ALVARO GONZALEZ HERNANDEZ
University of Warwick

Elliptic curves over discrete valuation rings

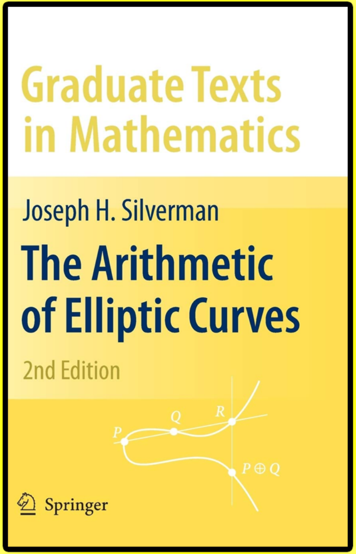
Study group on Mazur's Torsion Theorem

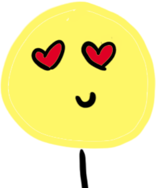
Plan for this session

WARWICK
THE UNIVERSITY OF WARWICK

1. Introduction to the theory of elliptic curves over DVRs.
2. Discussion of the types of reduction.
3. Reduction of torsion points.
4. The Néron-Ogg-Shaferevich criterion.

If in doubt... Chapter VII





Discrete valuation ring

WARWICK
THE UNIVERSITY OF WARWICK

DVR

A **discrete valuation ring** is a principal ideal domain R with exactly one non-zero maximal ideal $\mathfrak{p}$.

Discrete valuation ring

DVR

A **discrete valuation ring** is a principal ideal domain R with exactly one non-zero maximal ideal $\mathfrak{p}$. Alternatively, it is a PID endowed with a discrete valuation v on the field of fractions K of R such that

$$R = \{0\} \cup \{x \in K : v(x) \geq 0\}$$

Residue field

The **residue field** k of R is defined as $k = R/\mathfrak{p}$

Uniformiser

A **uniformiser** of R is an element $\pi \in R$ satisfying that $v(\pi) = 1$.

My fave example of DVR ($p \neq 2, 3$)

$$R = \mathbb{Z}_p$$

$$K = \mathbb{Q}_p$$

$$k = \mathbb{F}_p$$

$$\pi = p$$

Minimal Weierstrass equation

Let E/K be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$.

$$y^2 = x^3 + ax + b \quad \xleftrightarrow{x'=u^2x \qquad y'=u^3y} \quad (y')^2 = (x')^3 + u^{-4}ax' + u^{-6}b$$

Minimal Weierstrass equation

WARWICK
THE UNIVERSITY OF WARWICK

Let E/K be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$.

$$y^2 = x^3 + ax + b \quad \xleftarrow{x'=u^2x \quad y'=u^3y}\!\!\!\!\xrightarrow{} \quad (y')^2 = (x')^3 + u^{-4}ax' + u^{-6}b$$

Minimal Weierstrass equation

We say that a Weierstrass equation is **minimal** if a and b belong to R and $v(a) < 4$ or $v(b) < 6$ (equivalently $v(\Delta)$ is minimal).

Over $K = \mathbb{Q}_5$,

$$y^2 = x^3 + 30\,000\,x - 4\,000\,000 \quad \xrightarrow{u=10} \quad y^2 = x^3 + 3x - 4$$

Minimal Weierstrass equation

Let E/K be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$.

$$y^2 = x^3 + ax + b \quad \xleftrightarrow{x'=u^2x \quad y'=u^3y} \quad (y')^2 = (x')^3 + u^{-4}ax' + u^{-6}b$$

Minimal Weierstrass equation

We say that a Weierstrass equation is **minimal** if a and b belong to R and $v(a) < 4$ or $v(b) < 6$ (equivalently $v(\Delta)$ is minimal).

Over $K = \mathbb{Q}_5$,

$$y^2 = x^3 + 30\,000\,x - 4\,000\,000 \quad \xrightarrow{u=5} \quad y^2 = x^3 + 48x - 256$$

Definition time!

Minimal Weierstrass model

The **minimal Weierstrass model** for E is the projective scheme $\mathcal{E}$ over R defined by a minimal Weierstrass equation.

Definition time!

