The elliptic sieve and ideal norms

Edison Au-Yeung
University of Warwick

Warwick Swinnerton–Dyer Seminar
University of Warwick

5 October 2026

A counting problem

- Fermat: let $n \in \mathbb{N}$. Then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p \equiv 3 \bmod 4$ has even exponent in the prime factorisation of n.

A counting problem

- Fermat: let $n \in \mathbb{N}$. Then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p \equiv 3 \bmod 4$ has even exponent in the prime factorisation of n.
- Proof: $n = a^2 + b^2$ if and only if $n = |a + bi|^2 = \mathrm{Nm}(a + bi)$ for some $a + bi \in \mathbb{Z}[i]$. The result then follows from the classification of Gaussian primes.

  i.e. Sum of two squares problem = Norm problem for $\mathbb{Z}[i]$.

A counting problem

- Fermat: let $n \in \mathbb{N}$. Then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p \equiv 3 \bmod 4$ has even exponent in the prime factorisation of n.
- Proof: $n = a^2 + b^2$ if and only if $n = |a + bi|^2 = \mathrm{Nm}(a + bi)$ for some $a + bi \in \mathbb{Z}[i]$. The result then follows from the classification of Gaussian primes.

  i.e. Sum of two squares problem = Norm problem for $\mathbb{Z}[i]$.
- Landau and Ramanujan: almost all integers are not a sum of two squares when ordered by absolute value. More precisely,

$$\sum_{n \leq x} \mathbf{1}_{\{n = a^2 + b^2\}} \sim \frac{Kx}{\sqrt{\log x}} \quad \text{as } x \to \infty.$$

A counting problem

- Fermat: let $n \in \mathbb{N}$. Then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p \equiv 3 \bmod 4$ has even exponent in the prime factorisation of n.
- Proof: $n = a^2 + b^2$ if and only if $n = |a + bi|^2 = \mathrm{Nm}(a + bi)$ for some $a + bi \in \mathbb{Z}[i]$. The result then follows from the classification of Gaussian primes.

  i.e. Sum of two squares problem = Norm problem for $\mathbb{Z}[i]$.
- Landau and Ramanujan: almost all integers are not a sum of two squares when ordered by absolute value. More precisely,

$$\sum_{n \leq x} \mathbf{1}_{\{n = a^2 + b^2\}} \sim \frac{Kx}{\sqrt{\log x}} \quad \text{as } x \to \infty.$$

What about elliptic curves?

A counting problem - elliptic curve version

Theorem (Bhakta, Loughran, R-M, Nakahara, 2023)

Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. If $E(\mathbb{R})$ is connected and $P \in E(\mathbb{Q})$ has infinite order, then

$$\#\{n \in \mathbb{Z} : |n| \leq B, y(nP) \text{ is a sum of two squares}\} \ll_{E,P} \frac{B}{(\log B)^{\omega(E,P)}}$$

for some $\omega(E,P) > 0$.
i.e. for almost all multiples of P, the y–coordinate is not a sum of two squares.

Here an integral Weierstrass equation is

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{Z}.$$

A counting problem - elliptic curve version

Theorem (Bhakta, Loughran, R-M, Nakahara, 2023)

Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. If $E(\mathbb{R})$ is connected and $P \in E(\mathbb{Q})$ has infinite order, then

$$\#\{n \in \mathbb{Z} : |n| \leq B, y(nP) \text{ is a sum of two squares}\} \ll_{E,P} \frac{B}{(\log B)^{\omega(E,P)}}$$

for some $\omega(E,P) > 0$.
i.e. for almost all multiples of P, the y–coordinate is not a sum of two squares.

Here an integral Weierstrass equation is

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbb{Z}.$$

Note: this result is false for x–coordinate.

A counting problem - elliptic curve & norm version

Theorem (Bhakta, Loughran, R-M, Nakahara, 2023)

Let $K/\mathbb{Q}$ be a number field which contains a cyclic subfield which is not totally real. Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. If $E(\mathbb{R})$ is connected and $P \in E(\mathbb{Q})$ has infinite order, then

$$\#\{n \in \mathbb{Z} : |n| \leq B, y(nP) \text{ is a norm from } K\} \ll_{E,P,K} \frac{B}{(\log B)^{\omega(E,P)}}$$

for some $\omega(E,P) > 0$, where the implicit constant is $\exp\left(O_{E,K}\left(\widehat{h}(P)/\log \widehat{h}(P)\right)\right)$.

