# Shanksの3次多項式に関する幾つかの性質について

小松 亨 (上智大学)

## 1 導入

本稿ではShanksの生成的3次多項式の数論, とくに特殊化に関する不変量について考察する. まず生成的多項式の定義について述べる.

**定義.** $G$ を有限群, $k$ を体とする. 関数体 $k(\mathfrak{t})$ 上の多項式 $F(\mathfrak{t}, X) \in k(\mathfrak{t})[X]$, $\mathfrak{t} = (t_1, t_2, \ldots, t_m)$ が以下の条件を満たすとき, $F(\mathfrak{t}, X)$ は $k$ 上生成的な $G$ 多項式である, という.

> 体 $k$ 上の任意の拡大体 $K$ について, $K$ の全てのガロア $G$ 拡大 $L$ は $K$ 上のある特殊化 $\mathfrak{s} = (s_1, s_2, \ldots, s_m) \in K^m$ により $L = \mathrm{Spl}_K F(\mathfrak{s}, X)$ と表わされる.

例えばクンマー多項式 $X^n - t$ は生成的多項式の典型的な例である, つまり $X^n - t$ は $n$ 円分体 $\mathbb{Q}(\zeta_n)$ 上生成的な $n$ 次巡回多項式である. 但し $\zeta_n$ は $\bar{\mathbb{Q}}$ 内の1の原始 $n$ 乗根とする. 生成的多項式に関しては以下のような問題が考えられる.

**部分体問題 (Subfield problem)**(S 問題)**.** 体 $K$ 上の2つの特殊化 $\mathfrak{a}, \mathfrak{b}$ で与えられる拡大体たち $\mathrm{Spl}_K F(\mathfrak{a}, X), \mathrm{Spl}_K F(\mathfrak{b}, X)$ が $\mathrm{Spl}_K F(\mathfrak{a}, X) \subseteq \mathrm{Spl}_K F(\mathfrak{b}, X)$ となるための条件を $\mathfrak{a}$, $\mathfrak{b}$, $K$ の言葉で記述せよ.

**同型問題 (Isomorphism problem)**(I 問題)**.** 体 $K$ 上の2つの特殊化 $\mathfrak{a}, \mathfrak{b}$ で与えられる拡大体たち $\mathrm{Spl}_K F(\mathfrak{a}, X), \mathrm{Spl}_K F(\mathfrak{b}, X)$ が等しくなるための条件を $\mathfrak{a}$, $\mathfrak{b}$, $K$ の言葉で記述せよ.

**分岐およびフロベニウス問題 (Ramification and Frobenius problem)**(RF 問題)**.** 体 $K$ 上の拡大体 $\mathrm{Spl}_K F(\mathfrak{s}, X)$ の分岐およびフロベニウス置換を $\mathfrak{s}$, $K$ を用いて計算する方法を与えよ.

**アルゴリズム問題** (A 問題)**.** 与えられた数論的性質を満たすガロア $G$ 拡大体たちについて, それらを実現するための特殊化を見つける計算法を与えよ.

生成的多項式のアルゴリズム問題の解決は類体の構成問題に有効である. 以前の論文 [5] ではShanksの $\mathbb{Q}$ 上生成的な3次巡回多項式 $F(t, X) = X^3 - 3tX^2 - (3t+3)X - 1$ のアルゴリズム問題を解くことにより, 与えられた導手をもつ $\mathbb{Q}$ 上の3次巡回体を全て求めるアルゴリズムを完成させた. 本稿では, 論文 [5] でえられた幾つかの補題を用いてShanksの多項式 $F(t, X)$ のある性質について考察する.

## 2 知られている性質について

多項式 $F(t, X)$ をShanksの3次多項式

$$F(t, X) = X^3 - 3tX^2 - (3t+3)X - 1$$

とする. 3 次巡回体 ($\mathbb{Q}$ 上の 3 次ガロア拡大でそのガロア群が 3 次巡回群 $\mathcal{C}_3$ に同型な体) 全体の族を $\mathcal{L}$ と書く.

