p-adic measures and computation of Darmon–Dasgupta units

Mateo Crabit Nicolau

IMJ-PRG and Universiteit Leiden

Arithmetic and Geometry Examples Seminar

October 23, 2026

Outline

1. Bernoulli polynomials, zeta functions and p-adic measure over $\mathbb{Z}_p$
2. Darmon–Dasgupta units and p-adic measure over $\mathbb{Z}_p^2$
3. Computation of Darmon–Dasgupta units for big prime numbers
4. Examples

Hilbert's 12th Problem

Theorem (Kronecker–Weber)

Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

Theorem (Complex Multiplication)

Let K be an imaginary quadratic field and let $N \geq 1$. The ray class field of modulus $N\mathcal{O}_K$ is generated by the values of the j-invariant and the Weber function at suitable CM points.

Hilbert's 12th Problem

Give an explicit description of the abelian extensions of a number field using special values of analytic functions.

Real quadratic fields: Darmon–Vonk (2021); Roset–Xu (2025) generalize this to higher-degree totally real fields.
Radchenko–Wheeler (2026) proof of the Stark conjecture for real quadratic fields.

Fields with one complex place: Bergeron–Charollois–García (2023) for cubic fields; Morain (2026) for higher degrees.

Totally real fields: Dasgupta–Kakde (2023), proof of the Brumer–Stark conjecture.

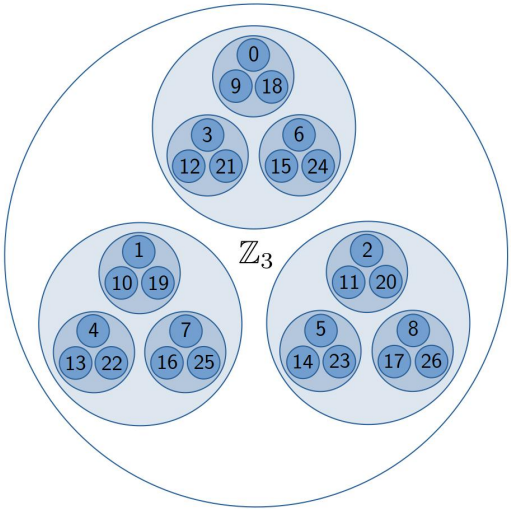
p-adic measure

Let p be a prime number. We want to define a p-adic measure on $\mathbb{Z}_p - p\mathbb{Z}_p$, i.e. a map μ from the set of compact open subsets of $\mathbb{Z}_p - p\mathbb{Z}_p$ to $\mathbb{Z}_p$ satisfying

$$\mu(U) = \sum_i \mu(U_i)$$

for every decomposition $U = \bigsqcup_i U_i$ into compact open subsets.

Compact open subsets in $\mathbb{Z}_3$



Source: Wikipedia.

p-adic measure

Let p be a prime number. We want to define a p-adic measure on $\mathbb{Z}_p - p\mathbb{Z}_p$, i.e. a map μ from the set of compact open subsets of $\mathbb{Z}_p - p\mathbb{Z}_p$ to $\mathbb{Z}_p$ satisfying

$$\mu(U) = \sum_i \mu(U_i)$$

for every decomposition $U = \bigsqcup_i U_i$ into compact open subsets.
For a continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ we can define

$$\int_{\mathbb{Z}_p - p\mathbb{Z}_p} f(t)d\mu(t) := \varprojlim_a \sum_{(\mathrm{mod}\ p^n)} f(a)\mu(a + p^n\mathbb{Z}_p)$$

Bernoulli distribution and generating series

Recall the definition of the Bernoulli polynomials:

$$f_t(x) := \frac{e^{tx}}{e^t - 1} = \sum_{k \geq 0} b_k(x) t^{k-1}.$$

Proposition

The assignment

$$a + p^r \mathbb{Z}_p \to \mu_{b,1}(a + p^r \mathbb{Z}_p) = b_1\left(\frac{a}{p^r}\right) = \frac{a}{p^r} - \frac{1}{2}$$

defines a distribution on $\mathbb{Z}_p - p\mathbb{Z}_p$.

Idea of the proof: The generating series $f_t(x)$ satisfies

$$\sum_{b=0}^{p-1} f_t\left(\frac{a_0 + bp^r}{p^{r+1}}\right) = f_{t/p}(a_0/p^r).$$

We conclude taking the constant coefficient.

