

実2次体の剰余体における単数の分布と Artin予想について

名大理 真島一成 (Kazusige Masima)

§0. Introduction ~ 動機 ~

K を代数体、 $\mathcal{O}$, E をそれぞれ K の整数環、単数群とする。 K の ideal $\mathfrak{m}$ に対して、 $\text{mod } \mathfrak{m}$ の ray class field の次数が、 $h((\mathcal{O}/\mathfrak{m})^\times; \bar{E})$ で与えられる。(h は K の類数、 $\bar{E} := E \text{ mod } \mathfrak{m}$) ここで、 h については多くのことが調べられているが、 $((\mathcal{O}/\mathfrak{m})^\times; \bar{E})$ についてはあまり分かっていない。

簡単のため、 $K = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}^+$: square-free とし、 $\mathfrak{p}$ を、素数 p を割る K の素 ideal とするとき、 $I_p := ((\mathcal{O}/\mathfrak{p})^\times; \bar{E})$ ($\bar{E} := E \text{ mod } \mathfrak{p}$) についてのみ考える。明らかに I_p は $\mathfrak{p}$ の取り方によらない。このとき容易に、 $I_p \geq l_p$

ただし、 $l_p := \begin{cases} 1 & (p \text{ が } K \text{ で分解 (または分岐)}) \\ p-1 & (p \text{ が } K \text{ で惰性かつ } N_E = 1) \\ \frac{p-1}{2} & (p \text{ が } K \text{ で惰性かつ } N_E = -1) \end{cases}$

(ℓ は k の基本単数)

が分かるが、「 k を固定したとき、前頁の不等号が等号になるような p が無限個あるだろうか。」ということが、問題としてあげられる。これに関して、

$$P_k^1(x) := \{p \leq x \mid p \text{ は } k \text{ で分解する素数}\}$$

$$P_k^2(x) := \{p \leq x \mid p \text{ は } k \text{ で惰性する素数}\}$$

$$P_k^i(x) := \#P_k^i(x) \quad (i=1, 2)$$

$$N_k^i(x) := \#\{p \in P_k^i(x) \mid l_p = \ell_p\} \quad (i=1, 2)$$

とおくとき、石川勝、北岡良え両氏が、[1]で、 $\frac{N_k^i(x)}{P_k^i(x)}$ について計算し、次のことを予想した。

Conjecture 1 (Ishikawa-Kitaoka)

$$\lim_{x \rightarrow \infty} \frac{N_k^i(x)}{P_k^i(x)} (\neq 0) \quad \text{が存在する。}$$

この予想は、次の「 $\text{mod } p$ の原始根に関する Artin 予想」と関連があるものと思われる。

Conjecture 2 (Artin 予想)

$a \in \mathbb{Z} \setminus \{0, \pm 1\}$, かつ a が平方数でないとする。このとき、

$$\lim_{x \rightarrow \infty} \frac{\#\{p \leq x \mid ((\mathbb{Z}/p\mathbb{Z})^* : \langle \overline{a} \rangle) = 1\}}{\#\{p \leq x\}} (\neq 0) \quad \text{が存在する。}$$

ここで特に、 Q がsquare-free かつ $Q \neq 1(4)$ とすると、この密度は、

$$A := \prod_{q:\text{prime}} \left(1 - \frac{1}{q(q-1)}\right) = 0.3739558136\cdots$$

であると予想される。この A を、Artin 定数と呼ぶことにする。

さて、Conjecture 1 に戻ると、その密度は、特に分解する素数に対しては、 $\frac{3}{2}A$ になるらしい。(中には多少異なるものもある。) 何故だろうか。

Artin 予想については、Hooley [2] が、一般Riemann 予想 (代数体 K のDedekind zeta 関数 $\zeta_K(s)$ の零点に関するRiemann 予想、以下GRHと略す。) を仮定して証明した。それと同様にして、Conjecture 1 も証明出来ないかどうか考える。その結果、分解する素数については、GRHを仮定すれば証明出来ることが分かった。以下、そのことについて、概略を報告する。

