condition depends only on π modulo $2D$.

13. Fermat's last theorem for $n = 3$

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

Proposition 13.1 (Descent Principle)**.** *Suppose that a subset T of $\mathbb{Z}^+$ satisfies the conditions*

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

Then $T = \emptyset$.

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

Proposition 13.2 (Fermat's Last Theorem for $n = 3$)**.** *The equation*

$$x^3 + y^3 + z^3 = 0 \tag{1}$$

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

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

- $D/\lambda D \cong \mathbb{F}_3 \cong \{-1, 0, 1\}$,

- If $\alpha = \pm 1 \bmod \lambda$ then $\alpha^3 = \pm 1 \bmod 9$. (For the "+" case note that $\alpha^3 - 1 = (\alpha - 1)(\alpha - \omega)(\alpha - \omega^2)$, and also that $\omega = 1 - \lambda$ and so $\omega^2 = -1 - \omega = -2 + \lambda$, so that $\alpha^3 - 1 = (\alpha - 1)(\alpha - 1 + \lambda)(\alpha + 2 - \lambda)$; write $\alpha = \beta\lambda + 1$ to get $\alpha^3 - 1 = \beta\lambda(\beta + 1)\lambda((\beta - 1)\lambda + 3)$, and this is the sum of two terms, the first term divisible by 9 because one of $\beta, \beta + 1, \beta - 1$ is divisible by λ and the second term clearly so,
$$\alpha^3 - 1 = \lambda^3\beta(\beta + 1)(\beta - 1) + 3\lambda^2\beta(\beta + 1).$$
The "−" case follows from the "+" case.)

Assume a solution of equation (1) in $(D - \{0\})^3$. 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

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

Consider the set of e-values that are possible in solutions of (2),
$$T = \{e \in \mathbb{Z}^+ : \text{there exists a solution } (x, y, z, u, e) \text{ of (2)}\}.$$
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,
$$\pm 1 \pm 1 = \pm u\lambda^3 \bmod 9.$$
The conditions $\pm 2 = \pm u\lambda^3 \bmod 9$ would force the false conditions $\pm 2 = 0 \bmod \lambda$, so they are impossible. The remaining possibility, $0 = \pm u\lambda^3 \bmod 9$, 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 $x^3 + y^3$ 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 $\lambda^2 \mid x + y$. We show that exactly one power of λ divides each of $x + \omega y$ and $x + \omega^2 y$. Indeed,
$$\gcd(x + y, x + \omega y) \mid (x + \omega y) - \omega(x + y) = \lambda x,$$
$$\gcd(x + y, x + \omega y) \mid (x + y) - (x + \omega y) = \lambda y,$$
and so, because x and y are coprime,
$$\gcd(x + y, x + \omega y) \mid \lambda.$$

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

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

Similarly,

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

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

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

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,

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

Cancel $u_1\lambda$ to get

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

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

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

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