RIMS Kôkyûroku Bessatsu
B32 (2012), 105–124

素数巾導手実アーベル体の岩澤不変量 (Iwasawa invariants of real abelian number fields with prime power conductors)

By

小松啓一 (Keiichi Komatsu) * , 福田隆 (Takashi Fukuda) ** ,
森澤貴之 (Takayuki Morisawa) ***

Abstract

For each prime number ℓ less than 10^4, we construct explicitly an infinite family of number fields for which both Iwasawa μ_ℓ and λ_ℓ invariants vanish.

§1. 結果

有限次代数体 k および素数 ℓ に対し、$\mu_\ell(k)$, $\lambda_\ell(k)$, $\nu_\ell(k)$ で k の円分 $\mathbb{Z}_\ell$-拡大 k_∞/k の岩澤 μ, λ, ν 不変量を表す。これらは k_∞/k の n-th layer k_n の類数の ℓ-part を ℓ^{e_n} で表す時、

$$e_n = \mu_\ell(k)\ell^n + \lambda_\ell(k)n + \nu_\ell(k) \quad (n >> 0)$$

という意味を持つ。k が総実代数体なら、全ての素数 ℓ に対し、

$$\mu_\ell(k) = \lambda_\ell(k) = 0$$

だろうと主張するのが、いわゆる Greenberg 予想であり (c.f. [6])、多くの状況証拠があるものの、未だに未解決である。これに関して、自然に次の問題が考えられる。

Received February 23, 2011. Revised September 13, 2011.
2000 Mathematics Subject Classification(s): 2000 Mathematics Subject Classification(s):11R30, 11R22, 11Y40
Key Words: *Iwasawa invariants, Greenberg conjecture*:

*Department of Mathematical Science, School of Fundamental Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan.
e-mail: `kkomatsu@waseda.jp`
**Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan.
e-mail: `fukuda.takashi@nihon-u.ac.jp`
***Department of Mathematical Science, School of Fundamental Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan.
e-mail: `da-vinci-0415@@moegi.waseda.jp`

Problem 1.1. 素数 ℓ を与えた時、$\mu_\ell(k) = \lambda_\ell(k) = 0$ となる総実代数体 k の無限族を構成せよ。

Problem 1.2. 総実代数体 k を与えた時、$\mu_\ell(k) = \lambda_\ell(k) = 0$ となる素数 ℓ の無限族を構成せよ。

まず自明な例を見てみよう。$\ell = 2$ とする。類数が 2 で割れず、2 が $k/\mathbb{Q}$ で分解しない実二次体 k が無限個存在することは、種の理論より直ちにわかる。岩澤の定理 (cf. [9]) より、これらの k に対しては $\mu_2(k) = \lambda_2(k) = \nu_2(k) = 0$ となる。逆に k を任意の総実代数体とする。$k/\mathbb{Q}$ で分解せず k の類数を割らない素数 ℓ が無限個存在することは明らかであり、これらの ℓ に対してはやはり $\mu_\ell(k) = \lambda_\ell(k) = \nu_\ell(k) = 0$ となる。

非自明な例もある。尾崎・田谷 [13] は、2 が分解し $\mu_2(k) = \lambda_2(k) = 0$ となる実二次体 k の無限族を具体的に構成しているし、類数が偶数で $\mu_2(k) = \lambda_2(k) = 0$ となる実二次体 k の無限族も構成している。Byeon [1] は、堀江・中川 [11], Ono [12] の後をうけ、任意の奇素数 ℓ に対し、ℓ が分解せず類数が ℓ で割れない実二次体 k が正の密度で存在することを示した。これらの k に対しては、もちろん $\mu_\ell(k) = \lambda_\ell(k) = \nu_\ell(k) = 0$ である。

尾崎・田谷、堀江・中川、Ono, Byeon の仕事は問題 1.1 に関連して実二次体 k を扱っている。我々はやはり問題 1.1 に興味をもち、別のタイプの体を考えた。素数 p と整数 $m \geq 0$ に対し、$\mathbb{B}_{p,m}$ で $\mathbb{Q}$ の円分 $\mathbb{Z}_p$-拡大の m-th layer を表す。今回我々が扱ったのは $p = 2, 3$ であり、この場合 $\mathbb{B}_{p,m}$ は次のように具体的に表せる。

$$\mathbb{B}_{2,m} = \mathbb{Q}(2\cos\frac{2\pi}{2^{m+2}}), \quad \mathbb{B}_{3,m} = \mathbb{Q}(2\cos\frac{2\pi}{3^{m+1}}).$$

Ferrero-Washington [2] により、任意の素数 ℓ および任意の素数 p に対して $\mu_\ell(\mathbb{B}_{p,m}) = 0$ であることに注意しておく。$p = 2$ の時は $\ell \equiv 1, 3 \pmod 4$ に応じて $2^c \mid\mid \ell - 1$, $2^c \mid\mid \ell^2 - 1$ で c を定め、$p = 3$ の時は $2^c \mid\mid \ell^2 - 1$ とする。

$$m_p = \begin{cases} 2c + \left[\dfrac{1}{2}\log_2(\ell - 1)\right] - 2 & \text{if } p = 2 \\ 2c + \left[\dfrac{1}{2}\log_3(\ell - 1) + \dfrac{1}{2}\right] - 1 & \text{if } p = 3 \end{cases} \tag{1.1}$$

で m_p を定めると、我々の得た主結果は次のようになる。

Theorem 1.3. $p = 2, 3$ とし、ℓ を p と異なる奇素数とする。もし $\lambda_\ell(\mathbb{B}_{p,m_p}) = 0$ なら、全ての $m \geq 0$ に対し $\lambda_\ell(\mathbb{B}_{p,m}) = 0$ である。

計算機で $\lambda_\ell(\mathbb{B}_{p,m_p}) = 0$ を確かめると、次の系が得られる。

Corollary 1.4. ℓ が 10^4 以下の素数なら、全ての $m \geq 0$ に対し $\lambda_\ell(\mathbb{B}_{2,m}) = \lambda_\ell(\mathbb{B}_{3,m}) = 0$.

Remark. 岩澤の定理より、全ての $m \geq 0$ に対し $\lambda_2(\mathbb{B}_{2,m}) = \lambda_3(\mathbb{B}_{3,m}) = 0$ であることはすぐにわかる。

Remark. $p = 2$ で $\ell \equiv 3, 5 \pmod 8$ の時は、ℓ は $\mathbb{B}_{2,m}$ で分解せず、堀江 [7] より $\mathbb{B}_{2,m}$ $(m \geq 0)$ の類数は ℓ で割れない。従って岩澤の定理より $\lambda_\ell(\mathbb{B}_{2,m}) = 0$ がわかる。$p = 3$ で $\ell \equiv 2, 4, 5, 7 \pmod 9$ の時は、ℓ は $\mathbb{B}_{3,m}$ で分解せず、堀江 [7] より $\mathbb{B}_{3,m}$ $(m \geq 0)$ の類数は ℓ で割れない。同じく岩澤の定理より $\lambda_\ell(\mathbb{B}_{3,m}) = 0$ である。