**補題.** $F(t,X)$ は $\mathbb{Q}$ 上生成的な 3 次巡回多項式である.

**補題.** 多項式 $F(t,X)$ の多項式判別式 $\mathrm{disc}_X F(t,X)$ は $3^4(t^2+t+1)^2$ である.

有理数 $s \in \mathbb{Q}$ に対して $F(s,X)$ の $\mathbb{Q}$ 上の最小分解体 $\mathrm{Spl}_{\mathbb{Q}}F(s,X)$ を $L_s$ と書く. 集合 $SCF(\mathbb{Q})$ を

$$SCF(\mathbb{Q}) = \{s \in \mathbb{Q} | 3s \in \mathbb{Z} \text{ かつ } \mu((3s)^2+3(3s)+9) \neq 0\}$$

と定義する, ただし $\mu$ はメビウス関数とする. ここで整数 $m \in \mathbb{Z}$ に対して $\mu(m) \neq 0$ であることは $m$ が平方因子を持たないことと同値である. この集合の元 $s \in SCF(\mathbb{Q})$ で構成される 3 次巡回体 $L_s$ は simplest cubic field と呼ばれている ([11]).

**補題 (**Washington [13]**).** $s \in SCF(\mathbb{Q})$ に対して体 $L_s$ の体判別式 $\mathrm{disc}(L_s)$ は $3^4(s^2+s+1)^2$ に等しい. $F(s,X)=0$ の解の 1 つを $x \in \bar{\mathbb{Q}}$ とすると $L_s$ の整数環 $\mathcal{O}(L_s)$ は加群として $1, x, x^2$ または $1, x, \sigma(x)$ で生成される, つまり $\mathcal{O}(L_s) = \mathbb{Z}+\mathbb{Z}x+\mathbb{Z}x^2 = \mathbb{Z}+\mathbb{Z}x+\mathbb{Z}\sigma(x)$ である. 但し $\sigma$ はガロア拡大 $L_s/\mathbb{Q}$ のガロア群 $\mathrm{Gal}(L_s/\mathbb{Q}) \simeq \mathcal{C}_3$ の生成元とする.

**補題 (**Washington [13]**).** $s \in SCF(\mathbb{Q})$ に対して $x, \sigma$ は上の補題と同じとする. このとき体 $L_s$ の単数群 $\mathcal{O}(L_s)^\times$ は乗法群として $-1, x, \sigma(x)$ で生成される, つまり

$$\mathcal{O}(L_s)^\times = \{\pm x^{m_1}\sigma(x)^{m_2} | m_1, m_2 \in \mathbb{Z}\}$$

である.

**注意.** Shanks の 3 次多項式 $F(t,X)$ の同型問題は Morton [6] (1994) と Chapman [1] (1996) によって解決されている. $F(t,X)$ の一般化 $R(t,X)$ が陸名氏 [9] (2002) によって与えられている. 陸名氏の巡回多項式 $R(t,X)$ の同型問題, 分岐およびフロベニウス問題を筆者 [4] (2004) が解決している. Shanks の 3 次多項式 $F(t,X)$ のアルゴリズム問題を筆者 [5] (2007) が解決している.

**補題.** 有理数 $s \in \mathbb{Q}$ に対して $v_2(s) \geq 0$ ならば $F(s,X)$ は有限体 $\mathbb{F}_2$ 上既約である, ただし $v_p$ は $p$ 進的加法付値とする. 特に $s \in \mathbb{Q}$ に対して $3s \in \mathbb{Z}$ ならば $F(s,X)$ は有理数体 $\mathbb{Q}$ 上既約であり, $L_s \in \mathcal{L}$ である.

**系.** $\{L_s | s \in \mathbb{Q} \cap \mathbb{Z}_2\} \subsetneq \mathcal{L}$, ただし $\mathbb{Z}_2$ は 2 進整数環とする.

**証明.** 1 つ上の補題により, $s \in \mathbb{Q} \cap \mathbb{Z}_2$ ならば拡大 $L_s/\mathbb{Q}$ で 2 は惰性する. しかし 3 次巡回体には素数 2 が完全分解するものも存在する. 例えば導手が 31 の 3 次巡回体 $L \in \mathcal{L}$ について素数 2 は拡大 $L/\mathbb{Q}$ で完全分解する. よって補集合 $\mathcal{L} - \{L_s | s \in \mathbb{Q} \cap \mathbb{Z}_2\}$ は空ではない. □

