So $F(x)=0$, a contradiction, since then $(x,0)$ has order 2 & order 3.

So $\psi_3(x) = 3(x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)$.

There are eight points of order 3 on $E$:

$$\beta_1 \pm \sqrt{F(\beta_1)},\ \beta_2 \pm \sqrt{F(\beta_2)},$$
$$\beta_3 \pm \sqrt{F(\beta_3)},\ \beta_4 \pm \sqrt{F(\beta_4)}.$$

So $E(\mathbb{Q})[3] = 9$.
Since all nonidentity points in $E(\mathbb{Q})[3]$ have order 3, $E(\mathbb{Q})[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. (QED)

Comments

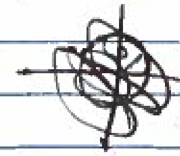
1) The points of order 3 are the points of inflection on the curve.

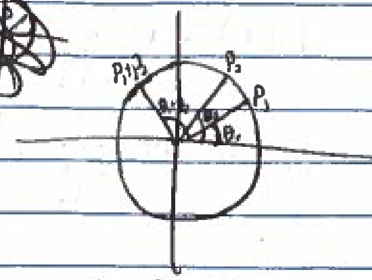
2) There are always exactly 3 points of order 3 points in $E(\mathbb{R})[3]$.
So we cannot have $\mathbb{Z}_3 \times \mathbb{Z}_3$ contained in $E(\mathbb{Q})_{tors}$.

§2.2// Real & complex points on cubic curves.

How can you parametrize the complex points on an elliptic curve?

There is a strong analogy with solutions to the equation $x^2+y^2=1$. This set has a group law too.






$$P_3 = P_1 * P_2 = (x_1,y_1)*(x_2,y_2) = (x_1x_2 - y_1y_2,\ x_1y_2 + x_2y_1)$$
$$P_i = (\cos(\theta_i), \sin\theta_i).$$

Weierstrauss's Elliptic functions

DEF| A lattice is $L = \{m\omega_1 + n\omega_2 : m,n \in \mathbb{Z}\}$ where $\omega_1$ & $\omega_2$ are fixed complex numbers and $\omega_1$ and $\omega_2$ are linearly independent over $\mathbb{R}$.

DEF| $$\wp_L(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

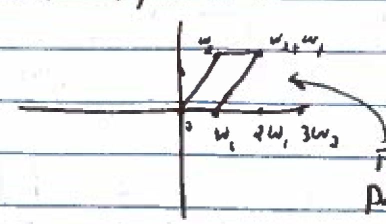
The Weierstrass p-function

$$\wp_L(z+\omega_1) = \wp_L(z)$$
$$\wp_L(z+\omega_2) = \wp_L(z).$$

Day 12

§2.2// Real and complex points on Elliptic curves

Latex! $\to$ (\wp)




$\wp_L(z)$ converges if $z \notin L$.

If $z$ is in $L$, $\wp_L$ has a double pole at $z$.

Crazy Fact!

There are constants $g_2(L)$ & $g_3(L)$ so that $\wp_L'(z)^2 = 4\wp_L^3(z) - g_2(L)\wp_L(z) - g_3(L)$ for all $z \notin L$.

$$g_2(L) = 60 \sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{w^4}$$

$$g_3(L) = 140 \sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{w^6}.$$

Addition Formula

$$\wp(u+v) = \frac{1}{4}\left(\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\right)^2 - \wp(u) - \wp(v)$$

$$\wp'(u+v) = \frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\wp(u+v) + \frac{\wp(u)\wp'(v)-\wp(v)\wp'(u)}{\wp(u)-\wp(v)}$$

Consequently, if we define $E: y^2 = 4x^3 - g_2(L)x - g_3(L)$ then the map $\phi: \mathbb{C} \to E(\mathbb{C})$

$z \longmapsto (\wp_L(z), \wp_L'(z))$

is a homomorphism.

Specifically, if $z, w \in \mathbb{C}$ and $\phi(z) = P$ and $\phi(w) = Q$, then

$$\phi(z+w) = P + Q$$

Group Law.