WARWICK
THE UNIVERSITY OF WARWICK

Minimal Weierstrass model

The **minimal Weierstrass model** for E is the projective scheme $\mathcal{E}$ over R defined by a minimal Weierstrass equation.

Reduction of E modulo $\mathfrak{p}$

The **reduction of E modulo $\mathfrak{p}$**, which we will denote by $\overline{E}$, is the special fiber $\mathcal{E}_k$ of $\mathcal{E}$. We will denote by $\overline{E}_{sm}$ the **smooth locus** of $\overline{E}$.

It is easy to see that $\overline{E}$ is an irreducible projective curve over k (maybe singular) and that we can define a group law on $\overline{E}_{sm}$ using the secant line construction.

Definition time!

Reduction map

The **reduction map** is the map

$$\begin{aligned} E(K) &\to \overline{E}(k) \\ P &\longmapsto \overline{P} \end{aligned}$$

induced by the natural morphism $R \to R/\mathfrak{p} = k$.

Definition time!

Reduction map

The **reduction map** is the map

$$E(K) \to \overline{E}(k)$$
$$P \longmapsto \overline{P}$$

induced by the natural morphism $R \to R/\mathfrak{p} = k$.
We also have,

$$E_0(K) = \{P \in E(K) : \overline{P} \in \overline{E}_{sm}(k)\}.$$

Definition time!

WARWICK
THE UNIVERSITY OF WARWICK

Reduction map

The **reduction map** is the map

$$\begin{aligned} E(K) &\to \overline{E}(k) \\ P &\longmapsto \overline{P} \end{aligned}$$

induced by the natural morphism $R \to R/\mathfrak{p} = k$.
We also have,

$$E_0(K) = \{P \in E(K) : \overline{P} \in \overline{E}_{sm}(k)\}.$$

$$E_1(K) = \{P \in E(K) : \overline{P} = \overline{O}\}.$$

Example

WARWICK
THE UNIVERSITY OF WARWICK

Over $\mathbb{Q}_5$,

$$E : y^2 = x^3 + 3x - 4 \quad \xrightarrow{\text{mod } 5} \quad \overline{E} : y^2 = x^3 - \overline{2}x + \overline{1} = (x - \overline{2})^2(x - \overline{1})$$

Then,

$$\begin{aligned}
\overline{E}(\mathbb{F}_5) &= \{\overline{O}, (\overline{0}, -\overline{1}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{2}, \overline{0})\} \\
\overline{E}_{sm}(\mathbb{F}_5) &= \{\overline{O}, (\overline{0}, -\overline{1}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0})\} \cong \mathbb{Z}/4\mathbb{Z} \\
E_0(\mathbb{Q}_5) &= \{(x, y) \in E(\mathbb{Q}_5) : x \not\equiv 2 \pmod 5\}
\end{aligned}$$

For example, $(1, 0)$ and $(0, \pm 2i)$ all belong to $E_0(\mathbb{Q}_5)$ (where i is considered to be one of the roots of the polynomial $x^2 + 1$).

Example

Over $\mathbb{Q}_5$,

$$E : y^2 = x^3 + 3x - 4 \quad \xrightarrow{\text{mod } 5} \quad \overline{E} : y^2 = x^3 - \overline{2}x + \overline{1} = (x - \overline{2})^2(x - \overline{1})$$

Then,

$$E_1(\mathbb{Q}_5) = \{(x, y) \in E(\mathbb{Q}_5) : v_5(y) < 0\} = \{(x, y) \in E(\mathbb{Q}_5) : v_5(x) < 0\}$$

For example, $[4](0, 2i) = \left(\frac{707679}{1537600}, \frac{3027727631}{1906624000} i\right) \in E_1(\mathbb{Q}_5)$.

Example

Over $\mathbb{Q}_5$,

$$E : y^2 = x^3 + 3x - 4 \quad \xrightarrow{\text{mod } 5} \quad \overline{E} : y^2 = x^3 - \overline{2}x + \overline{1} = (x - \overline{2})^2(x - \overline{1})$$

It is easy to check that if $x \equiv 2 \pmod 5$, then, $v(x^3 + 3x - 4) = 1$ and so, as $v(y^2)$ is even, this shows that there cannot be any point in $E(\mathbb{Q}_5)$ that reduces to $(\overline{2}, \overline{0})$. Therefore, $E(\mathbb{Q}_5) = E_0(\mathbb{Q}_5)$ and $\#E(\mathbb{Q}_5)/E_0(\mathbb{Q}_5) = 1$.

