数理解析研究所講究録
1154巻 2000年 106-116

実2次体の3次不分岐巡回拡大について

東京都立大学理学研究科　小松 亨 (Toru Komatsu)

§1. 序

2次体の類数の整除性については, 多くの研究がなされている. それぞれの正の整数 m に対して, 類数が m で割れる虚2次体が無限に存在することは古くから知られている (Nagell [N]). また, 実2次体についても そのようなものが無限に存在することが 示されている ($m=3$ のときは Honda [H], m が一般の正の整数のときは Yamamoto[Y] 及び Weinberger [W]). これらの結果は, 類数が m で割れるためのある十分条件を与えることによって 得られている. そして 類数が3で割れるためのある必要十分条件が示されている (Kishi-Miyake [K-M]). また, 1997年10月に行われた研究集会 "代数的整数論とその周辺 (京大数理研)" において, この結果についての講演がなされている (Kishi [K]). 今回述べる結果は, まず この Kishi-Miyake の定理の精密化である. さらに, 実2次体の3次不分岐巡回拡大をすべて求めるアルゴリズムが得られた (詳しくは [Ko] を見て下さい). §2 では, 主定理であるアルゴリズムを述べる. §3 では, Kishi-Miyake の定理及びその精密化した定理たちと主定理との関係について述べる. §4 と §5 では, アルゴリズムを用いて得られた幾つかの計算結果について述べる. §6 では, 虚2次体の場合についての注意を述べる.

§2. 主定理

定理 2.1 (実2次体のすべての3次不分岐巡回拡大及び *ideal* 類群の 3-*rank* を求めるアルゴリズム).

d は平方因子を持たない正の整数とする.

Step 1. 整数 e, e^* を

$$e = \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4, \\ 2 & \text{otherwise}, \end{cases}$$

$$e^* = \frac{2}{e} \quad (e \cdot e^* = 2)$$

とする.

(A) d が 3 で割れないときについて.

Step 2. 4 条件

$$\begin{cases} \text{(A.1)} & \dfrac{1}{e^*}\sqrt[3]{e^*(27d+1)} \le c < e\sqrt{d}, \\ \text{(A.2)} & a^2 + 27db^2 = e^{*2}c^3, \\ \text{(A.3)} & \gcd(a,c) \mid \operatorname{lcm}(e, 3d), \\ \text{(A.4)} & v_3(a) \neq 2 \end{cases}$$

をすべて満たす組 $(a,b,c)(\in \mathbb{N}\times\mathbb{N}\times\mathbb{N})$ 全体から成る集合を W_d とする. W_d のそれぞれの元 (a,b,c) に対して, 3 条件

$$\begin{cases} \text{(A.5)} & -\dfrac{c}{e} < s < \dfrac{c}{e}, \\ \text{(A.6)} & 3bs \equiv a \pmod{e^*c}, \\ \text{(A.7)} & s^2 \equiv -3d \pmod{e^{*2}c} \end{cases}$$

をすべて満たす整数 $s(\in \mathbb{Z})$ を求める. 整数 s は, それぞれの元 (a,b,c) に対し, 唯一つ存在するので, それを $s_{(a,b,c)}$ と書く. W_d の部分集合 V_d を

$$V_d = \left\{ (a,b,c) \in W_d \;\middle|\; \left| \frac{s_{(a,b,c)} + \sqrt{-3d}}{e^*c} \right| > 1 \right\}$$

と定義する.

Step 3. V_d のそれぞれの元 (a,b,c) に対して, 3 次多項式 $f_{a,c}(Z)$ を

$$f_{a,c}(Z) = Z^3 - 3cZ - ea$$

と定義する. 最後に, 整数 n 及び実数 r を

$$n = \sharp V_d, \quad r = \log_3(2n+1) \in \mathbb{R}$$

とおく.