Denominator

Recall the definition of the Bernoulli polynomials:

$$f_t(x) := \frac{e^{tx}}{e^t - 1} = \sum_{k \geq 0} b_k(x) t^{k-1}.$$

Proposition

The assignment

$$a + p^r\mathbb{Z}_p \to \mu_{b,1}(a + p^r\mathbb{Z}_p) = b_1\left(\frac{a}{p^r}\right) = \frac{a}{p^r} - \frac{1}{2}$$

defines a distribution on $\mathbb{Z}_p - p\mathbb{Z}_p$.

However,

$$v_p(\mu_{b,1}(1 + p^r\mathbb{Z}_p)) = v_p\left(\frac{1}{p^r} - \frac{1}{2}\right) = -r.$$

The distribution $\mu_{b,1}$ is not bounded p-adically.

ℓ-smoothing

Let $\ell \neq p$ be a prime number.

Proposition

The p-adic distribution $\mu_{b,1}^{(\ell)}$, whose value on a compact open subset U is given by

$$\mu_{b,1}^{(\ell)}(U) \coloneqq \mu_{b,1}(U) - \ell^{-1}\mu_{b,1}(\ell U),$$

is a p-adic measure.

Let $U = 1 + p^r\mathbb{Z}_p$. Then we have

$$\begin{aligned}\mu_{b,1}^{(\ell)}(1 + p^r\mathbb{Z}_p) &= \mu_{b,1}(1 + p^r\mathbb{Z}_p) - \ell^{-1}\mu_{b,1}(\ell + p^r\mathbb{Z}_p) \\ &= \frac{1}{p^r} - \frac{1}{2} - \ell^{-1}\left(\frac{\ell}{p^r} - \frac{1}{2}\right) \\ &= \frac{1}{2\ell} - \frac{1}{2}.\end{aligned}$$

Kubota–Leopoldt ζ function

Let

$$\zeta_p(1-k) = -(1-p^k)k!\, b_{k+1}(0)$$

be the Kubota–Leopoldt p-adic zeta function.

Proposition

$$\zeta_p(1-k) = \frac{1}{\ell^{-k-1}-1} \int_{\mathbb{Z}_p - p\mathbb{Z}_p} X^k d\mu_{b,1}^{(\ell)}(X).$$

Remark

Let

$$f_t^{(\ell)}(x) = f_t(x) - \ell^{-1} f_{t/\ell}(\ell x) \in \mathbb{Q}[[t]],$$

then

$$\text{Coeff } [t^k] f_t^{(\ell)}(0) = \text{const} \times \zeta_p(1-k).$$

Kummer congruences

Proposition (Kummer)

Let $N \geq 0$, and $k, k' \in \mathbb{Z}$ such that $k \equiv k' \mod (p-1)p^N$. Then

$$(1-p^k)k!b_{k+1}(0) \equiv (1-p^{k'})k'!b_{k'+1}(0) \mod p^{N+1}.$$

The construction in a nutshell

We constructed a family of generating series parametrized by $x \in \mathbb{Q}$

$$f_t^{(\ell)}(x) = f_t(x) - \ell^{-1} f_{t/\ell}(\ell x) \in \mathbb{Q}[[t]]$$

such that

- After the ℓ-smoothing, the generating series $f_t^{(\ell)}$ is regular at $t = 0$ and the denominator of its constant coefficient is bounded.
- The constant coefficient gives the value of a p-adic measure on certain compact-opens subsets.
- Its other coefficients are related to special moments of this measure.

Generating series for real quadratic fields

Let ℓ be an odd prime number, let $c \geq 1$ be divisible by ℓ, let $d \in \mathbb{Z}$ be prime to c, and let $v = (v_1, v_2) \in \mathbb{Q}^2$. Finally, let ω be a real quadratic number and set $\beta = c\omega + d$.

$$h_\omega(t, c, d, v) := \sum_{j=0}^{c-1} f_t\left(\left\{v_1 - \frac{d}{c}(j + v_2)\right\}\right) f_{\beta t}\left(\frac{j + \{v_2\}}{c}\right)$$
$$= \sum_{j=0}^{c-1} \frac{e^{t\{v_1 - \frac{d}{c}(j+v_2)\}}}{(e^t - 1)} \frac{e^{\beta t\left(\frac{j+\{v_2\}}{c}\right)}}{(e^{\beta t} - 1)} \in \frac{1}{t^2}\mathbb{Q}(\omega)[[t]].$$

