Elliptic Curve Class Pairings

Michael Griffin

Joint with Ken Ono and Wei-Lun Tsai

November 4, 2020

Integer Binary Quadratic Forms

$$Q(X,Y) = aX^2 + bXY + cY^2$$

- $a, b, c \in \mathbb{Z}$
- Positive definite: $a > 0$, discriminant $b^2 - 4ac < 0$.
- Primitive: $\mathrm{GCD}(a, b, c) = 1$

Integer Binary Quadratic Forms

- We say $Q_1 \sim Q_2$ if

$$Q_1(X, Y) = Q_2(aX + bY, cX + dY)$$

for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Integer Binary Quadratic Forms

- We say $Q_1 \sim Q_2$ if

$$Q_1(X, Y) = Q_2(aX + bY, cX + dY)$$

for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

- Equivalent forms represent the same integers.
- Dirichlet composition group law:

$$[Q_1(X, Y)] * [Q_2(X, Y)] = [Q_3(X, Y)]$$

Integer Binary Quadratic Forms

- We say $Q_1 \sim Q_2$ if
$$Q_1(X, Y) = Q_2(aX + bY, cX + dY)$$
for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.
- Equivalent forms represent the same integers.
- Dirichlet composition group law:
$$[Q_1(X, Y)] * [Q_2(X, Y)] = [Q_3(X, Y)]$$
- $\mathcal{Q}_D \simeq \mathrm{CL}(-D)$.
(Group of Equivalence classes for discriminant $-D$ is isomorphic to the ideal class group.)

The class number

- The class number

$$h(-D) = \#\mathrm{CL}(-D) = \#\mathcal{Q}_{-D}.$$

The class number

- The class number

$$h(-D) = \#\mathrm{CL}(-D) = \#\mathcal{Q}_{-D}.$$

Theorem (Siegel)

$$c_1 D^{1/2-\epsilon} < h(-D) < c_2 D^{1/2+\epsilon}.$$

The class number

- The class number

$$h(-D) = \#\mathrm{CL}(-D) = \#\mathcal{Q}_{-D}.$$

Theorem (Siegel)

$$c_1 D^{1/2-\epsilon} < h(-D) < c_2 D^{1/2+\epsilon}.$$

- Lower bound is completely inexplicit.

The class number

- Goldfeld and Gross–Zagier solved problem of finding an effective lower bound.

The class number

- Goldfeld and Gross–Zagier solved problem of finding an effective lower bound.

Theorem (Oesterlé)

$$h(-D) > \frac{1}{7000} \log D \prod_{\substack{p|D \text{ prime} \\ p \neq D}} \left(1 - \frac{\lfloor 2\sqrt{p} \rfloor}{p+1}\right).$$

Elliptic curves and quadratic twists

- $E/\mathbb{Q}$ is an elliptic curve

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

Elliptic curves and quadratic twists

- $E/\mathbb{Q}$ is an elliptic curve

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

- A *quadratic twist* of E is

$$E_D : Dy^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Elliptic curves and quadratic twists

- $E/\mathbb{Q}$ is an elliptic curve

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

- A *quadratic twist* of E is

$$E_D : Dy^2 = x^3 + a_2x^2 + a_4x + a_6.$$

- E and E_D are isomprophic over $\mathbb{Q}(\sqrt{D})$, but not over $\mathbb{Q}$.

Class Pairing

Theorem

Suppose $E/\mathbb{Q}$ has integer equation,

Class Pairing

Theorem

Suppose $E/\mathbb{Q}$ has integer equation, and $\Delta = dD$ is a factorization of a fundamental discriminant Δ into discriminants.

Class Pairing

Theorem

Suppose $E/\mathbb{Q}$ has integer equation, and $\Delta = dD$ is a factorization of a fundamental discriminant Δ into discriminants.
Then there is an explicit map

$$\Psi_{d,D} : E_d(\mathbb{Q}) \times E_D(\mathbb{Q}) \to CL(\Delta)$$

given below.