§ 1. 問題の書き換え

以後、 k で分解する素数 p についてのみ、 I_p を考えるので、§0の $P_k^1(x)$, $N_k^1(x)$ を単に、 $P_k(x)$, $N_k(x)$ と書く。また、これから q はすべて素数を表すものとする。さらに、 $x, \eta_1, \eta_2 \in \mathbb{R}^+$, $n \in \mathbb{Z}^+$ に対して、次のように定義する。

$$N_K(x, \eta_1) := \#\{p \in \mathbb{P}_K(x) \mid q \nmid I_p \text{ for } \forall q \leq \eta_1\}$$

$$M_K(x, \eta_1, \eta_2) := \#\{p \in \mathbb{P}_K(x) \mid \eta_1 < \exists q \leq \eta_2; q \mid I_p\}$$

$$P_K(x, n) := \#\{p \in \mathbb{P}_K(x) \mid n \mid I_p\}$$

このとき、 $\xi_1 = \frac{1}{6} \log x$, $\xi_2 = x^{\frac{1}{2}} (\log x)^{-2}$, $\xi_3 = x^{\frac{1}{2}} \log x$ とおくと、 $N_K(x)$ に対して、次の不等式が成り立つ。

$$\begin{aligned} & N_K(x, \xi_1) - M_K(x, \xi_1, \xi_2) - M_K(x, \xi_2, \xi_3) - M_K(x, \xi_3, x-1) \\ & \leq N_K(x) = N_K(x, x-1) \leq N_K(x, \xi_1) \end{aligned} \quad (1.1)$$

ここで、左辺の第3項と第4項について評価すると、

$$M_K(x, \xi_2, \xi_3) = O(x \log \log x (\log x)^{-2})$$

$$M_K(x, \xi_3, x-1) = O(x (\log x)^{-2})$$

となる。また、第1項と第2項については、 $P_K(x, n)$ を用いて、

$$N_K(x, \xi_1) = \sum_{n \mid Q(\xi_1)} \mu(n) P_K(x, n) \quad \text{ただし、} Q(\xi_1) := \prod_{q \leq \xi_1} q$$

$$M_K(x, \xi_1, \xi_2) = \sum_{\xi_1 < q \leq \xi_2} P_K(x, q)$$

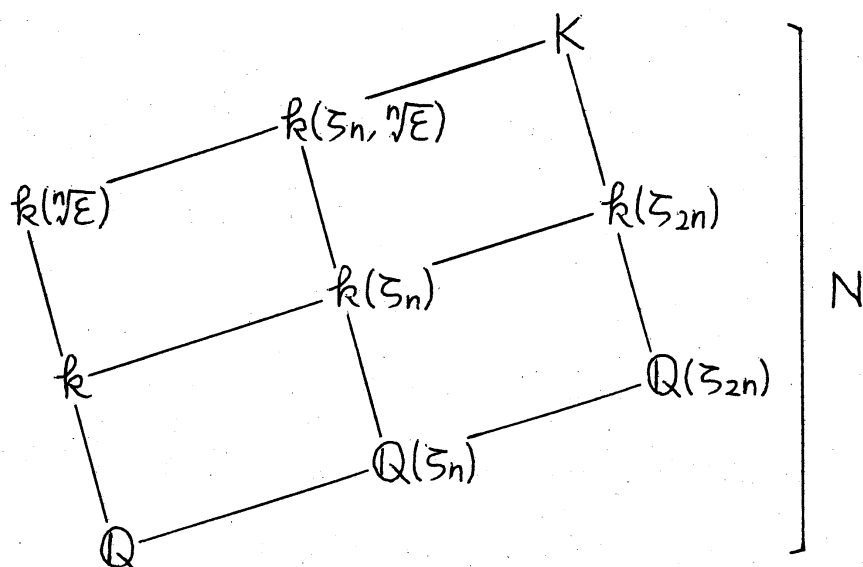
と表せる。よって、(1.1)は次のようになる。

$$\begin{aligned} N_K(x) &= \sum_{n \mid Q(\xi_1)} \mu(n) P_K(x, n) + O\left(\sum_{\xi_1 < q \leq \xi_2} P_K(x, q)\right) \\ &\quad + O(x \log \log x (\log x)^{-2}) \end{aligned} \quad (1.2)$$

§2. $P_K(x, n)$ と K の拡大体の関係について

次に、 $P_K(x, n)$ を評価するために、 $P_K(x, n)$ を別の関数を用いて表すことを考える。 K の基本単数を、 $\varepsilon = \frac{a+b\sqrt{m}}{2}$

($\varepsilon > 1$)とする。また、 $K = \mathbb{K}(\zeta_{2n}, \sqrt[\varepsilon]{E})$, $N = [K:\mathbb{Q}]$,
 $D = d(K)$ (K の判別式) とする。