THM ① The map $\phi: \mathbb{C} \to E(\mathbb{C})$ is a surjective homomorphism

② The kernel of $\phi$ is $L$.

③ So $E(\mathbb{C}) \cong \mathbb{C}/L$.

④ If $g_2$ & $g_3$ are any constants so that $4x^3 - g_2x - g_3$ has distinct roots, $\exists$ a lattice $L$ so that $g_2(L) = g_2$ & $g_3(L) = L$

Comment

How do we define $\wp_L(z)$ when $z \in L$?

We can take a limit.

$$\lim_{w \to z} (\wp_L(w), \wp_L'(z))$$

$$= \lim_{w \to z} (\wp_L(w) : \wp_L'(w) : 1)$$

$\wp_L(w) \approx \frac{c}{(w-z)^2}$, $c \neq 0$.

$\wp_L'(w) \approx \frac{-2c}{(w-z)^3}$

$$= \lim_{w \to z} (\wp_L(w)(w-z)^3 : \wp_L'(w) : (w-z)^3)$$

$$= (0 : -2c : 0)$$

$$= (0 : 1 : 0).$$

Comment 2

$E(\mathbb{C}) \cong \mathbb{C}/L$ because of the 1st Isomorphism THM.

Ex] $E: 4y^2 = x^3 - 13392x - 1080432$

$P = (168, 594)$ is a point of order 5.

We can take $w_1 = 0.211535\ldots \in \mathbb{R}$

$w_2 = 0.105767 + 0.243516i$

$\phi(z) = P$

$z = 0.1269209 = \frac{3}{5}w_1$.

$2z = 0.253841\ldots > w_1$

$\equiv 0.042307 \pmod{L} = \frac{1}{5}w_1$.

$2^2-1$ $3^2-1$ $4^4-1$ $5^4-1$

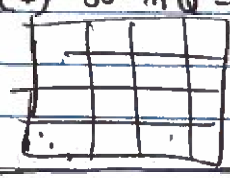
3, 8,

125 × 25 625 250 3125 $\boxed{3124}$

$$\boxed{E(\mathbb{C})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}}$$

As a consequence, If $P \in E(\mathbb{C})$ then there are $m^2$ points $Q \in E(\mathbb{C})$ so that $mQ = P$.

There are $m^2$ points $Q$ in $E(\mathbb{C})$ so $mQ = O$



$\boxed{\text{Day 13}}$

Points of Finite order $E(\mathbb{Q})$

THM (Lutz-Nagell)
Suppose $E: y^2 = x^3 + ax^2 + bx + c$ is an elliptic curve and $P = (x,y)$ is a point of finite order on $E$.
Then
1) $x, y \in \mathbb{Z}$
2) $y = 0$ or $y \mid D$ where $D$ is the discriminant of $E$.

$\boxed{\text{DEF}}$ If $f(x) = x^3 + ax^2 + bx + c$
$= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$
then the discriminant of $f$ is
$$D = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$$

Quadratic: If $D = b^2 - 4ac < 0$ then $f(x)$ has complex roots
If $D > 0$ then $f(x)$ has real root.
If $D = 0$ then $f(x)$ has a repeated root

Cubic
$D = 0 \iff f$ has a repeated root.
$D > 0$ iff all roots of $f(x)$ are real.

If $D \neq 0$ then if $p$ is prime $f(x)$ has a repeated root mod $p$
$\iff$
$p \mid D$. (i.e., $D = 0$ in $\mathbb{F}_p$).

Also, $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

THM
Any symmetric polynomial can be written as a polynomial in the elementary symmetric polynomials.

The discriminant is a symmetric polynomial, so we can express it in terms of
$a = -\alpha_1 - \alpha_2 - \alpha_3$
$b = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$
$c = -\alpha_1\alpha_2\alpha_3$

$D = 0 \iff f$ has a repeated root $\iff$
$\exists\, x$ s.t. $f(x) = f'(x) = 0$
If $D \neq 0$, $\gcd(f(x), f'(x)) = 1$.
You can write $D$ as a linear polynomial combination of $f(x)$ & $f'(x)$.