- $y(nP)$ is a norm from K: there exists an element $\alpha \in K^\times$ such that $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = y(nP)$.

A counting problem - elliptic curve & norm version

Theorem (Bhakta, Loughran, R-M, Nakahara, 2023)

Let $K/\mathbb{Q}$ be a number field which contains a cyclic subfield which is not totally real. Let E be an elliptic curve over $\mathbb{Q}$ given by an integral Weierstrass equation. If $E(\mathbb{R})$ is connected and $P \in E(\mathbb{Q})$ has infinite order, then

$$\#\{n \in \mathbb{Z} : |n| \leq B, y(nP) \text{ is a norm from } K\} \ll_{E,P,K} \frac{B}{(\log B)^{\omega(E,P)}}$$

for some $\omega(E,P) > 0$, where the implicit constant is $\exp\left(O_{E,K}\left(\widehat{h}(P)/\log \widehat{h}(P)\right)\right)$.

- $y(nP)$ is a norm from K: there exists an element $\alpha \in K^\times$ such that $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = y(nP)$.
- K contains a cyclic subfield which is not totally real: something to do with the sign of $y(nP)$ and the associated Dirichlet character

Main tool - elliptic divisibility sequence (EDS)

For $P = (x, y) \in E(\mathbb{Q})$, we can write

$$[n](x, y) = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3} \right)$$

with $\gcd(A_n, B_n) = \gcd(C_n, B_n) = 1$ and $B_n > 0$. In some literature $(B_n)_{n \in \mathbb{N}}$ is known as the EDS.

- Defined via the the denominators of the x–coordinates of the multiples of P.

Main tool - elliptic divisibility sequence (EDS)

For $P = (x, y) \in E(\mathbb{Q})$, we can write

$$[n](x, y) = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3} \right)$$

with $\gcd(A_n, B_n) = \gcd(C_n, B_n) = 1$ and $B_n > 0$. In some literature $(B_n)_{n \in \mathbb{N}}$ is known as the EDS.

- Defined via the the denominators of the x–coordinates of the multiples of P.
- A divisibility sequence: $n \mid m \implies B_n \mid B_m$.
- It has 'better' p–adic property.

Main tool - the elliptic sieve

- It originates from Kowalski, where it is a large sieve:
  1. Group/set: $E(\mathbb{Q})$
  2. Indexing set: set of primes $p \nmid \Delta(E)$, so E has good reduction modulo p
  3. Surjective map: $E(\mathbb{Q}) \to E(\mathbb{F}_p)$
- Goal of Kowalski's example: show that most rational points have denominators divisibile by many primes ($p \mid B_n$).

Main tool - the elliptic sieve

- It originates from Kowalski, where it is a large sieve:
  1. Group/set: $E(\mathbb{Q})$
  2. Indexing set: set of primes $p \nmid \Delta(E)$, so E has good reduction modulo p
  3. Surjective map: $E(\mathbb{Q}) \to E(\mathbb{F}_p)$
- Goal of Kowalski's example: show that most rational points have denominators divisibile by many primes ($p \mid B_n$).
- Modification required: we need to sieve modulo p^n with growing exponent n instead of just modulo p...

  (Fermat: let $n \in \mathbb{N}$. Then $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ if and only if $p \equiv 3 \bmod 4$ has even exponent in the prime factorisation of n)

(See *The Large Sieve and Its Applications : Arithmetic Geometry, Random Walks and Discrete Groups, Chapter 4.4* if you are interested!)

Limitations of the elliptic sieve

In short, it can only handle rank 1 case (i.e. consider $([n]P)_{n\in\mathbb{N}}$).

1. p-adic information about $[n]P$ and $[n]P+[m]Q$
   - we can use the subgroup filtration structure: denote by $E_0(K_\mathfrak{p})$ the set of points of $E(K_\mathfrak{p})$ with non–singular reduction modulo $\mathfrak{p}$. Then

     $$\cdots \subset E_2(K_\mathfrak{p}) \subset E_1(K_\mathfrak{p}) \subset E_0(K_\mathfrak{p}) \subseteq E(K_\mathfrak{p}),$$

     where $E_n(K_\mathfrak{p}) = \{P \in E_0(K_\mathfrak{p})\colon P \equiv O \bmod \mathfrak{p}^n\} \cup \{O\}$ for $n \geq 1$.
   - We don't have an equivalent tool for $[n]P+[m]Q$.

Limitations of the elliptic sieve

In short, it can only handle rank 1 case (i.e. consider $([n]P)_{n\in\mathbb{N}}$).

1. p-adic information about $[n]P$ and $[n]P + [m]Q$
2. Primes in $\mathbb{Z}$ VS primitive lattice points in $\mathbb{Z}^n$
   - Spoiler: the elliptic sieve gives a set of prime moduli $\ell \in \Lambda$ such that, roughly, a point $[n]P$ satisfying the norm condition must have $\ell \nmid n$ (i.e. we remove roughly $1/\ell$ of the integers).
   - Primes have density 0 in $\mathbb{Z}$, but there are enough primes in Λ for our sieve. In particular, Mertens' theorem says that

$$\log \prod_{\substack{\ell\in\Lambda \\ \ell\leq\sqrt{B}}} \left(1-\frac{1}{\ell}\right)^{-1} \geq \sum_{\substack{\ell\in\Lambda \\ \ell\leq\sqrt{B}}} \frac{1}{\ell} \longrightarrow \infty.$$

Limitations of the elliptic sieve

In short, it can only handle rank 1 case (i.e. consider $([n]P)_{n\in\mathbb{N}}$).

1. p-adic information about $[n]P$ and $[n]P+[m]Q$
2. Primes in $\mathbb{Z}$ VS primitive lattice points in $\mathbb{Z}^n$
   - Spoiler: the elliptic sieve gives a set of prime moduli $\ell \in \Lambda$ such that, roughly, a point $[n]P$ satisfying the norm condition must have $\ell \nmid n$ (i.e. we remove roughly $1/\ell$ of the integers).
   - Primes have density 0 in $\mathbb{Z}$, but there are enough primes in Λ for our sieve. In particular, Mertens' theorem says that

$$\log \prod_{\substack{\ell\in\Lambda\\ \ell\leq\sqrt{B}}} \left(1-\frac{1}{\ell}\right)^{-1} \geq \sum_{\substack{\ell\in\Lambda\\ \ell\leq\sqrt{B}}} \frac{1}{\ell} \longrightarrow \infty.$$

   - Consider $[n]P+[m]Q$, we know that primitive lattice points have positive density:

$$\frac{\#\{(m,n)\in\mathbb{Z}^2 \colon \gcd(m,n)=1, |m|,|n|\leq B\}}{\#\{(m,n)\in\mathbb{Z}^2 \colon |m|,|n|\leq B\}} \longrightarrow \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Pushing the elliptic sieve to its limit(?)

What if we impose extra conditions on the primitive lattice points in $\mathbb{Z}^2$? Let E has complex multiplication (again)!

- Let $E/\mathbb{C}$ be an elliptic curve over the complex numbers, then $\mathrm{End}(E)$ is always isomorphic to $\mathbb{Z}$ or $\mathbb{Z}[\tau] = \{a + b\tau : a, b \in \mathbb{Z}\}$, an order in an imaginary quadratic field F.

Pushing the elliptic sieve to its limit(?)

What if we impose extra conditions on the primitive lattice points in $\mathbb{Z}^2$? Let E has complex multiplication (again)!

- Let $E/\mathbb{C}$ be an elliptic curve over the complex numbers, then $\mathrm{End}(E)$ is always isomorphic to $\mathbb{Z}$ or $\mathbb{Z}[\tau] = \{a + b\tau : a, b \in \mathbb{Z}\}$, an order in an imaginary quadratic field F.
- When E/K has complex multiplicaton, it then makes sense for us to consider $[\alpha] : E \to E$, multiplication by $\alpha \in \mathbb{Z}[\tau] = \mathcal{O} \subset K$ in the group $E(K)$ (note: $\alpha \in \mathcal{O}$ is an element, not an ideal!).
- Example: $E : y^2 = x^3 - 35x + 98$ has complex multiplication by $\mathbb{Z}[\tau] = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$,

$$[\tau](x, y) = \left(\tau^{-2}\left(x - \frac{7(1-\tau)^4}{(x+\tau^2-2)}\right), \tau^{-3}y\left(1 + \frac{7(1-\tau)^4}{(x+\tau^2-2)^2}\right)\right)$$

- Identify $\mathcal{O}$ as $\mathbb{Z}^2$, then we have 'prime vectors' in $\mathbb{Z}^2$.