このとき、

$$n \parallel p \iff p \text{ が } K/\mathbb{Q} \text{ で完全分解}$$

がいえ、 $K/\mathbb{Q}$ で不分岐だが完全分解しない K の prime、
 および分岐する K の prime の個数は、それぞれ、 $Nx^{\frac{1}{2}}$,
 $N\omega(D)$ ($\omega(D)$: D の素因子の個数) で押さえられるので、

$$\begin{aligned} \pi_K(x) &:= \#\{\mathfrak{p}: K \text{ の prime} \mid N(\mathfrak{p}) \leq x\} \\ &= NP_{\mathbb{K}}(x, n) + O(Nx^{\frac{1}{2}}) + O(N\omega(D)) \end{aligned}$$

すなわち次のようになる。

$$P_{\mathbb{K}}(x, n) = \frac{1}{N} \pi_K(x) + O(x^{\frac{1}{2}} \omega(D)) \quad (2.1)$$

Remark) $N\varepsilon = -1$ のときは、 K が、 $\mathbb{K}(\sqrt[\varepsilon]{E})/\mathbb{Q}$ の Galois 閉包
 となる。 $N\varepsilon = 1$ のときは、 $\mathbb{K}(\sqrt[\varepsilon]{E})/\mathbb{Q}$ の Galois 閉包は、

$\mathbb{K}(\zeta_n, \sqrt[n]{\varepsilon})$ であるが、このとき、

$$n \mid ((\mathbb{O}/\mathbb{P})^\times : \langle \varepsilon \rangle) \iff \mathbb{P} \text{ が } \mathbb{K}(\zeta_n, \sqrt[n]{\varepsilon}) / \mathbb{Q} \text{ で完全分解}$$

が成り立ち、この $\langle \varepsilon \rangle$ を $\bar{\varepsilon}$ に変えるためには、 $\mathbb{K}$ まで拡大しなければならない。

ここで、 $N = [K:\mathbb{Q}]$ の値を計算しておこう。まず明らかに、 $N \mid 2n\varphi(2n)$ 。このとき、

$$\delta(n) := \frac{2n\varphi(2n)}{N} = [\mathbb{Q}(\zeta_{2n}) \cap \mathbb{K}(\sqrt[n]{\varepsilon}) : \mathbb{Q}]$$

であるが、 $\mathbb{Q}(\zeta_{2n}) \cap \mathbb{K}(\sqrt[n]{\varepsilon})$ は abel 体であり、 $\mathbb{K}(\sqrt[n]{\varepsilon})$ の部分体で abel 体となるものは、 $\mathbb{K}(\sqrt[n]{\varepsilon})$ の部分体しかあり得ない。

さらに、 $\mathbb{K}(\sqrt[n]{\varepsilon})$ は、 $N\varepsilon = -1$ のとき abel 体でないが、 $N\varepsilon = 1$ のときは、 $\mathbb{K}(\sqrt[n]{\varepsilon}) = \mathbb{K}\left(\frac{\sqrt{a+2} + \sqrt{a-2}}{2}\right) = \mathbb{Q}(\sqrt{a}, \sqrt{a+2})$ となり、abel 体である。これに注意して、 $D_0 := d(\mathbb{K})$ とおき、 $N\varepsilon = 1$ のときはさらに、 $D_1 := [4, d(\mathbb{Q}(\sqrt{a+2}))]$, $D_2 := [4, d(\mathbb{Q}(\sqrt{a-2}))]$ とおけば、次が成立する。

Lemma 2.1

$$N = [K:\mathbb{Q}] = \frac{2n\varphi(2n)}{\delta(n)}$$

ただし、

・ $N\varepsilon = -1$ のとき

$$\delta(n) := \begin{cases} 1 & (D_0 \nmid 2n) \\ 2 & (D_0 \mid 2n) \end{cases}$$

・ $N\varepsilon = 1$ のとき

$$\delta(n) := \begin{cases} 1 & (\nexists i; D_i \mid 2n) \\ 2 & (\exists! i; D_i \mid 2n) \\ 4 & (\forall i, D_i \mid 2n) \end{cases}$$

§3. $\pi_K(x)$ と $P_K(x, n)$ の評価

さて、ここですべての n に関する体 K で同時に $\pi_K(x)$ を評価したい。そのために、GRH を仮定し、次を使う。

Proposition 3.1 (Hooley)

