岩澤多項式の近似計算について

水沢 靖

この稿は主に文献 [1] [2] を参考にして、虚 2 次体の円分 $\mathbf{Z}_p$ 拡大体の最大不分岐アーベル pro-p 拡大の Galois 群の岩澤多項式を p 進近似計算する方法についてまとめたものです.

§1. 設定と方針

p を素数とし、m を平方因子を持たない正の整数として虚 2 次体 $K = \mathbf{Q}(\sqrt{-m})$ を考える．K に対応する Dirichlet 指標 χ は、K の判別式 $\mathfrak{D}$ を法とする Kronecker 指標に等しい[1]．奇素数 p に対しては $q = p$、$p = 2$ に対しては $q = 4$ と定める．$p = 2$ の場合には、K と $K^\vee = \mathbf{Q}(\sqrt{-2m})$ は円分 $\mathbf{Z}_2$ 拡大を共有するので、適当に入れ替えて m は奇数（即ち χ は第一種の指標）であると仮定する．この下で K が q 分体に含まれる場合、即ち $\mathfrak{D} = -q$ である場合には、岩澤多項式は自明であることがわかっている (cf. [5] Exercise 5.9, Theorem 6.17, etc.) ので、以下では $\mathfrak{D} \neq -q$ と仮定する．Q を q と $|\mathfrak{D}|$ の最小公倍数とし、$D = Q/q$ と定めると、以上の仮定から $D \neq 1$ である．自然な同型によって、円分 $\mathbf{Z}_p$ 拡大の Galois 群

$$\mathit{\Gamma} = \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q}) \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_{qp^\infty})/\mathbf{Q}(\zeta_q)) \simeq \mathrm{Gal}(K(\zeta_{qp^\infty})/K(\zeta_q)) \simeq \mathrm{Gal}(K_\infty/K)$$

を全て同一視し、$1 + q\mathbf{Z}_p = \kappa^{\mathbf{Z}_p}$ なる κ（例えば $\kappa = 1 + Q$, $1 + q$）と $\mathit{\Gamma}$ の位相的生成元

$$\gamma = \left(\zeta_{qp^n} \mapsto \zeta_{qp^n}^{\kappa} \ (\forall n \geq 0) \right)\big|_{\mathbf{Q}_\infty}$$

を固定して考える．また $\gamma_n = \gamma \mathit{\Gamma}^{p^n} \in \mathit{\Gamma}_n = \mathit{\Gamma}/\mathit{\Gamma}^{p^n}$ とし、この固定された κ と γ の下で

$$\mathit{\Lambda} = \mathbf{Z}_p[[T]] \simeq \mathbf{Z}_p[[\mathit{\Gamma}]] \ : \ 1 + T \ \leftrightarrow \ \gamma$$

であり、この両者を同一視する．Stickelberger 元から、群環 $\mathbf{Z}_p[\mathit{\Gamma}_n]$ の元

$$\xi_n = -\frac{1}{Qp^n} \sum_{0<a<Qp^n,\,(a,Q)=1} a\,\chi(a) \left(\frac{\mathbf{Q}_n/\mathbf{Q}}{a} \right)^{-1}$$

が定まる．ここで $\mathbf{Z}_p$ 内の原始 $\varphi(q)$ 乗根 α を一つ取り[2]、各 $n \geq 0$ に対して

$$\frac{1}{2} f_n(T) = -\frac{1}{D} \sum_{i=0}^{p^n-1} c_i\,(1+T)^{p^n-i} \in \mathbf{Z}_p[T], \qquad \underline{c_i = \sum_{t=0}^{\frac{\varphi(q)-2}{2}} \sum_{j=1}^{D-1} j\,\chi\big(s_n(\,\kappa^i\alpha^t\,) + jqp^n\big)} \ \bigstar$$

（ここに、$z \in \mathbf{Z}_p$ に対して $s_n(z) \equiv z \bmod qp^n$, $0 \leq s_n(z) < qp^n$ ）なる多項式 $f_n(T)$ とその係数を定める．すると [5] Proposition 7.9 などによって、

$$\frac{1}{2} f_n(T) \ \leftrightarrow \ \frac{1}{2}\xi_n = -\frac{1}{D} \sum_{i=0}^{p^n-1} c_i\,\gamma_n^{-i} \ \ : \ \ \mathit{\Lambda}/(\,(1+T)^{p^n} - 1\,) \ \simeq \ \mathbf{Z}_p[\mathit{\Gamma}_n]$$

[1] UBASIC の関数では $\chi(a) = \texttt{kro}(\mathfrak{D},a)$.

[2] φ は Euler 関数、即ち $p = 2$ ならば $\varphi(q) = 2$、$p \neq 2$ ならば $\varphi(q) = p - 1$.

なる対応が得られ、射影系で閉じていることから岩澤冪級数

$$f_\chi(T) = \varprojlim f_n(T) \ \leftrightarrow\ \varprojlim \xi_n \quad : \quad \Lambda = \varprojlim\ \Lambda/(\,(1+T)^{p^n}-1\,)\ \simeq\ \mathbf{Z}_p[[\Gamma]] = \varprojlim\ \mathbf{Z}_p[\Gamma_n]$$

が得られる．このとき、

$$f_\chi(T) \equiv f_n(T) \mod (1+T)^{p^n}-1$$

であることに注意する．ここで導手 q の Teichmüllar 指標を ω とすると、第一種の偶指標 $\omega\chi^{-1}$ に対する久保田-Leopoldt の p 進 L 関数が（岩澤関数として）

$$L_p(s,\omega\chi^{-1}) = f_\chi(\kappa^s-1)$$

と表される．Ferrero-Washington の定理と p 進 Weierstrass 準備定理とによって、ある $U_\chi(T)\in\Lambda^\times$ と monic な distinguished 多項式 $P_\chi(T)\in\mathbf{Z}_p[T]$ とによって、

$$\frac{1}{2}f_\chi(T) = U_\chi(T)P_\chi(T)$$

と表される．虚 2 次体 K の円分 $\mathbf{Z}_p$ 拡大体 K_∞ の最大不分岐アーベル pro-p 拡大の Galois 群 $\mathfrak{X}$ は有限生成捩れ Λ 加群であり、（$T=\gamma-1$ の $\mathfrak{X}\otimes_{\mathbf{Z}_p}\overline{\mathbf{Q}}_p$ への線形作用に関する）その特性多項式を $\mathrm{char}\mathfrak{X}(T)$ とすると、岩澤主予想（Mazur-Wiles の定理）から

$$P_\chi(T) = \mathrm{char}\mathfrak{X}(T)$$

が成り立つ．これが**岩澤多項式**であり、その次数 $\lambda=\deg P_\chi(T)$ とともに、その係数を p 進近似計算することがこの稿の目標である．ここで各 n に対して、p^n-1 次の多項式

$$g_n(T) = c_0 + \sum_{i=1}^{p^n-1} c_i\,(1+T)^{p^n-i} \ =\ a_0 + \sum_{\ell=1}^{p^n-1} a_\ell\,T^\ell, \quad a_0 = \sum_{i=0}^{p^n-1} c_i, \quad a_\ell = \sum_{i=0}^{p^n-\ell} c_i \binom{p^n-i}{\ell}$$