§ 2. 判定法

注意 1, 1 をみたさない ℓ に対して $\lambda_\ell(\mathbb{B}_{p,m}) = 0$ を確かめる方法を説明する。$\Delta_m = G(\mathbb{B}_{p,m}/\mathbb{Q})$ とおく。指標 $\psi : \Delta_m \longrightarrow \overline{\mathbb{Q}}_\ell$ に対し、idempotent $e_\psi \in \mathbb{Z}_\ell[\Delta_m]$ が

$$e_\psi = \frac{1}{|\Delta_m|} \sum_{\sigma \in \Delta_m} \mathrm{Tr}(\psi(\sigma))\sigma^{-1}$$

として定義され、$\lambda_\ell(\mathbb{B}_{p,m})$ は

$$\lambda_\ell(\mathbb{B}_{p,m}) = \sum_\psi \lambda_{\ell,\psi}(\mathbb{B}_{p,m})$$

と分解される。Tr は $\mathbb{Q}_\ell(\psi(\Delta_m))$ から $\mathbb{Q}_\ell$ への trace であり、ψ は Δ_m の $\mathbb{Q}_\ell$ 共役類の代表を動く。次の補題により $\lambda_\ell(\mathbb{B}_{p,m_p})$ は $\lambda_{\ell,\psi}(\mathbb{B}_{p,m})$ に帰着される。

Lemma 2.1. $1 \leq m \leq m_p$ の範囲の全ての m および Δ_m の位数 p^m の全ての指標の $\mathbb{Q}_\ell$ 共役類の代表 ψ に対し $\lambda_{\ell,\psi}(\mathbb{B}_{p,m}) = 0$ であれば、$\lambda_\ell(\mathbb{B}_{p,m_p}) = 0$ である。

大部分の (ℓ, ψ) に対しては Bernoulli 数を用いて $\lambda_{\ell,\psi}(\mathbb{B}_{p,m}) = 0$ を示すことができる。

Lemma 2.2. $|B_{1,\omega^{-1}\psi}|_\ell = 1$ であれば $\lambda_{\ell,\psi}(\mathbb{B}_{p,m}) = 0$ である。

$B_{1,\omega^{-1}\psi}$ の計算は容易であり、$\ell < 10^4$ の範囲で $|B_{1,\omega^{-1}\psi}|_\ell \neq 1$ となる (ℓ, ψ) は、$p = 2$ の時 7 個、$p = 3$ の時 4 個だけである。これらの (ℓ, ψ) に対しては市村・隅田の判定法を適用する。まず (ℓ, ψ) を具体的に示す。

ψ の位数を p^m とすると、$|B_{1,\omega^{-1}\psi}|_\ell \neq 1$ となる ℓ と ψ に対しては (計算の結果) $p^m \mid \ell - 1$ となっている。$\zeta_k = \exp(2\pi\sqrt{-1}/k)$ とする。$p = 2$ の時は $\zeta_{2^{n+2}} \mapsto \zeta_{2^{n+2}}^5$ から、$p = 3$ の時は $\zeta_{3^{n+1}} \mapsto \zeta_{3^{n+1}}^4$ から誘導される Δ_m の元を σ で表すと $\Delta_m = \langle \sigma \rangle$ である。g_ℓ を ℓ^2 の最小原始根とし、$\mathbb{Q}_\ell$ における 1 の原始 p^m 乗根 η_m を

$$\eta_m \equiv g_\ell^{\frac{\ell-1}{p^m}} \pmod \ell$$

をみたすものとして定める。Δ_m の指標 ψ_m を $\psi_m(\sigma)=\eta_m$ で定義すると $\widehat{\Delta}_m=\langle\psi_m\rangle$ となる。$|B_{1,\omega^{-1}\psi}|_\ell\neq 1$ となる ℓ と $\psi=\psi_m^k$ は以下の通り。$P_\psi(T)$ は ψ に付随する岩澤多項式、ℓ^* は [8, Corollary 2] における ℓ である。これらの (ℓ,ψ) は全て $p^m\mid\ell-1$ すなわち [8] の条件 (C1) をみたし、$(H_{P_i,n})=(H_{i,n})$ が $n=2$ で成立している。従って $\lambda_{\ell,\psi}(\mathbb{B}_{p,m})=0$ である。

Table 1. $p=2$

ℓ	ψ	case	$P_\psi(T)$ mod ℓ^2	ℓ^*
31	ψ_1	(C)	$T+186$	1429969
193	ψ_6^{25}	(A)	$T+33389$	5521195777
257	ψ_7^{97}	(A)	$T+12593$	52145949697
521	ψ_3	(A)	$T+204753$	18101857409
641	ψ_7^{17}	(A)	$T+223068$	1213630714369
3617	ψ_5^{23}	(A)	$T+11965036$	60569710224641
4513	ψ_5^{17}	(A)	$T+15930890$	235307606264321

Table 2. $p=3$

ℓ	ψ	case	$P_\psi(T)$ mod ℓ^2	ℓ^*
73	ψ_1	(C)	$T+2263$	56018449
109	ψ_3^{14}	(A)	$T+2289$	1888152283
487	ψ_4^{61}	(C)	$T+39934$	280668166291
1621	ψ_4^{55}	(A)	$T+2207802$	16560570765169

次に具体的な計算のテクニックを解説する。無造作にプログラムを書くと計算時間、メモリの両面で破綻するので、工夫が必要である。

§3. Bernoulli 数の定義

ℓ, p を異なる素数とし、

$$q=\begin{cases}4 & \text{if } p=2\\ p & \text{if } p>2\end{cases}$$

とおく。これから考える指標は $\overline{\mathbb{Q}}_\ell$ に値をとるものとする。ω を mod ℓ の Teichmüller 指標、ψ を $\bmod qp^m$ で定義され位数が p^m の偶指標とする。$\ell\neq p$ だから、全ての $a\in\mathbb{Z}$

に対して $\omega^{-1}\psi(a) = \omega^{-1}(a)\psi(a)$ であることに注意する。この時、一般 Bernoulli 数 $B_{1,\omega^{-1}\psi}$ が

$$B_{1,\omega^{-1}\psi} = \frac{1}{\ell qp^m}\sum_{a=1}^{\ell qp^m} a\omega^{-1}(a)\psi(a) \in \overline{\mathbb{Q}}_\ell$$

で定義される。これの ℓ-進付値を考えやすくするため変形する。$\ell \neq p$ だから、任意の j に対し

$$\{\, i\ell + j \bmod qp^m \mid 0 \le i < qp^m \,\} = \{\, i \mid 0 \le i < qp^m \,\}$$

であることに注意すると、

$$\begin{aligned} qp^m B_{1,\omega^{-1}\psi} &= \frac{1}{\ell}\sum_{0\le i<qp^m}\ \sum_{0\le j<\ell}(i\ell+j)\omega^{-1}(i\ell+j)\psi(i\ell+j) \\ &= \sum_{0\le j<\ell}\omega^{-1}(j)\sum_{0\le i<qp^m} i\psi(i\ell+j) \\ &\qquad + \frac{1}{\ell}\sum_{0\le j<\ell} j\omega^{-1}(j)\sum_{0\le i<qp^m}\psi(i\ell+j) \\ &= \sum_{0\le j<\ell}\omega^{-1}(j)\sum_{0\le i<qp^m} i\psi(i\ell+j) \qquad (3.1) \end{aligned}$$

となり、$B_{1,\omega^{-1}\psi}$ が ℓ-進整数であることがわかる。$|B_{1,\omega^{-1}\psi}|_\ell = 1$ かどうかを調べる必要があり、そのためには (3.1) を $\bmod \ell$ で計算すればよい。従って、

$$\omega^{-1}(j) \equiv \begin{cases} 0 & \text{if } j = 0 \\ \frac{1}{j} \pmod{\ell} & \text{if } 1 < j < \ell \end{cases}$$

