Elliptic Curves, Example Class 3

25/11/2019

Q1: Some numerical answers

1.

p	2	3	5	7	11	13
$\#\tilde{E}(\mathbb{F}_p)$	4	6	9	7		

Q2:

(i)	–	3	9	9	6	–
(ii)	–	7	7	7	14	–
(iii)	–	–	8	8	8	16

note where discrete is

For numerical answers, after $p=2$, might as well complete the square.

(ii). $\#E(\mathbb{Q})_{tors} \mid 2^9 \cdot 4$ for some a.
$\#E(\mathbb{Q})_{tors} \mid 5^b \cdot 9$

Putting together: $\#E(\mathbb{Q})_{tors} = 1$ (trivial)

(iii) Get a filtration:

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

$E_1(\mathbb{Q}_2) \to \{1\}$
$(\mathbb{Q}_2, +)$

$$E(\mathbb{Q}_2)_{tors} \hookrightarrow \frac{E(\mathbb{Q}_2)}{E_2(\mathbb{Q}_2)}$$

$r > \frac{e}{p-1}$

$p=2, \ e=1$

We need to bound: $\frac{E(\mathbb{Q}_2)}{E_1(\mathbb{Q}_2)}$ and $\frac{E_1(\mathbb{Q}_2)}{E_2(\mathbb{Q}_2)}$.

Now: $\frac{E(\mathbb{Q}_2)}{E_1(\mathbb{Q}_2)} \cong \hat{E}(\mathbb{F}_2)$ order 4 $\qquad \frac{E_1(\mathbb{Q}_2)}{E_2(\mathbb{Q}_2)} \cong (\mathbb{F}_2, +)$ order 2

$\therefore$ Order divides $4 \cdot 2 = 8$.

(iv): $E(\mathbb{Q}_7) \longrightarrow \hat{E}(\mathbb{F}_7)$

$7P \longmapsto O$

$7P \in E_1(\mathbb{Q}_7)$.

$E(\mathbb{Q}_5) \longrightarrow \hat{E}(\mathbb{F}_5)$

$aP \longmapsto O$

$aP \in E_1(\mathbb{Q}_5)$.

2 (i). By calculation, get order divides 3.
Check $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$ gen by $(0,0)$.

(ii) By calc, get order divides 7:
$E(\mathbb{Q}) \cong \mathbb{Z}/7\mathbb{Z}$ gen by $(0,0)$

(iii) $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

Note, clearly get 2-torsion points $E[2]$.

Can check a 2-torsion is twice something else.

$$E(\mathbb{Q})[2] \cup \{(-2, \pm 2), (2, \pm 6)\}$$

↑ this includes $\mathcal{O}_E$.

Q3: $y^2 = x^3 + \lambda x$

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

$$= p + 1 - a_p.$$

$$a_p = -\sum_{x \in \mathbb{F}_p} \left(\frac{x^3+\lambda x}{p}\right)$$

$$\equiv -\sum_{x \in \mathbb{F}_p} (x^3 + \lambda x)^{\frac{p-1}{2}} \pmod{p}$$

$$= -\sum_{x \in \mathbb{F}_p} (x^3 + \lambda x)^{2k}$$

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

(can factor out squares out here Legendre symbol)

Lemma: Let $r \in \mathbb{Z}$

$$\underbrace{\sum_{x \in \mathbb{F}_p^*} x^r}_{S} = \begin{cases} -1 & \text{if } (p-1) \mid r \\ 0 & \text{otherwise.} \end{cases}$$

Let $g \in \mathbb{F}_p^*$ be a generator.

$$S = \sum_{x \in \mathbb{F}_p^*} (gx)^r = g^r S$$

If $g^r \not\equiv 1 \pmod p$ we get $S \equiv 0 \pmod p$.

which finishes the lemma:

$\Longrightarrow$

If $p \equiv 2 \pmod 3$ then

$$\begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \mathbb{F}_p^* \\ x & \longmapsto & x^3 \end{array}$$

is an isomorphism

as $3 \nmid |\mathbb{F}_p^*|$.

The trivial kernel, thus surjective.

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

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

If $p \equiv 2 \pmod 3$,

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

For all suff. large primes p with $p \equiv 2 \pmod 3$, we've shown that $m \mid (p+1)$.

We must show that if $\ell \geq 5$ is a prime then $\ell \nmid m$. & $4 \nmid m$ or $9 \nmid m$.

- We must check all 3 cases, to get that $m \mid 6$.

Just use Dirichlet.

(ii): Many ways to do this. ☺

$E: y^2 = x^3 + 5 \qquad P = (-1, 2)$.

We know $\#E(\mathbb{Q})_{tors} \mid 6$.

- Can use $p = 7$ $\#\hat{E}(\mathbb{F}_7) = 7$
  Get subgp trick, use $P = (-1, 2)$
- Get 2-torsion: $\#E(\mathbb{Q})_{tors} \mid 3$.
- Look at real 3-torsion points:

$$E(\mathbb{R})[3] \cong \begin{cases} \mathbb{R}/\mathbb{Z} & \text{disc} > 0 \\ \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2 & \text{disc} < 0 \end{cases}$$

Thus, we get: $E(\mathbb{R})[3] \cong \{0, (0, \pm\sqrt{5})\}$
and check they're not rational.

- Or, note $P = (-1, 2)$, and $(-1, -2)$ and calculate $2P$ is another point, so can't be 3 torsion. Thus.

Q5: $\left[y^2 = x^3 + ax^2 + bx \right.$
$x = 0$ or $x \mid b$ and $x + a + \frac{b}{x} = q^2 = \left(\frac{y}{x}\right)^2$

Thus, most of the question is to prove $x \mid b$.

$P = (x, y)$ $\quad 2P = (x_3, y_3)$

2-torsion $\Rightarrow y = 0 \Rightarrow x = 0$ or $x^2 + ax + b = 0$

$\Downarrow$

Suppose roots $\alpha_1, \alpha_2 \in \mathbb{Z}$
$\Rightarrow \alpha_1 \alpha_2 = b$.

$P \notin E[2] \Rightarrow x, y \neq 0$.

$$x_3 = \left(\frac{3x^2 + 2ax + b}{2y}\right)^2 - a - 2x$$

$\Rightarrow y^2 = x^3 + ax^2 + bx \mid (3x^2 + 2ax + b)^2$

$\Rightarrow x(x^2 + ax + b) \mid (a - 3b)x^2 + abx + b^2$
$= b(x^2 + ax + b) + (a^2 - 4b)x^2$.

$\Rightarrow x \mid b(x^2 + ax + b)$
$\Rightarrow x \mid b^2$.

$\longrightarrow$.

Can play around with valuations to get $x \mid b$.
Two facts at our disposal.

$y^2 = x(x^2 + ax + b)$ - ①
$y \mid (3x^2 + 2ax + b)$ - ②

Suppose $\exists$ prime p with $v_p(x) > v_p(b)$.

① $\Rightarrow$ $2v_p(y) = v_p(x) + v_p(b)$

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

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

$v_p(x) \leq v_p(b)$ $\longrightarrow$ Get contradiction! $\longrightarrow$

OR: Use 2-isogeny: $(x,y) \xmapsto{\phi} \left(\left(\frac{y}{x}\right)^2, \dots\right)$

$\therefore$ $\left(\frac{y}{x}\right)^2$ is integer

$\therefore$ $x + a + \frac{b}{x}$ is integer ☺

Q: Def^n of minimal Weierstrass equation (not just short Weier) over all ~~they~~ long.

So they exist, but they might be long.

E/$\mathbb{Q}_p$. Take a minimal W eq^n:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$a_i \in \mathbb{Z}_p$.

We substitute: $y \leftarrow y - \frac{1}{2}a_1x - \frac{1}{2}a_3$

$x \leftarrow x - \frac{1}{3}a_2$.

$$\rightsquigarrow \quad y^2 = x^3 + ax + b.$$

Want $v(\Delta') = v(\Delta)$ and coefficients in $\mathbb{Z}_p$.

Want • coeffs in $\mathbb{Z}_p$

• $v(\Delta)$ same as before.

If $a=1$, then v is unchanged ✓.

Need $2, 3 \in \mathbb{Z}_p^*$ (are units) NB:

It really can happen that if $p=2, 3$ then cannot write down minimal Weierstrass eq^n in shorter form.

$\longrightarrow$

Get: $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}_p$ is minimal $\iff$

$$\begin{cases} v_p(a) < 4 \\ \text{or } v_p(b) < 6. \end{cases}$$

"$\Longrightarrow$" If $v_p(a) \geq 4$ & $v_p(b) \geq 6$.

then Consider: $y^2 = x^3 + \left(\frac{a}{p^4}\right)x + \left(\frac{b}{p^6}\right)$

which contradicts minimality.

"$\Leftarrow$" By (i), have a minimal Weierstrass equation.
$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}_p$.

$\therefore \begin{matrix} a = u^4 A \\ b = u^6 B \end{matrix}$ } for some $u \in \mathbb{Q}_p^*$

Then show $v_p(u) > 0$.

Must be an if and only if argument (both implications) are required. $\longrightarrow$

What about reduction?
Good reduction still true reduction of disc $v(\Delta)$ changes by even (but 0 goes to 0, so no change).

Additive reduction $\Rightarrow x^3 + ax + b \equiv (x-\alpha)^3 \pmod{p}$.
$\Rightarrow p \mid a$ and $p \mid b$.

(Note, if $p \mid \Delta$, then "$p \mid a \Leftrightarrow p \mid b$").

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

$\Rightarrow v_k(\Delta) > 0$ & $v_k(a) = 0$.

$\Rightarrow E/k$ has mult. red^n $\longrightarrow$.

W. eqn is still minimal.

Now, this doesn't work for additive reduction, as equation might <u>not</u> be minimal.

E.g: $y^2 = x^3 + p$] $E/\mathbb{Q}_p$ has additive reduction.
$p \geq 5$.

over K

$K = \mathbb{Q}_p(\sqrt[6]{p})$.

$y^2 = x^3 + 1$] E/K has good reduction

Q7: Need to find parameterisation:

$$X(t) = \frac{4t}{(1-t)^2}, \quad Y(t) = \frac{4t(1+t)}{(1-t)^3}$$ ← Use sub: $y = \lambda(t)x$ to get this.

$$K^\times \longrightarrow \tilde{E}_{ns}$$
$$t \longmapsto (x(t), y(t)).$$

$ax + by = 1.$

$$t = 1 - \frac{2}{y+1} = \frac{y-x}{y+x}$$

$$y^2 = x^2(x+1) \Rightarrow y^3 + y^2 = x^3 + y^3 + x^2$$
$$= (x+y)(x^2 - xy + y^2) + x^2$$

$$\left(\frac{y}{x}\right)^2(y+1) = (x+y)\left(1 - \frac{y}{x} + \left(\frac{y}{x}\right)^2\right) + 1.$$

Q8: Can calculate discriminants:

$$\Delta(E) = 2^{12} p$$
$$\Delta(E') = -2^{12} p^2.$$

First transform curves to ensure $v_2(\Delta) = 0$.

$$E' : y^2 = x((x-4)^2 + 64).$$

$$\rightsquigarrow \quad y^2 = (x+4)(x^2+64)$$
$$= x^3 + 4x^2 + 64x + 64 \cdot 4.$$

$$\rightsquigarrow \quad (y+x)^2 = x^3 + 4x^2 + 64x + 64 \cdot 4.$$

$$\Rightarrow \quad y^2 + 2xy = x^3 + (4-1)x^2 + 64x + 64 \cdot 4.$$

$$\rightsquigarrow \quad y^2 + xy = x^3 + \frac{4-1}{4} x^2 + 4x + 4.$$

Tamagawa numbers

$E/\mathbb{Q}_p$: $y^2 = x^3 + p$.

Does there exist $(x,y) \in E(\mathbb{Q}_p)$ reducing mod p to $(0,0) \in \tilde{E}(\mathbb{F}_p)$?

Answer: **No!** $\Rightarrow \quad c_p(E) = 1.$

i.e. want $x, y \in \mathbb{Z}_p$ s.t. $p \mid x$, $p \mid y$ & $y^2 = x^3 + p$.

$E/\mathbb{Q}_p$: $y^2 = x^3 + p^2$

Does there exist $(x,y) \in E(\mathbb{Q}_p)$ reducing mod p to $(0,0) \in \tilde{E}(\mathbb{F}_p)$.

Yes $(x, y) = (0, p)$

$\Rightarrow c_p(E) > 1.$

Q10: $y^2 + ax + b \equiv (x-\alpha)(x-\beta)^2 \pmod{p}$

Want: $4a^3 + 27b^2 \equiv 0 \pmod{p}$

e.g. $a \equiv -3 \pmod{p}$
$b \equiv 2 \pmod{p}$

If take $a = -3 + p^{\text{large num}}$
$b = 2 + p^{\text{large num}}$

then can get values as large as you like!!