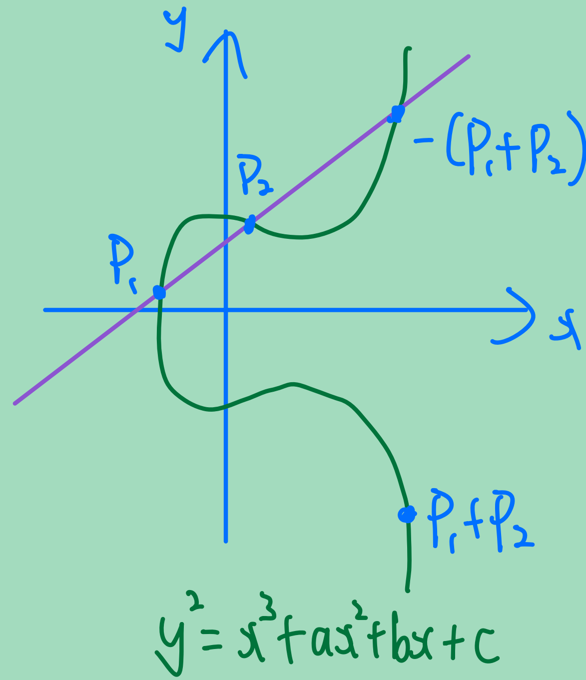
Addition



$P_1=(x_1,y_1)$ $P_2=(x_2,y_2)$ $P_1\neq P_2$

$l_{P_1P_2}: y=\lambda x+\mu$ $\lambda=\dfrac{y_2-y_1}{x_2-x_1}$

$(\lambda x+\mu)^2=x^3+ax^2+bx+c$

$x^3+(a-\lambda^2)x^2+\dots=0$

$x_1+x_2+x_3=\lambda^2-a$ $x_3=\left(\dfrac{y_2-y_1}{x_2-x_1}\right)^2-a-x_1-x_2$

If $P_1=P_2=(x,y)$ $\lambda=\dfrac{3x^2+2ax+b}{2y}$

Example: $y^2=x^3+x^2-9x$ generator $P=(-3,3)$ $2P=(9,-27)$

$3P=\left(-\frac{3}{4},\frac{21}{8}\right)$ $4P=\left(\frac{25}{9},-\frac{55}{27}\right)$ $5P=\left(-\frac{3}{169},-\frac{879}{2197}\right)$ $6P=\left(\frac{2601}{784},\frac{92259}{21952}\right)$

Height

If $q=\frac{a}{b}$ $\gcd(a,b)=1$, $H(q):=\max\{|a|,|b|\}$, $h(q):=\ln H(q)$

If $P=(x,y)$ is a rational point on E, $h(P):=h(x)$

Mordell's Theorem

If $E: y^2=x^3+ax^2+bx+c$, $f(x)=x^3+ax^2+bx+c$ has no double root,

then $E(\mathbb{Q})=\{(x,y)\in\mathbb{Q}^2: y^2=f(x)\}\cup\{O\}$ is finitely generated

Lemma 1. $\forall P_0\ \exists C>0\ \forall P\quad h(P+P_0)\le 2h(P)+C$

Lemma 2. $\exists C\ \forall P\quad h(2P)\ge 4h(P)-C$

Lemma 3 (Weak Mordell). $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite

Pf of Thm. Let $Q_1, Q_2, \dots, Q_n$ be a set of representatives for $E(\mathbb{Q})/2E(\mathbb{Q})$. Let C_1, C_2 be large enough so that

$\forall 1\le i\le n\quad \forall P\quad h(P-Q_i)\le 2h(P)+C_1$

& $\forall P\quad h(2P)\ge 4h(P)-C_2$

For any P, consider the sequence $P_0, P_1, P_2, \dots$ where $P_0=P$

$P_n = Q_{i_n} + 2P_{n+1}$ for some i_n

So $2h(P_n)+C_1 \ge h(P_n - Q_{i_n}) = h(2P_{n+1}) \ge 4h(P_{n+1}) - C_2$

$$h(P_{n+1}) \le \frac{1}{2}h(P_n) + \frac{C_1+C_2}{4}$$

$$h(P_{n+1}) \le \frac{3}{4}h(P_n) \text{ as long as } h(P_n)\ge C_1+C_2$$

Thus $E(\mathbb{Q})$ is generated by $\{Q_1,\dots,Q_n\}\cup\{P\in E(\mathbb{Q}) : h(P)\le C_1+C_2\}$

$\square$

Weak Mordell

If $E: y^2 = x^3 + ax^2 + bx$, can show that

$$\begin{aligned} \varphi: E(\mathbb{Q}) &\longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \\ \mathcal{O} &\longmapsto 1 \bmod \mathbb{Q}^{*2} \\ (x,y) &\longmapsto x \bmod \mathbb{Q}^{*2} \text{ if } (x,y) \neq (0,0) \\ (0,0) &\longmapsto b \bmod \mathbb{Q}^{*2} \end{aligned}$$

is a homomorphism with kernel $2E(\mathbb{Q})$ and finite image.

The proof of $\ker\varphi \subseteq 2E(\mathbb{Q})$ in Silverman-Tate is a bit ad hoc. We follow Cassels and [3]. For simplicity assume $E: y^2 = x^3 + ax + b$, where $f(x) = x^3 + ax + b$ irreducible. WLOG $a, b \in \mathbb{Z}$.

Let θ be a root of $f(x)$ and $K = \mathbb{Q}(\theta)$

Prop 1. $$\begin{aligned} \varphi: E(\mathbb{Q}) &\rightarrow K^*/K^{*2} \\ \mathcal{O} &\mapsto 1 \bmod K^{*2} \\ (x,y) &\mapsto x - \theta \bmod K^{*2} \end{aligned}$$ is a homomorphism.

Pf. $P_1 = (x_1, y_1)$ $P_2 = (x_2, y_2)$ $P_3 = (x_3, y_3)$

x_1, x_2, x_3 are roots of $(\lambda x + \mu)^2 = x^3 + ax + b$

$x_1 - \theta, x_2 - \theta, x_3 - \theta$ are roots of

$$(\lambda x + \lambda\theta + \mu)^2 = (x+\theta)^3 + a(x+\theta) + b$$

$$(x_1-\theta)(x_2-\theta)(x_3-\theta) = -[\theta^3 + a\theta + b - (\lambda\theta+\mu)^2]$$

$$= (\lambda\theta+\mu)^2 = 1 \mod K^{*2}$$

So $x_3 - \theta = (x_1-\theta)(x_2-\theta)(x_3-\theta)^2 \mod K^{*2}$

$$= (x_1-\theta)(x_2-\theta) \mod K^{*2} \qquad \square$$

Prop 2. $\operatorname{Ker}\varphi = 2E(\mathbb{Q})$

Pf. Suppose $P = (x_0, y_0)$ $x_0 - \theta = (p\theta^2 + q\theta + r)^2 = g(\theta)^2$ $p, q, r \in \mathbb{Q}$

By Euclidean algorithm, $f(x) = (sx+t)g(x) + (ux+v)$

$$(s\theta+t)g(\theta) = -(u\theta+v)$$

$$(s\theta+t)^2 g(\theta)^2 = (u\theta+v)^2$$

$$(s\theta+t)^2(x_0-\theta) = (u\theta+v)^2$$

So θ is a root of $h(x) = (sx+t)^2(x_0-x) - (ux+v)^2$

$f(x)$ irreducible, so must have $h(x) = -s^2 f(x)$

$$(sx+t)^2(x_0-x) - (ux+v)^2 = -s^2 f(x)$$

$$(x+\frac{t}{s})^2(x-x_0)+(\frac{u}{s}x+\frac{v}{s})^2=f(x)$$

$$(x+\frac{t}{s})^2(x-x_0)=f(x)-(\frac{u}{s}x+\frac{v}{s})^2$$

So the equation $(\frac{u}{s}x+\frac{v}{s})^2=f(x)$ has roots $-\frac{t}{s},-\frac{t}{s},x_0$

So $P=2P_0$ for some P_0 with x-coordinate $-\frac{t}{s}$. $\square$

Prop 3. $\operatorname{Im}\varphi$ is finite.

Pf. By elementary argument $P=(x,y)=(\frac{m}{e^2},\frac{n}{e^3})$ $\quad$ $\gcd(e,m)=1$, $\gcd(e,n)=1$

Let $f(X)=(X-\theta)(X-\theta')(X-\theta'')$, so

$$(\frac{n}{e^3})^2=(\frac{m}{e^2}-\theta)(\frac{m}{e^2}-\theta')(\frac{m}{e^2}-\theta'')$$

$$n^2=(m-\theta e^2)(m-\theta' e^2)(m-\theta'' e^2)$$

$\langle\alpha\rangle:=\alpha\mathcal{O}_L$

Let $L=\mathbb{Q}(\theta,\theta',\theta'')$. In $\mathcal{O}_L$ have

$$\langle n\rangle^2=\langle m-\theta e^2\rangle\langle m-\theta' e^2\rangle\langle m-\theta'' e^2\rangle$$

recall that

$P\supseteq I \iff \exists J\ I=PJ$

Write $\langle m-\theta e^2\rangle=IJ^2$ where I square-free. If P is a prime ideal dividing I then it divides $\langle m-\theta' e^2\rangle$ or $\langle m-\theta'' e^2\rangle$.

If $P\mid\langle m-\theta' e^2\rangle$, then $P\mid\underset{\langle\theta-\theta'\rangle\langle e\rangle^2}{\underset{\parallel}{\langle(\theta-\theta')e^2\rangle}}$ and $P\mid\underset{\langle\theta-\theta'\rangle\langle m\rangle}{\underset{\parallel}{\langle(\theta-\theta')m\rangle}}$

If $P \nmid \langle \theta - \theta' \rangle$ then $P | \langle e \rangle$ and $P | \langle m \rangle$, contradiction since $\gcd(e, m) = 1$.

Let $\mathcal{F}(K)$ be the group of non-zero fractional ideals in K.

$$E(\mathbb{Q}) \xrightarrow{\varphi} K^*/K^{*2} \xrightarrow{\psi} \mathcal{F}(K)/\mathcal{F}(K)^2 \xrightarrow{\eta} \mathcal{F}(L)/\mathcal{F}(L)^2$$

$$\left(\frac{m}{e^2}, \frac{n}{e^3}\right) \longmapsto \frac{m}{e^2} - \theta \longmapsto \left\langle \frac{m}{e^2} - \theta \right\rangle_K \longmapsto \left\langle \frac{m}{e^2} - \theta \right\rangle_L$$

What we have shown: if $\langle m - \theta e^2 \rangle_L = I J^2$ and $P | I$ then $P | \langle \theta - \theta' \rangle$ or $P | \langle \theta - \theta'' \rangle$, so there are finitely many possibilities for P.

So $\operatorname{Im} \eta \circ \psi \circ \varphi$ is finite.

$\operatorname{Ker} \eta$ is finite because if P is a prime ideal in $\mathcal{O}_K$ that becomes a square in $\mathcal{O}_L$ then it ramifies, and only finitely many primes ramify.

It remains to show that $\operatorname{Ker} \psi$ is finite. If $\alpha \in K^*$ and $\langle \alpha \rangle = I^2$ for some $I \in \mathcal{F}(K)$. By finiteness of class group there are finitely many possibilities for I modulo principle ideal, so can fix in advance $\alpha_1, \dots, \alpha_n$ s.t. for some α_i, $\left\langle \frac{\alpha}{\alpha_i} \right\rangle = \langle \beta \rangle^2$ for some $\beta \in K$, then $\alpha = \alpha_i \beta^2 \varepsilon$ for some $\varepsilon \in \mathcal{O}_K^*$. $\square$

Reference [1] Rational Points on Elliptic Curves, Silverman-Tate

[2] Lectures on Elliptic Curves, Cassels

[3] MSE question 3594791
[4] slides on my website