Counting certain imaginary quadratic fields with prescribed 2-class order

Takumi Tomita

2005 年 12 月 26 日

概要

Let $I^{(2)}$ be a set of imaginary quadratic fields whose discriminant $d = pq$ and let $I_s^{(2)}$ be the subset of $I^{(2)}$ whose elements have a given 2-class order s (2-class order is the 2-order of the ideal class group of K). It is conjectured that the density of $I_s^{(2)}$ in $I^{(2)}$ has positive proportion. Using a computer, we find out a conjectual such constant explicitly. This is ture for the cases where $s = 1$ by the result of F. Gerth in [G 84]. In this talk we give a sufficient condition for the cases where $s = 2$.

1 Motivation

1984 年 H. Cohen と H. W. Lenstra は論文 [C-L 84] において $\mathbf{Q}$ 上 (ここでは体は全て $\mathbf{Q}$ 上のものを考える) の n 次巡回 Galois 拡大体 K のイデアル類群[*1]の prime to p-part[*2] の分布に関し, とても興味深い予想をいくつも提出した. この講演では $p = 2$ の場合 (2 次体) にのみ制限して考える. $p = 2$ であれば「巡回 Galois 拡大」という仮定は自動的に満たされる. 簡単に 2 次体について復習しておくと, 一般に 2 次体は非平方整数 m を用いて $\mathbf{Q}(\sqrt{m})$ [*3]と書くことができ, m が正である時は実 2 次体 (real quadrat ic field), m が負の時は虚 2 次体 (imaginary quadratic field) と呼ばれる. イデアル類群 $Cl(K)$ の prime to 2-part を $Cl(K)_{\mathrm{odd}}$ と書くことにすると

(C1) $Cl(K)_{\mathrm{odd}}$ が cyclic になる確率は

$$\frac{\zeta(2)\zeta(3)}{3\zeta(6)C_\infty\eta_\infty(2)} \fallingdotseq 97.7575\ \%$$

(C2) 奇素数 p が $|Cl(K)_{\mathrm{odd}}|$ を割る確率は

$$f(3) \fallingdotseq 43.987\ \%, f(5) \fallingdotseq 23.967\ \%, f(7) \fallingdotseq 16.320\% \quad \text{etc}$$

といった $Cl(K)_{\mathrm{odd}}$ に関する様々な予想が定式化されており (詳しくは [C-L 84] 参照), これらはいずれも今だ未解決の問題である. さて, ここで Cohen-Lenstra では扱われていないイデアル類群の primary p-part[*4] はどうなるのか？という疑問がわいてくる. そこで「発見的方法 (heuristic method)」でなに

[*1] 定義は §2 で簡単に復習する, これは有限アーベル群.
[*2] p と素な元全体が作る部分群.
[*3] $\mathbf{Q}(\sqrt{m})$ は 1 と $\sqrt{m}$ で $\mathbf{Q}$ 上生成される $\mathbf{C}$ の部分体.
[*4] p 冪で消える元全体の作る部分群, Sylow p-部分群.

かしかの規則を求める為に虚 2 次体に限ってその primary 2-part をコンピューターを用いて類数の分布を調べた. そのデータを下に興味深い規則 (予想) を見つけることができたのでそのことについて報告する.

※ 虚 2 次体を題材に選んだ理由は, 後に述べるがその類数の表 (データ) を比較的簡単に作ることができるからである. 一般に代数体 (実 2 次体 or 3 次以上の $\mathbf{Q}$ の有限次拡大体) の類数を (沢山) 計算する事は容易ではない.

2 イデアル類群

以下 2 次体 $K_m = \mathbf{Q}(\sqrt{m})$ のみを考える.

