BASIC NUMBER THEORY: LECTURE 6

WENHAN DAI

1. The cubic reciprocity (continued)

Recall that, for a prime π of $\mathbb{Z}[\omega]$, we have defined a character

$$\left(\frac{\cdot}{\pi}\right)_3 : (\mathbb{Z}[\omega]/(\pi))^\times \longrightarrow \{1, \omega, \omega^2\}.$$

This will be appeared as the cubic Legendre/Jacobi symbol. Also recall that for $\pi \nmid \alpha \in \mathbb{Z}[\omega]$,

$$\left(\frac{\alpha}{\pi}\right)_3 = 1 \iff \exists x \in \mathbb{Z}[\omega] \text{ such that } x^3 \equiv \alpha \bmod \pi,$$

namely, α is a cubic residue of π. Moreover, in case where $\left(\frac{\alpha}{\pi}\right)_3 = 1$, we have a (non-canonical) isomorphism

$$\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] \simeq \mathbb{Z}/p\mathbb{Z},$$

where $p = N(\pi) = \pi \cdot \overline{\pi}$ is the prime lying below π. Note that this isomorphism possibly fails to exist when $p \equiv 2 \bmod 3$ and α is not a cubic residue (cf. Lemma 10(2) in Lecture 5). To state the law of cubic reciprocity (next time), we need one definition: a prime π is called *primary* if $\pi \equiv \pm 1 \bmod 3$. Given any prime $\pi \nmid 3$, one can show that exactly two of the six associates $\pm\pi, \pm\omega\pi$ and $\pm\omega^2\pi$ are primary.

Theorem 1 (The cubic reciprocity)**.** *Let π, θ be primary primes and $N(\pi) \neq N(\theta)$. Then*

$$\left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3.$$

There are also supplementary formulas for $\left(\frac{\omega}{\pi}\right)_3$ and $\left(\frac{1-\omega}{\pi}\right)_3$. Let π be prime and not associate to $1-\omega$. Then we may assume that $\pi \equiv -1 \bmod 3$ (if π is primary, one of $\pm\pi$ satisfies this condition). Writing $\pi = -1 + 3m + 3n\omega$, it can be shown that

$$\left(\frac{\omega}{\pi}\right)_3 = \omega^{m+n}, \left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}.$$

The first equality above is easy to prove, while the second is more difficult.

Here comes an immediate application of Theorem 1. Note that for an odd prime $p = x^2 + 27y^2$, one can deduce the necessary condition that -27 is a quadratic residue of p. We infer by the quadratic reciprocity law that $p \equiv 1 \bmod 3$. However, this is not sufficient.

Theorem 2. *Let p be a prime. Then $p = x^2 + 27y^2$ if and only if $p \equiv 1 \bmod 3$ and 2 is a cubic residue modulo p.*

Date: October 20, 2020.

Proof. Assume $p = x^2 + 27y^2$ and in particular $3 \nmid p$. Hence $p \equiv x^2 \equiv 1 \bmod 3$. Consider

$$p = (x + 3\sqrt{-3}y)(x - 3\sqrt{-3}y), \quad \pi = x + 3\sqrt{-3}y.$$

Then by the cubic reciprocity, for primary primes 2 and π with $N(2) \neq N(\pi)$,

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 \equiv \pi^{(N(2)-1)/3} \equiv \pi \bmod 2.$$

Since $3\sqrt{-3} = 3(2\omega + 1)$, this further becomes

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 \equiv x + y = 1 \bmod 2$$

as x, y are (consensually) assumed to be coprime. This shows that π is a cubic residue of 2, and hence 2 is a cubic residue of π as well. Then 2 is a cubic residue of p.