The quotient $E(K)/E_0(K)$

Finiteness of $E(K)/E_0(K)$

The group $E(K)/E_0(K)$ is finite. Furthermore, if $\overline{E}_{sm}(k) \cong k^*$ (i.e. E has split multiplicative reduction) then the group is cyclic of order $-v(j)$; otherwise, it has cardinality at most 4.

Types of reduction

As $\overline{E}$ is given by the equation $y^2 = x^3 + \overline{a}x + b$, so it is non-singular (hence an elliptic curve) if and only if $\overline{\Delta} \neq 0$.

Good reduction 😇

We say that E has **good reduction** if $\overline{\Delta} \neq 0$.

Example: $y^2 = x^3 + 1$ in $\mathbb{Q}_p$ for all $p \geq 5$ ($\Delta = -2^4\,3^3$).

Types of reduction

As $\overline{E}$ is given by the equation $y^2 = x^3 + \overline{a}x + b$, so it is non-singular (hence an elliptic curve) if and only if $\overline{\Delta} \neq 0$.

Bad reduction 😈

We say that E has **bad reduction** if $\overline{\Delta} = 0$.

If $\overline{\Delta} = 0$ and either $\overline{a} \neq 0$ or $\overline{b} \neq 0$, we say that E has **multiplicative reduction**.

If $\overline{\Delta} = 0$ and $\overline{a} = \overline{b} = 0$, we say that E has **additive reduction**.

Types of reduction

As $\overline{E}$ is given by the equation $y^2 = x^3 + \overline{a}x + \overline{b}$, so it is non-singular (hence an elliptic curve) if and only if $\overline{\Delta} \neq 0$.

Bad reduction 😈

We say that E has **bad reduction** if $\overline{\Delta} = 0$.

If $\overline{\Delta} = 0$ and either $\overline{a} \neq 0$ or $\overline{b} \neq 0$, we say that E has **multiplicative reduction**.

If $\overline{\Delta} = 0$ and $\overline{a} = \overline{b} = 0$, we say that E has **additive reduction**.

Examples:

$y^2 = x^3 + 3x - 4$ over $\mathbb{Q}_5$ has (split) multiplicative reduction.

$y^2 = x^3 + 5$ over $\mathbb{Q}_5$ has additive reduction.

Types of reduction

Good Reduction

Bad Reduction

Semistable Reduction

Good Reduction

$\Delta \in R^\times$

Multiplicative Reduction

$\Delta \notin R^\times$ but either $\begin{cases} a \in R^\times \\ b \in R^\times \end{cases}$

Additive Reduction

$\Delta \notin R^\times,\ a \notin R^\times,\ b \notin R^\times$

Behaviour of reduction type under extensions

Preservation of reduction type under extension

Let K'/K be a finite extension. Suppose that either K'/K is unramified or E has semi-stable reduction over K. Then a minimal Weierstrass equation for E over K is still minimal over K'. Therefore the reduction type of E over K is the same as that over K'.

Behaviour of reduction type under extensions

Preservation of reduction type under extension

Let K'/K be a finite extension. Suppose that either K'/K is unramified or E has semi-stable reduction over K. Then a minimal Weierstrass equation for E over K is still minimal over K'. Therefore the reduction type of E over K is the same as that over K'.