を定める．これを Λ の元として考え、また定め方から

$$g_n(T) \equiv -\frac{D}{2}f_n(T) \equiv -\frac{D}{2}f(T) \mod (1+T)^{p^n}-1$$

であることに注意する．p 進 Weierstrass 準備定理により、ある $U_n(T)\in\Lambda^\times$ と monic な distinguished 多項式 $P_n(T)\in\mathbf{Z}_p[T]$ および $\mu_n\geq 0$ とによって

$$g_n(T) = p^{\mu_n}U_n(T)P_n(T)$$

と書けるが、$(1+T)^{p^n}-1\equiv T^{p^n} \bmod p$ であることから、$p^n>\lambda$ であるほど n が十分大きいならば、$\mu_n=0$ かつ

$$\lambda = \deg P_n(T) = \min\{\ \ell\ \mid a_\ell\not\equiv 0 \bmod p\ \}$$

となる．このとき

$$r = \min\{\ 1\leq z\in\mathbf{Z}\ \mid\ p^z\geq\lambda\ \} \leq n$$

と定めると、[2] Lemma 5 によって [3]

$$P_n(T) \equiv P_\chi(T) \mod p^{n-r+1}$$

となる．これにより岩澤多項式の近似計算は、十分大きい n に対する $P_n(T)$ の次数および係数の近似値の計算に帰着される．以下、$p^n > \lambda$ なる n を一つ固定して考える．ここで shift operator τ とそれによる $g_n(T)$ の像

$$\tau \ : \ \Lambda \to \Lambda, \ \sum_{i=0}^{\infty} \bullet_i T^i \ \mapsto \ \sum_{i=0}^{\infty} \bullet_{i+\lambda} T^i, \quad V_n(T) = \tau\big(g_n(T)\big) = \sum_{\ell=0}^{p^n-1-\lambda} a_{\lambda+\ell} T^\ell \ \in \ \Lambda^\times$$

を定め、$g_n(T)$ を

$$g_n(T) = R_n(T) + T^\lambda V_n(T), \quad R_n(T) \ = \ \sum_{\ell=0}^{\lambda-1} a_\ell T^\ell \ \in \ p\mathbf{Z}_p[T]$$

と表す．これらを用いて Λ 上の $\mathbf{Z}_p$線型作用素

$$\mathbb{T} = \tau \circ (-V_n(T)^{-1} R_n(T)) \ : \ \Lambda \to \Lambda \ , \quad F(T) \ \mapsto \ \tau\big(- V_n(T)^{-1} R_n(T) F(T) \big)$$

を定めると、

$$U_n(T)^{-1} \ = \ V_n(T)^{-1} \sum_{j=0}^{\infty} \mathbb{T}^j(1)$$

と表すことができる．簡単のために $m = p^n - 1 - \lambda$, $b_\ell = a_{\lambda+\ell}$ とおくと、$V_n(T)^{-1}$ は

$$V_n(T)^{-1} \ = \ \sum_{j=0}^{\infty} B_j T^j \ = \ b_0^{-1} \Big\{ \sum_{j=0}^{\infty} \Big(- \sum_{\ell=0}^{m} b_0^{-1} b_\ell T^\ell \Big)^j \Big\}$$

として計算できる [4]．また

$$V_n(T)^{-1} R_n(T) \ = \ \sum_{k=0}^{\infty} A_k T^k, \quad A_k \ = \ \sum_{\ell=0}^{\min\{\lambda-1, k\}} B_{k-\ell} a_\ell \ \in \ p\mathbf{Z}_p$$

であり、$\mathbb{T}^j(1)$ の係数

$$\mathbb{T}^j(1) \ = \ \sum_{\ell=0}^{\infty} Z_\ell^{(j)} T^\ell \ \in \ p^j \Lambda, \quad Z_\ell^{(j)} \in \mathbf{Z}[A_0, \cdots, A_{\ell+j\lambda}]$$

および

$$Z_\ell \ = \ \sum_{j=0}^{n-r} Z_\ell^{(j)} \ \equiv \ \sum_{j=0}^{\infty} Z_\ell^{(j)} \mod p^{n-r+1}$$

[3] 証明を読むと、$\dot{\omega}_{z+\ell}$ を $\omega_{z+\ell}$ に代えても、また $p = 2$ の場合にも成立していることがわかる．
[4] 実際には 1 を $V_n(T)$ で割る方法によって、帰納的に計算する．

を定めておく．岩澤多項式は $\bmod p^{n-r+1}$ で近似され、また λ 次の monic な多項式になることが保証されているので、

$$\begin{aligned} P_\chi(T) \;\equiv\; P_n(T) \;=\; g_n(T)U_n(T)^{-1} \;&=\; \Big(\sum_{\ell=0}^{p^n-1} a_\ell\, T^\ell\Big)\Big(\sum_{k=0}^{\infty} B_k\, T^k\Big)\Big(\sum_{j=0}^{\infty}\sum_{\ell=0}^{\infty} Z_\ell^{(j)} T^\ell\Big) \\ &\equiv\; \Big(\sum_{\ell=0}^{p^n-1} a_\ell\, T^\ell\Big)\Big(\sum_{k=0}^{\infty} B_k\, T^k\Big)\Big(\sum_{\ell=0}^{\infty} Z_\ell T^\ell\Big) \\ &\equiv\; T^\lambda + \sum_{i=0}^{\lambda-1}\Big(\sum_{\ell=0}^{i}\sum_{k=0}^{i-\ell} a_\ell\, B_k\, Z_{i-\ell-k}\Big)\, T^i \qquad\qquad \bmod p^{n-r+1}\Lambda \end{aligned}$$

となる．よって岩澤多項式の係数の近似計算は、$0 \le \ell \le \lambda-1$ の範囲で $a_\ell,\ B_\ell,\ Z_\ell$ を $\bmod p^{n-r+1}$ で求めることに帰着される．$Z_\ell \bmod p^{n-r+1}$ は $0 \le \ell \le \lambda-1$ の範囲で求まればよいので、$Z_\ell^{(j)} \bmod p^{n-r+1}$ は $0 \le j \le n-r,\ 0 \le \ell \le \lambda-1$ の範囲で必要となる．$Z_\ell^{(j)}$ は $A_0,\ \cdots,\ A_{\ell+j\lambda}$ の多項式として表されるので、A_k は $0 \le k \le (\lambda-1)+(n-r)\lambda = (n-r+1)\lambda-1$ の範囲で求まればよい．B_k も同じ範囲で求めればよく、

$$\big\{\ b_\ell \;\big|\; 0 \le \ell \le \min\{\, p^n-1-\lambda,\, k\,\}\ \big\} = \big\{\ a_\ell \;\big|\; \lambda \le \ell \le \min\{\, p^n-1,\, k+\lambda\,\}\ \big\}$$

によって表されるので、a_ℓ は $0 \le \ell \le \min\{\, p^n-1,\, (\lambda-1)+(n-r)\lambda+\lambda\,\} = \min\{\, p^n-1,\, (n-r+2)\lambda-1\,\}$ まで求めておけばよい．

§2. 計算の手順

Step 1. [50-180]　素数 p と平方因子を持たない正の整数 m、および近似の精度に関する自然数 n を入力．$p=2$ で m が偶数の場合には、m を 2 で割った奇数で置き換える．$\mathfrak{D} = -q$ ならば $P_\chi(X)=1$ を出力して終了．$D,\ Q,\ \kappa$ および α を定め、配列 A1, $\cdots$, A7 を用意する [5]．

Step 2. [230-330]　$0 \le i \le p^n-1$ に対して次を計算する．

$$\mathbf{Z} \ni \mathtt{A1}(i) \equiv c_i \mod p^n\,, \quad 0 \le \mathtt{A1}(i) < p^n$$

ここに $s_n(\kappa^i\alpha^t)\kappa \equiv s_n(\kappa^{i+1}\alpha^t),\ s_n(\kappa^i\alpha^t)\alpha \equiv s_n(\kappa^i\alpha^{t+1}) \mod qp^n$ であることに注意．

Step 3. [350-780]　まず

$$\mathbf{Z} \ni \mathtt{A2}(0) \equiv a_0 \equiv \sum_{i=0}^{p^n-1} \mathtt{A1}(i) \mod p^n\,, \quad 0 \le \mathtt{A2}(0) < p^n$$

を計算し、$\mathtt{A2}(0) \not\equiv 0 \ (\bmod p)$ ならば $P_\chi(T)=1$ を出力して終了．次に $\ell \ge 1$ に対して、$\mathtt{A2}(\ell) \not\equiv 0 \mod p$ となるまで（即ち $\ell=\lambda$ まで）順に

$$\mathbf{Z} \ni \mathtt{A2}(\ell) \equiv a_\ell \equiv \sum_{i=0}^{p^n-\ell} \mathtt{A1}(i)\binom{p^n-i}{\ell} \mod p^n\,, \quad 0 \le \mathtt{A2}(\ell) < p^n$$

[5] 配列の長さについては後述．

を計算し、λ および r を確定する．全ての $1 \le \ell \le p^n - 1$ に対して $\mathtt{A2}(\ell) \equiv 0 \mod p$ となったならば、$\lambda > p^n - 1$ であるので n を増やしてやり直す．一方 λ が確定して $n = r$ ならば、$P_\chi(T) \equiv T^\lambda \mod p$ を出力して終了．さらに $\lambda = 1$ で p が K で分解しているならば、$P_\chi(T) = T$ を出力して終了してもよい．計算を続ける場合は、$\lambda + 1 \le \ell \le \min\{\, p^n - 1,\, (n-r+2)\lambda - 1 \,\}$ に対して

$$\mathbf{Z} \ni \mathtt{A2}(\ell) \equiv a_\ell \equiv \sum_{i=0}^{p^n-\ell} \mathtt{A1}(i) \binom{p^n - i}{\ell} \mod p^{n-r+1}, \quad 0 \le \mathtt{A2}(\ell) < p^{n-r+1}$$

を計算する．ここで $p^n - 1 < (n-r+2)\lambda - 1$ である場合には、次の Step 4 の計算のために、$p^n \le \ell \le (n-r+2)\lambda - 1$ に対して $\mathtt{A2}(\ell) = 0$ と定めておく．

Step 4. [800-870]　この状態で $0 \le \ell \le \min\{\, p^n - 1 - \lambda,\, (n-r+1)\lambda - 1 \,\}$ に対して $\mathtt{A2}(\ell + \lambda) \equiv b_\ell \mod p^{n-r+1}$ であり、$p^n - 1 - \lambda < (n-r+1)\lambda - 1$ である場合には $p^n - \lambda \le \ell \le (n-r+1)\lambda - 1$ に対して $b_\ell = \mathtt{A2}(\ell + \lambda) = 0$ が定まっていることに注意する．これらから $\mathtt{A3}(k) = B_k \bmod p^{n-r+1}$ $(\, 0 \le k \le (n-r+1)\lambda - 1 \,)$ を次のような手順で求めていく．（次頁の図も参照）簡単のために B_k を配列 $\mathtt{A3}(k)$ と同一視し、$x = (n-r+1)\lambda - 1$ とおく．

$B_0 = 1$ $B_1 = \cdots = B_x = 0$ とする．
$i = 0$ から $i = x - 1$ まで
『 B_i を $B_i b_0^{-1}$ で置き換えて、
　$k = i + 1$ から $k = x$ まで
　「B_k を $B_k - B_i b_{k-i}$ で置き換える.」
　を k について繰り返す．』
を i について繰り返す.
B_x を $B_x b_0^{-1}$ で置き換える.

$\mathtt{A3}(0) = 1$ $\mathtt{A3}(1) = \cdots = \mathtt{A3}(x) = 0$
for $i = 0$ to $x - 1$
　$\mathtt{A3}(i) \equiv \mathtt{A3}(i)\mathtt{A2}(\lambda)^{-1}$
　for $k = i + 1$ to x
　　$\mathtt{A3}(k) \equiv \mathtt{A3}(k) - \mathtt{A3}(i)\mathtt{A2}(k - i + \lambda)$
　next k
next i
$\mathtt{A3}(x) \equiv \mathtt{A3}(x)\mathtt{A2}(\lambda)^{-1}$

こうして帰納的に、$0 \le k \le (n-r+1)\lambda - 1$ の範囲で

$$\mathbf{Z} \ni \mathtt{A3}(k) \equiv B_k \mod p^{n-r+1}, \quad 0 \le \mathtt{A3}(k) < p^{n-r+1}$$

が定まる．この過程では $p^n - 1$ と $(n-r+2)\lambda - 1$ のどちらが大きいにしても、$\mathtt{A2}(\ell)$ の値は $\ell = (n-r+2)\lambda - 1$ まで定まっているものとして計算していることに注意.

Step 5. [890-950]　$0 \le k \le (n-r+1)\lambda - 1$ の範囲で次を定める．

$$\mathbf{Z} \ni \mathtt{A4}(k) \equiv \sum_{\ell=0}^{\min\{\,\lambda-1,\,k\,\}} \mathtt{A3}(k-\ell)\mathtt{A2}(\ell) \equiv A_k \mod p^{n-r+1}, \quad 0 \le \mathtt{A4}(k) < p^{n-r+1}$$

Step 6. [970-1120]　次に $0 \le k \le \lambda - 1$ の範囲で

$$\mathbf{Z} \ni \mathtt{A5}(\ell) \equiv Z_\ell = \sum_{j=0}^{n-r} Z_\ell^{(j)} \mod p^{n-r+1}, \quad 0 \le \mathtt{A5}(\ell) < p^{n-r+1}$$

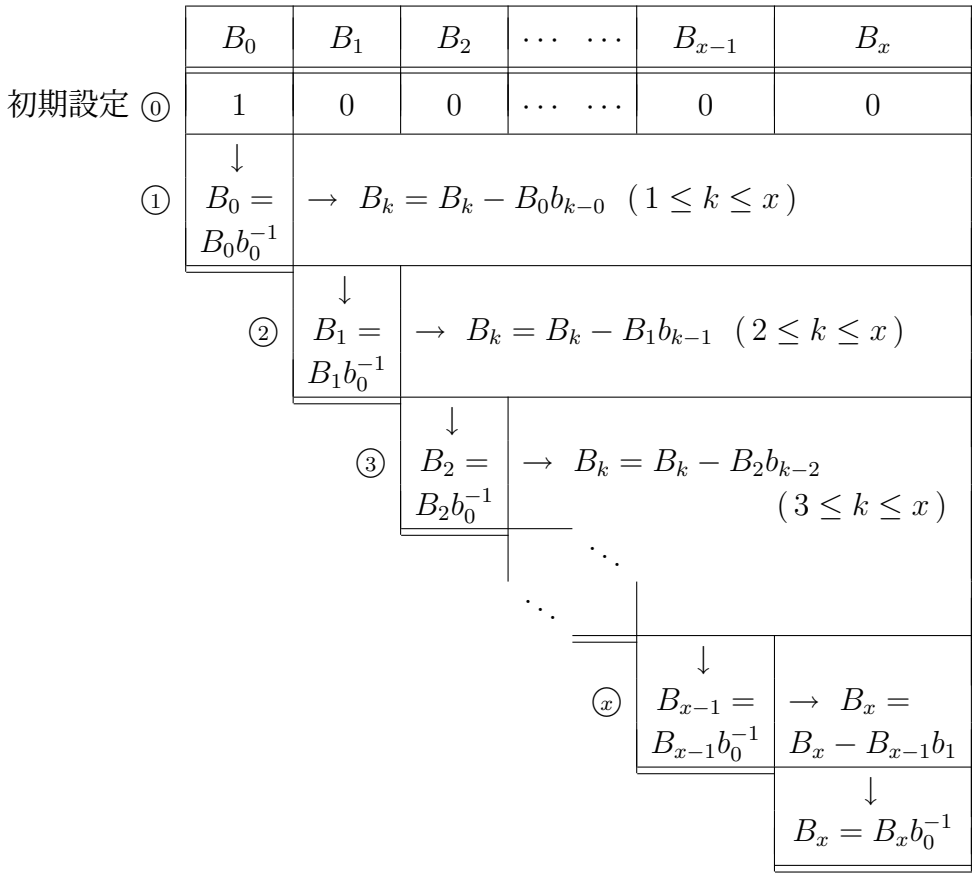
を求めたい．そのために各 j に対して

$$\mathbf{Z} \ni \mathtt{A6}(\ell) \equiv Z_\ell^{(j)} \mod p^{n-r+1}, \quad 0 \le \mathtt{A6}(\ell) < p^{n-r+1}$$

$$V_n(T) = b_0 + b_1 T + b_2 T^2 + \cdots + b_{p^n-1-\lambda} T^{p^n-1-\lambda} + 0\,T^{p^n-\lambda} + 0\,T^{p^n-\lambda+1} + \cdots$$

$x = (n-r+1)\lambda - 1$ 次の係数まで計算

$$\begin{array}{rl|llll|l}
 & & \overbrace{\phantom{b_0^{-1}\ +b_0^{-1}(-b_0^{-1}b_1)T\ +b_0^{-1}(-b_0^{-1}b_2-b_0^{-2}b_1^2)T^2\ +\cdots}} & & & \\
 & & b_0^{-1} & +b_0^{-1}(-b_0^{-1}b_1)T & +b_0^{-1}(-b_0^{-1}b_2-b_0^{-2}b_1^2)T^2 & +\cdots & = V_n(T)^{-1} \\
\cline{3-6}
V_n(T) &) & 1 & & & & \leftarrow ⓪ \\
 & & 1 & +b_0^{-1}b_1T & +b_0^{-1}b_2T^2+\cdots & & = B_0V_n(T) \\
\cline{3-6}
 & & & -b_0^{-1}b_1T & -b_0^{-1}b_2T^2+\cdots & & \leftarrow ① \\
 & & & -b_0^{-1}b_1T & -b_0^{-2}b_1^2T^2+\cdots & & = B_1V_n(T) \\
\cline{4-6}
 & & & & (-b_0^{-1}b_2-b_0^{-2}b_1^2)T^2 & +\cdots & \leftarrow ② \\
 & & & & (-b_0^{-1}b_2-b_0^{-2}b_1^2)T^2 & +\cdots & = B_2V_n(T) \\
\cline{4-6}
 & & & & & \cdots & \leftarrow ③ \\
 & & & & & \cdots & = B_3V_n(T)
\end{array}$$



Step 4 の参考図

を計算してゆく．$\mathbb{T}^0(1)=1$ 即ち $Z_0^{(0)}=1,\ Z_\ell^{(0)}=0\ (\forall\,\ell\ge 1)$ であるので、初期値として $\mathtt{A5}(0)=\mathtt{A6}(0)=1,\ \mathtt{A5}(\ell)=0\ (1\le\ell\le\lambda-1),\ \mathtt{A6}(\ell)=0\ (1\le\ell\le(n-r+1)\lambda-1)$ と定めておく．$1\le j\le n-r$ に関して帰納的に $\mathbb{T}$ を作用させながら、j 番目のステップで $\mathtt{A6}(\ell)\equiv Z_\ell^{(j)} \mod p^{n-r+1}$ を計算して A5 に加えてゆく．定義から

$$Z_\ell^{(j)}=-\sum_{i=0}^{\ell+\lambda} Z_i^{(j-1)}A_{\ell+\lambda-i}$$

であるので、j に関する帰納的な過程において、A6 を書き換える際には一つ前の j における A6 の情報が必要である．よって各 j 番目のステップにおいて、

$$\mathbf{Z}\ni \mathtt{A7}(\ell)\equiv\sum_{i=0}^{\ell+\lambda}\mathtt{A6}(i)\mathtt{A4}(\ell+\lambda-i)\equiv-\boxed{\text{上の式の右辺}} \mod p^{n-r+1},\ 0\le\mathtt{A7}(\ell)<p^{n-r+1}$$

