R. Vissar

Elliptic Curves - Example Sheet 3

1 (i) $y^2+xy = x^3+1$

p=2 $x=0 \Rightarrow y=1$; $x=1 \Rightarrow y=0$ or 1 $\Big\} \Rightarrow \#\tilde{E}(\mathbb{F}_2)=4$

p=3

x	-1	0	1
x^3+x^2+x+1	0	①	①

$\Big\} \Rightarrow \#\tilde{E}(\mathbb{F}_3)=6$

p=5

x	-2	-1	0	1	2
x^3-x^2-2x+1	3	①	①	④	①

$\Big\} \Rightarrow \#\tilde{E}(\mathbb{F}_5)=9$

p=7

x	-3	-2	-1	0	1	2	3
x^3+2x^2-2x+1	5	5	④	①	②	6	5

$\Big\} \Rightarrow \#\tilde{E}(\mathbb{F}_7)=7$

(ii) Taking $p=2$ & $p=5$ gives

$\#E(\mathbb{Q})_{tors} \mid 2^a$ some $a \geq 0$

$\#E(\mathbb{Q})_{tors} \mid 9.5^b$ some $b \geq 0$ $\Big\} \Rightarrow E(\mathbb{Q})_{tors} = 0$

(iii) $E_2(\mathbb{Q}_2) \subset E_1(\mathbb{Q}_2) \subset E_0(\mathbb{Q}_2) = E(\mathbb{Q}_2)$

$E_2(\mathbb{Q}_2)$: quotient $(\mathbb{F}_2,+)$ has order 2; $E_1(\mathbb{Q}_2)$: quotient $\tilde{E}(\mathbb{F}_2)$ has order 4; $E_0(\mathbb{Q}_2)$: good reduction

We have $E_r(\mathbb{Q}_2) \cong (\mathbb{Z}_2,+)$ for $r > \frac{e}{p-1} = \frac{1}{2-1}$

$\therefore E_2(\mathbb{Q}_2)_{tors} \hookrightarrow \dfrac{E(\mathbb{Q}_2)}{E_2(\mathbb{Q}_2)}$ which has order 8.

(iv) Let $P \in E(\mathbb{Q})$

$\#\tilde{E}(\mathbb{F}_7)=7 \Rightarrow 7P \in E_1(\mathbb{Q}_7) \Rightarrow 7$ in denominator

$\#\tilde{E}(\mathbb{F}_5)=9 \Rightarrow 9P \in E_1(\mathbb{Q}_5) \Rightarrow 5$ in denominator.

$\dfrac{E_0(\mathbb{Q}_7)}{E_1(\mathbb{Q}_7)} \cong \tilde{E}(\mathbb{F}_7)$

so if $P \in E(\mathbb{Q})$, then $7P=0$ in $\tilde{E}(\mathbb{F}_7)$ $\Rightarrow 7P=0$ in $\dfrac{E_0(\mathbb{Q}_7)}{E_1(\mathbb{Q}_7)}$ $\Rightarrow 7P \in \tilde{E}_1(\mathbb{Q}_7)$

2.

p	2	3	5	7	11	13
(i) $\Delta = -26 = -2.13$	—	3	9	9	6	—
(ii) $\Delta = -1664 = -2^7.13$	—	7	7	7	14	—
(iii) $\Delta = 2304 = 2^8.3^2$	—	—	8	8	8	16

(i) $E_1(\mathbb{Q}_3) \subset E(\mathbb{Q}_3)$ $\quad \therefore \#E(\mathbb{Q})_{tors} \leq 3.$

$E_1(\mathbb{Q}_3) \cong (\mathbb{Z}_3,+)$ (112); $E(\mathbb{Q}_3)$: quotient $\tilde{E}(\mathbb{F}_3) \cong \mathbb{Z}/3\mathbb{Z}$ (or use $p=3$ & $p=11$)

(ii) Taking $p=3$ & $p=5$ gives $\#E(\mathbb{Q})_{tors} \leq 7$

(iii) Taking $p=5$ & $p=7$ gives $\#E(\mathbb{Q})_{tors} \leq 8$

(i) $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z} = \{0, (0,0), (0,-1)\}$

(ii) $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/7\mathbb{Z} = \{0, (0,0), (4,8), (2,2), (2,4), (4,0), (0,4)\}$

