Extensions of $\mathbb{Q}_p$ (for proofs, see eg. Milnes ANT notes)

- Fix a prime p, & let K be a finite field ext. of $\mathbb{Q}_p$ (ie $[K:\mathbb{Q}_p]<\infty$)
- Write $\mathcal{O}_K$ for the integral closure of $\mathbb{Z}_p$ in K (so $\mathcal{O}_{\mathbb{Q}_p}=\mathbb{Z}_p$) - 'ring of integers'.

Fact: $\mathcal{O}_K$ is a discrete valuation ring.

Write $v: K \to \mathbb{Z}$ for the normalised valuation, & π for a uniformiser (ie ~~π~~ $v(\pi)=1$).

~~Def~~ D. WARNING: In general, the composite $\mathbb{Q}_p \hookrightarrow K \xrightarrow{v} \mathbb{Z}$ is NOT the normalised valuation on $\mathbb{Q}_p$. We say $\mathbb{Q}_p$ is unram. if it is.

In general, $\exists!\, e \in \mathbb{Z}_{\geq 1}$:
$$\begin{tikzcd} K \arrow[r, "v"] & \mathbb{Z} \\ \mathbb{Q}_p \arrow[u, hook] \arrow[r, "\mathrm{ord}_p"] & \mathbb{Z} \arrow[u, "\times e"'] \end{tikzcd}$$
commutes.

Fact (not strictly needed)

This 'e' is called the ramification index of ~~$\mathbb{Q}_p$ in~~ K over $\mathbb{Q}_p$.

Equivalent def: $K/\mathbb{Q}_p$ is unramified if it has ramification index 1

Fact: $\mathcal{O}_K$ is Henselian (satisfies Hensel's lemma).

~~Cor: All the theory we developed for E/$\mathbb{Q}_p$ works the same for E/K~~

Prop: Let $f \in \mathbb{F}_p[t]$ ~~[illegible]~~ an irreducible polynomial, & write $k=\frac{\mathbb{F}_p[t]}{f}$, a finite field ext. Choose any lift $\hat{f}$ of f to $\mathbb{Z}_p[t]$ & define $K=\frac{\mathbb{Q}_p[t]}{\hat{f}}$. Then the residue field of $\mathcal{O}_K$ is (via red. map) equal to k. Pf: omitted, cf A

~~Conditionally~~

Elliptic curves over extensions of $\mathbb{Q}_p$

Let $K/\mathbb{Q}_p$ be unramified. Note that p is a uniformiser in K (since it is one in $\mathbb{Q}_p$).

Let E/K be an elliptic curve, & assume p is good

(ie if $E: y^2 = x^3 + ax + b$ w. disc. Δ_E, we require

$$v(a) \geq 0, \quad v(b) \geq 0 \quad \& \; v(\Delta_E) = 0.)$$

Then we define a filtration

$$E(K) = E(K)^0 \supseteq E(K)^1 \supseteq \cdots ,$$

& by same pf as for $\mathbb{Q}_p$ we find

$$E^0(K)/E^1(K) = \underset{\substack{\text{res. field} \\ \text{of } K}}{\overline{E}(k)} , \quad \text{and} \quad E^n(K)/E^{n+1}(K) \cong k$$

for $n \geq 1$.

Again, same proofs as before yield that if $p \nmid m$ then $[m] : E^1(K) \longrightarrow E^1(K)$ is a bijection.

Made it to here, 30/03/2015.

<u>lemma</u> let E/k an elliptic curve w. good red'n, & let m not div. by p.

~~Then~~ Let $Q \in E(k)$. ~~Then~~ TFAE:

1) $\exists\, \hat{Q} \in E(k)$ s.t. $m\hat{Q} = Q$;

2) $\exists\, Q_0 \in \bar{E}(k)$ s.t. $mQ_0 = red(Q)$ in $\bar{E}(k)$.

<u>Pf</u>: The map $red : E(K) \to \bar{E}(k)$ is a gp hom, so $1 \Rightarrow 2$ is clear.
For $2 \Rightarrow 1$, consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & E'(K) \arrow[r] \arrow[dd, "\times m"', "\text{iso}"] & E(k) \arrow[r, "red"] \arrow[dd, "\times m"'] & \bar{E}(k) \arrow[r] \arrow[dd, "\times m"'] & 0 \\
 & & \underset{\text{choose}}{P} \arrow[u, phantom, sloped, "\in"] \arrow[r, mapsto] & Q_0 \arrow[dd, bend left] & \\
0 \arrow[r] & E'(k) \arrow[r] & E(k) \arrow[r, "red"] & \bar{E}(k) \arrow[r] & 0 \\
 & & Q \arrow[u, phantom, sloped, "\in"] \arrow[r, mapsto] & red(Q) \arrow[u, phantom, sloped, "\in"] &
\end{tikzcd}$$

(commutative, exact rows by def'n.)

