3705 Elliptic Curves Notes

Based on the 2014 spring lectures by Dr R M Hill

15.01.2014.

Elliptic Curves

Office Hour: Wednesday 10-11

Introduction:

Suppose $f(\underline{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$.

General Problem: Solve the equation $f(x_1, \ldots, x_n) = 0$ $(x_i \in \mathbb{Z})$

"Diaphontine equation".

First case: $n=1$ $f(x) = a_d x^d + \ldots + a_0$

every rational root is of the form $\frac{r}{s}$ where
$r \mid a_0$
$s \mid a_d$

next consider: $n=2$

$f(x,y) = 0$

If the degree of f is 1, then we can find solutions by linear algebra.

If degree $(f) = 2$, then the equation $f(x,y)=0$ is called a "conic".

Hard Theorem $\left\{ \begin{array}{l} \text{A conic has a rational solution iff it has} \\ \bullet \text{ a real solution} \\ \bullet \text{ solutions in } \mathbb{Z}/_n \text{ for every } n. \end{array} \right.$

next week $\left\{ \begin{array}{l} \text{Given one rational solution, there is an easy} \\ \text{method for finding all the others} \end{array} \right.$

<u>Next consider</u> : degree $(f)=3$.

→ elliptic curves are examples of these.

→ There are conjectures on how to find the solutions, but these are not proved.

The Affine & Projective Planes

Let K be a field. The affine plane (over k) is the vector space K^2.

We'll call it $\mathbb{A}^2(K)$.

The projective plane can be thought of as the affine plane together with some "points at infinity".

Definition

The projective plane $\mathbb{P}^2(K)$ is the set of lines through the origin in K^3.

Given any non-zero vector, (x, y, z) there is a unique line through (x, y, z) in K^3.

We'll write $(x : y : z)$ for this line, i.e. the point in $\mathbb{P}^2(K)$.

i.e. $\lambda \neq 0$

<u>Note:</u> $(x : y : z) = (x' : y' : z')$ if $\exists \lambda \in K^*$:

$$x' = \lambda x$$
$$y' = \lambda y$$
$$z' = \lambda z$$

We can think of $\mathbb{A}^2(k)$ as a subset of $\mathbb{P}^2(k)$ by identifying $(x,y) \in \mathbb{A}^2(k)$ with

$(x:y:1) \in \mathbb{P}^2(k)$

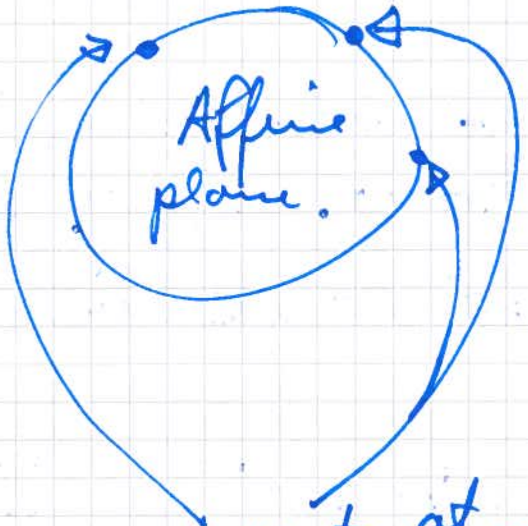
something not equal to ~~zero~~ & in a field $1 \neq 0$

<u>Remark</u>: if $z \neq 0$, then $(x:y:z) = \left(\frac{x}{z} : \frac{y}{z} : 1\right)$

$$= \left(\frac{x}{z}, \frac{y}{z}\right) \in \mathbb{A}^2(k)$$

The points in $\mathbb{P}^2(k)$ that are not affine points are $(x:y:0)$.

We'll call these <u>points at infinity</u>.



points at ∞ for each direction in the affine plane.

Curves

Let $f \in k[x,y]$ be a non-constant polynomial. Then affine curve defined by f is:

$$C_f(k) = \{(x,y) \in \mathbb{A}^2(k) : f(x,y)=0\}$$

The polynomial f also define a projective curve, which is a kind completion of $C_f(k)$. To define this, we let

$F(x,y,z)$ be the homogenization of $f(x,y)$, i.e. a polynomial of same degree d as f, s.t.

$F(x,y,1) = f(x,y)$ and F is homogeneous

$$F(x,y,z) = z^d f\left(\frac{x}{z}, \frac{y}{z}\right), \text{ where}$$

$d = \text{degree}(f)$.

eg.: $f(x,y) = x^3 - xy + 3$

$$F(x,y,z) = x^3 - xyz + 3z^3$$

The projective completion of C_f is

$$C_F(k) = \{(x:y:z) : F(x,y,z) = 0\}$$

To see this is well defined note;

$$F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x,y,z)$$

since F is homogeneous of degree d.

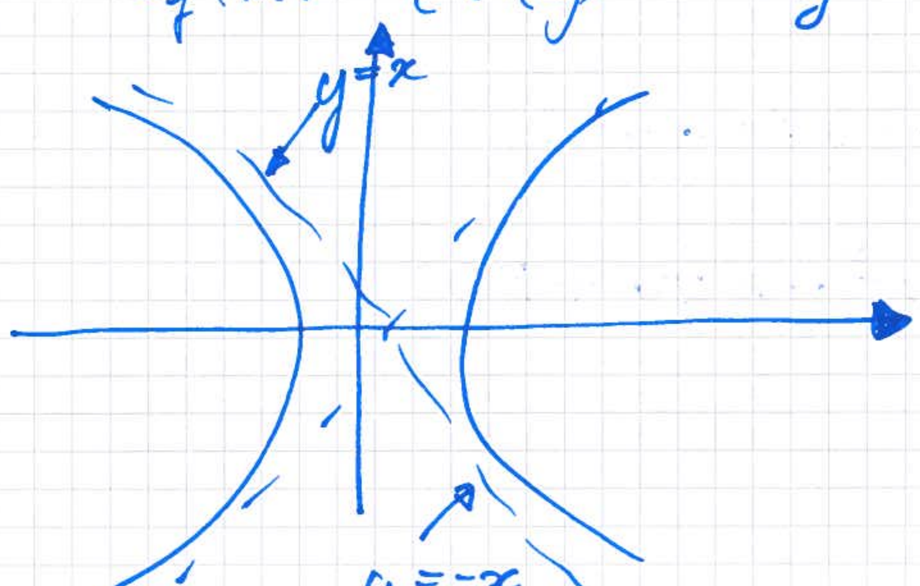
The affine points of C_F are $(x:y:1)$ where $\underbrace{F(x:y:1)}_{f(x,y)} = 0$ ... $\overset{(x:y:1)}{\parallel}$ $(x,y) : f(x,y) = 0$

so these are exactly the points in C_f.

Example:

$f(x,y) = x^2 - y^2 - 1$; $k = \mathbb{R}$.

$C_f(\mathbb{R}) = \{(x,y) : x^2 = y^2 + 1\}$



$$F(x,y,z) = x^2 - y^2 - z^2$$

points at ∞ on $C_F(\mathbb{R})$ are

$$(x:y:0) \;:\; x^2 - y^2 = 0$$

$$\therefore \quad x = \pm y$$

<u>Note:</u>

$$(x:x:0) = (1:1:0)$$
$$(x:-x:0) = (1:-1:0)$$

So there only two points at ∞, and they are $(1:1:0)$, $(1:-1;0)$ as you'd expect.

<u>Definition</u>

A projective curve is $C_F(K) = \{(x:y:z) \in k^3 : F(x,y,z) = 0\}$ where $F \in k[x,y,z]$ is non-constant & homogeneous.

<u>eg.</u>: $F(x,y,z) = z$.

$$C_F(K) = \{(x:y:0) : x,y \in k\}$$

This is the set of points at infinity. This is not the ~~com~~ projective completion of an affine curve.

Remark:

$$C_{f*g} = C_f \cup C_g$$

$$(fg)(x,y) = 0 \Leftrightarrow \left(\begin{array}{l} f(x,y) = 0 \text{ or} \\ g(x,y) = 0 \end{array} \right)$$

$$(x,y) \in C_{f*g} \Leftrightarrow (x,y) \in C_f \text{ or } (x,y) \in C_g$$

$$\therefore \quad C_{f^n} = C_f \cup C_f \cup \dots \cup C_f = C_f$$

$\therefore$ From now on we will assume that $f(x,y)$ is "square-free", i.e. not a multiple of a square of a polynomial.

Similarly, when talking about C_F, we'll assume F is not a multiple of a square of a homogeneous polynomial.

Elliptic Curves

17.01.2014

- An affine line in $\mathbb{A}^2(k)$ is a curve defined by $ax+by+c=0$ (a & b not both 0)
  i.e. $f(x,y)=ax+by+c$, $a, b, c \in k$

- A projective line is $L=\{(x:y:z) \in \mathbb{P}^2(k) : ax+by+cz=0\}$
  (a, b, c are not all 0)

<u>Note</u>: the projective line $z=0$ is the only one which is not the projective completion of an affine line. This is the line at infinity.

<u>Theorem</u>
Any two distinct lines in $\mathbb{P}^2(k)$ meet at exactly 1 point.

<u>Proof</u>: Suppose the lines are

$$L : ax+by+cz=0$$
$$L' : a'x+b'y+c'z=0$$

$$L \cap L' : \quad \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

Since $L \neq L'$, 2^{nd} line is not a multiple of 1^{st} line so, so the matrix has rank 2 .
Kernel is 1-dim. spanned by a non-zero vector $\underline{v}$. $\Rightarrow L \cap L' = \{\lambda \underline{v} : \lambda \in k\}$

This is exactly 1 point in $\mathbb{P}^2(k)$ $\square$

Fields of Definition

If $f \in k[x,y]$ then we've defied the curve C_f.
We'll say that C_f is "defined over k".
Obviously $C_f(L)$ makes sense for any field L containing k.
We'll think of C_f as a map

$$\{\text{fields containing } k\} \longrightarrow \{\text{sets}\}$$

If C_F is defined over $\mathbb{Q}$ then every point can be given integer coordinates.

$$(x:y:z) = (nx:ny:nz)$$

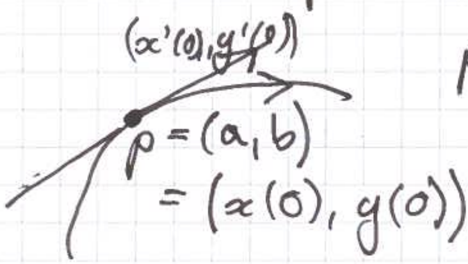
take $n = \mathrm{lcm}(\text{denominators of } x, y \,\&\, z)$

Singular points & tangent lines

For the moment assume $k = \mathbb{R}$.

$C = C_f \quad , \quad f \in \mathbb{R}[x,y]$

$p \in C(\mathbb{R})$



Let $(x(t), y(t))$ be a path along $C(\mathbb{R})$ with $(x(0), y(0)) = (a, b)$, where $p = (a, b)$.

$f(x(t), y(t)) = 0$, $\forall t$.

$\Rightarrow \left.\frac{\partial f}{\partial x}\right|_p x'(0) + \left.\frac{\partial f}{\partial y}\right|_p y'(0) = 0$, by the chain rule.

The tangent line is the line

$$\frac{\partial f}{\partial x}(p)(x-a) + \frac{\partial f}{\partial y}(p)(y-b) = 0$$

(assuming this is a line, i.e. assuming $\frac{\partial f}{\partial x}(p)$ & $\frac{\partial f}{\partial y}(p)$ are not both 0).

$\Rightarrow$ This is motivation for the definition of the tangent line at a point on a curve over any field:

<u>Definition</u>: Let C_f be an affine curve defined over a field k. Let $p \in C_f(k)$. We'll call p a <u>singular point</u> if $\frac{\partial f}{\partial x}(p) = \frac{\partial f}{\partial y}(p) = 0$. Otherwise p is called a non-singular point.

If p is a non-singular point then we define the tangent line at p,

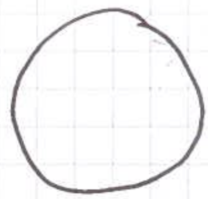
$$T_p(C_f): \frac{\partial f}{\partial x}(p)(x-a) + \frac{\partial f}{\partial y}(p)(y-b) = 0$$

where $p = (a, b) \in C_f(k)$.

Definition: The curve C_f is called a singular curve if it has at least one singular point in $C_f(L)$ for some field L containing k.

Examples:

1) Circle: $x^2+y^2=1$



Let $(a,b)\in C$, assume $2\neq 0$ in k.

Remark: $f(x,y)=x^2+y^2-1$

$\hookrightarrow$ if $2=0$ then $f(x,y)=(x+y+1)^2$ so f is not square-free.

$$p=(a,b) \Rightarrow \frac{\partial f}{\partial x}=2x \; ; \frac{\partial f}{\partial y}=2y$$

$$\Rightarrow \frac{\partial f}{\partial x}(p)=2a \; , \frac{\partial f}{\partial y}(p)=2b$$

Suppose p is a singular point on C_f

$\therefore \; 2a=0 \; , \; 2b=0 \; , \; a^2+b^2=1$

$\therefore \; 2\neq 0 \Rightarrow a=b=0 \Rightarrow 0=1. \times$

Thus p is non-singular.

The tangent line at P is

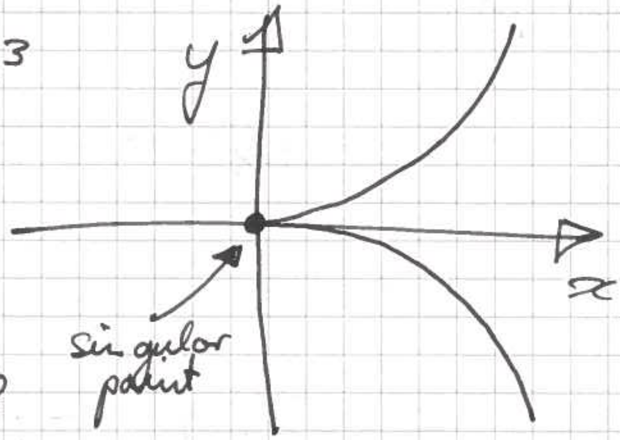
$$T_p(C): \ 2a(x-a) + 2b(y-b) = 0$$

$$ax + by = a^2 + b^2$$

$$\therefore \ ax + by = 1.$$

2.) $f(x,y) = y^2 - x^3$

→ assume neither 2 nor 3 is 0 in k.



Let $P = (a,b) \in C_f$

$$\frac{\partial f}{\partial x}(p) = -3a^2 \ ; \ \frac{\partial f}{\partial y}(p) = 2b$$

Suppose P is a singular point:

$$\therefore \ -3a^2 = 0 \quad \& \ 2b = 0 \ \& \ b^2 = a^3.$$

This has a unique solution : $a = b = 0$

So $p = (0,0)$ is the only singular point.
Suppose $P = (a,b)$ is non-singular.
The tangent line is

$$T_p(C): \ -3a^2(x-a) + 2b(y-b) = 0$$

Projective definitions of singular points & tangent lines

Let k be any field $F \in k[X, Y, Z]$ a homogeneous polynomial, square free.
$C = C_F$ (the projective curve). $p \in C_F(k)$

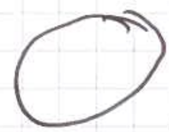
Definition: p is a singular point if

$$\frac{\partial F}{\partial X}(p) = \frac{\partial F}{\partial Y}(p) = \frac{\partial F}{\partial Z}(p) = 0$$

If p is non-singular, then the tangent line is

$$T_p C_F : \frac{\partial F}{\partial X}(p)\, X + \frac{\partial F}{\partial Y}(p)\, Y + \frac{\partial F}{\partial Z}(p)\, Z = 0$$

Example:



+ some complex points at infinity

$$F(X, Y, Z) = X^2 + Y^2 - Z^2$$

(assume $2 \neq 0$ since otherwise $F(X, Y, Z) = (X + Y + Z)^2$)

Let $p = (A : B : C) \in C_F$

$$\frac{\partial F}{\partial X}(p) = 2A$$

$$\frac{\partial F}{\partial Y}(p) = 2B$$

$$\frac{\partial F}{\partial Z}(p) = -2C$$

If p is singular then $A = B = C = 0$ $\times$.

$\therefore C_F$ is non-singular.

$$T_p(C) = 2AX + 2BY - 2CZ = 0$$

i.e. $AX + BY = CZ$

Recall: C_F is the projective completion of C_f, $f(x,y) = x^2 + y^2 - 1$, if $p = (a:b:1)$ is a finite point on C_F, so $(a,b) \in C_f$ then

$$T_p C_F : aX + bY = Z$$

$$T_p C_f : ax + by = 1$$

$\rightarrow$ we see that $T_p C_F$ is exactly the projective completion of $T_p C_f$.

We'll now show that this always happens:

Proposition

Let C_F be the projective completion of C_f and $P \in C_f \subseteq C_F$. Then $T_p C_F$ is the projective completion of $T_p C_f$.

Proof: $f(x,y) = F(x,y,1)$

$$\therefore \frac{\partial f}{\partial x}(x,y) = \frac{\partial F}{\partial X}(x,y)$$

Let $p = (a,b) = (a:b:1)$

also

$$\frac{\partial f}{\partial x}(p) = \frac{\partial F}{\partial X}(p)$$

$p = (a:b:1)$

$$\frac{\partial f}{\partial y}(p) = \frac{\partial F}{\partial Y}(p)$$

The projective tangent line is

$$\frac{\partial f}{\partial x}(p) X + \frac{\partial f}{\partial y}(p) Y + \frac{\partial F}{\partial Z}(p) Z = 0$$

$\Rightarrow$ we need:

Lemma

Let $F(X,Y,Z)$ be a homogeneous polynomial of degree d.

