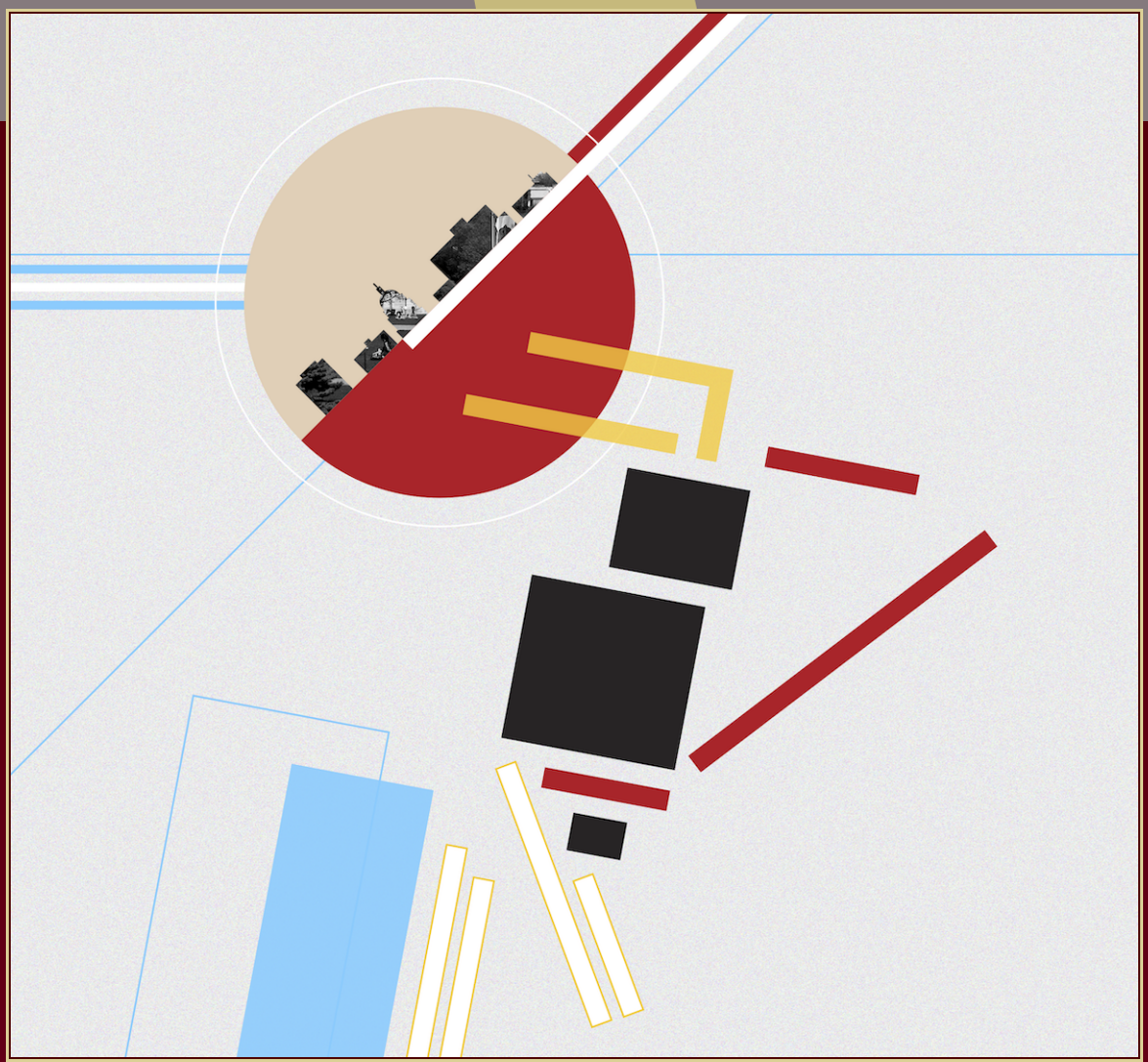
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth Algorithmic Number Theory Symposium

Cyclic extensions of prime degree and their p-adic regulators

Tommy Hofmann and Yinan Zhang



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.311

Cyclic extensions of prime degree and their p-adic regulators

Tommy Hofmann and Yinan Zhang

We present a conjecture on the distribution of the valuations of p-adic regulators of cyclic extensions of $\mathbb{Q}$ of odd prime degree. This is based on the observation of computational data of p-adic regulators of the 5 521 222 cyclic quintic and 329 708 cyclic septic extensions of $\mathbb{Q}$ for $2 < p < 100$ with discriminant up to 5×10^{31} and 10^{42} respectively, and noting that the observation matches the model that the entries in the regulator matrix are random elements with respect to the obvious restrictions.

1. Introduction

The class group and regulator of a number field are important invariants of the field, providing information about the multiplicative and unit group structure of the number field. These two invariants are intimately linked by the class number formula, and following the improvements to the class group algorithm by Buchmann [Buc90], can be computed together in the same algorithm. Despite various improvements to the algorithm, some in recent times, an efficient algorithm to compute the class group and regulator of arbitrary number fields remains elusive and a significant focus in computational number theory.

In [Leo62], Leopoldt introduced the p-adic regulator $R_p(K)$ of a number field K in his study of p-adic L-functions, and his conjecture states that it is nonvanishing. While its classical counterpart, the regulator of a number field, is well defined for all finite extensions of $\mathbb{Q}$, the p-adic regulator is only unambiguous for totally real or CM number fields, and very little is known about the actual value of p-adic regulators.

Previous efforts on computing the p-adic regulators of number fields were predominantly focused on numerical verification of Leopoldt's conjecture, and significant practical difficulties with p-adic computations restricted efforts to compute its exact value. Indeed, this was noted in the PhD thesis of Panayi [Pan95], who was one of the first to compute $R_p(K)$ explicitly.

Research on the valuation of p-adic regulators has also been limited. One investigator was Schirokauer [Sch93, Proposition 3.8], who provided heuristic arguments regarding the p-divisibility of the units, while Miki [Mik87] attempted to provide an upper bound on $v_p(R_p(K))$, and Hakkarainen provided a simple

MSC2010: primary 11Y40; secondary 11K41, 11R20, 11R27.
Keywords: p-adic regulator, distribution of p-adic regulators.

lower bound in his PhD thesis [Hak07], along with limited heuristics using the valuation of the class number and the class number formula.