Then $red(Q - mP) = 0$, so $\exists\, R \in E'(k)$ s.t. $Q - mP = R$.

But then $\exists\, R' \in E'(k)$ s.t. $mR' = R$, then

$Q - mP = mR'$ so ~~$P = m(Q-R')$~~ $Q = m(R' - P)$. □

<u>Cor</u>: let $E/\mathbb{Q}_p$ an EC of good red'n, & let $p \nmid n$. Let $Q \in E(\mathbb{Q}_p)$.

Then $\exists\, K/\mathbb{Q}_p$ finite unram. s.t. $Q \in n.E(K)$.

<u>Pf</u>. Since $[n] : \bar{E}(\bar{\mathbb{F}}_p) \to \bar{E}(\bar{\mathbb{F}}_p)$ surjective, $\exists\, R \in \bar{E}(\bar{\mathbb{F}}_p)$ s.t. $nR = red(Q)$.

~~$\bar{\mathbb{F}}_p =$ [illegible]~~ The pt R is defined by finitely many coeffs (namely 3), so $\exists$ finite ext. $k/\mathbb{F}_p$ s.t. $R \in \bar{E}(k)$.

~~By prev lemma~~ Say $k = \frac{\mathbb{F}_p[t]}{f}$, then by prev. lem. $\exists\, K/\mathbb{Q}_p$

finite unram s.t. k = res. field of $\mathcal{O}_K$.

~~By Hensel, red: $E(K) \to \bar{E}(k)$ is surjective, so~~

~~$\exists\ \tilde{R} \in E(K)$ s.t. $\mathrm{red}(\tilde{R}) = R$.~~

Situation:

$$\begin{tikzcd} E(K) \arrow[r, "red"] & \bar{E}(k) \ni R \\ E(\mathbb{Q}_p) \arrow[u, hook] \arrow[r, "red"] \arrow[ur, phantom, "G"] & \bar{E}(\mathbb{F}_p) \arrow[u, hook] \\ \overset{\cup}{Q} & \overset{\cup}{\mathrm{red}(Q)} \end{tikzcd}$$

$n.R = \mathrm{red}\,Q$.

Then by above lemma, $\exists\ \tilde{R} \in E(K)$ s.t. $n.\tilde{R} = Q$. $\square$

Next: Milne, prop 3.6, then pf of finiteness in special case, paying attention to computability.

Let $n>0$.

Prop Let $E/\mathbb{Q}$: $y^2 = x^3 + ax + b$ elliptic, with $a, b \in \mathbb{Z}$ (no restriction) & $\Delta_E :=$ disc. E. Let $T = \{$primes dividing $2n\Delta_E\}$. For any $\gamma \in S^{(n)}(\mathbb{Q})$ and any $p \in \Omega_{\mathbb{Q}} \setminus T$, $\exists$ finite unram $K/\mathbb{Q}_p$ s.t. γ maps to zero in $H^1(K, E[n])$.

Before proving, let's check it makes sense!

- $S^n(E/\mathbb{Q}) \subseteq H^1(\mathbb{Q}, E[n]) \xrightarrow[\text{extend field}]{} H^1(\mathbb{Q}_p, E[n]) \longrightarrow H^1(K, E[n])$

$\left[\text{recall } S^n(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E[n]) \to \prod_{p \in \Omega_{\mathbb{Q}}} H^1(\mathbb{Q}_p, E)\right)\right]$

see (P58)

Pf From defn of $S^n(E/\mathbb{Q})$, $\exists\, Q \in E(\mathbb{Q}_p)$ mapping to the image γ_p of γ in $H^1(\mathbb{Q}_p, E[n])$. Since $p \nmid 2\Delta$, E is good @ p, so $\exists$ finite unram. $K/\mathbb{Q}_p$ s.t. $Q \in nE(K)$, so γ_p maps to zero in $H^1(K, E[n])$.

□

Finally, we prove Selmer gp finite.