とすればよい。

以後 p は 2 または 3 とする。$p = 2$ の時は

$$\begin{cases} 2^s \,||\, \ell - 1 & \text{if } \ell \equiv 1 \pmod 4 \\ 2^s \,||\, \ell + 1 & \text{if } \ell \equiv 3 \pmod 4 \end{cases}$$

$$c = \begin{cases} s & \text{if } \ell \equiv 1 \pmod 4 \\ s + 1 & \text{if } \ell \equiv 3 \pmod 4 \end{cases}$$

$p = 3$ の時は

$$2^s \,||\, \ell^2 - 1, \quad c = s$$

とし、(1.1) で m_p を定める。この時、次のことが分っている。

Theorem 3.1. $m \geq m_p + 1$ の時、$\bmod qp^m$ で定義された位数 p^m の任意の偶指標 ψ に対し、

$$|B_{1,\omega^{-1}\psi}|_\ell = 1\ .$$

しかし今のところ、$1 \leq m \leq m_p$ に対して $|B_{1,\omega^{-1}\psi}|_\ell = 1$ かどうかは、具体的に計算して調べる以外に方法がない。$1 \leq m \leq 2c-2$ と $2c-1 \leq m \leq m_p$ で使う手法が異なるので、場合にわけて説明する。

§ 4. $p = 2,\ 1 \leq m \leq 2c-2$ の場合

$B_{1,\omega^{-1}\psi}$ を定義に基づいて計算するしかない。$\bmod 2^{m+2}$ で定義され、位数が 2^m の偶指標 ψ は 2^{m-1} 個あるが、すべてに亘って動かす必要はなく、$\mathbb{Q}_\ell$-共役類の代表を動かせばよい。η_m を $\overline{\mathbb{Q}}_\ell$ における 1 の原始 2^m 乗根とし、c_m で Δ_m の位数 2^m の偶指標の $\mathbb{Q}_\ell$-共役類の個数、d_m で拡大次数 $[\mathbb{Q}_\ell(\eta_m) : \mathbb{Q}_\ell]$ を表すと、

$$c_m d_m = 2^{m-1}$$

であり、

$$d_m = \begin{cases} 1 & \text{if } \ell \equiv 1 \pmod 4,\ 1 \leq m \leq s \\ 2^{m-s} & \text{if } \ell \equiv 1 \pmod 4,\ s+1 \leq m \\ 1 & \text{if } \ell \equiv 3 \pmod 4,\ m = 1 \\ 2 & \text{if } \ell \equiv 3 \pmod 4,\ 2 \leq m \leq s \\ 2^{m-s} & \text{if } \ell \equiv 3 \pmod 4,\ s+1 \leq m \end{cases}$$

であるから、

$$c_m = \begin{cases} 2^{m-1} & \text{if } \ell \equiv 1 \pmod 4,\ 1 \leq m \leq s \\ 2^{s-1} & \text{if } \ell \equiv 1 \pmod 4,\ s+1 \leq m \\ 1 & \text{if } \ell \equiv 3 \pmod 4,\ m = 1 \\ 2^{m-2} & \text{if } \ell \equiv 3 \pmod 4,\ 2 \leq m \leq s \\ 2^{s-1} & \text{if } \ell \equiv 3 \pmod 4,\ s+1 \leq m \end{cases}$$

となる。$\zeta_{2^{n+2}} \mapsto \zeta_{2^{n+2}}^5$ から誘導される $\Delta_m = G(\mathbb{B}_{2,m}/\mathbb{Q})$ の生成元を σ とし、$\widehat{\Delta}_m$ の生成元 ψ_m を $\psi_m(\sigma) = \eta_m$ で定める。$\widehat{\Delta}_m = \{\, \psi_m^k \mid 0 \leq k < 2^m \,\}$ だから、Δ_m の位数 2^m

の指標は $\psi = \psi_m^k$ の形をしている。

$$X_m = \begin{cases} \{\, 1 \le k < 2^m \mid k : \text{odd} \,\} & \text{if } \ell \equiv 1 \pmod 4,\ 1 \le m \le s \\ \{\, 1 \le k < 2^s \mid k : \text{odd} \,\} & \text{if } \ell \equiv 1 \pmod 4,\ s+1 \le m \\ \{\, 1 \,\} & \text{if } \ell \equiv 3 \pmod 4,\ m = 1 \\ \{\, 1 \le k < 2^{m-1} \mid k : \text{odd} \,\} & \text{if } \ell \equiv 3 \pmod 4,\ 2 \le m \le s \\ \{\, 1 \le k < 2^{s-1},\, 2^s < k < 2^s + 2^{s-1} \mid k : \text{odd} \,\} & \text{if } \ell \equiv 3 \pmod 4,\ s+1 \le m \end{cases}$$

とおけば、$|X_m| = c_m$ であり、$\{\, \psi_m^k \mid k \in X_m \,\}$ が Δ_m の位数 2^m の偶指標の $\mathbb{Q}_\ell$-共役類の代表になる。$B_{1,\omega^{-1}\psi_m^k}$ を (3.1) に基づいて計算すると計算量は $O(2^{m+2}\ell)$ であり、

$$B_{1,\omega^{-1}\psi_m^k} \quad (k \in X_m) \tag{4.1}$$

の計算量は $m \ge s+1$ なら $O(2^{s-1}2^{m+2}\ell)$ である。s がある程度大きくなると (eg. $\ell = 8191$ なら $s = 13$)、これは厳しい。そこで $B_{1,\omega^{-1}\psi_m}$ を (3.1) で求め、

$$B_{1,\omega^{-1}\psi_m} = \sum_{i=0}^{2^m-1} a_i \eta_m^i$$

としてから、

$$B_{1,\omega^{-1}\psi_m^k} = \sum_{i=0}^{2^m-1} a_i \eta_m^{ki} = \sum_{i=0}^{2^m-1} b_i \eta_m^i \tag{4.2}$$

とすれば (4.1) の計算量は $O(2^{m+2}\ell + 2^{s-1}2^m)$ となる。

$\psi = \psi_m$ に対する (3.1) の計算は、

$$\psi_m(\pm\, 5^i \bmod 2^{m+2}) = \eta_m^i$$

に注意して、$\{\, \psi_m(j) \mid 0 \le j < 2^{m+2} \,\}$ の表を作っておくとよい (j が偶数なら $\psi_m(j) = 0$)。さて (4.2) の形で $B_{1,\omega^{-1}\psi_m^k}$ が求まったら、多項式

$$B(X) = \sum_{i=0}^{2^m-1} b_i X^i$$

を η_m の最小多項式

$$F(X) = \begin{cases} X - \eta_m & \text{if } \ell \equiv 1 \pmod 4,\ 1 \le m \le s \\ X^{2^{m-s}} - \eta_s & \text{if } \ell \equiv 1 \pmod 4,\ s+1 \le m \\ X + 1 & \text{if } \ell \equiv 3 \pmod 4,\ m = 1 \\ X^2 - a_m X + 1 & \text{if } \ell \equiv 3 \pmod 4,\ 2 \le m \le s \\ X^{2^{m-s}} - a_{s+1} X^{2^{m-s-1}} - 1 & \text{if } \ell \equiv 3 \pmod 4,\ s+1 \le m \end{cases}$$