A recent development by Fieker and Zhang [FZ16] in a p-adic class number algorithm for totally real abelian fields allowed relatively efficient computation of the p-adic regulator of these fields. This algorithm was used in [HZ16] to compute the p-adic regulator of the almost 16 million cyclic cubic extensions of $\mathbb{Q}$ with discriminant less than 10^{16}, and from this experimental data, the authors were able to conjecture and provide heuristics on the distribution of the values of $v_p(R_p(K))$.

We continue this previous work by computing the p-adic regulator for a large number of cyclic quintic and septic extensions for $2 < p < 100$. Based on this new experimental data, we extend the previous heuristics to a conjecture for all cyclic extensions of $\mathbb{Q}$ with prime degree as follows.

Fix an odd prime ℓ and let $\mathcal{K}$ be the set of all cyclic extensions of $\mathbb{Q}$ with degree ℓ inside a fixed algebraic closure of $\mathbb{Q}$. Note that such extensions are necessarily totally real. For a prime p let $\mathcal{K}_p^{\mathrm{un}}$ and $\mathcal{K}_p^{\mathrm{ram}}$ denote the set of all fields in $\mathcal{K}$ which are unramified and ramified at p, respectively. Note that $\mathcal{K}_p^{\mathrm{ram}} = \varnothing$ and $\mathcal{K} = \mathcal{K}_p^{\mathrm{un}}$ in the case $p \not\equiv 1 \bmod \ell$ and $p \neq \ell$. For $D > 0$ we set $\mathcal{K}(D) = \{K \in \mathcal{K} \mid |d(K)| \leq D\}$, where $d(K)$ is the discriminant of K, $\mathcal{K}_p^{\mathrm{un}}(D) = \mathcal{K}_p^{\mathrm{un}} \cap \mathcal{K}(D)$, and $\mathcal{K}_p^{\mathrm{ram}}(D) = \mathcal{K}_p^{\mathrm{ram}} \cap \mathcal{K}(D)$. Let $\mathrm{ord}_\ell(p)$ be the multiplicative order of p modulo ℓ, and v_p be the p-adic valuation. Based on heuristics and numerical data, we claim the following conjecture:

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

This paper is organised as follows: some basic definitions are recalled in Section 2. We then conjecture a link between the distributions of $v_p(R_p(K))$ and $v_p(\det(M))$, where M is an arbitrary matrix in a particular form, in Section 3 (see Conjecture 1′). So far this is similar to [HZ16, §1–3], but we diverge in Section 4 to obtain some results about solutions of linear equations in p-adic rings. Applying this to the factorisation of $\det(M)$, we obtain Conjecture 1 in Section 5. Finally, in Section 6, we provide the numerical data from our computations.

2. Definition and notation

Let K be a number field of degree ℓ and p a prime. By $\mathbb{C}_p$ we denote the completion of an algebraic closure of $\mathbb{Q}_p$. By fixing an embedding from $\mathbb{C}_p$ into $\mathbb{C}$, any embedding of K into $\mathbb{C}_p$ can be considered as either real or complex, depending on the image of K in the composite embedding into $\mathbb{C}$. Note that for totally real or CM fields, whether an embedding from K to $\mathbb{C}_p$ is real or complex is independent of the choice of embedding from $\mathbb{C}_p$ to $\mathbb{C}$, but this is not well defined in general.

Let (r_1, r_2) be the signature of K and $r = r_1 + r_2 - 1$ the unit rank. Denote by $\tau_1, \dots, \tau_{r_1}$ the real and by $\tau_{r_1+1}, \overline{\tau}_{r_1+1}, \dots, \tau_{r_1+r_2}, \overline{\tau}_{r_1+r_2}$ the complex embeddings of K into $\mathbb{C}_p$. Let $\epsilon_1, \dots, \epsilon_r$ be a set of independent units of K such that, modulo torsion, the index of $\langle \epsilon_1, \dots, \epsilon_r \rangle$ in $\mathcal{O}_K^\times$ is coprime to p. Consider the submatrix formed by deleting one column of the matrix,

$$(\delta_i \log_p(\tau_j(\epsilon_i)))_{i,j} \in \mathbb{C}_p^{r \times (r+1)},$$

where $\delta_i = 1$ for $1 \le i \le r_1$ and $\delta_i = 2$ if $r_1 + 1 \le i \le r_1 + r_2$, and $\log_p \colon \mathbb{C}_p^\times \to \mathbb{C}_p$ is the p-adic Iwasawa logarithm (see [Iwa72]). As each row sums to zero, the determinant of such a submatrix is independent of the column deleted, up to a sign. The value of this determinant is also independent of the choice of the units $\epsilon_1, \dots, \epsilon_r$, up to a p-adic unit, and is known as the p-adic regulator $R_p(K)$ of the number field K.

There is an alternate definition introduced by Iwasawa [Iwa72] and subsequently implemented in the algorithm by Fieker and Zhang [FZ16]. Instead of deleting a column in the matrix, one can add a row of 1's to it, and divide the determinant by ℓ. Again, due to each row summing to zero, the value of the determinant is unaffected. In [HZ16] it was noted that while this does have the disadvantage of calculating the determinant of a matrix one dimension higher than necessary, it is outweighed by leaving the structure of the original matrix intact.

If G is a compact group, we denote by μ_G the unique left Haar measure with $\mu_G(G) = 1$. When no confusion can arise, we just write μ instead of μ_G. For two integers $n \in \mathbb{Z}_{\ge 1}$, $k \in \mathbb{Z}$ we denote by $k \bmod n$ the unique representative of $k + n\mathbb{Z}$ in the set $\{0, \dots, n-1\}$.

3. p-adic regulators and regulator matrices

Let ℓ be a prime and denote by K a cyclic extension of $\mathbb{Q}$ of degree ℓ. We start by collecting basic facts about p-adic regulators, beginning with lower bounds, a special case of which was observed in [HZ16, Lemma 3.1].