To circumvent some technical difficulties, we will

* · Assume $E(\mathbb{Q})[2] = E(\bar{\mathbb{Q}})[2]$ (if $E: y^2 = f$, we're saying f has 3 roots in $\mathbb{Q}$)

· only show $S^2(E/\mathbb{Q})$ finite - enough for our purposes, as it implies $\frac{E(\mathbb{Q})}{2E(\mathbb{Q})}$ finite.

So let $E/\mathbb{Q}$ elliptic, w/ coeffs in $\mathbb{Z}$, s.t. $\# E(\mathbb{Q})[2] = 4$.

Then

$$E(\bar{\mathbb{Q}})[2] = E(\mathbb{Q})[2] \overset{\text{choose iso}}{\cong} \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \cong (\mu_2)^2$$

all as $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules

Hence

$$H^1(\mathbb{Q}, E[2]) = H^1(\mathbb{Q}, (\mu_2)^2) \overset{\text{ok}}{\cong} \left(H^1(\mathbb{Q}, \mu_2)\right)^2 \cong \left(\frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}\right)^2$$

see p.57.

Now $S^2(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E[2]) \to \prod_{p\in\Omega_{\mathbb{Q}}} H^1(\mathbb{Q}_p, E)\right)$,

In particular $S^2(E/\mathbb{Q}) \subseteq H^1(\mathbb{Q}, E[2]) = \left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right)^2$.

Def
Let $T = \{$primes dividing $2\Delta_E\} \subseteq \Omega_{\mathbb{Q}}$. Let

$$\tilde{S}^2(E/\mathbb{Q}) = \left\{ \left[\left((-1)^{\varepsilon(\infty)}\prod_p p^{\varepsilon(p)},\ (-1)^{\varepsilon'(\infty)}\prod_p p^{\varepsilon'(p)}\right)\right] \;\middle|\; \begin{array}{l} \cdot\ 0 \le \varepsilon(p), \varepsilon'(p) \le 1 \\ \cdot\ \varepsilon(p) = \varepsilon'(p) = 0 \text{ if } p \notin T \end{array} \right\}$$

$$\subseteq \left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right)^2$$

Prop: $\tilde{S}^2(E/\mathbb{Q})$ finite.

Pf: obvious, as T is finite. □

Thm: $S^2(E/\mathbb{Q}) \subseteq \tilde{S}^2(E/\mathbb{Q})$.

Pf Let $\gamma \in$ [illegible] $S^2(E/\mathbb{Q})$ corresp to

$$\left((-1)^{\varepsilon(\infty)}\prod_p p^{\varepsilon(p)},\ (-1)^{\varepsilon'(\infty)}\prod_p p^{\varepsilon'(p)}\right) \text{ with } 0 \le \varepsilon(p), \varepsilon'(p) \le 1.$$

~~Wts $\varepsilon(p)$~~ Let p_0 a prime $\notin T$. Wts [illegible] $\varepsilon(p_0) = \varepsilon'(p_0) = 0$.

By prev. lemma (P63), $\exists$ finite unram $K/\mathbb{Q}_{p_0}$ s.t. γ maps to 0 in $H^1(K, E[2])$.

Note $E(\bar{k})[2] =$ [illegible] $E(\mathbb{Q})[2] = (\mathbb{Z}/2)^2$, so ~~$H^1(K, E[2])$~~

$$H^1(K, E[2]) = \left(K^*/K^{*2}\right)^2$$

⑥6 · the ~~m~~ canonical map $H^1(\mathbb{Q}, E[2]) \to H^1(K, E[2])$

becomes the obvious map

$$\left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right)^2 \longrightarrow \left(K^*/K^{*2}\right)^2.$$

We obtain a commutative diagram:

$$\begin{tikzcd}
\gamma \arrow[d, mapsto] & H^1(\mathbb{Q}, E[2]) \arrow[r, "\sim"] \arrow[dd] & \left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right)^2 \arrow[rr, "(\mathrm{ord}_p)^2"] \arrow[dd] & & \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \arrow[dd, "1"] \\
0 \arrow[rrr, mapsto] & & & 0 & \\
& H^1(K, E[2]) \arrow[r, "\sim"] & \left(K^*/K^{*2}\right)^2 \arrow[rr, "\mathrm{ord}_p"] & & \left(\mathbb{Z}/2\mathbb{Z}\right)^2
\end{tikzcd}$$

— key because $K/\mathbb{Q}_p$ $\boxed{\text{unramified}}$

Now clearly · $\mathrm{ord}_{p_0}(\gamma) = (\varepsilon(p_0), \varepsilon'(p_0))$, so $\varepsilon(p_0) = \varepsilon'(p_0) = 0$.