Definition

$$h_\omega^{(\ell)}(t, c, d, v) := h_{\ell\omega}\left(\frac{t}{\ell}, \frac{c}{\ell}, d, (\ell v_1, v_2)\right) - \ell h_\omega(t, c, d, v).$$

Generating series for real quadratic fields

Definition

$$h_\omega^{(\ell)}(t,c,d,v) := h_{\ell\omega}\left(\frac{t}{\ell},\frac{c}{\ell},d,(\ell v_1,v_2)\right) - \ell h_\omega(t,c,d,(v_1,v_2)).$$

Proposition

The generating series $h_\omega^{(\ell)}(t,c,d,v)$ is regular at $t=0$. Furthermore,

$$h_\omega^{(\ell)}(0,c,d,v) \in \mathbb{Z} \quad \text{if } \ell \geq 5, \qquad h_\omega^{(\ell)}(0,c,d,v) \in \frac{1}{3}\mathbb{Z} \quad \text{if } \ell = 3.$$

p-adic measure in the quadratic case

Proposition

Let p be a prime number inert in $F = \mathbb{Q}(\omega)$ and let $\ell \neq p$. The assignment

$$(a,b) + p^r\mathbb{Z}_p^2 \longmapsto \mu_\ell(c,d)((a,b) + p^r\mathbb{Z}_p^2) := \text{coeff } [t^0]h_\omega^{(\ell)}(t,c,d,a/p^r,b/p^r)$$

defines a p-adic measure on $\mathbb{Z}_p^2 - p\mathbb{Z}_p^2$.

Let $v = (a/p^r, b/p^r)$. Then

$$\mu_\ell(c,d)((a,b)+p^r\mathbb{Z}_p^2) = \sum_{j=0}^{c/\ell-1} b_1\left(\frac{v_2+j}{c/\ell}\right) b_1\left(v_1 - d\frac{v_2+j}{c/\ell}\right) - \ell \sum_{j=0}^{c-1} b_1\left(\frac{v_2+j}{c}\right) b_1\left(v_1 - d\frac{v_2+j}{c}\right).$$

This is a classical Dedekind sum.

Darmon–Dasgupta units

In 2006, Darmon and Dasgupta constructed a p-adic number $u_\ell(\omega)$ conjectured to be a p-unit in the narrow ring class field of $\mathbb{Q}(\omega)$. The algebraicity of $u_\ell(\omega)$ is now a theorem of Dasgupta–Kakde (2023).

Definition (Darmon–Dasgupta, 2006)

Let $\begin{pmatrix} d & * \\ c & * \end{pmatrix}$ be a generator of $\mathrm{Stab}_{SL_2(\mathbb{Z})}(\omega)$ and assume that $\ell \mid c$. Let $\mu_\ell = \mu_\ell(c,d)$. Then

$$\log_p(u_\ell(\omega)) \coloneqq \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} \log_p(X + \omega Y) d\mu_\ell(X,Y).$$

In fact, $\mu_\ell \in H^1(\Gamma_0(\ell), \mathrm{Meas}(\mathbb{Z}_p^2 - p\mathbb{Z}_p^2, \mathbb{Z}_p))$.

DD units and ζ functions

$$\log_p(u_\ell(\omega)) \coloneqq \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} \log_p(X + \omega Y) d\mu_\ell(X, Y)$$

Proposition

There exists a ℓ-smoothed ζ function $\zeta_p^{(\ell)}(\omega, s)$ such that

$$\zeta_p^{(\ell)\prime}(\omega, 0) = \log_p(\mathrm{Nm}_{\mathbb{Q}_p^2/\mathbb{Q}_p}(u_\ell(\omega))) = \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} \log_p((X + \omega Y)(X + \omega' Y)) d\mu_\ell(x, y)$$

In this sense, the construction of Darmon–Dasgupta is a refinement of the Gross–Stark conjecture.

Dasgupta's algorithm

$$\log_p(u_\ell(\omega)) = \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} \log_p(X + \omega Y) d\mu_\ell(x, y).$$

In 2008, Dasgupta gave an algorithm to compute $u_\ell(\omega)$ with M digits of p-adic precision, by computing moments of the form

$$\int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p} X^i Y^j \, d\mu_\ell(X, Y)$$

for $0 \leq i, j \leq p(M + \log M)$.

