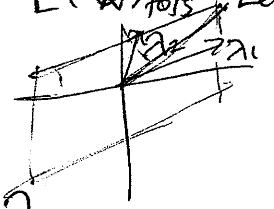
Brian Conrad

① 15.07.2011

Torsion in elliptic curves: points of finite order

1) Insights from complex analysis

E: elliptic curve over $\mathbb{Q}$. What can be said about $E(\mathbb{Q})_{tors}$? Let's first look at $E(\mathbb{C})$



$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda \longrightarrow$ lattice $\mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$

$E(\mathbb{C})[3] = \left(\frac{1}{3}\Lambda\right)/\Lambda \longrightarrow \frac{a}{3}\lambda_1 + \frac{b}{3}\lambda_2$

With the unit circle C: $C = \mathbb{R}/2\pi\mathbb{Z} \Rightarrow C[n] = \left(\frac{2\pi\mathbb{Z}}{n}\right)/2\pi\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$

regular n-gon $\Leftarrow$ cyclic $\Leftarrow$ generated by $2\pi/n$

Algebraically, on $\{y(x) = f(x)\}$, "$[5](P) = 0$" is messy in terms of (x,y)

In unit circle $(\cos(n\theta), \sin(n\theta)) = (1,0)$ $\quad ([n](P) = 0)$

$\underbrace{}$ polynomials over $\mathbb{Q}$ in terms of cos, sin $\Rightarrow$ n-torsion on C have algebraic coordinates

Likewise, points on $E(\mathbb{C})[n]$ have algebraic coordinates.
(lie in a number field depending on n,)

and $E(\mathbb{C})[n] \simeq (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$

We might guess that this works for elliptic curves in characteristic $p > 0$, if $p \nmid n$

Which points in $E(\mathbb{C})_{tors}$ have coordinates in $\mathbb{Q}$
relative to "$y^2 = f(x)$" equation

Is $E(\mathbb{Q})_{tors}$ finite or infinite?

2) A p-adic method to control $E(\mathbb{Q})_{tors}$

Warm-up: If $x_0^n \equiv 1 \bmod p$ and $p \nmid n$, then x_0 uniquely lifts to a solution of $x^n=1$ in

Why? Apply Hensel's Lemma to $f(x)=x^n-1$, $f'(x)=x^{n-1}\cdot n$, so $f'(x_0)=nx_0^{n-1}\not\equiv 0$.

Conclusion: for $p\nmid n$, $\{n^{th} \text{ roots of } 1 \text{ in } \mathbb{Z}_p^\times\} \xrightarrow{\text{reduction}} \{n^{th} \text{ roots of } 1 \text{ in } \mathbb{F}_p^\times\}$ is injective (even bijective)

Warning: $p=2, n=2$,

$$\begin{tikzcd} \mathbb{Z}_2^\times \arrow[r] \arrow[d] & \mathbb{F}_2^\times=\{1\} \\ \{\pm 1\} & \end{tikzcd}$$

This shows that {"prime-to-p" roots of unity in $\mathbb{Z}_p^\times$} is finite, because injec
n^{th} root for $p\nmid n$

into $\mathbb{F}_p^\times$. In fact, this group has size dividing $p-1$ $(=p-1)$

To adapt this to elliptic curves (and n-torsion in $E(\mathbb{Q})$), we need to make sense of "E mod p" (for most p)

Conundrum: there is no map between fields of different characteristics:

$$\begin{tikzcd} \mathbb{Z}_p \arrow[r, two heads] \arrow[d, phantom, "\cap"] & \mathbb{F}_p \\ \mathbb{Q}_p & \end{tikzcd}$$ eg

Likewise, no map of fields

$$\begin{tikzcd} \mathbb{Q} \arrow[r] \arrow[d, phantom, "\cup"] & \mathbb{F}_5 \\ \{q\in\mathbb{Q} \mid 5\nmid \mathrm{denom}(q)\} \arrow[ur] & \end{tikzcd}$$ $(\approx \mathbb{Z}_5)$

For any finite set of rational numbers and polynomial relation among them over $\mathbb{Q}$, only finitely many p occur in denominators (so, makes sense mod p^n for almost all p)