(iii) $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} = \{0, (0,0), (-1,0), (-4,0), (-2,\pm 2), (2,\pm 6)\}$

3. $$\#\tilde{E}(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3+\lambda x}{p}\right)\right)$$

$$= p+1-a_p$$

where $$a_p = -\sum_{x \in \mathbb{F}_p^*} \left(\frac{x+\lambda x^{-1}}{p}\right)$$ (by Euler's criterion)

$$\equiv -\sum_{x \in \mathbb{F}_p^*} (x+\lambda x^{-1})^{2k} \pmod p$$ (by lemma below)

$$\equiv \lambda^k \binom{2k}{k} \pmod p$$

Lemma Let $r \in \mathbb{Z}$. Then $\displaystyle\sum_{x \in \mathbb{F}_p^*} x^r = \begin{cases} -1 & \text{if } r \equiv 0 \pmod{p-1} \\ 0 & \text{if } r \not\equiv 0 \pmod{p-1} \end{cases}$

Proof Let $S = \displaystyle\sum_{x \in \mathbb{F}_p^*} x^r$. Let g be a primitive root mod p.

Replacing x by gx shows $S = g^r S$

If $r \not\equiv 0 \pmod{p-1}$ then $g^r \neq 1 \pmod p \Rightarrow S \equiv 0 \pmod p$

If $r \equiv 0 \pmod{p-1}$ then $S \equiv p-1 \equiv -1 \pmod p$ □

Since $p \neq 2$ and $\binom{2k}{k} = \frac{(2k)!}{(k!)^2}$ with $k<p$ it follows that $a_p \not\equiv 0 \pmod p$

If $p \equiv 3 \pmod 4$ then $\left(\frac{-1}{p}\right) = -1$. Since $f(x) = x^3 + 2x$ is an odd function it follows that $a_p = 0$.

4 (i) Let $E: y^2 = x^3 + d$ $\quad m = \#E(\mathbb{Q})_{tors}$

If $p \nmid 6dm$ then $E(\mathbb{Q})_{tors} \hookrightarrow \tilde{E}(\mathbb{F}_p)$

If $p \equiv 2 \pmod 3$ then $\mathbb{F}_p^* \to \mathbb{F}_p^*$; $x \mapsto x^3$ an isomorphism

$$\begin{aligned} \#\tilde{E}(\mathbb{F}_p) &= 1 + \#\{(x,y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + d\} \\ &= 1 + \#\{(x,y) \in \mathbb{F}_p^2 \mid y^2 = x + d\} \\ &= p+1 \end{aligned}$$

$\therefore$ For all sufficiently large primes p with $p \equiv 2 \pmod 3$ we have $m \mid (p+1)$.

If $\ell \mid m$ for some prime $\ell \geq 5$, or $4 \mid m$ or $9 \mid m$ then this contradicts Dirichlet's Theorem on Primes in Arithmetic Progression.

$\therefore$ $m \mid 6$.

(ii) $E: y^2 = x^3 + 5$ $\quad P = (-1, 2) \in E(\mathbb{Q})$

Clearly $E(\mathbb{Q})[2] = 0$.

By (i) it suffices to show $3P \neq 0$.

Either: $2P = \left(\left(\frac{3}{4}\right)^2 + 2, \dots\right) \neq -P$

or: $\#\tilde{E}(\mathbb{F}_7) = 7$

or: $\Delta < 0 \Rightarrow E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z} \Rightarrow E(\mathbb{R})[3] = \{0, (0, \pm\sqrt{5})\}$

⋮

5. Method (1) Let $P = (x,y) \in E(\mathbb{Q})_{tors}$. Then $x, y \in \mathbb{Z}$

Equation for $E \Rightarrow y^2 = x(x^2 + ax + b)$ $\quad (*)$

If $2P \neq 0$ then proof of Lutz-Nagell gives $y \mid 3x^2 + 2ax + b$ $\quad (**)$

We claim that $x \mid b$

If not then there exists a prime p with $v_p(x) > v_p(b)$

$(*) \Rightarrow 2v_p(y) = v_p(x) + v_p(b)$

$(**) \Rightarrow v_p(y) \leq v_p(b)$

$\therefore$ $v_p(x) + v_p(b) \leq 2v_p(b) \Rightarrow v_p(x) \leq v_p(b)$ ⚔

If $2P = 0$, yet $x \neq 0$ then x is a root of $x^2 + ax + b = 0$ and so again $x \mid b$.