**注意.** 多項式 $F(t,X)$ の生成性から $\{L_s | s \in \mathbb{Q}\} = \mathcal{L} \cup \{\mathbb{Q}\}$ である.

**補題 (**小松 [5]**).** 有理数 $s \in \mathbb{Q}$ に対して $v_2(s) \geq 0$ ならば $L_s \in \mathcal{L}$ であり, 拡大 $L_s/\mathbb{Q}$ で 2 は惰性する. 有理数 $s \in \mathbb{Q}$ に対して $v_2(s) < 0$ かつ $L_s \in \mathcal{L}$ であるならば, 拡大 $L_s/\mathbb{Q}$ で 2 は完全分解する.

**補題.** 3 次巡回体 $L \in \mathcal{L}$ と 3 以外の素数 $p$ に対して, 拡大 $L/\mathbb{Q}$ で $p$ が分解するならば $L = L_s$ かつ $v_p(s) = -1$ となる有理数 $s \in \mathbb{Q}$ が存在する.

## 3　ある不変量について

関数体 $\mathbb{Q}(t)$ 上の拡大体 $\mathrm{Spl}_{\mathbb{Q}(t)}F(t,X)$ のガロア群 $\mathrm{Gal}(\mathrm{Spl}_{\mathbb{Q}(t)}F(t,X)/\mathbb{Q}(t))$ は 3 次巡回群 $\mathcal{C}_3$ に同型であることから $\{L_s|s\in\mathbb{Q}\}\subseteq\mathcal{L}\cup\{\mathbb{Q}\}$ である．実際は多項式 $F(t,X)$ の $\mathbb{Q}$ 生成性により, 特殊化で与えられる拡大体たちの族 $\{L_s|s\in\mathbb{Q}\}$ は族 $\mathcal{L}\cup\{\mathbb{Q}\}$ に等しい．3 次巡回体 $L\in\mathcal{L}$ に対してその体を実現する特殊化の集まり $\{s\in\mathbb{Q}|L_s=L\}$ を $V_L$ と書く．ここで $F(t,X)$ の生成性により $V_L\neq\emptyset$ である．有理数 $s=a/b\in\mathbb{Q}$ $(a,b\in\mathbb{Z},\ \gcd(a,b)=1)$ に対して $H(s)$ を $s$ のベイユ高さ, つまり $H(s)=\max\{|a|,|b|\}$ とする．3 次巡回体 $L\in\mathcal{L}$ の不変量 $H_L$ を $H_L=\min\{H(s)|s\in V_L\}$ で定義する．$L$ の導手を $f_L$ と書き, $f_L$ の 3 と素な部分を $g_L$ と書く．ここで $3\mid f_L$ ならば $g_L=f_L/9$ となりそれ以外は $g_L=f_L$ であることに注意する．このとき次の大変興味深い不等式が成り立つ.

**命題 A(**小松 [5]**).**

$$1<\frac{H_L}{\sqrt{g_L/3}}<2.$$

この比 $H_L/\sqrt{g_L/3}$ を $R_L$ と書く．導手がある一定以下の 3 次巡回体 $L$ 全体に対して $R_L$ の分布 (点 $(f_L,R_L)$ の分布) 図は次のページの通りである．3 つの図での導手の上限はそれぞれ $3^7=2187$, $3^9=19683$, $3^{11}=177147$ である．これら図から容易に推測できるが, 次の命題が成り立つ.