GRH が成立する体 K で一様に、

$$\pi_K(x) = \text{li } x + O(Nx^{\frac{1}{2}} \log^N \sqrt{|D|} x) \quad \left(\text{li } x := \int_2^x \frac{dt}{\log t} \right)$$

が成り立つ。ただし、 $N = [K : \mathbb{Q}]$, $D = d(K)$

Remark) Hooley は [2] で、 $K = \mathbb{Q}(\zeta_n, \sqrt[n]{a})$ のとき、

$D | (n^2 |a| \omega(n))^N$ に注意して、 $\pi_K(x) = \text{li } x + O(Nx^{\frac{1}{2}} \log n x)$ を示した。しかし、それと全く同じ議論により、Proposition 3.1 に到達する。

再び $K = \mathbb{Q}(\zeta_{2n}, \sqrt[n]{E})$ とする。このとき、 $d(\mathbb{Q}(\zeta_{2n})) | (2n)^{\varphi(2n)}$, $d(\mathbb{Q}(\sqrt[n]{E})) | d^n n^{2n}$ に注意すれば、 $D | (2n^3 D_0)^N$ が成り立つ。これにより Proposition 3.1 は、 $\pi_K(x) = \text{li } x + O(Nx^{\frac{1}{2}} \log n x)$ と変形され、(2.1) は、 $\omega(n) = O(\log n)$ に注意をして、次のようになる。

Proposition 3.2

$\mathbb{Q}(\zeta_{2n}, \sqrt[n]{E})$, $\forall n \in \mathbb{Z}^+$ で GRH が成立
 $\Rightarrow P_K(x, n) = \frac{1}{N} \text{li } x + O(x^{\frac{1}{2}} \log n x)$

が n について一様に成り立つ。

§ 4. 定理

Lemma 2.1 と Proposition 3.2 により、(1.2) を変形する。

まず、右辺第 1 項について、

$$\begin{aligned} \sum_{n|Q(\xi_1)} \mu(n) P_k(x, n) &= \sum_{n|Q(\xi_1)} \left(\frac{\mu(n) \delta(n)}{2n \varphi(2n)} \right) \log x + O(x^{\frac{1}{2}} \log nx) \\ &= \frac{1}{2} \left(\sum_{n=1}^{\infty} \frac{\mu(n) \delta(n)}{n \varphi(2n)} \right) \log x + O\left(\frac{x}{(\log x)^2}\right) \end{aligned}$$

ここで、 $D_i^* := \frac{D_i}{(2, D_i)}$ ($i=0, 1, 2$) とおけば、 $N\varepsilon = -1$ のとき、

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\mu(n) \delta(n)}{n \varphi(2n)} &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n \varphi(2n)} + \sum_{\substack{n=1 \\ D_0^* | n}}^{\infty} \frac{\mu(n)}{n \varphi(2n)} \\ &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n \varphi(2n)} + \sum_{n=1}^{\infty} \frac{\mu(n D_0^*)}{n D_0^* \varphi(2n D_0^*)} \\ &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n \varphi(2n)} + \frac{\mu(D_0^*)}{D_0^* \varphi(2D_0^*)} \sum_{\substack{n=1 \\ (n, D_0^*)=1}}^{\infty} \frac{\mu(n)}{n \varphi(2n)} \\ &= \prod_q \left(1 + \frac{\mu(q)}{q \varphi(2q)} \right) + \frac{\mu(D_0^*)}{D_0^* \varphi(2D_0^*)} \prod_{q \nmid D_0^*} \left(1 + \frac{\mu(q)}{q \varphi(2q)} \right) \\ &= \left(1 + \frac{\mu(D_0^*)}{D_0^* \varphi(2D_0^*)} \prod_{q \mid D_0^*} \left(1 - \frac{1}{q \varphi(2q)} \right)^{-1} \right) \prod_q \left(1 - \frac{1}{q \varphi(2q)} \right) \end{aligned}$$

Artin 定数 A を用いると、

$$\sum_{n=1}^{\infty} \frac{\mu(n)\delta(n)}{n\varphi(2n)} = \frac{3}{2} \left(1 + \mu(D_0^*) \prod_{q|D_0^*} \frac{1}{q\varphi(2q)-1} \right) A$$