The Explicit Pairing

Fix $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E_d(\mathbb{Q})$, and $Q = (\frac{U}{W^2}, \frac{V}{W^3}) \in E_D(\mathbb{Q})$. Then

$$\Psi_{d,D}(P, Q) = \left[\frac{\alpha}{G}X^2 + LXY + \frac{L^2 - \Delta}{4\alpha/G}Y^2\right].$$

The Explicit Pairing

Fix $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E_d(\mathbb{Q})$, and $Q = (\frac{U}{W^2}, \frac{V}{W^3}) \in E_D(\mathbb{Q})$. Then

$$\Psi_{d,D}(P, Q) = \left[\frac{\alpha}{G} X^2 + LXY + \frac{L^2 - \Delta}{4\alpha/G} Y^2 \right].$$

- $\alpha = |AW^2 - UC^2|$

The Explicit Pairing

Fix $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E_d(\mathbb{Q})$, and $Q = (\frac{U}{W^2}, \frac{V}{W^3}) \in E_D(\mathbb{Q})$. Then

$$\Psi_{d,D}(P,Q) = \left[\frac{\alpha}{G}X^2 + LXY + \frac{L^2 - \Delta}{4\alpha/G}Y^2\right].$$

- $\alpha = |AW^2 - UC^2|$
- $G = \gcd(\alpha, B^2W^6, V^2C^6)$

The Explicit Pairing

Fix $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E_d(\mathbb{Q})$, and $Q = (\frac{U}{W^2}, \frac{V}{W^3}) \in E_D(\mathbb{Q})$. Then

$$\Psi_{d,D}(P, Q) = \left[\frac{\alpha}{G} X^2 + LXY + \frac{L^2 - \Delta}{4\alpha/G} Y^2 \right].$$

- $\alpha = |AW^2 - UC^2|$
- $G = \gcd(\alpha, B^2 W^6, V^2 C^6)$
- L is a unique integer $\mod 2\alpha/G$ such that

$$L \equiv d \frac{BW^3}{VC^3} \mod \frac{\alpha}{(\alpha, V^2 C^6))}$$

The Explicit Pairing

Fix $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E_d(\mathbb{Q})$, and $Q = (\frac{U}{W^2}, \frac{V}{W^3}) \in E_D(\mathbb{Q})$. Then

$$\Psi_{d,D}(P, Q) = \left[\frac{\alpha}{G} X^2 + LXY + \frac{L^2 - \Delta}{4\alpha/G} Y^2 \right].$$

- $\alpha = |AW^2 - UC^2|$
- $G = \gcd(\alpha, B^2 W^6, V^2 C^6)$
- L is a unique integer $\mod 2\alpha/G$ such that

$$\begin{aligned} L &\equiv d\frac{BW^3}{VC^3} \mod \frac{\alpha}{(\alpha, V^2C^6)} \\ &\equiv D\frac{VC^3}{BW^3} \mod \frac{\alpha}{(\alpha, B^2W^6)} \end{aligned}$$

The Explicit Pairing

Fix $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E_d(\mathbb{Q})$, and $Q = (\frac{U}{W^2}, \frac{V}{W^3}) \in E_D(\mathbb{Q})$.
Then

$$\Psi_{d,D}(P,Q) = \left[\frac{\alpha}{G}X^2 + LXY + \frac{L^2-\Delta}{4\alpha/G}Y^2\right].$$

- $\alpha = |AW^2 - UC^2|$
- $G = \gcd(\alpha, B^2W^6, V^2C^6)$
- L is a unique integer $\mod 2\alpha/G$ such that

$$\begin{aligned} L &\equiv d\frac{BW^3}{VC^3} \mod \frac{\alpha}{(\alpha, V^2C^6)} \\ &\equiv D\frac{VC^3}{BW^3} \mod \frac{\alpha}{(\alpha, B^2W^6)} \\ L^2 &\equiv \Delta \pmod{4\alpha/G} \end{aligned}$$

Variations

- Buell ('77): $d = 1$, $D = a_6$, and $Q = (0, 1)$

Variations

- Buell ('77): $d = 1$, $D = a_6$, and $Q = (0, 1)$
- Soleng ('94): $d = 1$, $Q = (n, 1)$.

Variations

- Buell ('77): $d = 1$, $D = a_6$, and $Q = (0, 1)$
- Soleng ('94): $d = 1$, $Q = (n, 1)$.
- G–Ono–Tsai ('20): $d = 1$

Variations

- Buell ('77): $d = 1$, $D = a_6$, and $Q = (0, 1)$
- Soleng ('94): $d = 1$, $Q = (n, 1)$.
- G–Ono–Tsai ('20): $d = 1$
- Blum–Choi–Hoey–Iskander–Lakein–Martinez (REU, '20): $d = 1$, $Q = (\frac{u}{w^2}, \frac{1}{w})$ with $w \mid D$.

Variations

- Buell ('77): $d = 1$, $D = a_6$, and $Q = (0, 1)$
- Soleng ('94): $d = 1$, $Q = (n, 1)$.
- G–Ono–Tsai ('20): $d = 1$
- Blum–Choi–Hoey–Iskander–Lakein–Martinez (REU, '20): $d = 1$, $Q = (\frac{u}{w^2}, \frac{1}{w})$ with $w \mid D$.

Buell, Soleng, and the REU showed their maps are linear in P.

Since $P \in E_d(\mathbb{Q})$ and $Q \in E_D(\mathbb{Q})$,

$$\begin{aligned} d\frac{B^2}{C^6} &= \frac{A^3}{C^6} + a_2\frac{A^2}{C^4} + a_4\frac{A}{C^2} + a_6 \\ D\frac{V^2}{W^6} &= \frac{U^3}{W^6} + a_2\frac{U^2}{W^4} + a_4\frac{U}{W^2} + a_6. \end{aligned}$$

Since $P \in E_d(\mathbb{Q})$ and $Q \in E_D(\mathbb{Q})$,

$$\begin{aligned} d\frac{B^2}{C^6} &= \frac{A^3}{C^6} + a_2\frac{A^2}{C^4} + a_4\frac{A}{C^2} + a_6 \\ D\frac{V^2}{W^6} &= \frac{U^3}{W^6} + a_2\frac{U^2}{W^4} + a_4\frac{U}{W^2} + a_6. \end{aligned}$$

Taking the difference:

$$d\frac{B^2}{C^6} - D\frac{V^2}{W^6} = \left(\frac{A^3}{C^6} - \frac{U^3}{W^6}\right) + a_2\left(\frac{A^2}{C^4} - \frac{U^2}{W^4}\right) + a_4\left(\frac{A}{C^2} - \frac{U}{W^2}\right)$$

Since $P \in E_d(\mathbb{Q})$ and $Q \in E_D(\mathbb{Q})$,

$$\begin{aligned} d\frac{B^2}{C^6} &= \frac{A^3}{C^6} + a_2\frac{A^2}{C^4} + a_4\frac{A}{C^2} + a_6 \\ D\frac{V^2}{W^6} &= \frac{U^3}{W^6} + a_2\frac{U^2}{W^4} + a_4\frac{U}{W^2} + a_6. \end{aligned}$$

Taking the difference:

$$d\frac{B^2}{C^6} - D\frac{V^2}{W^6} = \left(\frac{A^3}{C^6} - \frac{U^3}{W^6}\right) + a_2\left(\frac{A^2}{C^4} - \frac{U^2}{W^4}\right) + a_4\left(\frac{A}{C^2} - \frac{U}{W^2}\right)$$

Which gives

$$dB^2W^6 - DV^2C^6 \equiv 0 \pmod{AW^2 - UC^2}.$$

$$dB^2W^6 \equiv DV^2C^6 \pmod{\alpha}$$

$$dB^2W^6 \equiv DV^2C^6 \pmod{\alpha}$$

$$\left(d\frac{BW^3}{VC^3}\right)^2 \equiv dD \pmod{\frac{\alpha}{\gcd(V^2C^6, \alpha)}}$$

$$dB^2W^6 \equiv DV^2C^6 \pmod{\alpha}$$

$$\left(d\frac{BW^3}{VC^3}\right)^2 \equiv dD \pmod{\frac{\alpha}{\gcd(V^2C^6, \alpha)}}$$