Proposition 2. *For a prime $p \neq \ell$ we have*

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

Proof. By the theorem of Ax and Brumer (see [Bru67]) we know that Leopoldt's conjecture holds for abelian extensions of $\mathbb{Q}$ and in particular $R_p(K) \neq 0$. For a nonzero prime ideal $\mathfrak{p} \mid p\mathcal{O}_K$ denote by $\nu_\mathfrak{p}$ the number of p-power roots of unity in the completion of K at $\mathfrak{p}$. By [Coa77, Appendix, Lemma 5] we know that

$$\frac{\ell \cdot p \cdot R_p(K)}{\Delta_K^{1/2}} \prod_{\mathfrak{p} \mid p\mathcal{O}_K} (\nu_\mathfrak{p} \cdot N(\mathfrak{p}))^{-1}$$

has nonnegative p-adic valuation. Using that $v_p(\nu_\mathfrak{p}) \ge 0$ we obtain

$$v_p(R_p(K)) \ge \frac{v_p(\Delta_K)}{2} - v_p(\ell) - v_p(p) + \frac{\ell}{e(p)},$$

where $e(p)$ is the ramification index of p in K. Since $K/\mathbb{Q}$ is cyclic of prime degree ℓ, we know that if p is ramified, then $e(p) = \ell$. Moreover, as p is tamely ramified, we have $v_p(\Delta_K) = \ell - 1$ ([Ser79, Chapter III, §7, Proposition 13]) □

Definition 3. Let $R = \mathbb{Z}[X_1, \dots, X_{\ell-1}]$ and set $X_0 = -\sum_{i=1}^{\ell-1} X_i$. We define $M_\ell = (m_{ij})_{1\le i,j\le \ell} \in R^{\ell\times\ell}$ by

$$m_{ij} = \begin{cases} 1 & \text{if } i = 1, \\ X_{(i+j-2) \bmod \ell} & \text{otherwise.} \end{cases}$$

We call M_ℓ the *generic regulator matrix of degree* ℓ. Using the Haar measure μ on $\mathbb{Z}_p^{\ell-1}$ we define the random variable

$$P_{\ell,p} \colon \mathbb{Z}_p^{\ell-1} \longrightarrow \mathbb{R}_{\ge 0},\ (a_1, \dots, a_{\ell-1}) \longmapsto v_p(\det(M_\ell(a_1, \dots, a_{\ell-1}))),$$

where $M_\ell(a_1, \dots, a_{\ell-1})$ is obtained by setting $X_i = a_i$ in the matrix M_ℓ, so that for $i \in \mathbb{Z}_{\ge 0}$ we have $\operatorname{pr}(P_{\ell,p} = i) = \mu(\{a \in \mathbb{Z}_p^{\ell-1} \mid v_p(\det(M_\ell(a))) = i\})$.

The name of the generic regulator matrix is justified by the following result, which was also observed in [HZ16, Proposition 3.2] for $\ell = 3$.

Theorem 4. *Let $p \ne \ell$ be a prime. Then there exists $a \in \overline{\mathbb{Q}}_p^{\ell-1}$ such that $v_p(R_p(K)) = v_p(M_\ell(a))$. Moreover, if p is split in K, the vector a can be chosen in $\mathbb{Z}_p^{\ell-1}$.*

Proof. Let σ be a generator of $\operatorname{Gal}(K/\mathbb{Q})$ and $\tau \colon K \to \overline{\mathbb{Q}}_p$ a p-adic embedding. For $i \in \{1, \dots, \ell\}$ we define $\tau_i = \tau \circ \sigma^{i-1}$ and note that $\tau_1, \dots, \tau_\ell$ are the distinct p-adic embeddings of K. Due to [Mar96] there exists a p-Minkowski unit $\epsilon \in \mathcal{O}_K^\times$; that is, modulo torsion the subgroup $\langle \epsilon, \sigma(\epsilon), \dots, \sigma^{\ell-2}(\epsilon)\rangle$ of $\mathcal{O}_K^\times$ has index prime to p. Thus $v_p(R_p(K)) = v_p(\det((m_{ij})_{1\le i,j\le\ell}))$, where $m_{1j} = 1$ for $j \in \{1, \dots, \ell\}$ and $m_{ij} = \log_p(\tau_j(\sigma^{i-2}(\epsilon)))$ for $i \in \{2, \dots, \ell\},\ j \in \{1, \dots, \ell\}$. Now $\tau_j(\sigma^{i-2}) = \sigma^{(i+j-2) \bmod \ell}$ and the claim follows by setting $a_i = \log_p(\sigma^{i-1}(\epsilon))$ for $i = 1, \dots, \ell - 1$.

For the final statement first note that if p splits in K, then $\mathbb{Q}_p$ is a p-adic splitting field of K, that is, $\tau_i(\alpha) \in \mathbb{Q}_p$ for all $\alpha \in K$ and $i \in \{1, \dots, \ell\}$, and therefore $\tau_i(\epsilon) \in \mathbb{Z}_p$. □

Theorem 4 suggests that there could be a connection between the distribution of valuations of p-adic regulators and valuations of determinants of matrices of the form $M_\ell(a)$, where $a \in \overline{\mathbb{Q}}_p^{\ell-1}$ or $a \in \mathbb{Z}_p^{\ell-1}$ in the case p is split. Based on numerical observations for the quintic and septic fields, similar to [HZ16, Conjecture 6], we conjecture that the distribution of the valuations of the p-adic regulators in cyclic ℓ-extensions matches that of the corresponding random variable $P_{\ell,p} \colon \mathbb{Z}_p^{\ell-1} \to \mathbb{R}, a \mapsto v_p(\det(M_\ell(a)))$ associated to the generic regulator matrix of degree ℓ. Although Theorem 4 supports this only in the case p splits, numerical evidence suggests that it holds for all primes independent of the decomposition type. The lower bound of the regulator in the conjecture comes from Proposition 2.

Conjecture 1′. *For primes $2 < \ell,\ p \ne \ell$ and $\mathrm{T} \in \{\mathrm{un}, \mathrm{ram}\}$ the following holds*:

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

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

This is in agreement with the authors' previous work, since for the cubic case $\ell = 3$, Conjecture 1′ is equivalent to [HZ16, Conjecture 6]. Note that in the following it is shown that the value $\mathrm{pr}(P_{\ell,p}) = i$ on the right-hand side of Conjecture 1′ can be computed explicitly (see Theorem 9), making it possible to gather numerical evidence for Conjecture 1′ by only investigating statistics of valuations of p-adic regulators of cyclic number fields (see Section 6).