を計算し、A6 に $-$A7 の値をコピーしてから A5 に A6 を加えて、次の $j+1$ 番目のステップに移る．また、最終的に $\mathtt{A5}(\ell)\equiv Z_\ell^{(n-r)} \mod p^{n-r+1}$ が $0\le\ell\le\lambda-1$ の範囲で求まればよいので、j 番目のステップにおいて $\mathtt{A6}(\ell)=-\mathtt{A7}(\ell)\equiv Z_\ell^{(j)} \mod p^{n-r+1}$ は $0\le\ell\le x-j\lambda=(n-r+1)\lambda-1-j\lambda$ の範囲で求めればよい．こうして $j=n-r$ のステップが終了すると、A5 には Z_ℓ の情報が入っていることになる．

	$\mathtt{A6}(0)$ $Z_0^{(j)}$	$\mathtt{A6}(1)$ $Z_1^{(j)}$	$\cdots$	$\mathtt{A6}(\lambda-1)$ $Z_{\lambda-1}^{(j)}$	$\cdots$	$\mathtt{A6}(x-j\lambda)$ $Z_{x-j\lambda}^{(j)}$	$\cdots$	$\mathtt{A6}(x)$ $Z_x^{(j)}$
（初期値）$j=0$	1	0	$\cdots$	0	$\cdots$	0	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$	$\iddots$	
j	$Z_\ell^{(j)}=-\sum_{i=0}^{\ell+\lambda} Z_i^{(j-1)}A_{\ell+\lambda-i}\ \ (0\le\ell\le x-j\lambda)$							
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\iddots$			
$j=n-r$	$Z_0^{(n-r)}$	$Z_1^{(n-r)}$	$\cdots$	$Z_{\lambda-1}^{(n-r)}$				
（縦の総和）A5	Z_0	Z_1	$\cdots$	$Z_{\lambda-1}$				

Step 7. [1140-1260]　$0\le i\le\lambda-1$ に対して

$$\mathbf{Z}\ \ni\ \mathtt{C}_i\equiv\sum_{\ell=0}^{i}\sum_{k=0}^{i-\ell}\mathtt{A2}(\ell)\,\mathtt{A3}(k)\,\mathtt{A5}(i-\ell-k) \mod p^{n-r+1},\ \ 0\le\mathtt{C}_i<p^{n-r+1}$$

を計算し、

$$T^\lambda+\sum_{i=0}^{\lambda-1}\mathtt{C}_i\,T^i\ \equiv\ T^\lambda+\sum_{i=0}^{\lambda-1}\Big(\sum_{\ell=0}^{i}\sum_{k=0}^{i-\ell}a_\ell\,B_k\,Z_{i-\ell-k}\Big)T^i\ \equiv\ P_\chi(T) \mod p^{n-r+1}$$

を出力して終了.

§3. 配列の長さと α の計算

以上の計算過程からもわかるように、配列の長さは以下の表を目安に設定すればよい. ここで配列の長さの総和の限度を、H と設定しておくことにする. λ と r は計算しなければわからないので、入力 p, n に対して最も長くなる $r=1$ の場合を考えて、長さ H を分配する.

	c_i	a_ℓ	B_k	A_k	Z_ℓ	$Z_\ell^{(j)}$	$Z_\ell^{(j)}$	$0 \le$(添字)$\le$(長さ)-1
	A1	A2	A3	A4	A5	A6	A7	
長さ	p^n	$x+1+\lambda$	$x+1$	$x+1$	λ	$x+1$	$x+1$	$x=(n-r+1)\lambda-1$
比率	$-$	$n+1$	n	n	1	n	n	
設定	p^n	$\lfloor(n+1)\mathtt{Y}\rfloor$	$\lfloor n\mathtt{Y}\rfloor$	$\lfloor n\mathtt{Y}\rfloor$	$\lfloor\mathtt{Y}\rfloor$	$\lfloor n\mathtt{Y}\rfloor$	$\lfloor n\mathtt{Y}\rfloor$	$\mathtt{Y}=\dfrac{\mathtt{H}-p^n}{5n+2}$

また、Step 2 で $c_i \bmod p^n$ を計算するためには、ある原始 $\varphi(q)$ 乗根 $\alpha \in \mathbf{Z}_p^\times$ を qp^n を法として近似した値

$$\mathbf{Z} \ni \mathtt{a} \equiv \alpha \mod qp^n, \quad 0 \le \mathtt{a} < qp^n$$

を定めなければならない. $p \le 3$ の場合には $\alpha = \mathtt{a} = -1$ であるが、★式において t に関する和は $t=0$ の項のみなので無視してよい. 以下、$p \ge 5$ の場合を考える. 自然な全射 $(\mathbf{Z}/p^{n+1}\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times$ を考えれば、素数 p の原始根 $g \in \mathbf{Z}$ に対して $g \bmod p^{n+1} \in (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times$ の位数は $p-1$ の p 冪倍である. よって a を

$$\mathbf{Z} \ni \mathtt{a} \equiv g^{p^n} \mod p^{n+1}, \quad 0 \le \mathtt{a} < p^{n+1}$$

なるものとして定めると、$\mathtt{a} \bmod p^{n+1} \in (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times$ の位数は丁度 $p-1$ である. さらに $\mathtt{a}\omega(\mathtt{a})^{-1} \equiv 1 \pmod p$ なので $\mathtt{a}\omega(\mathtt{a})^{-1} \bmod p^{n+1}$ は $(\mathbf{Z}/p^{n+1}\mathbf{Z})^\times$ の p-Sylow 部分群に含まれるが、位数は $p-1$ の約数なので $\mathtt{a}\omega(\mathtt{a})^{-1} \equiv 1 \mod p^{n+1}$ となる. よって $\alpha = \omega(\mathtt{a})$ の位数も $p-1$、即ち原始 $p-1$ 乗根であって、$\mathtt{a} \equiv \alpha \mod p^{n+1}$ である. ★式において c_i は α の取り方に依らないので、この a を用いて Step 2 の計算を行えばよい.

§4. UBASIC でのプログラム

Iwapoly.ub [30] の配列の長さの総和の限度 H は、使うコンピュータのメモリに応じた制限を受ける. p, m, n を入力した後、[200-210] において各配列に配分する. $q =$ Qr, $Q =$ Q, $\kappa =$ G であり、[160] において κ として $1+Q$ を採用しているが、G=1+Qr 即ち $\kappa = 1+q$ の方を採用することもできる[6]. また、[180]（および[1430-1490]）における A=fnAlpha(Pr,N) が原始 $p-1$ 乗根 α ($p \ge 5$) の剰余値 a であり、その計算で必要な原始根 g は[1290-1410] において計算される.

[6]『$L_p(s, \omega\chi^{-1}) = f_\chi(\kappa^s - 1)$』であったことからもわかるように、この κ の選び方によって出力される値が異なることに注意！ [1] では同じく $\kappa = 1+Q$ を採用しているが、[4] では $\kappa = 1+q$ を採用している.

```
print "■虚二次体の円分 Z_p 拡大の岩澤多項式■"
'
H=54600 'H=99500
'
print:input "素数=";Pr:Isp=fnIsprm(Pr)
  if Isp=0 then print "素数ではありません。"
  :goto 50
  if Isp=2 then print "数値が大き過ぎます。"
  :goto 50
  if Pr=2 then Qr=4 else Qr=Pr
input "ルートの中身の絶対値=";M
  if moeb(M)=0 then print "平方因子があります。"
  :goto 90
  if Pr<>2 then jump elseif M@2=0 then M=M\2
  **
  if M@4=3 then M=-M else M=-4*M
  if M=-Qr then clr time:print "λ= 0"
    :print 1+0*_X:print time:goto 50
  Q=lcm(Qr,abs(M)):D=Q\Qr:G=1+Q ':G=1+Qr
print "近似する";Pr; input "冪の指数=";N
:clr time
  P=Pr^N:P1=P*Qr:Al=fnAlpha(Pr,N)
'
Y=(H-P)/(5*N+2):Y1=int((N+1)*Y)-1
:Y2=int(N*Y)-1:Y3=int(Y)-1
dim A1%(P-1),A2%(Y1),A3%(Y2),A4%(Y2),A5%(Y3),
A6%(Y2),A7%(Y2)
'
S=1
for I=0 to P-1
  C=0:S1=S
  for K=0 to (eul(Qr)-2)\2
    for J=1 to D-1
      C=(C+J*kro(M,S1+J*P1))@P
    next J
    S1=(S1*Al)@P1
  next K
  A1%(I)=C:S=(S*G)@P1
next I
'
C=0
for I=0 to P-1
  C=(C+A1%(I))@P
next I
if C@Pr<>0 then print "λ= 0":print 1+0*_X
:print time
  :erase A1%(),A2%(),A3%(),A4%(),A5%(),A6%(),
  A7%():goto 50
A2%(0)=C
'
L=1
while P-L
  C=0
  for I=1 to P-L
    C=(C+A1%(I)*combi(P-I,L))@P
  next I
  A2%(L)=C:if C@Pr<>0 then jump
  inc L
wend
print "λ>";P-1:print time
print "λを確定できません。";
print "近似する冪指数を増やしてやり直してください。"
erase A1%(),A2%(),A3%(),A4%(),A5%(),A6%(),
A7%():goto 170
'
**
print "λ=";L
if L>1 then jump elseif kro(M,Pr)<>1
then jump
print _X:print time
erase A1%(),A2%(),A3%(),A4%(),A5%(),A6%(),
A7%():goto 50
**
R=1
loop
  if L>Pr^R then inc R else jump
endloop
**
if N=R then print _X^L;" mod";Pr;"^";N-R+1
:print time
  :erase A1%(),A2%(),A3%(),A4%(),A5%(),A6%(),
  A7%():goto 50
Z=min(P-1,(N-R+2)*L-1):B=Pr^(N-R+1)
'
for K=L+1 to Z
  C=0
  for I=1 to P-K
    C=(C+A1%(I)*combi(P-I,K))@B
  next I
  A2%(K)=C
next K
'
A3%(0)=1:X=(N-R+1)*L-1:V=modinv(A2%(L),B)
for I=0 to X-1
  C=(A3%(I)*V)@B:A3%(I)=C
  for K=I+1 to X
    C=(A3%(K)-A3%(I)*A2%(K-I+L))@B:A3%(K)=C
  next K
next I
C=(A3%(X)*V)@B:A3%(X)=C
'
for K=0 to X
  C=0
  for I=0 to min(L-1,K)
    C=(C+A3%(K-I)*A2%(I))@B
  next I
  A4%(K)=C
next K
'
A5%(0)=1:A6%(0)=1
for J=1 to N-R
  for K=0 to X-J*L
    C=0
    for I=0 to L+K
      C=(C+A6%(I)*A4%(L+K-I))@B
    next I
    A7%(K)=C
  next K
  for K=0 to X-J*L
    A6%(K)=-A7%(K)
  next K
  for I=0 to L-1
    C=(A5%(I)+A6%(I))@B:A5%(I)=C
  next I
next J
'
Iwapoly#=_X^L
for I=0 to L-1
  C=0
  for J=0 to I
    for K=0 to I-J
      C=(C+A2%(J)*A3%(K)*A5%(I-J-K))@B
    next K
  next J
  Iwapoly#=Iwapoly#+C*_X^I
next I
'
print Iwapoly#;" mod";Pr;"^";N-R+1
print time
erase A1%(),A2%(),A3%(),A4%(),A5%(),A6%(),
A7%():goto 50
'
```

```
1290---fnGenshi(P)--------------------------------
  |   ubapl96/GENSHI.UB の "fnGenshi(P)" を append
1410---return(Gen)--------------------------------
1420   ’
1430   fnAlpha(Pr,N)
1440     local I=0,G=fnGenshi(Pr),X=G,P1=Pr^(N+1)
1450     if Pr<4 then return(1)
1460     while I-1
1470       X=modpow(X,Pr,P1):I=modpow(X,Pr-1,P1)
1480     wend
1490   return(X)
1500   ’
1510   fnIsprm(Pr)
1520     local X
1530     if Pr=1 then X=0:jump
1540     if Pr>prm(12251) then X=2:jump
1550     if Pr\prmdiv(Pr)<>1 then X=0 else X=1
1560     **
1570   return(X)
```

IwapolyF.ub　入力値を走らせて計算する場合を考えて、ユーザー定義関数を用いて書き直したものである．配列の長さ [210-270] や [360] の a = Al などは p と n のみに依存するものであるが、その都度それらをユーザー定義関数の内部で計算している．よって p と n を固定して m を走らせて（または n と m を固定して p を走らせて）計算する場合には、そのような値をあらかじめ計算して具体的な値で書き換えて用いる方が効率的である．

```
 10   print "■虚二次体の円分 Z_p 拡大の岩澤多項式■"
 20   ’
 30   H=54600 ’H=99500
 40   ’
 50   print:input "素数=";Pr:Isp=fnIsprm(Pr)
 60     if Isp=0 then print "素数ではありません．"
        :goto 50
 70     if Isp=2 then print "数値が大き過ぎます．"
        :goto 50
 80   input "ルートの中身の絶対値=";M
 90     if moeb(M)=0 then print "平方因子があります．"
        :goto 80
100   print "近似する";Pr; input "冪の指数=";N
      :clr time
110   ’
120   Iwapoly#=fnIwapoly(Pr,M,N,H)
130     if member(Iwapoly#,1)=0 then print "λ>"
          ;Pr^N-1:print time
140       :print "λを確定できません．";
150       :print "近似する冪指数を増やしてやり直して
          ください．"
160       :goto 100
170   print member(Iwapoly#,1);" mod";Pr;"^"
      ;member(Iwapoly#,2)
180   print time:goto 50
190   ’
200   fnIwapoly(Pr,M,N,H)
210     dim A1%(Pr^N-1)
220     dim A2%(int((N+1)*((H-Pr^N)/(5*N+2)))-1)
230     dim A3%(int(N*((H-Pr^N)/(5*N+2)))-1)
240     dim A4%(int(N*((H-Pr^N)/(5*N+2)))-1)
250     dim A5%(int(((H-Pr^N)/(5*N+2)))-1)
260     dim A6%(int(N*((H-Pr^N)/(5*N+2)))-1)
270     dim A7%(int(N*((H-Pr^N)/(5*N+2)))-1)
280     local Qr,Q,D,G,P,P1,Al,S,I,C,S1,K,J,L,R,Z,
        B,X,V,Iwapoly#
290     ’
300     if Pr=2 then Qr=4
310       :if M@2=0 then M=M\2 endif
320       :else Qr=Pr
330     if M@4=3 then M=-M else M=-4*M
340     if M=-Qr then return(pack(1+0*_X,0))
350     Q=lcm(Qr,abs(M)):D=Q\Qr:G=1+Q ’:G=1+Qr
360     P=Pr^N:P1=P*Qr:Al=fnAlpha(Pr,N)
370-----------------------------------------
  |     Iwapoly.ub の [220-380] に同じ
530-----------------------------------------
540     if C@Pr<>0 then
        return(pack(1+0*_X,0))
550-----------------------------------------
  |     Iwapoly.ub の [410-510] に同じ
650-----------------------------------------
660     return(pack(0*_X,0))
670     ’
680     **
690     if L=1 then
700       :if kro(M,Pr)=1 then
          return(pack(_X,0)) endif
710-----------------------------------------
  |     Iwapoly.ub の [630-670] に同じ
750-----------------------------------------
760     if N=R then return(pack(_X^L,1))
770-----------------------------------------
  |     Iwapoly.ub の [700-1230] に同じ
1300----------------------------------------
1310    ’
1320  return(pack(Iwapoly#,N-R+1))
1330  ’
1340----------------------------------------
  |   Iwapoly.ub の [1250-1570] に同じ
1620----------------------------------------
```

Iwapoly2.ub　$p = 2$ の場合に特化したものである．あらかじめ木田の公式 [3] を用いて λ を確定しておくことができるので、λ に依存して定まる部分も最初から定めておくことができる．特に、最終的な近似の精度 E $= n - r + 1$ を入力値とすることができる．

```
 10   print "■虚二次体の円分 Z_2 拡大の岩澤多項式■"
 20   ’
 30   print:input "ルートの中身の絶対値=";M
 40     if moeb(M)=0 then print "平方因子があります。"
          :goto 30
 50   input "近似する 2 冪の指数=";E:clr time
 60   ’
 70   L=member(fnLambda(M),1)
```

```
     :R=member(fnLambda(M),2):jump
 80  'Iwapoly#=fnIwapoly2(M,E,L,R) '<---- for UDF
 90  print Iwapoly#;" mod 2^";E
100  print time:goto 30
110  '
120  ** 'fnIwapoly2(M,E,L,R) '<---- for UDF
130    dim A1%(2^(E+R-1)-1),A2%((E+1)*L),A3%(E*L)
140    dim A4%(E*L),A5%(L),A6%(E*L),A7%(E*L)
150    'local Q,D,G,P,S,I,C,K,J,Z,B,X,V,Iwapoly#
       '<---- for UDF
160    '
170    if L=0 then Iwapoly#=1+0*_X:jump
180    '
190    if M@2=0 then M=M\2
200    if M@4=3 then M=-M else M=-4*M
210    if L=1 then if kro(M,2)=1 then Iwapoly#=_X
       :jump
220    Q=lcm(4,abs(M)):D=Q\4:G=1+Q ':G=1+4
230    P=2^(E+R-1):Z=min(P-1,(E+1)*L-1):B=2^E
240    '
250    S=1
260    for I=0 to P-1
270      C=0
280      for J=1 to D-1
290          C=(C+J*kro(M,S+J*P*4))@B
300      next J
310      A1%(I)=C:S=(S*G)@(P*4)
320    next I
330    '
340    C=0
350    for I=0 to P-1
360      C=(C+A1%(I))@B
370    next I
380    A2%(0)=C
390    '
400    for K=1 to Z
410      C=0
420      for I=1 to P-K
430         C=(C+A1%(I)*combi(P-I,K))@B
440      next I
450      A2%(K)=C
460    next K
470    '
480    A3%(0)=1:X=E*L-1:V=modinv(A2%(L),B)
490----------------------------------------
 |    Iwapoly.ub の [810-860] に同じ
540----------------------------------------
550    C=(A3%(X)*V)@B:A3%(X)=C
560    '
570----------------------------------------
 |    Iwapoly.ub の [890-950] に同じ
630----------------------------------------
640    '
650    A5%(0)=1:A6%(0)=1
660    for J=1 to E-1
670----------------------------------------
 |    Iwapoly.ub の [990-1110] に同じ
790----------------------------------------
800    next J
810    '
820----------------------------------------
 |    Iwapoly.ub の [1140-1230] に同じ
910----------------------------------------
920    '
930    **
940  erase A1%(),A2%(),A3%(),A4%(),A5%(),A6%(),
       A7%() ' '<---- for UDF
950  goto 90 'return(Iwapoly#) '<---- for UDF
960  '
970  fnLambda(M)
980    local L=-1,D=M,P,V,A,R
990    if D@2=0 then D=M\2
1000   if D<4 then L=0:R=0:jump
1010   while D-1
1020     P=prmdiv(D):V=0:A=(P^2-1)\8
1030     while A@2-1
1040       inc V:A=A\2
1050     wend
1060     L=L+2^V:D=D\P
1070   wend
1080   R=1
1090   loop
1100     if L>2^R then inc R else jump
1110   endloop
1120   **
1130 return(pack(L,R))
```