$$\left(D\frac{VC^3}{BW^3}\right)^2 \equiv dD \pmod{\frac{\alpha}{\gcd(B^2W^6, \alpha)}}$$

$$dB^2W^6 \equiv DV^2C^6 \pmod{\alpha}$$

$$\left(d\frac{BW^3}{VC^3}\right)^2 \equiv dD \pmod{\frac{\alpha}{\gcd(V^2C^6, \alpha)}}$$

$$\left(D\frac{VC^3}{BW^3}\right)^2 \equiv dD \pmod{\frac{\alpha}{\gcd(B^2W^6, \alpha)}}$$

$$\left(d\frac{BW^3}{VC^3}\right)\left(D\frac{VC^3}{BW^3}\right) = dD$$

$$dB^2W^6 \equiv DV^2C^6 \pmod{\alpha}$$

$$\left(d\frac{BW^3}{VC^3}\right)^2 \equiv dD \pmod{\frac{\alpha}{\gcd(V^2C^6, \alpha)}}$$

$$\left(D\frac{VC^3}{BW^3}\right)^2 \equiv dD \pmod{\frac{\alpha}{\gcd(B^2W^6, \alpha)}}$$

$$\left(d\frac{BW^3}{VC^3}\right)\left(D\frac{VC^3}{BW^3}\right) = dD$$

$$\left(d\frac{BW^3}{VC^3}\right) \equiv \left(D\frac{VC^3}{BW^3}\right) \pmod{\alpha/G}$$

Question?

When are the classes different?

When are the classes different?

Proposition

Let $\Delta < 0$. *Suppose* $Q_1, Q_2 \in \mathcal{Q}_\Delta$ *with*

$$
\begin{aligned}
Q_1(X, Y) &= A_1 X^2 + B_1 XY + \frac{B_1^2 - \Delta}{4A_1} Y^2 \\
Q_2(X, Y) &= A_2 X^2 + B_2 XY + \frac{B_2^2 - \Delta}{4A_2} Y^2
\end{aligned}
$$

and $Q_1 \sim Q_2$. *Then either* $A_1 = A_2$

When are the classes different?

Proposition

Let $\Delta < 0$. *Suppose* $Q_1, Q_2 \in \mathcal{Q}_\Delta$ *with*

$$\begin{aligned} Q_1(X,Y) &= A_1X^2 + B_1XY + \frac{B_1^2 - \Delta}{4A_1}Y^2 \\ Q_2(X,Y) &= A_2X^2 + B_2XY + \frac{B_2^2 - \Delta}{4A_2}Y^2 \end{aligned}$$

and $Q_1 \sim Q_2$. *Then either* $A_1 = A_2$ *or* $A_1A_2 \geq \left|\frac{\Delta}{4}\right|$.

When are the classes different?

- Suppose $Q_2(X, Y) = Q_1(aX + bY, cX + dY)$.

When are the classes different?

- Suppose $Q_2(X, Y) = Q_1(aX + bY, cX + dY)$.
- The leading term is (X=1,Y=0)

$$A_2 = Q_1(a, c).$$

When are the classes different?

- Suppose $Q_2(X, Y) = Q_1(aX + bY, cX + dY)$.
- The leading term is (X=1,Y=0)

$$A_2 = Q_1(a, c).$$

- If $c = 0$, then $a = \pm 1$, so $A_1 = A_2$.

When are the classes different?

- Suppose $Q_2(X, Y) = Q_1(aX + bY, cX + dY)$.
- The leading term is (X=1,Y=0)

$$A_2 = Q_1(a, c).$$

- If $c = 0$, then $a = \pm 1$, so $A_1 = A_2$.
- Otherwise,

$$A_2 = Q_1(a, c) \quad = \quad A_1 a^2 + B_1 ac + \frac{B_1^2 - \Delta}{4A_1} c^2$$

When are the classes different?

- Suppose $Q_2(X, Y) = Q_1(aX + bY, cX + dY)$.
- The leading term is (X=1,Y=0)

$$A_2 = Q_1(a, c).$$

- If $c = 0$, then $a = \pm 1$, so $A_1 = A_2$.
- Otherwise,

$$\begin{aligned} A_2 = Q_1(a, c) &= A_1 a^2 + B_1 ac + \frac{B_1^2 - \Delta}{4A_1} c^2 \\ &= \frac{1}{A_1}\left(\left(A_1 a + \frac{B_1}{2} c\right)^2 - \frac{\Delta}{4} c^2\right) \end{aligned}$$

When are the classes different?

- Suppose $Q_2(X,Y) = Q_1(aX + bY, cX + dY)$.
- The leading term is (X=1,Y=0)

$$A_2 = Q_1(a,c).$$

- If $c = 0$, then $a = \pm 1$, so $A_1 = A_2$.
- Otherwise,

$$\begin{aligned} A_2 = Q_1(a,c) &= A_1 a^2 + B_1 ac + \frac{B_1^2 - \Delta}{4A_1} c^2 \\ &= \frac{1}{A_1}\left(\left(A_1 a + \frac{B_1}{2} c\right)^2 - \frac{\Delta}{4} c^2\right) \\ &\geq \frac{|\Delta|}{4A_1}. \end{aligned}$$

Class number bounds

Theorem (G–Ono, G–Ono–Tsai)

Let $E : y^2 = x^3 + a_2x^4 + a_4x + a_6$, *have rank* r,

Class number bounds

Theorem (G–Ono, G–Ono–Tsai)

Let $E: y^2 = x^3 + a_2x^4 + a_4x + a_6$, have rank r, and $-D < 0$ a fundamental discriminant so that there is a "suitable" point $Q \in E_{-D}$.

Class number bounds

Theorem (G–Ono, G–Ono–Tsai)

Let $E : y^2 = x^3 + a_2x^4 + a_4x + a_6$, *have rank* r*,and* $-D < 0$ *a fundamental discriminant so that there is a "suitable" point* $Q \in E_{-D}$. *Then the class number satisfies*

$$h(-D) \geq \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{2^{r+1}\sqrt{R_{\mathbb{Q}}(E)}}\Omega_r(\log D)^{\frac{r}{2}} - \varepsilon(Q, E)(\log D)^{\frac{r-1}{2}}$$

- If $r \geq 3$, this beats the Gross–Zagier bound.

$$h(-D) \geq \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{2^{r+1}\sqrt{R_{\mathbb{Q}}(E)}}\Omega_r(\log D)^{\frac{r}{2}} - \varepsilon(Q, E)(\log D)^{\frac{r-1}{2}}$$

$$h(-D) \geq \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{2^{r+1}\sqrt{R_{\mathbb{Q}}(E)}}\Omega_r(\log D)^{\frac{r}{2}} - \varepsilon(Q,E)(\log D)^{\frac{r-1}{2}}$$

Here:

- $E_{\mathrm{tor}}(\mathbb{Q})$ is the torsion subgroup.

$$h(-D) \geq \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{2^{r+1}\sqrt{R_{\mathbb{Q}}(E)}}\Omega_r(\log D)^{\frac{r}{2}} - \varepsilon(Q, E)(\log D)^{\frac{r-1}{2}}$$

Here:

- $E_{\mathrm{tor}}(\mathbb{Q})$ is the torsion subgroup.
- $R_{\mathbb{Q}}(E)$ is the regulator.

$$h(-D) \geq \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{2^{r+1}\sqrt{R_{\mathbb{Q}}(E)}}\Omega_r(\log D)^{\frac{r}{2}} - \varepsilon(Q,E)(\log D)^{\frac{r-1}{2}}$$

Here:

- $E_{\mathrm{tor}}(\mathbb{Q})$ is the torsion subgroup.
- $R_{\mathbb{Q}}(E)$ is the regulator.
- Ω_r is the volume of the unit ball in $\mathbb{R}^r$:

$$\Omega_r = \frac{\pi^{r/2}}{\Gamma(\frac{r}{2}+1)}.$$

$$h(-D) \geq \frac{|E_{\mathrm{tor}}(\mathbb{Q})|}{2^{r+1}\sqrt{R_{\mathbb{Q}}(E)}}\Omega_r(\log D)^{\frac{r}{2}} - \varepsilon(Q,E)(\log D)^{\frac{r-1}{2}}$$

Here:

- $E_{\mathrm{tor}}(\mathbb{Q})$ is the torsion subgroup.
- $R_{\mathbb{Q}}(E)$ is the regulator.
- Ω_r is the volume of the unit ball in $\mathbb{R}^r$:

$$\Omega_r = \frac{\pi^{r/2}}{\Gamma(\frac{r}{2}+1)}.$$

- The error term is $\varepsilon(Q,E)$ is explicit.