While it may be possible to extend [HZ16, Lemmas 4.8 and 4.9] to cover $\mathrm{pr}(P_{\ell,p} = i)$ when $\mathrm{ord}_\ell(p) = 1$ and $\mathrm{ord}_\ell(p) = \ell - 1$, respectively, this would be extremely tedious due to the increasing complexity of $\det(M_\ell(a))$ as ℓ grows, and it remains unclear whether such an approach could be adapted for arbitrary values of ℓ. Furthermore, this leaves the case of $\mathrm{ord}_\ell(p) \neq 1, \ell - 1$ unresolved, which only occurs when $\ell \geq 5$. For these reasons we need a different approach, and we start by obtaining some results about solutions of linear equations in p-adic rings.

4. Solutions of linear equations

Let ℓ be a prime and $M_\ell \in \mathbb{Z}[X_1, \ldots, X_{\ell-1}]$ the generic regular matrix of degree ℓ. To investigate the associated random variable $P_{\ell,p}$, where p is a prime, we will determine properties of the image of $\mathbb{Z}_p^{\ell-1}$ under the polynomial $\det(M_\ell) \in \mathbb{Z}[X_1, \ldots, X_{\ell-1}]$ using the following general setup.

Let $R \subseteq S$ be an extension of p-adic rings, that is, valuation rings of p-adic fields, such that the residue fields have cardinalities p and q, respectively. We consider a system of k linear forms $f_1, \ldots, f_k \in S[X_1, \ldots, X_k]$ with k indeterminates. By $M \in S^{k\times k}$ we denote the unique matrix such that

$$\begin{pmatrix} f_1(a_1, \ldots, a_k) \\ f_2(a_1, \ldots, a_k) \\ \vdots \\ f_k(a_1, \ldots, a_k) \end{pmatrix} = M \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{pmatrix}.$$

For the remainder of this section we assume that $\det(M) \in S^\times$.

Lemma 5. *For $v_1, \ldots, v_k \in \mathbb{Z}_{\geq 0}$ we have*

$$\mu(\{a \in S^k \mid v_p(f_i(a)) = v_i,\ i = 1, \ldots, k\}) = q^{-s}(1 - q^{-1})^k,$$

where $s = v_1 + \cdots + v_k$.

Proof. Let Y be the set $\{(b_1, \ldots, b_k) \in S^k \mid v_p(b_i) = v_i,\ i = 1, \ldots, k\}$. Then

$$\begin{aligned} \{a \in S^k \mid v_p(f_i(a)) = v_i\} &= \{a \in S^k \mid (f_1(a), \ldots, f_k(a)) \in Y\} \\ &= \{a \in S^k \mid M \cdot a \in Y\} \\ &= \{M^{-1}b \mid b \in Y\}. \end{aligned}$$

Since M is invertible and measure-preserving, this implies that

$$\mu(\{a \in S^k \mid v_p(f_i(a)) = v_i,\ i = 1, \ldots, k\}) = \mu(Y) = \prod_{i=1}^{k} q^{-v_i}(1 - q^{-1}) = q^{-s}(1 - q^{-1})^k. \qquad \square$$

In our application, we will be mainly interested in counting solutions in R^k. While this seems rather difficult in general, we will see that in our case, the action of the associated Galois group of the p-adic fields on the set of polynomials $\{f_1, \dots, f_k\}$ is of a particular simple form, reflected in the following assumption: Assume that the field extension of the corresponding fraction fields of R and S is cyclic of degree d with Galois group $G = \langle\sigma\rangle$ and the system of linear forms $f_1, \dots, f_k$ satisfies the following property: there exists a partition $\{f_1, \dots, f_k\} = \bigcup_{i=1}^{l} F_i$ into disjoint sets F_i of cardinality d such that G acts transitively on each F_i. For $i \in \{1, \dots, l\}$ we write $F_i = \{f_{i,1}, \dots, f_{i,d}\}$. As G acts transitively we may order the polynomials such that $\sigma(f_{i,j}) = f_{i,(j+1) \bmod d}$ for all $i \in \{1, \dots, l\}$, $j \in \{1, \dots, d\}$.

Lemma 6. *Let $c = (c_{i,j})_{1\le i\le l, 1\le j\le d} = (c_{1,1}, \dots, c_{1,d}, c_{2,1}, \dots, c_{2,d}, \dots, c_{l,d}) \in S^k$ and $a = (a_1, \dots, a_k) \in S^k$ such that $M \cdot a = c$. Then $a \in R^k$ if and only if for each $1 \le i \le l$ we have $c_{i,j} = \sigma^{j-1}(c_{i,1})$ for $1 \le j \le d$.*

Proof. First assume that $a \in R^k$. We fix $1 \le i \le l$. Since $f_{i,1}(a) = c_{i,1}$ for all $1 \le j \le d$ we have

$$\sigma^{j-1}(c_{i,1}) = \sigma^{j-1}(f_{i,1}(a)) = (\sigma^{j-1}(f_{i,1}))(\sigma(a)) = f_{i,j}(a) = c_{i,j}.$$

Now assume that $c_{i,j} = \sigma^{j-1}(c_{i,1})$ for all $1 \le i \le l,\ 1 \le j \le d$; that is, $\sigma(c_{i,j}) = c_{i,(j+1) \bmod d}$. Then

$$c_{i,(j+1) \bmod d} = \sigma(c_{i,j}) = \sigma(f_{i,j}(a)) = (\sigma(f_{i,j}))(\sigma(a)) = f_{i,(j+1) \bmod d}(\sigma(a)),$$

implying that also $\sigma(a)$ satisfies $M \cdot \sigma(a) = c$. Since M is invertible it follows that $a = \sigma(a)$; that is, $a \in R^k$. □

We can now determine the number of solutions with prescribed valuation in the subring R. Since the valuation of an element is invariant under σ, a necessary condition for the existence of solutions in R is that the valuations in every block F_i must be equal.

Proposition 7. *For $v_1, \dots, v_l \in \mathbb{Z}_{\ge 0}$ we have*

$$\mu(\{a \in R^k \mid v_p(f_{i,j}(a)) = v_i,\ i = 1, \dots, l,\ j = 1, \dots, d\}) = p^{-s}(1 - p^{-d})^l,$$

where $s = d(v_1 + \cdots + v_l)$.