で割って

$$B(X) = F(X)G(X) + R(X), \quad \deg R < \deg B$$

とすれば $B_{1,\omega^{-1}\psi_m^k} = R(\eta_m)$ であり、

$$B_{1,\omega^{-1}\psi_m^k} = \sum_{i=0}^{d_m-1} c_i \eta_m^i \quad (k \in X_k) \tag{4.3}$$

と変形できる。この計算は mod ℓ で行えばよい。1 回の割算は $O(2^m)$ でできるから、(4.3) の計算量は $O(2^{m+2}\ell + 2^{s-1}2^m + 2^{s-1}2^m) = O(2^m(4\ell + 2^s))$ となる。$\eta_m \ (1 \le m \le s)$ は g_ℓ を ℓ^2 の最小原始根とするとき、

$$\eta_m \equiv g_\ell^{\frac{\ell-1}{2^m}} \pmod{\ell}$$

をみたすものとして決めておく[1]。$a_m = \mathrm{Tr}_{\mathbb{Q}_\ell(\eta_m)/\mathbb{Q}_\ell}(\eta_m) \ (2 \le m \le s+1)$ の求め方は [3] に載っている。再録すれば次のようになる。

Lemma 4.1. $a_2 = 0$ であり、$a_m \ (3 \le m \le s+1)$ は次の漸化式で求めればよい。

$$\begin{aligned} a_m &= \sqrt{2 + a_{m-1}} \quad (3 \le m \le s) \\ a_{s+1} &= \sqrt{-2 + a_s} \end{aligned}$$

平方根は $\mathbb{Q}_\ell$ における平方根であるが mod ℓ で計算すればよいので $\mathbb{F}_\ell$ における平方根と思えばよい。これも易しい。

Lemma 4.2. $\ell \equiv 3 \pmod 4$ とする。$a \in \mathbb{F}_\ell^\times$ に対し、

$$\sqrt{a} \in \mathbb{F}_\ell \Longleftrightarrow \left(\frac{a}{\ell}\right) = 1 \Longrightarrow \sqrt{a} = \pm\, a^{\frac{\ell+1}{4}}$$

η_m は $\mathbb{Q}_\ell(\eta_m)$ の整数環の $\mathbb{Z}_\ell$ 上の巾整数基を作るから、$B_{1,\omega^{-1}\psi^k}$ を (4.3) の形で表せば、ℓ で割れるかどうかの判定は次のようにできる。

Lemma 4.3.

$$B_{1,\omega^{-1}\psi_m^k} = \sum_{i=0}^{d_m-1} c_i \eta_m^i \quad (c_i \in \mathbb{Z}_\ell)$$

の時、

$$B_{1,\omega^{-1}\psi_m^k} \equiv 0 \pmod{\ell} \Longleftrightarrow c_i \equiv 0 \pmod{\ell} \quad \textit{for all } 0 \le i \le d_m - 1\,.$$

[1] ℓ の原始根でもよいが、後で ℓ^2 の原始根を使う箇所があるので、ここでも ℓ^2 の原始根を使っておいた方がまぎらわしくない

最も時間がかかるのは $\ell = 8191$ の時である。$c = 14$ だから $1 \le m \le 26$ に対して (3.1) を計算しなければならない。$m = 26$ の時のループ回数は $2^{28} \cdot 8191 = 2198754820096 \simeq 2.1 \cdot 10^{12}$ だから TC では厳しく、C で書かなければならない[2]。それでも数日かかる。

§ 5. $p = 2$, $2c - 1 \le m \le m_2$ の場合

$B_{1,\omega^{-1}\psi}$ を直接計算するよりも効率的な Sinnott-Washington の方法がある (c.f. [14, p.387])。

$$h(T) = \sum_{i=0}^{\ell-1} \omega^{-1}(1 + 2^c i)T^i \in \mathbb{Z}_\ell[T]$$

とおく。$h(T)$ は ψ とは無関係に定義される、つまり m に依らない。

Lemma 5.1. $m \ge 2c-1$ とする。$\overline{\mathbb{Q}}_\ell$ に含まれる任意の 1 の 2^{m+2-c} 乗根 η_{m+2-c} に対し $h(\eta_{m+2-c}) \not\equiv 0 \pmod{\ell}$ ならば、$\bmod 2^{m+2}$ で定義される位数が 2^m の任意の偶指標 ψ に対し $B_{1,\omega^{-1}\psi} \not\equiv 0 \pmod{\ell}$ である。

$h(\eta_{m+2-c})$ の計算量は $O(\ell)$ であり、$m + 2 - c \ge s + 1$ となるから、

$$[\mathbb{Q}_\ell(\eta_{m+2-c}) : \mathbb{Q}_\ell] = 2^{m+2-c-s}$$

つまり $h(\eta_{m+2-c})$ を巾整数基で表す計算量は $O(2^{m+2-c-s})$ である。従って $k \in X_{m+2-c}$ に対し $h(\eta^k_{m+2-c})$ を求める計算量は最大で $O(2^{s-1})O(2^{m+2-c-s}) = O(2^{m+1-c})$ である。$\ell = 8191$, $c = 14$, $m = m_2 = 32$ の時は $2^{m+1-c} = 2^{19} = 524288$ であり、意外なことに $1 \le m \le 2c - 2$ よりもずっと速く計算できる[3]。

§ 6. $p = 3$, $1 \le m \le 2c - 2$ の場合

$B_{1,\omega^{-1}\psi}$ を定義に基づいて計算する。$\bmod 3^{m+1}$ で定義され、位数が 3^m の偶指標 ψ は $2 \cdot 3^{m-1}$ 個あるが、すべてに亘って動かす必要はなく、$\mathbb{Q}_\ell$-共役類の代表を動かせばよい。η_m を $\overline{\mathbb{Q}}_\ell$ における 1 の原始 3^m 乗根とし、c_m で Δ_m の位数 3^m の偶指標の $\mathbb{Q}_\ell$-共役類の個数、d_m で拡大次数 $[\mathbb{Q}_\ell(\eta_m) : \mathbb{Q}_\ell]$ を表すと、

$$c_m d_m = 2 \cdot 3^{m-1}$$

[2] TC で書いたものを C に変換すれば効率よく作成できる。更に TC から C プログラムを呼べば、いろいろな面で楽である。

[3] C で書く必要はない。TC で十分である。

であり、

$$d_m = \begin{cases} 1 & \text{if } \ell \equiv 1 \pmod 3,\ 1 \le m \le s \\ 3^{m-s} & \text{if } \ell \equiv 1 \pmod 3,\ s+1 \le m \\ 2 & \text{if } \ell \equiv 2 \pmod 3,\ 1 \le m \le s \\ 2 \cdot 3^{m-s} & \text{if } \ell \equiv 2 \pmod 3,\ s+1 \le m \end{cases}$$

であるから、

$$c_m = \begin{cases} 2 \cdot 3^{m-1} & \text{if } \ell \equiv 1 \pmod 3,\ 1 \le m \le s \\ 2 \cdot 3^{s-1} & \text{if } \ell \equiv 1 \pmod 3,\ s+1 \le m \\ 3^{m-1} & \text{if } \ell \equiv 2 \pmod 3,\ 1 \le m \le s \\ 3^{s-1} & \text{if } \ell \equiv 2 \pmod 3,\ s+1 \le m \end{cases}$$