Semi-stable reduction theorem

There exists a finite extension K'/K such that E has semi-stable reduction over K'.

$$y^2 = x^3 + ax + b \quad \xleftrightarrow{x'=u^2x \quad y'=u^3y} \quad (y')^2 = (x')^3 + u^{-4}ax' + u^{-6}b$$

Behaviour of reduction type under extensions

Over $\mathbb{Q}_5$, $y^2 = x^3 + 5$ has additive reduction but over $\mathbb{Q}_5(5^{1/6})$, it has **good reduction**.

$$y^2 = x^3 + 5 \quad \xleftrightarrow{x'=(5^{1/6})^2 x \quad y'=(5^{1/6})^3 y} \quad (y')^2 = (x')^3 + 1$$

Behaviour of reduction type under extensions

Over $\mathbb{Q}_5$, $y^2 = x^3 + 5$ has additive reduction but over $\mathbb{Q}_5(5^{1/6})$, it has **good reduction**.

$$y^2 = x^3 + 5 \quad \xleftrightarrow{x'=(5^{1/6})^2 x \quad y'=(5^{1/6})^3 y} \quad (y')^2 = (x')^3 + 1$$

Over $\mathbb{Q}_5$, $y^2 = x^3 + 75x - 500$ has additive reduction but over $\mathbb{Q}_5(5^{1/2})$ it has **multiplicative reduction**.

$$y^2 = x^3 + 75x - 500 \quad \xleftrightarrow{x'=(5^{1/2})^2 x \quad y'=(5^{1/2})^3 y} \quad (y')^2 = (x')^3 + 3x - 4$$

Behaviour of reduction type under extensions

For all sufficiently large extensions K'/K, the curve E over K' has either good or multiplicative reduction.

Potential reduction

We say that E has **potentially good** or **potentially multiplicative** reduction according to the type of semistable reduction that E has over an extension of K.

Test of potentially good reduction

E has potentially good reduction if and only if $j(E) = -1728(4a)^3/\Delta$ is integral.

Reduction of torsion points

Suppose that E has good reduction. Since $\mathcal{E}$ is a proper smooth group over R, for any n its n-torsion $\mathcal{E}[n]$ is a finite flat group scheme over R.

Reduction of torsion points

Suppose E has good reduction

- If n is prime to the residue characteristic, then:
  - The reduction map $E[n](K) \to \overline{E}[n](k)$ is injective.
  - The reduction map $E_0[n](K) \to \overline{E}_{sm}[n](k)$ is injective.
  - The reduction map $E[n](\overline{K}) \to \overline{E}[n](\overline{k})$ is an isomorphism of Galois modules.
- If K is an extension of $\mathbb{Q}_p$ with $e < p - 1$, then it is also true that the reduction map $E[n](K) \to \overline{E}[n](k)$ is injective.

The Néron-Ogg-Shaferevich criterion

Let G_K be the absolute Galois group of K and I_K the inertia subgroup.

The Néron-Ogg-Shaferevich criterion

Let ℓ be a prime different from the residue characteristic. Then:

- E has good reduction if and only if I_K acts trivially on $T_\ell(E)$.
- E has semi-stable reduction if and only if I_K acts unipotently on $T_\ell(E)$.

Let's recall some definitions

As unramified extensions of K correspond to extensions of the residue field k, we have,

Inertia subgroup I_K

The **inertia subgroup** I_K of G_K is the set of elements of G_K that act trivially on $\overline{k}$.

Tate module

The ℓ-adic **Tate module** of E, denoted $T_\ell(E)$, is the inverse limit of the groups $E[\ell^n](\overline{K})$, where the transition maps are multiplication by ℓ. Explicitly, an element of $T_\ell(E)$ is a sequence $(x_0, x_1, \cdots)$ of $\overline{K}$-points of E, where $x_0 = O$ and $\ell x_i = x_{i-1}$ for $i > 0$.

The fact that $E[\ell^n](\overline{K}) = (\mathbb{Z}/\ell^n\mathbb{Z})^2$ allows us to define an isomorphism between $T_\ell(E)$ and $\mathbb{Z}_\ell^2$ through the inverse limit.