Main result

Theorem (A-Y, 2026+)

Let E/K be an elliptic curve over a number field K given by an integral Weierstrass equation, and suppose that E has complex multiplication by an order $\mathcal{O} \subset K$. Let L/K be a finite abelian extension.
Let $P \in E(K)$ be a non-torsion point. If P satisfies some technical conditions, then there exists $\omega = \omega(E, P) > 0$ such that, for every $\varepsilon > 0$,

$$\#\{\alpha \in \mathcal{O} : |\alpha| \leq B,\ y(\alpha P) \text{ is an ideal norm from } L\} \ll_{E,P,L} \frac{B}{(\log B)^{\omega-\varepsilon}},$$

where the implicit constant has dependence on P of the form $\exp\left(O_{E,L}\left(\widehat{h}(P)/\log \widehat{h}(P)\right)\right)$.

Necessary condition for ideal norm

Denote the group of fractional ideals in K by I_K.

- For any finite extension of number fields L/K, the norm map $\mathrm{Nm}_{L/K}\colon I_L \to I_K$ is the unique homomorphism such that for any prime ideal $\mathcal{P}$ of L, $\mathrm{Nm}_{L/K}(\mathcal{P}) = \mathfrak{p}^{f(\mathcal{P}/\mathfrak{p})}$ ($f(\mathcal{P}/\mathfrak{p}) = [\mathcal{O}_L/\mathcal{P}\colon \mathcal{O}_K/\mathfrak{p}]$ is the degree of the residue field extension).

Necessary condition for ideal norm

Denote the group of fractional ideals in K by I_K.

- For any finite extension of number fields L/K, the norm map $\mathrm{Nm}_{L/K}\colon I_L \to I_K$ is the unique homomorphism such that for any prime ideal $\mathcal{P}$ of L, $\mathrm{Nm}_{L/K}(\mathcal{P}) = \mathfrak{p}^{f(\mathcal{P}/\mathfrak{p})}$ ($f(\mathcal{P}/\mathfrak{p}) = [\mathcal{O}_L/\mathcal{P}\colon \mathcal{O}_K/\mathfrak{p}]$ is the degree of the residue field extension).
- Let L/K be an abelian extension, $\mathfrak{m}$ be an $\mathcal{O}_K$-ideal divisible by all primes ramified in L, then the global Artin map with respect to $\mathfrak{m}$ is

$$\mathrm{Art}^{\mathfrak{m}}_{L/K}\colon I_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K),$$

$$\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_t^{n_t} \mapsto \prod_{i=1}^{t} \mathrm{Frob}_{L/K}(\mathfrak{p}_i)^{n_i}.$$

- If an ideal $\mathfrak{a} \in \mathcal{O}_K$, coprime to $\mathfrak{m}$, is an ideal norm from L, then $\mathrm{Art}^{\mathfrak{m}}_{L/K}(\mathfrak{a}) = 1$ (i.e. $\mathfrak{a} \in \ker(\mathrm{Art}^{\mathfrak{m}}_{L/K})$).

Main result - technical conditions

Our EDS: for $P = (x, y) \in E(K)$, we can write

$$x\left([\alpha]P\right)\mathcal{O}_K = A_\alpha D_\alpha^{-2}, \alpha \in \mathcal{O} = \mathrm{End}(E),$$

where A_α and D_α are coprime $\mathcal{O}_K$–ideals (if K has class number 1, we denote $D_\alpha = (B_\alpha)$).

Main result - technical conditions

Our EDS: for $P = (x, y) \in E(K)$, we can write

$$x\left([\alpha]P\right)\mathcal{O}_K = A_\alpha D_\alpha^{-2}, \alpha \in \mathcal{O} = \mathrm{End}(E),$$

where A_α and D_α are coprime $\mathcal{O}_K$–ideals (if K has class number 1, we denote $D_\alpha = (B_\alpha)$).

Let L/K be an abelian extension. We need the existence of an $\alpha \in \mathcal{O}$ such that it satisfies the following:

1. D_α is coprime to all primes ramified in L; and
2. The image of D_α under the Artin map $\mathrm{Art}_{L/K}^{\mathfrak{m}} : I_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K)$ is nontrivial; and
3. $\alpha \in (\mathcal{O}/\pi\mathcal{O})^\times$, where π is an element in $\mathcal{O}$ that depends on P.

Recall: the result by Bhakta, Loughran, R-M, Nakahara assumes $E(\mathbb{R})$ is connected.

Overview of the elliptic sieve

$\mathcal{O}$ – prime ℓ

$\downarrow$

$\exists \mathfrak{p}$ such that $\mathrm{Ord}(\chi(\mathfrak{p})) \nmid \nu_{\mathfrak{p}}(D_\ell)$ $\qquad \chi\colon \mathrm{Gal}(L/K) \to \mathbb{C}^\times$

$\downarrow$

$(\ell) = \mathrm{ann}(P \bmod \mathfrak{p})$, so $\mathfrak{p} \mid D_\ell$ $\qquad$ # of such ℓ?

$\downarrow$

$\ell \nmid \alpha$ (roughly) $\implies D_\alpha \in \mathrm{Ker}(\mathrm{Art}^{\mathfrak{m}}_{L/K})$ $\qquad$ What is the sieve criterion?

$\downarrow$

sieve!

Local condition

Proposition

Let E, P be as above and assume all technical conditions are satisfied. Then

$$\#\{\ell \in \mathcal{O} : \ell \text{ generates a prime ideal in } \mathcal{O} \text{ and coprime to the conductor of } \mathcal{O}, \operatorname{Ord}(\chi(\mathfrak{p})) \nmid \nu_{\mathfrak{p}}(D_\ell) \text{ and } \mathfrak{p} \nmid \mathfrak{m} \text{ for some prime } \mathfrak{p} \subset \mathcal{O}_K \text{ with } \operatorname{Nm}(\ell) \leq X\} \gg_{E,P} \frac{X}{\log X}$$

Local condition

Proposition

Let E, P be as above and assume all technical conditions are satisfied. Then

$$\#\{\ell \in \mathcal{O} : \ell \text{ generates a prime ideal in } \mathcal{O} \text{ and coprime to the conductor of } \mathcal{O}, \operatorname{Ord}(\chi(\mathfrak{p})) \nmid \nu_{\mathfrak{p}}(D_\ell) \text{ and } \mathfrak{p} \nmid \mathfrak{m} \text{ for some prime } \mathfrak{p} \subset \mathcal{O}_K \text{ with } \operatorname{Nm}(\ell) \leq X\} \gg_{E,P} \frac{X}{\log X}$$

- We assumed the existence of $\alpha \in \mathcal{O}$ such that $\chi(D_\alpha) \neq 1$.

Local condition

Proposition

Let E, P be as above and assume all technical conditions are satisfied. Then

$$\#\{\ell \in \mathcal{O} : \ell \text{ generates a prime ideal in } \mathcal{O} \text{ and coprime to the conductor of } \mathcal{O}, \operatorname{Ord}(\chi(\mathfrak{p})) \nmid \nu_{\mathfrak{p}}(D_\ell) \text{ and } \mathfrak{p} \nmid \mathfrak{m} \text{ for some prime } \mathfrak{p} \subset \mathcal{O}_K \text{ with } \operatorname{Nm}(\ell) \leq X\} \gg_{E,P} \frac{X}{\log X}$$

- We assumed the existence of $\alpha \in \mathcal{O}$ such that $\chi(D_\alpha) \neq 1$.
- Periodicity of EDS: we showed that the corresponding ray classes of D_α is periodic in the ray class group.

$$\alpha \equiv \ell \bmod \pi \implies [D_\alpha] = [D_\ell] \text{ in } I_K^{\mathfrak{m}} / \ker(\operatorname{Art}_{L/K}^{\mathfrak{m}}).$$

(This is why we require $\alpha \in (\mathcal{O}/\pi\mathcal{O})^\times$ as a condition)

Local condition - periodicity

To deduce the periodicity, we consider CM division polynomials, rational functions on E.

For $z \in \mathcal{O} = \mathbb{Z}[\tau]$ and $P = (x, y)$, the CM division polynomial satisfies

$$x([z]P)\mathcal{O}_K = \frac{x\psi_z^2 - \psi_{z-1}\psi_{z+1}}{\psi_z^2}\mathcal{O}_K = A_z D_z^{-2},$$

and the recurrence relation

$$\psi_{\alpha+\beta}\psi_{\alpha-\beta}\psi_\gamma^2 = \psi_{\alpha+\gamma}\psi_{\alpha-\gamma}\psi_\beta^2 - \psi_{\beta+\gamma}\psi_{\beta-\gamma}\psi_\alpha^2 \text{ for any } \alpha, \beta, \gamma \in \mathcal{O}.$$

- Values of ψ_α are computed from the recurrence above and some initial conditions (e.g. $\psi_1 = \psi_\tau = \psi_{1+\tau} = 1, \psi_2 = 2y + a_1 x + a_3$).