Conversely, suppose 2 is a cubic residue modulo p and $p \equiv 1 \bmod 3$. Then $p = \pi\overline{\pi} = a^2 - ab + b^2$ is primary with $\pi = a + b\omega$. In particular, $a \equiv \pm 1 \bmod 3$ and $3 \mid b$. Suppose $b = 3b'$ for some $b' \in \mathbb{Z}$. Then

$$4p = 4a^2 - 12ab' + 36b'^2 = (2a - 3b')^2 + 27b'^2 = (\frac{2a - 3b'}{2})^2 + 27(\frac{b'}{2})^2.$$

On the other hand, by the cubic reciprocity,

$$1 = \left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 \equiv \pi \bmod 2.$$

Hence b is even and so also is b'. This proves that there are x, y such that $4p = x^2 + 27y^2$, which is enough. □

2. The biquadratic reciprocity

We now concern about the ring of the 4th root of unity, i.e. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ with $i = \sqrt{-1}$. We list out some basic properties of $\mathbb{Z}[i]$ without proof.

(1) $\mathbb{Z}[i]$ is an Euclidean domain.
(2) For $x + yi \in \mathbb{Z}[i]$, the norm $N(x + iy) = x^2 + y^2$.
(3) $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
(4) The primes in $\mathbb{Z}[i]$ are classified as follows:
   - $2 = i^3(1 + i)^2$,
   - if $p \equiv 1 \bmod 4$ then $p = \pi\overline{\pi}$ for some $\pi \mid p$, and
   - if $p \equiv 3 \bmod 4$ then p is inert as a prime in $\mathbb{Z}[i]$.
(5) For a prime π, the quotient $\mathbb{Z}[i]/(\pi)$ is a finite field of cardinality $N(\pi)$.

If a prime $\pi \nmid \alpha$ and $\pi \nmid 2$, we know that $\alpha^{N(\pi)-1} \equiv 1 \bmod \pi$ by (generalized) Fermat's little theorem. This heuristically forces us to define a multiplicative group homomorphism

$$\left(\frac{\cdot}{\pi}\right)_4 : \mathbb{Z}[i] \longrightarrow \{\pm 1, \pm i\}, \quad \left(\frac{\alpha}{\pi}\right)_4 = \alpha^{\frac{N(\pi)-1}{4}} \bmod \pi.$$

Here π is non-associate to $1 + i$.

Again, a prime π is called *primary* in $\mathbb{Z}[i]$ if $\pi \equiv 1 \bmod (2 + 2i)$. It turns out that exactly one of $\pm\pi, \pm i\pi$ is primary.

Theorem 3 (The biquadratic reciprocity)**.** *Let π, θ be distinct primes in $\mathbb{Z}[i]$ such that $\pi, \theta \nmid 2$. Then*

$$\left(\frac{\theta}{\pi}\right)_4 = \left(\frac{\pi}{\theta}\right)_4 \cdot (-1)^{\frac{N(\pi)-1}{4}\cdot\frac{N(\theta)-1}{4}}.$$

Write $\pi = a + bi$ and one can prove that

$$\left(\frac{i}{\pi}\right)_4 = i^{-\frac{a-1}{2}}, \quad \left(\frac{1+i}{\pi}\right)_4 = i^{\frac{a-b-1-b^2}{4}}.$$

When π is primary, $a - b - 1 - b^2$ is automatically divisible by 4.

Using the biquadratic reciprocity, the conjecture of Euler about $p = x^2 + 64y^2$ is proved.

Theorem 4 (Euler's conjecture)**.**

(1) *Let $\pi = a + bi$ be a primary prime in $\mathbb{Z}[i]$. Then*

$$\left(\frac{2}{\pi}\right)_4 = i^{\frac{ab}{2}}.$$

(2) *A prime number $p = x^2 + 64y^2$ if and only if $p \equiv 1 \bmod 4$ and 2 is a biquadratic residue modulo p.*

Proof. (1) A priori we obtain

$$\left(\frac{2}{\pi}\right)_4 = \left(\frac{i}{\pi}\right)_4^3 \left(\frac{1+i}{\pi}\right)_4^2 = i^{\frac{a-b-1-b^2}{2} - \frac{3(a-1)}{2}} = i^{\frac{2-2a-b-b^2}{2}}.$$