イデアル類群の定義

$$\omega := \begin{cases} \dfrac{1+\sqrt{m}}{2} & m \equiv 1 \pmod 4 \\ \sqrt{m} & m \equiv 2,3 \pmod 4 \end{cases}$$

とおいて $\mathbf{Q}(\sqrt{m})$ の部分環 $O_{K_m} := \mathbf{Z} + \mathbf{Z}w$ を K_m の整数環という ($\{1,\omega\}$ を基底とする rank 2 の自由 $\mathbf{Z}$-加群). この時 K_m の有限生成 O_{K_m}-部分加群 $\mathfrak{a}$ ($\neq 0$) を K_m の分数イデアルと呼ぶ. 分数イデアル全体は自然にアーベル群の構造を持ち[*5]それをイデアル群と呼び $\mathcal{I}_{K_m}$ と書く. 単項分数イデアル $(a) = aO_{K_m}$ 全体は $\mathcal{I}_{K_m}$ の部分群をなし, それを $\mathcal{P}_{K_m}$ と書く. K_m のイデアル類群 $Cl(K_m)$ とは商群 $\mathcal{I}_{K_m}/\mathcal{P}_{K_m}$ で定義されるものである (可換環論の初歩で習うように $\mathbf{Z}$ の全てのイデアルは一つの元から生成されるが ($\mathbf{Z}$ は PID である), O_{K_m} は一般にそうではない. $Cl(K_m)$ は O_{K_m} が PID からどのくらいずれているのかをあらわす群である). 簡単ではないがこれは有限アーベル群であることが知られており, その位数を類数とよび h_{K_m} と書く.

類数の求め方

$m < 0$ とする. 整数論では通常 K_m の類数 h_{K_m} の計算に「解析的類数公式」[*6] と呼ばれるものを使うわけであるが, その計算にはゼータ関数の特殊値を使うなど簡単にアルゴリズムを使って計算できるようなものではない. しかし 2 次体 K_m に関しては次のような 2 次形式を用いたシンプルな計算方法が知られている[*7](実際のアルゴリズムは [Co 93, Algotithm 5.3.5] 参照).

$$h(K_m) = \#\{f = ax^2 + bxy + cy^2 \in \mathbf{Z}[x,y] \mid (\text{条件})\}$$

条件は以下:

(i) $b^2 - 4ac = D_{K_m}$
(ii) $a > 0$
(iii) $|b| \leq a \leq c$ (但し $b \geq 0$ if $a = |b|$ or $a = c$)
(iv) $|b| \leq a \leq \sqrt{|D_{K_m}|/3}$

[*5] その単位元は $(1) = O_{K_m}$, $\mathfrak{a}$ の逆元は $\mathfrak{a}^{-1} := \{x \in K_m \mid x\mathfrak{a} \subset O_{K_m}\}$.
[*6] 「解析的類数公式」は 2 次体とは限らないより一般の代数体の公式.
[*7] Gauss の 2 次形式の理論に基づく.

※ D_{K_m} は K_m の判別式. 即ち

$$D_{K_m} = \begin{cases} m & \text{if } m \equiv 1 \pmod 4 \\ 4m & \text{if } m \equiv 2, 3 \pmod 4 \end{cases}$$

とする.

例えば $K = \mathbf{Q}(\sqrt{-119})$ の時, $-119 \equiv 1 \pmod 4$ なので $D_K = -119$. この時条件 (i)-(iv) を満たす (a, b, c) の組は $(1, 1, 30), (2, \pm 1, 15), (3, \pm 1, 10), (4, \pm 3, 8), (5, \pm 1, 6), (6, 5, 6)$ の 10 個. 従って $h_K = 10$.

3 実験結果と予想

§1 でも断ったように, 以下では虚 2 次体のみ考えることにする. 虚 2 次体 $K_m = \mathbf{Q}(\sqrt{-m})$ (m は非平方数) に対して $Cl(K_m)$ を K_m のイデアル類群とする. A_{K_m} を $Cl(K_m)$ の primary 2-part (i. e. Sylow 2-subgroup) とし, $Cl(K_m)$, A_{K_m} の位数を それぞれ $h(K_m), h_2(K_m)$ とする. 任意の正整数 t (ramification number) と非負整数 s (2-calss order) と正の実数 x に対して次のような記号を用意する:

$$\begin{array}{lcl} I^{(t)} & := & \{K_m \mid \text{exactly } t \text{ primes ramigy in } K_m/\mathbf{Q}\} \\ I^{(t)}(x) & := & \{K_m \in I^{(t)} \mid m \le x\} \\ I_s^{(t)} & := & \{K_m \in I^{(t)} \mid \mathrm{ord}_2(h_2(K_m)) = s\} \\ I_s^{(t)}(x) & := & \{K_m \in I^{(t)_s} \mid {}^{m \le x}\} \end{array}$$

※ ramification number t は 判別式 D_{K_m} の異なる素因子の数.