□

So $S^2(E/\mathbb{Q})$ finite, so $E(\mathbb{Q})/2E(\mathbb{Q})$ finite.

~~Hence~~ This concludes pf of wk MW (for $\# E(\mathbb{Q})[2] = 4$, which is all we will do.)

Maybe worked eg here?

Heights; conclusion of pf of MW.

Know $E(\mathbb{Q})/2E(\mathbb{Q})$ finite. Wts $E(\mathbb{Q})$ fin gen. Use heights.

Def Let $n \geq 0$, let $p \in \mathbb{P}^n(\mathbb{Q})$. We say $(a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$ is a primitive representative for p if

- $p = [(a_0 : \dots : a_n)]$
- $\gcd(a_0, \dots, a_n) = 1$.

The height of p is
$$H(p) = \max_{0 \leq i \leq n} |a_i|, \quad \text{where } (a_0, \dots, a_n) \text{ prim rep.}$$
(ex: indep of choice of $\pm$)

The log ht of p is
$$h(p) = \log H(p).$$

eg. $h\left(\left(\frac{1}{2} : \frac{1}{3}\right)\right) = \log 3$

$h((2000 : 3001)) = \log 3001$

Note: $\forall B$,
$\{p \in \mathbb{P}^n(\mathbb{Q}) : H(p) \leq B\}$ finite
& $\{p \in \mathbb{P}^n(\mathbb{Q}) : h(p) \leq B\}$ finite

Idea: $E: y^2 = x^3 + ax + b$ elliptic, $\overset{(x_p : y_p : 1)}{p} \in E(\mathbb{Q})$

Define $h(p) = h(x_p)$.

Will show $h(2p) \approx 4h(p)$, so h is 'approximately a quadratic form'. Also, h non-degenerate.

Then use this + weak MW to prove MW.

(68) First, need some basic results on heights.

Resultants

Let $f, g \in \mathbb{Z}[x]$, $f = f_m x^m + \cdots + f_0$ $\quad f_m, g_n \neq 0$.

$g = g_n x^n + \cdots + g_0$,

Def The resultant of f & g is

$$\mathrm{Res}(f,g) = \det \; M := \underbrace{\left[\begin{matrix} f_m & f_{m-1} & \cdots & f_0 & 0 & 0 & \cdots & 0 \\ 0 & f_m & \cdots & \cdots & f_0 & 0 & \cdots & 0 \\ \vdots & & & & & & & \\ 0 & \cdots & \cdots & 0 & f_m & \cdots & \cdots & f_0 \\ g_n & g_{n-1} & \cdots & \cdots & g_0 & 0 & \cdots & 0 \\ \vdots & & & & & & & \\ \vdots & & & & & & & \\ 0 & \cdots & \cdots & 0 & g_n & \cdots & \cdots & g_0 \end{matrix}\right]}_{m+n} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} n \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} m \end{matrix}$$

Rk. $\mathrm{Res}(f,g) = f_m^n \cdot f_n^m \cdot \prod_{\substack{p,q \in \overline{\mathbb{Q}} \\ f(p)=g(q)=0}} (p-q)$

Def: $\mathrm{recip}(f) = f_0 x^m + \cdots + f_m$

$\mathrm{recip}(g) = g_0 x^n + \cdots + g_n$

eg. $f = x + 2$ $\quad m = 1$

$g = 3x^2 + 4x + 5$ $\quad n = 2$

$$\mathrm{Res}(f,g) = \det \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 3 & 4 & 5 \end{bmatrix} = \; ?!$$

Prop 1) If $m = n$ then $\mathrm{Res}(\text{recip } f, \text{recip } g) = \pm \mathrm{Res}(f,g)$.

2) $\exists\, a, b \in \mathbb{Z}[x]$, $\deg a < n$, $\deg b < m$, s.t.

$$\mathrm{Res}(f,g) = af + bg;$$

3) $\mathrm{Res}(f,g) = 0 \Rightarrow \deg \gcd(f,g) > 0$. (follows from Rk, but we will prove)

Pf 1) Easy - swap some rows & columns.