Then

$$X\frac{\partial F}{\partial X} + Y\frac{\partial F}{\partial Y} + Z\frac{\partial F}{\partial Z} = dF.$$

In particular, if $(A:B:C) \in C_F$, then

$$A\frac{\partial F}{\partial X}(A,B,C) + B\frac{\partial F}{\partial Y}(A,B,C) + C\frac{\partial F}{\partial Z}(A,B,C) = 0$$

Using the last part of Lemma, with $(A,B,C)=(a,b,1)$:

$$\frac{\partial f}{\partial x}(p)X+\frac{\partial f}{\partial y}(p)Y+\left(-a\frac{\partial f}{\partial x}(p)-b\frac{\partial f}{\partial y}(p)\right)Z=0$$

This simplifies to

$$\frac{\partial f}{\partial x}(p)(X-aZ)+\frac{\partial f}{\partial y}(p)(Y-bZ)=0$$

This is the projective completion of

$$T_pC_f:\ \frac{\partial f}{\partial x}(p)(x-a)+\frac{\partial f}{\partial y}(p)(y-b)=0$$

$\square$

<u>Proof of Lemma</u>

$$F(X,Y,Z)=\sum a_{ijk}X^iY^jZ^k$$

$$X\frac{\partial F}{\partial X}=\sum i a_{ijk}X^iY^jZ^k$$

$$Y\frac{\partial F}{\partial Y}=\sum j a_{ijk}X^iY^jZ^k$$

$$Z\frac{\partial F}{\partial Z}=\sum k a_{ijk}X^iY^jZ^k$$

$$\Rightarrow X\frac{\partial F}{\partial X}+Y\frac{\partial F}{\partial Y}+Z\frac{\partial F}{\partial Z}=\sum \underbrace{(i+j+k)}_{=d}a_{ijk}X^iY^jZ^k$$

$$=dF$$

$\square$

<u>Example</u>:

1) assume $2 \neq 0$ in k.

$$F(X,Y,Z) = Y^2 Z - X^3 - X \cdot Z^2$$

Suppose $p = (A : B : C)$

$$\frac{\partial F}{\partial X}(p) = -3A^2 - C^2$$

$$\frac{\partial F}{\partial Y}(p) = 2BC$$

$$\frac{\partial F}{\partial Z}(p) = B^2 - 2AC$$

Assume P is singular:

$2BC = 0$ so $B = 0$ or $C = 0$,

↳ assume $B = 0$, then

$B^2 - 2AC \Rightarrow A = 0$ or $C = 0$

↳ assume $A = 0$

$-3A^2 - C^2 = 0 \Rightarrow C = 0$ $\cdot\!\!\times\!\!\cdot$

↳ assume $C = 0$

$-3A^2 - C^2 = 0 \Rightarrow A = 0$ $\cdot\!\!\times\!\!\cdot$

↳ assume $B \neq 0 \Rightarrow C = 0$

$\therefore 3A^2 = 0$, $B^2 = 0 \Rightarrow B = 0$ $\cdot\!\!\times\!\!\cdot$

$\therefore C_F$ is non-singular.

→ This curve contains at least one point $\mathcal{O} = (0:1:0) \in C_F(k)$

<u>Definition</u>: An <u>elliptic curve</u> over a field k is a projective, non-singular cubic curve defined over k, such that $C(k) \neq \emptyset$.

So the curve

$$C_F : Y^2Z - X^3 - XZ^2 = 0$$

is an elliptic curve over k, as long as $2 \neq 0$ in k.

We'll often just write down the affine equation of a curve C, but we'll mean the projective completion.

<u>Example</u>:
Let $f \in k[x]$ be a cubic polynomial
Consider the curve

$$C: \; y^2 = f(x)$$

(in fact we mean its projective completion
$$zy^2 = z^3 f\left(\frac{x}{z}\right))$$

<u>Claim</u>: C is an elliptic curve iff f has no repeated roots in any field containing k (assume $2 \neq 0$ in k).

<u>Proof</u>: $\mathcal{O} = (0:1:0)$ is a point in $C(k)$

We need to check that the curve is non-singular iff f has a repeated root.

Let a be a repeated root of f, i.e. $f(x) = (x-a)^2(x-b)$
we'll show that $p = (a,0)$ is a singular point.

$$\frac{\partial}{\partial x}(y^2 - f(x))(p) = -f'(a)$$

$$\frac{\partial}{\partial y}(y^2 - f(x))(p) = 0$$

$$\Rightarrow f(x) = (x-a)^2(x-b)$$

$$\Rightarrow f'(x) = 2(x-a)(x-b) + (x-a)^2$$

$$\hookrightarrow f'(a) = 0.$$

$\therefore$ p is a singular point as long as $0^2 = f(a)$ ✓
(so $p \in C$).

Intersection numbers & Bézout's Theorem

If $f \in \mathbb{C}[x]$ has degree d, then expect it has d zeros in $\mathbb{C}$. There are exceptions:
$f = 0$ (∞ ly many roots); $f(x) = (x-1)^2$ (only 1 root).
Similarly if $f, g \in \mathbb{C}[x,y]$ with degree d_1 & d_2, then after looking at some examples, we expect

$$|C_f(\mathbb{C}) \cap C_g(\mathbb{C})| = d_1 d_2,$$

i.e. $f(x,y) = g(x,y) = 0$ should have $d_1 d_2$ solutions.
Again there will be exceptions:

- $f = g$. Then $(C_f \cap C_g)(\mathbb{C})$ is infinite
- $f(x,y) = x^2 + y^2 - 1$
  $g(x,y) = x^2 + y^2 - 2$
  $\Rightarrow C_f \cap C_g = \emptyset$.
- C_f & C_g could cross tangentially (a bit like a single polynomial f having a double root).

Remark:
g, f can be factorized into irreducible polynomials
$f = f_1 \cdots f_r$
$g = g_1 \cdots g_s$

$\Rightarrow C_f = C_{f_1} \cup \ldots \cup C_{f_r}$

$C_g = C_{g_1} \cup \ldots \cup C_{g_s}$.

We call C_{f_i}, C_{g_j} the "irreducible components" of C_f & C_g.
C_f is called irreducible, if f is irreducible.

In order that $C_f \cap C_g$ is finite, we'll need to assume that C_f & C_g don't have a common irreducible component.

To deal with the 2nd problem, we need to count intersection points in $\mathbb{P}^2(\mathbb{C})$ instead of $\mathbb{A}^2(\mathbb{C})$.

To deal with the 3rd problem, we need to define the multiplicity of an intersection point.
This multiplicity is called the intersection number $I(C_f, C_g, P)$, $P \in C_f(\mathbb{C}) \cap C_g(\mathbb{C})$

Theorem (Bézout's Theorem)
Let C_F, C_G be projective curves with no common irreducible component, defined by polynomials F, G of degrees d_1, d_2: Then

$$\sum_{P \in C_F(\mathbb{C}) \cap C_G(\mathbb{C})} I(C_F, C_G, P) = d_1 d_2 .$$

Before defining $I(C_F, C_G, P)$ we'll look again at the multiplicity of a zero of $f(x)$.

Let $a \in \mathbb{C}$.

The local ring at a is $\mathbb{C}[x]_{(a)} = \left\{ \frac{f}{g} : f, g \in \mathbb{C}[x],\ g(a) \neq 0 \right\}$ (rational function with no pole at a).

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2}$$

& check multiplication

$$\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}$$

$$g_1(a) \neq 0 \ \& \ g_2(a) \neq 0 \Rightarrow (g_1 g_2)(a) \neq 0$$

$\therefore$ $\mathbb{C}[x]_{(a)}$ is closed under $+$ & $\cdot$, so it is a ring.

If we have any polynomial $f(x) \in \mathbb{C}[x]$. Then $f(x) = (x-\alpha)^d g(x)$, where $g(\alpha) \neq 0$.

Since $g(a) \neq 0$, g is invertible in $\mathbb{C}[x]_{(a)}$.

$\therefore$ $(f) = ((x-\alpha)^d)$; (= ideals in $\mathbb{C}[x]_{(a)}$).

The quotient ring

$$\mathbb{C}[x]_{(a)} \Big/ (f) = \mathbb{C}[x]_{(a)} \Big/ \left((x-a)^d\right)$$

is d-dimensional as a vector space over $\mathbb{C}$, with basis $\{1, (x-a), (x-a)^2, \ldots, (x-a)^{d-1}\}$

So we could define the multiplicity of a root of f to be

$$d = \dim_{\mathbb{C}} \left(\mathbb{C}[x]_{(a)} \Big/ (f) \right).$$

Generalizing this, we define for $f, g \in \mathbb{C}[x,y]$ and $P \in \mathbb{A}^2(\mathbb{C})$.

$$I(C_f, C_g, P) = \dim_{\mathbb{C}} \left(\mathbb{C}[x,y]_{(P)} \Big/ (f,g) \right)$$

In this definition the local ring $\mathbb{C}[x,y]_{(P)}$ is defined by

$$\mathbb{C}[x,y]_{(P)} = \left\{ \frac{a}{b} : a, b \in \mathbb{C}[x,y],\ b(P) \neq 0 \right\}$$

Lemma

Let $P=(a,b) \in \mathbb{A}^2(\mathbb{C})$

(i) $\forall f \in \mathbb{C}[x,y]$, $g \in \mathbb{C}[x]$.
There is a ring isomorphism

$$\mathbb{C}[x,y]_{(P)} \Big/ \big(f(x,y),\, y-g(x)\big) \cong \mathbb{C}[x]_{(a)} \Big/ \big(f(x,g(x))\big)$$

$$x \longmapsto x$$

$$y \longmapsto g(x)$$

(ii) if $h(a) \neq 0$ then h is unit in $\mathbb{C}[x]_{(a)}$.

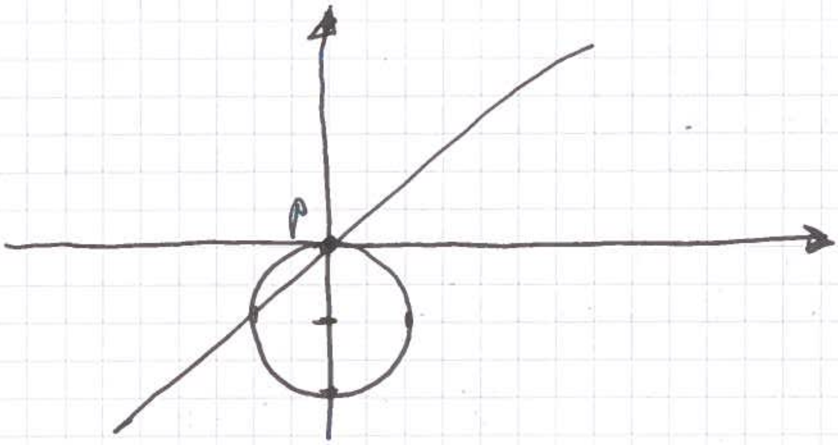
(iii) if $h(a) \neq 0$ then $\dim_{\mathbb{C}}\left(\mathbb{C}[x]_{(a)} \Big/ \big((x-a)^n h(x)\big)\right) = n.$

Examples:

$C_1: x^2+(y+1)^2-1$

$C_2: y = \lambda x.$

$p=(0,0).$



$$\mathbb{C}[x,y]_{(0,0)} \Big/ \left(x^2+(y+1)^2-1,\ y-\lambda x\right)$$

$$\cong \mathbb{C}[x]_0 \Big/ \left(x^2+(\lambda x+1)^2-1\right)$$

$$\left[\ x^2+(\lambda x+1)^2-1 = x^2+\lambda^2x^2+2\lambda x\ \right]$$

$$\cong \mathbb{C}[x]_{(0)} \Big/ \left((\lambda^2+1)x^2+2\lambda x\right)$$

if $\lambda \neq 0$, then $\mathbb{C}[x]_{(0)} \Big/ \left((\lambda^2+1)x^2+2\lambda x\right)$

$= \mathbb{C}[x]_{(0)} \Big/ (x^1)$, which is 1-dimensional.

$f, g \in R$ (ring)
$(f,g) = \{af + bg : a, b \in R\}$ an ideal in R

if $\lambda = 0$, then

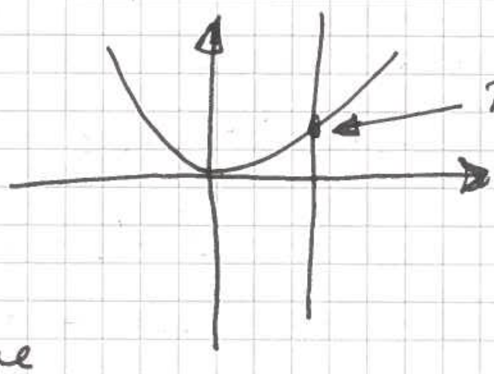
$\cong \mathbb{C}[x]_{(0)} / (x^2)$, which is 2-dimensional

$$\therefore I(C_1, C_2, P) = \begin{cases} 1, & \lambda \neq 0 \\ 2, & \lambda = 0. \end{cases}$$

<u>Example</u>:

$C_1: \; y = x^2$

$C_2: \; x = 1$



The projective curves are

$YZ = X^2 \; ; \quad X = Z.$

They intersect at $P = (1,1)$, let's find the intersection at ∞:

$Z = 0$

$\therefore X = 0$

$Q = (0 : 1 : 0)$

is another point of intersection.

$$I(C_1, C_2, P) = \dim_{\mathbb{C}} \frac{\mathbb{C}[x,y]_{(P)}}{(y-x^2, x-1)}$$

$$= \dim_{\mathbb{C}} \frac{\mathbb{C}[y]_{(1)}}{(y-1)} = 1.$$

Q is not in the x,y affine plane.
It is in the x,z - plane since its y-coordinate is non - zero.
$\therefore$ Change to x,z - coordinates

$$z - x^2 = 0$$
$$x - z = 0$$

$$I(C_1, C_2, Q) = \dim_{\mathbb{C}} \frac{\mathbb{C}[x,z]_{(Q)}}{(z-x^2, z-x)}$$

$$= \dim_{\mathbb{C}} \frac{\mathbb{C}[x]_{(0)}}{(x^2-x)}$$

$$= \dim_{\mathbb{C}} \frac{\mathbb{C}[x]_{(0)}}{(x)} = 1$$

$$\Rightarrow I(C_1, C_2, P) + I(C_1, C_2, Q) =$$
$$= 1 + 1 = 2 = 2 \times 1 = \deg(y - x^2) \cdot \deg(x-1)$$

so Bézout's Theorem holds.

Remark:

the only thing we use about $\mathbb{C}$ is the fact that every $f \in \mathbb{C}[x]$ is a product of linear factors.

We can replace $\mathbb{C}$ with any other field with this property and Bézout's Theorem will still be true.

Remark

Suppose $f, g \in k[x, y]$, wher $k \subseteq \mathbb{C}$.
and let

$$C_f(\mathbb{C}) \cap C_g(\mathbb{C}) = \{P_1, \dots, P_N\}$$

Then, if $P_1, \dots, P_{N-1} \in \mathbb{A}^2(k)$, then $P_N \in \mathbb{A}^2(k)$

<u>Defn</u>: $M \in GL_3(\mathbb{R})$

then M takes lines through the origin to lines through the origin in $\mathbb{R}^3$, so M gives a map

$$M: \mathbb{P}^2(\mathbb{R}) \longrightarrow \mathbb{P}^2(\mathbb{R}).$$

It also transforms polynomials

$$G(X,Y,Z) = F\left(M\begin{pmatrix} X \\ Y \\ Z \end{pmatrix}\right)$$

M is called a projective transformation.

<u>Proposition</u>

Let M be a projective transformation, $C = C_F$. Then,

- $M(C)$ is the curve defined by
$$G = F\left(M^{-1}\begin{pmatrix} X \\ Y \\ Z \end{pmatrix}\right)$$

- if $P \in C$, then P is singular in C $\Leftrightarrow$ $M(P)$ is singular in $M(C)$.

- $T_{M(P)}\, M(C) = M(T_P C)$.

- $I(C_1, C_2, P) = I(M(C_1), M(C_2), M(P))$.

This often makes it easier to prove things.

eg: <u>Lemma</u>: if $P \in C$, then
$I(C_{\alpha}, T_P C, P) \geq 2$.

<u>idea</u>: choose a projective transformation so that $P' = M(P) = (0,0)$.
$(C' = M(C))$

$T_{P'} C' : y = 0$

This reduces it to a much simpler question.

At end of last time; complete proof:

<u>Proposition</u>:

Let k be a field in which $2 \neq 0$ and let $f \in k[x]$ be a cubic polynomial.

$$C : y^2 = f(x) \quad \left(Y^2 Z = Z^3 f\left(\frac{X}{Z}\right)\right)$$

Then C is an elliptic curve $\Leftrightarrow$ f has no repeated roots in any field.

Recall that C is a cubic projective curve $\mathcal{O} = (0 : 1 : 0) \in C(k)$.

We needed to check that C is singular $\Leftrightarrow$ f has repeated root.

We did ($\Leftarrow$) of a is a repeated root of f then $(a,0)$ is a singular point of C.

($\Rightarrow$) Conversely let $(A:B:C)$ be a singular point.

C is defined by the polynomial

$$F(X,Y,Z) = Y^2Z - X^3 - pX^2Z - qXZ^2 - rZ^3$$

$$\frac{\partial F}{\partial X} = -3X^2 - 2pXZ - qZ^2$$

$$\frac{\partial F}{\partial Y} = 2YZ$$

$$\frac{\partial F}{\partial Z} = Y^2 - pX^2 - 2qXZ - 3rZ^2$$

$\therefore\ 2BC = 0$

$\therefore\ B = 0$ or $C = 0$

$\rightarrow$ if $C = 0$ $\therefore\ A^3 = 0 \Rightarrow A = 0$

$\therefore\ B^2 = 0 \Rightarrow B = 0$ $\times$

$\therefore\ C \neq 0 \Rightarrow B = 0$

$\Rightarrow$ normalise so $C = 1$

we're now in the x, y plane

$$\left.\begin{array}{l} f(A) = 0 \\ f'(A) = 0 \end{array}\right\} \Rightarrow A \text{ is a repeated root of } f.$$

$\square$

29.01.2014

Elliptic Curves

Intersection Numbers & Bézout's Theorem.

If C_1 & C_2 are curves defined by polynomials $f_1, f_2 \in$ ~~$\mathbb{C}[x_1, x_2]$~~ $\mathbb{C}[x,y]$. and $p \in C_1(\mathbb{C}) \cap C_2(\mathbb{C})$, then

$$I(C_1, C_2, P) = \dim_{\mathbb{C}}\left(\frac{\mathbb{C}[x,y]_{(p)}}{(f_1, f_2)}\right)$$

Bézout's Theorem

If C_1 & C_2 are projective curves defined by polynomials of degrees d_1 & d_2 then

$$\sum_{p \in C_1(\mathbb{C}) \cap C_2(\mathbb{C})} I(C_1, C_2, P) = d_1 d_2$$

if $p \in C$, then $\underline{I}(C, T_pC, P) \geq 2$

(This is an exercise).

Definition:

$p \in C$ is called a <u>point of inflection</u> if $I(C, T_pC, P) \geq 3$.

<u>Example</u>:

$$C : y^2 = f(x) \quad , \quad f(x) = x^3 + a x^2 + b x + c.$$

$$\mathcal{O} = (0:1:0)$$

<u>Claim</u> $\mathcal{O}$ is a point of inflection.