$N\varepsilon=1$ のときも同様にして、

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\mu(n)\delta(n)}{n\varphi(2n)} &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n\varphi(2n)} + \sum_{i=0}^2 \left(\sum_{\substack{n=1 \\ D_i^*|n}}^{\infty} \frac{\mu(n)}{n\varphi(2n)} \right) \\ &= \frac{3}{2} \left(1 + \sum_{i=0}^2 \mu(D_i^*) \prod_{q|D_i^*} \frac{1}{q\varphi(2q)-1} \right) A \end{aligned}$$

よって、ここで、

$$\begin{aligned} r(D_i^*) &:= \mu(D_i^*) \prod_{q|D_i^*} \frac{1}{q\varphi(2q)-1} \quad (i=0,1,2) \\ R &:= \begin{cases} r(D_0^*) & (N\varepsilon=-1) \\ \sum_{i=0}^2 r(D_i^*) & (N\varepsilon=1) \end{cases} \end{aligned} \quad (4.1)$$

とおくと、

$$\sum_{n|Q(\xi_1)} \mu(n) P_{\mathbb{R}}(x, n) = \frac{3}{4} (1+R) A \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right)$$

が成り立つ。

次に、(1.2)の右辺第2項については、

$$\begin{aligned} \sum_{\xi_1 < q \leq \xi_2} P_{\mathbb{R}}(x, q) &= \sum_{\xi_1 < q \leq \xi_2} \left(\frac{\delta(q)}{2q(q-1)} \log x + O(x^{\frac{1}{2}} \log x) \right) \\ &= O\left(\frac{x}{\xi_1 \log x}\right) + O\left(\frac{x^{\frac{1}{2}} \xi_2 \log x}{\log \xi_2}\right) = O\left(\frac{x}{(\log x)^2}\right) \end{aligned}$$

以上により、次の定理が証明される。

Theorem

$k(\zeta_{2n}, \sqrt[n]{\varepsilon}), \forall n \in \mathbb{Z}^+$ で GRH が成立

$$\Rightarrow N_k(x) = \frac{3}{4}(1+R)A \frac{x}{\log x} + O\left(\frac{x \log \log x}{(\log x)^2}\right)$$

§5. R の値について

さて、(4.1)より、 $N\varepsilon = -1$ のとき、 R の値は m から簡単に求められ、 $R \rightarrow 0 (m \rightarrow \infty)$ が分かる。しかし、 $N\varepsilon = 1$ のときはそのようにはならない。 $N\varepsilon = 1$ のときの R を求めるためには、基本単数の計算をしなければならず、簡単ではないが、いくつかの特殊な m については簡単に求められるので、最後にそれをあげておく。

Proposition 5.1

次の (i), (ii) のいずれかが成り立っているとする。

(i) $m = q$ または $2q, q \equiv 3(4)$ (このとき常に $N\varepsilon = 1$)

(ii) $m = 2q, q \equiv 1(4)$ かつ $N\varepsilon = 1$

(このためには、 $q \equiv 1(8)$ が必要条件)

このとき、 $R = \frac{1}{3\{q(q-1)-1\}}$

Proof) $\{D_0, D_1, D_2\} = \{4q, 8q, 8\}$ となることに注意して、計算すればよい。 ■

Proposition 5.2

q_1, q_2 を異なる素数とし、次の (iii), (iv) のいずれかが成り立っているとする。

(iii) $m = q_1 q_2, q_1 \equiv q_2 \equiv 3(4)$ (このとき常に $N\varepsilon = 1$)

(iv) $m = q_1 q_2, q_1 \equiv q_2 \equiv 1(4)$ かつ $N\varepsilon = 1$

(このためには、 $\left(\frac{q_2}{q_1}\right) = \left(\frac{q_1}{q_2}\right) = 1$ が必要条件)

$$\text{このとき、 } R = \frac{q_1(q_1-1) + q_2(q_2-1) + 1}{3\{q_1(q_1-1)-1\}\{q_2(q_2-1)-1\}}$$

Proof) $\{D_0, D_1, D_2\} = \{q_1 q_2, 4q_1, 4q_2\}$ となることに注意すればよい。 ■

◦ なお、詳細については、只今準備中です。

参考文献

- [1] M. Ishikawa and Y. Kitaoka, On the distribution of units modulo prime ideals in real quadratic fields, J. Reine Angew. Math. (to appear)
- [2] C. Hooley, On Artin's Conjecture, J. Reine Angew. Math. 225 (1967), 209-220.