

Castles of numbers, and a bit of rethinking

Antoine Leudière

University of Calgary

The PIMS Postdoctoral Fellow Seminar
November 19th, 2025

About me

PIMS PDF at UCalgary, under Renate Scheidler.

Usual research

- Algorithmic number theory (Drinfeld modules).
- Applications to:
 - cryptography,
 - coding theory,
 - computer algebra.
- SageMath developer.

Typical algorithmic number theory problem

Compute the number of points of an *elliptic curve* over a finite field.

Rethinking Number Theory

We believe that number theory should be not only accessible, but enjoyable to everyone. Join us for a joyful collaborative research experience, where people are valued and uplifted. Help us rethink the graduate school and postdoc experience, research seminars, hiring process, conferences, grant applications, and other aspects of our profession.

With J. Bajpai, S. Das, K. S. Kedlaya, N. H. Le, M. Lee and J. Mello.

- <https://arxiv.org/abs/2510.20435>
- <https://github.com/castle-gray-rnt6/cassels>

Main results

- Complete classification of cyclotomic integers with $\text{castle} \leq 5.01$.
- As a corollary, complete classification of cyclotomic integers with $\text{castle} < 2$. (First conjecture stated by Robinson in 1965.)

Cyclotomic integers are highly important in number theory, class field theory, coding theory...

Sounds made up?

- Part of a research program started in 1965.
- At the moment, best we can do?

Today: focus on computations.

Stating the problem

The Robinson program

Our approach

Our implementation

Rethinking Number Theory

Stating the problem

The Robinson program

Our approach

Our implementation

Rethinking Number Theory

Algebraic integers

In algebra, we want exact representations and operations... but we also need complex numbers.

Combining exact representations and complex numbers

An *algebraic integer* $\alpha \in \mathbb{C}$ is any root of a monic integer polynomial.

Algebraic integers are almost like integers

- Algebraic integers contain: $\mathbb{Z}$; roots of unity; $\sqrt{2}$, $\sqrt{3}$, etc.
- Algebraic integers form a ring.
- Excellent factorization properties (Dedekind rings).

Algebraic integers come in families: algebraic integers with same minimal polynomial are called *algebraic conjugates*.

A theorem of Kronecker

General question

For any $c > 0$, who are the algebraic integers α whose algebraic conjugates β all verify $|\beta| \leq c$?

Kronecker, 1857

If $c = 1$, then α is zero or a root of unity.

The house and castle of an algebraic integer

Definition

- The *house* of an algebraic integer α is $|\overline{\alpha}| = \max_{\beta \text{ conjugate of } \alpha} |\beta|$.
- The *castle* is the square of the house.

The house is invariant under:

- algebraic conjugation,
- multiplying by a root of unity.

Equivalence of algebraic numbers

Two algebraic numbers are declared equivalent if one is a root of unity times an algebraic conjugate of the other.

Cyclotomic integers

Towards a general result?

In full generality, not much hope to classify algebraic integers α (up to equivalence) with $|\alpha| \leq c$.

Robinson suggested (1965) one could get stronger results for *cyclotomic integers*:

Definition

A *cyclotomic integer* is an algebraic integer that is a sum of roots of unity.

Example:

- $1, 2 = 1 + 1, 3 = 1 + 1 + 1, \dots;$
- $e^{\frac{2i\pi}{N}}$ for any N ;
- $2 \cos\left(\frac{2\pi}{3}\right).$

Stating the problem

The Robinson program

Our approach

Our implementation

Rethinking Number Theory

The Robinson program

Two problems, five conjectures.

- Qualitative problems; answers given by Loxton.
- The conjectures are quantitative versions.

Problem 1. How can we tell whether there is any cyclotomic integer with a given absolute value? More generally, how can we find all the cyclotomic integers with this absolute value? Does it ever happen that there are infinitely many inequivalent cyclotomic integers with the same absolute value?

Problem 2. How can we tell whether a given cyclotomic integer can be expressed as a sum of a prescribed number of roots of unity?

Conjectures 3 & 4

Conjecture 3. The numbers $1 + 2i \cos \pi/N$ and $\sqrt{5} \cos \pi/N + i \sin \pi/N$ are equivalent only for $N = 2, 10, 30$.

Proved by Schinzel in 1966; see also McKee and Smyth in 2021.