C is defined by

$$F = Y^2 Z - X^3 - a X^2 Z - b X Z^2 - c Z^3.$$

$$\frac{\partial F}{\partial X} = -3X^2 - 2a XZ - bZ^2$$

$$\frac{\partial F}{\partial Y} = 2YZ$$

$$\frac{\partial F}{\partial Z} = -aX^2 - 2bXZ - 3cZ^2 + Y^2$$

$$\Rightarrow \frac{\partial F}{\partial X}(\mathcal{O}) = 0$$

$$\frac{\partial F}{\partial Y}(\mathcal{O}) = 0$$

$$\frac{\partial F}{\partial Z}(\mathcal{O}) = 1$$

$$T_{\mathcal{O}} C : \quad 0X + 0Y + 1 \cdot Z = 0$$

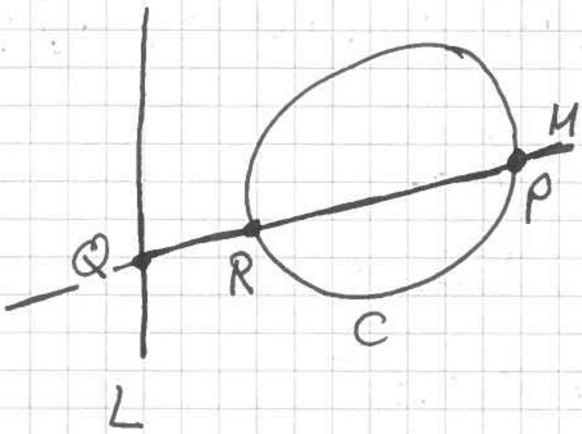
$$\text{i.e. } \quad Z = 0.$$

$$I(C, T_{\mathcal{O}} C, \mathcal{O}) = \dim_{\mathbb{C}} \frac{\mathbb{C}[x,z]_{(\mathcal{O})}}{(z - x^3 - axz - bxz^2 - cz^3, z)}$$

$$= \dim_{\mathbb{C}} \frac{\mathbb{C}[x]_{(\mathcal{O})}}{(-x^3)} = 3.$$

Rational Points in a conic

Let C be a conic defined over $\mathbb{Q}$.
Suppose we have one rational point $P \in C(\mathbb{Q})$.
There is a method for finding all the other points.



Let L be a rational line not containing P.

we'll get a bijection

$$L(\mathbb{Q}) \longleftrightarrow C(\mathbb{Q})$$

$$\begin{array}{c} \in \\ Q \longmapsto R. \end{array}$$

Given $Q \in L(\mathbb{Q})$. Let M be the line through P & Q.

Then $M \cap C$ has 2 points counting multiplicity. One of these is P. We'll call the other one R.
So far we just know $R \in C(\mathbb{C})$.

But M & C are defined over $\mathbb{Q}$,

$M \cap C = \{P, R\}$ and $P \in \mathbb{P}^2(\mathbb{Q}) \therefore R \in \mathbb{P}^2(\mathbb{Q})$.

Conversely, given R in $C(\mathbb{Q})$ there is unique line M s.t. $M \cap C = \{P, R\}$
(this notation means P with multiplicity 2 if $P = R$).

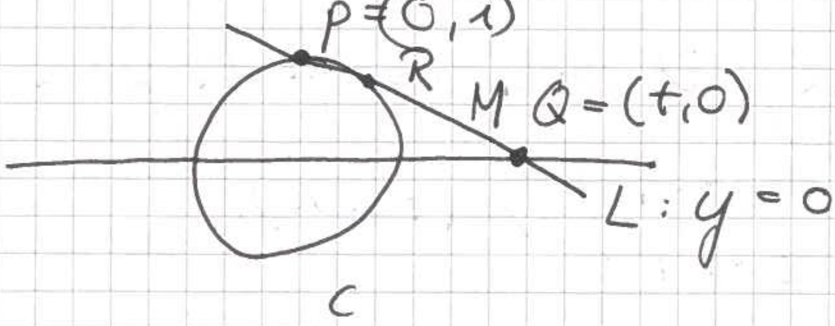
M is a rational line, and we can recover $Q \in L(\mathbb{Q})$ by $M(\mathbb{Q}) \cap L(\mathbb{Q}) = \{Q\}$.

<u>Example</u>: (Pythagorean triples)

Find all integer solutions to

$$X^2 + Y^2 = Z^2$$

equivalently, find all rational solutions to $C: x^2 + y^2 = 1$.



Let $P = (0,1)$

Let L be the line $y=0$. a point on L has the form $Q=(t,0)$.
Let M be the line through Q & P. A general point on M has the form $\lambda Q + (1-\lambda) P =$
$= (\lambda t, 1-\lambda)$.

At the point R, we have

$$(\lambda t)^2 + (1-\lambda)^2 = 1$$

$$\therefore \quad t^2\lambda^2 + 1 - 2\lambda + \lambda^2 = 1$$

$$(t^2+1)\lambda^2 - 2\lambda = 0$$

this has 2 roots $\lambda = 0$

$$\lambda = \frac{2}{t^2+1}$$

$\lambda = 0$ corresponds to the point P.

$$\therefore \text{ at } R, \quad \lambda = \frac{2}{t^2+1}$$

$$\therefore \quad R = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right)$$

$\therefore$ the rational points on C are of the form
$$\left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right), \quad (t \in \mathbb{Q}).$$

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

$$= \frac{t^4+2t^2+1}{(t^2+1)^2} = 1.$$

2 Elliptic Curves

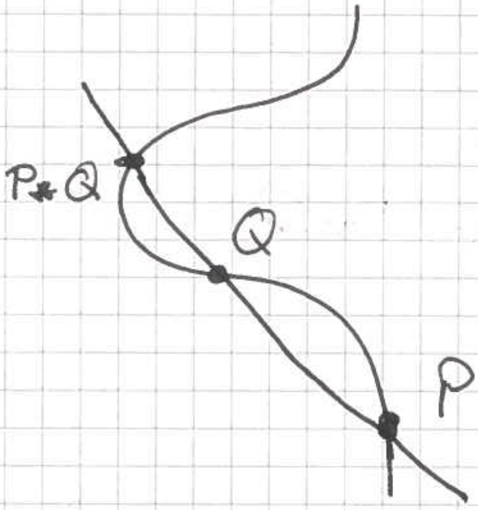
Recall: Let K be a field.

An elliptic curve over K is a projective cubic curve C, defined over k such that

- C is non-singular
- $C(k)$ is non-empty.

~~Let~~

Let O be some point in $C(k)$.
We'll show that the points in $C(k)$ form a group.



<u>Definition</u>

Given $P, Q \in C(\mathbb{R})$, there is a unique line L such that $L \cap C \supset \{P, Q\}$.

(if $P \neq Q$), this is just the line through P & Q. If $P = Q$, this is a tangent line.).

By Bézout's Theorem

$$C \cap L = \{P, Q, R\}.$$

- Since P, Q have coordinates in $\mathbb{R}$,

$$R \in C(\mathbb{R})$$

we define $P * Q = R$.

<u>Remarks:</u>

- $P * Q = Q * P$
- If $P * Q = R$, then $P * R = Q$.

The operation $*$ is not the group law.

Definition:

We define $P \dot{+} Q = \mathcal{O} * (P * Q)$

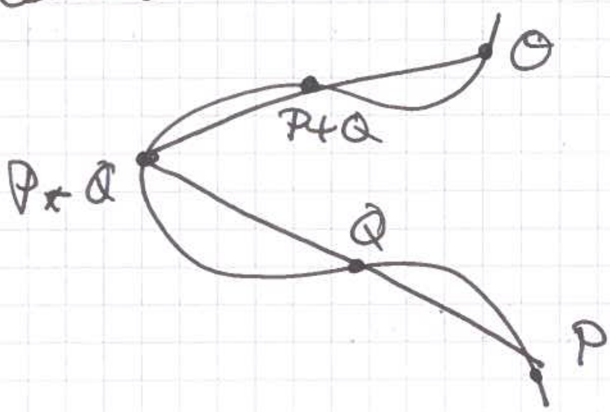
Theorem

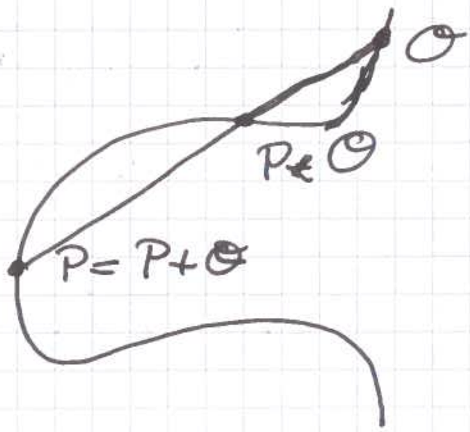
$C(\mathbb{Q})$ is an abelian group with the operation $+$.
The point $\mathcal{O}$ is the identity element.

Proof:

- Since $P * Q = Q * P$, it follows that $P + Q = Q + P$. (abelian).

- Next we'll show that $\mathcal{O}$ is the identity element.





Let $P = P * \mathcal{O}$

By the remark, $\mathcal{O} * R = P$.

$$\therefore \quad P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = \mathcal{O} * R = P$$

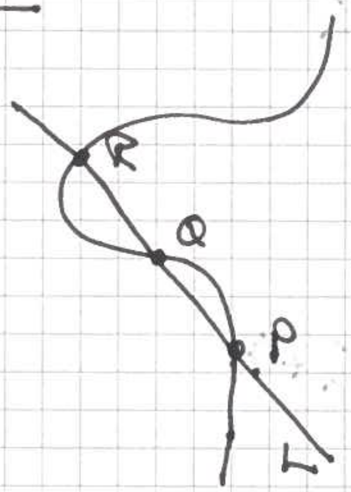
2.) Elliptic Curves

k a field. an elliptic curve over k is a non-singular projective cubic C, such that $C(k) \neq \emptyset$. Choose a point $O \in C(k)$.

Theorem

$(C(k), +)$ is an abelian group. O is the identity element.

recall:



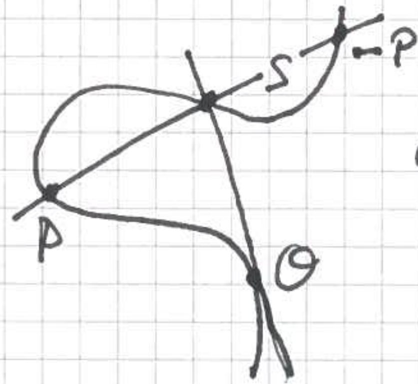
$R = P * Q$

L is the line through P & Q (or $T_P C$ if $P = Q$)

$L \cap C = \{P, Q, R\}$

$$P + Q = O * (P * Q)$$
$$R = P * Q \Leftrightarrow P = R * Q \Leftrightarrow Q = P * R.$$

$\Rightarrow$ next we'll prove that every element has an inverse:



Let $S = O * O$

define $-P = S * P$

claim: $P + (-P) = O$

since $-P = S * P$,

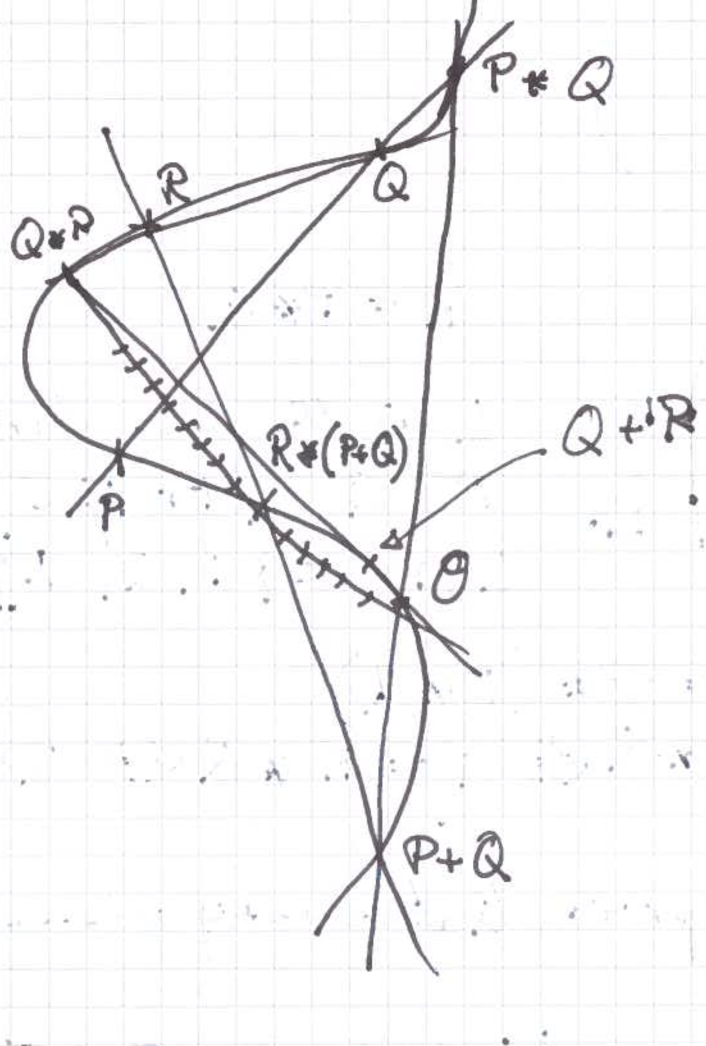
$$-P * P = S$$

$$P + (-P) = \mathcal{O} * S.$$

since $S = \mathcal{O} * \mathcal{O}$, $\mathcal{O} = \mathcal{O} * S$

$$\therefore \quad P + (-P) = \mathcal{O}$$

$\Rightarrow$ Remains to check associativity.

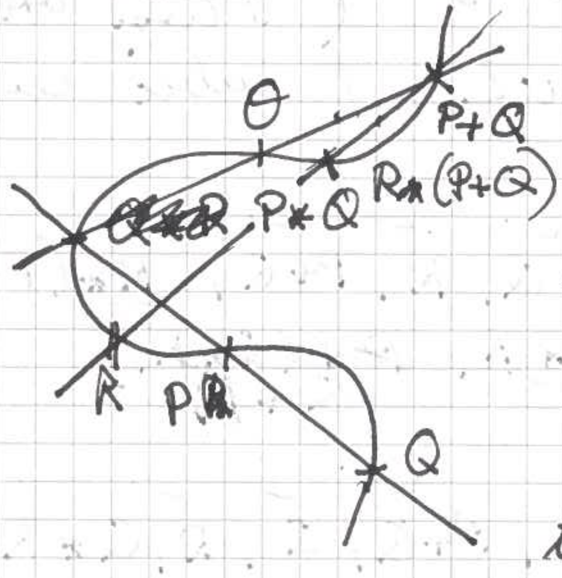


We'll use the cubic Cayley Bacharach theorem.

<u>Cubic Cayley Bacharach Theorem</u>

Let C_1, C_2, C_3 are three projective cubics (not necessarily irreducible or non-singular).
Assume $C_1 \cap C_2$ is finite.
Let $C_1 \cap C_2 = \{P_1, \ldots, P_9\}$

Suppose $P_1, \ldots, P_8 \in C_3$, then $P_9 \in C_3$.
(Proof uses Bezout's theorem a lot).



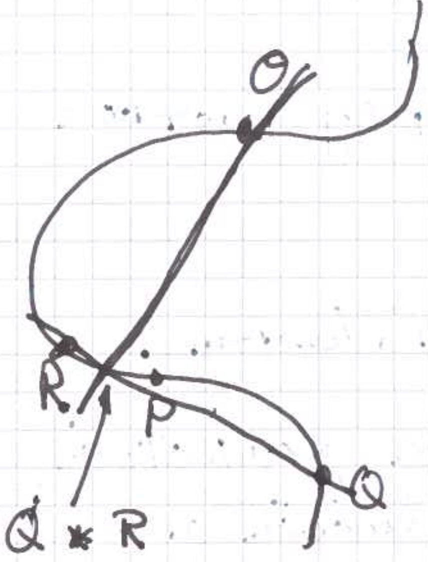
Let L_1 be the line through ~~...~~ P & Q
$L_1 \cap C = \{P, Q, P*Q\}$

Let L_2 be the line through O & $P*Q$

$L_2 \cap C = \{O, P*Q, P+Q\}$

Let L_3 be the line through R & $P+Q$.

$L_3 \cap C = \{R, P+Q, R*(P+Q)\}$



L_4 is the line through Q & R.

L_5 is the line through $Q * R$ and O.

$$L_5 \cap C = \{O, Q * R, Q + R\}$$

L_6 is the line through $P, Q+R$,

$$L_6 \cap C = \{P, Q + R, P * (Q+R)\}$$

Let $C_1 = L_1 \cup L_3 \cup L_5$, $C_2 = L_2 \cup L_4 \cup L_6$ } These are cubic curves.

$$C_1 \cap C = \{P, Q, P * Q, R, P+Q, \underline{R * (P+Q)}, O, Q * R, \cancel{P * (Q*R)}\ Q+R\}$$

$$C_2 \cap C = \{O, P * Q, P+Q, Q, R, Q * R, P, Q + R, \underline{P * (Q+R)}\}$$

By the theorem, $R * (P+Q) = P * (Q+R)$.

$$\therefore \; O * (R * (P+Q)) = O * (P * (Q+R))$$

$$R + (P+Q) = P + (Q+R)$$

$$R + (P+Q) = (P+Q) + R$$

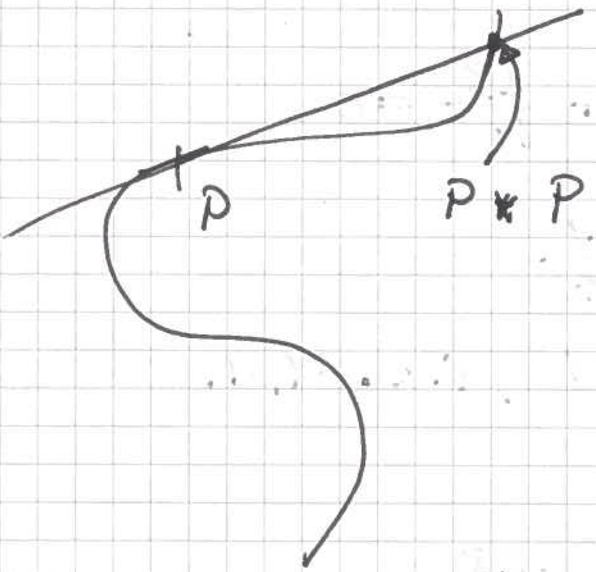
$\square$

We can use the operations $*$, $+$ to find point on $C(\mathbb{Q})$.

example:

$C: y^2 = x^3 + 3$

There is an obvious rational point $P = (1,2)$.



we'll calculate $P * P$.

$$f(x,y) = y^2 - x^3 - 3$$

$$\frac{\partial f}{\partial x}(p) = -3 \; ; \; \frac{\partial f}{\partial y}(p) = 4.$$

T_pC : $\cancel{-3(x-1)+}$

$$-3(x-1) + 4(y-2) = 0$$

$$\Rightarrow y = \frac{3x+5}{4}.$$

on $T_p \cap C$ we have:

$$y^2 = x^3 + 3, \quad y = \frac{3x+5}{4}$$

$$\frac{9x^2 + 30x + 25}{16} = x^3 + 3.$$

$$x^3 - \frac{9}{16}x^2 - \frac{30}{16}x + \frac{23}{16} = 0$$

Sum of roots $= \frac{9}{16}$

two of roots are at P, i.e. $1, 1$.