結論. V_d と実 2 次体 $\mathbb{Q}(\sqrt{d})$ のすべての 3 次不分岐巡回拡大は 1 対 1 に対応する. 具体的には

$$V_d \quad \overset{1:1}{\longleftrightarrow} \quad \text{実 2 次体 } \mathbb{Q}(\sqrt{d}) \text{ のすべての 3 次不分岐巡回拡大}$$

$$(a,b,c) \quad \longmapsto \quad \mathrm{Spl}_{\mathbb{Q}}(f_{a,c}(Z))$$

と対応する. ここで, $\mathrm{Spl}_{\mathbb{Q}}(f_{a,c}(Z))$ は $f_{a,c}(Z)$ の $\mathbb{Q}$ 上の最小分解体とする. 整数 n は, 実 2 次体の 3 次不分岐巡回拡大の個数に一致する. 実数 r は, 整数であり, 実 2 次体の *ideal* 類群の 3-*rank* に一致する.

(B) d が 3 で割れるときは, 上記の 7 条件 (A.1) ~ (A.7) を

$$\begin{cases} \text{(B.1)} & \dfrac{1}{3e^*}\sqrt[3]{9e^*(d+3)} \le c < \dfrac{e\sqrt{d}}{3}, \\ \text{(B.2)} & a^2 + \dfrac{d}{3}b^2 = e^{*2}c^3, \\ \text{(B.3)} & \gcd(a,c) \mid \mathrm{lcm}(e, \dfrac{d}{3}), \\ \text{(B.4)} & \max\{v_3(a^2e^2 - d - 4), v_3(a), v_3(b)\} \ge 2. \end{cases}$$

$$\begin{cases} \text{(B.5)} & -\dfrac{c}{e} < s < \dfrac{c}{e}, \\ \text{(B.6)} & bs \equiv a \pmod{e^*c}, \\ \text{(B.7)} & s^2 \equiv -\dfrac{d}{3} \pmod{e^{*2}c}. \end{cases}$$

にそれぞれ変える. そして, V_d の定義を

$$V_d = \left\{ (a,b,c) \in W_d \;\middle|\; \left| \frac{s_{(a,b,c)} + \sqrt{-d/3}}{e^*c} \right| > 1 \right\}$$

とする. このとき, 結論は, 場合 (A) と同様である.

注意 2.2. 集合 W_d は, 高々有限集合である. 定理 2.1 のそれぞれの step は, 高々有限回の計算で行われる. V_d のそれぞれの組 (a,b,c) に対し, 多項式 $f_{a,c}(Z)$ は $\mathbb{Q}$ 上既約である.

§ 3. Kishi-Miyake の定理及びその精密化した定理と主定理との関係

まず, Kishi-Miyake の定理について述べる.

定理 **3.1**([K-M]). d を平方因子を持たない整数とする. このとき, 次の 2 条件 (I), (II) は同値である.

(I) 2 次体 $\mathbb{Q}(\sqrt{d})$ の類数が 3 で割れる.

(II) 以下の 4 条件 (1), (2), (3) 及び (4) をすべて満たすそれぞれ 0 でない整数の組 $(x,u,w) \in \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\neq 0}$ が存在する.

(1) $\gcd(u,w) = 1$,

(2) $Z^3 - uwZ - u^2$ は $\mathbb{Q}$ 上既約,

(3) $dx^2 = 4uw^3 - 27u^2$,

(4) 条件

(4.i) $3 \nmid w$,

(4.ii) $3 \mid w$, $uw \not\equiv 3 \pmod 9$, $u \equiv w \pm 1 \pmod 9$,

(4.iii) $3 \mid w$, $uw \equiv 3 \pmod 9$, $u \equiv w \pm 1 \pmod{27}$

のうち 少なくとも 1 つを満たす.

さらに, このような組が存在するとき, $Z^3 - uwZ - u^2 = 0$ の根は, $\mathbb{Q}(\sqrt{d})$ の 3 次不分岐巡回拡大を生成する. 逆に, $\mathbb{Q}(\sqrt{d})$ の 3 次不分岐巡回拡大は, このようにして すべて得られる.

定理 3.1 を次のように精密化する.

定理 **3.2.** d を平方因子を持たない整数とする. このとき, 次の 2 条件 (I), (II) は同値である.

(I) 2 次体 $\mathbb{Q}(\sqrt{d})$ の類数が 3 で割れる.