A table of Fleischer–Liu

Table 1: $p = 3$, $\ell = 5$

D	G	ord_p	$P(X)$
44	C_2	± 2	$X^2 + \frac{7}{3^2}X + 1$
56	C_2	± 3	$X^2 - \frac{46}{3^3}X + 1$
161	C_2	± 9	$X^2 + \frac{28234}{3^9}X + 1$
209	C_2	± 2	$X^2 + \frac{7}{3^2}X + 1$
221	C_4	$\pm 3, \pm 15$	$X^4 + (\frac{-423812}{3^{13}} + \frac{71680\sqrt{D}}{3^{15}})X^3 + (\frac{76348630}{3^{18}} + \frac{-5218304\sqrt{D}}{3^{16}})X^2 + (\frac{-423812}{3^{13}} + \frac{71680\sqrt{D}}{3^{15}})X + 1$
236	C_2	± 6	$X^2 - \frac{1433}{3^6}X + 1$
284	C_2	± 14	$X^2 - \frac{7162162}{3^{14}}X + 1$
329	C_2	± 15	$X^2 - \frac{26326214}{3^{15}}X + 1$

Computing Darmon–Dasgupta units part 1

We want to compute with M digits of p-adic precision

$$\log_p(u_\ell(\omega)) = \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} \log_p(X + \omega Y) d\mu_\ell(x, y).$$

Theorem (Charollois, 2026)

$$\text{coeff } [t^m] p^m m! h_\omega^{(\ell)}\left(t, c, d, \left(\frac{a}{p}, \frac{b}{p}\right)\right) = \int_{(a,b)+p\mathbb{Z}_p^2} (X + \omega Y)^m d\mu_\ell(X, Y).$$

When $(a, b) = (0, 0)$. We have

$$\text{coeff } [t^m](1 - p^m) m! h_\omega^{(\ell)}(t, c, d, (0, 0)) = \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} (X + \omega Y)^m d\mu_\ell(X, Y).$$

Computing Darmon–Dasgupta units part 2

$$\log_p(u_\ell(\omega)) = \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} \log_p(X + \omega Y) d\mu_\ell(x, y) = \sum_{(a,b)[p]}{}' \int_{(a,b)+p\mathbb{Z}_p^2} \log_p(X + \omega Y) d\mu_\ell(x, y).$$

Developing $\log_p$ around 1, it is enough to compute

$$\text{coeff } [t^m] h_\omega^{(\ell)}\left(t, c, d, \left(\frac{a}{p}, \frac{b}{p}\right)\right) = (*) \int_{(a,b)+p\mathbb{Z}_p^2} (X + \omega Y)^m d\mu_\ell(X, Y)$$

for $(a, b) \neq (0, 0) \mod p$ and $0 \leq m \leq M + \log(M)$.

Recovering $u_\ell(\omega)$

To recover $u_\ell(\omega)$ from $\log_p(u_\ell(\omega))$ we need:

- $$\operatorname{ord}_p(u_\ell(\omega)) = \zeta^{(\ell)}(\omega, 0) = \operatorname{coeff}[t^0]\, h_\omega^{(\ell)}(t, c, d, (0,0))$$
- The value $\log_{\beta_p}(u_\ell(\omega))$, where β_p is a (p^2-1)-st root of unity in $\mathbb{Q}_{p^2}$:

$$\log_{\beta_p}(u_\ell(\omega)) = \int_{\mathbb{Z}_p^2 - p\mathbb{Z}_p^2} \log_{\beta_p}(X + \omega Y) d\mu_\ell(X, Y).$$

We only need to know

$$\operatorname{coeff}[t^0]\, h_\omega^{(\ell)}(t, c, d, (a/p, b/p)) \quad \text{for } a, b = 0, \ldots, p-1.$$

Minimal polynomials

Proposition

The minimal polynomial of $u_\ell(\omega)$ over F is given by

$$P_{u_\ell(\omega)}(x) = \prod_i (x - u_\ell(\omega_i)) \in F[x].$$

We need to identify the coefficients of $P_{u_\ell(\omega)}$ that are of the form

$$x_1 + x_2\sqrt{D} \quad \text{with } x_1, x_2 \in \mathbb{Q}_p.$$

`lindep`'s litany

The `lindep` function in PARI/GP is a function that takes a vector of values $[x_1, ..., x_n]$ and try to find a linear combination with integer coefficients between them.
It uses an algorithm to find a short vector (LLL) in the lattice generated by the matrix

$$\begin{pmatrix} Mx_1 & Mx_2 & \cdots & Mx_n \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

where M is very big (relative to the precision).