Let $P * P = (a, b)$.

$$2 + a = \frac{9}{16} \; ; \; a = \frac{-23}{16}$$

$$b = \frac{3a+5}{4} = \frac{-\frac{69}{16} + 5}{4} = \frac{11}{64}.$$

$\therefore \left(-\frac{23}{16}, \frac{11}{64}\right)$ is another solution to $y^2 = x^3 + 3$.

$$\left(\frac{11}{64}\right)^2 = \frac{121}{2^{12}}$$

$$\left(-\frac{23}{16}\right)^3 + 3 = \frac{-23^3 + 3 \cdot 2^{12}}{2^{12}} = \frac{-12167 + 12288}{4096}$$

$$= \frac{121}{2^{12}}$$

Weierstrass Normal Form

Suppose we have two curves C, D defined over a field k.
A birational equivalence $f: C \to D$ is a function given by rational functions with coefficients in k such that there is an inverse function $g: D \to C$, which is also given by rational functions with coefficients in k.

$\therefore$ if we can find all the points in $C(\mathbb{Q})$, then we can find the points in $D(\mathbb{Q})$

$$D(\mathbb{Q}) = \{ f(p) : p \in C(\mathbb{Q}) \}$$

Example:

$$C: y = x^2$$

$$D: y = 0$$

The birational equivalence is

$$f : C \to D \quad ; \quad f(x,y) = (x,0)$$

$$g : D \to C \quad ; \quad g(x,y) = (x,x^2)$$

$$f(g(x,y)) = f(x, x^2) = (x,0)$$

since $(x,y) \in D$, $y = 0$

so $(x,0) = (x,y)$

$$g(f(x,y)) = g(x,0) = (x,x^2) = (x,y)$$

since $y = x^2$ on C.

Both these curves have points at infinity

$(0:1:0) \in C$.
$(1:0:0) \in D$.

$(0:1:0)$ is in the (x,z)-plane
$(1:0:0)$ is in the (y,z)-plane.

We'll redefine f as a map from x,z-coordinates to y,z-coordinates.

$f(x,y) = (x,0)$

$f(X:Y:Z) = \left(\frac{X}{Z} : 0 : 1\right)$

$= \left(1 : 0 : \frac{Z}{X}\right)$

$f(x,z) = \left(1 : 0 : \frac{z}{x}\right)$

since $(x,z) \in C$, $z = x^2$.

$f(x,z) = (1 : 0 : x)$

$\therefore f(0:1:0) = (1:0:0)$.

similarly $g(1:0:0) = (0:1:0)$

More generally, if C is a conic with a point (non-singular), then C is birationally equivalent to a line, by stereographic projection.

A cubic is in Weierstrass normal form if it is $y^2 = x^3 + ax + b$, $a, b \in k$

or generalised Weierstrass normal form if it is $y^2 = x^3 + ax^2 + bx + c$
$a, b, c \in k$.

<u>Theorem</u>

If $2 \neq 0$ in k, then every elliptic curve is birationally equivalent to one in generalised Weierstrass normal form.

If $2 \neq 0$ and $3 \neq 0$ in k, then we can change this to Weierstrass normal form.

Algorithm

Start with a curve C and a point $O \in C(\mathbb{Q})$. Let $L_1 = T_O C$.

case 1:
(O is not a point of inflection)

$L_1 \cap C = \{O, O, P\}$, $P \neq O$.

Let $L_2 = T_P C$

Let L_3 be another line through O.
(not equal to L_1).

case 2:
(O is a point of inflection).

Let $L_1 = T_O C$

L_2 another line through O

L_3 a line not going through O.

Change variables, so these 3 lines are

$L_1 : Z = 0$

$L_2 : X = 0$

$L_3 : Y = 0$

Step 2

Assume O was not a point of inflection (otherwise we miss out this step).

The curve has the form

$$xy^2 + (ax+b)y = cx^2 + dx + e$$
$$(a, b, c, d, e \in k).$$

multiply both sides by x & then replace y by $\frac{y}{x}$.

$$\therefore\ y^2 + (ax+b)y = cx^3 + dx^2 + ex.$$

Step 3

Complete the square on LHS; i.e. replace y by $y - \frac{ax+b}{2}$ (we can do this since $2 \neq 0$).

This gives

$$y^2 = ax^3 + bx^2 + cx + d$$
$$\text{new } a, b, c, d \in k$$

Step 4

replace x by $\frac{x}{a}$ and y by $\frac{y}{a}$

$$\frac{y^2}{a^2} = \frac{x^3}{a^2} + \frac{bx^2}{a^2} + \frac{cx}{a} + d$$

$\therefore \quad y^2 = x^3 + ax^2 + bx + c$, new $a, b, c \in k$

This is in generalised Weierstrass normal form. $\bigcirc$

Step 5: Complete the cube if $3 \neq 0$.

i.e. replace x by $x - \frac{a}{3}$.

After this, the curve is in Weierstrass normal form.

Example:

$$C: \underbrace{U^3 + V^3 - 2W^3}_{=F} = 0.$$

$$\mathcal{O} = (1:1:1)$$

$$\frac{\partial F}{\partial U} = 3U^2$$

$$\frac{\partial F}{\partial V} = 3V^2$$

$$\frac{\partial F}{\partial W} = -6W^2$$

$T_O C: \; 3U + 3V - 6W = 0.$

$L_1: U + V - 2W = 0$

on $L_1 \cap C$: $\quad V = 2W - U$

$$U^3 + (2W - U)^3 - 2W^3 = 0$$

$$6W^3 - 12W^2U + 6WU^2 = 0$$

$W(U - W)^2 = 0$, there is a double root at O; the other root is $W = 0$, $V = -U$

$P = (1 : -1 : 0)$

so O is not a point of inflection.

$T_P C: \quad 3U + 3V = 0$

$L_2: \quad U + V = 0$

let $L_3: U - V =$

$\therefore$ let $z = u + v - 2w$

$x = u + v$

$y = u - v$

$\Rightarrow u = \frac{x+y}{2}$; $v = \frac{x-y}{2}$; $-w = \frac{z-x}{2}$

$$F = \left(\frac{x+y}{2}\right)^3 + \left(\frac{x-y}{2}\right)^3 + 2\left(\frac{z-x}{2}\right)^3$$

$$\Rightarrow F = \frac{1}{8}\left(2x^3 + 6xy^2 + 2z^3 - 6z^2x + 6zx^2 - 2x^3\right)$$

in $(x;y)$ - coordinates :

$$C: \cancel{x^3} + 3xy^2 + 1 - 3x + 3x^2 \cancel{- x^3}$$

$$3xy^2 = -3x^2 + 3x - 1$$

04. 02. 2014.

Elliptic Curves

Weierstrass Normal Form

Method:

Start off with a curve C and a point $O \in C(\mathbb{Q})$

if O is not a point of inflection:

$$L_1 = T_O C$$

$$L_1 \cap C = \{O, O, P\} \quad (P \neq O)$$

$$L_2 = T_P C$$

L_3 another line through O.

$L_1: Z = 0$
$L_2: X = 0$
$L_3: Y = 0$

alfter this change of variable

$$xy^2 + (ax+b)y = cx^2 + dx + e$$

replace y by $\frac{y}{x}$ & multiply by x

$$y^2 + (ax+b)y = cx^3 + dx + e.$$

replace y by $y - \frac{ax+b}{2}$.

$$y^2 = ax^3 + bx^2 + cx + d$$

replace x by $\frac{x}{a}$ and y by $\frac{y}{a}$

$\therefore\ y^2 = x^3 + ax^2 + bx + c.$

if $3 \neq 0$, then replace x by $x - \frac{a}{3}$.

$$y^2 = x^3 + ax + b.$$

<u>Example:</u>

$$u^3 + v^3 - 2w^3 = 0$$

$$O = (1:1:1)$$

$L_1 = T_O C \quad : \quad u + v - 2w = 0$

$\qquad\qquad Z = u + v - 2w.$

$L_1 \cap C = \{O, O, P\} \quad ; \quad P = (1:-1:0)$

$L_2 = T_P C \quad : \quad u + v = 0 \quad ; \quad X = u + v$

$L_3 : u - v = 0 \quad ; \quad Y = u - v.$

$$u = \frac{X + Y}{2}$$

$$v = \frac{X - Y}{2}$$

$$w = \frac{X - Z}{2}$$

$$F = U^3 + V^3 - 2W^3$$

$$= \left(\frac{X+Y}{2}\right)^3 + \left(\frac{X-Y}{2}\right)^3 - 2\left(\frac{X-Z}{2}\right)^3$$

$$= \frac{1}{8}\Big(\cancel{X^3} + \cancel{3X^2Y} + 3XY^2 + \cancel{Y^3}$$

$$+\cancel{X^3} - \cancel{3X^2Y} + 3XY^2 - \cancel{Y^3}$$

$$\cancel{-2X^3} + 6X^2Z - 6XZ^2 + 2Z^3\Big)$$

$$= \frac{1}{8}\left(6XY^2 + 6X^2Z - 6XZ^2 + 2Z^3\right)$$

in (x,y)-coordinates, the curve is

$$3xy^2 = -3x^2 + 3x - 1$$

$\rightarrow$ replace y by $\frac{y}{x}$ & multiply by x.

$$3x\,\frac{y^2}{x^2} = -3x^2 + 3x - 1$$

$$\therefore\ 3y^2 = -3x^3 + 3x^2 - x$$

Don't need to complete the square.

$$y^2 = -x^3 + x^2 - \frac{1}{3}x.$$

replace x by $-x$ & y by $-y$

$$y^2 = x^3 + x^2 + \frac{x}{3}.$$

next: complete the cube: (replace x by $x-\frac{1}{3}$)

$$y^2 = x^3 - \cancel{x^2} + \cancel{\frac{1}{3}x} - \frac{1}{27} \cancel{+ x^2} - \cancel{\frac{2}{3}x} + \cancel{\frac{1}{9}}$$
$$\cancel{+\frac{1}{3}x} - \cancel{\frac{1}{9}}.$$

$$= x^3 - \frac{1}{27}$$

This is in Weierstrass Normal form.

We can get rid of the fraction by replacing x by $\frac{x}{3^2}$, y by $\frac{y}{3^3}$.

$$\frac{y^2}{3^6} = \frac{x^3}{3^6} - \frac{1}{3^3}$$

$$\therefore y^2 = x^3 - 3^3 = x^3 - 27.$$

<u>Proposition</u>

Let $C: y^2 = x^3 + ax^2 + bx + c$. and let $d \in k^*$.
Then C is birationally equivalent to

$$C': y^2 = x^3 + ad^2x^2 + bd^4x + cd^6.$$

<u>Proof</u>: replace y by $\frac{y}{d^3}$ and x by $\frac{x}{d^2}$

$$\frac{y^2}{d^6} = \frac{x^3}{d^6} + a\frac{x^2}{d^4} + b\frac{x}{d^2} + c$$

multiply by d^6 to get the equation of C' $\square$

<u>Remark:</u>

If $K = \mathbb{Q}$, then using the proposition, we can get C in the form $y^2 = x^3 + ax + b$ $(a, b \in \mathbb{Z})$.

<u>Example:</u>

$$U^3 + V^3 + W^3 = 0$$

$$\mathcal{O} = (1 : -1 : 0)$$

$$F = U^3 + V^3 + W^3$$

$$\frac{\partial F}{\partial U} = 3U^2, \quad \frac{\partial F}{\partial V} = 3V^2, \quad \frac{\partial F}{\partial W} = 3W^2.$$

$$L_1 = T_{\mathcal{O}} C : \quad 3U + 3V + 0W = 0$$

i.e. $U + V = 0$.

on $L_1 \cap C$: $V = -U$

$$U^3 + (-U)^3 + W^3 = 0$$

$$\therefore W = 0$$

so $L_1 \cap C = \{(1:-1:0, (1:-1:0), (1:-1:0)\}$

$\therefore$ $\mathcal{O}$ is a point of inflection.

L_2: any other line through $\mathcal{O}$.

L_3: any line not going through $\mathcal{O}$.

$$L_2 : W = 0.$$

$$L_3 : U = 0$$

$Z = U + V$	$U = Y$
$X = W$	$V = Z - Y$
$Y = U$	$W = X$

$$F = U^3 + V^3 + W^3 = \cancel{Y^3} + Z^3 - 3Z^2Y + 3ZY^2 - \cancel{Y^3} + X^3$$

in (x,y)-coordinates, the curve is

$$1 - 3y + 3y^2 + x^3 = 0.$$

$$y^2 - y = -\frac{1}{3}x^3 - \frac{1}{3}.$$

complete the square: replace y by $y + \frac{1}{2}$.

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

$$y^2 = -\frac{1}{3}x^3 \underbrace{- \frac{1}{3} - \frac{1}{4} + \frac{1}{2}}_{-\frac{1}{12}}$$

$$= -\frac{1}{3}x^3 - \frac{1}{12}$$

→ replace x by $-3x$, y by $-3y$

$$9y^2 = 9x^3 - \frac{1}{12}$$

$$y^2 = x^3 - \frac{1}{108} \qquad (108 = 2^2 \cdot 3^3)$$

using the proposition, we get

$$y^2 = x^3 - 2^4 \cdot 3^3 = x^3 - 432.$$

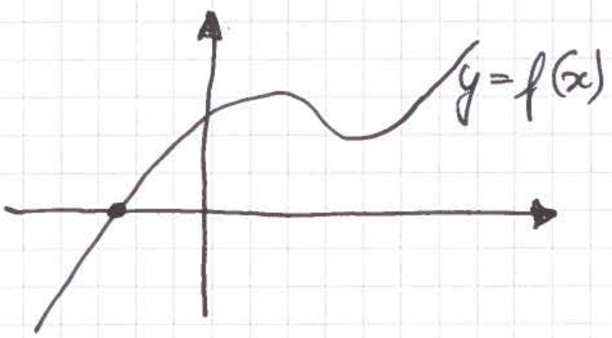
Cubic curves over $\mathbb{R}$

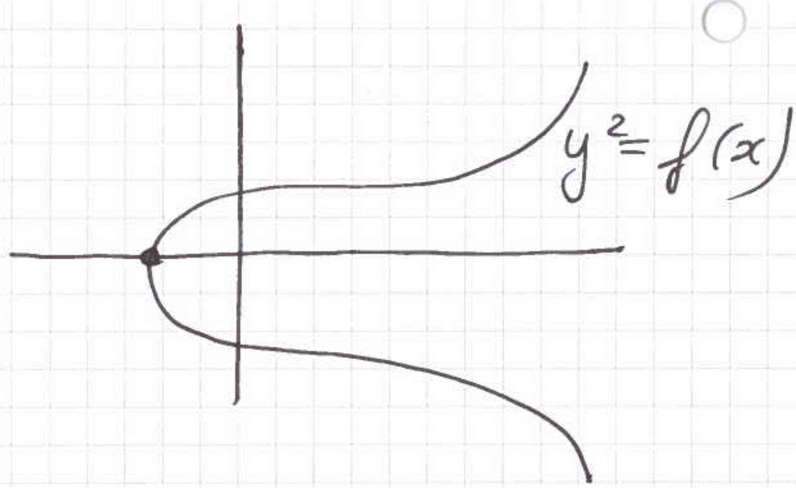
over $\mathbb{R}$ every cubic curve which is irreducible has a Weierstrass normal form. If C is an elliptic curve, then

$$C:\ y^2 = \underbrace{x^3 + ax + b}$$

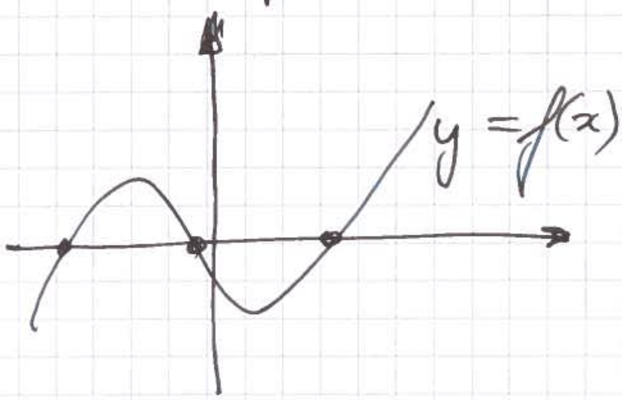
where $f(x)$ has no repeated root.

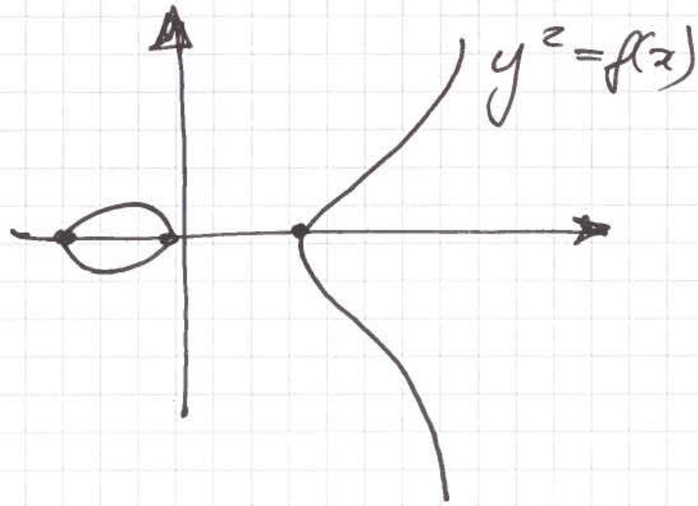
Case 1: f has 1 root:





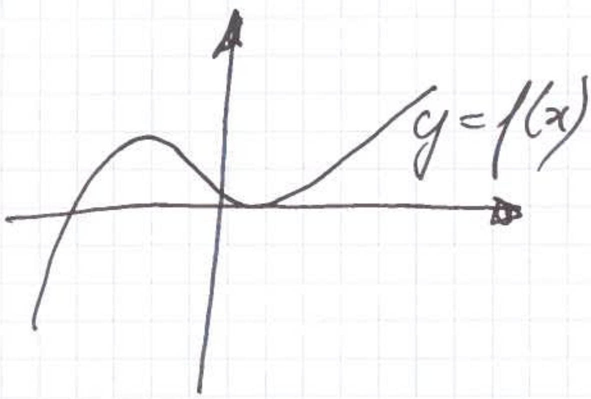
Case 2: f has 3 real roots

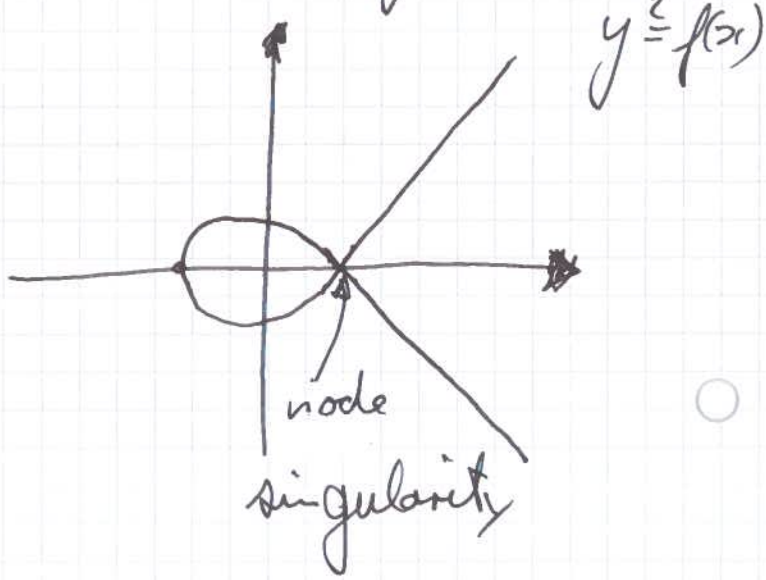




The singular curves has 2 kinds:

Case 3 1 double root & 1 single root.

