BASIC NUMBER THEORY: LECTURE 10

WENHAN DAI

1. Hilbert class field (continued)

We have stated the main theorem about primes like $p = x^2 + ny^2$ last time.

Theorem 1 (Primes of the form $p = x^2 + ny^2$)**.** *Fix a square-free integer $n > 0$ satisfying $n \not\equiv 3 \bmod 4$. Then there is a monic irreducible $f_n \in \mathbb{Z}[x]$ of degree $h(-4n) = [K^{\mathrm{Hilb}} : K]$ such that if p is an odd prime, with $p \nmid n \cdot \mathrm{disc}(f_n)$, then $p = x^2 + ny^2$ if and only if $\left(\frac{-n}{p}\right) = 1$ and $f_n(x) \equiv 0 \bmod p$ has an integer solution.*

Example 2. We specialize Theorem 1 to the case $n = 14$. Let $K = \mathbb{Q}(\sqrt{-14})$ and L the Hilbert class field of K. To compute L, one may need the intermediate augment field $K_1 = K(2\sqrt{2} - 1)$. And then prove that $L = K_1(\sqrt{2\sqrt{2} - 1}) = K(\sqrt{2\sqrt{2} - 1})$. On the other hand, this can be checked via the genus theory. Recall from the genus theory that $h(-4n) = h(-56) = 4$ and the number of proper equivalence classes of genera is $|C(-56)/C(-56)^2| = 2^{\mu - 1} = 2$. These force $C(-56) \cong \mathbb{Z}/4\mathbb{Z}$.

Lemma 3. *Let K be a number field and $L = K(\sqrt{u})$ a quadratic extension for $u \in \mathcal{O}_K$. Take $\mathfrak{p} \subseteq \mathcal{O}_K$ a prime. Then*

(1) *whenever $2u \notin \mathfrak{p}$, $\mathfrak{p}$ is unramified.*
(2) *if for some $b, c \in \mathcal{O}_K$, $u = b^2 - 4c \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified.*

Proof. For (1), note that the minimal polynomial for $\sqrt{u}$ is $f = x^2 - u$ with $\mathrm{disc}(f) = 4u$. Since $p \nmid 2u$ we get $p \nmid \mathrm{disc}(f)$, so that f is separable modulo $\mathfrak{p}$. For (2), the polynomial $f = x^2 + bx + c$ has root $(-b \pm \sqrt{u})/2 = \alpha$ such that $L = K(\alpha)$. We also have $\mathfrak{p} \nmid \mathrm{disc}(f) = u$ and again $\mathfrak{p}$ is unramified. $\square$

Let us resume on the example with $n = 14$. The claim that L/K is the Hilbert class field of K in Example 2 follows from two assertions:

- K_1/K is unramified, and
- L/K_1 is unramified.

For the first one, we have $K_1 = K(\sqrt{2})$ with $u = 2$. So $\mathfrak{p}$ is unramified in K_1 if $p \nmid 2$. Suppose $2 \in \mathfrak{p}$. As $\sqrt{-14} \in K$ we get $\sqrt{-7} \in K_1$. However, $-7 \notin$ for $u = -1 = 1^4 = 4 \cdot 2$. By Lemma 3(2) $\mathfrak{p}$ is still unramified. For the second assertion, let $u = 2\sqrt{2} - 1$, $u' = -2\sqrt{2} - 1$ and $L = K_1(\sqrt{2\sqrt{2} - 1})$. Then $\sqrt{u} \cdot \sqrt{u'} = \sqrt{-7} \in K_1$ and thus $u' \in L = K_1(u) = K_1(u')$. If $2 \in \mathfrak{p}$ then $u = (1 + \sqrt{2})^2 - 4 \notin \mathfrak{p}$. By Lemma 3(2) $\mathfrak{p}$ is unramified. If $2 \notin \mathfrak{p}$ then $u \notin \mathfrak{p}$ or $u' \notin \mathfrak{p}$. It suffices to check for the case $u' \notin \mathfrak{p}$, which implies $2u' \notin \mathfrak{p}$; so $\mathfrak{p}$ is unramified as

Date: November 6, 2020.

well by Lemma 3(1). To summarize, we have proved that L/K is the Hilbert class field of K.

For $\alpha = \sqrt{2\sqrt{2}-1}$, its monic minimal polynomial over K is $f(x) = (x^2+1)^2 - 8 = x^4 + 2x^2 - 7$ with $\mathrm{disc}(f) = -2^{14}\cdot 7$.

Corollary 4. *Let $p \neq 7$ be an odd prime. Then $p = x^2 + 14y^2$ if and only if $\left(\frac{-14}{p}\right) = 1$ and $x^2 + 2x^2 - 7 \equiv 0 \bmod p$ has a solution.*

2. Genus theory revisited via the Hilbert class field

Let K be an imaginary quadratic extension of $\mathbb{Q}$. Let d_K denote the discriminant of $K/\mathbb{Q}$. Recall from Theorem 11 in Lecture 9 that

$$C(d_K) \simeq C(\mathcal{O}_K) \cong \mathrm{Gal}(L/K).$$

Here L is the Hilbert class field of K. By the genus theory there is an important subgroup $C(d_K)^2$ contained in $C(d_K)$.