Examples

For $D = 316, \ell = 3$ and $p = 223$

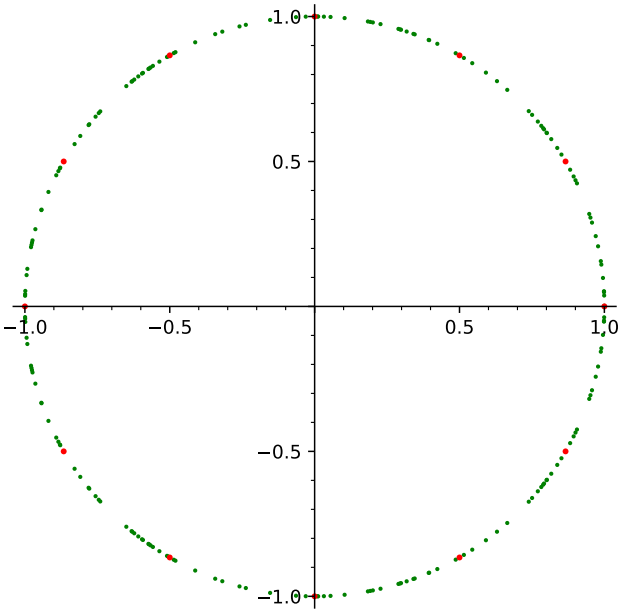
$$P_{u_\ell(\omega)}(x) = x^6 + \left(-\frac{2379794051942991931973229870334566 4}{223^{15}}\sqrt{D} + \frac{1109207863982925505423331160000701 42}{223^{15}}\right)x^5$$
$$+ \left(-\frac{3441593020757024061989877710113376694968 32}{223^{18}}\sqrt{D} + \frac{4296297987701498650844884379097668755610303}{223^{18}}\right)x^4$$
$$+ \left(-\frac{1813201160055871681929975963497976944738644340736}{223^{21}}\sqrt{D} + \frac{1081636401628606582335814207132770226829424358955 56}{223^{21}}\right)x^3$$
$$+ \ldots$$

Examples

For $D = 60$, $\ell = 3$, $p = 1213$,

$$P_{u_\ell(\omega)}(x) = x^4 - \frac{4370727949910}{1213^4}x^3 + \frac{7699010627101587891}{1213^6}x^2 - \frac{4370727949910}{1213^4}x + 1$$

Roots of $P_{u_\ell(\omega)}(x)$ for $D = 60$, $\ell = 3$, $1 \leq p \leq 563$

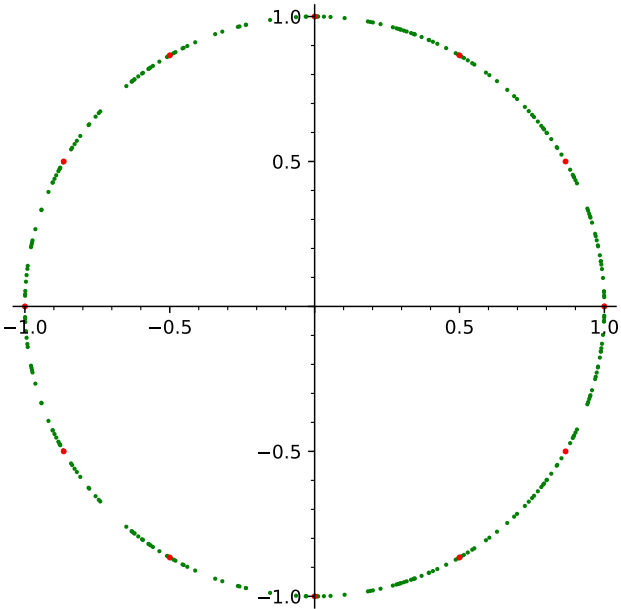


Legend

- embeddings of $u_\ell(\omega)$
- Roots of unity in $H = F(u_\ell(\omega))$

Number of primes: 50.