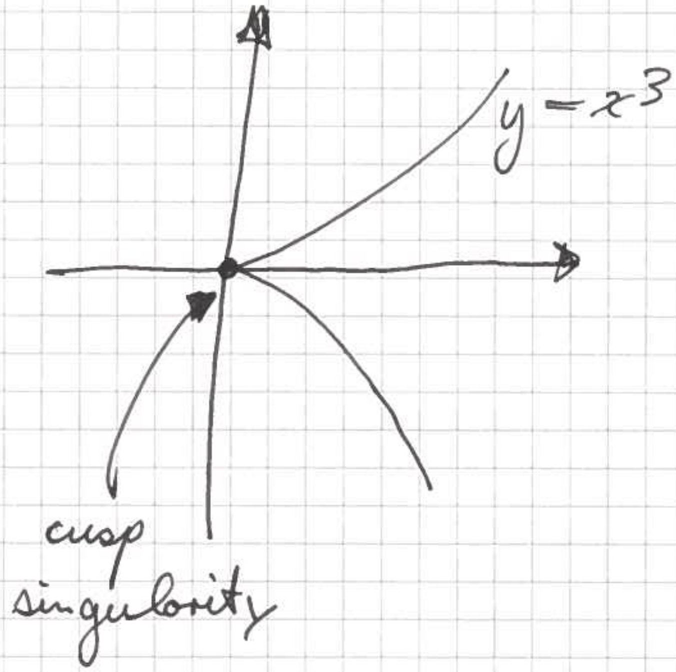




Case 4 :

f has a triple root

eg.: $y^2 = x^3$



Elliptic 07. 02. 2014

$y^2 = x^3 + ax + b$

$Y^2 Z = X^3 + aXZ^2 + bZ^3$

$Z = 0$

- $P, Q \in E(K)$
- $P * Q$ the 3rd point of intersection of the line PQ with E line for $\mathcal{O}$ (zero) & $P * Q$ the third point is $P+Q$.
- Given P on $E(\mathbb{Q})$

  $-P = P * S$ with $S = \mathcal{O} * \mathcal{O}$

$\Rightarrow \mathcal{O} = (0:1:0)$, 0-element

Prop.: The tangent line at $\mathcal{O}$ for E is $Z=0$ (= line at infinity).

Proof:

$f(X,Y,Z) = 0 \Rightarrow \nabla f \cdot (X,Y,Z) = 0$ is the tangent.

$\Rightarrow f(X,Y,Z) = Y^2 Z - (X^3 + aXZ^2 + bZ^3)$

$\frac{\partial f}{\partial X} = -3X^2 - aZ^2 \; ; \; \frac{\partial f}{\partial X}(0,1,0) = 0$

$\frac{\partial f}{\partial Y} = 2YZ \; ; \; \frac{\partial f}{\partial Y}(0,1,0) = 0$

$\frac{\partial f}{\partial Z} = Y^2 - aX2Z - 3bZ^2 \; ; \; \frac{\partial f}{\partial Z}(0,1,0) = 1$

$\Rightarrow (0,0,1)(X,Y,Z) = 0 \Rightarrow Z = 0$ //

Proposition

$\mathcal{O} = (0 : 1 : 0)$ is the only point at infinity of $E(\mathbb{R})$.

Proof: line at infinity $\Leftrightarrow$ $Z = 0$

$$0 = X^3 + 0 + 0 \Rightarrow X^3 = 0 \Rightarrow X = 0$$

$$\Rightarrow (0 : Y : 0)$$

//

Proposition

$\mathcal{O}$ is an inflection point for $E(\mathbb{R})$

Proof:

To show that the intersection of E with $T_{\mathcal{O}}(E)$ is triple $E \cap T_{\mathcal{O}}(E) = \{\mathcal{O}, \mathcal{O}, \mathcal{O}\}$.

//

Theorem 1:

Let $P = (a, b) \in E$ (finite), then $-P = (a, -b) = \mathcal{O} * P$.

Theorem 2:

$P + Q + R = 0$, for P, Q, R on $E(\mathbb{R})$

iff P, Q, R lie on the same line.

$$P + Q + R = 0 \iff P + Q = -R$$

<u>Proof for Theorem 1:</u>

$S = O * O$

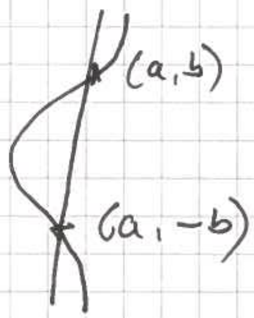
$-P = P * S$

$E \cap T_O(E) = \{O, O, O\}$

$S = O$

$-P = P * O.$

$\Rightarrow (a, b) * (a, -b) = O$



$X = a \Rightarrow X = aZ$

$O = (0 : 1 : 0)$

//

<u>Proof for Theorem 2:</u>

($\Leftarrow$) Let P, Q, R lie on a line & $E(2)$.

$R = P * Q$

Theorem 1.

$P + Q = O * R = -R \Rightarrow P + Q = -R$

$\Rightarrow P + Q + R = 0$

($\Rightarrow$) Let $P + Q + R = O$ show they lie on the same line:

$$P + Q = -R \overset{\text{previous}}{=} O * R.$$

$$O * (P * Q) = O * R = -R$$

$$\Rightarrow \quad -(P * Q) = -R$$

$$\Rightarrow \quad P * Q = R$$

<u>example:</u>

$\Rightarrow$ $y^2 = x^3 + ax^2 + bx + c$; two point $P = (x_1, y_1)$; $Q = (x_2, y_2)$

$P + Q$? $\qquad P + Q + R = 0$ iff they are colinear.

$P \neq Q$

$P \neq -Q$

$\Rightarrow$ line from P to Q : $y = \lambda x + \nu$

$$\lambda = \text{slope} = \frac{y_2 - y_1}{x_2 - x_1} \; ; \; \nu = y_1 - \lambda x_1 \text{ or } y_2 - \lambda x_2$$

$$\Rightarrow (\lambda x + \nu)^2 = x^3 + ax + b$$

$$\lambda^2 x^2 + 2\lambda x \nu + \nu^2 = x^3 + ax^2 + bx + c$$

$$0 = x^3 + (-\lambda^2 + a)x^2 + (b - 2\lambda\nu)x + c = 0$$

If (x_3, y_3) is the point R

$$x_1 + x_2 + x_3 = -a + \lambda^2$$

$$x_3 = -a + \lambda^2 - x_2 - x_2 .$$

$\Rightarrow$ example:

$$y^2 = x^3 + 17$$

$$\left.\begin{array}{l} Q = (2,5) \\ P = (-1,4) \end{array}\right\} \text{spot points!}$$

$P+Q$?

$$\lambda = \frac{5-4}{2-(-1)} = \frac{1}{3}$$

$$y = \frac{1}{3}x + \nu \Rightarrow 5 = \frac{2}{3} + \nu \Rightarrow \nu = 5 - \frac{2}{3}$$

$$= \frac{13}{3}$$

$$\Rightarrow y = \frac{x}{3} + \frac{13}{3}.$$

$$\Rightarrow a = 0$$

$$\Rightarrow x_3 = \lambda^2 - x_1 - x_2 = \left(\frac{1}{3}\right)^2 - (-1) - 2$$

$$= -\frac{8}{9}$$

Plug into $y = \frac{1}{3}x + \frac{13}{3}$

$$y_3 = \frac{1}{3}\left(-\frac{8}{9}\right) + \frac{13}{3} = \frac{109}{27}$$

$\Rightarrow$ found $R = \left(-\frac{8}{9}, \frac{109}{27}\right)$

$$\Rightarrow \quad P+Q = -R = \left(-\frac{8}{9}, -\frac{109}{27}\right).$$

If f is holomorphic on $D(z_0, \varepsilon)$
then $f(z) = \sum_{n \geq 0} a_n (z-z_0)^n$

If f is holomorphic on the punctured disc
$D'(z_0, \varepsilon) = D(z_0, \varepsilon) \setminus \{z_0\}$ there is an isolated singularity.

z_0 is a pole of order n if $\frac{1}{f(z)}$ has removable singularity at z_0 &
$\frac{1}{f}$ has a zero of order n at z_0 :

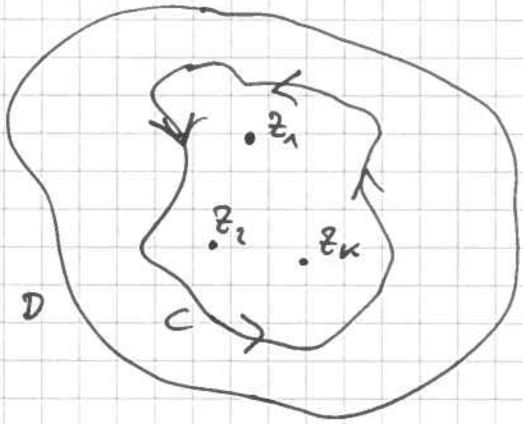
In this case

$$f(z) = \frac{A_{-n}}{(z-z_0)^n} + \frac{A_{-n+1}}{(z-z_0)^{n-1}} + \dots + \frac{A_{-1}}{z-z_0} + A_0 + A_1(z-z_0) + A_2(z-z_0)^2 + \dots$$

$A_{-1} = \text{Res}(f, z_0)$; if $n = 1$, i.e. pole at z_0 is simple

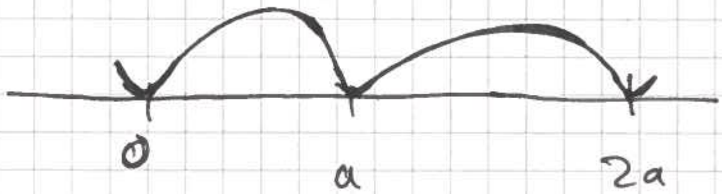
$$A_{-1} = \text{Res}(f, z_0) = \lim_{z \to z_0} (z - z_0) f(z)$$

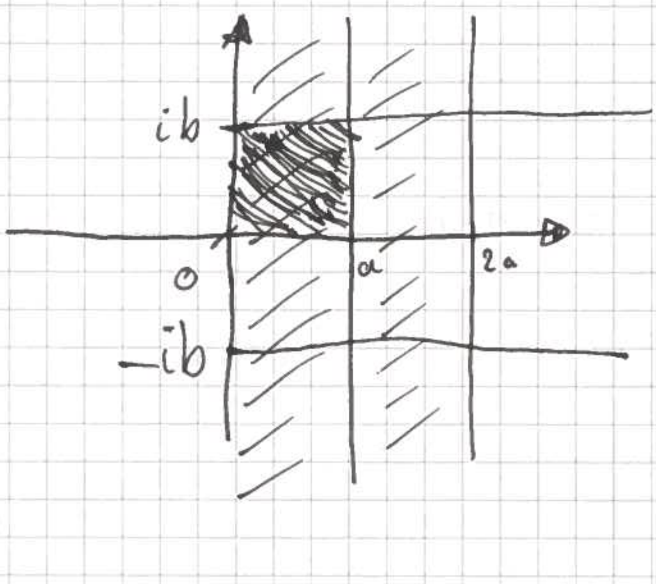
Residue Theorem



$$\int_C f(z)\,dz = 2\pi i \cdot \sum_K \text{Res}(f, z_K)$$

$f(z+a) = f(z)$; $z \in \mathbb{R} \Rightarrow$ Period a

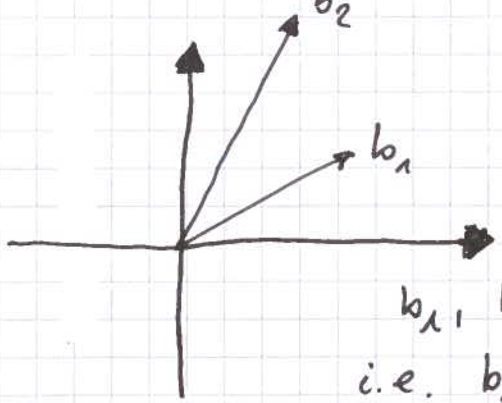




$f(z+a) = f(z)$, $\forall z \in \mathbb{C}$. ($a \in \mathbb{R}$)

$f(z+ib) = f(z)$

If f is holomorphic on $\mathbb{C}$ & satisfies $f(z+a) = f(z) = f(z+ib)$ $(\forall z \in \mathbb{C})$, then f is constant.



$b_1, b_2 \in \mathbb{C} \to$ basis of $\mathbb{C}$ over $\mathbb{R}$
i.e. b_1, b_2 are linearly independent over $\mathbb{R}$.

$$\left.\begin{array}{l} f(z+b_1) = f(z) \\ f(z+b_2) = f(z) \end{array}\right\} \forall z \in \mathbb{C}$$, then f is called doubly periodic.

$$f(z+2b_1) = f(z+b_1+b_1) = f(z+b_1) = f(z)$$

$$f(z+b_2k) = f(z), \ \forall k \in \mathbb{Z}.$$

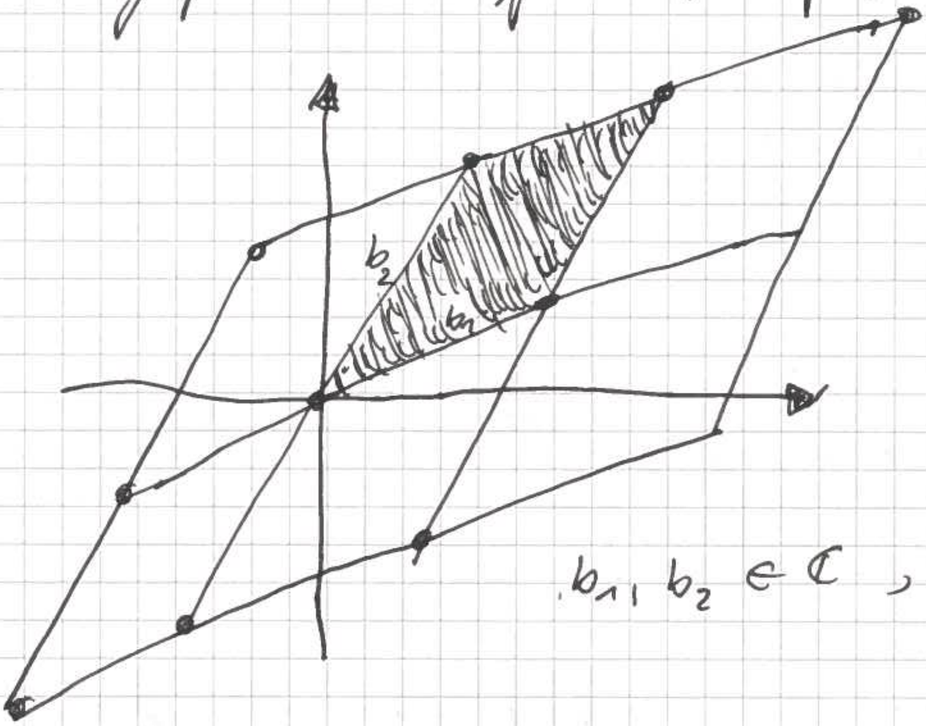
$$f(z+kb_2+mb_1) \underset{\substack{mb_1 \\ \text{period}}}{=} f(z+kb_2) \underset{\substack{kb_2 \\ \text{period}}}{=} f(z); k,m \in \mathbb{Z}$$

we care for the set of periods

$$L = \{kb_2 + mb_1 ; k,m \in \mathbb{Z}\}$$

lattice.

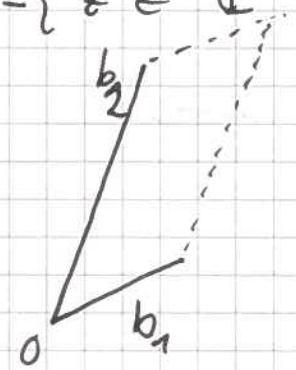
doubly periodic $\iff f(z+l) = f(z)$, $\forall z \in \mathbb{C}$, $\forall l \in L$



$b_1, b_2 \in \mathbb{C}$, as bases for $\mathbb{C}$

Fundamental set is

$$\mathcal{F} = \{ z \in \mathbb{C} \ ; \ z = x b_1 + y b_2 \ , \ x, y \in [0,1) \}$$



$\overline{\mathcal{F}}$ is the closed fundamental set

$$= \{ z \ ; \ z = x b_1 + y b_2 \ , \ x, y \in [0,1] \}$$

<u>Def.</u>: A meromorphic function which is double periodic w.r.t. L is called an elliptic function.

Prop.:

If f is elliptic & holomorphic on $\mathbb{C}$, then it is constant.

Proof:

- f is holomorphic on $\overline{F}$ $\Rightarrow$ continuous on $\overline{F}$ compact.

$\Rightarrow$ f is bounded on $\overline{F}$ compact

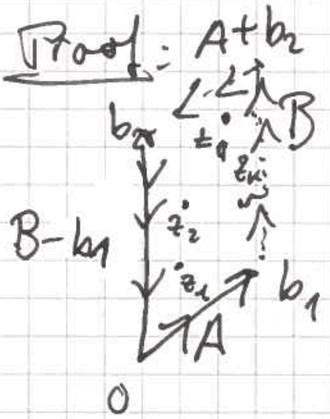
- $\exists M \geq 0 \quad |f(z)| \leq M \quad , \forall z \in \overline{F}$
- Since f is double periodic $|f(z)| \leq M$, $\forall z \in \mathbb{C}$.
- f is holomorphic on $\mathbb{C}$ (i.e. entire) &
  $|f(z)| \leq M$ on $\mathbb{C}$ bounded.
- Liouville Theorem: An entire bounded function is constant.

Theorem

Let f be elliptic w.r.t. L & $z_1, z_2, \dots, z_k$ be the set of poles in $\mathcal{F}$ (fundamental set).

Then $\displaystyle\sum_{j=1}^{k} \operatorname{res}(f, z_j) = 0$.

Proof:



call boundary of $\mathcal{F}$ by C

$$\int_C f(z)\,dz = 2\pi i \sum_{j=1}^{k} \operatorname{Res}(f, z_j)$$

residue theorem.

$$\int_C f(z)\,dz = \int_A f(z)\,dz + \int_B f(z)\,dz - \int_{A+b_2} f(z)\,dz - \int_{B-b_1} f(z)\,dz$$

To show $\displaystyle\int_{A+b_2} f(z)\,dz = \int_A f(z)\,dz$ &

similarly $\displaystyle\int_{B-b_1} f(z)\,dz = \int_B f(z)\,dz$.

$$\int_{A+b_2} f(z)\,dz$$

Let A be parametrized by $z = z(t)$; $a \leq t \leq b$.