Proof. By defining

$$Y = \{(b_i, \sigma(b_i), \dots, \sigma^{d-1}(b_i))_{1\le i\le l} \mid (b_1, \dots, b_l) \in S^l,\ v_p(b_i) = v_i\} \subseteq S^k,$$

Lemma 6 shows that

$$\{a \in R^k \mid v_p(f_{i,j}(a)) = v_i,\ i = 1, \dots, l,\ j = 1, \dots, d\} = \{M^{-1}b \mid b \in Y\}.$$

The remainder of the proof is analogous to the proof of Lemma 5. □

5. Distribution for cyclic field of prime degree

Let K be a cyclic field of odd prime degree ℓ, and $p \ne 2, \ell$. Let M_ℓ be the generic regulator matrix of K. To find the associated random variable $P_{\ell,p}$ using the results from Section 4, we first need to determine the factorisation of $\det(M_\ell) \in \mathbb{Z}[X_1, \dots, X_{\ell-1}]$.

Proposition 8. *Denote by ζ a primitive ℓ-th root of unity and by $\sigma\colon \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$ a generator of* $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. *Define* $f_0 = X_0 + \zeta X_1 + \cdots + \zeta^{\ell-1} X_{\ell-1}$.

(1) *We have*

$$\det(M_\ell) = (-1)^{(\ell-1)/2} \cdot \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(f_0) = (-1)^{(\ell-1)/2} \cdot \prod_{i=0}^{\ell-2} \sigma^i(f_0).$$

(2) *For $i \in \{1, \ldots, \ell-2\}$ define $f_i = \sigma^i(f_0)$. 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 $\det(M)^2 = (-1)^{(\ell-1)/2} \cdot \ell^{\ell-2}$.

Proof. (1) Recall that

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

As $X_0 = -X_1 - X_2 - \cdots - X_{\ell-1}$, we may treat X_0 as an indeterminate and prove the result for M_ℓ by considering it as an $\ell \times \ell$ matrix over $\mathbb{Z}[X_0, \ldots, X_{\ell-1}]$. By applying to M_ℓ the column transpositions $(i+1, \ell-(i-1))$, $i \in \{1, \ldots, (\ell-1)/2\}$, we see that $\det(M_\ell) = (-1)^{(\ell-1)/2} \cdot \det(N)$, where

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

On the other hand, the circulant matrix

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

has determinant $\det(N') = (X_0 + X_1 + \cdots + X_{\ell-1}) \cdot \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(f_0)$ (see [Dav79, Section 3.2]). Adding the last $\ell-1$ rows of N' to the first row of N', we see that

$$\det(N') = (X_0 + X_1 + \cdots + X_{\ell-1}) \cdot \det(N).$$

This shows that

$$\det(M_\ell) = (-1)^{(\ell-1)/2} \cdot \det(N) = (-1)^{(\ell-1)/2} \cdot \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(f_0).$$

(2) As the matrix M is equal to $(\sigma^i(\zeta^j))_{0\le i,j\le \ell-2}$ and $\{\zeta^j \mid j\in\{0,\dots,\ell-2\}\}$ is an integral basis of the cyclotomic field $\mathbb{Q}(\zeta)$, we obtain $\det(M)^2=\operatorname{disc}(\mathbb{Q}(\zeta))=(-1)^{(\ell-1)/2}\cdot\ell^{\ell-2}$ (see [Lan94, Chapter IV, §1]). □

We can now apply the results of Section 4 to determine $P_{\ell,p}$.

Theorem 9. *Let* $\operatorname{ord}_\ell(p)=m$ *and* $\ell-1=mn$. *Then for* $i\in\mathbb{Z}_{\ge 0}$ *the following holds*:

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

Proof. We use the same notation as in Proposition 8. Let $i\in\mathbb{Z}_{\ge 0}$ and $v_1,\dots,v_n\in\mathbb{Z}_{\ge 0}$ such that $i=v_1+\cdots+v_n$.

As $\operatorname{ord}_\ell(p)=m$ we know that $\mathbb{Z}_p\subseteq\mathbb{Z}_p[\zeta]$ is an extension of degree m. Using Proposition 8, by setting $F_k=\{f_j \mid j\equiv k \bmod m\}$, $k\in\{1,\dots,n\}$, we find ourselves in the situation stated in Section 4, and Proposition 7 implies

$$\mu(\{a\in\mathbb{Z}_p^{\ell-1} \mid v_p(f_k(a))=v_j,\ j=1,\dots,n,\ f_k\in F_j\})=\frac{1}{p^{m(v_1+\cdots+v_n)}}\left(1-\frac{1}{p^m}\right)^n.$$

As there are a total of $\binom{i+n-1}{n-1}$ choices of $(v_1,\dots,v_n)$ with $v_1+\cdots+v_n=i$, we have

$$\begin{aligned}\mu(\{a\in\mathbb{Z}_p^{\ell-1} \mid v_p(\det(M(a)))=mi\}) &= \sum_{v_1+\cdots v_n=i}\frac{1}{p^{m(v_1+\cdots+v_n)}}\left(1-\frac{1}{p^m}\right)^n\\ &=\binom{i+n-1}{n-1}\frac{1}{p^{mi}}\left(1-\frac{1}{p^m}\right)^n.\end{aligned}$$

□

In particular, Conjecture 1 is just a reformulation of Conjecture 1′ using Theorem 9.