となる。$\zeta_{3^{m+1}} \mapsto \zeta_{3^{m+1}}^4$ から誘導される $\Delta_m = G(\mathbb{B}_{3,m}/\mathbb{Q})$ の生成元を σ とし、$\widehat{\Delta}_m$ の生成元 ψ_m を $\psi_m(\sigma) = \eta_m$ で定める。$\widehat{\Delta}_m = \{\, \psi_m^k \mid 0 \le k < 3^m \,\}$ だから、Δ_m の位数 3^m の指標は $\psi = \psi_m^k$ の形をしている。

$$X_m = \begin{cases} \{\, 1 \le k < 3^m \mid 3 \not| \ k \,\} & \text{if } \ell \equiv 1 \pmod 3,\ 1 \le m \le s \\ \{\, 1 \le k < 3^s \mid 3 \not| \ k \,\} & \text{if } \ell \equiv 1 \pmod 3,\ s+1 \le m \\ \{\, 1 \le k < \dfrac{3^m - 1}{2} \mid 3 \not| \ k \,\} & \text{if } \ell \equiv 2 \pmod 3,\ 1 \le m \le s \\ \{\, 1 \le k < \dfrac{3^s - 1}{2} \mid 3 \not| \ k \,\} & \text{if } \ell \equiv 2 \pmod 3,\ s+1 \le m \end{cases}$$

とおけば、$|X_m| = c_m$ であり、$\{\, \psi_m^k \mid k \in X_m \,\}$ が Δ_m の位数 3^m の偶指標の $\mathbb{Q}_\ell$-共役類の代表になる。後は $p = 2$ の場合と同様。ψ_m の値は

$$\psi_m(\pm\, 4^i \bmod 3^{m+1}) = \eta_m^i$$

で定まる。 (j が 3 で割れれば $\psi_m(j) = 0$)。η_m の最小多項式は

$$\begin{cases} X - \eta_m & \text{if } \ell \equiv 1 \pmod 3,\ 1 \le m \le s \\ X^{3^{m-s}} - \eta_s & \text{if } \ell \equiv 1 \pmod 4,\ s+1 \le m \\ X^2 - a_m X + 1 & \text{if } \ell \equiv 2 \pmod 3,\ 1 \le m \le s \\ X^{2 \cdot 3^{m-s}} - a_s X^{3^{m-s}} + 1 & \text{if } \ell \equiv 2 \pmod 3,\ s+1 \le m \end{cases}$$

となる。これで、

$$B_{1,\omega^{-1}\psi_m^k} = \sum_{i=0}^{d_m - 1} c_i \eta_m^i \quad (k \in X_k)$$

が求まる。η_m $(1 \le m \le s)$ は g_ℓ を ℓ^2 の最小原始根とするとき、

$$\eta_m \equiv g_\ell^{\frac{\ell-1}{3^m}} \pmod{\ell}$$

をみたすものとする。$a_m = \mathrm{Tr}_{\mathbb{Q}_\ell(\eta_m)/\mathbb{Q}_\ell}(\eta_m)$ $(1 \le m \le s+1)$ の求め方は [10] に載っている。再録すれば次のようになる。

Lemma 6.1. $a_1 = -1$ であり、

$$X^3 - 3X - a_{m-1} = 0 \quad (2 \le m \le s)$$

の *(*任意の*)* 根を a_m とすればよい。

$p = 3$ の時も η_m は $\mathbb{Q}_\ell(\eta_m)$ の整数環の $\mathbb{Z}_\ell$ 上の巾整数基を作るから、補題 4.3 は同様に成立する。

§7. $p = 3$, $2c-1 \le m \le m_3$ の場合

やはり Sinnott-Washington の方法が使える (c.f. [14, p.387])。

$$h(T) = \sum_{i=0}^{\ell-1} \omega^{-1}(1 + 3^c i) T^i \in \mathbb{Z}_\ell[T]$$

とおく。

Lemma 7.1. $m \ge 2c-1$ とする。$\overline{\mathbb{Q}_\ell}$ に含まれる任意の 1 の 3^{m+1-c} 乗根 η_{m+1-c} に対し $h(\eta_{m+1-c}) \not\equiv 0 \pmod{\ell}$ ならば、mod 3^{m+1} で定義される位数が 3^m の任意の偶指標 ψ に対し $B_{1,\omega^{-1}\psi} \not\equiv 0 \pmod{\ell}$ である。

§8. 岩澤多項式の計算

ψ を $\Delta_m = G(\mathbb{B}_{p,m}/\mathbb{Q})$ の位数 p^m の指標とする。ψ は偶指標である。ℓ-進 L-関数 $L_\ell(s,\psi)$ を与える、すなわち

$$L_\ell(s,\psi) = g_\psi((1 + qp^m\ell)^{1-s} - 1)$$

をみたす巾級数 $g_\psi(T) \in \mathbb{Z}_\ell[[T]]$ が (一意的に) 存在し、岩澤巾級数と呼ばれる。$g_\psi(T)$ から distinguished 多項式 $P_\psi(T) \in \mathbb{Z}_\ell[T]$ が

$$g_\psi(T) = u_\psi(T) P_\psi(T) \tag{8.1}$$

として (一意的に) 定まる。$u_\psi(T)$ は $\mathbb{Z}_\ell[[T]]$ の単元、すなわち $u_\psi(0) \not\equiv 0 \pmod{\ell}$ である巾級数である。$P_\psi(T)$ は岩澤多項式と呼ばれ、非常に重要な性質を持っている。$P_\psi(T)$ は Stickelberger 元

$$\xi_n = -\frac{1}{2qp^m\ell^{n+1}} \sum_{a=1}^{qp^m\ell^{n+1}} a\omega^{-1}(a)\psi(a) \left(\frac{\mathbb{B}_{\ell,n}/\mathbb{Q}}{a}\right)^{-1} \in \mathbb{Z}_\ell[\Gamma_n]$$

を経由して計算することができる。$\Gamma_n = G(\mathbb{B}_{\ell,n}/\mathbb{Q}) = G(\mathbb{B}_{p,m}\mathbb{B}_{\ell,n}/\mathbb{B}_{p,m})$ であり、

$$\left(\frac{\mathbb{B}_{\ell,n}/\mathbb{Q}}{a}\right)$$

は Frobenius 写像である。$(a, p\ell) \neq 1$ なら $\omega^{-1}(a)\psi(a) = 0$ であることに注意する。まず ξ_n の定義式を計算しやすいように変形する。

$$\begin{aligned}
-2qp^m\xi_n &= \frac{1}{\ell^{n+1}} \sum_{0\le i<qp^m} \sum_{0\le j<\ell^{n+1}} (i\ell^{n+1}+j)\omega^{-1}(i\ell^{n+1}+j)\psi(i\ell^{n+1}+j) \left(\frac{\mathbb{B}_{\ell,n}/\mathbb{Q}}{i\ell^{n+1}+j}\right)^{-1} \\
&= \sum_{0\le j<\ell^{n+1}} \sum_{0\le i<qp^m} i\omega^{-1}(j)\psi(i\ell^{n+1}+j) \left(\frac{\mathbb{B}_{\ell,n}/\mathbb{Q}}{j}\right)^{-1} \\
&\qquad + \frac{1}{\ell^{n+1}} \sum_{0\le j<\ell^{n+1}} j\omega^{-1}(j) \left(\frac{\mathbb{B}_{\ell,n}/\mathbb{Q}}{j}\right)^{-1} \sum_{0\le i<qp^m} \psi(i\ell^{n+1}+j) \\
&= \sum_{\substack{0\le j<\ell^{n+1} \\ (j,\ell)=1}} \omega^{-1}(j) \left(\frac{\mathbb{B}_{\ell,n}/\mathbb{Q}}{j}\right)^{-1} \sum_{0\le i<qp^m} i\psi(i\ell^{n+1}+j)
\end{aligned}$$

g_ℓ を ℓ^2 の原始根とすると、任意の $n \geq 0$ に対し、

$$(\mathbb{Z}/\ell^{n+1}\mathbb{Z})^\times = \langle\, g_\ell + \ell^{n+1}\mathbb{Z} \,\rangle$$

だから、

$$-2qp^m\xi_n = \sum_{j=0}^{(\ell-1)\ell^n} \omega^{-1}(g_\ell^j) \left(\frac{\mathbb{B}_{\ell,n}/\mathbb{Q}}{g_\ell}\right)^{-j} \sum_{i=0}^{qp^m-1} i\psi(i\ell^{n+1} + (g_\ell^j \bmod \ell^{n+1}))\,.$$

ここで、

$$\gamma = \left(\frac{\mathbb{B}_{\ell,n}/\mathbb{Q}}{1+qp^m\ell}\right) = \left(\frac{\mathbb{B}_{\ell,n}/\mathbb{Q}}{g_\ell}\right)^{r_n}$$

すなわち

$$g_\ell^{r_n} \equiv 1 + qp^m\ell \pmod{\ell^{n+1}}$$

をみたす r_n を求める。r_0 の計算量は $O(\ell)$ である。

Lemma 8.1.

$$r_{i+1} \equiv r_i \pmod{(\ell-1)\ell^i} \quad (i \geq 0)$$

すなわち、

$$r_{i+1} \in \{\, r_i + k(\ell-1)\ell^i \mid 0 \leq k \leq \ell - 1 \,\}$$

Proof.

$$\begin{aligned} g_\ell^{r_{i+1}} &\equiv 1 + qp^m\ell \pmod{\ell^{i+2}} \\ &\equiv g_\ell^{r_i} \pmod{\ell^{i+1}} \end{aligned}$$

より

$$g_\ell^{r_{i+1}-r_i} \equiv 1 \pmod{\ell^{i+1}}$$

よって

$$r_{i+1} - r_i \equiv 0 \pmod{\varphi(\ell^{n+1})}$$

□

これより r_n は $O(\ell^{n+1})$ でなく $O(\ell(n+1))$ で計算できる。

$$xr_n \equiv 1 \pmod{\ell^n}$$

とすれば、

$$-2qp^m\xi_n = \sum_{j=0}^{(\ell-1)\ell^n} \omega^{-1}(g_\ell^j)(\gamma^{-1})^{xj} \sum_{i=0}^{qp^m-1} i\psi(i\ell^{n+1} + (g_\ell^j \bmod \ell^{n+1}))\,. \tag{8.2}$$

ψ は $\psi = \psi_m^k$ の形であり、ψ_m の値は、

$$\begin{aligned} \psi_m(\pm\, 5^i \bmod 2^{m+2}) &= \eta_m^i \quad \text{if } p = 2 \\ \psi_m(\pm\, 4^i \bmod 3^{m+1}) &= \eta_m^i \quad \text{if } p = 3 \end{aligned}$$

で決まる。(8.2) より岩澤多項式 $P_\psi(T)$ が定まるのであるが、$-2qp^m$ は (8.1) の $u_\psi(T)$ に吸収されるので無視してよい。予備計算によれば $|B_{1,\omega^{-1}\psi}|_\ell \neq 1$ となる全ての場合において $\deg P_\psi = 1$ となっている。従って (8.2) を $\bmod\, \ell^n$ で求めれば $P_\psi(T)$ も $\bmod\, \ell^n$ で求まる。$\eta_m \in \mathbb{Z}_\ell$ は

$$\eta_m \equiv g_\ell^{\frac{\ell-1}{p^m}} \pmod{\ell}$$

をみたす 1 の原始 p^m 乗根であったから、

$$\eta_m \equiv \left(g_\ell^{\frac{\ell-1}{p^m}}\right)^{\ell^{n-1}} \pmod{\ell^n}$$

となっている。ω については、

$$\omega(a) \equiv a^{\ell^{n-1}} \pmod{\ell^n}$$

に注意すればよい。これで (8.2) より、

$$\xi_n \equiv \sum_{i=0}^{\ell^n-1} a_i(\gamma^{-1})^i \pmod{\ell^n} \qquad (a_i \in \mathbb{Z}) \tag{8.3}$$

が求まる。ここまでの計算量が大部分を占め、以後の多項式の変換に関する部分は殆んど無視できる。(8.3) が求まれば、

$$\begin{aligned} g_\psi(T) &\equiv \sum_{i=0}^{\ell^n-1} a_i\left(\frac{1+T}{1+qp^m\ell}\right)^i \pmod{\ell^n} \\ &\equiv \sum_{i=0}^{\ell^n-1} b_i(1+T)^i \pmod{\ell^n} \end{aligned}$$

となる。$g_\psi(T)$ は T の多項式として表現しなければならない。$\min(n+1, \ell^n-1) = n+1$ 次まで求めれば十分である。2 項展開するのでなく、

$$\begin{aligned} &g_\psi(T) \longleftarrow 0 \\ &g_\psi(T) \longleftarrow (1+T)g_\psi(T) + b_i \quad (i = \ell^n-1, \dots, 0) \end{aligned}$$

と $1+T$ を次々とかけるのがよい。もちろん $n+2$ 次以上の項は無視する。これで、

$$g_\psi(T) \equiv \sum_{i=0}^{n+1} c_i T^i \pmod{(T^{n+2}, \ell^n)}$$

が求まり、[5, 補題 5.3] より、

$$P_\psi(T) \equiv T + \alpha \pmod{\ell^n}$$

が求まる。$\alpha \equiv 0 \pmod{\ell}$, $\alpha \not\equiv 0 \pmod{\ell^2}$ となっている。

§9. 市村・隅田の判定

$$W(T) = \begin{cases} (1+T)^{\ell^n} - 1 & \text{if } \psi(\ell) \neq 1 \\ \dfrac{(1+T)^{\ell^n} - 1}{T} & \text{if } \psi(\ell) = 1 \end{cases}$$

とおく。

$$Y(T)P_\psi(T) \equiv \ell^a \pmod{W(T)}$$

とくに

$$W(T) = Y(T)P_\psi(T) + \ell^a \tag{9.1}$$

をみたす $Y(T)$ を求める。$P_\psi(T)$ は $\bmod \ell^n$ で求めているから (9.1) も $\bmod \ell^n$ で考えることになり、$W(-\alpha) \equiv 0 \pmod{\ell^n}$ だから、

$$W(T) \equiv (T+\alpha)Y(T) \pmod{\ell^n}$$

をみたす $Y(T) \bmod \ell^n$ を求めればよい。この $Y(T)$ を $T \leftrightarrow \gamma - 1$ として円単数に作用させるのだから $Y(T)$ を $1+T$ の多項式で表しておくと楽である。つまり $Y(T) = Y_1(1+T)$ となる $Y_1(T)$ を

$$W(T-1) \equiv (T-1+\alpha)Y_1(T) \pmod{\ell^n}$$

として求めればよい。これは漸化式で簡単に求められる。

Lemma 9.1. $b_0 = 1,\ b_{i+1} = (1-\alpha)b_i \quad (i \geq 0)$ で $\{b_i\}_{i=0}^\infty$ を定めると、任意の $k \geq 0$ に対し

$$T^k - 1 = (T-1+\alpha)\Big(\sum_{i=0}^{k-1} b_{k-1-i}\,T^i\Big) + b_k - 1$$

Proof. $k=0$ の時は成立。k で成立するとして $k+1$ の時を考える。

$$\begin{aligned}
T^{k+1} - 1 &= T(T^k - 1) + T - 1 \\
&= (T-1+\alpha)\Big(\sum_{i=0}^{k-1} b_{k-1-i}\,T^{i+1}\Big) + (b_k - 1)T + T - 1 \\
&= (T-1+\alpha)\Big(\sum_{i=1}^{k} b_{k-i}\,T^{i}\Big) + b_k(T-1+\alpha) + (1-\alpha)b_k - 1 \\
&= (T-1+\alpha)\Big(\sum_{i=0}^{k} b_{k-i}\,T^{i}\Big) + b_{k+1} - 1
\end{aligned}$$

□

$k = \ell^n$ まで計算し、念のため $b_{\ell^n} \equiv 1 \pmod{\ell^n}$ を確かめる。

Lemma 9.2. $b_0 = 0,\ \ b_{i+1} = (1-\alpha)b_i + 1 \quad (i \geq 0)$ で $\{b_i\}_{i=0}^{\infty}$ を定めると、任意の $k \geq 0$ に対し

$$\frac{T^k - 1}{T-1} = (T - 1 + \alpha)\Big(\sum_{i=0}^{k-2} b_{k-1-i}\, T^i\Big) + b_k$$

Proof. $k = 0$ の時は成立。k で成立するとして $k+1$ の時を考える。

$$\begin{aligned}
\frac{T^{k+1}-1}{T-1} &= \frac{T(T^k-1)+T-1}{T-1} \\
&= T\,\frac{T^k-1}{T-1} + 1 \\
&= (T-1+\alpha)\Big(\sum_{i=0}^{k-2} b_{k-1-i}\, T^{i+1}\Big) + b_k T + 1 \\
&= (T-1+\alpha)\Big(\sum_{i=1}^{k-1} b_{k-i}\, T^{i}\Big) + b_k(T-1+\alpha) + (1-\alpha)b_k + 1 \\
&= (T-1+\alpha)\Big(\sum_{i=0}^{k-1} b_{k-i}\, T^{i}\Big) + b_{k+1}
\end{aligned}$$

□

$k = \ell^n$ まで計算し、念のため $b_{\ell^n} \equiv 0 \pmod{\ell^n}$ を確かめる。

$\psi = \psi_m^k$ に対し idempotent

$$e_\psi = \frac{1}{|\Delta_m|} \sum_{\sigma \in \Delta_m} \psi(\sigma^{-1})\sigma \in \mathbb{Z}_\ell[\Delta_m]$$

があり、e_ψ と $Y_1(\gamma)$ を円単数

$$c_n = N_{\mathbb{Q}(\zeta_f)/\mathbb{B}_{p,m}\mathbb{B}_{\ell,n}}(1-\zeta_f), \quad f = qp^m\ell^{n+1}$$

に作用させる。作用を考えやすくするため、

$$\zeta_f = \zeta_{\ell^{n+1}}\zeta_{qp^m}$$

とする。g_ℓ を ℓ^2 の原始根とし、

$$\begin{aligned}
x_1 &\equiv g_\ell^{\ell^n} \pmod{\ell^{n+1}}, \quad x_1 \equiv 1 \pmod{qp^m} \\
x_2 &\equiv 1 \pmod{\ell^{n+1}}, \quad x_2 \equiv -1 \pmod{qp^m}
\end{aligned}$$

をみたす $x_1, x_2 \in \mathbb{Z}$ を一組求め、

$$H = \{\, x_1^i x_2^j \bmod f \mid 0 \leq i < \ell,\ 0 \leq j \leq 1 \,\}$$

とおけば、

$$c_n = \prod_{x \in H} (1 - \zeta_f^x)$$

となる[4]。

$$\begin{aligned} x_\gamma \equiv 1 + qp^m\ell \pmod{\ell^{n+1}}, \quad x_\gamma \equiv 1 \pmod{qp^m} \\ x_\sigma \equiv 1 \pmod{\ell^{n+1}}, \quad x_\sigma \equiv 5 \pmod{2^{m+2}} \text{ if } p = 2 \\ x_\sigma \equiv 1 \pmod{\ell^{n+1}}, \quad x_\sigma \equiv 4 \pmod{3^{m+1}} \text{ if } p = 3 \end{aligned}$$

をみたす $x_\gamma, x_\sigma \in \mathbb{Z}$ を求めておく。更に

$$Y_1(\gamma) \equiv \sum_{i=0}^{\ell^n - 1} a_i \gamma^i \pmod{\ell^n}$$
$$e_\psi \equiv \sum_{j=0}^{p^m - 1} b_i \sigma^i \pmod{\ell^n}$$

も求めておく。$\ell^* \equiv 1 \pmod{qp^m\ell^{n+1}}$ をみたす素数 ℓ^* をとり、ℓ^* の原始根 g_{ℓ^*} に対し、

$$z \equiv g_{\ell^*}^{\frac{\ell^*-1}{\ell^n}} g_{\ell^*}^{\frac{\ell^*-1}{p^m}} \pmod{f}$$

となる $z \in \mathbb{Z}$ も求める。この時、

Lemma 9.3.
$$\left(\prod_{j=0}^{p^m-1} \left(\prod_{i=0}^{\ell^n-1} \left(\prod_{x \in H} (1 - z^{x x_\gamma^i x_\sigma^j}) \right)^{a_i} \right)^{b_j} \right)^{\frac{\ell^*-1}{\ell^n}} \not\equiv 1 \pmod{\ell^*}$$

なら $\lambda_{\ell,\psi}(\mathbb{B}_{p,m}) = 0$ である。

補題 9.3 の計算量は $O(qp^m\ell^{n+1})$ である。岩澤多項式の計算量も $O(qp^m\ell^{n+1})$ であるが、$\bmod \ell^n$ の計算だから高速に処理できる。補題 9.3 は $\bmod \ell^*$ の巾乗計算があるためどうしても遅くなる。$p = 2, m = 5, \ell = 4513, n = 2$ の時、岩澤多項式の計算は Xeon 2GHz で 3 日かかり、補題 9.3 はクワッドコアで分散処理を行い 25 日かかった[5]。つまり補題 9.3 の計算は岩澤多項式の計算より約 60 倍時間がかかる。分散処理する時は、

$$y_j = \prod_{i=0}^{\ell^n-1} \left(\prod_{x \in H} (1 - z^{x x_\gamma^i x_\sigma^j}) \right)^{a_i} \quad (0 \le j \le p^m - 1)$$

[4] この等式は一般の素数 p に対して成立する。
[5] どちらも TC から C プログラムを呼んでいる。

を複数のプロセスで並行して計算し、終了したら (ファイルに記録した y_j を読みこんで)

$$\left(\prod_{j=0}^{p^m-1} y_j^{b_j}\right)^{\frac{\ell^*-1}{\ell^n}} \not\equiv 1 \pmod{\ell^*}$$