※ 2-class order $\mathrm{ord}_2(*) = s$ は $*$ を素因数分解した時の 2 の冪の個数をあらわす. 例えば $\mathrm{ord}_2(40) = \mathrm{ord}_2(2^3 \cdot 5) = 3$, $\mathrm{ord}_2(7/32) = \mathrm{ord}_2(2^{-5} \cdot 7) = -5$ など.

定義 3.1.

$$\begin{array}{lcl} d_s^{(t)}(x) & := & \dfrac{|I_s^{(t)}(x)|}{|I^{(t)}(x)|} \\ d_s^{(t)} & := & \lim\limits_{x \to \infty} d_s^{(t)}(x) \end{array}$$

先のアルゴリズムを用いて $d_s^{(t)}(x)$ を $x \le 10^7$ の範囲で (10000 を 1 メモリとしてインプット) グラフ化したものが図 1 である[*8]. この図より $t = 2$ の場合次のような予想を立てることができる:

予想 3.2.

$$d_s^{(2)} = \frac{1}{2^s}$$

この予想は次と同値である:

予想 3.3.

$$|I_s^{(2)}(x)| \sim \frac{1}{2^{s+1}} \frac{x \log\log x}{\log x}$$

[*8] (Benchmark) この単純なアルゴリズムを用いて $x \le 10^7$ までの表 (図 1) を作るのに Pentium 4 CPU 3.00GHz マシンでおよそ 70h かかる (プログラムには C を用いた).

※ $f(x) \sim g(x)$ とは $f(x)/g(x) \to 1$ $(x \to \infty)$ であることをいう. 例えば $1+x \sim x$, $\sin(x) \sim x$ など.

この予想に関して F. Gerth 氏による次のような結果 $(s=1)$ がある:

定理 3.4. [G 84, Proposition 2.1.]

$$d_1^{(2)} = 1/2$$

詳しくは述べられないが, Gerth 氏のこの定理に関する証明の主要部分は, 定理の十分条件として, 次の Legendre symbol の和に関する評価式を証明することである:

命題 3.5 (F. Gerth)**.** p, q を $p \equiv -q \equiv 1 \pmod 4$ なる奇素数とする. この時

$$\sum_{pq \leq x} \left(\frac{q}{p}\right) = o\left(\frac{x \log\log x}{\log^2 x}\right)$$

が成り立つ.

※ 一般に整数 a, b に対して

$$\left(\frac{a}{b}\right)_n := \begin{cases} 1 & \text{if } x^n \equiv a \pmod b \text{ が解を持つ} \\ -1 & \text{otherwise} \end{cases}$$

と定める. 特に $n=2$ の時は Legendre Symbol と呼ばれ, 下付の添え字を省略する.

※ $f(x) = o(g(x))$ とは $f(x)/g(x) \to 0$ $(x \to \infty)$ であることをいう. 例えば $x = o(x^2)$, $\sin(x) = o(x)$ など.

同様の議論を高次の s (≥ 2) に拡張しようとすると, 一般には予想の十分条件として上のような指標和の評価式のようなきれいな条件を書くことができないが, $s=2$ の場合は 2 次の diophantus 方程式 $ax^2 + by^2 = z^2$ の可解性に関する Legendre の定理などを用いることによって, 4 乗剰余記号を用いて次のような十分条件を得ることができる (cf [B 04]):

定理 3.6. 次の 2 つの評価式

$$\begin{cases} \displaystyle\sum_{pq \leq x} \left(\frac{-q}{p}\right)_4 = o\left(\frac{1}{2}\frac{x(\log\log x)}{\log x}\right) \\ \displaystyle\sum_{pq \leq x} \left(\frac{-q}{p}\right)_4 \left(\frac{q}{p}\right) = o\left(\frac{1}{2}\frac{x(\log\log x)}{\log x}\right) \end{cases}$$

が正しければ $d_2^{(2)} = 1/4$ となる.