2) Let $C_1, \ldots, C_{m+1}$ be collums of M. Then

$$C := \begin{bmatrix} x^{m-1} f \\ x^{m-2} f \\ \vdots \\ f \\ x^{n-1} g \\ \vdots \\ g \end{bmatrix} = x^{m+n-1} C_1 + \cdots + C_{m+n}.$$

So $\mathrm{Res}(f,g) = $ degree 0 part of $\left(\det(C_1, \ldots, C_{m+n-1}, C)\right)$.

Expand RHS, result follows.

← to here

3) Say $\mathrm{Res}(f,g) = 0$, write $0 = \mathrm{Res}(f,g) = fa + gb$ by (2).

Say $f(\alpha) = 0$, ~~then~~ some $\alpha \in \overline{\mathbb{Q}}$. Then $g(\alpha) = 0$ or $b(\alpha) = 0$.

If $g(\alpha) = 0$, done. If $b(\alpha) = 0$, then $0 = a\left(\frac{f}{x-\alpha}\right) + \left(\frac{b}{x-\alpha}\right) \cdot g$.

Let α_1 a root of $\frac{f}{x-\alpha}$, repeat. Since $\deg b < \deg f$, this eventually gives a common root of f & g.

$\square$

Back to heights

Prop let $F, G \in \mathbb{Q}[x,y]$ homog. of same degree $m>0$, s.t. $V_F^P \cap V_G^P = \phi$ ('no common zeros'). Define

$$\varphi : \mathbb{P}^1(\mathbb{Q}) \longrightarrow \mathbb{P}^1(\mathbb{Q})$$

$$(x:y) \longmapsto (F(x,y) : G(x:y))$$

(ex: well defined!)

Then, $\exists B \in \mathbb{R}$ s.t. $\forall p \in \mathbb{P}^1(\mathbb{Q})$, have

$$\boxed{|h(\varphi(p)) - m h(p)| \leq B.}$$

Pf Wlog F & G have integer coeffs. let $p \in \mathbb{P}^1(\mathbb{Q})$ with prim. rep. (a,b). Then $\forall c \in \mathbb{Z}$ have

$$|c a^i b^{m-i}| \leq |c| \max(|a|^m, |b|^m),$$

hence, setting $c = (m+1). \max |\text{coeffs of } F \& G|$, have

$$|F(a,b)|, \; |G(a,b)| \leq C \max(|a|, |b|)^m.$$

Now $H(\varphi(p)) \leq \max(|F(a,b)|, |G(a,b)|)$

$$\leq C \max(|a|,|b|)^m = C. H(p)^m,$$

$$\Rightarrow h(\varphi(p)) \leq m h(p) + \log C.$$

Other inequality harder.

Since ~~F & G~~ $V_F^P \cap V_G^P = \phi$, we have that

$$F(\tfrac{x}{y}, 1) \;\&\; G(\tfrac{x}{y}, 1) \in \mathbb{Z}[\tfrac{x}{y}]$$ have no comon root in $\overline{\mathbb{Q}}$,

hence $R := \mathrm{Res}(F(\frac{x}{y}, 1), G(\frac{x}{y}, 1)) \neq 0$.

Hence $\exists u, v \in \mathbb{Z}[\frac{x}{y}]$, of degree $< m$, s.t.

$R = u(\frac{x}{y}) F(\frac{x}{y},1) + v(\frac{x}{y}) G(\frac{x}{y},1)$.

Multiply through by y^{2m-1} & setting

$U(x,y) = y^{m-1}u(\frac{x}{y})$, $V(x,y) = y^{m-1}v(\frac{x}{y}) \in \mathbb{Z}[x,y]$,

we find

$U(x,y) F(x,y) + V(x,y) G(x,y) = y^{2m-1} R$.

Similarly (swapping x & y), $\exists$ $U', V' \in \mathbb{Z}[x,y]$ s.t.

$U' F + V' G = x^{2m-1} R$.

~~Setting~~ Substituting in $x = a$, $y = b$, we obtain

$U(a,b) F(a,b) + V(a,b) G(a,b) = b^{2m-1} R$

$U'(a,b) F(a,b) + V'(a,b) G(a,b) = a^{2m-1} R$.

Hence

$\gcd(F(a,b), G(a,b)) \mid \gcd(Ra^{2m-1}, Rb^{2m-1}) = R$. ⊛

Imitating argument from earlier ~~mk~~ proof, $\exists$ c' (indep of a,b) s.t. $|U(a,b)|, |U'(a,b)|, |V(a,b)|, |V'(a,b)| \leq c' \max(|a|,|b|)^{m-1}$,

hence

$$2 \max(|a|,|b|)^{m-1} \max(|F(a,b)|, |G(a,b)|) \geq R|a|^{2m-1}$$
$$\geq R|b|^{2m-1},$$

so combine with ⊛ to get

$$H(\varphi(P)) \geq \frac{1}{R} \max(|F(a,b)|, |G(a,b)|) \geq \frac{1}{2c'} H(P)^{m},$$

take logs, done.