Conjecture 4. If α is a cyclotomic integer with $\|\alpha\| \leq \sqrt{5}$, then either $\|\alpha\|$ has one of the forms

$$2 \cos \pi/N, \quad \sqrt{(1 + 4 \cos^2 \pi/N)},$$

where N is a positive integer, or else is equal to one of the two numbers

$$\sqrt{\frac{5 + \sqrt{13}}{2}}, \quad \frac{\sqrt{7} + \sqrt{3}}{2}.$$

Enhanced and proved by Robinson and Wurz in 2013.

Conjecture 5

Conjecture 5. The only cyclotomic integers satisfying $\|\alpha\| \leq \sqrt{5}$ which are expressible as sums of three roots of unity are those equivalent to numbers of the forms

$$2 \cos \pi/N, \quad 1 + 2i \cos \pi/N,$$

where N is a positive integer, or to one of the five numbers

$$\frac{1 + i\sqrt{7}}{2}, \quad \frac{\sqrt{5} + i\sqrt{3}}{2}, \quad 2 \cos \frac{2\pi}{7} + \frac{1 + i\sqrt{3}}{2},$$
$$1 + e^{2\pi i/13} + e^{8\pi i/13}, \quad 1 + e^{2\pi i/24} + e^{14\pi i/24}.$$

Proved by Jones in 1968.

Conjecture 2—Cassels' theorem

Conjecture 2. There are only a finite number of inequivalent cyclotomic integers with $\|\alpha\| \leq \sqrt{5}$ which are not equivalent to a number of one of the following forms, where N is a positive integer:

$$2 \cos \pi/N, \quad 1 + 2i \cos \pi/N, \quad \sqrt{5} \cos \pi/N + i \sin \pi/N.$$

Enhanced to $\sqrt{5.01}$ (suggestion of Jones) and proved by Cassels in 1969.

Definition

Exceptional cyclotomic integers in Cassels' theorem are *Cassels exceptions*.

Our result

Compute all Cassels exceptions!

The Cassels exceptions

N	Cassels exception
11	$1 + \zeta + \zeta^2 + \zeta^4 - \zeta^5 + \zeta^7$
19	$1 + \zeta + \zeta^4 + \zeta^7 + \zeta^8 + \zeta^9 + \zeta^{10} + \zeta^{12} + \zeta^{14}$
20	$1 + \zeta + \zeta^3 - \zeta^4$
24	$1 + \zeta + \zeta^5 - \zeta^6$
31	$1 + \zeta + \zeta^3 + \zeta^8 + \zeta^{12} + \zeta^{18}$
51	$1 + \zeta^3 - \zeta^{10} + \zeta^{15} + \zeta^{21} + \zeta^{24} + \zeta^{30} + \zeta^{33} + \zeta^{39}$
84	$1 - \zeta^4 - \zeta^{13} - \zeta^{16} + \zeta^{19} + \zeta^{21} + \zeta^{22} + \zeta^{31}$
91	$1 + \zeta^7 + \zeta^{14} - \zeta^{17} + \zeta^{21} + \zeta^{42} - \zeta^{69} + \zeta^{70} - \zeta^{82}$
33	$1 + \zeta^6 - \zeta^8 + \zeta^{21}$
28	$1 + \zeta - \zeta^3 - \zeta^{11}$
33	$1 + \zeta^6 - \zeta^7 - \zeta^{10}$
21	$1 - \zeta - \zeta^5 + \zeta^{18}$
28	$1 + \zeta - \zeta^3 + \zeta^4$
21	$1 - \zeta + \zeta^6 + \zeta^{18}$

N	Cassels exception
60	$1 - \zeta^3 - \zeta^6 - \zeta^8$
11	$1 + \zeta + \zeta^2 + \zeta^5$
7	$(1 + \zeta_7 + \zeta_7^3)^2 = \zeta + \zeta^3 + \zeta^4 - \zeta^5$
28	$(1 + i)(1 + \zeta_7 + \zeta_7^3)$
39	$1 - \zeta^2 - \zeta^5 - \zeta^8 - \zeta^{11} - \zeta^{20} - \zeta^{32}$
55	$1 - \zeta - \zeta^{16} + \zeta^{22} - \zeta^{26} - \zeta^{31} - \zeta^{36}$
60	$(1 + i)(1 - \zeta_{15} + \zeta_{15}^{12})$
105	$(1 + \zeta_7 + \zeta_7^3)(1 - \zeta_{15} + \zeta_{15}^{12})$
21	$1 - \zeta - \zeta^{13}$
11	$1 + \zeta + \zeta^2 + \zeta^4 + \zeta^7$
13	$1 + \zeta + \zeta^3 + \zeta^9$
35	$1 - \zeta + \zeta^7 - \zeta^{11} - \zeta^{16}$
7	$1 + \zeta + \zeta^3$

On each row $\zeta = e^{\frac{2i\pi}{N}}$.