Then $A + b_2$ is parametrized by $z = z(t) + b_2$; $a \leq t \leq b$.

$$\int_A f(z)\,dz = \int_a^b f(z(t))\, z'(t)\,dt$$

$\parallel$ since f has period b_2.

$$\int_{A+b_2} f(z)\,dz = \int_a^b f(z(t)+b_2)\, z'(t)\,dt)$$

Let f have a zero of order n at z_0, then we can find a holomorphic function on $D(z_0, \delta)$ s.t.

$$f(z) = (z-z_0)^n g(z) \quad \& \quad g(z) \neq 0, \ \forall z \in D(z_0, \delta)$$

$$\log f(z) = n \log(z - z_0) + \log(g(z))$$

Differentiate:

$$\frac{f'(z)}{f(z)} = \frac{n}{z-z_0} + \frac{g'(z)}{g(z)}$$

$\Rightarrow \dfrac{f'}{f}$ has a simple pole at z_0 with residue n.

Suppose f has a pole of order n at z_0, then $\dfrac{f'(z)}{f(z)}$ has a simple pole at z_0 with residue $-n$.

$\Rightarrow f(z) = (z - z_0)^{-n} g(z)$ with $g(z)$ holomorphic & non zero on $D(z_0, \delta)$

$$\frac{f'(z)}{f(z)} = \frac{-n}{z - z_0} + \frac{g'(z)}{g(z)}.$$

<u>Theorem</u>:

Let f be a nonzero elliptic function. Then the number of zeros (counting multiplicities) = number of poles of f [inside F].

<u>Proof</u>:

$$\int_C \frac{f'(z)}{f(z)}\, dz = (\#\text{ zeros} - \#\text{ poles}) \cdot 2\pi i$$

$$\int_C \frac{f'(z)}{f(z)}\,dz = 2\pi i \sum_{j=1}^{k} \operatorname{res}\left(\frac{f'}{f}, z_j\right)$$

zeros or poles of $f(z)$

$$= 2\pi i\,(\#\text{ zeros} - \#\text{ poles})$$

[counted with multiplicity].

$$\Rightarrow \int_C \frac{f'(z)}{f(z)}\,dz = \int_A \frac{f'(z)}{f(z)}\,dz + \int_B \frac{f'(z)}{f(z)}\,dz$$

$$- \int_{\dots} \dots - \int_{\dots} \dots$$

Since f is periodic, f' is periodic & $\frac{f'}{f}$ is periodic. ($\frac{f'}{f}(z+l) = \frac{f'}{f}(z)$ $l \in L$.)

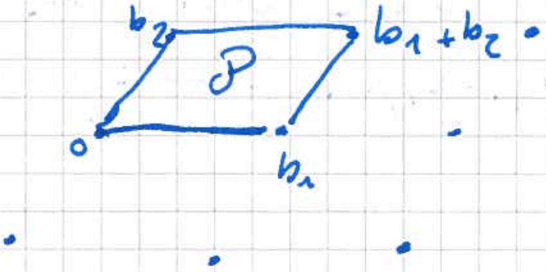
$$\Rightarrow \int_C \frac{f'}{f}\,dz = 0 \quad \square$$

12.02.2014

Elliptic

Let $\mathcal{B} = \{b_1, b_2\}$ basis for $\mathbb{C}$ over $\mathbb{R}$.

$L = \{x b_1 + y b_2 : x, y \in \mathbb{Z}\}$



$\mathcal{P} = \{x b_1 + y b_2 : x, y \in [0,1)\}$

An elliptic function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ such that

$$f(z + l) = f(z) \quad , z \in \mathbb{C}, \ l \in L.$$

- if f is an elliptic function with no poles, then f is constant.
- if $p_1, \dots, p_n$ are the poles of f. (in $\mathcal{P}$).

  Then $\sum_1^n \mathrm{Res}_{p_i}(f) = 0$.

- number of zeros of f (counting multiplicity) = number of poles (in $\mathcal{P}$).

<u>Proof</u>: $\frac{f'(z)}{f(z)}$ is an elliptic function. if

$f(z) = (z - z_0)^n g(z)$, where g has no zero of pole at z_0 !

Then $\operatorname{Res}_{z_0}\left(\frac{f'}{f}\right) = n$.

<u>Proposition</u>

Let f be an elliptic function with zeros $z_1, \dots, z_n$ and poles $p_1, \dots, p_n$ (counting multiplicity)

Then

$$\sum z_i - \sum p_i \in L$$

<u>Proof</u>:

<u>idea</u>: integrate $\dfrac{z f'(z)}{f(z)}$ around ∂P.

The integral will not vanish as before because $\dfrac{z f'(z)}{f(z)}$ is not an elliptic function.

Suppose $f(z) = (z-a)^n g(z)$; $g(a) \neq 0$, so

$$f'(z) = n(z-a)^{n-1} g(z) + (z-a)^n g'(z)$$

$$\frac{z f'(z)}{f(z)} = \frac{nz}{z-a} + \underbrace{\frac{z g'(z)}{g(z)}}_{\text{no pole at } a!}$$

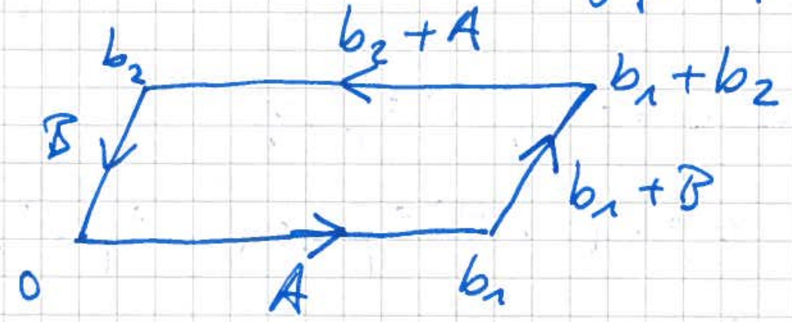
$$= \frac{n(z-a)}{z-a} + \frac{na}{z-a} + \text{no pole at } a.$$

$$= \frac{na}{z-a} + \text{no pole at } a$$

$$\operatorname{Res}_{z=a} \frac{z f'(z)}{f(z)} = na.$$

$$\therefore \sum{}' z_i - \sum{}' p_i = \sum_{a \in P} \operatorname{Res}_a \left(\frac{z f'(z)}{f(z)} \right)$$

$$2\pi i \sum{}' \operatorname{Res}_a \left(\frac{z f'(z)}{f(z)} \right) = \int_{\partial P} \frac{z f'(z)}{f(z)}\, dz.$$



$$2\pi i \sum{}' \operatorname{Res}_a \frac{z f'(z)}{f(z)} = \left\{ \int_A - \int_{A+b_2} + \int_B - \int_{B+b_1} \right\} \frac{z f'}{f}\, dz$$

Let $I = \left(\int_A - \int_{A+b_2} \right) \frac{z f'}{f}\, dz.$

we'll show that $I \in 2\pi i L$.

$$I = \int_A \left(\frac{z f'}{f} - \frac{(z+b_2)\, f'(z+b_2)}{f(z+b_2)} \right) dz$$

$$= \int_A \left(z \frac{f'}{f} - (z+b_2) \frac{f'}{f} \right) dz$$

$$= -b_2 \int_A \frac{f'}{f}\, dz = -b_2 \int_\gamma \frac{1}{w}\, dw$$

$w = f(z)$; γ is the path w takes as z goes along A.

when $z = 0$, $w = f(z)$

$z = b_1$, $w = f(b_1) = f(0)$

γ is a closed path.

$I = -b_2 \cdot 2\pi i \cdot n$, where n is the number of times γ winds around the pole 0.

since $I = -2\pi i b_1 n$

$\therefore\ I \in 2\pi i L$

Similarly $\left(\int_B - \int_{B+b_1} \right) \frac{z f'}{f}\, dz = 2\pi i L$

$\therefore\ 2\pi i \left(\sum' z_i - \sum' p_i \right) \in 2\pi i L$

$\square$

The Weierstrass $\wp$ - function.

If f is a non - constant elliptic function, then f must have at least 2 poles or a double pole (because $\sum' \text{Res}(f) = 0$)

$\therefore$ simplest imaginable elliptic function would have a double pole at 0 & no other poles. (i.e. a double pole at every point of L).

→ Try this

$$\sum_{l \in L}' \frac{1}{(z-l)^2}$$

⇒ unfortunately this doesn't converge absolutely.

→ 2nd attempt

$$\therefore \sum_{l \in L}' \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

⇒ unfortunately $\frac{1}{0^2}$ makes no sense.

Correct definition

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{l \in L \\ l \neq 0}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

Facts:

$\wp$ converges absolutely for $z \notin L$.

(So we don't worry about the order of summation).

If $B = \overline{B(0,R)}$, then

$$\sum_{\substack{l \in L \\ l \notin B}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$ converges uniformly on B, so is analytic on B.

$\therefore$ $\wp(z)$ is meromorphic on B with double poles at each point of L in B, and no other poles. The residues are all ~~zero~~ 0.

Letting $R \to \infty$, we find that $\wp$ is meromorphic on $\mathbb{C}$, its poles are double poles at each $l \in L$ with residue 0.

Proposition

$\wp$ is an elliptic function.

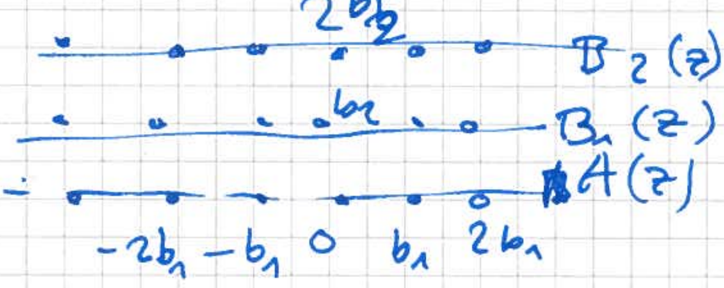
Proof:

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\ell \in L \\ \ell \neq 0}}^{\#} \left(\frac{1}{(z-\ell)^2} - \frac{1}{\ell^2} \right)$$

$$= A(z) + \sum_{\substack{y \in \mathbb{Z} \\ y \neq 0}}' B_y(z)$$

$$A(z) = \frac{1}{z^2} + \sum_{\substack{n \in \mathbb{Z} \\ n \neq 0}}' \left(\frac{1}{(z-nb_1)^2} - \frac{1}{(nb_1)^2} \right)$$

$$B_y(z) = \sum_{n \in \mathbb{Z}}' \frac{1}{(z-nb_1+yb_2)^2} - \frac{1}{(nb_1+yb_2)^2}$$



Claim: $A(z+b_1) = A(z)$
$B_y(z+b_1) = B(z)$

$\Rightarrow \wp(z+b_1) = \wp(z)$.

14.02.2014

Elliptic

Elliptic Functions

$f: \mathbb{C} \to \mathbb{C} \cup \{\infty\}$, which is meromorphic and $f(z+l) = f(z)$, $\forall z \in \mathbb{C}$, $l \in L$

- every noncont. elliptic function has a pole
- $\#$ poles $= \#$ zeroes
- $\sum' \mathrm{Res}(f) = 0$
- if z_i are the zeros, p_i are the poles, then
  $\sum' z_i - \sum' p_i \in L$.

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{l \in L \\ l \neq 0}}' \left(\left(\frac{1}{(z-l)^2}\right) - \frac{1}{l^2} \right)$$

$\wp(z)$ is meromorphic on $\mathbb{C}$ its only poles are double poles at each $l \in L$.

Proposition

$\wp$ is an elliptic function.

($\wp(z)$ converges absolutely).

Proof:

$$\wp(z) = A(z) + \sum_{\substack{y \in \mathbb{Z} \\ y \neq 0}}' B_y(z)$$

$$A(z) = \sum_{\substack{n \in \mathbb{Z} \\ n \neq 0}}' \left(\frac{1}{(z - nb_1)^2} - \frac{1}{(nb_1)^2} \right) + \frac{1}{z^2}$$

$$B_y(z) = \sum_{n \in \mathbb{Z}}' \left(\frac{1}{z - (nb_1 + yb_2)^2} - \frac{1}{(nb_1 + yb_2)^2} \right)$$

sufficient to prove $\wp(z + b_1) = \wp(z)$.

$$A(z) = \sum_{\substack{n \in \mathbb{Z} \\ n \neq 0}}' \left(\frac{1}{(z - nb_1)^2} - \frac{1}{(nb_1)^2} \right) + \frac{1}{z^2}$$

$$= \sum_{n \neq 0}' \frac{1}{(z - nb_1)^2} - \underbrace{\sum_{n \neq 0}' \frac{1}{(nb_1)^2}}_{= C} + \frac{1}{z^2}$$

(these sums converge individually).

$$\therefore A(z) = \sum_{n \in \mathbb{Z}}' \frac{1}{(z - nb_1)^2} - C.$$

$$A(z+b_1) = \sum_{n\in\mathbb{Z}}' \frac{1}{(z+b_1-nb_1)^2} - C$$

$$= \sum_{n\in\mathbb{Z}}' \frac{1}{(z-(n-1)b_1)^2} - C$$

$$= \sum_{m\in\mathbb{Z}}' \frac{1}{(z-mb_1)^2} - C = A(z)$$

$$(m = n-1)$$

$$B_y(z) = \sum_{n\in\mathbb{Z}}' \left(\frac{1}{(z-(nb_1+yb_2)^2)} - \frac{1}{(nb_1+yb_2)^2} \right)$$

Again we can pull the two sums apart.

$$B_y(z) = \sum_{n\in\mathbb{Z}}' \frac{1}{(z-(nb_1+yb_2))^2} - D$$

for another constant D.

$$B_y(z+b_1) = \sum_{n\in\mathbb{Z}}' \frac{1}{(z+b_1-(nb_1+yb_2))^2} - D$$

$$= \sum_{n\in\mathbb{Z}}' \frac{1}{(z-((n-1)b_1+yb_2))^2} - D$$

$$= \sum_{n\in\mathbb{Z}}' \frac{1}{(z-(nb_1+yb_2))^2} - D = B_y(z)$$

$\therefore \wp(z+b_1) = \wp(z)$

Similarly $\wp(z+b_2) = \wp(z)$

$\therefore \wp$ is elliptic $\square$

<u>Lemma:</u>

$\wp$ is an even function.

<u>Proof:</u>

$$\wp(-z) = \sum_{\substack{\ell \in L \\ \ell \neq 0}}' \left(\frac{1}{(-z-\ell)^2} - \frac{1}{\ell^2} \right) + \frac{1}{(-z)^2}$$

$$= \sum_{\substack{\ell \in L \\ \ell \neq 0}}' \left(\frac{1}{(z+\ell)^2} - \frac{1}{\ell^2} \right) + \frac{1}{z^2}$$

$$= \sum_{\substack{\ell \in L \\ \ell \neq 0}}' \left(\frac{1}{(z-\ell)^2} - \frac{1}{\ell^2} \right) + \frac{1}{z^2}$$ Replace ℓ by $-\ell$

$= \wp(z)$. $\square$

We'll work out the first few terms in the Laurent series of $\wp(z)$ at $z=0$.

Let $$g_2 = 60 \sum_{\substack{l \in L \\ l \neq 0}}' \frac{1}{l^4}$$

$$g_3 = 140 \sum_{\substack{l \in L \\ l \neq 0}}' \frac{1}{l^6}$$

<u>Lemma:</u>

for z near 0.

$$\wp(z) = \frac{1}{z^2} + \frac{g_2}{20} z^2 + \frac{g_3}{28} z^4 + O(z^6)$$

<u>Proof:</u>

$$\underbrace{\wp(z) - \frac{1}{z^2}}_{=f(z)} = \sum_{\substack{l \in L \\ l \neq 0}}' \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

We can differentiate this term by term. (convergence is uniform on $B(0,\varepsilon)$).

$$f'(z) = \sum_{\substack{l \in L \\ l \neq 0}}' \frac{-2}{(z-l)^3} \; ; \; f''(z) = \sum_{\substack{l \in L \\ l \neq 0}}' \frac{6}{(z-l)^4}$$

$$f'''(z) = \sum_{\substack{\ell \in L \\ \ell \neq 0}}' \frac{-24}{(z-\ell)^5} \; ; \; f^{(4)}(z) = \sum_{\substack{\ell \in L \\ \ell \neq 0}}' \frac{120}{(z-\ell)^6}$$

(linear $\equiv 0$).

$\Rightarrow f'(0), f'''(0), f'''''(0) = 0$, since f is even.

$$f''(0) = \sum_{\substack{\ell \in L \\ \ell \neq 0}}' \frac{6}{\ell^4} = \frac{g_2}{10}$$

$$f^{(4)}(0) = 120 \sum_{\substack{\ell \in L \\ \ell \neq 0}}' \ell^{-6} = \frac{6}{7} g_3$$

$$f(0) = \sum' \left(\frac{1}{(0-\ell)^2} - \frac{1}{\ell^2} \right) = 0.$$

$$f(z) = 0 + \frac{f''(0) z^2}{2!} + \frac{f^{(4)}(0) z^4}{4!} + O(z^6)$$

$$= \frac{g_2}{20} z^2 + \frac{g_3}{28} z^4 + O(z^6) \quad \square$$

<u>Theorem</u>:

$$(\wp'(z))^2 = 4 \wp(z)^3 - g_2 \wp(z) - g_3$$

i.e. $(\wp(z), \wp'(z))$ is a point on the elliptic curve $y^2 = 4x^3 - g_2 x - g_3$.

Proof:

let $g(z) = \wp'^2 - 4\wp^3 + g_2\wp + g_3$.

Clearly g is an elliptic function.
The only possible pole of g is at $z=0$.

$$\wp(z) = \frac{1}{z^2} + \frac{g_2}{20}z^2 + \frac{g_3}{28}z^4 + O(z^6).$$

$$\therefore \wp'(z) = \frac{-2}{z^3} + \frac{g_2}{10}z + \frac{g_3 z^3}{7} + O(z^5)$$

$$\therefore \wp'(z)^2 = \frac{4}{z^6} - 2\cdot(-2)\cdot\frac{g_2}{10}z^{-2}$$

$$+ 2(-2)\frac{g_3}{7} + O(z^2)$$

$$= \frac{4}{z^6} - \frac{2}{5}g_2\frac{1}{z^2} - \frac{4}{7}g_3 + O(z^2)$$

$$\wp(z)^3 = \frac{1}{z^6} + 3\cdot 1\cdot\frac{g_2}{20}z^{-2} + 3\cdot 1\cdot\frac{g_3}{28}$$

$$+ O(z^2)$$

$$4\wp(z)^3 - g_2\wp(z) - g_3 = \frac{4}{z^6} + \left(\frac{3g_2}{5} - g_2\right)\frac{1}{z^2}$$
$$+ \left(\frac{3g_3}{7} - g_3\right) + O(z^2)$$
$$= \frac{4}{z^6} - \frac{2g_2}{5}\frac{1}{z^2} - \frac{4g_3}{7} + O(z^2).$$

$\therefore f(z) = O(z^2)$

$\therefore$ f has no poles & $f(0) = 0$.

but f is constant so $f = 0$ $\square$

Let L be a lattice, we have $\wp$-complex numbers g_2, g_3.