Local condition - periodicity

To deduce the periodicity, we consider CM division polynomials, rational functions on E.

For $z \in \mathcal{O} = \mathbb{Z}[\tau]$ and $P = (x, y)$, the CM division polynomial satisfies

$$x([z]P)\mathcal{O}_K = \frac{x\psi_z^2 - \psi_{z-1}\psi_{z+1}}{\psi_z^2}\mathcal{O}_K = A_z D_z^{-2},$$

and the recurrence relation

$$\psi_{\alpha+\beta}\psi_{\alpha-\beta}\psi_\gamma^2 = \psi_{\alpha+\gamma}\psi_{\alpha-\gamma}\psi_\beta^2 - \psi_{\beta+\gamma}\psi_{\beta-\gamma}\psi_\alpha^2 \text{ for any } \alpha, \beta, \gamma \in \mathcal{O}.$$

- Values of ψ_α are computed from the recurrence above and some initial conditions (e.g. $\psi_1 = \psi_\tau = \psi_{1+\tau} = 1, \psi_2 = 2y + a_1 x + a_3$).
- This recurrence relation is the key to proving periodicity.

Local condition - periodicity

To deduce the periodicity, we consider CM division polynomials, rational functions on E.

For $z \in \mathcal{O} = \mathbb{Z}[\tau]$ and $P = (x, y)$, the CM division polynomial satisfies

$$x([z]P)\mathcal{O}_K = \frac{x\psi_z^2 - \psi_{z-1}\psi_{z+1}}{\psi_z^2}\mathcal{O}_K = A_z D_z^{-2},$$

and the recurrence relation

$$\psi_{\alpha+\beta}\psi_{\alpha-\beta}\psi_\gamma^2 = \psi_{\alpha+\gamma}\psi_{\alpha-\gamma}\psi_\beta^2 - \psi_{\beta+\gamma}\psi_{\beta-\gamma}\psi_\alpha^2 \text{ for any } \alpha, \beta, \gamma \in \mathcal{O}.$$

- Values of ψ_α are computed from the recurrence above and some initial conditions (e.g. $\psi_1 = \psi_\tau = \psi_{1+\tau} = 1, \psi_2 = 2y + a_1x + a_3$).
- This recurrence relation is the key to proving periodicity.
- Unfortunately, we don't usually have $D_z = \psi_z\mathcal{O}_K$ and D_z does not need to satisfy this recurrence relation either (and they are ideals!).

Local condition - periodicity

In short, D_α satisfies a weakened recurrence.

Local condition - periodicity

In short, D_α satisfies a weakened recurrence.

Theorem (A-Y, 2026)

Let M be an element in $\mathcal{O}$ such that $[M]P$ has everywhere good reduction. Let α, β and γ be elements of $\mathcal{O} = \mathrm{End}(E)$ and suppose at least two of α, β and γ are multiples of M.

1. *If $\mathrm{Cl}(K) = 1$, then the sequence of elements (B_α) can be chosen to satisfy*

$$B_{\alpha+\beta}B_{\alpha-\beta}B_\gamma^2 = B_{\alpha+\gamma}B_{\alpha-\gamma}B_\beta^2 - B_{\beta+\gamma}B_{\beta-\gamma}B_\alpha^2.$$

2. *If $\mathrm{Cl}(K) > 1$, then there is a sequence of fractional ideals $\{\mathfrak{g}_\alpha\}$ in $\mathcal{O}_K$ with*

$$D_\alpha = \psi_\alpha \mathfrak{g}_\alpha^{-1},$$
$$\psi_{\alpha+\beta}\psi_{\alpha-\beta}\psi_\gamma^2 = \psi_{\alpha+\gamma}\psi_{\alpha-\gamma}\psi_\beta^2 - \psi_{\beta+\gamma}\psi_{\beta-\gamma}\psi_\alpha^2,$$
$$\mathfrak{g}_{\alpha+\beta}\mathfrak{g}_{\alpha-\beta}\mathfrak{g}_\gamma^2 = \mathfrak{g}_{\alpha+\gamma}\mathfrak{g}_{\alpha-\gamma}\mathfrak{g}_\beta^2 = \mathfrak{g}_{\beta+\gamma}\mathfrak{g}_{\beta-\gamma}\mathfrak{g}_\alpha^2.$$