**命題 B.** 集合 $\{R_L|L\in\mathcal{L}\}$ は集合 $[1,2]=\{r\in\mathbb{R}|1\leq r\leq 2\}$ で稠密である．特に命題 $A$ の不等式は最良である.

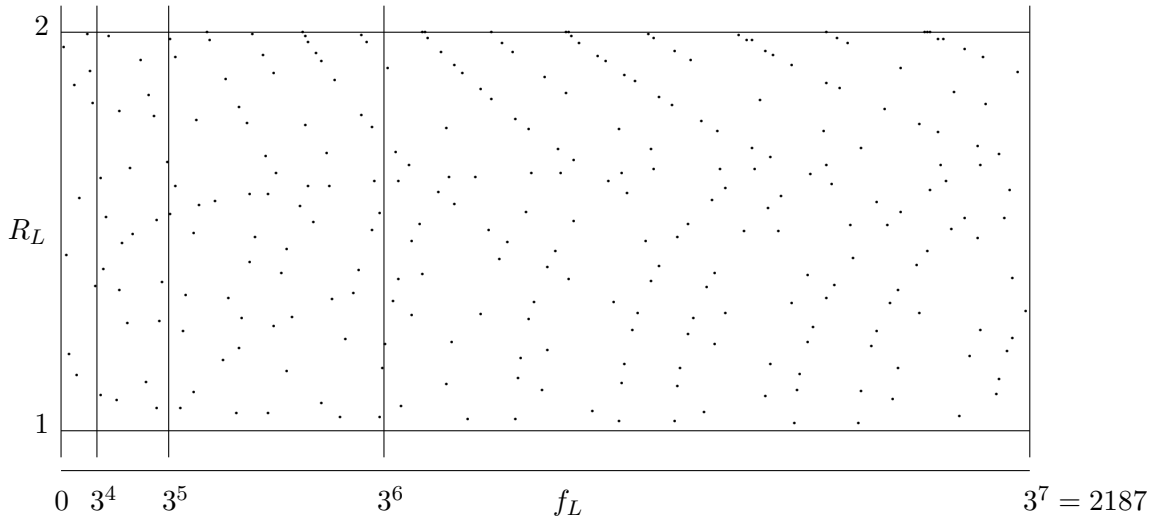
実数 $\xi\in\mathbb{R}$ と正の実数 $\varepsilon>0$ に対して 4 条件

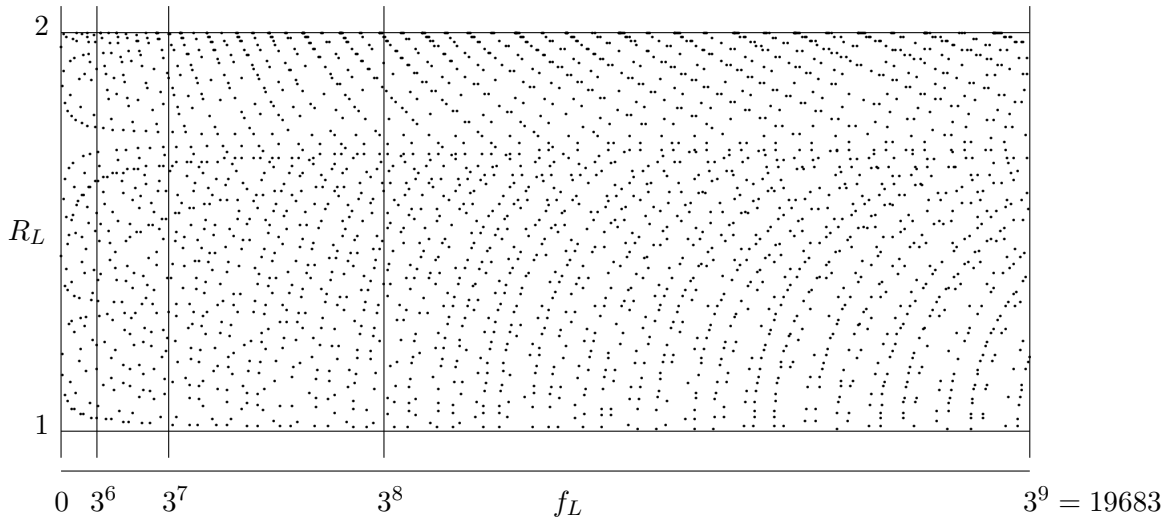
$$\begin{array}{ll}(1) & b\geq 1, b\in 3\mathbb{Z}\\ (2) & -b/2<a<b\\ (3) & |a/b-\xi|<\varepsilon\\ (4) & \mu(a^2+ab+b^2)\neq 0\end{array}$$

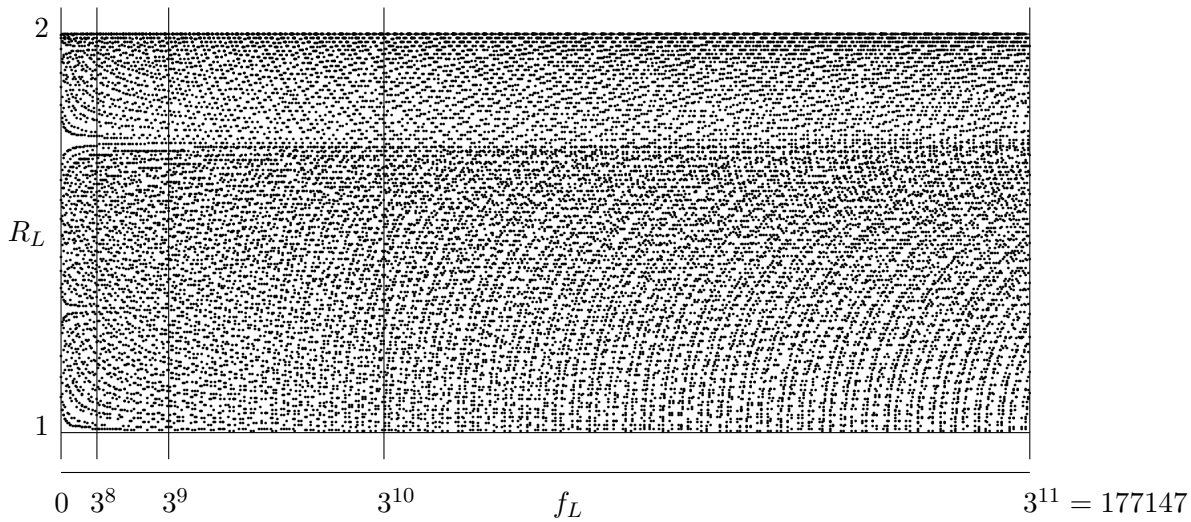
を満たす整数 $a,b$ の組 $(a,b)$ 全体の集合を $W(\xi,\varepsilon)$ と書く.

**命題 C.** 不等式 $-1/2\leq\xi\leq 1$ を満たす任意の実数 $\xi\in\mathbb{R}$ と任意の正の実数 $\varepsilon>0$ に対して $W(\xi,\varepsilon)\neq\emptyset$ である.

**証明.** $-1/2\leq\xi<1$ となる有理数 $\xi\in\mathbb{Q}$ を 1 つ固定する．整数 $\alpha\in\mathbb{Z}$ と正の整数 $\beta\geq 1$ を $\xi=\alpha/\beta$ となるものとする．正の整数 $m\in\mathbb{Z}$, $m\geq 1$ に対して数列 $\{a_m\}$, $\{b_m\}$ を $a_m=3\alpha\beta m+1$, $b_m=3\beta^2m$ で定義する．ここで $-\beta/2\leq\alpha<\beta$ より, $m\geq 1$ ならば $-b_m/2<a_m<b_m$ であることに注意する．正の実数 $\varepsilon>0$ に対して, $m>(3\beta^2\varepsilon)^{-1}$ ならば $|a_m/b_m-\xi|<\varepsilon$ である．いま $q_{\alpha,\beta}(X)=9(\alpha^2+\alpha\beta+\beta^2)\beta^2X^2+3(2\alpha+\beta)\beta X+1$ と定義すると $a_m^2+a_mb_m+b_m^2=q_{\alpha,\beta}(m)$ である．Nagell の定理 [7] により $\mu(q_{\alpha,\beta}(m))\neq 0$ となる正の整数 $m$ が無数に存在することが分かる．以上から共通部分 $W(\xi,\varepsilon)\cap\{(a_m,b_m)|m\geq 1\}$ は無限集合である．従って $-1/2\leq\xi<1$ となる有理数 $\xi\in\mathbb{Q}$ に対して $W(\xi,\varepsilon)$ は空集合ではない．集合 $\{\xi\in\mathbb{Q}|-1/2\leq\xi<1\}$ は集合 $\{\xi\in\mathbb{R}|-1/2\leq\xi\leq 1\}$ で稠密であることに注意する．よって $-1/2\leq\xi\leq 1$ となる実数 $\xi\in\mathbb{R}$ に対して $W(\xi,\varepsilon)$ は空集合ではない．　□


2
$R_L$
1
0
$3^4$
$3^5$
$3^6$
$f_L$
$3^7 = 2187$


2
$R_L$
1
0
$3^6$
$3^7$
$3^8$
$f_L$
$3^9 = 19683$


2
$R_L$
1
0
$3^8$
$3^9$
$3^{10}$
$f_L$
$3^{11} = 177147$

**命題 D.** 整数 $a$, $b$ を条件 $b \geq 1$, $a \geq -b/2$, $a^2+ab+b^2 \not\equiv 0 \pmod 3$, $\mu(a^2+ab+b^2) \neq 0$ を全て満たすものとする. このとき $s = a/b$ に対して $H_{L_s} = H(s)$ が成り立つ.