Class number bounds

- To prove, we need to count points with $\alpha = |AW^2 - UC^2|$ "small."

Class number bounds

- To prove, we need to count points with $\alpha = |AW^2 - UC^2|$ "small."
- Use theory of heights.

Heights

Let $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E(\mathbb{Q})$.

- The "Naive" height is

$$H(P) = \max(|A|, |C^2|).$$

Heights

Let $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E(\mathbb{Q})$.

- The "Naive" height is

$$H(P) = \max(|A|, |C^2|).$$

- The Weil (or logarithmic) height is

$$h_W(P) = \log H(P)$$

Heights

Let $P = (\frac{A}{C^2}, \frac{B}{C^3}) \in E(\mathbb{Q})$.

- The "Naive" height is
$$H(P) = \max(|A|, |C^2|).$$
- The Weil (or logarithmic) height is
$$h_W(P) = \log H(P)$$
- The canonical height is
$$\widehat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{h_W(nP)}{n^2}.$$

The canonical height

Properties

- $\widehat{h}(P) = 0$ if and only if P is a torsion point.

The canonical height

Properties

- $\widehat{h}(P) = 0$ if and only if P is a torsion point.
- Parallelogram law:

$$\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q)$$

The canonical height

Properties

- $\widehat{h}(P) = 0$ if and only if P is a torsion point.
- Parallelogram law:
$$\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q)$$
- There is a bound δ_E so that
$$\left|\widehat{h}(P) - \tfrac{1}{2}h_W(P)\right| < \delta_E.$$

Geometric map

The Point Lattice of $E(\mathbb{Q})$

There is a **linear** map $\phi : E(\mathbb{Q}) \to \Lambda \subseteq \mathbb{R}^r$ so that

- Λ is a lattice of full rank.

Geometric map

The Point Lattice of $E(\mathbb{Q})$

There is a **linear** map $\phi : E(\mathbb{Q}) \to \Lambda \subseteq \mathbb{R}^r$ so that

- Λ is a lattice of full rank.
- $\|\phi(P)\|^2 = \widehat{h}(P)$.

Geometric map

The Point Lattice of $E(\mathbb{Q})$

There is a **linear** map $\phi : E(\mathbb{Q}) \to \Lambda \subseteq \mathbb{R}^r$ so that

- Λ is a lattice of full rank.
- $\|\phi(P)\|^2 = \widehat{h}(P)$.
- $$\phi(P) \cdot \phi(Q) \quad = \quad < P, Q >$$

Geometric map

The Point Lattice of $E(\mathbb{Q})$

There is a **linear** map $\phi : E(\mathbb{Q}) \to \Lambda \subseteq \mathbb{R}^r$ so that

- Λ is a lattice of full rank.
- $\|\phi(P)\|^2 = \widehat{h}(P)$.
- $$\begin{aligned} \phi(P) \cdot \phi(Q) &= < P, Q > \\ &= \frac{1}{2}\left(\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)\right). \end{aligned}$$

Geometric map

The Point Lattice of $E(\mathbb{Q})$

There is a **linear** map $\phi : E(\mathbb{Q}) \to \Lambda \subseteq \mathbb{R}^r$ so that

- Λ is a lattice of full rank.
- $\|\phi(P)\|^2 = \widehat{h}(P)$.
- $$\begin{aligned} \phi(P)\cdot\phi(Q) &= < P, Q > \\ &= \frac{1}{2}\left(\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)\right). \end{aligned}$$
- If $\mathcal{P}$ is any fundamental parallelepiped of Λ

Geometric map

The Point Lattice of $E(\mathbb{Q})$

There is a **linear** map $\phi : E(\mathbb{Q}) \to \Lambda \subseteq \mathbb{R}^r$ so that

