LECTURE NOTES ON ANT (PART II)- SUMMER SCHOOL 2019

YE TIAN

In the later half of this course, we will mainly study quadratic fields and cyclotomic fields. For quadratic fields, we will introduce Gauss' reduction theory of quadratic forms to study ideal class groups and unit group; and use Eisenstein series to give meromorphic continuation of Dedekind zeta functions and residue formula; and complex multiplication gives the explicit construction of class fields of imaginary quadratic fields. For cyclotomic field, we introduce Stickelberger' s theorem and Thaine's theorem, and the proof of Catalan's conjecture as an application.

For a quadratic field K of fundamental discriminant D, let $\chi_D = \left(\frac{D}{\cdot}\right) : (\mathbb{Z}/D\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ be the associated quadratic character of conductor $|D|$. Sometime we also write $\mathrm{Cl}_D, h_D, \epsilon_D$ for the ideal class group Cl_K, ideal class number h_K, and fundamental units ϵ_K (when $D > 0$).

Contents

1. Lecture I: The equation $y^2 + 14 = x^3$

We review what we have studied in the last two weeks via the following Diophantine equation

$$y^2 + 14 = x^3, \qquad \text{with } x, y \in \mathbb{Z}.$$

Let $K = \mathbb{Q}(\sqrt{-14})$ and $\mathcal{O} = \mathbb{Z}[\sqrt{-14}]$ its ring of integers. The equation factors as an equality of ideals of $\mathcal{O}$

$$(y + \sqrt{-14})(y - \sqrt{-14}) = (x)^3.$$

We claim that the principal ideals of $\mathcal{O}$

$$(y + \sqrt{-14}), \qquad (y - \sqrt{-14})$$

must be co-prime. Otherwise, let $\mathfrak{p}$ be a common prime divisor. Then $y \pm \sqrt{-14} \in \mathfrak{p}$ and therefore $2\sqrt{-14} \in \mathfrak{p}$, $\mathfrak{p}|2$ or 7. On the other hand, $\mathfrak{p}|(y + \sqrt{-14})$ implies that $\mathrm{N}\mathfrak{p}|y^2 + 14$ so that $\mathfrak{p}$ is coprime to $2, 7$ since $2, 7 \nmid y$. It is now a contradiction. It follows that

$$(y + \sqrt{-14}) = \mathfrak{a}^3$$

for some ideal $\mathfrak{a}$ of $\mathcal{O}$. But the ideal class number of K is 4, then $\mathfrak{a}$ itself is a principal. Moreover $\mathcal{O}^\times = \{\pm 1\}$, so the element $y + \sqrt{-14}$ is a cubic of an element in $\mathcal{O}$, say

$$y + \sqrt{-14} = (a + \sqrt{-14}b)^3, \qquad \text{for some } a, b \in \mathbb{Z}.$$

It follows that $1 = 3a^2b - 14b^3 = b(3a^2 - 14b^2)$, and then $b = \pm 1$ and $3a^2 = 15, 13$. It is impossible.

Summary. For any number field K, the following exact sequence is fundamental

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \longrightarrow I_K \longrightarrow \mathrm{Cl}(K) \longrightarrow 0,$$

where I_K is the group of non-zero fractional ideals of K, which is free abelian group with bases all non-zero prime ideals; the unit group $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r_1 + r_2 - 1$; and the ideal class group $\mathrm{Cl}(K)$ is a finite abelian group. (These invariants are useful for some Diophantine equations; The relation of ideal class number and L-values is given by the class number formula, which is useful for many questions:

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}}.$$

when $K/\mathbb{Q}$ is Galois sometime we even need to know the $\mathrm{Gal}(K/\mathbb{Q})$-module structure of $\mathrm{Cl}(K)$ and $\mathcal{O}_K^\times$. A typical example is the proof of Catalan's conjecture. Let's recall the proof of finiteness of ideal class number and discuss ideal class number of imaginary quadratic field.

Let K be a number field. Note that for any $M \geq 1$, there exist only finite many integral ideals of $\mathcal{O}_K$ with norm bounded by M. Thus enough to show exists a constant M_K only depends on K such that for any fractional ideal $\mathfrak{a}$, exists $\alpha \in \mathfrak{a}$ such that $|\mathrm{N}(\alpha)| \leq M_K \mathrm{N}(\mathfrak{a})$, i.e. $\mathrm{N}(\alpha\mathfrak{a}^{-1}) < M_K$. Consider the embedding

$$K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n, \qquad n = [K : \mathbb{Q}]$$

Here the last isomorphism is given by maps $z = x + yi \in \mathbb{C}$ to $(x, y) \in \mathbb{R}^2$. A fractional ideal $\mathfrak{a}$ can be viewed as a lattice in $\mathbb{R}^n$. Consider the following centrally symmetric convex connected region

$$S_t = \Big\{(x, z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \;\Big|\; \sum_{i=1}^{r_1} |x_i| + \sum_{j=1}^{r_2} 2|z_j| \leq t\Big\}.$$

If $\mathrm{Vol}(S_t) = 2^n \mathrm{Vol}(\mathbb{R}^n/\mathfrak{a})$ (or equivalently $t^n \mathrm{Vol}(S_1) = 2^n \mathrm{Vol}(\mathbb{R}^n/\mathcal{O}_K)\mathrm{N}(\mathfrak{a})$), then S_t contains a non-zero $\alpha \in \mathfrak{a}$ (one may think to choose other symmetric domain) so that

$$|\mathrm{N}(\alpha)| \leq \left(\frac{t}{n}\right)^n = \frac{2^n \mathrm{Vol}(\mathbb{R}^n/\mathcal{O}_K)}{n^n \mathrm{Vol}(S_1)} \cdot \mathrm{N}\mathfrak{a}.$$

Thus we obtain a desired constant

$$M_K = \frac{2^n \mathrm{Vol}(\mathbb{R}^n/\mathcal{O}_K)}{n^n \mathrm{Vol}(S_1)}.$$

For K imaginary quadratic field with discriminant d_K (so that $\mathcal{O}_K$ has a $\mathbb{Z}$-basis $1, (d_K + \sqrt{d_K})/2$ in $\mathbb{C}$ and thus $(1, 0), (d_K/2, \sqrt{|d_K|}/2)$ in $\mathbb{R}^2$), we have

$$\mathrm{Vol}(S_1) = \frac{\pi}{4}, \quad \mathrm{Vol}(\mathbb{R}^2/\mathcal{O}_K) = \sqrt{|d_K|}/2, \quad M_K = \frac{2}{\pi}\sqrt{|d_K|}.$$

Thus for an imaginary quadratic field K, Cl_K consists of ideal classes of integral ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $\mathrm{N}(\mathfrak{a}) \leq \frac{2}{\pi}\sqrt{|d_K|}$. Example, for $K = \mathbb{Q}(\sqrt{-14})$, we have $M_K < 5$ and therefore one can find that the ideal class of $\mathfrak{p} = (3, 1 + \sqrt{-14})$ is of order 4 and generates Cl_K. In general, one can show that

$$M_K = = \frac{n!(4/\pi)^{r_2}}{n^n} \cdot \sqrt{|d_K|}.$$

Proposition 1.1. *Let $D < 0$ be a fundamental discriminant of an imaginary quadratic field K. Then*

$$ax^2 + bxy + cy^2 \leftrightsquigarrow \tau = \frac{-b + \sqrt{D}}{2a} \leftrightsquigarrow \Big(a, (b + \sqrt{D})/2\Big)$$

induces a bijection among

1. $\mathrm{SL}_2(\mathbb{Z})$*-equivalence classes of primitive positive definite quadratic forms of discriminant D;*
2. *imaginary quadratic points in fundamental domain of $\mathcal{H}$ by $\mathrm{SL}_2(\mathbb{Z})$ with minimal integral polynomial with discriminant D.*
3. *the ideal class group of K;*

Moreover, in (1) any integral primitive definite positive binary quadratic form of discriminant D is $\mathrm{SL}_2(\mathbb{Z})$-equivalent (or properly equivalent) to a unique reduced form $ax^2 + bxy + cy^2$ in the sense

$$|b| \leq a \leq c, \text{ and } b \geq 0 \text{ if either } a = |b| \text{ or } a = c.$$

In (2), any quadratic number τ in the upper plane $\mathcal{H}$ with discriminant D is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to a unique point in the domain F:

$$\mathrm{Re}(\tau) \in (-1/2, 1/2], \ |\tau| \geq 1, \quad \text{if } |\tau| = 1 \text{ then } \mathrm{Re}(\tau) \geq 0.$$

The above correspondence maps reduced forms to quadratic points in the fundamental domain F.

Remark. Note that $b^2 + |D| = 4ac \geq 4b^2$. Thus $3b^2 \leq |D|$. This shows that the number of reduced forms and therefore ideal class number is finite. It gives rise to another proof of finiteness of ideal class number for imaginary quadratic fields.

Example. Let $D = -56$, then the corresponding (reduced) quadratic forms are

$$x^2 + 14y^2; \qquad 2x^2 + 7y^2; \qquad 3x^2 \pm 2xy + 5y^2.$$

The corresponding quadratic points in F are $\sqrt{-14}, \sqrt{-14}/2, (\pm 1 + \sqrt{-14})/3$ and corresponding ideals are

$$\mathcal{O}_K, \qquad (2, \sqrt{-14}), \qquad (3, \pm 1 + \sqrt{-14}).$$

Let $\mathcal{H}$ denote the upper half plane. Prove that the Eisenstein series defined by

$$E(z, s) = \pi^{-s}\Gamma(s) \cdot \frac{1}{2} \sum_{(m,n)\neq(0,0)} \frac{y^s}{|mz + n|^{2s}}, \qquad z = x + iy \in \mathcal{H}$$

is absolutely convergent if $\mathrm{Re}(s) > 1$, has meromorphic continuation to the whole s-plane; it is analytic except at $s = 0, 1$ where it has simple poles. The residue $\mathrm{Res}_{s=1} E(z, s) = \frac{1}{2}$ independent of z. The Eisenstein series satisfies the functional equation

$$E(z, s) = E(z, 1 - s).$$

Moreover, $E(x + iy, s) = O(y^\sigma)$ as $y \to \infty$ where $\sigma = \max(\mathrm{Re}(s), 1 - \mathrm{Re}(s))$. The function $E(z, s)$ in z is automorphic i.e.

$$E(\gamma z, s) = E(z, s), \qquad \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Let $D < 0$ be a fundamental discriminant of an imaginary quadratic field K and w_K the number of roots of unity in K. Then we have

$$\left(\frac{\sqrt{|D|}}{2\pi}\right)^s \Gamma(s)\zeta_K(s) = \frac{2}{w_K} \cdot \sum_{\substack{b^2-4ac=D,\\ -a<b\leq a\leq c \text{ or } 0<b\leq a=c}} E\left(\frac{-b + \sqrt{D}}{2a}, s\right).$$

Compare residues at $s = 1$ on both sides, we have

Theorem 1.2 (Dirichlet)**.** *Let K be an imaginary quadratic field. Then we have that*

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2\pi}{w_K\sqrt{|d_K|}} \cdot h_K.$$

Exercise. 1. Daniel Bump, *Automorphic Forms and Representations*, Chapter 1, §6 Ex 1.6.1-1.6.2. and prove the equality above between sum of evaluations of $E(z, s)$ at quadratic points and $\zeta_K(s)$.

2. Let χ_K be the quadratic character modulo $|d_K|$ such that $\chi_K(p) = 1$ (resp -1) iff p is split (resp. inert) over K. Recall that

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \qquad \zeta_K(s) = \sum_{0\neq\mathfrak{a}\subset\mathcal{O}_K} \mathrm{N}\mathfrak{a}^{-s}, \qquad L(\chi_K, s) = \sum_{n=1}^{\infty} \chi_K(n)n^{-s}.$$

Then $\zeta_K(s) = \zeta(s)L(\chi_K, s)$ and $\mathrm{Res}_{s=1}\, \zeta_K(s) = L(\chi_K, 1)$. Deduce that for imaginary quadratic field K of discriminant D and ideal class number h_K (or denoted as h_D). We have

$$h_K = \frac{w_K}{2(2 - \chi(2))} \cdot \sum_{1\leq a<|D|/2} \chi(a).$$

Using this formula compute the ideal class number of $\mathbb{Q}(\sqrt{-14})$. Let $p \equiv 3 \mod 4$ be a prime. Prove that there are more quadratic residue more than non-residue in the interval $(0, p/2)$.