Back to $E(\mathbb{Q})$:

$E=\{y^2=f(x)\}$ over $\mathbb{Q}$. Consider ~~points~~ $p \nmid$ denom(coefficient of f)

$\Longleftrightarrow$ f has coefficients in $\mathbb{Z}_p$ $(\subset \mathbb{Q}_p)$

$\Rightarrow$ OK for almost all p. Consider $\{y^2=\underbrace{\bar{f}(x)}_{f \bmod p}\}$ over $\mathbb{F}_p$

Ex $\{y^2=x^3-51\}$ — 17 is bad/no distinct roots

Call such p good for E if $\bar{f}$ has distinct roots in an extension of $\mathbb{F}_p$.

nonzero rational

i.e. $\mathrm{disc}(f)\in\mathbb{Z}_p^\times \Longleftrightarrow \mathrm{disc}(\bar{f})\not\equiv 0 \pmod p$

p good $\iff$ $p \nmid$ denom of coef. of f and $p \nmid$ numerator of disc(f)

almost all p.

for good p, we can define $\bar{E} = E \bmod p = \{ y^2 = \bar{f}(x) \}$ over $\mathbb{F}_p$

Ex $\{y^2 = x^3 - 51\}$ bad $p = 2, 3, 17$

$\{y^2 = x^3 - n^2 x = x(x-n)(x+n)\}$ bad p: $2, 3$, $p \mid n$

Lemma Suppose p is good for E. $E(\mathbb{Q}_p) \to \bar{E}(\mathbb{F}_p)$ is a homomorph

$$\infty \mapsto \bar{\infty}$$

$$(x,y) \mapsto \begin{cases} (\bar{x}, \bar{y}) & \text{if } x, y \in \mathbb{Z}_p \\ \bar{\infty} & \text{otherwise} \end{cases}$$

Thm For good p, $E(\mathbb{Q}_p)_{tors} \to \bar{E}(\mathbb{F}_p)$ is injective on prime-to-p tor

$\left(\begin{matrix} \cup \\ E(\mathbb{Q})_{tors} \end{matrix} \right)$ ← we care about this anyways

Pf Same as Hensel's Lemma w/ algebraic geometry.

3) Applications

Thm If p, p' are two distinct good primes for E over $\mathbb{Q}$, then

$$E(\mathbb{Q})_{tors} \to E(\mathbb{F}_p) \times E(\mathbb{F}_{p'})$$ is injective ($E(\mathbb{Q})_{tors}$ finit

Pf $n = p^r n'$, $p \nmid n'$

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \quad (\text{since } \mathbb{Z}/n\mathbb{Z} \subset E(\mathbb{Q}))$$

Ex $E = (y^2 = x^3 - 51)$ we know there are no $\mathbb{Z}$-points, but $\exists\, \mathbb{Q}$-points, $\left(\frac{1375}{9}, \ldots\right.$

5, 7 good. So, $E(\mathbb{Q})_{tors} \to E(\mathbb{F}_5)$ injective away from 5-part.

$\#6$

$\Rightarrow$ All torsion is for $\{2, 3, 5\}$, thus $E(\mathbb{Q})_{tors} \hookrightarrow E(\mathbb{F}_7) \Rightarrow E(\mathbb{Q})_{tors} = 1$

Ex $(y^2 = x^3 - n^2 x) = E_n$

Claim: $\# E_n(\mathbb{Q})_{tors} = 4$ ($\Rightarrow E_n(\mathbb{Q})_{tors} = E_n[2]$) Most p are good for E_n; $p >$

Earlier exercise: $\# E_n(\mathbb{F}_p) = p+1$ for $p \equiv 3\ (4)$, $p > 6n$

$\Rightarrow \# E(\mathbb{Q})_{tors} \xrightarrow{\text{prime-to-}p} \Big|\ p+1$

$\Longrightarrow \# E(\mathbb{Q})_{tors} \ \Big|\ \underset{\substack{p \equiv 3(4) \\ p > \text{big}}}{\gcd}(p+1) = 4$ ↳ Dirichlet