§5. 計算例

(p,m,n)	$\kappa = 1+Q$	$\kappa = 1+q$
$(2,17,15)$	$T^3 + 11302\,T^2 + 14174\,T + 2658 \bmod 2^{14}$	$T^3 + 11350\,T^2 + 12830\,T + 14194 \bmod 2^{14}$
$(2,21,15)$	$T^2 + 28484\,T + 26058 \bmod 2^{15}$	$T^2 + 15604\,T + 26266 \bmod 2^{15}$
$(2,47,15)$	$T^3 + 16376\,T^2 + 1758\,T \bmod 2^{14}$	$X^3 + 13644\,T^2 + 9986\,T \bmod 2^{14}$
$(2,65,15)$	$T + 5828 \bmod 2^{15}$	$T + 29124 \bmod 2^{15}$
$(2,113,15)$	$T^3 + 1706\,T^2 + 11660\,T + 14540 \bmod 2^{14}$	$T^3 + 1290\,T^2 + 172\,T + 8972 \bmod 2^{14}$
$(2,119,15)$	$T^5+7168\,T^4+1770\,T^3+6106\,T^2+3694\,T \bmod 2^{13}$	$T^5+1354\,T^4+5156\,T^3+2474\,T^2+3918\,T \bmod 2^{13}$
$(2,565,15)$	$T^4+8984\,T^3+1284\,T^2+7164\,T+2446 \bmod 2^{14}$	$T^4+2920\,T^3+2516\,T^2+3988\,T+13990 \bmod 2^{14}$

$(2, 257, 13)$	$T^{63}+168\,T^{62}+6\,T^{61}+224\,T^{60}+184\,T^{59}+190\,T^{58}+194\,T^{57}+10\,T^{56}+168\,T^{55}+212\,T^{54}+102\,T^{53}+236\,T^{52}+24\,T^{51}+230\,T^{50}+124\,T^{49}+26\,T^{48}+200\,T^{47}+246\,T^{46}+160\,T^{45}+210\,T^{44}+66\,T^{43}+234\,T^{42}+126\,T^{41}+44\,T^{40}+252\,T^{39}+142\,T^{38}+168\,T^{37}+90\,T^{36}+230\,T^{35}+154\,T^{34}+118\,T^{33}+254\,T^{32}+204\,T^{31}+134\,T^{30}+178\,T^{29}+78\,T^{28}+74\,T^{27}+228\,T^{26}+130\,T^{25}+240\,T^{24}+24\,T^{23}+112\,T^{22}+82\,T^{21}+26\,T^{20}+16\,T^{19}+130\,T^{18}+70\,T^{17}+174\,T^{16}+74\,T^{15}+40\,T^{14}+12\,T^{13}+38\,T^{12}+90\,T^{11}+176\,T^{10}+114\,T^{9}+76\,T^{8}+108\,T^{7}+242\,T^{6}+68\,T^{5}+26\,T^{4}+186\,T^{3}+186\,T^{2}+180\,T+40 \bmod 2^8$	$T^{63}+40\,T^{62}+150\,T^{61}+224\,T^{60}+136\,T^{59}+174\,T^{58}+226\,T^{57}+90\,T^{56}+8\,T^{55}+68\,T^{54}+54\,T^{53}+124\,T^{52}+8\,T^{51}+118\,T^{50}+108\,T^{49}+202\,T^{48}+56\,T^{47}+54\,T^{46}+64\,T^{45}+50\,T^{44}+226\,T^{43}+58\,T^{42}+62\,T^{41}+204\,T^{40}+140\,T^{39}+78\,T^{38}+24\,T^{37}+106\,T^{36}+166\,T^{35}+186\,T^{34}+38\,T^{33}+158\,T^{32}+28\,T^{31}+150\,T^{30}+162\,T^{29}+30\,T^{28}+154\,T^{27}+36\,T^{26}+178\,T^{25}+80\,T^{24}+104\,T^{23}+224\,T^{22}+226\,T^{21}+74\,T^{20}+224\,T^{19}+194\,T^{18}+198\,T^{17}+222\,T^{16}+186\,T^{15}+72\,T^{14}+252\,T^{13}+150\,T^{12}+218\,T^{11}+18\,T^{9}+60\,T^{8}+76\,T^{7}+34\,T^{6}+100\,T^{5}+234\,T^{4}+186\,T^{3}+90\,T^{2}+116\,T+168 \bmod 2^8$
$(3, 239, 8)$	$T^6+1284\,T^5+1404\,T^4+672\,T^3+1764\,T^2+1128\,T \bmod 3^7$	$T^6+207\,T^5+1740\,T^4+804\,T^3+705\,T^2+1815\,T \bmod 3^7$
$(5, 111111, 4)$	$T^4+325\,T^3+130\,T^2+10\,T \bmod 5^4$	$T^4+425\,T^3+605\,T^2+460\,T \bmod 5^4$
$(7, 5017, 4)$	$T^3+1834\,T^2+1701\,T \bmod 7^4$	$T^3+2303\,T^2+2338\,T \bmod 7^4$
$(11, 1414, 3)$	$T^4+539T^3+44T^2+594T \bmod 11^3$	$T^4+1111T^3+550T^2+649T \bmod 11^3$
$(13, 3, 4)$	$T^2+25740\,T \bmod 13^4$	$T^2+24973\,T \bmod 13^4$

参考文献

[1] 田谷久雄, 福田 隆, “岩澤不変量の計算”, 日本応用数理学会論文誌 **12** (2002), no. 4, 293–306.

[2] H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields II*, Inter. J. Math. **7** (1996), no. 6, 721–744.

[3] Y. Kida, *On cyclotomic $\mathbf{Z}_2$-extensions of imaginary quadratic fields*, Tohoku Math. J. (2) **31** (1979), no. 1, 91–96.

[4] M. Koike, *On the isomorphism classes of Iwasawa modules associated to imaginary quadratic fields with $\lambda = 2$*, J. Math. Sci. Univ. Tokyo **6** (1999), 371–396.

[5] L. C. Washington, *Introduction to Cyclotomic Fields* (2nd. edition), Graduate Texts in Math. **83**, Springer (1997).

平成 19 年 3 月 28 日版