Finally $x \mid b \Rightarrow x + a + \frac{b}{x} = \left(\frac{y}{x}\right)^2 \in \mathbb{Z}$

$\Rightarrow x + a + b/x$ is a perfect square.

Method (2) There is a 2-isogeny $\phi: E \to E'$

$(x,y) \mapsto \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2-b)}{x^2}\right)$

$P = (x,y) \in E(\mathbb{Q})_{tors} \Rightarrow \phi(P) \in E'(\mathbb{Q})_{tors}$

$\Rightarrow \left(\frac{y}{x}\right)^2 \in \mathbb{Z}$

$\Rightarrow x \mid b$ and $x + a + \frac{b}{x}$ is a perfect square.

6. (i) Take a minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_i \in \mathbb{Z}_p$$

$p \neq 2, 3 \Rightarrow \frac{1}{2}, \frac{1}{3} \in \mathbb{Z}_p$

$\Rightarrow$ the substitutions $y \leftarrow y - \frac{1}{2}a_1x - \frac{1}{2}a_3$, $x \leftarrow x - \frac{1}{3}a_2$ preserve that $a_i \in \mathbb{Z}_p$ (& give $a_1 = a_2 = a_3 = 0$)

Since the discriminant is unchanged the equation is still minimal

(ii) Lemma $y^2 = x^3 + ax + b$ is minimal $\iff$ $v_p(a) < 4$ or $v_p(b) < 6$

Proof "$\Rightarrow$" If $v_p(a) \geq 4$ and $v_p(b) \geq 6$ then

$y^2 = x^3 + p^{-4}ax + p^{-6}b$ is an integral (i.e. $\mathbb{Z}_p$-coefficient) Weierstrass equation with smaller valuation of the discriminant, contradicting minimality of the original equation.

"$\Leftarrow$" By (i) have minimal W. equation $y^2 = x^3 + Ax + B$

$a = u^4 A$, $b = u^6 B$ for some $u \in \mathbb{Q}_p^*$ $\quad \therefore 4a^3 + 27b^2 = u^{12}(4A^3 + 27B^2)$

$y^2 = x^3 + ax + b$ not minimal $\Rightarrow v_p(4a^3 + 27b^2) > v_p(4A^3 + 27B^2)$

$\Rightarrow v_p(u) > 0$

$\Rightarrow v_p(a) \geq 4$ and $v_p(b) \geq 6$ $\square$

(iii) $E/\mathbb{Q}_p$ has good reduction $\Leftrightarrow v_p(\Delta) = 0$

$E/\mathbb{Q}_p$ has multiplicative reduction

$\Leftrightarrow v_p(\Delta) > 0$ & $v_p(a) = v_p(b) = 0$

$E/\mathbb{Q}_p$ has additive reduction $\Leftrightarrow v_p(a) > 0$ & $v_p(b) > 0$

Indeed for additive reduction $x^3 + ax + b \equiv (x - \alpha)^3 \pmod p$

$\Rightarrow p \mid a$ and $p \mid b$

(Also note that if $p \mid \Delta$ then $p \mid a \Leftrightarrow p \mid b$)

$E/\mathbb{Q}_p$ has good reduction $\Rightarrow v_p(\Delta) = 0 \Rightarrow v_K(\Delta) = 0$

$\therefore$ Weierstrass equation still minimal over K

$\therefore$ E/K has good reduction.

$E/\mathbb{Q}_p$ has ~~additive~~ multiplicative reduction $\Rightarrow v_p(\Delta) > 0$ & $v_p(a) = 0$

$\Rightarrow v_K(\Delta) > 0$ & $v_K(a) = 0$

$\therefore$ Weierstrass equation still minimal over K

$\therefore$ E/K has multiplicative reduction

Let E: $y^2 = x^3 + p$ $\qquad K = \mathbb{Q}_p(\sqrt[6]{p})$

Then $E/\mathbb{Q}_p$ has additive reduction, yet E/K has good reduction.

7. $y^2 = x^2(x+1)$.