6. Numerical evidence

We have investigated Conjecture 1 (and Conjecture 1′) numerically for $\ell\in\{5,7\}$. Recall that Conjecture 1 states that for a prime $p\ne 2,\ell$ with $\operatorname{ord}_\ell(p)=m$, $\ell-1=mn$ and $\mathrm{T}\in\{\mathrm{un},\mathrm{ram}\}$ we have $v_p(R_p(K))\in m\mathbb{Z}+v_{\mathrm{T}}$ for all $K\in\mathcal{K}_p^{\mathrm{T}}$ and for $i\ge 0$ we have

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

where $v_{\mathrm{un}}=\ell-1$ and $v_{\mathrm{ram}}=(\ell-1)/2$. As the right-hand side of this equation is straightforward to calculate, only the limit on the left-hand side had to be investigated. Thus to test our conjecture we needed algorithms to compute both a large number of cyclic extensions and their p-adic regulators. We used an algorithm based on global class field theory as provided by Fieker in [Fie01] to obtain a list of cyclic quintic and septic extensions. For the computation of the p-adic regulators, we relied on the methods from Fieker and Zhang [FZ16]. A more detailed discussion of the algorithms can be found in these references.

p	$\#\mathcal{K}_p^{\mathrm{un}}(5\cdot 10^{31})$	4	5	6	7	8	9	10
11	4 049 077	0.68249	0.24878	0.05655	0.01026	0.00162	$2.37\cdot 10^{-2}$	$3.26\cdot 10^{-3}$
Conjecture 1		0.68301	0.24836	0.05644	0.01026	0.00163	$2.37\cdot 10^{-2}$	$3.23\cdot 10^{-3}$
31	4 890 617	0.87712	0.11313	0.00913	$5.67\cdot 10^{-2}$	$3.31\cdot 10^{-3}$	$2.04\cdot 10^{-4}$	$2.04\cdot 10^{-5}$
Conjecture 1		0.87707	0.11317	0.00912	$5.88\cdot 10^{-2}$	$3.32\cdot 10^{-3}$	$1.71\cdot 10^{-4}$	$8.30\cdot 10^{-6}$
41	5 030 537	0.90597	0.08837	0.00538	$2.53\cdot 10^{-2}$	$1.15\cdot 10^{-3}$	$1.98\cdot 10^{-5}$	0
Conjecture 1		0.90595	0.08838	0.00538	$2.62\cdot 10^{-2}$	$1.12\cdot 10^{-3}$	$4.37\cdot 10^{-5}$	$1.60\cdot 10^{-6}$
61	5 181 713	0.93575	0.06163	0.00252	$8.49\cdot 10^{-3}$	$1.73\cdot 10^{-4}$	0	0
Conjecture 1		0.93602	0.06137	0.00251	$8.24\cdot 10^{-3}$	$2.36\cdot 10^{-4}$	$6.20\cdot 10^{-6}$	$1.52\cdot 10^{-7}$
71	5 226 957	0.94495	0.05311	0.00187	$5.49\cdot 10^{-3}$	$7.65\cdot 10^{-5}$	0	0
Conjecture 1		0.94484	0.05323	0.00187	$5.27\cdot 10^{-3}$	$1.30\cdot 10^{-4}$	$2.93\cdot 10^{-6}$	$6.19\cdot 10^{-8}$

Table 1. Distribution of valuations of p-adic regulators where $\mathrm{ord}_5(p)=1$ and p is unramified.

p	$\#\mathcal{K}_p^{\mathrm{ram}}(5\cdot 10^{31})$	2	3	4	5	6	7	8
11	1 472 145	0.68262	0.24847	0.05671	0.01028	0.00161	$2.47\cdot 10^{-2}$	$3.19\cdot 10^{-3}$
Conjecture 1		0.68301	0.24836	0.05644	0.01026	0.00163	$2.37\cdot 10^{-2}$	$3.23\cdot 10^{-3}$
31	630 605	0.87763	0.11259	0.00909	$6.29\cdot 10^{-2}$	$4.28\cdot 10^{-3}$	$1.58\cdot 10^{-4}$	0
Conjecture 1		0.87707	0.11317	0.00912	$5.88\cdot 10^{-2}$	$3.32\cdot 10^{-3}$	$1.71\cdot 10^{-4}$	$8.30\cdot 10^{-6}$
41	490 685	0.90685	0.08748	0.00538	$2.58\cdot 10^{-2}$	$1.42\cdot 10^{-3}$	0	0
Conjecture 1		0.90595	0.08838	0.00538	$2.62\cdot 10^{-2}$	$1.12\cdot 10^{-3}$	$4.37\cdot 10^{-5}$	$1.60\cdot 10^{-6}$
61	339 509	0.93634	0.06122	0.00234	$8.54\cdot 10^{-3}$	0	0	0
Conjecture 1		0.93602	0.06137	0.00251	$8.24\cdot 10^{-3}$	$2.36\cdot 10^{-4}$	$6.26\cdot 10^{-6}$	$1.52\cdot 10^{-7}$
71	294 265	0.94497	0.05291	0.00207	$4.07\cdot 10^{-3}$	0	0	0
Conjecture 1		0.94484	0.05323	0.00187	$5.27\cdot 10^{-3}$	$1.30\cdot 10^{-4}$	$2.93\cdot 10^{-6}$	$6.19\cdot 10^{-8}$

Table 2. Distribution of valuations of p-adic regulators where $\mathrm{ord}_5(p)=1$ and p is ramified.

p	$\#\mathcal{K}_p^{\mathrm{un}}(5\cdot 10^{31})$	4	6	8	10
19	5 521 222	0.99447	0.00550	$2.10\cdot 10^{-3}$	$1.81\cdot 10^{-5}$
Conjecture 1		0.99446	0.00550	$2.28\cdot 10^{-3}$	$8.45\cdot 10^{-6}$
29	5 521 222	0.99762	0.00237	$5.07\cdot 10^{-4}$	0
Conjecture 1		0.99762	0.00237	$4.23\cdot 10^{-4}$	$6.70\cdot 10^{-7}$
59	5 521 222	0.99942	$5.70\cdot 10^{-2}$	$3.62\cdot 10^{-5}$	0
Conjecture 1		0.99942	$5.74\cdot 10^{-2}$	$2.47\cdot 10^{-5}$	$9.47\cdot 10^{-9}$
79	5 521 222	0.99967	$3.24\cdot 10^{-2}$	0	0
Conjecture 1		0.99967	$3.20\cdot 10^{-2}$	$7.69\cdot 10^{-6}$	$1.64\cdot 10^{-9}$
89	5 521 222	0.99974	$2.52\cdot 10^{-2}$	0	0
Conjecture 1		0.99974	$2.52\cdot 10^{-2}$	$4.78\cdot 10^{-6}$	$8.04\cdot 10^{-10}$

Table 3. Distribution of valuations of p-adic regulators where $\mathrm{ord}_5(p)=2$.