3. Let $K = \mathbb{Q}(\sqrt{-17})$. Compute the ideal class number using (i) Minkowski constant M_K; (ii) Gauss' reduced forms; (iii) Dirichlet's class number formula above. Moreover, find the Hilbert class field of K.

Based on Dirichlet formula, we have

Theorem 1.3 (Siegel)**.** *For any $\epsilon > 0$, $h_D \gg |D|^{1/2-\epsilon}$.*

In particular, for any given $h \in \mathbb{Z}_{\geq 1}$, there are only finitely many imaginary quadratic fields with ideal class number h. A problem is that the constant in the above estimation is not effective, how can one determines those field? D. Goldfeld solved this problem.

2. Lecture II-III: Primes of form $p = x^2 + ny^2$ and Class Field Theory

Now we consider the second question. It is clear that $2, 7$ is not form $x^2 + 14y^2$. Let $p \nmid 14$ be a prime of form $p = x^2 + 14y^2$. Then $p \nmid xy$, and therefore -14 is a quadratic residue modulo p; equivalently, p is complete split in $K = \mathbb{Q}(\sqrt{-14})$. Furthermore,

$$p = x^2 + 14y^2 = (x + \sqrt{-14}y)(x - \sqrt{-14}y)$$

implies the two (distinct) prime ideals of K above p are principal, generated by $x \pm \sqrt{-14}y$. How to describe principal ideal of K? there is a way through class field theory (Important things should be repeated three times (30 times)).

Remark. We make a remark on Galois Group of Number Field Extension. Let L/K be a finite Galois extension of number fields. How to describe the elements in its Galois group $\mathrm{Gal}(L/K)$? There are two ways.

- Explicit way: The L must be a splitting field of a polynomial f over K. Thus the Galois group $\mathrm{Gal}(L/K)$ can be realized as a subgroup of the permutation group of the roots of f;
- For each primes $\mathfrak{P}|\mathfrak{p}$ of L/K unramified, $\mathrm{Frob}_{L/K}(\mathfrak{P}) \in \mathrm{Gal}(L/K)$ is the unique element fixing $\mathfrak{P}$ and induces the Frobenius morphism in the Galois of residue field extension $k(\mathfrak{P})/k(\mathfrak{p})$. For any $\sigma \in \mathrm{Gal}(L/K)$, we have

  $$\sigma \cdot \mathrm{Frob}_{L/K}(\mathfrak{P}) \cdot \sigma^{-1} = \mathrm{Frob}_{L/K}(\sigma\mathfrak{P}).$$

  Thus, the prime $\mathfrak{p}$ of K defines a conjugacy class of $\mathrm{Gal}(L/K)$, denoted by $\mathrm{Frob}_{L/K}(\mathfrak{p})$. For a given conjugacy class C of $G = \mathrm{Gal}(L/K)$, the density of prime ideals $\mathfrak{p}$ of K with $\mathrm{Frob}_{L/K}(\mathfrak{p}) = C$ is $|C|/|G|$. When L/K is abelian, then $\mathrm{Frob}_{L/K}(\mathfrak{P})$ only dependents on $\mathfrak{p}$, and is also denoted by $\mathrm{Frob}_{L/K}(\mathfrak{p})$.

Recall that we say a finite Galois extension L/K is unramified at a prime ideal $\mathfrak{p}$ of K (resp. a real embedding σ, also called a real place) if the ramification index of any prime $\mathfrak{P}$ of L above $\mathfrak{p}$ is one (resp. any extension of σ to L is still real). If L/K is unramified at all prime ideals of K and all real embeddings, then we call L/K is an unramified extension or unramified everywhere. Example, $\mathbb{Q}(\sqrt{-3}, i)/\mathbb{Q}(\sqrt{3})$ is ramified at the real places.

Theorem 2.1. *Let K be a number field. There is a finite Galois extension H of K such that*

- *H is an unramified (including ∞) abelian extension of K;*
- *any unramified abelian extension of K lies in H.*

The field H (called the Hilbert class field of K) is the maximal unramified abelian extension of K and is clearly unique. Moreover, the group homomorphism

$$I_K \longrightarrow \mathrm{Gal}(H/K), \qquad \mathfrak{p} \mapsto \mathrm{Frob}_{H/K}(\mathfrak{p})$$

is surjective with kernel P_K. Thus it induces an isomorphism, called Artin map,

$$\mathrm{Art} : \mathrm{Cl}_K \xrightarrow{\sim} \mathrm{Gal}(H/K).$$

In particular, a prime $\mathfrak{p}$ of K is principal iff $\mathfrak{p}$ is completely split over H.

For the number field $K = \mathbb{Q}(\sqrt{-14})$, we have seen that $\mathrm{Cl}(K) \cong \mathbb{Z}/4\mathbb{Z}$. The genus field of K is $L := K(\sqrt{-7}) = K(\sqrt{2})$ (i.e. the one contained in H and abelian over $\mathbb{Q}$), and therefore $H = L(\alpha)$; one may choose $\alpha = \sqrt{u}$ and $u \in L \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$ and then one can show that $u = 2\sqrt{2} - 1$ is a desired one. The minimal polynomial of α over K (and also over $\mathbb{Q}$) is $X^4 + 2X^2 - 7 = 0$, which discriminant $\mathrm{disc}(\alpha) = -\mathrm{N}_{H/K} f'(\alpha) = -7 \cdot 2^{14}$ only has prime factors 2 and 7; thus for any prime $\mathfrak{p} \nmid 14$ of K, $\mathfrak{p}$ is complete split over H_K iff

$$X^4 + 2X^2 - 7 \equiv 0 \mod \mathfrak{p}$$

has a solution (and then all solutions) over $\mathcal{O}_K$. If $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$ is split in $K/\mathbb{Q}$, then $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$ and it is equivalent to require

$$X^4 + 2X^2 - 7 \equiv 0 \mod p$$

has a solution in $\mathbb{Z}$. Now we conclude that

- A prime p has form $p = x^2 + 14y^2$ iff p completely splits over H_K with $K = \mathbb{Q}(\sqrt{-14})$; By density theorem (which we will state later), we also know that primes of form $x^2 + 14y^2$ has density $1/8 = 1/|\mathrm{Gal}(H_K/K)|$.

- A prime p has form $p = x^2 + 14y^2$ iff $\left(\frac{-14}{p}\right) = 1$ and $X^4 + 2x^2 - 7 \equiv 0 \mod p$ has an integral solution $a \in \mathbb{Z}$. (For a given prime p, how to determine whether this condition holds? It relates to the question: determine the solvability of $x^2 \equiv a \ modp$ and actually find a solution in $\mathbb{F}_p$).

Remark. Starting with the CFT isomorphism, A. Smith showed that for any finite abelian group A of cardinality power of 2, imaginary quadratic fields K with $\mathrm{Cl}_K[2^\infty] \cong A$ has positive density according to discriminants.

Exercise. Can you find infinitely many abelian extensions L over K with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z}$?

Exercise. Let L be s splitting field over $\mathbb{Q}$ of the polynomial $x^5 - x + 1$. Show that L contains a unique real quadratic field $F = \mathbb{Q}(\sqrt{19 \cdot 151})$ and L/F is Galois extension of Galois group A_5 and unramified everywhere.

How about replacing 14 by general positive integer n and consider primes of form $x^2 + ny^2$? The decomposition

$$p = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$$

show that p splits in $K = \mathbb{Q}(\sqrt{-n})$ and the primes $\mathfrak{p}$ of K above p is principal with generator of form $\alpha = x + \sqrt{-n}y \in \mathcal{O}_K$; If write $-4n = d_K f^2$, then

$$\alpha \equiv a \mod f\mathcal{O}_K$$

with some $a \in \mathbb{Z}$. Thus $\mathfrak{p}$ completely split over H_K is just a necessary condition. We are looking for a larger class field related to the above condition.

Let L/K be a Galois extension of number fields with Galois group G. Let $\mathfrak{p}$ be a non-zero prime of K. Then G acts transitively on the finite set $\Sigma = \{\mathfrak{P}_1, \cdots, \mathfrak{P}_g\}$ of primes of L above $\mathfrak{p}$, i.e. with $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$. Let $\mathfrak{P} = \mathfrak{P}_i \in \Sigma$.

- $D_{\mathfrak{P}} = \{\sigma \in G |\ \sigma(\mathfrak{P}) = \mathfrak{P}\}$ is a subgroup of G, called the decomposition group of $\mathfrak{P}$; There is a natural group homomorphism

$$D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}\left(\frac{k(\mathfrak{P})}{k(\mathfrak{p})}\right)$$

  is surjective; denote by $I_{\mathfrak{P}}$ its kernel. Then $\mathfrak{P}/\mathfrak{p}$ is unramified iff $I_{\mathfrak{P}} = 1$, and iff $\mathfrak{p} \nmid \mathrm{disc}_{L/K}$. In this case, the homomorphism is an isomorphism. For any prime $\mathfrak{p}$ unramified over L, let $\mathrm{Frob}_{L/K}(\mathfrak{P}) \in D_{\mathfrak{P}}$ denote the element mapping to the Frobenius in the Galois group of residue field extension under this isomorphism. If $\mathrm{Frob}_{L/K}(\mathfrak{P}) = 1$, then $\mathfrak{p}$ is completely split over L, i.e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ with $g = [L : K]$.
- For any $\sigma \in G$, $D_{\sigma\mathfrak{P}} = \sigma D_{\mathfrak{P}} \sigma^{-1}$ and moreover, $\mathrm{Frob}_{L/K}(\sigma\mathfrak{P}) = \sigma \mathrm{Frob}_{L/K}\mathfrak{P}\sigma^{-1}$. Let $\mathrm{Fr}_{L/K}(\mathfrak{p})$ denote its conjugacy class. Let S denote the finite set of primes ramified over L (equivalently, $\mathfrak{p} | \mathrm{disc}_{L/K}$) and $\mathcal{P}(S)$ the set of non-zero prime ideals not in S. Thus we have a map

$$\mathcal{P}(S) \longrightarrow \mathrm{Gal}(L/K)/\sim, \qquad \mathfrak{p} \mapsto \mathrm{Frob}_{L/K}(\mathfrak{p})$$

  Here $\sim$ means conjugacy equivalence.

  Theorem 2.2. *Let C be a conjugacy class of G, then the subset of $\mathcal{P}(S)$ of prime ideals $\mathfrak{p}$ with $\mathrm{Frob}_{L/K}(\mathfrak{p}) = C$ has density $|C|/|G|$.*

  Corollary 2.3. *Suppose $L_i \subset \overline{K}, i = 1, 2$ are two finite Galois extension of number field K and let Σ_i be the set of primes of K completely split in L_i. If there exists a finite set S of primes of K such that $\Sigma_1 \setminus S = \Sigma_2 \setminus S$, then $L_1 = L_2$.*

  When L/K is finite abelian. Let $I_K(S)$ be the group of fractional ideals generated by primes coprime to S. Then the above map induces a group homomorphism (called Artin map)

$$\mathrm{Art} : I_K(S) \longrightarrow \mathrm{Gal}(L/K), \qquad \prod_i \mathfrak{p}_i^{n_i} \mapsto \prod_i \mathrm{Frob}_{H_{\mathfrak{m}}/K}(\mathfrak{p}_i)^{n_i}.$$

- Let $\mathfrak{m}_f$ be an integral ideal of K, $\mathfrak{m}_\infty$ a set of some real embeddings of K, and write $\mathfrak{m} = \mathfrak{m}_f\mathfrak{m}_\infty$. Let $I_{\mathfrak{m}}$ denote the group of fraction ideals whose support disjoint from $\mathfrak{m}_f$ and let $P_{\mathfrak{m}} \subset I_{\mathfrak{m}}$ the subgroup of principal ideals (α) with generator $\alpha \equiv 1 \mod m_f$ (i..e for any $\mathfrak{p}|m_f$, $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(m_f)$ and $\sigma(\alpha) > 0$ for any $\sigma \in m_\infty$. We call $\mathrm{Cl}_{K,\mathfrak{m}} := I_{\mathfrak{m}}/P_{\mathfrak{m}}$ the generalized ideal class group modulo $\mathfrak{m}$. When $m = 1$, $\mathrm{Cl}_{K,\mathfrak{m}}$ is the ideal class group Cl_K of K. The generalized ideal class group is finite abelian group.

Denote $K_{\mathfrak{m}_f}^\times$ the subgroup of $K^\times$ which is units at $\mathfrak{m}_f$ and $K_{\mathfrak{m},1}^\times$ the subgroup of $K_{\mathfrak{m}}$ that congruent to 1 modulo $\mathfrak{m}$ (so that under $\sigma \in m_\infty$ is positive). Then we have the following exact sequence

$$0 \to \mathcal{O}_K^\times/\mathcal{O}_K^\times \cap K_{\mathfrak{m},1}^\times \to K_{\mathfrak{m}_f}^\times/K_{\mathfrak{m},1}^\times \to \mathrm{Cl}_{K,\mathfrak{m}} \to \mathrm{Cl}(K) \to 1.$$

In particular, $\#\mathrm{Cl}_{K,\mathfrak{m}}$ is finite. We also have a canonical isomorphism

$$K_{\mathfrak{m}}^\times/K_{\mathfrak{m},1}^\times \simeq \{\pm 1\}^{\#m_\infty} \times (\mathcal{O}_K/\mathfrak{m}_f)^\times.$$

- The maximal abelian extension H_K over K is finite over K, and moreover, the Artin map induces an isomorphism $\mathrm{Cl}_K \xrightarrow{\sim} \mathrm{Gal}(H_K/K)$. Together with Galois theory, it gives a bijection between subgroup of I_K containing P_K and the subfields of H_K (i.e. all unramified abelian extensions over K). In general, we have

  Theorem 2.4 (Class Field Theory)**.** *For a given $\mathfrak{m} = \mathfrak{m}_f\mathfrak{m}_\infty$, there exists a unique finite abelian extension $H_{\mathfrak{m}}$ (unramified outside $\mathfrak{m}$) such that the Artin map, which is surjective,*

$$\mathrm{Art}: \ I_{\mathfrak{m}} \longrightarrow \mathrm{Gal}(H_{\mathfrak{m}}/K), \qquad \prod_i \mathfrak{p}_i^{n_i} \mapsto \prod_i \mathrm{Frob}_{H_{\mathfrak{m}}/K}(\mathfrak{p}_i)^{n_i}$$

  has kernel exactly $P_{\mathfrak{m}}$. The induced isomorphism $I_{\mathfrak{m}}/P_{\mathfrak{m}} \cong \mathrm{Gal}(H_{\mathfrak{m}}/K)$ and Galois theory gives rise to a bijection between subgroups Q: $P_{\mathfrak{m}} \subset Q \subset I_{\mathfrak{m}}$ and subfields L: $K \subset L \subset H_{\mathfrak{m}}$ so that $Q = P_{\mathfrak{m}}\mathrm{N}_{L/K}(I_{\mathfrak{m}}(L))$ and $I_{\mathfrak{m}}/P_{\mathfrak{m}}\mathrm{N}_{L/K}I_{\mathfrak{m}}(L) \cong \mathrm{Gal}(L/K)$ under Artin map. If $\mathfrak{m}|\mathfrak{m}'$, then $H_{\mathfrak{m}} \subset H_{\mathfrak{m}'}$.

  Any finite abelian extension L over K is contained in some $H_{\mathfrak{m}}$. The maximal such $\mathfrak{m}$ is called the conductor of L, denoted by $\mathfrak{f}_{L/K}$. We have that $\mathfrak{p}|\mathfrak{f}_{L/K}$ iff $\mathfrak{p}$ is ramified over L. (Note that not all $\mathfrak{m}$ can be conductor).

  A congruence subgroup Q (over K) modulo $\mathfrak{m}$ is a subgroup of $I_{\mathfrak{m}}$ containing $P_{\mathfrak{m}}$. Call congruence subgroups Q_i modulo $\mathfrak{m}_i$ are equivalent if there exists $\mathfrak{m}$ divisible by $\mathfrak{m}_i, i = 1, 2$ such that $I_{\mathfrak{m}} \cap Q_1 = I_{\mathfrak{m}} \cap Q_2$ (so that if we call the intersection Q then $I_{\mathfrak{m}_1}/Q_1 \cong I_{\mathfrak{m}}/Q \cong I_{\mathfrak{m}_2}/Q_2$). Denote by $[Q]$ the equivalence class of Q. There are one-to-one correspondence between finite abelian extensions L over K and congruence subgroup classes $[Q]$ over K.

  It will be very convenient if use adéliclanguage. Note that let $U_{\mathfrak{m}} \subset \mathbb{A}_K^\times$ be the modulo $\mathfrak{m}$ congruence subgroup, then there is a canonical isomorphism $\mathbb{A}_K^\times/K^\times U_{\mathfrak{m}}$ onto $I_{\mathfrak{m}}/P_{\mathfrak{m}}$. There is a one-to-one correspondence between finite abelian extensions over K and idéle class groups over K.
- Let $L \subset H_{\mathfrak{m}}$ be an abelian extension over K corresponding to group $Q : P_{\mathfrak{m}} \subset Q \subset I_{\mathfrak{m}}$ so that the Artin morphism

$$I_{\mathfrak{m}}/Q \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

  Then for any $\sigma \in \mathrm{Aut}(L)$, we the commutative diagram

$$\begin{array}{ccc} I_{\mathfrak{m}}/Q & \xrightarrow{\sim} & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow \\ \sigma(I_{\mathfrak{m}})/\sigma(Q) & \xrightarrow{\sim} & \mathrm{Gal}(\sigma(L)/\sigma(K)) \end{array}$$

Exercise. 1. Taking $\mathfrak{m} = 1$, then $H_{\mathfrak{m}} = H_K$ is the Hilbert class field and the norm of any ideal of $H_{\mathfrak{m}}$ to K is principal. What is $H_{(2)}$ for $K = \mathbb{Q}$? Recall Kronecker-Weber theorem: any finite abelian extension over $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_N)$.

2. Do you think the following statement is the essential part of CFT: *For a divisor $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ of K, there exists a unique finite abelian extension L (denoted by $H_{\mathfrak{m}}$) over K such that for any prime ideal $\mathfrak{p} \nmid \mathfrak{m}_0$, $\mathfrak{p}$ completely splits over L iff $\mathfrak{p} \in P_{\mathfrak{m}}$. Moreover, the maximal abelian extension K^{ab} over K is union of all $H_{\mathfrak{m}}$'s.*

3. If one is interested in which integers have form $x^2 + ny^2$, note that

$$(x_1 + \sqrt{-n}y_1)(x_2 + \sqrt{-n}y_2) = (x_1x_2 - ny_1y_2) + \sqrt{-n}(x_1y_2 + x_2y_1).$$

Therefore if a, b have such form, then so is ab. But the converse is false in general (What is the condition on n such that the converse is true?)

Recall our question. For a given positive integer n, which primes p can be expressed in the form $p = x^2 + ny^2$ with x, y integers? For primes $p \nmid 4n$, if there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + ny^2$. Then $p \nmid x, y$ and therefore

$$-ny^2 \equiv x^2 \mod p.$$

It follows that $-n$ is a non-zero residue square modulo p, or equivalently by quadratic reciprocity law, p is split in the field $K = \mathbb{Q}(\sqrt{-n})$. Not only this, but

$$p = (x + \sqrt{-n}y)(x - \sqrt{-n}y),$$

any prime $\mathfrak{p}|p$ of K is also a principal ideal. By the class field theory

$$\mathrm{Cl}(K) \longrightarrow \mathrm{Gal}(H_K/K),$$

the prime $\mathfrak{p}$ must be completely split over H_K. It should not be sufficient in general. If replace n by nd^2 with d non-zero integer, the field K, H_K does not change, but the condition becomes more restricted. Taking primes $p \nmid 14$, there exist infinitely many prime $p = 15, 127, \cdots$ such that

$$p = x^2 + 14 \cdot y^2; \qquad p \neq x^2 + 56 \cdot y^2.$$

In fact, the prime ideal $\mathfrak{p}|p$ is not only principal, but if we write $-4n = c^2 d_K$ with d_K the fundamental discriminant of K, then $2|d_K c$ and

$$x + y\sqrt{-n} \equiv x - y \cdot (d_K c/2) \mod \mathfrak{c}, \qquad \mathfrak{c} = c\mathcal{O}_K.$$

Let $I_{\mathfrak{c}}$ denote the group of non-zero fractional ideals of K with support disjoint from c, and let $P_{c,\mathbb{Z}}$ be its subgroup of principal ideals $(\alpha) \in I_{\mathfrak{c}}$ such that $\alpha \equiv a \mod c\mathcal{O}_K$ for some integer $a \in \mathbb{Z}$ (prime to c). The Class field theory tell us that there exists a unique abelian extension L over K, unramified outside $\mathfrak{c}$ and containing the Hilbert class field H_K of K, such that the Artin morphism

$$I_{\mathfrak{c}} \longrightarrow \mathrm{Gal}(L/K),$$

induces an isomorphism $I_{\mathfrak{c}}/P_{c,\mathbb{Z}}(f) \longrightarrow \mathrm{Gal}(L/K)$. Moreover, L is Galois over $\mathbb{Q}$ with generalized dihedral Galois group. Such field is called a ring class field over K of conductor c (Its CFT conductor may not be $\mathfrak{c} := c\mathcal{O}_K$). It is clear that $\mathfrak{p}|p$ is completely split over L. It follows from the above isomorphism, for primes $p \nmid 4n$, if p completely split over L, then a prime ideal $\mathfrak{p}|p$ of K is generated by an element of form $x + y\sqrt{-n}$, thus $p = x^2 + ny^2$.

Theorem 2.5. *The ring class field L over K of conductor c (so that $-4n = d_K c^2$) is the unique number field L Galois over $\mathbb{Q}$ such that*

$$\{p \mid p \text{ completely split over } L\} = \{p \mid p \nmid 4n, p = x^2 + ny^2\}.$$

Proof. We only need to show L is Galois over $\mathbb{Q}$ and the complex conjugation τ acts on $\mathrm{Gal}(L/K)$ via inverse. It is easy to see that for any $\sigma \in \mathrm{Aut}(L)$, $\sigma(I_{\mathfrak{c}}) = I_{\mathfrak{c}}$ and $\sigma(P_{c,\mathbb{Z}}) = P_{c,\mathbb{Z}}$. Thus $\sigma(L) = L$ and thus L is Galois over $\mathbb{Q}$. Moreover,

$$\tau \mathrm{Frob}_{L/K}(\mathfrak{p})\tau = \mathrm{Frob}_{L/K}(\overline{\mathfrak{p}}),$$

but $\mathfrak{p}\overline{\mathfrak{p}} \in P_{c,\mathbb{Z}}$. Thus $\mathrm{Gal}(L/\mathbb{Q})$ is a generalized dihedral group. □

Exercise: 1. Let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$. Then $\mathcal{O}_c$ is an order of K. Show that $\mathrm{Pic}(\mathcal{O}_c) \cong I_{\mathfrak{c}}/P_{c,\mathbb{Z}}$. Moreover,

$$h(\mathcal{O}_c)/h(\mathcal{O}_K) = \frac{c}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \cdot \prod_{p|c}(1 - \eta_K(p)p^{-1}).$$

2. Ray class group and ring class group: Let L be the ring class field of conductor c over K and $\mathfrak{f} \subset \mathcal{O}_K$ its class field conductor. Then we have

$$\mathfrak{f} = \begin{cases} \mathcal{O}_K, & \text{if } K = \mathbb{Q}(i) \text{ and } c = 2, \text{ or } K = \mathbb{Q}(\sqrt{-3}) \text{ and } c = 2, 3, \\ c/2 \cdot \mathcal{O}_K, & \text{if } 2\|c \text{ and 2 splits completely in } K, \\ c \cdot \mathcal{O}_K, & \text{otherwise.} \end{cases}$$

Note that $H_{d_K c_2^2} \subset H_{d_K c_1^2}$ does not imply $c_2|c_1$.