It reduces to show that $ab \equiv 2 - 2a - b - b^2 \bmod 8$. Consider

$$\begin{aligned} ab - (2 - 2a - b - b^2) &= b^2 + ab + b + 2a - 2 \\ &= (b+2)(b-1) + a(b+2) \\ &= (b+2)(a+b-1). \end{aligned}$$

Then the required condition is equivalent to $8 \mid (b+2)(a+b-1)$. On the other hand, since π is primary, $\pi - 1 = a - 1 + bi = (2+2i)(\lambda + \mu i)$ for some $\lambda, \mu \in \mathbb{Z}$ by definition. Hence $(a-1)/2$ and $b/2$ must have the same parity mod 2. The condition is deduced from this.

(2) The "only if" part is relatively easy to check. As for the "if" part, suppose $p \equiv 1 \bmod 4$. Consequently, $p = \pi\overline{\pi}$ for some primary $\pi = a + bi$. Then $p = N(\pi) = a^2 + b^2$, where $2 \nmid a$ and $2 \mid b$. Also, 2 is a biquadratic residue modulo p if and only if $\left(\frac{2}{\pi}\right)_4 = 1 = i^{ab/2}$ by (1). Hence

$$\left(\frac{2}{\pi}\right)_4 = 1 \iff 8 \mid ab \iff 8 \mid b.$$

This completes the proof of Euler's conjecture. □

3. Proof of the cubic reciprocity

The material refers to §9.4 of the textbook [IR82] by Ireland and Rosen.[1]

[1] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, Berlin, Heidelberg, and New York, 1982.

3.1. **Multiplicative character on $\mathbb{F}_p$.** Let $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a character such that $\chi(0) = 0$ if $\chi \neq \epsilon$, and $\chi(0) = 1$ if $\chi = \epsilon$, where ϵ denotes the trivial character on $\mathbb{F}_p^\times$. Hence

$$\sum_{t \in \mathbb{F}_p} \chi(t) = \begin{cases} p, & \chi = \epsilon; \\ 0, & \chi \neq \epsilon. \end{cases}$$

Moreover, $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{F}_p^\times$.

3.2. **Gauss sum.** Fix an element $a \in \mathbb{F}_p$. Define the *Gauss sum with respect to* a to be the function in a multiplicative character χ that

$$g_a(\chi) := \sum_{t \in \mathbb{F}_p} \chi(t)\zeta_p^{at}, \quad \zeta_p = \exp(\frac{2\pi i}{p}).$$

For simplicity we denote $g(\chi) := g_1(\chi)$. It turns out for $a \in \mathbb{F}_p^\times$ that, by the left multiplication,

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(a^{-1}t)\zeta_p^t = \chi(a^{-1})g(\chi)$$

as χ is multiplicative.

Remark 5. Let p be a prime. Consider the cyclotomic extension of $\mathbb{Q}$ by ζ_p that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{F}_p^\times.$$

Here the first isomorphism is the correspondence between the (arithmetic) Frobenius automorphism $x \mapsto x^p$ and a selected generator of $(\mathbb{Z}/p\mathbb{Z})^\times$ (hence the isomorphism is non-canonical). For $a \in \mathbb{F}_p^\times$ we correspondingly obtain (by abuse of notation)

$$a \longleftrightarrow (a : \zeta \mapsto \zeta^a) \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}).$$

Then in $\mathbb{Q}(\zeta_p)$, the Galois action

$$a(g(\chi)) = g_a(\chi) = \chi(a^{-1})g(\chi),$$

hence $g(\chi)$ is invariant under the action of $\ker \chi = \{a \in \mathbb{F}_p^\times : \chi(a^{-1}) = 1\}$.

Proposition 6. *Assume $\chi \neq \epsilon$. Then*

$$|g(\chi)| = \sqrt{p},$$

where we view $g(\chi)$ as an element in $\mathbb{Q}(\zeta_p)$ and then take the complex norm.

