Cyclic extensions of prime degree and their p-adic regulators

Tommy Hofmann
Technische Universität Kaiserslautern

Yinan Zhang
Australian National University

ANTS XIII, 19 July 2018

The regulator $R(K)$ of a number field K is an important invariant, providing information on its unit group structure.

Its p-adic analogue $R_p(K)$ was introduced by Leopoldt in his investigation of p-adic L-functions.

Computation of $R_p(K)$ remains difficult, and previous research has been predominantly focused on numerical verification of Leopoldt's conjecture.

In 2016, the authors were able to conjecture and provide heuristics on the distribution of $v_p(R_p(K)))$ for cyclic cubic fields K.

This was based on observations of computational data of $v_p(R_p(K))$ of almost 16 million fields.

We extend this result to a conjecture about all cyclic extensions of odd prime degree.

We use a definition of $R_p(K)$ introduced by Iwasawa, which differs slightly from the usual definition.

Let K be a totally real number field of degree ℓ, $\{\epsilon_i\}$ a p-maximal set of independent units, and $\{\tau_j\}$ the embeddings of K into $\mathbb{C}_p$. Then the p-adic regulator $R_p(K)$ is given by

$$R_p(K) = \frac{1}{\ell}\det\begin{pmatrix} 1 & \cdots & 1 \\ \log_p(\tau_1(\epsilon_1)) & \cdots & \log_p(\tau_\ell(\epsilon_1)) \\ \vdots & \ddots & \vdots \\ \log_p(\tau_1(\epsilon_{\ell-1})) & \cdots & \log_p(\tau_\ell(\epsilon_{\ell-1})) \end{pmatrix}$$

This is more costly to compute but maintains the structure of the matrix.

Basic overview:

1. Model $R_p(K)$ with the matrix M_ℓ
2. Factorise $\det(M_\ell)$ as $\prod f_i$
3. Count solutions to the equation $\sum v_p(f_i) = v$ for some v

Based on observation of $v_p(R_p(K))$ computed for quintic fields up to $d(K) = 5 \times 10^{31}$ and septic fields up to $d(K) = 10^{42}$.

We note the following about $R_p(K)$:

1. There is a lower bound on $v_p(R_p(K))$: for a prime $p \neq \ell$ we have

$$v_p(R_p(K)) \geq \begin{cases} \frac{\ell-1}{2}, & \text{if } p \text{ is ramified in } K, \\ \ell - 1, & \text{if } p \text{ is unramified in } K. \end{cases}$$

2. The matrix whose determinant gives $R_p(K)$ has a fixed structure:

$$M_\ell = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ X_1 & X_2 & X_3 & \cdots & X_{\ell-1} & X_0 \\ X_2 & X_3 & X_4 & \cdots & X_0 & X_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ X_{\ell-1} & X_0 & X_1 & \cdots & X_{\ell-3} & X_{\ell-2} \end{pmatrix}$$

   with $X_0 = -\sum_{i=1}^{\ell-1} X_i$
   If $p \neq \ell$, then there exist $a \in \bar{\mathbb{Q}}_p^{\ell-1}$ such that $v_p(R_p(K)) = v_p(M_\ell(a))$.

These suggest that there may be a connection between the distribution of the valuations of the p-adic regulators in cyclic ℓ-extensions and that of $\det(M_\ell)$.

Let $P_{\ell,p} \colon \mathbb{Z}_p^{\ell-1} \to \mathbb{R}, a \mapsto v_p(\det(M_\ell(a)))$ be a random variable, and $\mathcal{K}_p^{\mathrm{T}}(D)$ be the set of fields with $d(K) < D$ and $\mathrm{T} \in \{\mathrm{un}, \mathrm{ram}\}$. For primes $2 < \ell$ and $p \neq \ell$ we conjecture that

$$\lim_{D\to\infty} \frac{\#\{K \in \mathcal{K}_p^{\mathrm{T}}(D) \mid v_p(R_p(K)) = i + v_{\mathrm{T}}\}}{\#\mathcal{K}_p^{\mathrm{T}}(D)} = \mathrm{pr}(P_{\ell,p} = i),$$

where $v_{\mathrm{un}} = \ell - 1$ and $v_{\mathrm{ram}} = (\ell - 1)/2$.

It turns out the factorisation of $\det(M_\ell)$ has some unique properties, which is useful for finding $P_{\ell,p}$:

Let ζ be a primitive ℓ-th root of unity, σ a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $f_0 = X_0 + \zeta X_1 + \cdots + \zeta^{\ell-1} X_{\ell-1}$ and $f_i = \sigma^i(f_0)$ for $i \in \{1, \ldots, \ell-2\}$. Then

1. $$\det(M_\ell) = (-1)^{(\ell-1)/2} \cdot \prod_{i=0}^{\ell-2} \sigma^i(f_0).$$

2. The matrix $M \in \mathbb{Q}(\zeta)^{(\ell-1)\times(\ell-1)}$ defined by
$$\begin{pmatrix} f_0 \\ \vdots \\ f_{\ell-2} \end{pmatrix} = M \begin{pmatrix} X_1 \\ \vdots \\ X_{\ell-1} \end{pmatrix}$$
satisfies $\det(M)^2 = (-1)^{(\ell-1)/2} \cdot \ell^{\ell-2}$.

Since $v_p(\det(M_\ell)) = \sum v_p(f_i)$, we are interested in counting solutions to the equations $\{v_p(f_i(a)) = v_i\}$ for some fixed $\sum v_i$. While this seems rather difficult in general, we can make use of the fact that $f_i = \sigma^i(f_0)$.

In $\mathbb{Z}_p$ with $\mathrm{ord}_\ell(p) = m$ and $\ell - 1 = mn$, if $v_p(f_1) = v_1$, then there are $m-1$ other f_i also with valuation v_1. The same applies for $f_2, \dots, f_n$.

The probability for a particular set of $\{v_1, \dots, v_n\}$ is given by

$$\frac{1}{p^{m(v_1 + \dots v_n)}} \left(1 - \frac{1}{p^m}\right)^n .$$

For a fixed i there are $\binom{i+n-1}{n-1}$ choices of $v_1, \dots, v_n$ with $v_1 + \cdots + v_n = i$, so for $i \in \mathbb{Z}_{\geq 0}$ we have:

$$\operatorname{pr}(P_{\ell,p} = mi) = \binom{i+n-1}{n-1} \frac{1}{p^{mi}} \left(1 - \frac{1}{p^m}\right)^n .$$

Conjecture

Let $p \neq 2, \ell$ *be a prime,* $\mathrm{ord}_\ell(p) = m$, $\ell - 1 = mn$ *and* $\mathrm{T} \in \{\mathrm{un}, \mathrm{ram}\}$. *Then* $v_p(R_p(K)) \in m\mathbb{Z} + v_{\mathrm{T}}$ *for all* $K \in \mathcal{K}_p^{\mathrm{T}}$ *and for* $i \geq 0$ *we have*

$$\lim_{D \to \infty} \frac{\#\{K \in \mathcal{K}_p^{\mathrm{T}}(D) \mid v_p(R_p(K)) = mi + v_{\mathrm{T}}\}}{\#\mathcal{K}_p^{\mathrm{T}}(D)} = \binom{i+n-1}{n-1} \frac{1}{p^{mi}} \left(1 - \frac{1}{p^m}\right)^n,$$

where $v_{\mathrm{un}} = \ell - 1$ *and* $v_{\mathrm{ram}} = (\ell - 1)/2$.

$p = 3$, $\ell = 5$

$v_p(R_p(K))$	Obs	Conj
4	.98766	.98765
8	.01218	.01219
12	.142E-3	.150E-3
16	.181E-5	.185E-5

$p = 29$, $\ell = 7$, p unramified

$v_p(R_p(K))$	Obs	Conj
6	.81036	.81014
7	.16753	.16761
8	.01990	.02022
9	.00204	.00186
10	.135E-3	.144E-3
11	.109E-4	.995E-5

Questions/comments

$p = 3$, $\ell = 5$

$v_p(R_p(K))$	Obs	Conj
4	.98766	.98765
8	.01218	.01219
12	.142E-3	.150E-3
16	.181E-5	.185E-5

$p = 29$, $\ell = 7$, p unramified

$v_p(R_p(K))$	Obs	Conj
6	.81036	.81014
7	.16753	.16761
8	.01990	.02022
9	.00204	.00186
10	.135E-3	.144E-3
11	.109E-4	.995E-5

Questions/comments