p	$\#\mathcal{K}_p^{\mathrm{un}}(5\cdot 10^{31})$	4	8	12	16
3	5 521 222	0.98766	0.01218	$1.42\cdot 10^{-2}$	$1.81\cdot 10^{-4}$
Conjecture 1		0.98765	0.01219	$1.50\cdot 10^{-2}$	$1.85\cdot 10^{-4}$
7	5 521 222	0.99958	$4.13\cdot 10^{-2}$	0	0
Conjecture 1		0.99958	$4.16\cdot 10^{-2}$	$1.73\cdot 10^{-5}$	$7.22\cdot 10^{-9}$
13	5 521 222	0.99996	$3.54\cdot 10^{-3}$	0	0
Conjecture 1		0.99996	$3.50\cdot 10^{-3}$	$1.22\cdot 10^{-7}$	$4.29\cdot 10^{-12}$
17	5 521 222	0.99998	$1.10\cdot 10^{-3}$	0	0
Conjecture 1		0.99998	$1.19\cdot 10^{-3}$	$1.43\cdot 10^{-8}$	$1.71\cdot 10^{-13}$
23	5 521 222	0.99999	$2.71\cdot 10^{-4}$	0	0
Conjecture 1		0.99999	$3.57\cdot 10^{-4}$	$1.27\cdot 10^{-9}$	$4.56\cdot 10^{-15}$
37	5 521 222	0.99999	$1.26\cdot 10^{-4}$	0	0
Conjecture 1		0.99999	$5.33\cdot 10^{-5}$	$2.84\cdot 10^{-11}$	$1.51\cdot 10^{-17}$
43	5 521 222	0.99999	$1.81\cdot 10^{-5}$	0	0
Conjecture 1		0.99999	$2.92\cdot 10^{-5}$	$8.55\cdot 10^{-12}$	$2.50\cdot 10^{-18}$
47	5 521 222	0.99999	$1.81\cdot 10^{-5}$	0	0
Conjecture 1		0.99999	$2.04\cdot 10^{-5}$	$4.19\cdot 10^{-12}$	$8.60\cdot 10^{-19}$
53	5 521 222	1	0	0	0
Conjecture 1		0.99999	$1.26\cdot 10^{-5}$	$1.60\cdot 10^{-12}$	$2.03\cdot 10^{-19}$
67	5 521 222	1	0	0	0
Conjecture 1		0.99999	$4.96\cdot 10^{-6}$	$2.46\cdot 10^{-13}$	$1.22\cdot 10^{-20}$
73	5 521 222	1	0	0	0
Conjecture 1		0.99999	$3.52\cdot 10^{-6}$	$1.23\cdot 10^{-13}$	$4.36\cdot 10^{-21}$
83	5 521 222	1	0	0	0
Conjecture 1		0.99999	$2.10\cdot 10^{-6}$	$4.43\cdot 10^{-14}$	$9.35\cdot 10^{-22}$
97	5 521 222	1	0	0	0
Conjecture 1		0.99999	$1.12\cdot 10^{-6}$	$1.27\cdot 10^{-14}$	$1.44\cdot 10^{-22}$

Table 4. Distribution of valuations of p-adic regulators where $\mathrm{ord}_5(p)=4$.

6.1. ***Cyclic quintic extensions.*** We computed the valuation of p-adic regulators for all cyclic quintic extensions with discriminant up to $5\cdot 10^{31}$ for $2<p<100$, $p\neq\ell$. The computations were carried out using Magma [BCP97]. For these 5 521 222 fields, the values

$$\frac{\#\{K\in\mathcal{K}_p^{\mathrm{T}}(5\cdot 10^{31})\mid v_p(R_p(K))=j\}}{\#\mathcal{K}_p^{\mathrm{T}}(5\cdot 10^{31})}$$

are presented in Tables 1–4 and compared to the values as predicted by Conjecture 1. Note that in Tables 1 and 2 for $p=11$ the fields with $v_p(R_p(K))\in\{11,12,13\}$ and $v_p(R_p(K))\in\{9\}$ respectively have been omitted for brevity.

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	7	8	9	10	11
29	273 289	0.81036	0.16753	0.01990	0.00204	$1.35\cdot10^{-2}$	$1.09\cdot10^{-3}$
Conjecture 1		0.81014	0.16761	0.02022	0.00186	$1.44\cdot10^{-2}$	$9.95\cdot10^{-4}$
43	289 489	0.86861	0.12041	0.01034	$5.71\cdot10^{-2}$	$4.97\cdot10^{-3}$	$3.45\cdot10^{-4}$
Conjecture 1		0.86833	0.12116	0.00986	$6.11\cdot10^{-2}$	$3.20\cdot10^{-3}$	$1.48\cdot10^{-4}$
71	304 141	0.91805	0.07774	0.00400	$1.74\cdot10^{-2}$	$1.31\cdot10^{-3}$	0
Conjecture 1		0.91841	0.07761	0.00382	$1.43\cdot10^{-2}$	$4.55\cdot10^{-4}$	$1.28\cdot10^{-5}$

Table 5. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p)=1$ and p is unramified.

p	$\#\mathcal{K}_p^{\mathrm{ram}}(10^{42})$	3	4	5	6	7
29	56 419	0.81070	0.16575	0.02164	0.00171	$1.77\cdot10^{-2}$
Conjecture 1		0.81014	0.16761	0.02022	0.00186	$1.44\cdot10^{-2}$
43	40 219	0.86861	0.12041	0.01034	$5.71\cdot10^{-2}$	$4.97\cdot10^{-3}$
Conjecture 1		0.86833	0.12116	0.00986	$6.11\cdot10^{-2}$	$3.20\cdot10^{-3}$
71	25 567	0.91977	0.07713	0.00297	$1.17\cdot10^{-2}$	0
Conjecture 1		0.91841	0.07761	0.00382	$1.43\cdot10^{-2}$	$4.55\cdot10^{-4}$

Table 6. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p)=1$ and p is ramified.