Proof. By computation,

$$\begin{aligned} g(\chi)\overline{g(\chi)} &= \left(\sum_{t_1 \in \mathbb{F}_p^\times} \chi(t_1)\zeta^{t_1}\right)\left(\sum_{t_2 \in \mathbb{F}_p^\times} \chi(t_2)^{-1}\zeta^{-t_2}\right) \\ &= \sum_{t_1, t_2 \in \mathbb{F}_p^\times} \chi(t_1 t_2^{-1})\zeta^{t_1 - t_2} \\ &= \sum_{\lambda \in \mathbb{F}_p^\times} \chi(\lambda) \sum_{t \in \mathbb{F}_p^\times} \zeta^{\lambda t - t} \\ &= \chi(1)(p-1) + \sum_{\lambda \neq 1} \chi(\lambda) \sum_{t \in \mathbb{F}_p^\times} \zeta^{(\lambda - 1)t}. \end{aligned}$$

The second last equality is given by the change of variables $t_1 = \lambda t_2$. Note that for $\lambda \neq 1$, $\sum_{t\in\mathbb{F}_p^\times} \zeta^{(\lambda-1)t} = -1$. Hence

$$g(\chi)\overline{g(\chi)} = p - 1 - \sum_{\lambda\neq 1} \chi(\lambda) = p.$$

This completes the proof. □

3.3. **Jacobi sum.** Let χ, λ be two characters on $\mathbb{F}_p$. Define their *Jacobi sum* to be

$$J(\chi, \lambda) := \sum_{a+b=1} \chi(a)\lambda(b), \quad a, b \in \mathbb{F}_p.$$

Lemma 7. *If $\chi\lambda \neq \epsilon$, then*

$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Proof. This can be done simply by computation:

$$\begin{aligned} g(\chi)g(\lambda) &= \sum_{t\in\mathbb{F}_p} \sum_{a+b=t} \chi(a)\lambda(b)\zeta^t \\ &= \sum_{t\in\mathbb{F}_p^\times} \sum_{a+b=t} \chi(a)\lambda(b)\zeta^t + \underbrace{\sum_{a\in\mathbb{F}_p} \chi(a)\lambda(-a)}_{=0} \\ &= \left(\sum_{t\in\mathbb{F}_p^\times} (\chi\lambda)(t)\zeta^t\right)\left(\sum_{a+b=1} \chi(a)\lambda(b)\right) \\ &= g(\chi\lambda)J(\chi, \lambda). \end{aligned}$$

It is necessary to point out in the end that $\sum_{a\in\mathbb{F}_p} \chi(a)\lambda(-a) = 0$ uses the assumption $\chi\lambda \neq \epsilon$. Otherwise this sum equals the sum of square of all elements in $\mathbb{F}_p$. □

Proposition 8 ([Prop 8.3.3, IR82])**.** *Fix $n > 2$ and let $p \equiv 1 \bmod n$ be a prime number. Suppose χ is a multiplicative character of order n, i.e. $\chi^n = \epsilon$. Then*

$$g(\chi)^n = p \cdot \chi(-1) \cdot J(\chi, \chi)J(\chi, \chi^2) \cdots J(\chi, \chi^{n-2}).$$

Proof. By Lemma 7 above, $g(\chi)g(\lambda) = g(\chi\lambda)J(\chi, \lambda)$. The recipe is to apply this relation inductively, say

$$\begin{aligned} g(\chi)^n &= J(\chi, \chi)g(\chi^2)J(\chi)^{n-2} \\ &= J(\chi, \chi)J(\chi, \chi^2)g^(\chi^3)J(\chi)^{n-3} \\ &= J(\chi, \chi)J(\chi, \chi^2) \cdots J(\chi, \chi^{n-2})g(\chi^{n-1}). \end{aligned}$$

Since χ has order n,

$$g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = g(\chi)g(\overline{\chi})\chi(-1) = p\chi(-1)$$

by Proposition 6 above. □

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn