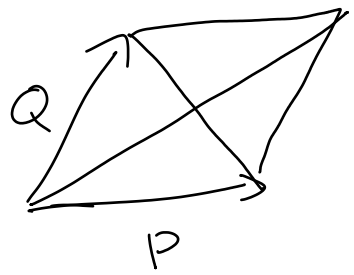
Cor 2.4.5 (Parallelogram law)

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

Pf Apply theorem to nP, nQ. Divide by n^2. Take $n \to \infty$. □



Cor 2.4.6 $\hat{h} : E(\bar{K}) \to \mathbb{R}$ is a quadratic form:

$$\langle \cdot, \cdot \rangle : E(\bar{K}) \times E(\bar{K}) \to \mathbb{R}$$
$$(P, Q) \mapsto \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$$

is bilinear.

Pf HW. "□"

Final paper

7 - 10 pages

Due May 7 at 1:59pm (ET)

Draft: ~ May 2 (optional, but highly recommended!)

Some ideas for topics:

- Elliptic curves over $\mathbb{C}$

  $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for a rank 2 lattice Λ in $\mathbb{C}$

  (cf. Silverman-Tate, II.2 or Silverman, V)

- Complex multiplication:

  Class field theory over imaginary quadratic number fields has to do with elliptic curves over $\mathbb{C}$.

- Abelian varieties over $\mathbb{C}$

  $A(\mathbb{C}) \cong \mathbb{C}^g / \Lambda$ for a rank $2g$ lattice Λ in $\mathbb{C}^g$

  such that is a positive definite hermitian form $\langle \cdot, \cdot \rangle$ on $\mathbb{C}^g$ with $\langle a, b \rangle \in \mathbb{Z} \ \forall a, b \in \Lambda$.

- Nagell-Lutz theorem:

  "Torsion points have integral x and y-coordinate in the affine chart with $z = 1$."

- Bombieri-Lang conjecture (higher-dimensional generalisation of Faltings's theorem),

  Erdős-Ulam problem

  (Is there a dense subset S of $\mathbb{R}^2$ for the Euclidean topology s.t. $d(x, y) \in \mathbb{Q} \ \forall x, y \in S$?)

- Algorithms on ell. curves (chapter III in Cremona, Algorithms for ell. curves)
- Elliptic curve factorisation algorithm

2.5. The Mordell-Weil Theorem

M-W Thm Let E be an ell. curve over a number field K. Then, the group $E(K)$ is finitely generated.

Cor $E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$ for some $r \geq 0$

called the rank of E over K.

$E(K)_{tors}$ is finite!

Rmk Isogenous ell. curves have the same ranks.

Pf Let $\phi : E_1 \to E_2$ be a nonzero isogeny (def. over K).

$$\begin{array}{ccc} \phi : & E_1(K) & \longrightarrow E_2(K) \\ & \| & \| \\ & E_1(K)_{tors} \times \mathbb{Z}^{r_1} & E_2(K)_{tors} \times \mathbb{Z}^{r_2} \end{array}$$

has finite kernel (of size $\leq \deg(\phi)$).

$\Rightarrow r_1 \leq r_2$

The dual isogeny $\hat{\phi} : E_2 \to E_1$ shows that $r_2 \leq r_1$.

$\square$

Weak M-W Thm

Let K be a number field and $\phi: E_1 \to E_2$ be a nonzero isogeny between ell. curves over K with $\ker(\phi) \subseteq E_1(K)$. Then, the group $E_2(K)/\phi(E_1(K))$ is finite.

Pf that weak M-W implies M-W (Descent argument)

Pick $m \geq 2$ and consider the mult. by m isogeny $[m]: E \to E$. ($\rightsquigarrow$ m-descent)

We have $\ker([m]) = E[m] \subseteq E(L)$ for some finite field ext. L/K. Since any subgroup ($E(K)$) of any fin. gen. grp. ($E(L)$), we can assume that $E[m] \subseteq E(K)$.

By weak M-W, the group

$$E(K)/mE(K) \text{ is finite.}$$

Let $Q_1, \dots, Q_a \in E(K)$ be coset representatives.

Recall that for any $T \in \mathbb{R}$, the set

$$S_T := \{P \in E(K) \mid \underbrace{\hat{h}(P)}_{\approx h(P)} \leq T\} \text{ is finite.}$$

Let G_T be the subgroup of $E(K)$ generated by $Q_1, \dots, Q_a$ and the elements of S_T.

We want to show that $G_T = E(K)$ for sufficiently large T.

Assume $P \in E(K) \setminus G_T$ with minimal $\hat{h}(P)$.