Example: Action of the inertia subgroup on the 4-torsion of E

$$
P_{(0,0)} = O \begin{cases}
P_{(0,2)} = (2,0) \begin{cases} P_{(0,1)} = (2-\sqrt{5}, -5+\sqrt{5}) \\ P_{(0,3)} = (2-\sqrt{5}, \quad 5-\sqrt{5}) \\ P_{(2,1)} = (2+\sqrt{5}, -5-\sqrt{5}) \\ P_{(2,3)} = (2-\sqrt{5}, \quad 5+\sqrt{5}) \end{cases} \\
P_{(2,0)} = (1,0) \begin{cases} P_{(1,0)} = (1-2i, -2-4i) \\ P_{(3,0)} = (1-2i, \quad 2+4i) \\ P_{(1,2)} = (1+2i, -2+4i) \\ P_{(3,2)} = (1+2i, \quad 2-4i) \end{cases} \\
P_{(2,2)} = (-3,0) \begin{cases} P_{(1,1)} = (-3-2\sqrt{5}, \quad 2i(5+2\sqrt{5})) \\ P_{(3,3)} = (-3-2\sqrt{5}, -2i(5+2\sqrt{5})) \\ P_{(1,3)} = (-3+2\sqrt{5}, -2i(5-2\sqrt{5})) \\ P_{(3,1)} = (-3+2\sqrt{5}, \quad 2i(5-2\sqrt{5})) \end{cases}
\end{cases}
$$

$$E : y^2 = x^3 - 7x + 6$$

$$\Delta = 2^8\, 5^2$$

$$(\mathbb{Z}/4\mathbb{Z})^2 \longrightarrow E[4](K)$$

$$(n,m) \longmapsto P_{(n,m)}$$

Example: Action of the inertia subgroup on the 4-torsion of E

$$P_{(0,0)} = O \begin{cases} P_{(0,2)} = (2,0) \begin{cases} P_{(0,1)} = (2-\sqrt{5}, -5+\sqrt{5}) \\ P_{(0,3)} = (2-\sqrt{5}, \quad 5-\sqrt{5}) \\ P_{(2,1)} = (2+\sqrt{5}, -5-\sqrt{5}) \\ P_{(2,3)} = (2-\sqrt{5}, \quad 5+\sqrt{5}) \end{cases} \\ P_{(2,0)} = (1,0) \begin{cases} P_{(1,0)} = (1-2i, -2-4i) \\ P_{(3,0)} = (1-2i, \quad 2+4i) \\ P_{(1,2)} = (1+2i, -2+4i) \\ P_{(3,2)} = (1+2i, \quad 2-4i) \end{cases} \\ P_{(2,2)} = (-3,0) \begin{cases} P_{(1,1)} = (-3-2\sqrt{5}, \quad 2i(5+2\sqrt{5})) \\ P_{(3,3)} = (-3-2\sqrt{5}, -2i(5+2\sqrt{5})) \\ P_{(1,3)} = (-3+2\sqrt{5}, -2i(5-2\sqrt{5})) \\ P_{(3,1)} = (-3+2\sqrt{5}, \quad 2i(5-2\sqrt{5})) \end{cases} \end{cases}$$

$$E : y^2 = x^3 - 7x + 6$$

$$\Delta = 2^8\, 5^2$$

$$(\mathbb{Z}/4\mathbb{Z})^2 \longrightarrow E[4](K)$$
$$(n,m) \longmapsto P_{(n,m)}$$

Over $K = \mathbb{Q}_7$ the curve has good reduction.

Indeed, $i, \sqrt{5} \notin \mathbb{Q}_7$, but they are both in the extension $\mathbb{Q}_7(i)$.

Example: Action of the inertia subgroup on the 4-torsion of E

$$
P_{(0,0)} = O \begin{cases}
P_{(0,2)} = (2,0) & \begin{cases} P_{(0,1)} = (2-\sqrt{5}, -5+\sqrt{5}) \\ P_{(0,3)} = (2-\sqrt{5}, \quad 5-\sqrt{5}) \\ P_{(2,1)} = (2+\sqrt{5}, -5-\sqrt{5}) \\ P_{(2,3)} = (2-\sqrt{5}, \quad 5+\sqrt{5}) \end{cases} \\
P_{(2,0)} = (1,0) & \begin{cases} P_{(1,0)} = (1-2i, -2-4i) \\ P_{(3,0)} = (1-2i, \quad 2+4i) \\ P_{(1,2)} = (1+2i, -2+4i) \\ P_{(3,2)} = (1+2i, \quad 2-4i) \end{cases} \\
P_{(2,2)} = (-3,0) & \begin{cases} P_{(1,1)} = (-3-2\sqrt{5}, \quad 2i(5+2\sqrt{5})) \\ P_{(3,3)} = (-3-2\sqrt{5}, -2i(5+2\sqrt{5})) \\ P_{(1,3)} = (-3+2\sqrt{5}, -2i(5-2\sqrt{5})) \\ P_{(3,1)} = (-3+2\sqrt{5}, \quad 2i(5-2\sqrt{5})) \end{cases}
\end{cases}
$$

Over $K = \mathbb{Q}_7$,

As $\mathbb{Q}_7(i)$ is unramified, we deduce that $I_{\mathbb{Q}_7(i)/\mathbb{Q}_7} = \{id\}$ and therefore the inertia group acts trivially on $E[4](\overline{\mathbb{Q}_7})$.

Example: Action of the inertia subgroup on the 4-torsion of E

$$
P_{(0,0)} = O
\begin{cases}
P_{(0,2)} = (2,0) & \begin{cases}
P_{(0,1)} = (2-\sqrt{5}, -5+\sqrt{5}) \\
P_{(0,3)} = (2-\sqrt{5}, \quad 5-\sqrt{5}) \\
P_{(2,1)} = (2+\sqrt{5}, -5-\sqrt{5}) \\
P_{(2,3)} = (2-\sqrt{5}, \quad 5+\sqrt{5})
\end{cases} \\
P_{(2,0)} = (1,0) & \begin{cases}
P_{(1,0)} = (1-2i, -2-4i) \\
P_{(3,0)} = (1-2i, \quad 2+4i) \\
P_{(1,2)} = (1+2i, -2+4i) \\
P_{(3,2)} = (1+2i, \quad 2-4i)
\end{cases} \\
P_{(2,2)} = (-3,0) & \begin{cases}
P_{(1,1)} = (-3-2\sqrt{5}, \quad 2i(5+2\sqrt{5})) \\
P_{(3,3)} = (-3-2\sqrt{5}, -2i(5+2\sqrt{5})) \\
P_{(1,3)} = (-3+2\sqrt{5}, -2i(5-2\sqrt{5})) \\
P_{(3,1)} = (-3+2\sqrt{5}, \quad 2i(5-2\sqrt{5}))
\end{cases}
\end{cases}
$$

Over $K = \mathbb{Q}_5$ the curve has multiplicative reduction.

We know that $i \in \mathbb{Q}_5$, but $\sqrt{5} \notin \mathbb{Q}_5$. As the extension $\mathbb{Q}_5(\sqrt{5})/\mathbb{Q}_5$ is ramified, the element $\sigma \in \mathrm{Gal}(\mathbb{Q}_5(\sqrt{5})/\mathbb{Q}_5)$ such that $\sigma(\sqrt{5}) = -\sqrt{5}$ is in $I_{\mathbb{Q}_5}$.

Example: Action of the inertia subgroup on the 4-torsion of E

WARWICK
THE UNIVERSITY OF WARWICK

$$
P_{(0,0)} = O \begin{cases}
P_{(0,2)} = (2,0) & \begin{cases} P_{(0,1)} = (2-\sqrt{5}, -5+\sqrt{5}) \\ P_{(0,3)} = (2-\sqrt{5}, \quad 5-\sqrt{5}) \\ P_{(2,1)} = (2+\sqrt{5}, -5-\sqrt{5}) \\ P_{(2,3)} = (2-\sqrt{5}, \quad 5+\sqrt{5}) \end{cases} \\
P_{(2,0)} = (1,0) & \begin{cases} P_{(1,0)} = (1-2i, -2-4i) \\ P_{(3,0)} = (1-2i, \quad 2+4i) \\ P_{(1,2)} = (1+2i, -2+4i) \\ P_{(3,2)} = (1+2i, \quad 2-4i) \end{cases} \\
P_{(2,2)} = (-3,0) & \begin{cases} P_{(1,1)} = (-3-2\sqrt{5}, \quad 2i(5+2\sqrt{5})) \\ P_{(3,3)} = (-3-2\sqrt{5}, -2i(5+2\sqrt{5})) \\ P_{(1,3)} = (-3+2\sqrt{5}, -2i(5-2\sqrt{5})) \\ P_{(3,1)} = (-3+2\sqrt{5}, \quad 2i(5-2\sqrt{5})) \end{cases}
\end{cases}
$$

Over the basis $\{(1,0),(0,1)\}$, the action of σ over $(\mathbb{Z}/4\mathbb{Z})^2$ is given by the matrix

$$M_\sigma = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

showing that the action of $I_{\mathbb{Q}_5}$ on $E[4](\overline{\mathbb{Q}_5})$ is unipotent.