かどうか調べればよい。

§10. 証明

p を任意の素数、ℓ を p と異なる奇素数とし、$m,n \geq 1$ とする。$G(\mathbb{B}_{p,m}\mathbb{B}_{\ell,\infty}/\mathbb{B}_{\ell,\infty})$ と $G(\mathbb{B}_{p,m}/\mathbb{Q})$ を同一視し Δ_m で表す。$\mathbb{B}_{p,m}$ の円分 $\mathbb{Z}_\ell$-拡大の n-th layer $\mathbb{B}_{p,m}\mathbb{B}_{\ell,n}$ のイデアル類群の ℓ-part を $A_{m,n}$ で表す。指標 $\psi : \Delta_m \longrightarrow \overline{\mathbb{Q}}_\ell$ から定まる idempotent

$$e_\psi = \frac{1}{|\Delta_m|}\sum_{\sigma\in\Delta_m} \mathrm{Tr}(\psi(\sigma))\sigma^{-1} \in \mathbb{Z}_\ell[\Delta_m]$$

は自然に $A_{m,n}$ に作用し、$A_{m,n}$ の ψ-part $A_{m,n,\psi} = \varepsilon_\psi A_{m,n}$ が定義される。Tr は $\mathbb{Q}_\ell(\psi(\Delta_m))$ から $\mathbb{Q}_\ell$ への trace である。この時 $A_{m,n}$ は

$$A_{m,n} = \bigoplus_{\psi} A_{m,n,\psi}$$

と直和分解される。ただし ψ は Δ_m の指標の $\mathbb{Q}_\ell$ 共役類の代表を動く。さて岩澤により、n に依らない整数 $\lambda_{\ell,m,\psi} \geq 0$, $\nu_{\ell,m,\psi}$ が存在し、

$$|A_{m,n,\psi}| = \lambda_{\ell,m,\psi}\, n + \nu_{\ell,m,\psi} \quad (n >> 0)$$

となることが知られている。この時、$\lambda_{\ell,m} = \lambda_\ell(\mathbb{B}_{p,m})$ は

$$\lambda_{\ell,m} = \sum_{\psi} \lambda_{\ell,m,\psi} \tag{10.1}$$

と分解される。ここで、ψ は Δ_m の指標の $\mathbb{Q}_\ell$ 共役類の代表を動く。

ψ が単射でない時、Kerψ の固定体を $\mathbb{B}_{p,m'}$ とすれば、ψ は自然に $\Delta_{m'}$ の指標と考えることができ、$A_{m,n,\psi} \cong A_{m',n,\psi}$ となるから、(10.1) は

$$\lambda_{\ell,m} = \sum_{1\leq m'\leq m}\sum_{\psi} \lambda_{\ell,m',\psi} \tag{10.2}$$

と変形できる。ただし、ψ は $\Delta_{m'}$ の単射指標の $\mathbb{Q}_\ell$ 共役類の代表を動く。(10.2) よりただちに次の補題が得られる。

Lemma 10.1. $m > m_p$ の時、

$$\lambda_\ell(\mathbb{B}_{p,m}) - \lambda_\ell(\mathbb{B}_{p,m_p}) = \sum_{m_p<m'\leq m}\sum_{\psi} \lambda_{\ell,m',\psi}\,.$$

ただし、ψ は $\Delta_{m'}$ の単射指標の $\mathbb{Q}_\ell$ 共役類の代表を動く。

さて ψ を Δ_m の単射指標、ω を $\bmod \ell$ の Teichmüller 指標とし、$\psi^* = \psi^{-1}\omega$ とおく。$\lambda_{\ell,m,\psi}$ と同様にして λ_{ℓ,m,ψ^*} が定義され、鏡像原理より

$$\lambda_{\ell,m,\psi} \leq \lambda_{\ell,m,\psi^*} \tag{10.3}$$

となる。λ_{ℓ,m,ψ^*} は Bernoulli 数 $B_{1,\omega^{-1}\psi}$ と関係している。

Lemma 10.2. $|B_{1,\omega^{-1}\psi}|_\ell = 1$ と $\lambda_{\ell,m,\psi^*} = 0$ は同値である。

Proof.

$$B_{1,\omega^{-1}\psi} \not\equiv 0 \pmod{\ell} \Longleftrightarrow \xi_0 \not\equiv 0 \pmod{\ell}$$

であり、Mazur-Wiles によって証明された岩澤主予想により、

$$\xi_0 \not\equiv 0 \pmod{\ell} \Longleftrightarrow \lambda_{\ell,m,\psi^*} = 0$$

である。 □

不等式 (10.3)、補題 10.1 と組み合わせれば次が得られる。

Corollary 10.3. $|B_{1,\omega^{-1}\psi}|_\ell = 1$ なら $\lambda_{\ell,m,\psi} = 0$ である。

Corollary 10.4. $m > m_p \Longrightarrow \lambda_\ell(\mathbb{B}_{p,m}) = \lambda_\ell(\mathbb{B}_{p,m_p})$.

これより直ちに定理 1.3 が得られる。

Remark. 隅田浩樹氏より、Table 1,2 の case (A) の場合は岩澤多項式を計算しなくても $\lambda_{\ell,\psi}(\mathbb{B}_{p,m}) = 0$ がわかると教えて頂いた (cf. [8, Remark 4])。つまり市村・隅田の判定法を適用しなければならないのは 11 個の内 3 個のみである。

References

[1] D. Byeon, *Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields*, Compositio Math. **126** (2001), 249–256.

[2] B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. Math. **109** (1979), 377–395.

[3] T. Fukuda and K. Komatsu, Weber の類数問題に対する計算的アプローチ, 第 8 回代数学と計算研究集会報告集, `http://tnt.math.metro-u.ac.jp/ac/2007/proceedings/`

[4] T. Fukuda, K. Komatsu and T. Morisawa, *On λ-invariants of $\mathbb{Z}_\ell$-extensions over real abelian number fields of prime power conductors*, preprint, 2010.

[5] T. Fukuda and H. Taya, 岩澤不変量の計算, 応用数理学会誌, **12** (2002), 293–306.

[6] R. Greenberg, *On the Iwasawa invariants of totally real number fields.* Amer. J. Math. **98**(1976), 263–284.

[7] K. Horie, *Certain primary components of the ideal class group of the $\mathbb{Z}_p$-extension over the rationals*, Tohoku Math. J. **59** (2007), 259–291.

[8] H. Ichimura and H. Sumida, *On the Iwasawa Invariants of certain real abelian fields II*, Inter. J. Math. **7** (1996), 721–744.

[9] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

[10] T. Morisawa, *A Class Number Problem in the Cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$*, Tokyo J. Math. **32** (2009), 549–558.

[11] J. Nakagawa and K. Horie, *Elliptic curves with no rational points*, Proc. Amer. Math. Soc. **104** (1988), 20–24.

[12] K. Ono, *Indivisibility of class numbers of real quadratic fields*, Compositio Math. **119** (1999), 1–11.

[13] M. Ozaki and H. Taya, *On the Iwasawa λ_2-invariants of certain families of real quadratic fields*, Manuscripta Math. **94** (1997), no. 4, 437- 444.

[14] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edition, Graduate Texts in Math., 83, Springer-Verlag, New York, Heidelberg, Berlin, 1997.