(II) 定理 3.1 の (1), (2), (3) 及び以下の条件 (4′) をすべて満たすそれぞれ 0 でない整数の組 $(x,u,w) \in \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\neq 0}$ が存在する.

(4′) ある素数 $p > 3$ が存在して $w = p^4$, $u = dk^2 (k \in \mathbb{N})$.

さらに, このような組が存在するとき, $Z^3 - uwZ - u^2 = 0$ の根は, $\mathbb{Q}(\sqrt{d})$ の 3 次不分岐巡回拡大を生成する. 逆に, $\mathbb{Q}(\sqrt{d})$ の 3 次不分岐巡回拡大は, このようにして すべて得られる.

注意 3.3. 定理 3.1 と定理 3.2 の異なる所は, 条件 (4) と (4′) である. (4′) を満たす組 (x, u, w) は, (4.i) を満たす. 特に, 定理 3.1 の主張から (4.ii)(4.iii) を外しても, 同値性は保たれる. それぞれの 3 次不分岐巡回拡大に対して, (4′) を満たす素数 p は, いくらでも大きく取ることができる. 1 つの 3 次不分岐巡回拡大に対して, その拡大を与える組は 無限に存在する.

注意 3.4. 定理 2.1 の条件 (A.1)〜(A.4) たちは, 定理 3.1 及び定理 3.2 の条件 (1)〜(4) 及び (4′) と対応する.

定理 2.1		定理 3.1 及び定理 3.2
(A.1)	$\longleftrightarrow$	(2)
(A.2)	$\longleftrightarrow$	(3)
(A.3)	$\longleftrightarrow$	(1)
(A.4)	$\longleftrightarrow$	(4) 並びに (4′)

§ 4. 計算例

定理 2.1 をプログラム化し, 平方因子を持たない $1 \leq d \leq 10^5 = 100{,}000$ を満たす整数 d に対して, 実 2 次体 $\mathbb{Q}(\sqrt{d})$ の 3 次不分岐巡回拡大をすべて求めた. その結果をまとめた表が 表 4.5 である.

注意 4.1 (表 4.5 の見方について). $m = m_0$ の行の n-sf の列の数字は, $1000(m_0 - 1) + 1 \leq d \leq 1000m_0$ を満たす整数 d の中で, 平方因子を持つもの (non-squarefree) の個数である. また, $m = m_0$ 行の 0 の列の数字は, $1000(m_0 - 1) + 1 \leq d \leq 1000m_0$ を満たす平方因子を持たない整数 d の中で, 実 2 次体 $\mathbb{Q}(\sqrt{d})$ の ideal 類群の 3-rank r_d が 0 となるものの個数である. 同様に, 1(及び 2) の列の数字は, r_d が 1(及び 2) と

なるものの個数である. なお, $1 \leq d \leq 10^5$ を満たす整数 d の中で, r_d が 3 以上となるものは 存在しない.

表 4.5 をグラフ化したのが 図 4.6 及び 4.7 である.

注意 4.2 (図 4.6 と 4.7 の見方について). 図 4.6 では, 横軸を m とし, 縦軸を $1000(m-1)+1 \leq d \leq 1000m$ の中でそれぞれ n-pt, $r_d = 0, 1, 2$ となる割合 (%) とする. 一方, 図 4.7 では, 横軸を m とし, 縦軸を $1 \leq d \leq 1000m_0$ の中でそれぞれ n-pt, $r_d = 0, 1, 2$ となる割合 (%) とする.

注意 4.3 ($r_d = 2$ となる実 2 次体 $\mathbb{Q}(\sqrt{d})$ について). $1 \leq d \leq 10^5$ を満たす平方因子を持たない整数 d の中で, $r_d = 2$ となるものは

$d = 23659, 32009, 42817, 43063, 43486, 51694, 53507, 53678, 62501, 62687,$

$72329, 83414, 85431, 85666, 97719$

の 15 個である. これらのうち, d が小さい方から 8 個に対しての計算結果を§5 ((i)〜(viii)) に記すことにする.