Corollaries of the Néron-Ogg-Shaferevich criterion

WARWICK
THE UNIVERSITY OF WARWICK

Corollary 1

If I_k acts trivially (or unipotently) on one $T_\ell(E)$ then it does so on all of them.

Corollary 2

E has potentially good reduction if and only if I_K acts through a finite quotient on $T_\ell(E)$.

Corollary 3

Isogenous curves have the same reduction type.

Thank you!

Any questions?

Questions

Proof of the Néron-Ogg-Shafarevich criterion I

First, note that I_K acts trivially on $T_\ell(E)$ if and only if it does so on $E[\ell^n](\overline{K})$ for all n. Thus, if E has good reduction then I_K acts trivially on $T_\ell(E)$ by what we've already shown.

Proof of the Néron-Ogg-Shaferevich criterion I

First, note that I_K acts trivially on $T_\ell(E)$ if and only if it does so on $E[\ell^n](\overline{K})$ for all n. Thus, if E has good reduction then I_K acts trivially on $T_\ell(E)$ by what we've already shown.

Conversely, suppose I_K acts trivially on $T_\ell(E)$. Thus all ℓ^n torsion points belong to $E(K^{un})$. Let d be the order of $E(K^{un})/E_0(K^{un})$, which is finite. Then $E_0(K^{un})[\ell^n]$ is the kernel of the map $E(K^{un})[\ell^n] \to E(K^{un})/E_0(K^{un})$, and thus has cardinality at least ℓ^{2n}/d.

Since the reduction map $E_0(K^{un}) \to \overline{E}_{sm}(\overline{K})$ is injective on ℓ-power torsion, it follows that $\overline{E}_{sm}(\overline{k})[\ell^n]$ has cardinality at least ℓ^{2n}/d. But this is not true for G_m (where the cardinality is ℓ^n) or G_a (where the cardinality is 1), and so E cannot have multiplicative or additive reduction. Thus E has good reduction.

Proof of the Néron-Ogg-Shaferevich criterion II

Now suppose that I_K acts unipotently on $T_\ell(E)$. It thus fixes some vector in $T_\ell(E)$, which implies that $E(K^{un})[\ell^n]$ has cardinality at least ℓ^n. Arguing as in the previous slide, we see that $\overline{E}_{sm}$ cannot be G_a, and so E has semi-stable reduction.

Proof of the Néron-Ogg-Shaferevich criterion II

Now suppose that I_K acts unipotently on $T_\ell(E)$. It thus fixes some vector in $T_\ell(E)$, which implies that $E(K^{un})[\ell^n]$ has cardinality at least ℓ^n. Arguing as in the previous slide, we see that $\overline{E}_{sm}$ cannot be G_a, and so E has semi-stable reduction.

Finally, suppose that E has semi-stable reduction. The multiplication-by-ℓ^n map on the smooth locus $\overline{E}_{sm}$ of E is flat, and so $\overline{E}_{sm}[\ell^n]$ is a flat group scheme over R. Let G be the scheme-theoretic closure in $\overline{E}_{sm}[\ell^n]$ of the set of $\overline{K}$-points which extend to $\overline{R}$-points. Then G is finite and flat, and $G_k = \overline{E}_{sm}[\ell^n]$.

Since G has ℓ-power order, it is étale, and so $G(K^{un}) = \overline{E}_{sm}[\ell^n](\overline{k})$, which contains $\mathbb{Z}/\ell^n\mathbb{Z}$ (since E is semi-stable). Thus $E[\ell^n](K^{un})$ contains $\mathbb{Z}/\ell^n\mathbb{Z}$ for all n, which shows that I_K fixes a vector in $T_\ell(E)$. Since the determinant of $T_\ell(E)$ is the ℓ-cyclotomic character, which is trivial on I_K, the result follows.