- Λ is a lattice of full rank.
- $\|\phi(P)\|^2 = \widehat{h}(P)$.
- $$\begin{aligned} \phi(P) \cdot \phi(Q) &= \ < P, Q > \\ &= \tfrac{1}{2}\left(\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)\right). \end{aligned}$$
- If $\mathcal{P}$ is any fundamental parallelepiped of Λ

$$\mathrm{Vol}(\mathcal{P}) = \sqrt{R_Q(E)}$$

Geometric map

The Point Lattice of $E(\mathbb{Q})$

There is a **linear** map $\phi : E(\mathbb{Q}) \to \Lambda \subseteq \mathbb{R}^r$ so that

- Λ is a lattice of full rank.
- $\|\phi(P)\|^2 = \widehat{h}(P)$.
- $$\begin{aligned} \phi(P) \cdot \phi(Q) &= < P, Q > \\ &= \frac{1}{2}\left(\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)\right). \end{aligned}$$
- If $\mathcal{P}$ is any fundamental parallelepiped of Λ
$$\mathrm{Vol}(\mathcal{P}) = \sqrt{R_Q(E)}$$
- The kernel of ϕ is $E_{\mathrm{tor}}(\mathbb{Q})$.

- Want to count points $P \in E(\mathbb{Q})$ with

$$|AW^2 - UC^2| \leq \sqrt{|D|/4}.$$

- Want to count points $P \in E(\mathbb{Q})$ with

$$|AW^2 - UC^2| \leq (|u| + w^2)H(P) \leq \sqrt{|D|/4}.$$

- Almost same as counting points with $\widehat{h}(P) < T$ with

$$T = \frac{1}{4} \log \left| \frac{D}{4(|u| + w^2)^2} \right| - \delta_E.$$

- Same as counting $|E_{\mathrm{tor}}(\mathbb{Q})| \cdot \# \left(\mathbf{v} \in \Lambda \cap B(\sqrt{T}) \right),$

Lattice counting

Standard lattice counting arguments give

$$\begin{aligned}\#\left(\mathbf{v} \in \Lambda \cap B(\sqrt{T})\right) &\sim \frac{\Omega_r}{2^r \mathrm{Vol}(\mathcal{P})} \\ &= \frac{\Omega_r}{2^r \sqrt{R_{\mathbb{Q}}(E)}} T^{r/2} - O(T^{\frac{r-1}{2}}),\end{aligned}$$

Lattice counting

Standard lattice counting arguments give

$$\begin{aligned}\#\left(\mathbf{v} \in \Lambda \cap B(\sqrt{T})\right) &\sim \frac{\Omega_r}{2^r \mathrm{Vol}(\mathcal{P})} \\ &= \frac{\Omega_r}{2^r \sqrt{R_{\mathbb{Q}}(E)}} T^{r/2} - O(T^{\frac{r-1}{2}}),\end{aligned}$$

With explicit error terms.

Minimal heights

We can reverse the process above to bound the height of a non-torsion point in terms of a known class number:

Minimal heights

We can reverse the process above to bound the height of a non-torsion point in terms of a known class number:

Theorem (G–Ono–Tsai)

Suppose $P \in E(\mathbb{Q})$ is a point of infinite order.

Minimal heights

We can reverse the process above to bound the height of a non-torsion point in terms of a known class number:

Theorem (G–Ono–Tsai)

Suppose $P \in E(\mathbb{Q})$ is a point of infinite order. Let $-D$ is a fundamental discriminant so that E_{-D} has a "suitable" point $Q = (t, 1)$.

Minimal heights

We can reverse the process above to bound the height of a non-torsion point in terms of a known class number:

Theorem (G–Ono–Tsai)

Suppose $P \in E(\mathbb{Q})$ is a point of infinite order. Let $-D$ is a fundamental discriminant so that E_{-D} has a "suitable" point $Q = (t, 1)$. Then

$$\widehat{h} \geq \frac{|E_{\mathrm{tor}}(\mathbb{Q})|^2}{(h(-D) + |E_{\mathrm{tor}}(\mathbb{Q})|)^2} \left(\log\left(\frac{D}{4(t+1)^2} \right) - 4\delta(E) \right).$$

Previous lower bounds on $\widehat{h}(P)$

- Anderson and Masser ('80):

$$\widehat{h}(P) \geq \frac{\gamma_E}{\log(3)^6}$$

where γ is computable in terms of the Weierstrass $\wp$ and σ.