We also denote the ring class field over K of conductor c by $H_{\mathcal{O}} = H_{d_K c^2}$ with $\mathcal{O} = \mathbb{Z} + c\mathcal{O}_K$. Now one can ask if there is a way to construct $H_{\mathcal{O}}$ explicitly?

Theorem 2.6. *Let $\mathcal{O} = \mathcal{O}_c$ be the order of conductor c (and thus discriminant $d_K c^2$). Then the field L is generated over K by the real number $j(\mathcal{O})$. Let $\mathfrak{a}_1, \cdot, fa_h$, $h = \#\mathrm{Pic}(\mathcal{O})$, be ideal class representatives. Then*

$$H_{\mathcal{O}}(X) = \prod_{i=1}^{h}(X - j(\mathfrak{a}_i)) \in \mathbb{Z}[X]$$

is the minimal polynomial of $j(\mathcal{O})$. Moreover, there is an algorithm for computing the class equation $H_{\mathcal{O}}(X)$.

Note that for $p \nmid 4n$, if $p|\operatorname{disc} H_{-4n}(X)$, then $(-4n/p) \neq 1$ by During's result on prime divisors of the difference of two singular moduli (Gross-Zagier's work further determines exactly which primes divide such a difference). Thus we have

Theorem 2.7. *Let n be a positive integer. There is a monic irreducible polynomial $f_n(X)$ of degree $h(-4n)$ such that for all primes $p \nmid 4n$, $p = x^2 + ny^2$ iff $\left(\frac{-n}{p}\right) = 1$ and $f_n(x) = 0 \mod p$ has an integer solution. Furthermore, there is an algorithm for finding $f_n(X)$.*

Proof. Take $f_n(X) = H_{\mathcal{O}}(X)$. □

3. Lecture IV: Archimedes' Cattle Problem and Pell's equation

One main result of this section is

Theorem 3.1. *Let K be a real quadratic field of discriminant D and fundamental unit ϵ. Then we have*

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2h_K \log \epsilon}{|\sqrt{D}|}.$$

Consider the equation: $x^2 - 14y^2 = \pm 1$ with $x, y \in \mathbb{Z}$. It is clear that the set of solutions to this equation has a bijection to $\mathcal{O}_K^\times$ for $K = \mathbb{Q}(\sqrt{14})$. We have continued fraction of $3 + \sqrt{14} = [6, 1, 2, 1]$ with minimal period 4, so that $[3, 1, 2, 1] = 15/4$ is fair approximates to $\sqrt{14}$ and gives the generator of $\mathcal{O}_K^\times / \pm 1$, i.e. $15 + 4\sqrt{14}$. In fact for any real quadratic field K, $\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$. Thus there exists a unique unit $\epsilon > 1$, called the fundamental unit, generates $\mathcal{O}_K^\times / \pm 1$ and $\log \epsilon$ is called the regulator of K.

Theorem 3.2. *Let $D \equiv 0, 1 \mod 4$ be a positive non-square integer. For $ax^2 - bx + c \in \mathbb{Z}[x]$ a primitive form with discriminant D, the following conditions (called reduced) are equivalent*

- $0 < \sqrt{D} - b < 2a < \sqrt{D} + b$,
- *it has roots $\xi > 1$ and $\xi' \in (-1, 0)$,*
- *the continued fraction of ξ is periodic,say $\xi = [\overline{u_0, \cdots, u_{\ell-1}}]$.*

For example, $\xi = \sqrt{d} + [\sqrt{d}]$ if $D = 4d$ and $(1 + \sqrt{D})/4 + [(-1 + \sqrt{D})/4]$ if $d \equiv 1 \mod 4$. Define

$$\begin{pmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} p_{j-1} & p_{j-2} \\ q_{j-1} & q_{j-2} \end{pmatrix} = \begin{pmatrix} u_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} u_{j-1} & 1 \\ 1 & 0 \end{pmatrix}, \forall j \geq 1.$$

Then fundamental unit $\epsilon = \frac{x_1 + y_1\sqrt{D}}{2}$ is equal to

$$\epsilon = \xi q_{\ell-1} + q_{\ell-2}.$$

Moreover, $\epsilon\epsilon' = (-1)^\ell$, i.e. $x_1^2 - Dy_1^2 = (-1)^\ell 4$. The field $\mathbb{Q}(\sqrt{D})$ has units of norm -1 iff ℓ is odd.

Two reduced quadratic numbers of discriminant D are equivalent iff they are complete quotients to each other (i.e. permutation in continued fractions). The set of all reduced quadratic numbers of discriminant D has h_D (narrow ideal class number?) equivalence classes.

Remark. Gauss did give the composition of forms, namely, we can also determine the group structure of ideal class group using forms. To relates to ideal class group, the related equivalence relation of quadratic forms is under the action of $\mathrm{GL}_2(\mathbb{Z})$, for any $\gamma \in \mathrm{GL}_2(\mathbb{Z})$,

$$\gamma \circ \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = \det \gamma \cdot \gamma \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} {}^t\gamma.$$

If one consider $\mathrm{SL}_2(\mathbb{Z})$-action, then the equivalence classes corresponds to narrow ideal classes. The related equivalence relation among continued fractions should be given by

$$[u_0, \cdots, u_{\ell-1}] \sim [u_{2i}, u_{2i+1}, \cdots, u_{\ell-1}, u_0, \cdots, u_{2i-1}].$$

Example. 1. There are 4 reduced form of discriminant 56:

$$(a, b, c) = (2, 4, -5), \quad (5, 4, -2), \quad (1, 6, -5), \quad (5, 6, -1).$$

Computation

$$\sqrt{14} + 3 = [6, (\sqrt{14} + 3)/5] = [6, 1, (\sqrt{14} + 2)/2] = [6, 1, 2, (\sqrt{14} + 2)/5] = [6, 1, 2, 1, \sqrt{14} + 3].$$

It follows that $h_D = 1$ and ϵ is the above one.

2. Let $d \in \mathbb{Z}_{\geq 1}$, then the fundamental unit of $\mathbb{Q}(\sqrt{1 + d^2})$ is $\sqrt{1 + d^2} + d$. The quadratic field $\mathbb{Q}(\sqrt{62501})$, $p := 62501 = 250^2 + 1$ is a prime $\equiv 1 \mod 4$, has ideal class group A isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.

It follows that the quotient group E/C of its units E by cyclotomic units C is isomorphic to $(\mathbb{Z}/9\mathbb{Z})$. This gives an example that for the field $F := \mathbb{Q}(\zeta_p)^+$, $E/C[3^\infty]$ and $A[3^\infty]$ have the same cardinality, but not isomorphic as $\mathbb{Z}_3[\mathrm{Gal}(F/\mathbb{Q})]$-modules; however, Mazur-Wiles and Kolyvagin's theorem implies that they have the same Jordan-Holder series as $\mathbb{Z}_3[\mathrm{Gal}(F/\mathbb{Q})]$-module.

The field $\mathbb{Q}(\sqrt{62501})$ has 43 reduced forms (a,b,c) and corresponding continued fractions $[u_0,u_1,\cdots,u_{\ell-1}]$ as follows. (Note that the inverse of class of (a,b,c) is the one of $(-c,b,-a)$).

1.$[249,1,1]$; $(1,249,-125),(125,249,-1),(125,1,-125)$;

2.$[49,9,1]$; $(5,241,-221),(25,249,-5),(221,201,-25)$;

3.$[49,1,9]$; $(5,249,-25),(221,241,5),(25,201,-221)$;

4.$[7,1,2,18,1]$; $(29,195,-211),(155,211,-29),(85,99,-155),(13,241,-85),(211,227,-13)$;

5.$[7,1,18,2,1]$; $(29,211,-155),(211,195,-29),(13,227,-211),(85,241,-13),(155,99,-85)$;

6.$[3,2,14,3,1]$; $(59,161,-155),(107,193,-59),(17,235,-107),(65,241,-17),(155,149,-65)$;

7.$[1,3,14,2,3]$; $(155,161,-59),(65,149,-155),(17,241,-65),(107,235,-17),(59,193,-107)$;

8.$[7,2,3,2,1,1,1]$; $(31,211,*),(103,223,*),(65,189,*),(85,201,*),(127,139,*),(97,115,*),(145,79,*)$;

9.$[1,1,1,2,3,2,7]$; $(145,211,*),(97,79,*),(127,115,*),(85,139,*),(65,201,*),(103,189,*),(31,223,*)$

There is a famous problem involving the unit group of real quadratic field. The Archimedes's Cattle problem: Compute, O friend, the number of the cattle of the sun which once grazed upon the plains of Sicily, divided according to color into four herds, one milk-white, one black, one dappled and one yellow. The number of bulls is greater than the number of cows, and the relations between them are as follows: (Let W,B,D,Y (resp. w,b,d,y) be White, Black, Yellow, Dappled bulls (resp. cows), respectively,)

$$W=\left(\frac{1}{2}+\frac{1}{3}\right)B+Y,\quad B=\left(\frac{1}{4}+\frac{1}{5}\right)D+Y,\quad D=\left(\frac{1}{6}+\frac{1}{7}\right)W+Y,$$

and moreover,

$$w=\left(\frac{1}{3}+\frac{1}{4}\right)(B+b),\quad b=\left(\frac{1}{4}+\frac{1}{5}\right)(D+d),\quad d=\left(\frac{1}{5}+\frac{1}{6}\right)(Y+y),\quad y=\left(\frac{1}{6}+\frac{1}{7}\right)(W+w).$$

If thou canst give, O friend, the number of each kind of bulls and cows, thou art no novice in numbers, yet can not be regarded as of high skill. Consider, however, the following additional relations between the bulls of the sun:

$$W+B=\square,\qquad D+Y=\triangle$$

(where $\square,\triangle$ represent square number and triangle number, respectively.) If thou hast computed these also, O friend, and found the total number of cattle, then exult as a conqueror, for thou hast proved thyself most skilled in numbers.

The first part of the problem is just linear algebra.The number of (homogenous) equations is one less than variables (and in fact the equation are independent), thus the general solution $(W,B,D,Y,w,b,d,y)=t(W_0,B_0,D_0,Y_0,w_0,b_0,d_0,y_0)$ must be a common multiple $t\in\mathbb{Z}_{\geq 1}$ of the minimal one. The last two conditions tell us that if denote $(B_0+W_0)^0$ by its square-free part,

$$t=(B_0+W_0)^0y^2,\qquad 1+8(D_0+Y_0)t=x^2.$$

Thus we obtain a Pell equation

$$x^2-8(B_0+W_0)^0(D_0+Y_0)y^2=1.$$

It turns out that

$$(W_0,B_0,D_0,Y_0)=4657\cdot(2226,1602,1580,891).$$

and then $(B_0+W_0)^0=3\cdot 11\cdot 29\cdot 4657$ and $D_0+Y_0=7\cdot 353\cdot 4657$. Thus reduced to solve the equation

$$\begin{cases}x^2-dy^2=1,\quad \text{where } d=609\cdot 7766\equiv 2 \mod 4,\\ x,y\in\mathbb{Z},\qquad 2\cdot 4657|y.\end{cases}$$

Let $\epsilon>1$ be the generator of the related unit group. We choose minimal n such that ϵ^n gives a solution (x_n,y_n) with $2\cdot 4657|y_n$. It turns out $n=(4657+1)/2=2329$. Nevertheless, the core part of the problem is to calculate ϵ. Amthor found the period length of continued fraction for d is 92, and the generator is

$$10993198673282973497986623282143354390108804 9+5054948523431503307447781973554040898634 0\sqrt{d}.$$

The regulator is $R\sim 102.101583$.