Overview of the elliptic sieve

$\mathcal{O}$ – prime ℓ

↓

$\exists \mathfrak{p}$ such that $\mathrm{Ord}(\chi(\mathfrak{p})) \nmid \nu_{\mathfrak{p}}(D_\ell)$ — # of such $\ell \gg X/\log X$

↓

$(\ell) = \mathrm{ann}(P \bmod \mathfrak{p})$, so $\mathfrak{p} \mid D_\ell$ — $\#\ell - \#\{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \mid D_1\}$

↓

$\ell \nmid \alpha$ (roughly) $\implies D_\alpha \in \mathrm{Ker}(\mathrm{Art}^{\mathfrak{m}}_{L/K})$ — What is the sieve criterion?

↓

sieve!

Sieve criterion

Therefore, now we have $\ell = \mathrm{ann}(P \bmod \mathfrak{p})$ for some $\mathfrak{p}$ with $\mathrm{Ord}(\chi(\mathfrak{p})) \nmid \nu_{\mathfrak{p}}(D_\ell)$ (i.e. D_ℓ fails the norm condition 'locally at $\mathfrak{p}$').

Lemma

Suppose $\ell \in \mathcal{O}$ and $\mathfrak{p} \subset \mathcal{O}_K$ are as above and $\mathfrak{p} \nmid D_1$. If $\alpha \in \mathcal{O}$ satisfies $\alpha \in (\ell)$ and

$$\left(\alpha \ell^{-1}\right) \mathcal{O}_K + \mathfrak{p} = \mathcal{O}_K \text{ (think it as } \mathfrak{p}\ell \nmid \alpha),$$

then D_α fails the norm condition 'locally at $\mathfrak{p}$'.

Sieve criterion

Therefore, now we have $\ell = \mathrm{ann}(P \bmod \mathfrak{p})$ for some $\mathfrak{p}$ with $\mathrm{Ord}(\chi(\mathfrak{p})) \nmid \nu_{\mathfrak{p}}(D_\ell)$ (i.e. D_ℓ fails the norm condition 'locally at $\mathfrak{p}$').

Lemma

Suppose $\ell \in \mathcal{O}$ and $\mathfrak{p} \subset \mathcal{O}_K$ are as above and $\mathfrak{p} \nmid D_1$. If $\alpha \in \mathcal{O}$ satisfies $\alpha \in (\ell)$ and

$$\left(\alpha \ell^{-1}\right) \mathcal{O}_K + \mathfrak{p} = \mathcal{O}_K \text{ (think it as } \mathfrak{p}\ell \nmid \alpha),$$

then D_α fails the norm condition 'locally at $\mathfrak{p}$'.

- Result about valuation of points: let $P \in E_1(K)$ and $\alpha \in \mathrm{End}(E)$, then $\nu_{\mathfrak{p}}\left([\alpha]P\right) \geq \nu_{\mathfrak{p}}(P) + \nu_{\mathfrak{p}}(\alpha)$, with equality if $\mathfrak{p} \nmid \alpha\mathcal{O}_K$.
- Apply this to $[\ell]P = [\alpha\ell^{-1}\ell]P$:

$$\nu_{\mathfrak{p}}([\alpha]P) = \nu_{\mathfrak{p}}\left(\alpha\ell^{-1}\right) + \nu_{\mathfrak{p}}\left([\ell]P\right) = \nu_{\mathfrak{p}}\left([\ell]P\right) \implies \nu_{\mathfrak{p}}(D_\alpha) = \nu(D_\ell).$$

Sieve criterion

Overall, we showed the following:

$$\begin{aligned}
&\#\{\alpha \in \mathcal{O} \colon |\alpha| \leq B, y(\alpha P) \text{ is an ideal norm from } L\} \\
&\ll \#\{\mathrm{Nm}_{F/\mathbb{Q}}(\alpha) \leq B \colon \alpha \in \mathcal{O}, \alpha \not\equiv 0 \bmod \ell \text{ for all } \ell \in \Lambda, \mathrm{Nm}_{F/\mathbb{Q}}(\ell) \leq B\} \\
&+ \#\{\mathrm{Nm}(\alpha \mathcal{O}_K) \leq B \colon \alpha \equiv 0 \bmod (\ell \mathfrak{p}) \mathcal{O}_K \text{ for some } \mathfrak{p} \text{ with } \mathrm{Nm}(\ell) \leq B\} \\
&= N_0(B) + N_1(B).
\end{aligned}$$

Sieve criterion

Overall, we showed the following:

$$\begin{aligned}
&\#\{\alpha \in \mathcal{O} \colon |\alpha| \leq B, y(\alpha P) \text{ is an ideal norm from } L\} \\
&\ll \#\{\mathrm{Nm}_{F/\mathbb{Q}}(\alpha) \leq B \colon \alpha \in \mathcal{O}, \alpha \not\equiv 0 \bmod \ell \text{ for all } \ell \in \Lambda, \mathrm{Nm}_{F/\mathbb{Q}}(\ell) \leq B\} \\
&+ \#\{\mathrm{Nm}(\alpha \mathcal{O}_K) \leq B \colon \alpha \equiv 0 \bmod (\ell \mathfrak{p}) \mathcal{O}_K \text{ for some } \mathfrak{p} \text{ with } \mathrm{Nm}(\ell) \leq B\} \\
&= N_0(B) + N_1(B).
\end{aligned}$$

- Using the proposition (for # of ℓ) and Selberg sieve (for number fields), we deduce that

$$N_0(B) \ll \frac{B}{(\log B)^{\omega(E,P,L)}} \exp\left(\#\{\mathfrak{p} \subset \mathcal{O}_K \colon \mathfrak{p} \mid D_1\}\right)$$

Sieve criterion

Overall, we showed the following:

$$\begin{aligned}
&\#\{\alpha \in \mathcal{O} \colon |\alpha| \leq B, y(\alpha P) \text{ is an ideal norm from } L\} \\
&\ll \#\{\mathrm{Nm}_{F/\mathbb{Q}}(\alpha) \leq B \colon \alpha \in \mathcal{O}, \alpha \not\equiv 0 \bmod \ell \text{ for all } \ell \in \Lambda, \mathrm{Nm}_{F/\mathbb{Q}}(\ell) \leq B\} \\
&+ \#\{\mathrm{Nm}(\alpha \mathcal{O}_K) \leq B \colon \alpha \equiv 0 \bmod (\ell \mathfrak{p})\mathcal{O}_K \text{ for some } \mathfrak{p} \text{ with } \mathrm{Nm}(\ell) \leq B\} \\
&= N_0(B) + N_1(B).
\end{aligned}$$

- Using the proposition (for # of ℓ) and Selberg sieve (for number fields), we deduce that

$$N_0(B) \ll \frac{B}{(\log B)^{\omega(E,P,L)}} \exp\left(\#\{\mathfrak{p} \subset \mathcal{O}_K \colon \mathfrak{p} \mid D_1\}\right)$$

- We claim that $\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{p}) \gg \mathrm{Nm}_{F/\mathbb{Q}}(\ell)$ (proved using Hasse's bound), then

$$N_1(B) \ll B \sum_{n \leq \log B} \frac{1}{n^{[K\colon F]+1}} \ll \frac{1}{[K\colon F]} \frac{B}{(\log B)^{[K\colon F]}}.$$

References

1. Au-Yeung, H. L. E. Explicit valuation of elliptic nets for elliptic curves with complex multiplication. Canadian Mathematical Communications. (2026). Vol 1. View online.
2. Bhakta, S. and Loughran, D. and R-M, S. L. and Nakahara, M. The elliptic sieve and Brauer groups. Proceedings of the London Mathematical Society. (2023). Vol. 126, no. 6, 1884–1922. View online.
3. Cox, D. Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. (2013). John Wiley & Sons, Inc. 2nd edition.
4. Kowalski, E. The Large Sieve and its Applications: Arithmetic Geometry, Random Walks and Discrete Groups. Cambridge University Press (2008). View online.
5. Landau, E. Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate. Archiv der Mathematik und Physik. (1908). Vol 13. pp 305–312. View online.
6. Stange, Katherine E. Elliptic nets and elliptic curves. (2011). Algebra Number Theory 5, no. 2, 197–229. View online
7. Streng, M. Divisibility sequences for elliptic curves with complex multiplication. (2008). Algebra & Number Theory, no. 2, 183-208. View online
8. Silverman, J. H. Advanced topics in the arithmetic of elliptic curves. Springer-Verlag (1994). View online.
9. Silverman, J. H. The arithmetic of elliptic curves. Springer-Verlag (2009). View online.