Notes on computing Iwasawa polynomials by PARI/GP

Yasushi Mizusawa

By referring [1] [2] and [5], we compute Iwasawa polynomials for the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields.

Preliminaries. Let p be a prime number and $k = \mathbb{Q}(\sqrt{-m})$ an imaginary quadratic field with the discriminant d. If $p = 2$ and $d \equiv 0 \pmod 8$, we replace m by $m/2$. Let χ be the odd Dirichlet character associated to k. Put $q = p$ if $p \neq 2$, and $q = 4$ if $p = 2$. Put a topological generator $g = 1 + q$ of $1 + q\mathbb{Z}_p$ as in [3] (or $g = 1 + \mathrm{lcm}(q, |d|)$ as in [1] [5]).

Let k_∞/k be the cyclotomic $\mathbb{Z}_p$-extension. Put $\gamma_n \in \Gamma_n = \mathrm{Gal}(k(\zeta_{qp^n})/k(\zeta_q))$ satisfying $\zeta_{qp^n}^{\gamma_n} = \zeta_{qp^n}^{g}$. Then $\gamma = \lim \gamma_n$ is a topological generator of $\Gamma = \varprojlim \Gamma_n \simeq \mathrm{Gal}(k_\infty/k)$. Let X be the Galois group of the maximal unramified abelian pro-p-extension over k_∞. The Iwasawa polynomial $P(x) = \det(x + 1 - \gamma | X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \in \mathbb{Z}_p[x]$ is defined as a monic distinguished polynomial. Since $P(x) = 1$ if $d = -q$, we assume that $d \neq -q$.

Coefficients of Stickelberger elements. Put $d_0 = \mathrm{lcm}(q, |d|)/q$ and $\theta = \omega\chi^{-1}$ where ω is the Teichmüller character. The χ-part of the Stickelberger element is written as

$$\tfrac{1}{2}\xi_n(\theta) = -\tfrac{1}{d_0}\sum_{i=0}^{p^n-1} c_i\gamma_n^{-i} \in \mathbb{Z}_p[\Gamma_n], \ \ c_i = \sum_{k=0}^{\frac{\varphi(q)-2}{2}} \sum_{j=1}^{d_0-1} j\chi(s_n(g^i\alpha^k) + jqp^n)$$

where α is a primitive $\varphi(q)$th root of 1 in $\mathbb{Z}_p$, and $s_n(z) \equiv z \pmod{qp^n}$, $0 \leq s_n(z) < qp^n$ (cf. [5] Proposition 7.9 (b)). We compute $\texttt{F[}i+1\texttt{]} = c_i \bmod p^n$.

Put $f_n(x) = c_0 + \sum_{i=1}^{p^n-1} c_i(1+x)^{p^n-i}$ and $f(x) = \lim f_n(x) \in \Lambda = \mathbb{Z}_p[[x]] = \varprojlim \Lambda/((1+x)^{p^n} - 1)$. Since $\Lambda/((1+x)^{p^n} - 1) \simeq \mathbb{Z}_p[\Gamma_n] : -\frac{1}{d_0}f_n(x) \leftrightarrow \frac{1}{2}\xi_n(\theta)$, the p-adic L-function $L_p(s, \theta) = -\frac{2}{d_0}f(g^s - 1)$, and $f(x)\Lambda = P(x)\Lambda$.

Iwasawa power series and lambda invariants. Let a_ℓ be the coefficients of $f_n(x) = \sum_{\ell=0}^{p^n-1} a_\ell x^\ell$. Then $a_0 = \sum_{i=0}^{p^n-1} c_i$ and $a_\ell = \sum_{i=1}^{p^n-\ell} c_i\binom{p^n-i}{\ell}$ for $\ell \geq 1$. Put $\lambda = \deg P(x)$. If $f_n(x) \equiv 0 \pmod p$, then $\lambda \geq p^n$. Assume that $f_n(x) \not\equiv 0 \pmod p$. Then $\lambda = \min\{\ell \,|\, a_\ell \not\equiv 0 \pmod p\} = \texttt{L}$. If $\lambda = 1$ and $\chi(p) = 1$, then $P(x) = x$. Put $r = \min\{r \geq 1 \,|\, p^r \geq \lambda\}$ and $g_n(x) = \sum_{\ell=0}^{\min\{p^n-1, (n-r+1)\lambda-1\}} a_\ell x^\ell$. We compute $\texttt{g} = g_n(x) \bmod p^{n-r+1}$.

Distinguished polynomials. Let $\tau : \Lambda \to \Lambda : \sum_{i=0}^\infty b_i x^i \mapsto \sum_{i=0}^\infty b_{i+\lambda}x^i$ be the shift operator. Put $q_n(x) = \tau(f_n(x)) \in \Lambda^\times$ and $q_n'(x) = \tau(g_n(x)) = \texttt{v}^{-1} \in \Lambda^\times$. Then $f_n(x) = r_n(x) + x^\lambda q_n(x)$ and $g_n(x) = r_n(x) + x^\lambda q_n'(x)$ with some $\texttt{F} = r_n \equiv 0 \pmod p$. Let $P_n(x)$ be the monic distinguished polynomial satisfying $f_n(x) = u_n(x)P_n(x)$ with $u_n(x) \in \Lambda^\times$. We compute

$$\begin{aligned} P_n(x) &\equiv r_n(x)u_n(x)^{-1} = \tfrac{r_n}{q_n}\sum_{j=0}^{\infty}(-\tau \circ \tfrac{r_n}{q_n})^j(1) \mod x^\lambda \\ &\equiv \texttt{F}\cdot\texttt{v}\cdot\texttt{u} = \tfrac{r_n}{q_n'}\sum_{j=0}^{n-r-1}(-\tau \circ \tfrac{r_n}{q_n'})^j(1) \mod (x^\lambda, p^{n-r+1}) \end{aligned}$$

(cf. [5] Proof of Proposition 7.2). Note that

$\mathtt{t} = (-\tau \circ \frac{r_n}{q'_n})^j(1) + O(x^{(n-r-j)\lambda}) = (-\tau \circ \frac{r_n}{q'_n})\big((-\tau \circ \frac{r_n}{q'_n})^{j-1}(1) + O(x^{(n-r+1-j)\lambda})\big)$

for $1 \le j \le n-r-1$. Since $f(x) \equiv f_n(x) \pmod{(1+x)^{p^n}-1}$, we have $P(x) \equiv P_n(x) \pmod{p^{n-r+1}}$ (cf. [2] Lemma 5 and the proof). Then we obtain $P(x) \bmod p^{n-r+1}$.

Programing. `Iwapoly.gp` computes $P(x) \bmod p^{n-r+1}$ on PARI/GP calculator [4]. `Iwapoly(`p`,`m`,`n`)` returns `[`$P(x) \bmod p^{n-r+1}$`,`$n-r+1$`]` for $g = 1+q$ if $\lambda < p^n$, and `[0,0]` if $\lambda \ge p^n$, or `[`$P(x)$`,0]` when $P(x) = 1$, x. `Iwapoly(`p`,`m`,`n`,1)` returns the results for $g = 1 + \mathrm{lcm}(q, |d|)$. `Iwapoly(`$p$`,`$m$`,`$n$`,2)` returns λ if $\lambda < p^n$, and `-1` if $\lambda \ge p^n$.

Examples.

```
? \r ./Iwapoly.gp
? Iwapoly(3,239,8)
%1 = [x^6 + 207*x^5 + 1740*x^4 + 804*x^3 + 705*x^2 + 1815*x, 7]
? Iwapoly(3,239,8,1)
%2 = [x^6 + 1284*x^5 + 1404*x^4 + 672*x^3 + 1764*x^2 + 1128*x, 7]
? Iwapoly(3,239,8,2)
%3 = 6
? Iwapoly(2,257,5)
%4 = [0, 0]
? Iwapoly(2,257,5,2)
%5 = -1
? Iwapoly(2,257,6)
%6 = [x^63, 1]
? Iwapoly(2,257,13)
%7 = [x^63 + 40*x^62 + 150*x^61 + 224*x^60 + 136*x^59 + 174*x^58 + 226
*x^57 + 90*x^56 + 8*x^55 + 68*x^54 + 54*x^53 + 124*x^52 + 8*x^51 + 118
*x^50 + 108*x^49 +202*x^48 + 56*x^47 + 54*x^46 + 64*x^45 + 50*x^44 + 2
26*x^43 + 58*x^42 + 62*x^41+ 204*x^40 + 140*x^39 + 78*x^38 + 24*x^37 +
 106*x^36 + 166*x^35 + 186*x^34 + 38*x^33 + 158*x^32 + 28*x^31 + 150*x
^30 + 162*x^29 + 30*x^28 + 154*x^27 + 36*x^26 + 178*x^25 + 80*x^24 + 1
04*x^23 + 224*x^22 + 226*x^21 + 74*x^20 + 224*x^19 + 194*x^18 + 198*x^
17 + 222*x^16 + 186*x^15 + 72*x^14 + 252*x^13 + 150*x^12 + 218*x^11 +
18*x^9 + 60*x^8 + 76*x^7 + 34*x^6 + 100*x^5 + 234*x^4 + 186*x^3 + 90*x
^2 + 116*x + 168, 8]
```

References.

[1] T. Fukuda and H. Taya, *Computation of Iwasawa invariants* (Japanese), Trans. JSIAM, **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] 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.

[4] The Pari Group, *PARI/GP*, Bordeaux, 2008. `http://pari.math.u-bordeaux.fr/`

[5] L. C. Washington, *Introduction to cyclotomic fields (Second edition)*, Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.