$\square$

Veronese map.

Prop Define $\nu : \mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q}) \longrightarrow \mathbb{P}^2(\mathbb{Q})$

$$((a:b),(c:d)) \longmapsto (ac : ad+bc : bd).$$

(ex: well def'd!)

Then $\forall\, p, q \in \mathbb{P}^1(\mathbb{Q})$, have

$$\frac{1}{2} \leq \frac{H(\nu(p,q))}{H(p)\,H(q)} \leq 2$$

Pf: see Homework $\square$

Heights on Elliptic Curves

Let $E: y^2 = x^3 + ax + b$, ~~$a, b \in \mathbb{Q}$~~, elliptic curve / $\mathbb{Q}$.

Given $p \in E(\mathbb{Q})$, define

$$H(p) = \begin{cases} H((x(p) : z(p)) & \text{if } p \neq (0:1:0) \\ 1 & \text{if } p = (0:1:0). \end{cases}$$

Let $h(p) = \log H(p)$.

lemma $\forall B \in \mathbb{R}$, $\{p \in E(\mathbb{Q}) \mid h(p) \leq B\}$ is finite

Pf. Analogue for $\mathbb{P}^1$ is clear. For each $(x:z)$, there are at most 2 possible y-coordinates. $\square$

Prop $\exists$ a constant $A = A(E)$ s.t. $\forall p \in E(\mathbb{Q})$, have:

$$|h(2p) - 4h(p)| \leq A.$$

Pf If $p = (0:1:0)$, easy. Else, let $p = (x:y:z)$, $2p = (x_2:y_2:z_2)$

~~Apply~~ let $F, G \in \mathbb{Q}[x, z]$ homog. deg 4 s.t.

$$F(x,1) = (3x^2+a)^2 - 8x(x^3+ax-b)$$

$$G(x,1) = 4(x^3+ax+b),$$

Then $\dfrac{x_2}{z_2} = \dfrac{F(x,z)}{G(x,z)}$ (if $y \neq 0$; if $y = 0$ then $2p = 1$, & only ≤ 3 options for P, so done).

Since E smooth, deduce F & G have no common root (even: $V_F^{\mathbb{P}} \cap V_G^{\mathbb{P}} = \emptyset$), so by prev. prop. get ~~the~~ result $\square$.

Prop: $\exists$ at most one fctn $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ s.t.

a) $\hat{h}(p) - h(p)$ bounded on $E(\mathbb{Q})$

& b) $\hat{h}(2p) = 4\hat{h}(p)$.

Pf Say $\forall p$, $|\hat{h}(p) - h(p)| \leq B$. ~~Then~~ Given $p \in E(\mathbb{Q})$, have $|\hat{h}(2^n p) - h(2^n p)| \leq B$, so

$$\left|\hat{h}(p) - \frac{h(2^n p)}{4^n}\right| \leq B/4^n,$$

So $\dfrac{h(2^n p)}{4^n}$ converges to $\hat{h}(p)$ as $n \to \infty$. $\square$

Lemma $\forall p \in E(\mathbb{Q})$, the sequence

$$\frac{h(2^n p)}{4^n} \text{ is cauchy } (\text{in } \mathbb{R}).$$

Pf Know $\exists A = A(E)$ s.t. $\forall p$,

$$|h(2p) - 4h(p)| < A.$$

For $N \geq M \geq 0$ & $p \in E(\mathbb{Q})$, have

$$\left| \frac{h(2^N p)}{4^N} - \frac{h(2^M p)}{4^M} \right| = \left| \sum_{n=M}^{N-1} \frac{h(2^{n+1} p)}{4^{n+1}} - \frac{h(2^n p)}{4^n} \right|$$

$$\leq \sum_{n=M}^{N-1} \frac{1}{4^{n+1}} \left| h(2^{n+1} p) - 4h(2^n p) \right|$$

$$\leq \sum_{n=M}^{N-1} \frac{1}{4^{n+1}} A \leq \frac{A}{3 \cdot 4^M}.$$

□

Def Given $p \in E(\mathbb{Q})$, set

$$\hat{h}(p) = \lim_{n \to \infty} \frac{h(2^n p)}{4^n} \in \mathbb{R}.$$

The 'canonical' or 'Néron-Tate' height of p.

