Bounding class numbers using elliptic curves

Corijn Rudrum

October 17, 2023

The introduction is based on [Gol85], and the second part on [GO20]. See also my master's thesis.

1 Bedtime mathematics

Theorem 1.1 (Euler, 1772)**.**

$$x^2 - x + 41 = \textit{ prime}, \qquad \textit{for } x = 1, 2, \ldots, 40.$$

Theorem 1.2 (Rabinovitch, 1913)**.** *For $D < 0$, $D \equiv 1 \pmod 4$,*

$$x^2 - x + \frac{1 + |D|}{4} = \textit{ prime}, \qquad \textit{for } x = 1, 2, \ldots, \frac{|D| - 3}{4},$$

if and only if elements of $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ factorize uniquely as a product of primes, i.e. $\mathrm{Cl}(\mathbb{Q}(\sqrt{D})) = \{1\}$

Euler's result follows from the fact that $\mathbb{Q}(\sqrt{-163})$ has class number 1.
Can we do better? Gauss class number one problem.
Gauss considered class groups not in terms of ideals but of binary quadratic forms.

Definition 1.3. A binary quadratic form over $\mathbb{Z}$ is a homogeneous polynomial

$$F(X, Y) = aX^2 + bXY + cY^2, \qquad a, b, c \in \mathbb{Z}.$$

The *discriminant* of F is $D = b^2 - 4ac$. If $D < 0$, then F is called *positive definite* if $a > 0$. In that case $F(x, y) \geq 0$ for all $(x, y) \in \mathbb{Z}^2$ with equality only at $(0, 0)$.

There is an action by $\mathrm{SL}_2(\mathbb{Z})$ on the set of binary quadratic forms over $\mathbb{Z}$ by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} F(X, Y) = F(\alpha X + \beta Y, \gamma X + \delta Y),$$

preserving the discriminant and positive definiteness. We say that two forms are equivalent if they lie in the same orbit under this action.

Definition 1.4. An integer $D \in \mathbb{Z}$ is called a *fundamental discriminant* if it is the discriminant of a quadratic number field. Equivalently, $D \neq 1$ and either

- $D \equiv 1 \pmod 4$ and D square-free, or

- $D \equiv 0 \pmod 4$ and $D/4$ square-free and $D/4 \equiv 2$ or $3 \pmod 4$.

Theorem 1.5. *For a given fundamental discriminant D, the equivalence classes of positive definite forms of discriminant D form a finite abelian group. (Gauss, 1801)*
If $D < 0$, then this group is isomorphic to the ideal class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$

We let $h(D)$ denote the order of this group.

Conjecture 1.6. *(Gauss, 1801) We have $h(D) \to \infty$ as $D \to -\infty$.*

Gauss class number one problem: if $D < 0$ and $h(D) = 1$, show that

$$D \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}. \tag{1.1}$$

This turned out to be very hard problem. Gauss' conjecture was proven by Hecke, Deuring and Heilbronn in the early 20th century, by proving that both correctness and falsity of the generalized Riemann hypothesis implied it!

Theorem 1.7 (Siegel, 1934)**.** *For every $\varepsilon > 0$ there exists a constant c (ineffective) such that*

$$h(D) > c|D|^{\frac{1}{2}-\varepsilon}.$$

But, due to the ineffectivity of these results, the class number one problem was still open! The first full proof that the list in (1.1) is complete was given by Baker in 1966, using his theory of linear forms in logarithms. Heegner, with a completely different method, was over a decade earlier, but his paper contained some mistakes. The state-of-the art effective lower bound for $h(D)$ is as follows:

Theorem 1.8 (Goldfeld–Gross–Zagier, 1983)**.** *For every $\varepsilon > 0$ there exists an effectively computable constant c such that*

$$h(D) > c(\log D)^{1-\varepsilon}.$$

Note that this lower bound is asymptotically much weaker than the one given by Siegel, so there is room for improvement. In this presentation, we will improve on this bound for certain families of discriminants following [GO20].

2 From elliptic curves to class groups

Take an elliptic curve

$$E : y^2 = x^3 + a_4x + a_6, \qquad a_4, a_6 \in \mathbb{Z},$$

with rank $r \geq 1$.

We will consider fundamental discriminants in the family

$$D_E(t) = -4(t^3 + a_4t - a_6). \tag{2.1}$$

Note that $D_E(t)$ is not a fundamental discriminant for all $t \in \mathbb{Z}_{>0}$. We just consider discriminants that happen to be of this form for some positive integer t. Note that $D_E(t)$ is a fundamental discriminant if and only if $t^3 + a_4t - a_6$ is square-free and not equivalent to 3 (mod 4). Erdös proved in [Erd53, Theorem 1.1] that $t^3 + a_4t - a_6$ is square-free for infinitely many $t \in \mathbb{Z}_{>0}$. If we want to be absolutely sure that there exist fundamental discriminants of the form (2.1), we could put some congruence conditions on a_4 and a_6 modulo 4.