Let $C_L : y^2 = 4x^3 - g_2 x - g_3$

this is an elliptic curve over $\mathbb{C}$.

We have a map

$$\Phi : \frac{\mathbb{C}}{L} \longrightarrow C_L(\mathbb{C})$$

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

if $z \in L$

We extend the definition to $z \in L$ by continuity (w.r.t. x, z-coordinates).

If z is close to 0, then

$$\wp(z) = \frac{1}{z^2}\left(1 + O(z^2)\right)$$

$$\wp'(z) = -\frac{2}{z^3}\left(1 + O(z^2)\right)$$

$$\Phi(z) = \left(\wp(z) ; \wp'(z) : 1\right)$$

$$= \left(\frac{\wp(z)}{\wp'(z)} : 1 : \frac{1}{\wp'(z)}\right) \xrightarrow[z \to 0]{} (0 : 1 : 0) = O$$

So we define $\Phi(0) = 0$.

Theorem:

$\Phi : \mathbb{C}/L \to C_L(\mathbb{C})$ is a bijection.

Lemma:

The zeros of $\wp'$ are at $z = \frac{b_1}{2}, \frac{b_2}{2}, \frac{b_1+b_2}{2}$

They are all simple zeros.

They are the solutions to $2z \in L$
$z \notin L$

Proof of Lemma:

Since $\wp$ is even, $\wp'$ must be odd

If $z \in \left\{ \frac{b_1}{2}, \frac{b_2}{2}, \frac{b_1+b_2}{2} \right\}$, then

$2z \in L$

$\therefore z = -z + l \quad (l \in L)$

$\wp'(z) = \wp'(-z) = -\wp'(z) \;\Big|\; \therefore \wp'(z) = 0.$

But $\wp'$ has only a triple pole, so it can only have these 3 zeros and they must all be simple. $\square$

Proof of theorem:

(surjectivity):
let $P = (x, y) \in C_L(\mathbb{C})$:
clearly $\mathcal{O}$ has the preimage 0; so we'll assume $P \neq \mathcal{O}$).

Want a solution to

$$\wp(z) = x, \ \wp'(z) = y$$

let $f(z) = \wp(z) - x$

This is an elliptic function with a double pole at 0.

$\therefore$ it has a zero at some $z \in \mathbb{C}$, i.e. $\wp(z) = x$

note: (x, y) & $(x, \wp'(z))$ are both solutions to

$$(\wp'(z))^2 = y^2 = 4x^3 - g_2 x - g_3$$

$\therefore y = \pm \wp'(z)$, if $y = -\wp'(z)$, then

$$y = \wp'(-z); \ x = \wp(-z)$$

since $\wp$ is even and $\wp'$ is odd.

$\Rightarrow$ that proves surjectivity.

(injectivity).

Assume $\Phi(a) = \Phi(b) = (x,y) \in C_L(\mathbb{C})$.

$$a, b \in \mathbb{C}/L$$

want to show : $a \equiv b \ (L)$

let $f(z) = \wp(z) - x$

$$\wp(a) = \wp(b) = x$$
$$\wp'(a) = \wp'(b) = y$$

a & b are zeros of f.

But f only has a double pole, so these are all the zeros.

→ since $\sum' z_i - \sum' p_i \in L$

$$\Rightarrow a + b - 0 - 0 \in L$$

$$\therefore \quad a \equiv -b \quad (L)$$

⇒ Since $\wp'$ is odd : $\wp'(a) = -\wp'(b)$

but $\wp'(a) = \wp'(b) = 0$

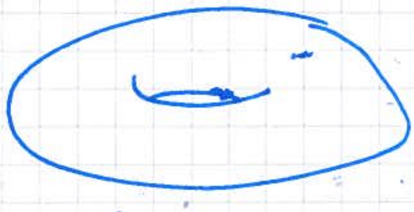
$$\therefore \wp'(a) = \wp'(b) = 0$$

$$\therefore 2a \in L$$

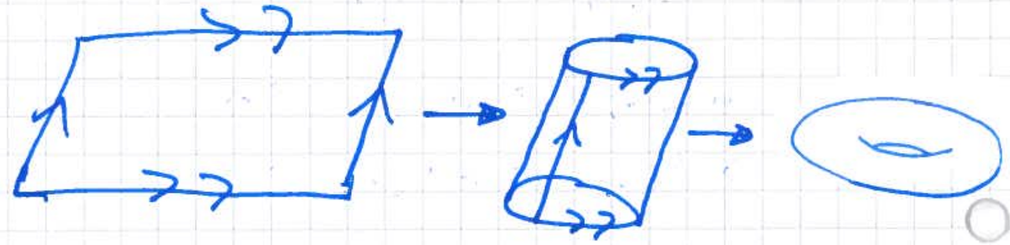
$$\therefore a \equiv -a \ (L)$$

$$\therefore a \equiv b \ (L) \quad \square$$

$\mathbb{C}/L$ looks like this



$\Rightarrow$ since



$\mathbb{C}/L$ and $C_L(\mathbb{C})$ are both groups
($\mathbb{C}/L$ is a group, where the operation is + of complex numbers).

<u>Theorem</u>

$\Phi : \mathbb{C}/L \longrightarrow C_L(\mathbb{C})$ is a group isomorphism.

<u>Lemma</u>

Let G, H be groups and $\varphi : G \to H$. Then φ is a group homomorphism iff

$\varphi(1_g) = 1_H$ and if $g_1 g_2 g_3 = 1_g$, then

$$\varphi(g_1)\varphi(g_2)\varphi(g_3) = 1_H$$

Proof: $(\Rightarrow)$ trivial

$(\Leftarrow)$ assume $\varphi: G \to H$ satisfies the two conditions:

$\therefore gg^{-1}1_G = 1_G$

$\Rightarrow$ by 2^{nd} condition: $\varphi(g)\varphi(g^{-1})\varphi(1_g) = 1_H$

by 1^{st} condition: $\varphi(g)\varphi(g^{-1}) = 1_H$

$\therefore \varphi(g)^{-1} = \varphi(g^{-1})$.

let $g, h \in G$

$gh(gh)^{-1} = 1_G$

By 2^{nd} condition: $\varphi(g)\varphi(h)\varphi((gh)^{-1}) = 1_H$

By what we've already shown,

$\varphi((gh)^{-1}) = \varphi(gh)^{-1}$

$\therefore \varphi(g)\varphi(h)\varphi(gh)^{-1} = 1_H$

$\therefore \varphi(g)\varphi(h) = \varphi(gh)$

$\therefore \varphi$ is a group homomorphism $\square$

Proof of Theorem

We have a bijection

$$\Phi : \mathbb{C}/L \longrightarrow C_L(\mathbb{C})$$

we'll use the lemma to show that

$$\Phi^{-1} : C_L(\mathbb{C}) \longrightarrow \mathbb{C}/L \text{ is a group}$$

homomorphism.

We have to check:

- $\Phi^{-1}(\mathcal{O}) = 0$ (this is clearly true because we defined $\Phi(0) = \mathcal{O}$).

- if $P + Q + R = \mathcal{O}$, in $C_L(\mathbb{C})$, then $\Phi^{-1}(P) + \Phi^{-1}(Q) + \Phi^{-1}(R) \in L$

(→ assume for simplicity that none of P, Q, R are $\mathcal{O}$).

→ since $P + Q + R = \mathcal{O}$, there is a line M such that $M \cap C_L = \{P, Q, R\}$

let M is $ax + by + c = 0$.

since $P, Q, R \neq \mathcal{O}$, $b \neq 0$.

Let $f(z) = a\wp(z) + b\wp'(z) + c$.

f has only a triple pole, so it has 3 zeros
they are obviously

$$\Phi^{-1}(P), \Phi^{-1}(Q), \Phi^{-1}(R)$$

use : $\sum_1^{} z_i - \sum_1^{} p_i \in L$

$$\Phi^{-1}(P) + \Phi^{-1}(Q) + \Phi^{-1}(R) - 0 - 0 - 0 \in L.$$

$$\therefore \Phi^{-1}(P) + \Phi^{-1}(Q) + \Phi^{-1}(R) \in L \quad \square$$

<u>we won't prove this:</u>

If C is any elliptic curve of the form

$$y^2 = 4x^3 - Ax - B,$$

then $\exists$ a lattice L such that $g_2(L) = A$

$$g_3(L) = B.$$

In particular for any

$C/\mathbb{C}$, $C(\mathbb{C}) \cong \mathbb{R}^2/\mathbb{Z}^2$

since $\mathbb{C}/L \cong \mathbb{R}^2/\mathbb{Z}^2$

26. 02. 2014.

Elliptic Curves

4 Rational Torsion Points

<u>Def.</u>: Let A be an abelian group. $n \in \mathbb{N}$. An n-torsion element in A is an element $x \in A$ such that $\underbrace{x + \ldots + x}_{n} = 0$ i.e. $nx = 0$ in A.

<u>Notation</u>: $A[n]$ is the set of n-torsion elements. Since A is abelian $A[n]$ is a subgroup of A.

$A^{tors} \doteq \cup A[n]$ (the set of all torsion element. This is also a subgroup of A).

Recall that if C is an elliptic curve over $\mathbb{C}$, then $$C(\mathbb{C}) \cong \mathbb{R}^2/\mathbb{Z}^2$$

$$\therefore \; C(\mathbb{C})[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n$$

$$\left\{ \left(\frac{i}{n}, \frac{j}{n} \right) : i, j = 0, \ldots, n-1 \right\}$$

$$\therefore \; C(\mathbb{C})^{tors} \cong \mathbb{Q}^2/\mathbb{Z}^2$$

Now suppose C is in Weierstrass form $y^2 = f(x)$

$f(x) = x^3 + ax^2 + bx + c$ has no repeated roots.

<u>Lemma</u>:

A point $(x,y) \in C$ is a 2-torsion point iff $y = 0$.

<u>Proof</u>: (Recall: $-(x,y) = (x,-y)$)

Obviously $2(x,y) = 0 \Leftrightarrow (x,y) = -(x,y)$

$\Leftrightarrow y = 0$

$\square$

<u>Lemma</u>

$p \in C$ is a 3-torsion point iff p is a point of inflection.

<u>Proof</u>: (Recall: $-(x,y) = (x,-y) = \mathcal{O} * (x,y)$)

$$
\begin{aligned}
3p = \mathcal{O} &\Leftrightarrow p + p = -p \\
&\Leftrightarrow p * p = \mathcal{O} * (-p) = p \\
&\Leftrightarrow C \cap T_p C = \{P, P, P\} \\
&\Leftrightarrow p \text{ is a point of inflection}
\end{aligned}
$$

$\square$

The discriminant and the Nagel-Lutz Theorem

Let $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ be a cubic polynomial. The discriminant of f is

$$\Delta(f) = \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{vmatrix}^2$$

$$\Delta(f) = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$$

Proof:

$$\begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{vmatrix} = \begin{vmatrix} 1 & \alpha & \alpha^2 \\ 0 & \beta-\alpha & \beta^2-\alpha^2 \\ 0 & \gamma-\alpha & \gamma^2-\alpha^2 \end{vmatrix} = \begin{vmatrix} \beta-\alpha & \beta^2-\alpha^2 \\ \gamma-\alpha & \gamma^2-\alpha^2 \end{vmatrix}$$

$$= (\beta-\gamma)(\gamma-\alpha)\begin{vmatrix} 1 & \beta+\alpha \\ 1 & \gamma+\alpha \end{vmatrix} = (\beta-\alpha)(\gamma-\alpha)(\gamma-\beta)$$

$\square$

- $\Delta(f) = -f'(\alpha)f'(\beta)f'(\gamma)$

Proof: $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$

$$f'(x) = (x-\beta)(x-\gamma) + (x-\alpha)(x-\gamma) + (x-\alpha)(x-\beta).$$

$\therefore f'(\alpha) = (\alpha - \beta)(\alpha - \mu)$

$$\therefore f'(\alpha) f'(\beta) f'(\mu) = (\alpha-\beta)(\alpha-\mu)(\beta-\alpha)(\beta-\mu)(\mu-\alpha)(\mu-\beta) = -\Delta(f) \quad \square$$

Corollary:

$\Delta(f) = 0 \Leftrightarrow f$ has a repeated root.

Proof:

$\Delta(f) = (\alpha-\beta)^2(\beta-\mu)^2(\mu-\alpha)^2 \quad \square$

Corollary:

Let $g(x) = f(x+c)$. Then $\Delta(g) = \Delta(f)$.

Proof:

the roots of g are $\alpha - c$, $\beta - c$, $\mu - c$.

$$\Delta(g) = \left((\alpha-c)-(\beta-c)\right)^2\left((\beta-c)-(\mu-c)\right)^2\left((\mu-c)-(\alpha-c)\right)^2 = \Delta(f) \quad \square$$

Lemma:

$$\Delta(x^3+ax+b) = -27b^2-4a^3$$

To prove this, start from

$$\Delta = -f'(\alpha) f'(\beta) f'(\mu).$$

This is a symmetric polynomial in α, β, μ so we can write this in terms of $a = \alpha\beta + \beta\mu + \mu\alpha$

$b = -\alpha\beta\mu$

$(\alpha + \beta + \mu = 0)$.

By completing the cube, we get

<u>Lemma</u>

$$\Delta(x^3 + ax^2 + bx + c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

<u>Proof</u>:

Let $f(x) = x^3 + ax^2 + bx + c$.

Define $g(x) = f(x - \frac{a}{3}) = x^3 + a'x + b'$

$$\begin{array}{c} \Delta(g) = \Delta(f) \\ \parallel \\ -27b'^2 - 4a'^3. \end{array}$$

$\square$

<u>Theorem</u> (Nagel - Lutz Theorem)

Let C be an elliptic curve of the form $y^2 = x^3 + ax^2 + bx + c$; $a, b, c \in \mathbb{Z}$.

If $p = (x, y)$ is a torsion point in $C(\mathbb{Q})$

Then (i) $x, y \in \mathbb{Z}$

(ii) either $y = 0$ or $y^2 \mid \Delta(x^3 + ax^2 + bx + c)$

Using the theorem, we can make a finite list of points which might be torsion points.

$\{p_1, \dots, p_N\}$

To find out which are torsion points, calculate a formula for $p * p = -2p$ in terms of p.

For each p in the list calculate the sequence

$p, -2p, 4p, -8p, \dots$

either one point in this sequence is outside the list of possible torsion points.

$$(-2)^a p \notin C(\mathbb{Q})^{tors}$$

$\therefore p \notin C(\mathbb{Q})^{tors}$ (because $C(\mathbb{Q})^{tors}$ is a group

or the sequence contains the same point twice.

i.e. $(-2)^a p = (-2)^b p \quad (a \neq b)$

$\therefore \left((-2)^a - (-2)^b\right) p = 0$, so p is a torsion point.

<u>Example:</u>

$y^2 = x^3 - 1$

$\Delta(x^3 + ax + b) = -27b^2 - 4a^3$

$\Delta(x^3 - 1) = -27$

if (x, y) is a torsion point then $x, y \in \mathbb{Z}$ and $y = 0$ or $y^2 \mid -27$

$\Rightarrow y = 0$ or ± 1 or ± 3.

y	points
0	$(1,0)$
± 1	—
± 3	—
	$\mathcal{O}$

$\Rightarrow$ possible torsion points are $\mathcal{O}$, $(1,0)$
both of these are torsion points.

$y=0$: $x^3-1=0 \Rightarrow x=1$

$y=\pm 1$: $x^3-1=(\pm 1)^2=1$

$\therefore x^3=2$ ↯

$y=\pm 3$: $x^3-1=9$; $x^3=10$ ↯

$C(\mathbb{Q})^{tors}=\{\mathcal{O}, (1,0)\}$, cyclic group of order 2.

28th Feb '14

If A is an abelian group, then
$$A^{tor} = \{a \in A : na = 0 \text{ for some } n > 0\}.$$

Aim: Calculate torsion elements in $C(\mathbb{Q})$
ie
$$C(\mathbb{Q})^{tor}$$

Theorem: (Nagel-Lutz)

Let $C: y^2 = f(x)$. $f(x) = x^3 + ax^2 + bx + c$. $a, b, c \in \mathbb{Z}$
If $(x,y) \in C(\mathbb{Q})^{tor}$ then

- $x, y \in \mathbb{Z}$
- $y = 0$ or $y^2 \mid \Delta(f)$.

Recall: $\Delta(x^3 + ax + b) = -27b^2 - 4a^3$

Method:

1) Make a list of all possible torsion points (always only finitely many).

2) For each point P in this list, calculate the sequence
$P, -2P, 4P, -8P, \ldots$
   - if some $(-2)^n P$ is NOT a possible torsion point, then P is not a torsion point (Torsion points are a subgroup.
   - if $(-2)^n P = (-2)^m P$ $(n \neq m)$ then P is a torsion point

(one of these two things must happen.

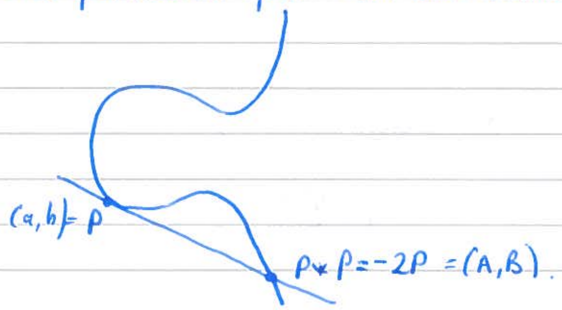
Example: $C: y^2 = x^3 + 1$
$\Delta = -27$.

The largest square dividing 27 is 3^2.
$\Rightarrow$ Either $y = 0$ or $y \mid 3$ at torsion points.

y	Possible torsion pts
0	$(-1, 0)$ $\Rightarrow$ definite torsion point (2-torsion) if $y=0$
± 1	$(0,1), (0,-1)$
± 3	$(2,3)$ $(2,-3)$

& point at ∞, $\mathcal{O}$ 1-torsion (identity)

Find a formula for $-2P$ in terms of P.



$$y^2 = f(x)$$

$$\lambda = \frac{f'(a)}{2b}.$$

$$T_p C : y = \lambda x + \nu$$

in our case $\lambda = \dfrac{3a^2}{2b}$

On $T_p C \cap C$, $(\lambda x + \nu)^2 = x^3 + 1$.

$$x^3 - \lambda^2 x^2 + \ldots\ldots = 0.$$

NOTE: Sum of roots $= \lambda^2$

$$2a + A = \lambda^2$$

We can then obtain a formula for (A,B) in terms of (a,b).

$$A = \frac{9a^4}{4b^2} - 2a = \frac{9a^4}{4(a^3+1)} - 2a. = \frac{a^4 - 8a}{4(a^3+1)}$$

(We really only care about the x-coordinates).

If $x = 0 \Rightarrow A = \dfrac{0^4 - 8 \cdot 0}{4 \cdot 0^3 + 1}$ $\therefore$ $(0,1)$ & $(0,-1)$ are torsion points

$x = 2 \Rightarrow A = \dfrac{2^4 - 8 \times 2}{4(2^3+1)} = 0$ $\therefore$ $(2,3), (-2,3)$ are torsion points

In this case, all of these possible torsion points are torsion

$C(\mathbb{Q})^{tor}$ has 6 elements, is abelian (since must be by defn)
& so $C(\mathbb{Q})$ is an abelian group.