Roots of $P_{u_\ell(\omega)}(x)$ for $D = 60$, $\ell = 3$, $1 \leq p \leq 859$

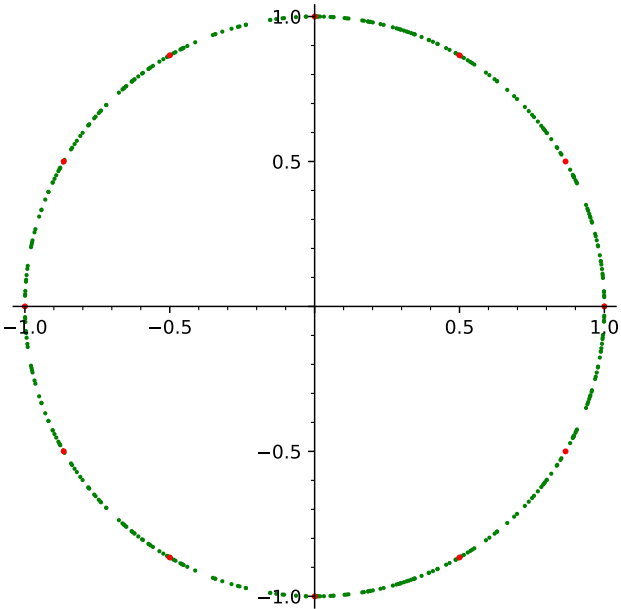


Legend

- ● embeddings of $u_\ell(\omega)$
- ● Roots of unity in $H = F(u_\ell(\omega))$

Number of primes: 75.

Roots of $P_{u_\ell(\omega)}(x)$ for $D = 60$, $\ell = 3$, $1 \leq p \leq 1213$



Legend

- ● embeddings of $u_\ell(\omega)$
- ● Roots of unity in $H = F(u_\ell(\omega))$

Number of primes: 103.

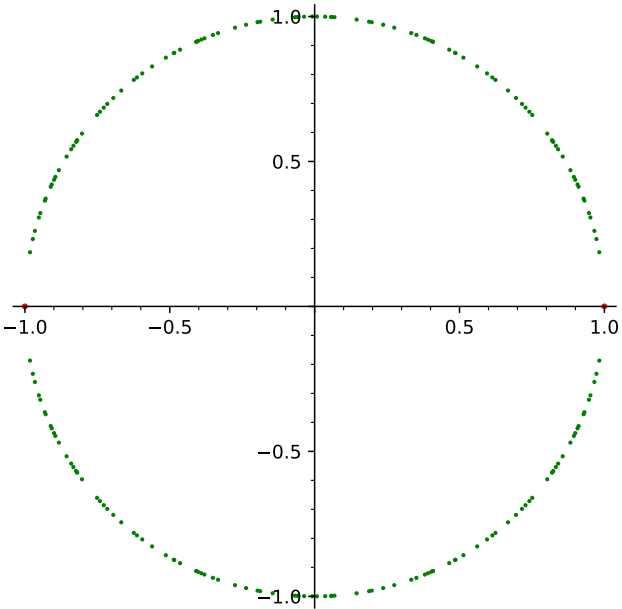
More examples in a specific case

When the narrow class group of $\mathbb{Q}(\omega)$ is $\mathbb{Z}/2\mathbb{Z}$ and $u_\ell(\omega) \in \mathbb{Q}_p$, we can try to guess $P_{u_\ell(\omega)}$ as

$$P_{u_\ell(\omega)}(x) = x^2 - \frac{a}{p^r}x + 1,$$

with $|a| \leq 2p^r$. Since $P_{u_\ell(\omega)}$ generates the narrow Hilbert class field of $\mathbb{Q}(\omega)$, there are only few possibilities left.

Roots of $P_{u_\ell(\omega)}(x)$ for $D = 56$, $\ell = 7$, $1 \leq p \leq 563$

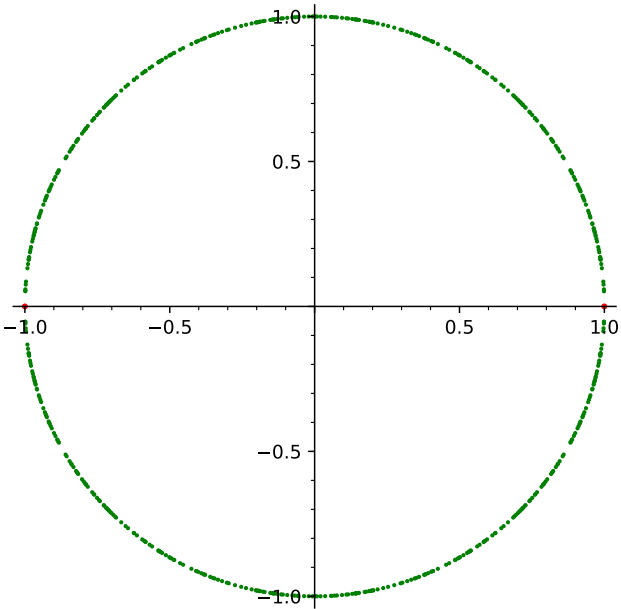


Legend

- embeddings of $u_\ell(\omega)$
- Roots of unity in $H = F(u_\ell(\omega))$

Number of primes: 50.