Conjecture 1—~~The last open conjecture~~

Conjecture 1. Any cyclotomic integer α with $\|\alpha\| < 2$ is either the sum of two roots of unity, is equivalent to a number of the form $(\sqrt{a} + i\sqrt{b})/2$, where a and b are positive integers, or is equivalent to one of the following three numbers:

$$\frac{3 + \sqrt{13} + i\sqrt{(26 - 6\sqrt{13})}}{4}, \quad 1 + i\frac{\sqrt{5} + 1}{2}, \quad 2\cos\frac{2\pi}{7} + \frac{1 + i\sqrt{3}}{2}.$$

We proved it!

Proof

Apply Cassels' theorem and look in the Cassels exceptions.

Stating the problem

The Robinson program

Our approach

Our implementation

Rethinking Number Theory

An unfeasible computation

Cassels' observation

All Cassels exceptions lie in the subring of algebraic integers $\mathbb{Z}$ -generated by

$$e^{\frac{2i\pi}{n}}, \quad \text{with } n = 4692838820715366441120.$$

The Cassels exceptions live in a finite set (intersection of a disk and a discrete).
...But finding a short vector in a lattice is computationally hard.

How do we go from an unfeasible computation to a feasible computation?

Measuring cyclotomic integers

For a cyclotomic integer α :

$$\begin{aligned}\text{CASSELSHEIGHT}(\alpha) &= \text{average of } |\beta|^2 \text{ for algebraic conjugates } \beta \text{ of } \alpha; \\ \text{MINIMALWEIGHT}(\alpha) &= \text{smallest number of roots of unity whose sum is } \alpha; \\ \text{MINIMALLEVEL}(\alpha) &= \text{minimal } N \text{ such that } \alpha \in \mathbb{Q}(e^{\frac{2i\pi}{N}}).\end{aligned}$$

- $\text{CASSELSHEIGHT}(\alpha)$ is entirely determined by $|\alpha|^2$.
- $\text{CASSELSHEIGHT}(\alpha)^{\frac{1}{2}} \leq |\alpha|^2 \leq \text{MINIMALWEIGHT}(\alpha)$.

Loxton

“For a given castle, the minimal weight cannot be so large.”

The partial result of Robinson and Wurz

The rule of the game

Control all these measures.

Robinson-Wurz, 2013

Let α be a cyclotomic integer with $|\alpha|^2 < 5.01$. Then one of the following holds:

- $\text{CASSELSHEIGHT}(\alpha) < 3\frac{1}{4}$, which implies $\text{CASSELSHEIGHT}(\alpha) \leq 3\frac{1}{5}$.
- $(|\alpha|^2, \text{CASSELSHEIGHT}(\alpha)) \in \left\{ \left(1 + 4 \cos^2 \frac{\pi}{15}, 3\frac{1}{4}\right), \left(1 + 4 \cos^2 \frac{\pi}{14}, 3\frac{1}{3}\right), \left(1 + 4 \cos^2 \frac{\pi}{10}, 3\frac{1}{2}\right) \right\}$.
- $|\alpha|^2 = \text{CASSELSHEIGHT}(\alpha) = 4$.
- $|\alpha|^2 = \text{CASSELSHEIGHT}(\alpha) = 5$.

Outline of the work

1. Theoretical work to eliminate as much possibilities for Cassels exceptions as possible.
 - Carefully re-read Robinson-Wurz; track and enhance their bounds.
 - Combinatorial analysis of decomposition patterns of candidates α as sums of roots of unity.
 - Use results from algebraic number theory to analyze the factorization patterns of candidates α embedded in higher number fields.
2. “Smart exhaustive search” to create a list of Cassels exceptions.
 - Exact algebra in SageMath.
 - Lower level computations in Rust.
3. For each case of Robinson-Wurz, prove that the cyclotomic integer is either covered by Cassels’ theorem, or a Cassels exception.