Thm: The fctn $\hat{h}: E(\mathbb{Q}) \to \mathbb{R}$ satisfies:

a) $\hat{h}(p) - h(p)$ bounded on $E(\mathbb{Q})$;

b) $\hat{h}(2p) = 4\hat{h}(p)$

c) $\forall c \in \mathbb{R}$, $\{p \in E(\mathbb{Q}) \mid \hat{h}(p) \leq c\}$ is finite.

d) $\hat{h}(p) \geq 0 \ \forall p$ & $\hat{h}(p) = 0 \iff p \in E(\mathbb{Q})_{tors}$.

Pf a) In pf of last lemma, showed $\forall N \geq M \geq 0$, have

$$\left| \frac{h(2^N p)}{4^N} - \frac{h(2^M p)}{4^M} \right| \leq \frac{A}{3 \cdot 4^M}.$$

Taking $M = 0$, get $\forall N \geq 0$ that

$$\left| \frac{h(2^N p)}{4^N} - h(p) \right| \leq \frac{A}{3}.$$

Letting $N \to \infty$, result follows.

b) $\hat{h}(2p) = \lim_{n \to \infty} \frac{h(2^{n+1}p)}{4^n} = 4 \lim_{n \to \infty} \frac{h(2^{n+1}p)}{4^{n+1}} = 4h(p)$.

c) Say $\forall p$, $|\hat{h}(p) - h(p)| \leq B$. Then

$\{p \in E(\mathbb{Q}) \mid \hat{h}(p) \leq c\} \subseteq \{p \in E(\mathbb{Q}) \mid h(p) \leq B + c\}$, which is finite.

d) $H(p) \geq 1$, so $h(p) \geq 0$, so $\hat{h}(p) \geq 0$.

($\Leftarrow$) If $p \in E(\mathbb{Q})_{tors}$ then $S := \{2^n p : n \in \mathbb{N}\}$ is finite, so $\hat{h}$ is bounded on S, say by D. But $\hat{h}(2^n p) = 4^n \hat{h}(p)$, so $\hat{h}(p) = \frac{\hat{h}(2^n p)}{4^n} \leq \frac{D}{4^n} \ \forall n$.

$\Rightarrow$ Say p has infinite order. If $\hat{h}(p)=0$ then

~~$S:=\{2^n p : n\in\mathbb{N}\}$~~ $\forall n\in\mathbb{N}$, $\hat{h}(2^n p)=0$.

So $\hat{h}$ vanishes on the infinite set $\{2^n p : n\in\mathbb{N}\}$,

contradicting (c).

$\square$

Def Let Π be an abelian gp & k a field, $2\in k^*$. A fctn

$f:\Pi\to k$ is called a quadratic form if

$\forall x,y\in\Pi$: 1) $f(2x)=4f(x)$

& 2) $B(x,y):=f(x+y)-f(x)-f(y)$ is bi-additive.

Note: $B(x,y)=B(y,x)$, & $f(x)=\frac{1}{2}B(x,x)$. (needs $2\in k^*$!)

Prop: Π, k as above. Let $f:\Pi\to k$ satisfy the parallelogram law:

$\forall x,y\in\Pi$: $f(x+y)+f(x-y)=2f(x)+2f(y)$.

Then f is a quadratic form.

Pf Set $x=y=0$, $\Rightarrow f(0)=0$.
Set $x=y$, $\Rightarrow f(2x)=4f(x)$.

Remains to show $B(x,y):=f(x+y)-f(x)-f(y)$ biadditive.

By symmetry, enough to show that $\forall x,y,z\in\Pi$, have

$B(x+y,z)=B(x,z)+B(y,z)$, i.e.

$f(x+y+z)-f(x+y)-\cancel{f(z)}-f(x+z)+f(x)+\cancel{f(z)}-f(y+z)+f(y)+f(z)=0$

For this, apply parallelogram law to get 4 identities:

- $f(x+y+z) + f(x+y-z) - 2f(x+y) - 2f(z) = 0$;
- $f(x+y-z) + f(x-y+z) - 2f(x) - 2f(y-z) = 0$;
- $f(x+y+z) + f(x-y+z) - 2f(x+z) - 2f(y) = 0$;
- $2f(y+z) + 2f(y-z) - 4f(y) - 4f(z) = 0$.