Let Q_i lie in the same coset as P, so we can write

$$P = Q_i + mP' \quad \text{for some } P' \in E(K).$$

Note that $P' \in E(K) \setminus G_T$, $P \pm Q_i \in E(K) \setminus G_T$

$$\hat{h}(P - Q_i) + \underbrace{\hat{h}(P + Q_i)}_{\geq \hat{h}(P) \text{ by assumption}} = 2(\hat{h}(P) + \hat{h}(Q_i))$$

$$\Rightarrow \hat{h}(P - Q_i) \leq \hat{h}(P) + 2\hat{h}(Q_i)$$

$$\hat{h}(mP') = m^2 \hat{h}(P') \geq m^2 \hat{h}(P) \quad \text{(by assumption)}$$

$$\Rightarrow \hat{h}(P) \leq \frac{2}{m^2 - 1} \cdot \hat{h}(Q_i).$$

$\Rightarrow$ If we choose

$$T \geq \underbrace{\frac{2}{m^2-1} \cdot \max(\hat{h}(Q_1), \dots, \hat{h}(Q_a))}_{\text{indep. of } P},$$

then $P \in S_T \subseteq G_T$. $\lightning$

□

Rmk $E(K) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^r$

because $P \otimes 1 = \underbrace{nP}_{O} \otimes \frac{1}{n} = O$ if $nP = O$.

Thm 2.5.1 The quadratic form $\hat{h}$ on $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$ defined by $\hat{h}(\sum P_i \otimes a_i) = \sum_{i,j} \langle P_i, P_j \rangle a_i a_j$

(so $\langle \sum P_i \otimes a_i, \sum Q_j \otimes b_j \rangle = \sum_{i,j} \langle P_i, Q_j \rangle a_i b_j$)

is positive definite.

Pf of Thm

Assume $\hat{h}(x) = 0$ for some

$$0 \neq x = \sum_{i=1}^{m} P_i \otimes a_i \in E(K) \otimes \mathbb{R}.$$

Let $\Lambda \subseteq E(K) \otimes \mathbb{R} \cong \mathbb{R}^r$ be the $\mathbb{Z}$-lattice spanned by the elements $Q \otimes 1$ with $Q \in E(K)$.

Choose a basis $e_1, \dots, e_r$ of $\mathbb{R}^r$ s.t.

$$\hat{h}\left(\sum c_i e_i\right) = \sum_{i=1}^{a} c_i^2 - \sum_{i=a+1}^{a+b} c_i^2$$

for all $c_1, \dots, c_r \in \mathbb{R}$.

By assumption, $a < r$.

The convex centrally symmetric set

$$S_\varepsilon := \left\{ \sum c_i e_i \mid \sum_{i=1}^{a} c_i^2 < \varepsilon \right\}$$

has volume ∞ for all $\varepsilon > 0$.

By Minkowski's theorem, $\Lambda \cap S_\varepsilon$ contains a nonzero element

$$x = Q \otimes 1 \quad \text{with } Q \in E(K).$$

$$\Rightarrow \hat{h}(Q) < \varepsilon.$$

$$x \neq 0 \Rightarrow Q \notin E(K)_{\text{tors}}$$

$\Rightarrow E(K)$ contains non-torsion points Q with arbitrarily small $\hat{h}(Q) > 0$.

But there are only fin. many $Q \in E(K)$ of bounded $\hat{h}(Q)$! $\lightning$ ∎

2.6. Some algorithms

Let E be an ell. curve over a number field K.

Rmk The error bounds for approx. eq ($\approx$) in section 2.4 can be made explicit (using the coefficients of the elliptic curve).

Therefore, we can approximate $\hat{h}(P) = \lim_{n \to \infty} \frac{h(2^n P)}{4^n}$ to any given precision.

Thm 2.6.1 It's decidable whether a given point $P(K)$ is torsion.

Pf In parallel:

compute $P, 2P, 3P, \dots$

If P is torsion, you eventually find $nP = O$.

compute more and more digits of $\hat{h}(P)$.

If P is non-torsion, then $\hat{h}(P) \neq 0$.

□

More generally:

Thm 2.6.2 It's decidable whether $P_1, \dots, P_n \in E(K)$ are linearly independent in $E(K) \otimes \mathbb{R} \cong \mathbb{R}^r$.

Pf If they are linearly dependent, there are $O \neq (a_1, \dots, a_n) \in \mathbb{Z}^n$ s.t. $a_1 P_1 + \dots + a_n P_n = O$.

If they are lin. independent, then $(\langle P_i, P_j \rangle)_{i,j}$ has nonzero determinant because $\langle \cdot, \cdot \rangle$ is positive definite.

compute more and more digits of the determinant until finding a nonzero digit. □