Stating the problem

The Robinson program

Our approach

Our implementation

Rethinking Number Theory

Choice of languages

	SageMath	Rust
Foss	✓	✓
Widely used	✓	✓
Math	✓	Not yet
Speed	✗	✓
Memory safety	✗	✓

Generating the exceptions

Representation

For any (n, N) and $(0 < j_1, \dots, j_n < N)$, we have a cyclotomic integer α with

$$|\overline{\alpha}|^2 = \max_{\substack{0 \leq k \leq N \\ \gcd(k, N) = 1}} \left(\left(\sum_{\ell=1}^n \cos \left(\frac{2i\pi j_\ell}{N} \right) \right)^2 + \left(\sum_{\ell=1}^n \sin \left(\frac{2i\pi j_\ell}{N} \right) \right)^2 \right).$$

Steps

1. Create a table of cosines and sines (floats) using Rust.
2. Use Rust to generate some* tuples $(0 < j_1, \dots, j_n < N)$, and discard those representing elements α with $\text{cast} |\overline{\alpha}|^2 > 5.01$.
3. For each tuple, use SageMath to check if it is covered by Cassels' theorem, or if it is a Cassels exception.



Set $N' = \text{lcm}(2, N)$; we can write $\alpha = \sum_{i=1}^{n'} \zeta_{N'}^{j_i}$ with $n' = \text{MINIMALWEIGHT}(\alpha) \leq n$ for some $0 \leq j_1, \dots, j_{n'} < N'$. As the claim is apparent when α is equivalent to an element of $\mathbb{Z}$, we may assume that the j_i are not all equal. We may also assume that $n' \geq 3$, as otherwise α is covered. Without loss of generality, we may make some further assumptions on the indices j_i :

- $j_1 = 0$ (by multiplying α by a root of unity);
- $\gcd(j_i, N') \geq \gcd(j_2, N')$ for $i = 3, \dots, n'$ (by relabeling);
- $j_2 = d$ is a proper divisor of N' (by applying a field automorphism and using that the j_i are not all equal);
- $j_3 \leq \dots \leq j_{n'}$ (by relabeling);
- $N' - j_{n'} > j_3 - j_2$ (by applying $j_i \mapsto d - j_i \pmod{N'}$ if needed);
- there are no indices $i < i'$ with $j_{i'} - j_i$ a nonzero multiple of $N'/2$ or $N'/3$ (as otherwise $n' > \text{MINIMALWEIGHT}(\alpha)$);
- there are no indices $i < i' < i''$ with $j_{i'} - j_i, j_{i''} - j_{i'}$ nonzero multiples of $N'/5$ (as otherwise $n' > \text{MINIMALWEIGHT}(\alpha)$);
- there are no indices $i < i' < i'' < i'''$ with $j_{i'} - j_i, j_{i''} - j_{i'}, j_{i'''} - j_{i''}$ nonzero multiples of $N'/7$ (as otherwise $n' > \text{MINIMALWEIGHT}(\alpha)$);
- if $n' = 3$, then there is no permutation k_1, k_2, k_3 of j_1, j_2, j_3 such that $k_1 + k_2 \equiv 2k_3 + N'/2 \pmod{N'}$ (as otherwise α is covered);
- if $n' = 4$ and $5 \mid N$, then there is no permutation k_1, k_2, k_3, k_4 of j_1, j_2, j_3, j_4 such that $k_1 - k_2, k_3 - k_4 \equiv 0 \pmod{N'/5}$ and $k_1 - k_2 + k_3 - k_4, k_1 - k_2 - k_3 + k_4 \not\equiv 0 \pmod{N'}$ (as otherwise α is covered).

Conclusion

Timing

Generating indices costs one hour on Intel Core Ultra 5 135U, 14 cores @4.4GHz with parallelization.

Controlling accuracy

Control accuracy with SageMath interval arithmetic and Rust being IEEE-compliant.

Stating the problem

The Robinson program

Our approach

Our implementation

Rethinking Number Theory

Rethinking Number Theory

What is *Rethinking Number Theory*?

- Workshop, started in 2020, on the model of AMS's *Mathematical Research Communities* or *Women in Numbers*.
- Every year, the RNT organizers recruit around six project leaders.
- Participants are recruited among students and post-docs.

Objective

- Work on open problems with joy, respect and open-mindedness.
- Rethink our profession.

Rethinking Number Theory

Organization

- Two weeks remote full time (if possible). Then it's up to the participants!
- *Rethinking sessions*. In 2025:
 - Building and supporting research collaborations.
 - Adapting to a changing world.
 - Activism and organization in academia.
- It works very well.

Thank you Allechar Serrano López, Heidi Goodson and Jen Berg!

<https://sites.google.com/view/rethinkingnumbertheory/>