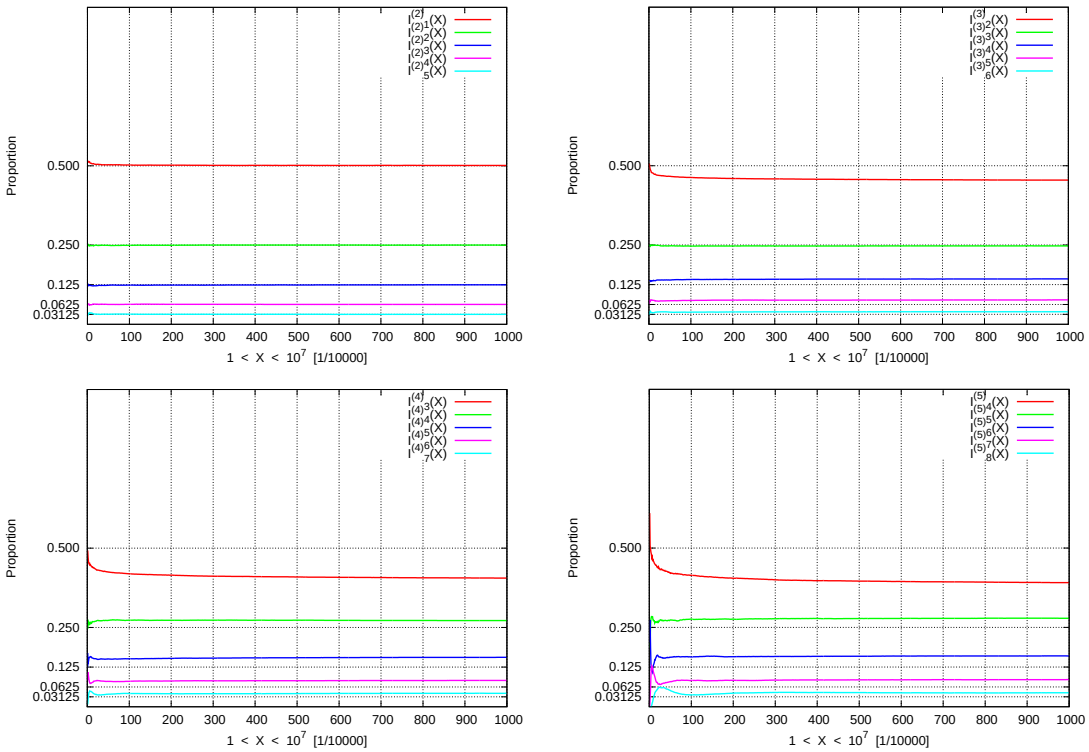

図 1　$d_s^{(t)}(10000x)$ のグラフ

$$
\begin{aligned}
&I_1^{(2)}, I_2^{(2)}, I_3^{(2)}, I_4^{(2)}, I_5^{(2)} \quad \rightarrow(\text{左上})\\
&I_2^{(3)}, I_3^{(3)}, I_4^{(3)}, I_5^{(3)}, I_6^{(3)} \quad \rightarrow(\text{右上})\\
&I_3^{(4)}, I_4^{(4)}, I_5^{(4)}, I_6^{(4)}, I_7^{(4)} \quad \rightarrow(\text{左下})\\
&I_4^{(5)}, I_5^{(5)}, I_6^{(5)}, I_7^{(5)}, I_8^{(5)} \quad \rightarrow(\text{右下})
\end{aligned}
$$

※ [G 84] より $d_1^{(2)} = 0.5, d_2^{(3)} = 0.4375, d_3^{(4)} = 0.375, d_4^{(5)} = 0.350586$ が知られている.

参考文献

[B 04] J. M. Basilla, *The quadratic fields with discriminant divisible by exactly two primes and with "narrow" class number divisible by 8.*, Proc. Japan Acad. Ser. A Math. Sci. 80 (2004), no. 10, pp. 187–190 (2005).

[C-L 84] H. Cohen and H. W. Lenstra, *Heuristics on class groups of number fields.*, Lecture Notes in Math., 1068, Springer, Berlin, 1984, pp. 33-62.

[Co 93] H. Cohen, *A course in computational algebraic number theory.*, Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[G 84] F. Gerth III, *The 4-class ranks of quadratic fields.*, Invent. Math. 77 (1984), no. 3, pp. 489–515.