注意 4.4. 計算を実行するための数式処理ソフトは, Maple V を使用した. また, 定理 2.1 をプログラム化したものの text file 並びに Maple Internal Format File, $1 \leq d \leq 10^5$ を満たす整数 d に対しての計算結果, 表 4.5 等については, 都立大の TNT(Tools on Number Theory Web) サーバ内の以下の所に置かさせていただいている.

ftp://tnt.math.metro-u.ac.jp/pub/table/UnramCubExt_RealQuadField.tar.gz

m	n-sf	0	1	2	m	n-sf	0	1	2	m	n-sf	0	1	2
1	392	573	35	0	36	393	535	72	0	71	392	531	77	0
2	393	557	50	0	37	393	543	64	0	72	391	530	79	0
3	391	557	52	0	38	396	542	62	0	73	394	528	77	1
4	391	557	52	0	39	394	528	78	0	74	396	527	77	0
5	391	550	59	0	40	392	542	66	0	75	392	531	77	0
6	396	544	60	0	41	390	532	78	0	76	393	529	78	0
7	391	555	54	0	42	390	539	71	0	77	393	544	63	0
8	390	543	67	0	43	387	528	84	1	78	390	545	65	0
9	392	544	64	0	44	389	546	63	2	79	391	538	71	0
10	390	549	61	0	45	394	541	65	0	80	397	528	75	0
11	396	539	65	0	46	390	558	52	0	81	391	531	78	0
12	394	537	69	0	47	389	546	65	0	82	397	524	79	0
13	392	546	62	0	48	391	529	80	0	83	386	548	66	0
14	392	544	64	0	49	394	520	86	0	84	392	536	71	1
15	389	549	62	0	50	395	542	63	0	85	390	546	64	0
16	392	535	73	0	51	389	528	83	0	86	395	533	70	2
17	389	547	64	0	52	391	522	86	1	87	391	528	81	0
18	394	543	63	0	53	395	540	65	0	88	390	521	89	0
19	392	546	62	0	54	395	543	60	2	89	387	541	72	0
20	393	544	63	0	55	390	529	81	0	90	395	526	79	0
21	391	537	72	0	56	396	532	72	0	91	391	536	73	0
22	390	538	72	0	57	393	533	74	0	92	390	519	91	0
23	397	553	50	0	58	390	536	74	0	93	389	526	85	0
24	390	536	73	1	59	399	529	72	0	94	391	549	60	0
25	395	529	76	0	60	390	540	70	0	95	394	532	74	0
26	388	540	72	0	61	386	550	64	0	96	394	533	73	0
27	397	537	66	0	62	391	541	68	0	97	393	542	65	0
28	389	543	68	0	63	394	535	69	2	98	393	529	77	1
29	393	539	68	0	64	392	536	72	0	99	394	539	67	0
30	388	552	60	0	65	394	535	71	0	100	390	532	78	0
31	393	541	66	0	66	392	548	60	0	計	39206	53828	6951	15
32	397	530	73	0	67	393	524	83	0					
33	395	531	73	1	68	389	539	72	0					
34	384	547	69	0	69	398	528	74	0					
35	395	533	72	0	70	388	542	70	0					