Roots of $P_{u_\ell(\omega)}(x)$ for $D = 56$, $\ell = 7$, $1 \leq p \leq 1901$

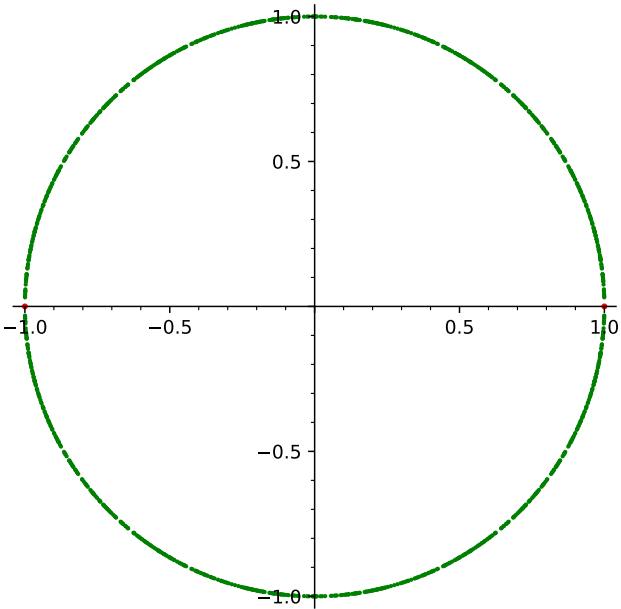


Legend

- embeddings of $u_\ell(\omega)$
- Roots of unity in $H = F(u_\ell(\omega))$

Number of primes: 150.

Roots of $P_{u_\ell(\omega)}(x)$ for $D = 56$, $\ell = 7$, $1 \leq p \leq 4327$

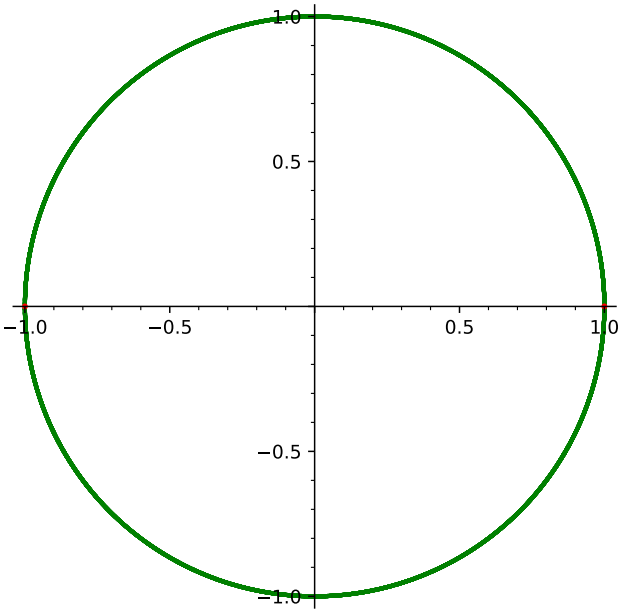


Legend

- embeddings of $u_\ell(\omega)$
- Roots of unity in $H = F(u_\ell(\omega))$

Number of primes: 300.

Roots of $P_{u_\ell(\omega)}(x)$ for $D = 56$, $\ell = 7$, $1 \leq p \leq 104723$

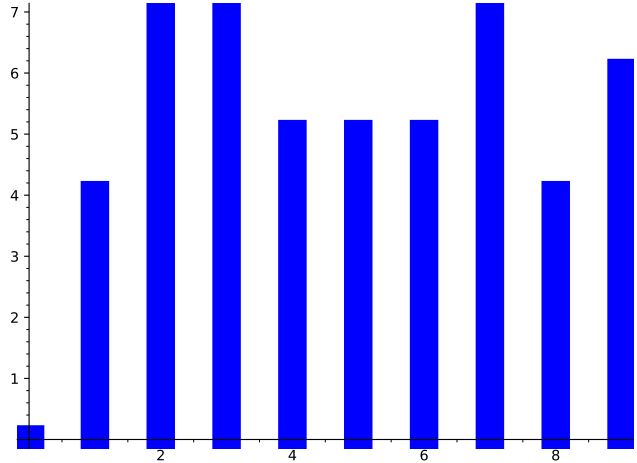


Legend

- • embeddings of $u_\ell(\omega)$
- • Roots of unity in $H = F(u_\ell(\omega))$

Number of primes: 5000.