**証明.** 論文 [5] Proposition 2.7 参照. □

**命題 B の証明.** $1 \leq r \leq 2$ である実数 $r \in \mathbb{R}$ に対して $\xi = (-1+\sqrt{-3+12/r^2})/2 \in \mathbb{R}$ とおく. このとき $-1/2 \leq \xi \leq 1$ である. 正の実数 $\varepsilon > 0$ を 1 つ固定すると補題 C から集合 $W(\xi, \varepsilon)$ は空でないのでその集合の元を 1 つとり $(a, b)$ とおく. $\varepsilon' = a/b - \xi \in \mathbb{R}$ とおくと定義より

$$r = \sqrt{\frac{3}{\xi^2+\xi+1}} = \sqrt{\frac{3}{(a/b+\varepsilon')^2+(a/b+\varepsilon')+1}}$$

であり $|\varepsilon'| < \varepsilon$ である. いま $s = a/b$ とおくと $\mu(a^2+ab+b^2) \neq 0$ より $L_s$ の導手 $f_{L_s}$ は $a^2+ab+b^2$ であり, $f_{L_s}$ の 3 と素な部分 $g_{L_s}$ も $a^2+ab+b^2$ に等しくなる. 一方, 補題 D から $H_{L_s} = \max\{|a|, |b|\} = b$ である. よって $R_{L_s} = b/\sqrt{(a^2+ab+b^2)/3} = \sqrt{3/((a/b)^2+(a/b)+1)}$ となる. 以上の議論は任意の正の実数 $\varepsilon > 0$ に対してできるので $|r - R_{L_s}|$ がいくらでも小さくなる有理数 $s \in \mathbb{Q}$ が存在することが分かる. 従って $|r - R_L|$ がいくらでも小さい 3 次巡回体 $L \in \mathcal{L}$ が存在する. よって集合 $\{R_L | L \in \mathcal{L}\}$ は閉集合 $[1, 2]$ で稠密である. □

## 4 謝辞

この度, 第 2 回福岡数論研究集会での講演の機会を与えていただいた九州大学の金子昌信氏, 権 寧魯氏, 福岡教育大学の岸 康弘氏にこの場をおかりして厚くお礼を申し上げます.

## 参考文献

[1] R.J. Chapman, *Automorphism polynomials in cyclic cubic extensions*, J. Number Theory **61** (1996), no. 2, 283–291.

[2] H. Cohen, A course in computational algebraic number theory, Grad. Texts in Math. **138**, 1993.

[3] M. Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), no. 2, 427–447.

[4] T. Komatsu, *Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory*, Manuscripta Math. **114** (2004), no. 3, 265–279.

[5] T. Komatsu, *Cyclic cubic field with explicit Artin symbols*, Tokyo J. Math. **30** (2007), no. 1, 169–178.

[6] P. Morton, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory **49** (1994), no. 2, 183–208.

[7] T. Nagell, *Zur Arithmetik der Polynome*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 178–193.

[8] H. Ogawa, *Quadratic reduction of multiplicative group and its applications*, (Japanese) Algebraic number theory and related topics (Kyoto, 2002). Surikaisekikenkyusho Kokyuroku **1324** (2003), 217–224.

[9] Y. Rikuna, *On simple families of cyclic polynomials*, Proc. Amer. Math. Soc. **130** (2002), no. 8, 2215–2218.

[10] J.P. Serre, Topics in Galois theory, Res. Notes in Math. **1**.

[11] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

[12] N. Suwa, *Twisted Kummer and Kummer-Artin-Schreier theories*, (Japanese) Algebraic number theory and related topics (Kyoto, 2004). Surikaisekikenkyusho Kokyuroku **1451** (2005), 243–256.

[13] L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), 371–384.