表 4.5

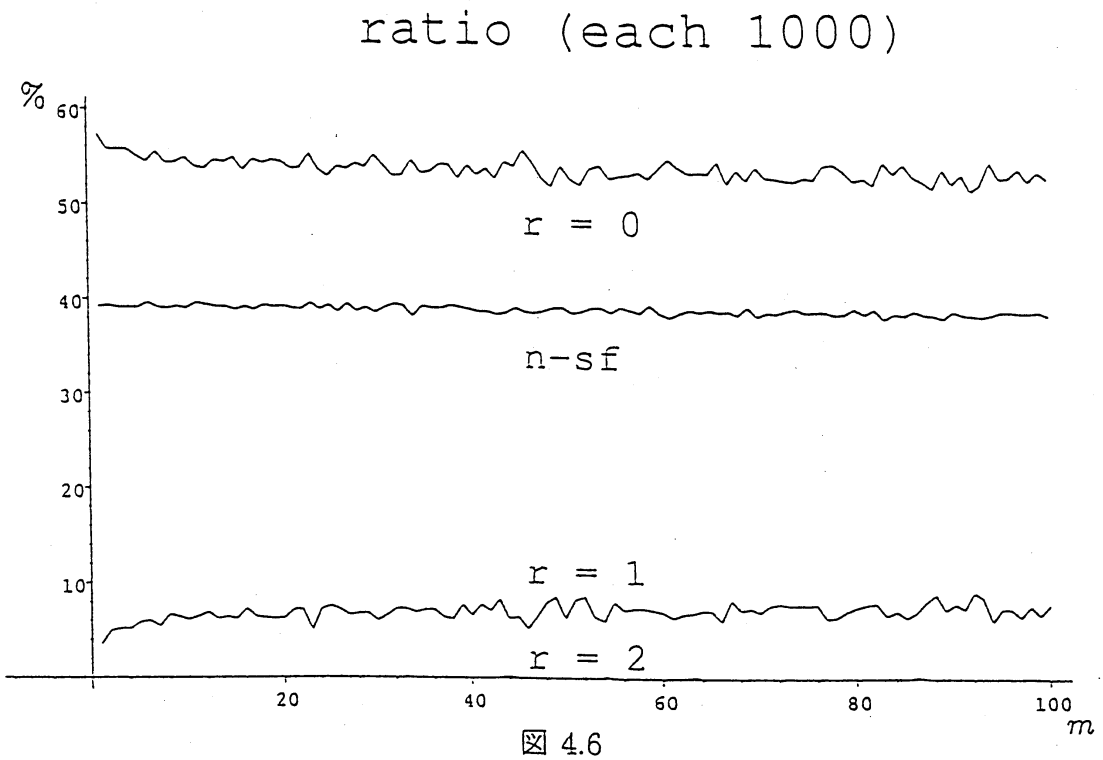
ratio (each 1000)
%
60
50
40
30
20
10
r = 0
n-sf
r = 1
r = 2
20
40
60
80
100
m

図 4.6

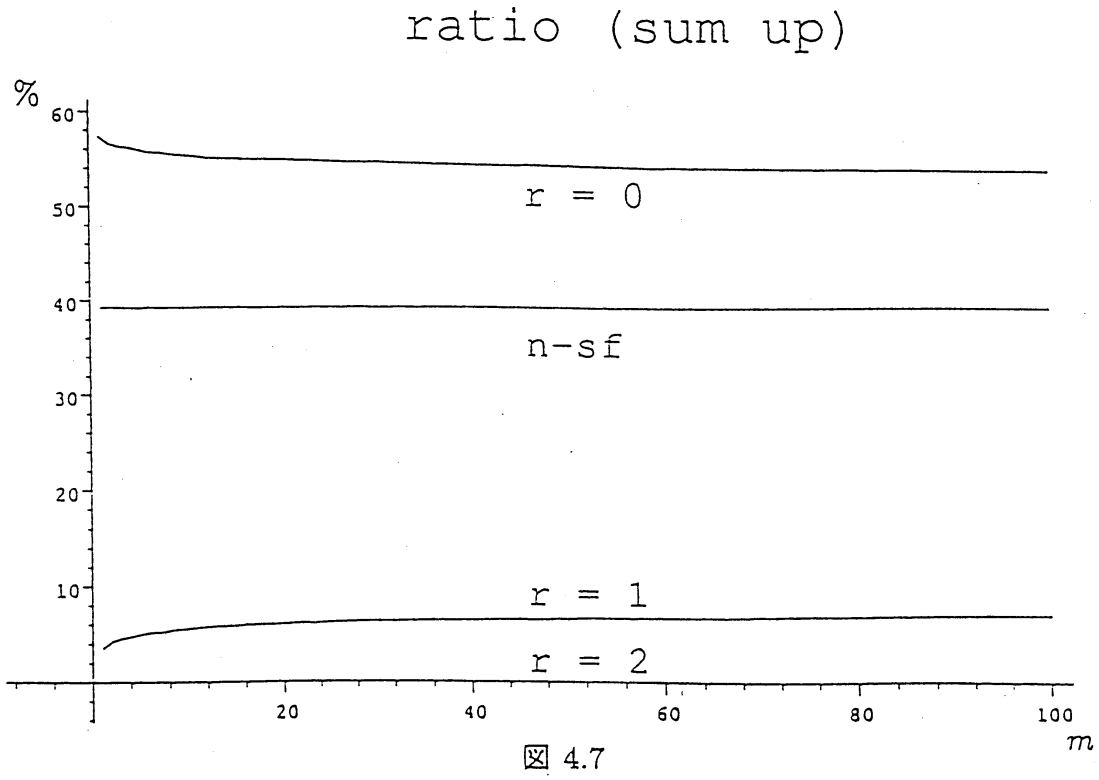
ratio (sum up)
%
60
50
40
30
20
10
r = 0
n-sf
r = 1
r = 2
20
40
60
80
100
m

図 4.7

§ 5. ideal 類群の 3-rank が 2 となる実 2 次体 $\mathbb{Q}(\sqrt{d})$ $(1 \leq d \leq 6.0 \times 10^4)$

(i) $d = 23659$. $(e = 2,\ e^* = 1,\ d_0 = -70977.)$

c	a	b	s	$\lvert\frac{s+\sqrt{d_0}}{e^*c}\rvert$	$f_{a,c}(Z)$
138	270	2	45	$1.9\cdots$	$Z^3 - 414Z - 540$
181	1837	2	−86	$1.5\cdots$	$Z^3 - 543Z - 3674$
226	2998	2	−103	$1.2\cdots$	$Z^3 - 678Z - 5996$
241	2872	3	−29	$1.1\cdots$	$Z^3 - 723Z - 5744$
298	1862	6	−29	$0.8\cdots$	—

(ii) $d = 32009$. $(e = 1,\ e^* = 2,\ d_0 = -96027.)$

c	a	b	s	$\lvert\frac{s+\sqrt{d_0}}{e^*c}\rvert$	$f_{a,c}(Z)$
61	209	1	29	$2.5\cdots$	$Z^3 - 183Z - 209$
103	956	2	−81	$1.5\cdots$	$Z^3 - 309Z - 956$
123	2565	1	117	$1.3\cdots$	$Z^3 - 369Z - 2565$
157	3823	1	123	$1.06\cdots$	$Z^3 - 471Z - 3823$
177	4617	1	123	$0.94\cdots$	—

(iii) $d = 42817$. $(e = 1,\ e^* = 2,\ d_0 = -128451.)$

c	a	b	s	$\lvert\frac{s+\sqrt{d_0}}{e^*c}\rvert$	$f_{a,c}(Z)$
75	729	1	−57	$2.4\cdots$	$Z^3 - 225Z - 729$
103	1793	1	−89	$1.7\cdots$	$Z^3 - 309Z - 1793$
115	1208	2	−67	$1.5\cdots$	$Z^3 - 345Z - 1208$
183	4833	1	147	$1.05\cdots$	$Z^3 - 549Z - 4833$
205	5771	1	147	$0.94\cdots$	—

(iv) $d = 43063$. $(e = 2,\ e^* = 1,\ d_0 = -129189.)$

c	a	b	s	$\lvert\frac{s+\sqrt{d_0}}{e^*c}\rvert$	$f_{a,c}(Z)$
190	1486	2	−69	$1.9\cdots$	$Z^3 - 570Z - 2972$
237	2943	2	−102	$1.5\cdots$	$Z^3 - 711Z - 5886$
265	2854	3	111	$1.4\cdots$	$Z^3 - 795Z - 5708$
310	5014	2	9	$1.1\cdots$	$Z^3 - 930Z - 10028$

(v) $d = 43486$. ($e = 2$, $e^* = 1$, $d_0 = -130458$.)

c	a	b	s	$\lvert\frac{s+\sqrt{d_0}}{e^*c}\rvert$	$f_{a,c}(Z)$
169	361	2	32	$2.1\cdots$	$Z^3 - 507Z - 722$
174	756	2	-48	$2.0\cdots$	$Z^3 - 522Z - 1512$
259	2609	3	-113	$1.4\cdots$	$Z^3 - 777Z - 5218$
331	2629	5	87	$1.1\cdots$	$Z^3 - 993Z - 5258$
417	8235	2	-87	$0.8\cdots$	—

(vi) $d = 51694$. ($e = 2$, $e^* = 1$, $d_0 = -155082$.)

c	a	b	s	$\lvert\frac{s+\sqrt{d_0}}{e^*c}\rvert$	$f_{a,c}(Z)$
201	1593	2	-36	$1.9\cdots$	$Z^3 - 603Z - 3186$
282	4104	2	120	$1.4\cdots$	$Z^3 - 846Z - 8208$
331	1171	5	56	$1.2\cdots$	$Z^3 - 993Z - 2342$
394	3304	6	96	$1.02\cdots$	$Z^3 - 1182Z - 6608$
417	8181	2	-96	$0.97\cdots$	—

(vii) $d = 53507$. ($e = 2$, $e^* = 1$, $d_0 = -160521$.)

c	a	b	s	$\lvert\frac{s+\sqrt{d_0}}{e^*c}\rvert$	$f_{a,c}(Z)$
186	810	2	-51	$2.1\cdots$	$Z^3 - 558Z - 1620$
213	1971	2	9	$1.8\cdots$	$Z^3 - 639Z - 3942$
265	2368	3	57	$1.5\cdots$	$Z^3 - 795Z - 4736$
325	4618	3	152	$1.3\cdots$	$Z^3 - 975Z - 9236$

(viii) $d = 53678$. ($e = 2$, $e^* = 1$, $d_0 = -161034$.)

c	a	b	s	$\lvert\frac{s+\sqrt{d_0}}{e^*c}\rvert$	$f_{a,c}(Z)$
222	2268	2	-66	$1.8\cdots$	$Z^3 - 666Z - 4536$
249	3105	2	-105	$1.6\cdots$	$Z^3 - 747Z - 6210$
331	179	5	34	$1.2\cdots$	$Z^3 - 993Z - 358$
379	4267	5	-44	$1.06\cdots$	$Z^3 - 1137Z - 8534$
430	5228	6	-44	$0.93\cdots$	—

§ 6. 虚 2 次体の場合についての注意

虚 2 次体についても, 定理 2.1 と同様な結果が得られるように思われる. 実際に, (A.2),(A.3) 及び (A.4) は, 一般の 2 次体に対して有効である. また, (A.1) と同様なものが 虚 2 次体についてもある. 問題になるのが (A.5),(A.6) 及び (A.7) に対応する議論である. 定理 2.1 が efficient なものになった理由として, "議論が 虚 2 次体 $\mathbb{Q}(\sqrt{-3d})$ の方に移り, また 虚 2 次体の単数群が有限である" ということが挙げられる. 一方, 虚 2 次体 $\mathbb{Q}(\sqrt{d'})$ について, 定理 2.1 と同様な結果を得ようとすると, 今度は実 2 次体 $\mathbb{Q}(\sqrt{-3d'})$ の方に議論が移る. ここで 実 2 次体の単数群は, 階数 1 の自由 $\mathbb{Z}$ 加群であり, 議論が 若干 複雑になる. しかしながら, 我々は その問題を克服し, 定理 2.1 と同様な結果を虚 2 次体についても得ている.

References

[H] T. Honda, *On real quadratic fields whose class number are multiples of* 3, J. Reine Angew. Math. **233** (1968), 101–102.

[K] Y. Kishi, 類数が 3 で割れる二次体の特徴づけ, 数理解析研究所講究録 **1026** (1998), 151–155.

[K-M] Y. Kishi and K. Miyake, *Parametrization of the Quadratic Fields Whose Class Numbers are Divisible by Three*, J. Number Theory **80** (2000), 209–217.

[Ko] T. Komatsu, *On unramified cyclic cubic extensions of real quadratic fields (preprint)*.

[N] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hanburg **1** (1922), 140–150.

[W] P. J. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory **5** (1973), 237–241.

[Y] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.

Department of Mathematics, Tokyo Metropolitan University, Minami-Ohsawa 1-1 Hachioji-shi Tokyo, 192-0397 Japan

E-mail address: trkomatu@comp.metro-u.ac.jp