Previous lower bounds on $\widehat{h}(P)$

- Anderson and Masser ('80):

$$\widehat{h}(P) \geq \frac{\gamma_E}{\log(3)^6}$$

where γ is computable in terms of the Weierstrass $\wp$ and σ.

- Autissier, Hindry, and Pazuki ('18):

$$\widehat{h}(P) \geq c\frac{|E_{\mathrm{tor}}|^2}{h\log(3)^2}\log(3h)^{4/3}$$

where c is absolute, and $h = \max(1, h_W(J(E))$.

Previous lower bounds on $\widehat{h}(P)$

- Anderson and Masser ('80):

$$\widehat{h}(P) \geq \frac{\gamma_E}{\log(3)^6}$$

where γ is computable in terms of the Weierstrass $\wp$ and σ.

- Autissier, Hindry, and Pazuki ('18):

$$\widehat{h}(P) \geq c \frac{|E_{\mathrm{tor}}|^2}{h \log(3)^2} \log(3h)^{4/3}$$

where c is absolute, and $h = \max(1, h_W(J(E)))$.

- In general all these bounds are orders of magnitude smaller than the truth.

Linearity

- Buell and Soleng proved their maps were linear using Dirichlet composition.
- The REU group proved linearity for their map using Bhargava cubes.

Linearity

Theorem

REU Group Let $E/\mathbb{Q}$ be an elliptic curve and $-D$ a negative fundamental discriminant so that $E_D(\mathbb{Q})$ has a "suitable" point Q. Then the map

$$\Psi_{1,-D}(\ ,Q) : E(\mathbb{Q}) \to CL(-D)$$

is linear.

Linearity

Theorem

REU Group Let $E/\mathbb{Q}$ be an elliptic curve and $-D$ a negative fundamental discriminant so that $E_D(\mathbb{Q})$ has a "suitable" point Q. Then the map

$$\Psi_{1,-D}(\ ,Q) : E(\mathbb{Q}) \to CL(-D)$$

is linear.

- Uses Bhargava cubes rather than Dirichlet composition.

Linearity

Theorem

REU Group Let $E/\mathbb{Q}$ be an elliptic curve and $-D$ a negative fundamental discriminant so that $E_D(\mathbb{Q})$ has a "suitable" point Q. Then the map

$$\Psi_{1,-D}(\ ,Q) : E(\mathbb{Q}) \to CL(-D)$$

is linear.

- Uses Bhargava cubes rather than Dirichlet composition.
- Under certain conditions $E_{\mathrm{tor}}(\mathbb{Q})$ injects into $\mathrm{CL}(-D)$.

Corollary

Assume the hypotheses of the theorem. Then there are infinite families of class groups $CL(-D)$ with subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $2 \leq n \leq 8$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $1 \leq n \leq 3$.

Results

- Generalized pairing

$$\Psi_{d,D} : E_d(\mathbb{Q}) \times E_D(\mathbb{Q}) \to \mathrm{CL}(dD)$$

Results

- Generalized pairing

$$\Psi_{d,D} : E_d(\mathbb{Q}) \times E_D(\mathbb{Q}) \to \mathrm{CL}(dD)$$

- Explicit lower bounds on class numbers.

Results

- Generalized pairing

$$\Psi_{d,D} : E_d(\mathbb{Q}) \times E_D(\mathbb{Q}) \to \mathrm{CL}(dD)$$

- Explicit lower bounds on class numbers.
- Lower bounds on Non-trivial heights.

Results

- Generalized pairing

$$\Psi_{d,D} : E_d(\mathbb{Q}) \times E_D(\mathbb{Q}) \to \mathrm{CL}(dD)$$

- Explicit lower bounds on class numbers.
- Lower bounds on Non-trivial heights.
- Explicit subgroups of the class group. (REU)

Thank You!