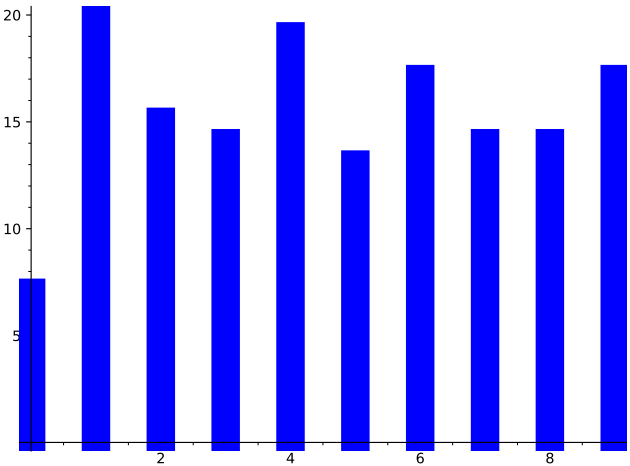
Repartition of the roots for $D = 56$, $\ell = 7$



Legend

Number of primes: 50.

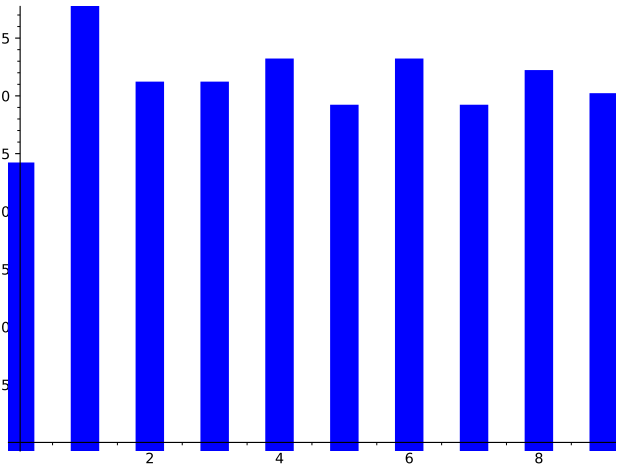
Repartition of the roots for $D = 56$, $\ell = 7$



Legend

Number of primes: 150.

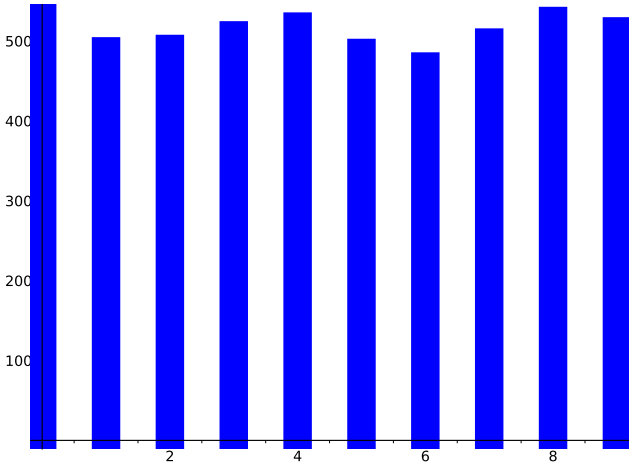
Repartition of the roots for $D = 56$, $\ell = 7$



Legend

Number of primes: 300.

Repartition of the roots for $D = 56$, $\ell = 7$



Legend

Number of primes: 5000.

Thank you for your attention!

$$P_u(x) = x^4 + (-2309526/5^{10}\omega^2 + -12739482/5^{10}\omega + 11479268/5^{10})x^3 + (2246075481951/5^{20}\omega^2 + 478277239149/5^{19}\omega + 44987525734384/5^{19})x^2 + ...$$

with

$$\omega^3 + 2\omega^2 - 6\omega - 1 = 0.$$