Remark. Even though it is not easy to write down the fundamental units ϵ of a real quadratic field $K = \mathbb{Q}(\sqrt{D})$ with discriminant $D > 0$. But one can easily show that $K \subset \mathbb{Q}(\zeta_D)$ and write the following unit in K, called cyclotomic unit

$$\eta := \sum_{(a \in \mathbb{Z}/D\mathbb{Z})^\times} (1 - \zeta_D)^{-\chi_D(a)}, \qquad \zeta_D = e^{2\pi i/D},$$

Theorem 3.3. *Let K be a real quadratic field with fundamental discriminant $D > 0$. Let ϵ be its fundamental unit and η the cyclotomic unit. Then*

$$\eta = \epsilon^{2h},$$

where h is the class number of K.

The proof of this theorem involves L-functions.

Theorem 3.4. *Let K be a real quadratic field with fundamental discriminant $D > 0$. Let ϵ be its fundamental unit and η the cyclotomic unit. Then we have*

- $\operatorname*{Res}_{s=1} \zeta_K(s) = \dfrac{2}{\sqrt{D}} \cdot \log \epsilon \cdot h$;
- $\operatorname*{Res}_{s=1} \zeta_K(s) = \dfrac{1}{\sqrt{D}} \cdot \log \eta$.

Let

$$\eta_0 = \prod_{0<b<D/2, \chi(b)=-1} \sin \frac{\pi b}{D} \Big/ \prod_{0<a<D/2, \chi(a)=1} \sin \frac{\pi a}{D} \in \mathcal{O}_K^\times \cap \mathbb{R}_{\geq 1}.$$

Then $\eta_0 = \epsilon^h$.

We will show the above result in the next section.

Exercise. Let $D \equiv 1 \mod 4$ be a positive square-free integer. Then the quadratic residues modulo D cluster at the beginning of the interval $(0, D/2)$, and the non-residues at the end.

At the end of this section, we include here Dirichlet's theorem on units of general number fields.

Theorem 3.5 (Dirichlet)**.** *Let K be a number field with r_1 real embeddings and r_2 pairs of complex embeddings. Then $\mathcal{O}_K^\times$ is finitely generated abelian group of rank $r := r_1 + r_2 - 1$.*

Proof. Note that the group homomorphism

$$\ell : \mathcal{O}_K^\times \longrightarrow \mathbb{R}^{r_1+r_2}, \qquad x \mapsto (\log |\sigma_i(x)|^{e_i})$$

(where $e_i = 1, 2$ according to σ_i is real or complex) has discrete image in the hyperplane $H : \sum_i x_i = 0$ of $\mathbb{R}^{r_1+r_2}$. We now prove that $\ell(\mathcal{O}_K^\times)$ is actually a full lattice in H, i.e. of rank $r_1 + r_2 - 1$.

Consider the embedding

$$\sigma : K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^\times.$$

Let $C > 0$ be a constant such that for any $t_i > 0, 1 \leq i \leq r_1 + r_2$ such that $\prod_{i=1}^{r_1} t_i \prod_{j=1}^{r_2} t_{r_1+i}^2 = C$, then

$$\mathcal{O}_K \cap \Big\{ (x_i) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \;\Big|\; |x_i| \leq t_i \Big\} \neq \{0\}.$$

(Since the volume of the above symmetric domain is $2^{r_1}\pi^{r_2}C$). Fix $i_0 : 1 \leq i_0 \leq r_1 + r_2$, take $0 \neq \alpha_n$ belong to the above intersection with $t_i = 1/n, i \neq i_0$. Then it has a subsequence $\alpha_{n_k}, k = 1, \cdots$, such that

- $|\sigma_i(\alpha_{n_k})|$ is decreasing for all $i \neq i_0$;
- (α_{n_k}) are the same principal ideal of $\mathcal{O}_K$.

Then $\epsilon_{i_0} := \alpha_{n_2}/\alpha_{n_1} \in \mathcal{O}_K^\times$ such that $\log |\sigma_i(\epsilon_{i_0})| < 0$ for all $i \neq i_0$. Thus $\log |\sigma_i(\epsilon_j)|$ for a matrix of rank $r = r_1 + r_2 - 1$ and then $\epsilon_1, \cdots, \epsilon_r$ are linear independent in $\mathcal{O}_K^\times$. □

Exercise. Let $\theta(t) = \frac{1}{2} \sum_{n \in \mathbb{Z}} e^{-\pi t n^2} = t^{-1/2}\theta(t^{-1})$. Study Riemann zeta function

$$\zeta(s) = \sum_{n=1} n^{-s} = \prod_p (1 - p^{-s})^{-1}, \qquad \mathrm{Re}(s) > 1.$$

Show that it is absolutely convergent on $\mathrm{Re}(s) > 1$, and satisfies

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \int_0^\infty (\theta(t) - 1) t^{s/2} \frac{dt}{t},$$

from which, deduce the meromorphic continuation, functional equation, and residue formula at $s = 1$. How to generalize to Dirichlet's L-series?

Exercise. Read Bump's book, the first section and exercises 1.1.1-1.1.2.

Appendix. If $a_n, b_n, n \geq 1$ are two sequences of complex numbers, A_n, B_n their partial sums. Then

$$\sum_{n=1}^{N} a_n b_n = A_N b_N + \sum_{n=1}^{N-1} A_n (b_n - b_{n+1}).$$

If the Dirichlet series $\sum a_n n^{-s}$ converges for some $s = s_0$, then it converges for any s with $\mathrm{Re}(s) > \mathrm{Re}(s_0)$, uniformly on any compact subset of this region.

Proof. Write $P_n(s_0) = \sum_{k=1}^{n} a_k k^{-s_0}$, then

$$\sum_{k=m+1}^{n} a_k k^{-s_0} \cdot k^{-(s-s_0)} = P_n(s_0) n^{-(s-s_0)} + \sum_{k=m+1}^{n-1} P_k(s_0)(k^{-(s-s_0)} - (k+1)^{-(s-s_0)}) - P_m(s_0)(m+1)^{-(s-s_0)}$$

But

$$\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}} = (s - s_0) \int_k^{k+1} x^{-(s-s_0+1)} dx$$

whose absolute value is easily estimated. □

2. if there exists $C, \sigma > 0$ such that

$$|A_n| \leq C n^{\sigma}, \qquad \forall n.$$

Then the abscissa of convergence of $\sum a_n n^{-s}$ is $\leq \sigma$.

Proof.

$$P_n(s) - P_m(s) = A_n n^{-s} + \sum_{k+m+1}^{n-1} A_k (k^{-s} - (k+1)^{-s} = A_n n^{-s} + \sum_{k+m+1}^{n-1} \int_k^{k+1} x^{-(s+1)} dx.$$

It follows that for $\mathrm{Re}(s) \geq \sigma + \delta$ with $\delta > 0$,

$$|P_n(s) - P_m(s)| \leq C n^{-\delta} + C|s|\delta^{-1}(m+1)^{-s}.$$ □

Example. We obtain the analytic continuation of $\zeta(s)$ to $\mathrm{Re}(s) > 0$.

$$(1 - 2^{-(s-1)})\zeta(s) = \sum_n (-1)^{n+1} n^{-s}.$$

4. Lecture V: Eisenstein series and Class Number Formula of Quadratic Fields

In this subsection, we show class number formula for quadratic fields.

Lemma 4.1 (Possion formula)**.** *Let $f \in \mathcal{S}(\mathbb{R}^n)$, then we have*

$$\sum_{\xi \in \mathbb{Z}^n} f(\xi) = \sum_{\xi \in \mathbb{Z}^n} \widehat{f}(\xi),$$

where $\widehat{f}$ is the Fourier transformation of f defined by

$$\widehat{f}(x) = \int_{\mathbb{R}^n} f(y) e^{2\pi i \langle x, y \rangle} dy, \qquad \langle x, y \rangle = \sum_i x_i y_i.$$

Proof. Let $\phi(x) = \sum_{\xi} f(x + \xi)$, which is periodic w.r.t $\mathbb{Z}^n$, and therefore admits a Fourier expansion $\phi(x) = \sum_{\eta \in \mathbb{Z}^n} a_\eta e^{2\pi i \langle \eta, x \rangle}$, with

$$a_\eta = \int_{\mathbb{R}^n/\mathbb{Z}^n} \phi(x) e^{-2\pi i \langle \eta, x \rangle} dx = \int_{\mathbb{R}^n} f(x) e^{-2\pi i \langle \eta, x \rangle} dx = \widehat{f}(\eta).$$

Thus we have the equality

$$\sum_{\xi \in \mathbb{Z}^n} f(x + \xi) = \sum_{\eta \in \mathbb{Z}^n} \widehat{f}(\eta) e^{2\pi i \langle \eta, x \rangle}.$$

Evaluating at $x = 0$ gives the Poisson summation formula. □

Example. Let Q be a positive definite quadratic form on $\mathbb{R}^n$. Then $f(x) := e^{-\pi Q(x)} \in \mathcal{S}(\mathbb{R}^n)$. Let $Q(x) = x^t Ax$ with A positive definite symmetric and $Q'(x) = x^t A^{-1} x$. Then

$$\widehat{f}(x) = \sqrt{\det A}^{1/2} e^{-2\pi Q'(x)}.$$

Proof. Let $A = {}^tBB$, then the Fourier transformation of $f(x) = e^{-\pi Q(x)}$ is (let $\psi(t) = e^{2\pi i t}$, and note that the Fourier transformation of $e^{-\pi x^2}$ is itself):

$$\begin{aligned}\widehat{f}(x) &= \int_{\mathbb{R}^n} e^{-\pi {}^t y A y} \psi({}^t xy) dx = \int_{\mathbb{R}^n} e^{-\pi \left({}^t(By)(By)\right)} \psi({}^t({}^tB^{-1}x)(By)) dy = \int_{\mathbb{R}^n} e^{-\pi {}^t yy} \psi({}^t({}^tB^{-1}x)y) dy \\ &= |\det B|^{-1} e^{-\pi {}^t({}^tB^{-1}x)({}^tB^{-1}x)} = \det(A)^{-1/2} e^{-\pi {}^t xx}.\end{aligned}$$

□

In particular, the quadratic form of 2 variables

$$Q_\tau(x, y) := \frac{|x\tau + y|^2}{\mathrm{Im}(\tau)}, \qquad \tau \in \mathcal{H}$$

has discriminant -4 so that the Fourier transformation of $e^{-\pi Q_\tau(x,y)}$ is $e^{-\pi Q_\tau(-y,x)}$. It follows that

$$\Theta_\tau(t) := \sum_{(m,n)\in\mathbb{Z}^2} e^{-\pi t Q_\tau(m,n)} = t^{-1} \sum_{(m,n)\in\mathbb{Z}^2} e^{-\pi t^{-1} Q_\tau(m,n)} = t^{-1}\Theta_\tau(t^{-1}).$$

Remark. Let (V, q) be an Euclidean space over $\mathbb{R}$ and $\Lambda \subset V$ a lattice. Let $\Lambda^\vee$ its dual. Let dx be the Haar measure such that the lattice spanned by an orthorm=normal basis has measure one. Define the Fourier transformation by: for any $f \in \mathcal{S}(V)$,

$$\widehat{f}(y) = \int_V f(x) e^{-2\pi i \langle x, y\rangle} dx.$$

Then

$$\sum_{\lambda\in\Lambda} f(\lambda) = \frac{1}{\mathrm{Vol}(L)} \sum_{\lambda'\in\Lambda^\vee} \widehat{f}(\lambda').$$

Proof. By choosing an orthonormal basis of V, we may identify V with the standard Euclidean space, and dx with the Lebesgue measure. Let $A \in \mathrm{GL}_n(\mathbb{R})$ be such that $\Lambda = A\mathbb{Z}^n$. Then

$$\mathrm{Vol}(\Lambda) = |\det A|, \qquad \Lambda^\vee = {}^tA^{-1}\mathbb{Z}^n.$$

The desired equality is equivalent to the Poisson formula for the function $g(x) := f(Ax)$ and $\widehat{g}(x) = \frac{1}{\mathrm{Vol}(\Lambda)} \widehat{f}({}^tA^{-1}x)$. □

Theorem 4.2. *The Eisenstein series*

$$E(z, s) = \pi^{-s}\Gamma(s) \cdot \frac{1}{2} \sum_{(m,n)\neq(0,0)} \frac{\mathrm{Im}(z)^s}{|mz + n|^{2s}}, \qquad z \in \mathcal{H}$$

is absolutely convergent if $\mathrm{Re}(s) > 1$*, has meromorphic continuation to the whole s-plane; it is analytic except at* $s = 0, 1$ *where it has simple poles. The residue* $\mathrm{Res}_{s=1} E(z, s) = \frac{1}{2}$ *independent of* z*. The Eisenstein series satisfies the functional equation*

$$E(z, s) = E(z, 1 - s).$$

Moreover, $E(x + iy, s) = O(y^\sigma)$ *as* $y \to \infty$ *where* $\sigma = \max(\mathrm{Re}(s), 1 - \mathrm{Re}(s))$*. The function* $E(z, s)$ *in* z *is automorphic i.e.*

$$E(\gamma z, s) = E(z, s), \qquad \forall \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Proof. For $z \in \mathcal{H}$ and $t > 0$, let

$$\Theta_z(t) = \sum_{(m,n)\in\mathbb{Z}^2} e^{-\pi \frac{|mz+n|^2}{\mathrm{Im}(z)} \cdot t}.$$

It follows from the Poisson summation formula $\Theta(1/t) = t\Theta(t)$. Thus we have

$$\begin{aligned}E(z, s) &= \frac{1}{2} \int_0^\infty (\Theta(t) - 1) t^s \frac{dt}{t} \\ &= \frac{1}{2} \int_1^\infty (\Theta(t) - 1) t^s \frac{dt}{t} + \frac{1}{2} \int_0^1 (t^{-1}\Theta(t^{-1}) - 1) t^s \frac{dt}{t} \\ &= \frac{1}{2} \int_1^\infty (\Theta(t) - 1) t^s \frac{dt}{t} + \frac{1}{2} \int_1^\infty (\Theta(t) - 1) t^{1-s} \frac{dt}{t} + \frac{1}{2}\left(\frac{1}{s-1} - \frac{1}{s}\right)\end{aligned}$$

This gives the analytic continuation, functional equation, and residue formula of $E(z,s)$. For the information about the behavior of $E(z,s)$ in the neighborhood of the cusp, see Bump's book: automorphism forms and representations, proof of Theorem 1.6.1. □

4.1. **CNF of Imaginary Quadratic Fields.** . Let $Q(m,n) = ax^2+bxy+cy^2, a,b,c \in \mathbb{R}$ be a positive definite forms of discriminant $D<0$. Let $z_Q = \frac{-b+\sqrt{D}}{2a} \in \mathcal{H}$, then

$$\pi^{-s}\Gamma(s)\cdot\frac{1}{2}\sum_{(m,n)\neq(0,0)} Q(m,n)^{-s} = (\sqrt{|D|}/2)^{-s}E(z_Q,s).$$

Note that for any $z\in\mathcal{H}$, then $Q_z(m,n) := \frac{|mz+n|^2}{\operatorname{Im} z}$ has discriminant -4.

We associate to a positive definite form $Q(x,y)=ax^2+bxy+cy^2$ of discriminant D the integral ideal

$$[a, \frac{b+\sqrt{D}}{2}] = \mathbb{Z}a + \mathbb{Z}\frac{b+\sqrt{D}}{2},$$

whose norm is a and its ideal class is denoted as A. Thus $\mathfrak{b} := [a, (-b+\sqrt{D})/2] \in A^-$ has also norm a.

$$\begin{aligned}\zeta(A,s) :&= \sum_{\mathfrak{a}\in A, \mathfrak{a}\subset\mathcal{O}_K} \mathrm{N}\mathfrak{a}^{-s} = \sum_{\lambda\in\mathfrak{b}/\mathcal{O}_K^\times} (\mathrm{N}\lambda\mathfrak{b}^{-1})^{-s}\\ &= \frac{1}{w_K}a^s \sum_{0\neq\lambda\in\mathbb{Z}a+\mathbb{Z}(-b+\sqrt{D})/2} |\lambda|^{-2s}\\ &= \frac{1}{w_K}\sum_{(m,n)\neq(0,0)} Q(m,n)^{-s}.\end{aligned}$$

Thus

$$\left(\frac{\sqrt{|D|}}{2\pi}\right)^{-s}\Gamma(s)\cdot\zeta_K(s) = \frac{2}{w_K}\sum_{Q_i} E(z_{Q_i},s). \qquad \mathrm{Re}(s)>0.$$

The meromorphic continuation and function equation of $E(z,s)$ implies the meromorphic continuation of ζ_K and functional equation

$$\xi_K(s) := \sqrt{|D|}^{s/2}2(2\pi)^{-s}\Gamma(s)\zeta_K(s) = \xi_K(1-s).$$

Moreover, Taking residue at $s=1$, we have that

$$\operatorname*{Res}_{s=1}\zeta_K(s) = \frac{2\pi}{w_K\sqrt{|D|}}\cdot h_K.$$

4.2. **CNF for Real Quadratic Fields.** Let K be a real quadratic field of discriminant $D>0$ and ϵ the fundamental unit. Let A be an ideal class of K and $\mathfrak{b}\in A^-$. Let

$$c(s) := \int_0^\infty \frac{dv}{(e^v+e^{-v})^s} = \frac{\Gamma(s/2)^2}{2\Gamma(s)}.$$

(We do not need the last equality). For any real a,b such that $ab\neq 0$,

$$\frac{1}{|ab|^s}\cdot c(s) = \int_{-\infty}^\infty \frac{dv}{(a^2e^v+b^2e^{-v})^s}.$$

Let A be an ideal class of K and $\mathfrak{b}\in A^-$. We have

$$\zeta(s,A) = \sum_{\lambda\in\mathfrak{b}/\mathcal{O}_K^\times}\frac{1}{(\mathrm{N}(\lambda\mathfrak{b}^{-1}))^s} = \frac{1}{2}\sum_{\lambda\in\mathfrak{b}/\epsilon^{\mathbb{Z}}}\frac{(\mathrm{N}\mathfrak{b})^s}{|\mathrm{N}\lambda|^s}$$

and if let $\Delta = \mathrm{N}\mathfrak{b}\sqrt{D} = \operatorname{disc}\mathfrak{b}$ and write λ' for the conjugation of $|lambda\in K$, then

$$\begin{aligned}2^{s+1}D^{s/2}c(s)\zeta(s,A) &= \sum_{\lambda\in\mathfrak{b}/\epsilon^{\mathbb{Z}}} c(s)\frac{1}{|\lambda\lambda'|^s}(2\Delta)^s\\ &= \sum_{\lambda\in\mathfrak{b}/\epsilon^{\mathbb{Z}}}\int_{-\infty}^\infty \frac{(2\Delta)^s}{(\lambda^2e^v+\lambda'^2e^{-v})^s}dv\\ &= \sum_{\lambda\in\mathfrak{b}}\int_{-\log\epsilon}^{\log\epsilon}\frac{(2\Delta)^s}{(\lambda^2e^v+\lambda'^2e^{-v})^s}dv\end{aligned}$$

Choose $\mathfrak{b} = \mathbb{Z} + \mathbb{Z}w$ with $w > w'$, then let Q_v be the quadratic form

$$Q_v = \frac{1}{2\Delta}(mw+n)^2 e^v + (mw'+n)e^{-v}$$

then the discriminant of Q_v is -1 and thus we have

$$\begin{aligned} 2^{s+1}D^{s/2}c(s)\pi^{-s}\Gamma(s)\frac{1}{2}\zeta(s,A) &= \int_{-\log\epsilon}^{\log\epsilon} \pi^{-s}\Gamma(s)\frac{1}{2}\sum_{(m,n)\neq(0,0)} Q_v(m,n)^{-s}dv \\ &= \int_{-\log\epsilon}^{\log\epsilon} 2^s E(z_{Q_v},s)dv \end{aligned}$$

Thus we have that

$$\pi^{-s}D^{s/2}\Gamma(s/2)^2\zeta_K(s) = 2\sum_Q \int_{-\log\epsilon}^{\log\epsilon} E(z_{Q_v},s)dv.$$

Taking residue

$$\operatorname*{Res}_{s=1}\zeta_K(s) = \frac{2h\log\epsilon}{\sqrt{D}}.$$

5. Catalan's Conjecture

For general number fields K, Tate's thesis gives a proof, via Harmonic analysis, of meromorphic continuation and functional equation of L-series of any Hecke character over K, together with formula

$$\operatorname*{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{w_K\cdot\sqrt{|D_K|}}.$$

We will see how the Galois structure of ideal class groups and unit groups, together with the refinement of the CNF, play an essential role in the proof of the Catalan's conjecture.

Theorem 5.1 (Catalan's Conjecture)**.** *The equation*

$$\begin{cases} x^p - y^q = 1 \\ p,q \in \mathbb{Z}_{\geq 2},\ x,y \in \mathbb{Z}_{\neq 0} \end{cases}$$

has no solutions (x,y) in positive integers other that the ones given by $(\pm 3)^3 - 2^3 = 1$.

The cases of $q=2$ and $p=2$ are proved by Lebesgue and Chao Ko, respectively. Then to prove the conjecture, it reduces to the following

Theorem 5.2 (Mihailescu)**.** *Let $p,q>2$ be two distinct primes. Then the equation*

$$(*) \qquad \begin{cases} x^p - y^q = 1, \\ x,y \in \mathbb{Z}\setminus\{0\} \end{cases}$$

has no solutions. (We call the above Diophantine equation $(*)$ the Catalan's equation.)

From now on, we assume that x,y is a solution to the Catalan's equation and derive a contradiction.

5.1. **Cassels' result: elementary number theory.** We start with the following result of Cassels (whose proof will be given later) according the v-adic properties of x,y for $v=p,q$ and ∞.

Proposition 5.3 (Cassels)**.** *Assume that (x,y) is a solution to the Catalan equation. Then we have*

1. *$q|x$ and $p|y$;*
2. *$x \equiv 1 \pmod{p^{q-1}}$ and $y \equiv -1 \pmod{q^{p-1}}$;*
3. *$|x| \geq \max(p^{q-1}(q-1)^q - 1,\ q^{p-1}+q)$ and $|y| \geq \max(q^{p-1}(p-1)^p - 1,\ p^{q-1}+p)$.*

Proof. If $p \nmid y$, then $\left(x-1, \frac{x^p-1}{x-1}\right) = 1$ and therefore $x-1 = a^q$ for some $a \neq 0, -1$. Thus

$$(a^q+1)^p - y^q = 1,$$

or

$$y = ((a^q+1)^p - 1)^{1/q} = a^p F(a^{-q}), \quad \text{with } F(t) = ((1+t)^p - t^p)^{1/q}.$$

If $q > p$, the decreasing function $f(y) = (a^q+1)^p - y^q$ has $f(a^p) > 1$ and $f(a^p+1) < 0$, a contradiction. (Thus we have $p|y$ if $q > p$, and similarly, $q|x$ if $p > q$). Now assume $p > q$, let F_k be deg $\le k$-partial sum of the Taylor expansion of F around $t = 0$, and consider rational numbers:

$$\beta := \beta_k := a^{q^k}(F(t) - F_k(t))\Big|_{t=a^{-q}}, k \ge 0.$$

It is clear $a^{q^k}F(a^{-q}) \in \mathbb{Z}$. But if $k < p$, then F_k is the same as the deg $\le k$-partial sum of the Taylor expansion of $(1+t)^{p/q}$, i.e. $\sum_{i=0}^{k}\binom{p/q}{i}t^i$. Thus for $p/q < k < p$, $\beta \in \mathbb{Z}[q^{-1}]$ is a q-integer. Its q-adic valuation is $\mathrm{ord}_q\binom{p/q}{k} = -k - \mathrm{ord}_q k!$. Thus we obtained a lower bound of β:

$$|\beta| \ge q^{-k-\mathrm{ord}_q(k!)}.$$

On the other hand, since $q|x$, consider the decomposition

$$(y+1)\cdot\frac{y^q+1}{y+1} = x^p.$$

It follows that

$$y+1 = q^{p-1}u^p, \quad \frac{y^q+1}{y+1} = qv^p, \quad x = quv.$$

Thus

$$q^{p-1} \mid y+1 \mid \frac{y^q+1}{y+1} - q = q(v^p-1),$$

and $v^p \equiv 1 \mod q^{p-2}$. Since $(\mathbb{Z}/q^{p-2}\mathbb{Z})^\times \cong \mathbb{F}_q^\times \times \mathbb{Z}/q^{p-3}\mathbb{Z}$, together with $(p, q-1) = 1$ since $p > q$, we have $v \equiv 1 \mod q^{p-2}$. Thus $|x| \ge q^{p-1} + q$. For $k = [p/q] + 1$, we have

$$|F(t) - F_k(t)| \le \frac{|t|^{k+1}}{(1-|t|)^2}, \qquad \forall t \in \mathbb{R}, |t| \le 1.$$

The bound of x implies that

$$|\beta_k| \le \frac{|a|^q}{(|a|^q-1)^2} \le \frac{1}{|a|^q-2} \le q^{1-p} < q^{-k-\mathrm{ord}_q(k!)}. \qquad \square$$

5.2. **Selmer group and the element $[x-\zeta]$.** Let $\zeta \in \mu_p$ be a primitive root of unity and $K = \mathbb{Q}(\zeta)$. Then $\mathbb{Z}[\zeta]$ is the ring of integers in K. Decompose the equation $x^p - 1 = y^q$, one has

$$\prod_a (x - \zeta^a) = y^q.$$

If a prime ideal $\mathfrak{l}|(x-\zeta^a, x-\zeta^b)$, then $\mathfrak{l}|(\zeta^a-\zeta^b)$. Taking a, b distinct modulo p, we have that $\mathfrak{l} = \mathfrak{p} := (1-\zeta)$ the unique prime ideal of K above p. It shows that $q|\,\mathrm{ord}_{\mathfrak{l}}(x-\zeta)$ for all $\mathfrak{l} \ne \mathfrak{p}$. By Cassels' result $x \equiv 1 \mod p^2$, we have that

$$\mathrm{ord}_{\mathfrak{p}}\left(\frac{x-\zeta}{1-\zeta}\right) = 0.$$

Define the q-Selmer group (of $\mathbb{Z}_p(1)$) over K

$$\mathrm{Sel}(K, \mu_q) := \{[\alpha] \in K^\times/K^{\times q} \mid (\alpha) = \mathfrak{a}^q \text{ for some ideal } \mathfrak{a} \text{ of } K\} \subset H^1(K, \mu_q).$$

Here for $\alpha \in K^\times$ we denote by $[\alpha]$ its class modulo $K^{\times 3}$. We have see that the class ξ of $\frac{x-\zeta}{1-\zeta}$ modulo $K^\times$ belongs to $\mathrm{Sel}(K, \mu_q)$.

Then the map $[\alpha] \mapsto$ the ideal class of $\mathfrak{a}$ gives rise to a well-defined surjective homomorphism $\mathrm{Sel}(K, \mu_q) \longrightarrow \mathrm{Cl}_K[q]$. Its kernel is clearly $\mathcal{O}_K^\times/\mathcal{O}_K^{\times q}$. Then we have the short exact sequence of $R := \mathbb{F}_q[\Delta]$-modules, (here $\Delta = \mathrm{Gal}(K/\mathbb{Q})$),

$$1 \longrightarrow \mathcal{O}_K^\times/\mathcal{O}_K^{\times q} \longrightarrow \mathrm{Sel}(K, \mu_q) \longrightarrow \mathrm{Cl}_K[q] \longrightarrow 1.$$

Some variations of Selmer groups are also useful. Define

$$H := \{[\alpha] \in K^\times/K^{\times q} \mid (\alpha) = \mathfrak{a}^q\mathfrak{p}^n \text{ for some ideal } \mathfrak{a} \text{ of } K \text{ and } n \in \mathbb{Z}\} \subset H^1(K, \mu_q).$$

It is clear that $[x-\zeta]$ belongs to H.

Remark. Recall for the equation $y^2 + 14 = x^3$, let $K = \mathbb{Q}(\sqrt{-14})$ and consider the class $\xi := y + \sqrt{-14}$ mod $K^{\times 3}$. Since $(y+\sqrt{-14}), (y-\sqrt{-14})$ are coprime, we know that $(y+\sqrt{-14}) = \mathfrak{a}^3$ for some ideal $\mathfrak{a}$, thus $\xi \in \mathrm{Sel}(K, \mu_3)$. In the short exact sequence

$$1 \longrightarrow \mathcal{O}_K^\times/\mathcal{O}_K^{\times 3} \longrightarrow \mathrm{Sel}(K, \mu_3) \longrightarrow \mathrm{Cl}_K[3] \longrightarrow 0,$$

we have that $\mathrm{Cl}_K[3] = 0$ since $\mathrm{Cl}_K \cong \mathbb{Z}/4\mathbb{Z}$ and $\mathcal{O}_K^\times/\mathcal{O}_K^{\times 3} = 1$ since $\mathcal{O}_K^\times = \{\pm 1\}$. Thus $\mathrm{Sel}(K, \mu_3) = 0$. However, look at the class of $y + \sqrt{-14}$ in $\mathrm{Sel}(K, \mu_3) \subset K^\times/K^{\times 3}$ must be non-trivial, since one can show that $y^2 + 14 = x^3$ has no integral solution by showing that any elements in $K^{\times 3}$ can not have $\sqrt{-14}$-coefficient 1. In our situation, the minus part of $[x - \zeta]$ play the similar role in Catalan's conjecture. Let $x \mapsto \overline{x} = \iota(x)$ denote the complex conjugation.

Theorem 5.4. *Let $p, q \geq 3$ be two distinct prime and x, y non-zero integer solution to Catalan's equation $x^p - y^q = 1$. Then the minus part $(x - \zeta)^- := (x - \zeta)^{1-\iota}$ of $x - \zeta$ is non-trivial in H. Therefore, $\mathrm{Cl}_K^-[q] \cong H^- \neq 0$.*

Proof. The proof is by p-adic argument based on the fact $x \equiv 1 \mod p^{q-1}$. The following lemma is obvious.

Lemma 5.5. *Let $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha - \beta \in \mathcal{O}_K^\times$ and $\alpha/\beta \in K^{\times q}$. Let $\alpha^{1/q}, \beta^{1/q} \in \overline{K}$ be q-th roots of α, β, respectively, such that $\alpha^{1/q}/\beta^{1/q} \in K$. Then*

$$\gamma := (\alpha^{1/q} - \beta^{1/q})^q \in \mathcal{O}_K^\times$$

independent of the choice of these q-th roots.

Assume now that $[(x - \zeta)^-]$ is trivial in H (actually $[x - \zeta] \in S^- \subset H^-$). Let $\gamma \in \mathcal{O}_K^\times$ be the unit constructed in the above lemma by taking

$$\alpha = \frac{x - \zeta}{1 - \zeta}, \qquad \beta = \frac{x - \overline{\zeta}}{1 - \zeta}.$$

Thus $\mathrm{N}(\gamma) = 1$ since K has no real embedding. Using $x \equiv 1 \mod p^{q-1}$, we compute the $\mathrm{N}(\gamma)$ in the totally ramified extension $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ such that the p-adic argument will produce a contradiction.

Let $\pi = \zeta - 1$ a parameter of $\mathbb{Q}_p(\zeta)$. Let $\mu = (x - 1)\pi^{-1}$. Then

$$\alpha = 1 + \mu, \qquad \beta = -\overline{\zeta}(1 + \overline{\mu}),$$

with $p^{q-1}\pi | \mu, \overline{\mu}$. We may choose above q-th roots of α, β in K_π as below:

$$w := (1+\mu)^{1/q} := \sum_{i=0} \binom{1/q}{i} \mu^i \equiv 1 \mod \pi, \qquad w' = (-\overline{\zeta}(1+\overline{\mu})^{1/q} := -\zeta^{-1/q} \sum_{i=0} \binom{1/q}{i} \overline{\mu}^i \equiv -1 \mod \pi.$$

These choices work since the unique element $\delta \in K^\times$ with $\delta^q = x - \zeta/x - \overline{\zeta}$ satisfies $\delta \equiv -1 \mod \pi$ (since $\delta^q \equiv -1 \mod \pi$ and $1 = \delta\overline{\delta} \equiv \delta^2 \mod \pi$).

- Considering $1 = \mathrm{N}(w - w')^q \mod \mu^2$, we have

  $$\mathrm{N}(w - w')^q \equiv 1 + \frac{(x-1)(1-q)}{2q} \mod (\pi(x-1)),$$

  which implies $p | 1 - q$ and

  $$w - w' \equiv (1 + \mu/q) + \zeta^{-1/q}(1 + \overline{\mu}/q) \equiv 1 + \overline{\zeta} \mod \mu^2.$$

- Considering $1 = \mathrm{N}(w - w')^q \mod \mu^3$, we further have

  $$\mathrm{N}(w - w')^q \equiv 1 + \frac{(1-q)(x-1)^2}{2q} \cdot \frac{1 - p^2}{12} \mod \mu^3,$$

  which implies $p^{q-1} | \pi^3(q-1)/3$, a contradiction. □

Corollary 5.6. *If Catalan's equation has solutions, then $p, q \geq 41$.*

Proof. Assume that $p < q$. We have that the minus class number h_p^- is equal to 1 for $p \leq 19$; for $p = 23, 29, 31, 41$, $h_p^- = 3, 8, 3^2, 37, 11^2$, respectively, which is not divisible by $q > p$. □

Example. 1. Prove that $\mathbb{Q}(\zeta_p)$ has class number 1 for $p = 3, 5, 7$. 2. There is an example with $p | h_q^-$ and $q | h_p^-$.

$$h_{47}^- = 5 \cdot 139, \qquad h_{139}^- = 3^2 \cdot 47 \cdot 277^3 \cdot 967 \cdot 1188961909.$$

Theorem 5.7. *Let $p, q \geq 7$ be distinct primes and $G+ = \mathrm{Gal}(\mathbb{Q}(\mu_p)^+/\mathbb{Q})$. Then $\mathbb{F}_q[G^+]$-annihilator of $[x - \zeta]^+ : [(x - \zeta)(x - \overline{\zeta})]$ is trivial.*

The proof is via a ∞-adic argument based on the fact that $|x| \geq q^{p-1} + q$.

Proof. Since $x \equiv 1 \mod p$, there is an element $\theta \in \mathbb{Z}[G]$ such that its reduction to $\mathbb{F}_q[G]$ is the product of $(1+\iota)$ and a lift of $\pm\psi$ to $\mathbb{F}_p[G]$ with the following properties:

- $n_\sigma = n_{\sigma\iota}$ for all $\sigma \in G$;
- $n_\sigma \geq 0$ for each $\sigma \in G$;
- $\sum_\sigma n_\sigma = mq$ for some integer m satisfying $0 \leq m \leq (p-1)/2$;
- $(x-\zeta)^\theta = \alpha^q$ for some (unique) algebraic integer $\alpha \in \mathbb{Q}(\zeta)^+$.

We need to show that $q|n_\sigma$ for all σ. If $m = 0$, nothing to prove. We now assume that $m > 0$. Note that any non-zero element has at most one q-th root in $K^\times$. Fix any embedding of K into $\mathbb{C}$ and consider the real number (since $K^{\times q} \cap K^{+\times} = K^{+\times q}$),

$$(x-\zeta)^{\theta/q} = x^{\deg\theta/q}(1-\zeta x^{-1})^{\theta/q} = x^{\deg\theta/q}G(x^{-1}),$$

where $G(x) = (1-\zeta t)^{\theta/q}$ is defined to be the analytic function around $t = 0$, via a fixed embedding $\zeta + \zeta^{-1} \in \mathbb{R}$, write $\theta = \sum n_a\sigma_a$,

$$G(t) = \prod_a \sum_{i=0}^\infty \binom{n_a/q}{i}(-\zeta^a)^i t^i = \sum_{k=0}^\infty \left(\sum_{\sum i_a = k} \prod_a \binom{n_a/q}{i_a}(-\zeta^a)^{i_a} \right) t^k = \sum_{k=0}^\infty \frac{a_k}{k!\cdot q^k} t^k,$$

where

$$\begin{aligned} a_k &= k!q^k \sum_{\sum i_a = k} \prod_a \binom{n_a/q}{i_a}(-\zeta^a)^{i_a} \\ &= \sum_{\sum i_a = k} \frac{k!}{\prod_a i_a!} \prod_a n_a(n_a-q)\cdots(n_a-(i_a-1)q)(-\zeta^a)^{i_a} \\ &\equiv \left(-\sum_a n_a\zeta^a \right)^k \mod q \end{aligned}$$

Note that q is unramified over K, we will show that $q|a_m$ for $m = \deg\theta/q$. Let

$$\beta := q^{m+\mathrm{ord}_q\, m!}x^m(G(x^{-1}) - G_m(x^{-1})) \in \mathcal{O}_K, \qquad \beta \equiv a_m \mod q,$$

and we show now that $\beta = 0$. Comparing $G(t)$ and $H(t) := (1-t)^{-k}$, we have

$$|\beta| \leq q^{m+\mathrm{ord}_q\, m!}|x|^m(H(|x|^{-1}) - H_k(|x|^{-1})) \leq q^{m+\mathrm{ord}_q\, m!}|x|^m \left| |x|^{-m+1}\binom{-m}{m+1}(1-|x|^{-1})^{-m-(m+1)} \right| < 1,$$

where the last inequality follows from $|x| \geq q^{p-1} + q$ and the assumption $0 < m \leq (p-1)/2$. For any $\sigma \in G$,

$$\left((1-\zeta x^{-1})^{\theta/q}\right)^\sigma = (1-\zeta x^{-1})^{\sigma\theta/q} \in K^{+\times}.$$

By the same argument, we have $|\beta^\sigma| < 1$ for all $\sigma \in G$. Thus $\beta = 0$ and $q|a_m$. □

5.3. **Stickelberger Theorem and Minus argument.** Define the Stickelberger element Θ and Stickelberger ideal I in $\mathbb{Q}[G]$ by

$$\Theta = \sum_{a=1}^{p-1} \left\{ \frac{a}{p} \right\} \sigma_a^{-1}, \qquad I = \mathbb{Z}[G] \cap \mathbb{Z}[G]\Theta.$$

One can show that I is generated by

$$\theta_a = (a - \sigma_a)\Theta = \sum_b \left[\frac{ab}{p} \right] \sigma_b^{-1}, \qquad (a,p) = 1.$$

and $(1-\iota)I$ is generated by

$$(1-\iota)(\theta_{a+1} - \theta_a), \qquad 1 \leq a \leq (p-1)/2.$$

It is easy to see that odd prime $q \nmid (1-\iota)\theta_2$.

Theorem 5.8 (Stickelberger)**.** *$I \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(\mathrm{Cl}_K)$. In particular,*

$$(I \otimes \mathbb{F}_q)^- \subseteq \mathrm{Ann}_{\mathbb{F}_q[G]}\mathrm{Sel}(K, \mu_q)^-.$$

Theorem 5.9. *$q^2|x$ and $p^2|y$. Therefore $\mathrm{loc}_q(x-\zeta)^+ \in K_q^{\times q}$.*

Proof. Let $\theta = (1-\iota)\theta_2$ so that $q \nmid \theta$. But by Stickelberger's theorem $(1-\zeta x)^\theta = b^p$ for some $b \in K^\times$. Since $q|x$, $b^q \equiv 1 \mod q$ and therefore $b^q \equiv 1 \mod q^2$. Now we have $q \nmid \theta$ and $(1-\zeta x)^\theta \equiv 1 \mod q^2$, which implies $q^2|x$. Similarly, $p|y$ and Stickelberger's theorem also implies $p^2|y$. □

Theorem 5.10. *$q < 4p^2$ and $p < 4q^2$. Therefore $q \nmid p-1$ and $p \nmid q-1$.*

Proof. Consider the injective group homomorphism:

$$\left\{\theta \in (1-\tau)\mathbb{Z}[G] |\ (x-\zeta)^\theta \in K^{\times,q}\right\} \longrightarrow \left\{\alpha \in K^\times \ \middle|\ |\varphi(\alpha)| = 1,\ \forall \varphi : K \to \mathbb{C}\right\}$$

which maps θ to $\alpha = \alpha_\theta$ with $\alpha_\theta^q = (x-\zeta)^\theta$. We will estimate $N(\alpha_\theta - 1)$ for $\theta \neq 0$ in terms of $\|\theta\|$ where for $\theta = \sum_{\sigma\in G} n_\sigma \sigma$, $\|\theta\| = \sum_{\sigma\in G} |n_\sigma|$.

(1) the norm of the denominator J of (α_θ) gives a lower bound of $N(\alpha_\theta - 1) \geq \mathrm{N}(J)^{-1}$:
Write $(\alpha_\theta) = \frac{J'}{J}$ with J and J' integral coprime, then $N(J') = N(J)$ and

$$(JJ')^q = (\prod_{\sigma\in G}(x - \sigma(\zeta))^{|n_\sigma|}),$$

thus

$$N(\alpha_\theta - 1) \geq N(J)^{-1} \geq (|x|+1)^{-\frac{||\theta||(p-1)}{2q}}.$$

(2) On the other hand, since $|\varphi(\alpha_\theta)| = 1$ for any embedding $\varphi : K \to \mathbb{C}$, we have

$$|\arg(\varphi(\alpha_\theta)^q)| = |\log(\varphi(\alpha_\theta)^q)| = |\log(1-\varphi(\zeta)/x)^\theta| (\text{principle branch}) \leq \frac{||\theta||}{|x|-1}$$

thus there exists a q-th root of unity $\zeta_q \in \mu_q \subset \mathbb{C}$ such that

$$|\varphi(\alpha) - \zeta_q| \leq \frac{||\theta||}{q(|x|-1)}.$$

Now assume that $q > 4p^2$, by Stickelberger theorem, there exists at least $q+1$ elements $\theta \in I^-$ with $||\cdot|| \leq \frac{3q}{2(p-1)}$, where I is the Stickelberger ideal. Thus by box principle, there exists $\theta \in I^-$ such that (note for any φ, $|\varphi(\alpha_\theta) - 1) \leq 2$)

$$|N(\alpha_\theta - 1)| \leq 2^{p-1}\left(\frac{||\theta||}{q(|x|-1)}\right)^2, \qquad \text{with } ||\theta|| \leq \frac{3q}{p-1}.$$

The above upper and lower bound for $\mathrm{N}(\alpha - 1)$ is contradict to the conditions $q > 4p^2$, together with $|x| > q^{p-1}$ and $p, q \geq 5$. □

5.4. **Thaine's Theorem and Plus argument.** We have the following theorem.

Theorem 5.11. *Let $K = \mathbb{Q}(\mu_p)$ with p odd prime, and K^+ the maximal totally real subfield of K. Let $E = \mathcal{O}_K^\times$, C its subgroup of cyclotomic units, and A^+ the ideal class group of K^+. Then we have*

- *(Kummer) $[E : C] = |A^+|$;*
- *(Mazur-Wiles, Kolyvagin) Let $q \nmid p-1$ be a prime and $\chi : \Delta^+ \longrightarrow \overline{\mathbb{Z}_q}^\times$ any character. Then we have that the q-parts of E/C and A^+ have the same Jordan-Holder series as $\mathbb{Z}_q[G^+]$-modules, or equivalently,*

$$[E_\chi : C_\chi] = |A^+_\chi|.$$

Here for any $\mathbb{Z}[\Delta]$-module M, let M_χ denote $M \otimes_{\mathbb{Z}[\Delta],\chi} \mathbb{Z}_q[\mathrm{Im}\,\chi]$. It follows that for $R := \mathbb{F}_q[\Delta^+]$-modules E/CE^q and A^+/qA^+, we have

$$\mathrm{Ann}_R(E/CE^q) = \mathrm{Ann}_R(A^+/qA^+).$$

An element $\alpha \in K^\times$ is called p-unit if (α) is supported on the unique prime of K above p. There is a version with p-units, which we will use later.

Theorem 5.12 (Thaine)**.** *Let E, C be p-unit and p-cyclotomic units of K. Then we have that E/E^q is a free $R := \mathbb{F}_q[G^+]$-module of rank one and*

$$\mathrm{Ann}_R(E/CE^q) \subseteq \mathrm{Ann}_R(A^+/qA^+) = \mathrm{Ann}_R(A^+[q]).$$

Now we give the proof of Catalan's conjecture. Assume $p > q$. We already have that $\mathbb{F}_q[G^+]$ is semi-simple. Consider the exact sequence

$$0 \longrightarrow E/E^q \longrightarrow H^+ \longrightarrow A^+ \longrightarrow 0.$$

By Thaine's theorem, rigidity of $\xi^+ \in H^+$, and $\mathrm{loc}_q \xi^+ = 0$, we have that

$$\mathrm{Ann}_R(C_q E^q/E^q)\mathrm{Ann}_R(E/CE^q) = 0,$$

Here $C_q = \left\{x \in C \mid \mathrm{loc}_q(x) \in K_q^{\times q}\right\}$. The fact that $E/E^q \cong R$ implies $\mathrm{Ann}_R(CE^q/C_qE^q) = R$, i.e. $CE^q = C_qE^q$. But this is impossible when $p > q$.

References

[1] Bilu, *Catalan's conjecture.*
[2] John Coates, A. Raghuram, Anupam Saikia, and R. Sujatha, *The Bloch-Kato conjecture for the Riemann zeta function.*
[3] , *The equivariant Tamagawa number conjecture: a survey*, Contemporary Mathematics.
[4] E. de Shalit, *The Iwasawa theory of elliptic curves with complex muliplication.*
[5] Greenberg, *On p-adic L-functions and cyclotomic fields.II.*
[6] Cornelius Greither, *Class groups of abelian fields, and the main conjecture.*
[7] Kazuya Kato, *P-adic Hodge theory and values of zeta functions of modular forms.*
[8] V. A. Kolyvagin, *On the structure of Shafarevich-Tate groups.*
[9] V. A. Kolyvagin, *Euler systems*, In: The Grothendieck Festschrift (Vol. II).
[10] Serge Lang, *Cyclotomtic fields I and II.*
[11] Metsankyl, *Catalan's conjecture: Another old Diophantine problem solved.*
[12] Mihailescu, *Primary cyclotomic units and a proof of Catalan's conjecture.*
[13] Karl Rubin, *Euler Systems*, Annals of Mathematics Studies.
[14] Rubin, *The Main conjecture.* (Appendix in Serge lang's Cyclotomtic fields I and II)
[15] Karl Rubin, *Kolyvagin's system of Gauss sums.*
[16] René Schoof, *Catalan's Conjecture.*
[17] Francisco Thaine, *On the ideal class groups of real abelian number fields.*
[18] Washington, *Introduction to cyclotomtic fields.*