The aim of the rest of this talk is to prove the following theorem:

Theorem 2.1. *There exists an effectively computable constant $c(E)$, such that: for every $\varepsilon > 0$ there is an effectively computable constant $N(E, \varepsilon)$, such that: if $t \geq N(E, \varepsilon)$ and $D = D_E(t)$ is a fundamental discriminant, then*

$$h(D) \geq c(E)(1-\varepsilon)(\log(D))^{\frac{r}{2}}$$

Let $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ be any affine rational point. Then P is of the form

$$P = \left(\frac{A}{C^2}, \frac{B}{C^3}\right), \qquad A, B, C \in \mathbb{Z}, \ \gcd(A, C) = \gcd(B, C) = 1$$

We define

$$\alpha(t) = |A + tC^2|$$

Theorem 2.2 ([GO20, Theorem 2.1])**.** *Evaluate $t \in \mathbb{Z}_{\geq 0}$ such that $D = D_E(t)$ is a negative fundamental discriminant. Then there exist infinitely many integers ℓ for which*

$$F_P(X, Y) = \alpha X^2 + \frac{2B + \alpha\ell}{C^3} XY + \frac{(2B + \alpha\ell)^2 - C^6 D}{4C^6\alpha} Y^2$$

is a discriminant D positive definite binary quadratic form over $\mathbb{Z}$. Further, the choice of ℓ does not affect its $\mathrm{SL}_2(\mathbb{Z})$-equivalence class $[F_P]$.

By Theorem 1.5, this gives us a map

$$\Psi : E(\mathbb{Q}) \to \mathrm{Cl}(\mathbb{Q}(\sqrt{D})), \qquad P \longmapsto [F_P].$$

Group homomorphism (at least on a subgroup of $E(\mathbb{Q})$)! (but we're not going to use that).

To give a lower bound for the class number, we want to know which points get mapped to distinct elements in the class group.

Theorem 2.3. *Let E be given (with explicit generators of $E(\mathbb{Q})$). Then there exists an effectively computable constant $N \in \mathbb{Z}$ and an effectively computable function $\tau_E(t) : \mathbb{Z} \to \mathbb{R}_{>0}$ such that, if $t \geq N$ and $P_1, P_2 \in E(\mathbb{Q})$ satisfy $\hat{h}(P_1), \hat{h}(P_2) \leq \tau_E(t)$ and $P_1 \neq \pm P_2$, then*

$$\Psi(P_1) \neq \Psi(P_2).$$

So, to give a lower bound for the class number we just need a lower bound for the number of points in $E(\mathbb{Q})$ with canonical height below a certain bound. This is easy! Because, in a sense, it just comes down to counting lattice points contained in an r-dimensional ball (r rank of E).

The canonical height $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ measures the "complexity" of a rational point. In particular, we have

$$\hat{h}([m]P) = m^2 \hat{h}(P).$$

The canonical height of a torsion point is 0, and it is well-defined on the quotient $\Lambda = E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$. Every point in Λ corresponds to $|E(\mathbb{Q})_{\mathrm{tors}}|$ points on $E(\mathbb{Q})$ of the same canonical height.

We have the *height pairing* $\langle \cdot, \cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$

$$\langle P, Q \rangle = \tfrac{1}{2}(\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)).$$

This is a positive definite bilinear form and satisfies $\langle P, P \rangle = \hat{h}(P)$.

We have

$$\Lambda \cong \mathbb{Z}^r.$$

and therefore

$$E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R} \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^r$$

which contains Λ.

Theorem 2.4. *The pairing $\langle \cdot, \cdot \rangle$ extends uniquely to an inner product on $\Lambda \otimes \mathbb{R}$.*

So we can think of Λ as a lattice inside r-dimensional Euclidean space. The distance of a point to the origin, is exactly the square root of its canonical height.

(Draw picture for counting points of bounded height).

Combining everything, we get

Theorem 2.5. *There exists an effectively computable constant $c(E)$, such that: for every $\varepsilon > 0$ there is an effectively computable constant $N(E, \varepsilon)$, such that: if $t \geq N(E, \varepsilon)$ and $D = D_E(t)$ is a fundamental discriminant, then*

$$h(D) \geq c(E)(1 - \varepsilon)(\log(D))^{\frac{r}{2}}$$

Example 2.6. Take

$$E : y^2 = x^3 - 16x + 1$$

or rank $r = 3$. Then for large enough discriminants of the form

$$D_E(t) = -4(t^3 - 16t - 1)$$

we have

$$h(D) \geq \frac{1}{20}(\log |D|)^{\frac{3}{2}}.$$

$\diamondsuit$

References

[Erd53] Paul Erdös. Arithmetical properties of polynomials. *J. London Math. Soc.*, 28:416–425, 1953.

[GO20] Michael Griffin and Ken Ono. Elliptic curves and lower bounds for class numbers. *J. Number Theory*, 214:1–12, 2020.

[Gol85] Dorian Goldfeld. Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)*, 13(1):23–37, 1985.