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	8	10
13	329 708	0.98216	0.01766	$1.75\cdot10^{-2}$
Conjecture 1		0.98235	0.01743	$2.06\cdot10^{-2}$
41	329 708	0.99814	0.00184	$3.03\cdot10^{-4}$
Conjecture 1		0.99821	0.00178	$2.11\cdot10^{-4}$
83	329 708	0.99957	$4.21\cdot10^{-2}$	0
Conjecture 1		0.99956	$4.35\cdot10^{-2}$	$1.26\cdot10^{-5}$
97	329 708	0.99971	$2.88\cdot10^{-2}$	0
Conjecture 1		0.99968	$3.18\cdot10^{-2}$	$6.77\cdot10^{-6}$

Table 7. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p)=2$.

Moreover, the conjecture predicts that the valuations occur in an arithmetic progression with an initial value of $\ell-1$ or $(\ell-1)/2$ and common difference $\mathrm{ord}_\ell(p)$; indeed, no valuations not in this arithmetic progression were observed. For example, when $p=13$ we have $\mathrm{ord}_5(13)=4$, and the conjecture predicts that all valuations must be multiples of 4, and no valuation that is not a multiple of 4 was observed.

6.2. ***Cyclic septic extensions.*** The same computations as in the quintic case were carried out for all 329 708 cyclic septic extensions of discriminant $\le 10^{42}$; see Tables 5–9. Again, no valuations not predicted by Conjecture 1 were observed in the computation.

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	9
11	329 708	0.99857	0.00142
Conjecture 1		0.99849	0.00150
23	329 708	0.99984	$1.57 \cdot 10^{-2}$
Conjecture 1		0.99983	$1.64 \cdot 10^{-2}$
37	329 708	0.99996	$3.63 \cdot 10^{-3}$
Conjecture 1		0.99996	$3.94 \cdot 10^{-3}$

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	9
53	329 708	0.99998	$1.51 \cdot 10^{-3}$
Conjecture 1		0.99998	$1.34 \cdot 10^{-3}$
67	329 708	0.99998	$1.21 \cdot 10^{-3}$
Conjecture 1		0.99999	$6.64 \cdot 10^{-4}$
79	329 708	0.99999	$3.03 \cdot 10^{-4}$
Conjecture 1		0.99999	$4.05 \cdot 10^{-4}$

Table 8. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p) = 3$.

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	12
3	329 708	0.99865	0.00134
Conjecture 1		0.99862	0.00136
5	329 708	0.99992	$7.58 \cdot 10^{-3}$
Conjecture 1		0.99993	$6.39 \cdot 10^{-3}$
17	329 708	1	0
Conjecture 1		0.99999	$4.14 \cdot 10^{-6}$
19	329 708	1	0
Conjecture 1		0.99999	$2.12 \cdot 10^{-6}$
31	329 708	1	0
Conjecture 1		0.99999	$1.12 \cdot 10^{-7}$

p	$\#\mathcal{K}_p^{\mathrm{un}}(10^{42})$	6	12
47	329 708	1	0
Conjecture 1		0.99999	$9.27 \cdot 10^{-10}$
59	329 708	1	0
Conjecture 1		0.99999	$2.37 \cdot 10^{-9}$
61	329 708	1	0
Conjecture 1		0.99999	$1.94 \cdot 10^{-9}$
73	329 708	1	0
Conjecture 1		0.99999	$6.60 \cdot 10^{-10}$
89	329 708	1	0
Conjecture 1		0.99999	$2.01 \cdot 10^{-10}$

Table 9. Distribution of valuations of p-adic regulators where $\mathrm{ord}_7(p) = 6$.

Acknowledgements

We would like to thank Pierre Guillot and Christian Wüthrich, who communicated to us a proof of Proposition 8. Hofmann was supported by Project II.2 of SFB-TRR 195 "Symbolic Tools in Mathematics and their Application" of the German Research Foundation (DFG).

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR 1484478

[Bru67] Armand Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124. MR 0220694

[Buc90] Johannes Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Progr. Math., no. 91, Birkhäuser, Boston, MA, 1990, pp. 27–41. MR 1104698

[Coa77] John Coates, *p-adic L-functions and Iwasawa's theory*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham), Academic, London, 1977, pp. 269–353. MR 0460282

[Dav79] Philip J. Davis, *Circulant matrices*, John Wiley & Sons, New York, 1979. MR 543191

[Fie01] Claus Fieker, *Computing class fields via the Artin map*, Math. Comp. **70** (2001), no. 235, 1293–1303. MR 1826583

[FZ16] Claus Fieker and Yinan Zhang, *An application of the p-adic analytic class number formula*, LMS J. Comput. Math. **19** (2016), no. 1, 217–228. MR 3506905

[Hak07] Tuomas Hakkarainen, *On the computation of class numbers of real abelian fields*, Ph.D. thesis, University of Turku, 2007.

[HZ16] Tommy Hofmann and Yinan Zhang, *Valuations of p-adic regulators of cyclic cubic fields*, J. Number Theory **169** (2016), 86–102. MR 3531231

[Iwa72] Kenkichi Iwasawa, *Lectures on p-adic L-functions*, Annals of Mathematics Studies, no. 74, Princeton University Press, University of Tokyo Press, 1972. MR 0360526

[Lan94] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, no. 110, Springer, 1994. MR 1282723

[Leo62] Heinrich-Wolfgang Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern*, J. Reine Angew. Math. **209** (1962), 54–71. MR 0139602

[Mar96] František Marko, *On the existence of p-units and Minkowski units in totally real cyclic fields*, Abh. Math. Sem. Univ. Hamburg **66** (1996), 89–111. MR 1418221

[Mik87] Hiroo Miki, *On the Leopoldt conjecture on the p-adic regulators*, J. Number Theory **26** (1987), no. 2, 117–128. MR 889379

[Pan95] Peter Panayi, *Computation of Leopoldt's p-adic regulator*, Ph.D. thesis, University of East Anglia, 1995.

[Sch93] Oliver Schirokauer, *Discrete logarithms and local units*, Philos. Trans. Roy. Soc. London Ser. A **345** (1993), no. 1676, 409–423. MR 1253502

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, no. 67, Springer, 1979. MR 554237

Received 2 Mar 2018. Revised 13 Jun 2018.

TOMMY HOFMANN: thofmann@mathematik.uni-kl.de
Fachbereich Mathematik, Technische Universität Kaiserslautern, Kaiserslautern, Germany

YINAN ZHANG: yinan.zhang@anu.edu.au
Mathematical Sciences Institute, Australian National University, Canberra, Australia

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine