26.4 .1 (= 27.1)

Lemma. (Silverman – Tate, p. 72)

Let ϕ, ψ be integer polynomials w/no common roots. Let d be the maximum of the degrees.

(a) There is an integer $R \geq 1$ depending on ϕ, ψ s.t. for all rational numbers $\frac{m}{n}$,

$$\gcd\left(n^d \phi\left(\frac{m}{n}\right), n^d \psi\left(\frac{m}{n}\right)\right) \text{ divides } R.$$

(b) There are constants c_1, c_2 ~~each~~ depending on ϕ, ψ s.t. for all rational numbers $\frac{m}{n}$, not roots of ψ,

$$d\,h\left(\frac{m}{n}\right) - c_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq d\,h\left(\frac{m}{n}\right) + c_2.$$

In some sense (a) is the point. You don't get much cancellation in $\dfrac{\phi(m/n)}{\psi(m/n)}$.

Proof. (a) WLOG $d = \deg(\phi) \geq \deg(\psi)$. (Can switch!!)

Write $n^d \phi\left(\frac{m}{n}\right) = a_0 m^d + a_1 m^{d-1} n + \cdots + a_d n^d$

with all $a_i \in \mathbb{Z}$.

Now $\phi(X)$ and $\psi(X)$ have no common roots. By the Euclidean algorithm there exist $F(X), G(X) \in \mathbb{Q}[X]$ with

$$F(X)\phi(X) + G(X)\psi(X) = 1.$$

Choose $A \in \mathbb{Z}$ with $AF(X), AG(X) \in \mathbb{Z}[X]$.

Write $D = \max(\deg F, \deg G)$.

26.5. (= 27.2)

Evaluate our identity at $X = \frac{m}{n}$

$$F\left(\frac{m}{n}\right) \phi\left(\frac{m}{n}\right) + G\left(\frac{m}{n}\right) \psi\left(\frac{m}{n}\right) = 1$$

$$\left(n^D A F\left(\frac{m}{n}\right)\right) \cdot n^d \phi\left(\frac{m}{n}\right)$$
$$+ \left(n^D A G\left(\frac{m}{n}\right)\right) \cdot n^d \psi\left(\frac{m}{n}\right) = A n^{D+d}.$$

Let $\gamma = \gcd\left(n^d \phi\left(\frac{m}{n}\right), n^d \psi\left(\frac{m}{n}\right)\right)$, $\gamma \mid A n^{D+d}$.

we claim $\gamma \mid A a_0^{D+d}$. (this will prove (a)) (no dependence on n.)

why?

$$\gamma \mid A n^{D+2d-1} \phi(m,n) = A a_0 m^d n^{D+d-1} + A a_1 m^{d-1} n^{D+d}$$
$$+ \cdots + A a_d n^{D+2d-1}.$$

Every term after the first is an integer times $A n^{D+d}$

So $\gamma \mid A a_0 m^d n^{D+d-1}$ and $\gamma \mid A n^{D+d}$ $(m,n) = 1$.

So $\gamma \mid A a_0 n^{D+d-1}$.

So repeat the above with $\gamma \mid A a_0 n^{D+2d-2}$

$$\Rightarrow \gamma \mid A a_0^2 n^{D+d-2}$$

etc. Get $\gamma \mid A a_0^{D+d}$.

26.6 = 27.3

Proof of (b). (lower bound)

May assume: (1) $\frac{m}{n}$ is not a root of ϕ

(2) ϕ has deg d, ψ deg e, $e \le d$.

Estimate height of

$$\xi := \frac{\phi(m/n)}{\psi(m/n)} = \frac{n^d \phi\left(\frac{m}{n}\right)}{n^d \psi\left(\frac{m}{n}\right)}$$

We have $H(\xi) \ge \frac{1}{R} \max\left(\left|n^d \phi\left(\frac{m}{n}\right)\right|, \left|n^d \psi\left(\frac{m}{n}\right)\right|\right)$

$$\ge \frac{1}{2R}\left(\left|n^d \phi\left(\frac{m}{n}\right)\right| + \left|n^d \psi\left(\frac{m}{n}\right)\right|\right),$$

$$\frac{H(\xi)}{H(m/n)^d} \ge \frac{1}{2R} \frac{\left|n^d \phi\left(\frac{m}{n}\right)\right| + \left|n^d \psi\left(\frac{m}{n}\right)\right|}{\max\left(|m|^d, |n^d|\right)}$$

$$= \frac{1}{2R} \frac{\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|}{\max\left(\left|\frac{m}{n}\right|^d, 1\right)}$$

This is bounded away from zero:

On a bounded closed interval, because ϕ and ψ have no common zeroes.

Away, because $\displaystyle\lim_{t \to \pm\infty} \frac{\left|\phi\left(\frac{m}{n}\right)\right|}{\left|\frac{m}{n}\right|^d} = |a_0| \neq 0.$

So it's $\ge C_1$ for some positive constant C_1.

$$\log H(\xi) \ge d \log H\left(\frac{m}{n}\right) - C_1.$$

What we wanted to prove.

28.1. Heights and Descent.

(Show axioms again). (Use $m=2$ as we proved)

Proof of finite generation. (Weak MW $\Rightarrow$ MW.)

We will argue that E is generated by

(*) $\{P \in E : h(P) \le Z\}$ for a parameter Z to be determined.

Let $Q_1, \dots, Q_r$ be any set of representatives for $E/2E$, take Z larger than all of the $h(Q_i)$.

Arguing by contradiction, let P_0 be any point <u>not</u> generated by (*), of <u>minimal</u> <u>height</u> among all such points.

Write $P_0 = 2R + Q_i$ for some $R \in E$, some Q_i.

<u>Then</u>:

~~$h(P_0) = h(2R + Q_i) \le 2h(2R) + c_1$ for some constant c_1 depending on Q_i. (There are <u>finitely</u> <u>many</u> Q_i, so choose one c_1 working for all of them.)~~

This is true but not helpful!

$h(2R) \ge 4h(R) - c_2$ for another constant c_2

but

$h(2R) \ge$

Then: $h(2R) = h(P_0 - Q_i) \leq 2h(P_0) + c_1$

for some constant c_1 depending on Q_i. Since there are finitely many Q_i, choose one c_i which works for all of them.

$$h(2R) \geq 4h(R) - c_2$$

and so $$4h(R) - c_2 \leq 2h(P_0) + c_1$$

$$h(R) \leq \frac{1}{2} h(P_0) + \frac{c_1 + c_2}{4}$$

Now, if $\frac{1}{2}h(P_0) > \frac{c_1+c_2}{4}$, i.e. $h(P_0) > \frac{c_1+c_2}{2}$,

which we may guarantee by choosing $z \geq \frac{c_1+c_2}{2}$,

then $h(R) < h(P_0)$.

By minimality of $h(P_0)$, R is generated by $(*)$.

But $P_0 = 2R + Q_i$, so P_0 is too (contradiction).

The canonical height.

Definition. The canonical height $\hat{h}(P)$ is defined by

$$\hat{h}(P) = \lim_{N\to\infty} 4^{-N} h(2^N P).$$

We had $h(2Q) = 4h(Q) + O(1)$, hence seq. is Cauchy hence converges.

Theorem. The canonical height satisfies:

(1) $\hat{h}(P) = h(P) + O(1)$ (const depends on E).
(easy.)

(2) $\hat{h}(P) = 0 \longleftrightarrow P$ is a torsion point.
($\leftarrow$ is obvious. $\rightarrow$ b/c points of bounded height form a finite set.)

(3) $\hat{h}(mP) = m^2 \hat{h}(P)$ for all $m \in \mathbb{Z}$, $P \in E(\mathbb{Q})$.

(4) $\hat{h}(P+Q) \overset{+}{\cdot} \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$.
(Requires some work.)

(5) Define $\langle -, - \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}$

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

(here $\langle P, P \rangle = 2\hat{h}(P)$.)

This is a bilinear form.

Equivalently, $\hat{h}$ is a quadratic form.

Think: $\hat{h}(P+Q) = \hat{h}(P) + \hat{h}(Q) + \langle P, Q \rangle$
kind of like FOILing.

Note that (4) implies immediately

$\hat{h}(P+Q) \leq 2\hat{h}(P) + 2\hat{h}(Q)$, get all our previous axioms.

This will show up in the BSD conjecture.

28.4. The Week Mordell - Weil Theorem.

Prove: $E(\mathbb{Q}) / mE(\mathbb{Q})$ is finite (for any $m \geq 2$) ($m=2$ will do).

The plan.

(1) Give the proof in Silverman - Tate. (Easy but dull)

(2) Explain why it works. (Hard)

Assume: E has a rational point of order 2.

Equivalently: $E: y^2 = f(x)$ where f has a rational root.

By translation this root is at $(0,0)$ so E has the form $y^2 = x^3 + ax^2 + bx$.

Define a curve $\bar{E}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x$ $\quad \bar{a} = -2a$, $\bar{b} = a^2 - 4b$.

Then $\bar{\bar{E}}$ is

$$
\begin{aligned}
y^2 &= x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x \\
&= x^3 + \overline{-2a}\,x^2 + \overline{\bar{a}^2 - 4b}\,x \\
&= x^3 - 2\bar{a}x^2 + (\bar{a}^2 - 4\bar{b})x \\
&= x^3 + 4ax^2 + (4a^2 - 4(a^2 - 4b))x \\
&= x^3 + 4ax^2 + 16bx
\end{aligned}
$$

and $\bar{\bar{E}} \xrightarrow{\sim} E$ $\quad (x,y) \in E \longleftrightarrow (4x, 8y) \in \bar{\bar{E}}$, so

$(x,y) \longrightarrow \left(\frac{x}{4}, \frac{y}{8}\right)$.

So essentially the same procedure gives a map $\bar{E} \to E$.

28.5.

Proposition.

(1) There is an isogeny $E \to \bar{E}$

$$(x,y) \xrightarrow{\phi} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) \text{ if } (x,y) \neq \infty, (0,0)$$

$\infty, (0,0) \longrightarrow \infty$. (i.e. a morphism and group homomorphism)

(2) There is therefore also an isogeny $\bar{E} \to E$ (the dual isogeny)

$$(\bar{x},\bar{y}) \xrightarrow{\psi} \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}\right).$$

(3) The composition $\psi \circ \phi$ is multiplication by 2.

None of this is obvious. You can check it all.

Proposition. $\phi(E(\mathbb{Q}))$ contains:

(1) ∞,

(2) $(0,0)$ iff $\bar{b} = a^2 - 4b$ is a perfect square,

(3) A rational point $(\bar{x},\bar{y}) \in \bar{E}(\mathbb{Q})$ iff $\bar{x}$ is the square of a rational number.

Same for ψ!

~~We get an exact sequence~~

Define a homomorphism $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$

$$\infty \longrightarrow 1$$
$$(0,0) \longrightarrow b$$
$$(x,y) \longrightarrow x.$$

28.6.

Proposition.

(1) α is actually a homomorphism.

(2) The kernel of α is $\psi(\bar{E}(\mathbb{Q}))$, so get an injective homorphism

$$\text{finite!} \longrightarrow \frac{E(\mathbb{Q})}{\psi(\bar{E}(\mathbb{Q}))} \xrightarrow{\alpha} \frac{\mathbb{Q}^\times}{(\mathbb{Q}^\times)^2}.$$

(3) Its image lies in a finite set which we can describe explicitly and locally.
(This is the first example of a Selmer group)

29.1.

Goal: Prove that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

State basic proposition again (on 28.5).

<u>Proof 1.</u> Pages of messy computations.

<u>Proof 2.</u> The rational map is a <u>morphism</u> for free (Sil II.2.1)

Check $\infty \to \infty$ (not so obvious), hence an <u>isogeny</u>

hence a group homomorphism for free:

(Sil III.4.8)

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "\sim"'] & \bar{E} \arrow[d, "\sim"] \\ \mathrm{Pic}^0(E) \arrow[r, "\phi_*"] & \mathrm{Pic}^0(\bar{E}) \end{tikzcd}$$

Check that rational functions on E map to rational functions on $\bar{E}$.

(Note: the push-<u>forward</u> of rat'l fns is weird)

Now, $\phi^{-1}((0,0)) = \{(x,y) \neq (0,0) : y = 0\}$

And $(\psi \circ \phi)^{-1}(\infty) = \phi^{-1}(\infty) \cup \phi^{-1}((0,0))$

$= \infty \cup \{(x,y) \in E : y = 0\}$

$= E[2]$.

So the kernel of $\psi \circ \phi$ equals that of $[2]$.

So they're equal.

29.2

The image of $E(\mathbb{Q}) \xrightarrow{\phi} \bar{E}(\mathbb{Q})$.

Proposition.

(1) $\infty \in \phi(E(\mathbb{Q}))$ (obvious)

(2) $(0,0) \in \phi(E(\mathbb{Q})) \longleftrightarrow \bar{b} = a^2 - 4b$ is a square

(3) $\bar{P} = (\bar{x}, \bar{y}) \in \bar{E}(\mathbb{Q})$ is in $\operatorname{Im}(\phi)$ iff $\bar{x}$ is in $(\mathbb{Q}^\times)^2$.

Proof. (2) $\phi((x,y)) = \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right)$.

If this is $(0,0)$ then $\underline{\underline{y=0}}$ and $x \neq 0$.

Can we find $x \in \mathbb{Q}$ with $0 = x(x^2 + ax + b)$

$0 = x^2 + ax + b$?

iff $a^2 - 4b$ is a square.

(3) $\Rightarrow$ obvious by the formula for ϕ.