Take alternating Σ of these 4, then divide by 2 to get required identity.

□

lemma $\exists\, C \in \mathbb{R}$ s.t. $\forall\, P_1, P_2 \in E(\mathbb{Q})$ have

$$H(P_1 + P_2)\, H(P_1 - P_2) \leq C\, H(P_1)^2 H(P_2)^2$$

Pf. Set $P_3 = P_1 + P_2$, $P_4 = P_1 - P_2$, write $P_i = (x_i : y_i : z_i)$, primitive representatives.

Then addition formula yields

$$(x_3 x_4 : x_3 z_4 + x_4 z_3 : z_3 z_4) = (w_0 : w_1 : w_2) \text{ where}$$

$$w_0 = x_1^2 x_2^2 - 2a x_1 x_2 z_1 z_2 - 4b(x_1 z_1 z_2^2 + x_2 z_1^2 z_2) + a^2 z_1^2 z_2^2;$$

$$w_1 = 2(x_1 x_2 + a z_1 z_2)(x_1 z_2 + x_2 z_1) + 4b z_1^4 z_2^4;$$

$$w_2 = (x_2 z_1 - x_1 z_2)^2$$

So $\exists\, c \in \mathbb{R}$ s.t.
$H(w_0 : w_1 : w_2) \leq C\, H(P_1)^2 H(P_2)^2$.

Recall formula for hts under Veronese (cf HW),

$$\frac{1}{2} \leq \frac{H(w_0 : w_1 : w_2)}{H(x_3 : z_3)\, H(x_4 : z_4)} \leq 2, \quad \text{so}$$

$$H(w_0 : w_1 : w_2) \geq \frac{1}{2} H(P_3, P_4).$$

Lemma The canonical ht $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ satisfies the parallelogram law (& so is a quadratic form).

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

~~Va~~ Taking logs in previous lemma, $\exists$ B s.t.

$$h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + B.$$

Replace P by $2^n P$, Q by $2^n Q$, divide by 4^n & take $\lim_{n\to\infty}$, to get

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

To get reverse inequality, ~~replace~~ set

$$P' = P+Q, \quad Q' = P-Q, \text{ then}$$

$$\begin{aligned} 2\hat{h}(P') + 2\hat{h}(Q') &\leq 4\hat{h}(P) + 4\hat{h}(Q) \\ &= \hat{h}(2P) + \hat{h}(2Q) \\ &= \hat{h}(P'+Q') + \hat{h}(P'-Q'). \end{aligned}$$

$\square$

Thm [Mordell-Weil] Let $E/\mathbb{Q}$ an elliptic curve. Then

$E(\mathbb{Q})$ is a fin-gen. ab. gp.

(assuming $E(\mathbb{Q})/2E(\mathbb{Q})$ finite, which we proved under some restrictions for simplicity).

Pf Let $P_1, \dots, P_n$ be coset reps for $E(\mathbb{Q})/2E(\mathbb{Q})$.

Let $C := \max_i \hat{h}(P_i)$.

Set $S = \{P \in E(\mathbb{Q}) \mid \hat{h}(P) \le C\}$, a finite set.

Then
claim S generates $E(\mathbb{Q})$.

Pf: Suppose $E(\mathbb{Q}) \setminus \langle S \rangle \neq \emptyset$. Then let $Q \in E(\mathbb{Q}) \setminus \langle S \rangle$ be of minimal $\hat{h}$ (possible since $\{P \mid \hat{h}(P) \le B\}$ always finite)

We know $\exists\ 1 \le i \le n$ & $R \in E(\mathbb{Q})$ s.t.

$Q = P_i + 2R$. Then $R \notin \langle S \rangle$ (else $Q \in \langle S \rangle$),

so $\hat{h}(R) \geq \hat{h}(Q)$. Then

$$
\begin{aligned}
2\hat{h}(P_i) &= \hat{h}(P_i + Q) + \hat{h}(P_i - Q) - 2\hat{h}(Q) \\
&= \hat{h}(P_i + Q) + \hat{h}(-2R) - 2\hat{h}(Q) \\
&= \hat{h}(P_i + Q) + 4\hat{h}(R) - 2\hat{h}(Q), \\
&\geq 0 + 4\hat{h}(R) - 2\hat{h}(Q) \\
&\geq 2\hat{h}(Q), \quad ↯
\end{aligned}
$$

$\square$.

Done!