Putting $y = ux$ gave parametrisation $(x, y) = (u^2 - 1, u(u^2 - 1))$

$u = \pm 1 \Leftrightarrow$ singular point $\Leftrightarrow t = 0, \infty$

$u = \infty \Leftrightarrow$ point at ∞ $\Leftrightarrow t = 1$

This suggests putting $t = \frac{u-1}{u+1}$, ie. $u = \frac{1+t}{1-t}$

$$\phi(t) = \left(\frac{1+t}{1-t}\right)^2 - 1 = \frac{4t}{(1-t)^2}$$

$$\psi(t) = \frac{1+t}{1-t}\,\phi(t) = \frac{4t(t+1)}{(1-t)^3}$$

There is a bijection $E_{ns}(K) \longleftrightarrow K^*$

$(x, y) \longmapsto \frac{y-x}{y+x}$

$(\phi(t), \psi(t)) \longleftarrow\!\shortmid\ t$

To show this is a group homomorphism, consider

$P_1, P_2, P_3 \in E_{ns}(K)$ with $P_1 + P_2 + P_3 = 0$, $\quad P_1, P_2, P_3 \neq O$

Write $P_i = (\phi(t_i), \psi(t_i))$

P_1, P_2, P_3 are collinear, say lying on the line $ax + by = 1$

Then t_1, t_2, t_3 are the roots of

$$4a\,t(1-t) + 4b\,t(t+1) = (1-t)^3$$

Coefficients of t^3 and t^0 $\Rightarrow t_1 t_2 t_3 = 1$ $\quad -1$

$\Rightarrow t_2 = t_1 t_3$ so iso to $K^\times$

8. We have 2-isogenous elliptic curves

E: $y^2 = x(x^2 + ax + b)$

E': $y^2 = x(x^2 + a'x + b')$ $\qquad a' = -2a, b' = a^2 - 4b$

Taking $a = u, b = -16$ gives $a' = -2u$, $b' = u^2 + 64 = p$

Moreover $\Delta(E) = 16\,b^2(a^2 - 4b) = 2^{12} p$

$\Delta(E') = 16\,p^2(4u^2 - 4p) = -2^{12} p^2$

To show E has good reduction at 2

E: $(y + x)^2 = x^3 + ux^2 - 16x$

$\rightsquigarrow$ $y^2 + 2xy = x^3 + (u-1)x^2 - 16x$

$\rightsquigarrow$ $y^2 + xy = x^3 + \frac{u-1}{4}x^2 - x$ $\qquad (\Delta = p)$

To show E' has good reduction at 2

E' : $y^2 = x((x-u)^2+64)$

$\rightsquigarrow$ $(y+x)^2 = (x+u)(x^2+64)$

$\rightsquigarrow$ $y^2+2xy = x^3+(u-1)x^2+64x+64u$

$\rightsquigarrow$ $y^2+xy = x^3+\frac{u-1}{4}x^2+4x+u$ $\quad(\Delta=-p^2)$

Tamagawa numbers at p?

E : $y^2 = x\left((x+\frac{1}{2}u)^2-\frac{1}{4}p\right)$

If $(x,y)\in E(\mathbb{Q}_p)$ reduces to the singular point then

$v_p(x+\frac{1}{2}u)\geq 1$ & $v_p(y)\geq 1$ $\Rightarrow$ $v_p(\frac{1}{4}p)\geq 2$ ⨯

$\therefore$ $c_p(E)=1$

On E' the point $T=(0,0)$ reduces to the singular point

$\therefore$ $c_p(E')>1$

(If $P=(x,y)\in E'(\mathbb{Q}_p)$ then $P+T=\left(\frac{p}{x},\dots\right)$

$\therefore$ exactly one out of P and $P+T$ reduces to the singular point $\therefore$ $c_p(E')=2$)

9 (i) Consider the morphism $\psi: E\to E$; $P\mapsto \phi(P)-P$

If ψ is surjective then ϕ has a fixed point.

Otherwise ψ is constant, so ϕ (& hence ϕ^n) is a translation map.

(ii) Say $C\subset\mathbb{P}^d$. Let $\phi: C\to C$, $(x_0:\dots:x_d)\mapsto(x_0^q:\dots:x_d^q)$] Frobenius

We have $C(\mathbb{F}_{q^n}) = \{P\in C \mid \phi^n(P)=P\}$

Picking $P\in C(\overline{\mathbb{F}}_q)$ gives an elliptic curve (E,P) over $\overline{\mathbb{F}}_q$

If $P=(a_0:\dots:a_d)$, $a_i\in\overline{\mathbb{F}}_q$ then $[\mathbb{F}_q(a_0,\dots,a_d):\mathbb{F}_q]<\infty$

So $\exists\, n\geq 1$ s.t. $0<|C(\mathbb{F}_{q^n})|<\infty$

$\Rightarrow$ ϕ^n cannot be a translation map

$\Rightarrow$ ϕ cannot be a translation map $\Rightarrow$ ϕ has fixed point

$\Rightarrow$ $C(\mathbb{F}_q)\neq\emptyset$ by (i)

10. $E/\mathbb{Q}_p$ $y^2=x^3+ax+b$ $a,b\in\mathbb{Z}_p$ $p\geq 5$

(i) Taking $a=-3$, $b=2+p^n$ gives a minimal W. equation with $4a^3+27b^2 = 27(4p^n+p^{2n}) \Rightarrow v_p(\Delta)=n$

(ii) If $E/\mathbb{Q}_p$ has additive reduction then

$x^3+ax+b\equiv(x-\alpha)^3 \pmod p$ for some $\alpha\in\mathbb{Z}_p$

Coefficient of x^2 $\Rightarrow$ $\alpha\equiv 0\pmod p$ $\Rightarrow$ $p\mid a$ and $p\mid b$

If $v_p(\Delta_E)\geq 12$ then $p^{12}\mid(4a^3+27b^2)$

Then $p^3\mid b^2$ $\Rightarrow$ $p^2\mid b$

& $p^4\mid a^3$ $\Rightarrow$ $p^2\mid a$

& $p^5\mid b^2$ $\Rightarrow$ $p^3\mid b$

Let E' : $y^2=x^3+p^{-2}ax+p^{-3}b$] quadratic twist of E by p

If $E'/\mathbb{Q}_p$ has additive reduction then repeating the above argument gives $p^4\mid a$ and $p^6\mid b$. This contradicts that we started with a minimal Weierstrass equation.

Therefore at least one out of E and E' has multiplicative red^n.

11. Let $C = B/A$. Applying the snake lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ & & \downarrow{\scriptstyle\times n} & & \downarrow{\scriptstyle\times n} & & \downarrow{\scriptstyle\times n} & & \\ 0 & \to & A & \to & B & \to & C & \to & 0 \end{array}$$

gives an exact sequence

$$0\to A[n]\to B[n]\to C[n]\to \frac{A}{nA}\to\frac{B}{nB}\to\frac{C}{nC}\to 0$$

$\Rightarrow$ $q(B)=q(A)\,q(C)$

The exact sequence $0\to C[n]\to C\xrightarrow{\times n} C\to\frac{C}{nC}\to 0$

shows that if C is finite then $q(C)=1$

$\therefore$ $q(A)=q(B)$

12. Lemma $\mathcal{O}_K^*$ and $E(K)$ have subgroups of finite index isomorphic to $(\mathcal{O}_K, +)$

Proof

$$\begin{array}{ccccccc} \hat{\mathbb{G}}_m(\pi^r \mathcal{O}_K) & & & & \hat{\mathbb{G}}_m(\pi \mathcal{O}_K) & & \\ \| & & & & \| & & \\ 1+\pi^r \mathcal{O}_K & \subset & \cdots & \subset & 1+\pi \mathcal{O}_K & \subset & \mathcal{O}_K^* \\ \text{if } r > \frac{e}{p-1} \longrightarrow \| & & & & & & \\ (\mathcal{O}_K, +) & & \text{quotients} \cong (k,+) & & & & \text{quotient} \cong k^* \end{array}$$

For $E(K)$ the result was proved in lectures $\square$

By Question 11

$$\frac{|\mathcal{O}_K^* / (\mathcal{O}_K^*)^n|}{|\mu_n(K)|} = \frac{|\mathcal{O}_K / n\mathcal{O}_K|}{1}$$

$$\frac{|E(K)/nE(K)|}{|E(K)[n]|} = \frac{|\mathcal{O}_K / n\mathcal{O}_K|}{1}$$