$\Leftarrow$: Let $\bar{x} = w^2$, (given $(\bar{x}, \bar{y})$)

$P_1 = (x_1, wx_1)$ $\quad x_1 = \frac{1}{2}\left(w^2 - a + \frac{\bar{y}}{w}\right)$

$P_2 = (x_2, -wx_2)$ $\quad x_2 = \frac{1}{2}\left(w^2 - a - \frac{\bar{y}}{w}\right)$.

These are rational points, so just check:

(1) They're on E;

(2) They both map to $(\bar{x}, \bar{y})$.

This is just a computation, you're done.

29.3

Define a map
$$\begin{aligned} E(\mathbb{Q}) &\xrightarrow{\alpha} \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \\ \infty &\longrightarrow 1 \\ (0,0) &\longrightarrow b \\ (x,y) &\longrightarrow x. \end{aligned}$$

Proposition.

(1) α is a homomorphism. (not obvious!)

(2) There is an exact sequence

$$0 \longrightarrow \bar{E}(\mathbb{Q}) \xrightarrow{\psi} E(\mathbb{Q}) \xrightarrow{\alpha} \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

(3) ~~The~~ Let $p_1, \dots, p_t$ be the primes dividing b. Then $\mathrm{Im}(\alpha)$ is contained in (note: doesn't necessarily equal)

$$\{\pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} : \text{each } \varepsilon_i \text{ is } 0 \text{ or } 1\} \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

(This is $\mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$.)

Proof. (1) must check that if P_1, P_2, P_3 are $E \cap \ell$ for some line ℓ, $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1$.

Assume that none of them are ∞ or $(0,0)$.

(This case must be checked also.)

Let each $P_i = (x_i, y_i)$, $\ell : y = \lambda x + v$

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

The x_i are the solutions to this.

You get $x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x - v^2$

$$= (x - x_1)(x - x_2)(x - x_3)$$

so $x_1 x_2 x_3 = v^2 = 1$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

29.4.

(2) follows from the previous proposition.

In particular, $P \in E(\mathbb{Q})$ is in $\mathrm{Im}(\varphi)$ if and only if x is a rational square.

(Except: ∞ is always; $(0,0)$ is iff b is.) Immediate!

(3) What x-coordinates can occur?

Write $(x,y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$ with $m, n \in \mathbb{Z}$, $\frac{m}{e^2}$ in lowest terms

$$y^2 = x^3 + ax^2 + bx$$
$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4)$$

Case 1. m and $m^2 + ame^2 + be^4$ are coprime.

Then $x = \frac{m}{e^2}$ is a square (maps to 1 in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$)

Case 2. $d = \gcd(m, m^2 + ame^2 + be^4) > 1$

So d divides m and be^4, hence b.

Now $n^2 = m(m^2 + ame^2 + be^4)$ so any prime dividing m and not b must do so to an even power.

So $m = \pm(\text{integer})^2 \cdot p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t}$ ← all 0 or 1

and $\varphi(P) = x = \frac{m}{e^2} = \pm p_1^{\varepsilon_1} \cdots p_t^{\varepsilon_t} \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

This assumed $x \neq 0$. But if $x = 0$ we map it to b, which is in the image demanded.

29.5

Since $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ injects into a finite set,

$$[E(\mathbb{Q}) : \psi(\bar{E}(\mathbb{Q}))] < \infty .$$

By exactly the same reasoning

$$[\bar{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))] < \infty$$

$$\begin{tikzcd} E(\mathbb{Q}) \arrow[r, "\phi"] \arrow[rr, bend left, "\times 2"] & \bar{E}(\mathbb{Q}) \arrow[r, "\psi"] & E(\mathbb{Q}) \end{tikzcd}$$

Claim. $[E(\mathbb{Q}) : (\psi \circ \phi)(E(\mathbb{Q}))] = [E(\mathbb{Q}) : 2E(\mathbb{Q})] < \infty$.

Proof. Let $P_1, \dots, P_r$ be a set of representatives for

$E(\mathbb{Q})/\mathrm{Im}(\psi)$.

Similarly $\bar{P}_1, \dots, \bar{P}_s$ for $\bar{E}(\mathbb{Q})/\mathrm{Im}(\phi)$.

Then any $P \in E(\mathbb{Q})$ is equivalent mod $2E(\mathbb{Q})$ to some $P_i + \psi(\bar{P}_j)$.

To see this, write

$$\begin{aligned} P &= P_i + \psi(Q) \quad \text{for some } P_i,\ Q \in \bar{E}(\mathbb{Q}) \\ &= P_i + \psi(\bar{P}_j + \phi(R)) \quad \text{for some } \bar{P}_j,\ R \in E(\mathbb{Q}) \\ &= P_i + \psi(\bar{P}_j) + \psi(\phi(R)) \\ &= P_i + \psi(\bar{P}_j) + 2R, \end{aligned}$$

done!