Definition 5. The *genus field* of K is a subextension M of K contained in $L = K^{\mathrm{Hilb}}$ given by $\mathrm{Gal}(L/M) \cong C(\mathcal{O}_K)^2$.

$$\begin{tikzcd} L \arrow[d, dash, "C(\mathcal{O}_K)^2"] \arrow[dd, dash, bend right=60, "C(\mathcal{O}_K)"'] \\ M = \text{genus field} \arrow[d, dash] \\ K \end{tikzcd}$$

Here comes a reformulation of the elementary genus theory in terms of the genus field. Fix $L/M/K$ as before. For each odd prime p denote $p^* = (-1)^{\frac{p-1}{2}}p \equiv 1 \bmod 4$.

Theorem 6. *Denote μ the number of primes dividing d_K. Let $p_1, \dots, p_r$ be all odd primes dividing d_K. Then*

(1) *The genus field of K is the maximal unramified extension of K which is an abelian extension of $\mathbb{Q}$.*[1]
(2) *The genus field $M = K(\sqrt{p_1^*}, \dots, \sqrt{p_r^*})$.*
(3) *The number of genera of discriminant d_K equals*
$$2^{\mu-1} = |C(\mathcal{O}_K)/C(\mathcal{O}_K)^2| = |\mathrm{Gal}(M/K)|.$$
(4) *The principal genus consists of square classes, i.e. the image of elements in $C(d_K)^2$.*

Proof of (1). Since $L/\mathbb{Q}$ is Galois, we see $\mathrm{Gal}(L/\mathbb{Q})$ is generated by $\mathrm{Gal}(L/K)$ together with τ, where τ is the complex conjugation. Suppose N is another subextension of L/K and $N/\mathbb{Q}$ is abelian. Then $\mathrm{Gal}(L/N)$ contains the commutator subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, which is

$$\langle \tau g \tau^{-1} g^{-1} \rangle_{g \in \mathrm{Gal}(L/K)} = \left\langle \tau \left(\frac{L/K}{\mathfrak{p}}\right) \tau^{-1} \left(\frac{L/K}{\mathfrak{p}}\right)^{-1} \right\rangle_{\mathfrak{p} \in I_K}.$$

[1]cf. The Hilbert class field is the maximal unramified abelian extension of K. Caution: $C(\mathcal{O}_K)^2$ is abelian as $C(\mathcal{O}_K)$ is; but the semi-direct product of two abelian groups is in general not necessarily abelian. Hence a priori $M \neq L$ in general.

Also, for each $\mathfrak{p} \in I_K$, since $\mathfrak{p}\overline{\mathfrak{p}}$ is principal, we have $\mathfrak{p} = \overline{\mathfrak{p}}^{-1}$ in the ideal class group. Therefore,

$$\tau \left(\frac{L/K}{\mathfrak{p}}\right) \tau^{-1} = \left(\frac{L/K}{\tau(\mathfrak{p})}\right) = \left(\frac{L/K}{\overline{\mathfrak{p}}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)^{-1}.$$

And then

$$\left\langle \tau \left(\frac{L/K}{\mathfrak{p}}\right) \tau^{-1} \left(\frac{L/K}{\mathfrak{p}}\right)^{-1} \right\rangle_{\mathfrak{p}\in I_K} = \left\langle \left(\frac{L/K}{\mathfrak{p}}\right)^{-2} \right\rangle_{\mathfrak{p}\in I_K} = \mathrm{Gal}(L/K)^2.$$

So $N \subseteq M$ and $M/\mathbb{Q}$ is abelian. $\square$

Now we are working on the proof of (2) for $M = K(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*})$. Notice that

$$\mathrm{Gal}(M/\mathbb{Q}) = \mathrm{Gal}(L/\mathbb{Q})/C(\mathcal{O}_K)^2 = \langle \mathrm{Gal}(M/K), \tau \rangle.$$

As $\mathrm{Gal}(M/K) \simeq C(\mathcal{O}_K)/C(\mathcal{O}_K)^2$, we see every element of $\mathrm{Gal}(M/\mathbb{Q})$ is of order 1 or 2. Therefore,

$$\mathrm{Gal}(M/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^m$$

for some integer $m \geqslant 1$. This implies that M is a compositum of quadratic extensions of $\mathbb{Q}$. Lemma 7 will be applied to the following tower diagram.

$$\begin{tikzcd}[column sep=small]
 & K(\sqrt{a}) \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbb{Q}(\sqrt{a}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Lemma 7. *Let L, M be two abelian extensions of a number field K. Fix $\mathfrak{p} \subseteq \mathcal{O}_K$ an odd prime. Then*

(1) *$\mathfrak{p}$ is unramified in LM if and only if $\mathfrak{p}$ is unramified in both L and M respectively.*
(2) *If $\mathfrak{p}$ is unramified in LM, then the natural group homomorphism*

$$\begin{aligned} \mathrm{Gal}(LM/K) &\longrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K) \\ \left(\frac{LM/K}{\mathfrak{p}}\right) &\longmapsto \left(\left(\frac{L/K}{\mathfrak{p}}\right), \left(\frac{M/K}{\mathfrak{p}}\right)\right) \end{aligned}$$

is injective.

The proof of Lemma 7(1) can be reduced to prove $[L:K][M:K] = [LM:K]$. For this, we construct

$$\begin{aligned} \mathrm{Gal}(LM/K) &\longrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K) \\ \sigma &\longmapsto \left(\left(\frac{L/K}{\mathfrak{p}}\right), \left(\frac{M/K}{\mathfrak{p}}\right)\right) \end{aligned}$$

for σ such that $\sigma(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{p}$ and prove this is an isomorphism.

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