Exercise: $(2,3)$, $(-2,3)$ are both generators

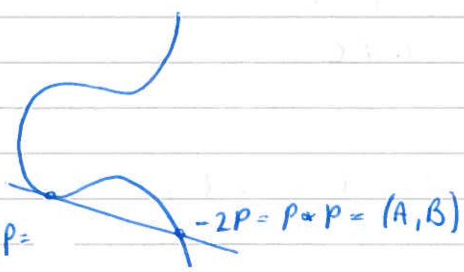
Example: $y^2 = x^3 + 8$

$$\Delta = -27 \times 8^2 = -(3 \times 8)^2$$

& so largest square dividing Δ is 24.

y	Possible torsion points
0	$(-2,0)$ — ✓
± 1	—
± 2	$(2,4)$, $(2,-4)$ ✗
± 4	—
± 8	$(1,3)$, $(1,-3)$
± 3	—
± 6	—
± 12	—
± 24	—
	O ✓

$24^2 = 576$
$x^3 = 568$
568 → 71, 8
71 not a cube & so 568 not.



$T_pC : y = \lambda x + \nu$.

$$\lambda = \frac{f'(a)}{2b} = \frac{3a^2}{2b}$$

$T_pC \cap C$: $\quad = x^3 + 8$

$$x^3 - \lambda^2 x^2 + \dots = 0$$

$$2a + A = \lambda^2 = \frac{9a^4}{4b^2} \Rightarrow A = \frac{9a^4}{4(a^3+8)} - 2a = \frac{a^4 - 64a}{4(a^3+8)}$$

Substituting the x coordinates.

$$x = 2 \longrightarrow \frac{2^4 - 64 \times 2}{4(2^3+8)} = \frac{16-128}{64} = \frac{1}{4} - 2$$

Not even an integer & so is not x coord of a point in our list

$\therefore$ $(2,4)$, $(2,-4)$ are not torsion points.

$x=1 \longrightarrow \dfrac{1^4 - 64\cdot 1}{4(1^3+8)} = \dfrac{-63}{3} \notin \mathbb{Z}$.

& so $(1,3)$, $(1,-3)$ are not torsion points

So we have $C(\mathbb{Q})^{tor} \cong C_2$ with generator $(-2,0)$
($id = \mathcal{O}$).

We can then deduce $C(\mathbb{Q})$ is infinite
($(2,\pm 4)$, $(1,\pm 3)$ have infinite order).

finitely many integer solutions, but infinitely many rational solutions

(Prime number Theory) Notation (for the proof of the Nagel-Lutz theorem).

Let p be a prime. For $n \in \mathbb{Z}$, we'll write

$$V_p(n) = \begin{cases} \max\{a : p^a \mid n\} & n \neq 0 \\ \infty & n = 0 \end{cases}$$

We can extend this to the rational numbers by

$$V_p\left(\tfrac{n}{m}\right) = V_p(n) - V_p(m).$$

This is called the valuation of n/m at p

Define the ring:

$$\mathbb{Z}_{(p)} = \{ x \in \mathbb{Q} : V_p(x) \geq 0 \}$$
$$= \{ \tfrac{n}{m} \text{ st } p \nmid m \}$$

which is clearly a ring (closed under $+, -, \times$)
It is the set of rational numbers which can be reduced mod p^a for all a.

Suppose now we have an elliptic curve

$$C : y^2 = x^3 + ax^2 + bx + c.$$
$$a, b, c \in \mathbb{Z}.$$

If $V_p(y) = -n$ for some $n > 0$, then

$V_p(y^2) = -2n$

$\Rightarrow V_p(x^3 + ax^2 + bx + c) = -2n.$

If $V_p(x) = -r$ $(r > 0)$ then $V_p(x^3 + ax^2 + bx + c) = -3r$

$$-2n = -3r$$

$\Rightarrow n = 3a, \ r = 2a$ for some $a > 0.$

We've shown:

Lemma: If $(x,y) \in C(\mathbb{Q})$, $V_p(x) < 0 \Leftrightarrow V_p(y) < 0$ & if this is the case

$$V_p(x) = -2a \quad V_p(y) = -3a.$$
for some $a \in \mathbb{Z}$

Notation: $C(p^n) = \left\{ (x,y) \in C(\mathbb{Q}) : \begin{array}{l} V_p(y) \leq -3n \\ V_p(x) \leq -2n \end{array} \right\} \cup \mathcal{O}$

We'll change to the (x,z)-plane, in order to write the conditions on $C(p^n)$ as congruences.

In (x,y)-coordinates

$$y^2 = x^3 + ax^2 + bx + c$$

In (x,z)-coordinates

$$(y^2 \underset{?}{\rightarrow} y^2 z \rightarrow z) \ : \ z = x^3 + ax^2 z + bxz^2 + cz^3$$

$\mathcal{O} = (0,0)$ in the (x,z)-plane. Points at ∞ in the (x,z)-plane are 2-torsions (since $y = 0$).

In the (x,z) plane, $-(x,z) = (-x,-z)$

Proof: $-(x,z) = -(x:1:z)$ (divide by z) $-\left(\frac{x}{z} : \frac{1}{z} : 1\right)$

$$= \left(\frac{x}{z} : -\frac{1}{z} : 1\right)$$

$$= (-x : 1 : -z) = (-x,-z)$$

$\square$

Lemma: In (x,z)-coordinates

$$C(p^n) = \{(x,z) \in C(\mathbb{Q}) : V_p(x) = m, \; V_p(z) = 3m \text{ for some } m \geq n\}.$$

Proof: Let $\underset{\text{xz plane}}{(x;1:z)} = \underset{\text{xy plane}}{(r:s:1)}$

$$\therefore \left(\frac{x}{z} : \frac{1}{z} : 1\right) = (r : s : 1)$$

$r = \dfrac{x}{z}$ $\quad s = \dfrac{1}{z}$. If $(x,z) \in C(p^n)$.

$$V_p(r) = -2a \quad V_p(s) = -3a. \qquad a \in \mathbb{Z} \;\; a \geq n.$$

$$V_p(x) - V_p(z) = -2(a) \quad (= V_p(r)).$$

$$V_p(z) = -V_p(s) = 3a$$

$$V_p(x) = -2a + 3a = a \qquad \square.$$

Lemma: Let $P, Q \in C(p^n)$.
Let L be the line through P & Q. (or $T_P C$ if $P = Q$).
$L = z = \lambda x + \mu$.

Then $V_p(\lambda) \geq 2n \qquad \lambda \equiv 0 \mod p^{2n}$
$V_p(\mu) \geq 3n \qquad \mu \equiv 0 \mod p^{3n}$

Proof: For simplicity, we assume $P \neq Q$.

Let $P = (x_1, z_1)$ $\quad Q = (x_2, z_2)$.

$$\lambda = \frac{z_2 - z_1}{x_2 - x_1} \quad \& \quad \begin{aligned} z_1 &= x_1^3 + a x_1^2 z_1 + b x_1 z_1^2 + c z_1^3 \\ z_2 &= x_2^3 + a x_2^2 z_2 + b x_2 z_2^2 + c z_2^3 \end{aligned}$$

$$\begin{aligned} z_2 - z_1 &= x^3 - x^3 + a(x_2^2 z_2 - x_1^2 z_1) + b(x_2 z_2^2 + x_1 z_1^2) + c(z_2^3 - z_1^3) \\ &= (x_2 - x_1)(x_2^2 + x_1 x_2 + x_1^2) + a(x_2^2(z_2 - z_1) + (x_2^2 - x_1^2) z_1) \\ &\quad + b(x_2(z_2^2 - z_1^2) + (x_2 - x_1) z_1^2) + c(z_2 - z_1)(z_2^2 + z_1 z_2 + z_1^2) \end{aligned}$$

Simplify to regroup (& divide by $x_2 - x_1$)

Move all the terms of multiple of $x_2 - x_1$ to one side.

$$= (x_2 - x_1)\left(x_2^2 + x_1 x_2 + x_1^2\right) + a z_1 (x_2 + x_1) + b z_1^2)$$
$$+ \ (z_2 - z_1)(a x_2^2 + b x_2 (z_2 + z_1) + c(z_2^2 + z_1 z_2 + z_1^2)).$$

$$(z_2 - z_1)\underbrace{(1 - a x_2^2 + b x_2 (z_2 + z_1) + c(z_2^2 + z_1 z_2 + z_1^2))}_{A}$$
$$= (x_2 - x_1)\underbrace{(x_2^2 + x_1 x_2 + x_1^2 + a z_1 (x_2 + x_1) + b z_1^2)}_{B}.$$

$V_p(A) = 0$ $(1 - kp^{6n}$ or something...$)$.

$V_p(B) \geq 2n.$

$$V_p(\lambda) \geq 2n - 0 = 2n.$$

$\Rightarrow \lambda \equiv 0 \mod p^{2n}.$

$z_i = \lambda x_i + \nu$
$\nu = z_i - \lambda x_i \equiv 0 \ (p^n).$

$V_p(\nu) \geq 3n$

Proposition: Each $C(p^n)$ is a subgroup of $C(\mathbb{Q})$ & is torsion free (no torsion elements except for the identity.

If we assume this for the moment, then if (x, y) is a torsion point then $(x,y) \notin C(p)$.

$\Rightarrow V_p(x), V_p(y) \geq 0.$

If this is true $\forall p$ (prime) $\Rightarrow x, y \in \mathbb{Z}$. This proves the first half of the Nagel-Lutz theorem.

Proof. Let $P = (x_1, z_1)$
$Q = (x_2, z_2)$
$P + Q = (x_3, z_3).$
so $P * Q = (-x_3, -z_3).$

Assume $P, Q \in C(p^n)$. we need to show $P + Q \in C(p^n)$.

Let L be the line through $P, Q, P * Q$

$L =: z = \lambda x + \nu$, by the lemma $\lambda = 0 \mod p^{2n}$
$\nu = 0 \mod p^{3n}$

$(x_1, x_2 \equiv 0 \mod p^n \quad z_1, z_2 \equiv 0 \mod p^{3n}$

we want to consider $C \cap L$.

$$\lambda x + \nu = x^3 + a x^2(\lambda x + \nu) + b x(\lambda x+\nu)^2 + c(\lambda x + \nu)^3$$

Collecting all the terms.

$$x^3(1 + a\lambda + b\lambda^2 + c\lambda^3) + x^2(a\nu + b2\lambda\nu + c3\lambda^2\nu) + O(\ldots) = 0$$

Sum of roots. $= \dfrac{-(a\nu + 2\lambda\nu b + 3\lambda^2 c\nu)]①}{(1 + a\lambda + b\lambda^2 + c\lambda^3)\quad]②}$ $\left(\dfrac{-B}{A}\right)$ $y = ax^3 + bx^2 \ldots$

$= x_1 + x_2 - x_3$.

$V_p(1 + a\lambda + b\lambda^2 + c\lambda^3) = 0$ (since $V_p(\lambda) = 2n$).

$V_p(x_1 + x_2 \quad x_3) = V_p(①) \geq 3n$

$* \; x_3 \equiv x_1 + x_2 \mod p^{3n}$.

Since $p^n | x_1$ $p^n | x_2$ It follows that $p_n | x_3 \equiv x_1 + x_2$

$\therefore P + Q \in C(p^n)$

$\Rightarrow C(p^n)$ is a group & so a subgroup of $C(\mathbb{Q})$.

05/03/2014

Elliptic

<u>N.L. Theorem</u> if $(x,y) \in C(\mathbb{Q})^{tors}$, then

- $x, y \in \mathbb{Z}$
- either $y=0$ or $y^2 \mid \Delta$

Let p be a prime number.
idea show that $x, y \in \mathbb{Z}(p)$ if this holds for all p then $x, y \in \mathbb{Z}$.

$$C(p^n) = \{(x,y) \in C(\mathbb{Q}) : v_p(x) \leq -2n, \ v_p(y) < -3n\}$$

<u>idea</u>: Show that each $C(p^n)$ is a torsion-free subgroup

in (x,z)-coordinates

$$C(p^n) = \{(x,z) \in C(\mathbb{Q}) : v_p(x) \geq n, \ v_p(z) \geq 3n\}$$

i.e. $x \equiv 0 \ (p^n)$
$z \equiv 0 \ (p^{3n})$

<u>Lemma</u>:
if $P, Q \in C(p^n)$, L is the line through P, Q, then $L: z = \lambda x + \mu$

$\lambda \equiv 0 \ (p^{2n})$, $\mu \equiv 0 \ (p^{3n})$

We started proving that $C(p^n)$ is a torsion-free subgroup.

Let $P, Q \in C(p^n)$

$$P = (x_1, z_1)$$
$$Q = (x_2, z_2)$$

$$P+Q = (x_3, z_3)$$

$$P * Q = (-x_3, -z_3)$$

$$x_1 + x_2 - x_3 \equiv 0 \ (p^{3n}) \qquad (*)$$

In particular:

$$\underbrace{x_1 + x_2}_{\equiv 0 (p^n)} - x_3 \equiv 0 \ (p^n)$$

$$\therefore \ x_3 \equiv 0 (p^n) \ \therefore \ P+Q \in C(p^n)$$

$\therefore$ $C(p^n)$ is a subgroup of $C(\mathbb{Q})$

Assume P is a torsion point of order m, i.e. $mP = \mathcal{O}$ but $lP \neq \mathcal{O}$ if $0 < l < m$.

Let $P = (x_1, z_1)$

Let $p \in C(p^n) \setminus C(p^{n+1})$

i.e. $x_1 \equiv 0 \ (p^n)$

$x_1 \not\equiv 0 \ (p^{n+1})$

Case 1:

Assume $p \nmid m$. By the congruence (*)

$$m x_1 \equiv 0 \quad (p^{3n})$$

Since $p \nmid m$, m is invertible mod p^{3n} so

$$x_1 \equiv 0 \quad (p^{3n})$$ ↯ contradiction since $x_1 \not\equiv 0 \ (p^{n+1})$

Case 2: $p \mid m$, $m = pl$, for some l. ∴

Let $Q = lP$.

The Q has order exactly p.

Assume $Q \in C(p^n) \setminus C(p^{n+1})$, i.e. if $Q = (x_2, z_2)$ then $x_2 \equiv 0 \ (p^n)$ but $x_2 \not\equiv 0 \ (p^{n+1})$.

By (*) $p x_2 \equiv 0 \ (p^{3n})$

∴ $x_2 \equiv 0 \ (p^{3n-1})$

i.e. $Q \in C(p^{3n-1})$ ↯ contradiction.

∴ $C(p^n)$ is torsion-free in particular $C(p)$ is torsion-free. □

Reduction modulo a prime

Let $C: \quad y^2 = x^3 + ax^2 + bx + c$

$a, b, c \in \mathbb{Z}$, be an elliptic curve, i.e. $\Delta \neq 0$.

Let p be an odd prime such that $p \nmid \Delta$
So, the polynomial $x^3 + ax^2 + bx + c \mod p$ has non-zero Δ as a polynomial in $\mathbb{F}_p[x]$.

$\therefore$ this polynomial has no repeated roots in any field containing $\mathbb{F}_p$.

$\therefore$ the equation $y^2 \equiv x^3 + ax^2 + bx + c \ (p)$ defines an elliptic curve $\overline{C}$ over the field $\mathbb{F}_p$.

If we have a point $(X : Y : Z) \in \mathbb{P}^2(\mathbb{Q})$ this gives a point

$$\Phi(X : Y : Z) \in \mathbb{P}^2(\mathbb{F}_p)$$

let $n = \min \{ v_p(X), v_p(Y), v_p(Z) \}$

then we define

$$\Phi(X : Y : Z) = \left(\frac{X}{p^n} \bmod p : \frac{Y}{p^n} \bmod p : \frac{Z}{p^n} \bmod p \right) \in \mathbb{P}^2(\mathbb{F}_p)$$

example:

$p = 3$

$\Phi\left(\frac{1}{3} : 10 : 9\right) = (1 : 30 : 27) \underset{\text{mod}p}{=} (1 : 0 : 0)$

$\Phi(3, 27, 30) = (1 : 0 : 1)$

Remark:

if $p \in C(\mathbb{Q})$, then $\Phi(p) \in \overline{C}(\mathbb{F}_p)$

(if we have a solution to a polynomial equation, then it is a solution to a congruence)

Proposition:

$\Phi : C(\mathbb{Q}) \longrightarrow \overline{C}(\mathbb{F}_p)$ is a group homomorphism.
Its kernel is $C(p)$.

Proof:

to show that Φ is a homomorphism, we need to check

① $\Phi(\Theta) = \Theta$

② if $P + Q + R = \Theta$ in $C(\mathbb{Q})$

then $\Phi(P) + \Phi(Q) + \Phi(R) = 0$ in $\overline{C}(\mathbb{F}_p)$.

since $P + Q + R = 0$ there is a line $L : aX + bY + cZ = 0$ such that $L \cap C = \{P, Q, R\}$.

w.l.o.g. $a, b, c \in \mathbb{Z}$ and are coprime

$$\therefore \quad \overline{L} : aX + bY + cZ \equiv 0 \ (p)$$

is a line in $\mathbb{P}^2(\mathbb{F}_p)$.

but $\Phi(P), \Phi(Q), \Phi(R) \in \overline{L}$

$$\therefore \quad \Phi(P) + \Phi(Q) + \Phi(R) = \mathcal{O} \text{ in } \overline{C}(\mathbb{F}_p).$$

If $P = (x, z)$ in x, z-coordinates

i.e. $P = (x : 1 : z)$

$$P \in C(p) \iff x \equiv z \equiv 0 \ (p)$$
$$\iff \Phi(P) = (0 : 1 : 0)$$
$$\iff P \in \operatorname{Ker}(\Phi) \quad \square$$

<u>Corollary</u>
The restriction of Φ to $C(\mathbb{Q})^{tors}$ is an injective homomorphism $\Phi : C(\mathbb{Q})^{tors} \longrightarrow \overline{C}(\mathbb{F}_p)$

i.e. $C(\mathbb{Q})^{tors}$ is isomorphic to a subgroup of $\overline{C}(\mathbb{F}_p)$.

Proof:

$$\operatorname{Ker}\{\Phi : C(\mathbb{Q})^{tors} \to \overline{C}(\mathbb{F}_p)\}$$

$$= \{P \in C(\mathbb{Q})^{tors} : P \in C(p)\} = \{\mathcal{O}\}$$

since $C(p)$ is torsion-free $\square$

Example:

Calculate $C(\mathbb{Q})^{tors}$ for $y^2 = x^3 + 5x + 5$

$$\Delta = -5^2 \cdot 47$$

$\Rightarrow$ take $p = 3$

$$y^2 \equiv x^3 + 2x + 2 \quad (3)$$

x	x^3+2x+2
0	2
1	2
2	2

$\Rightarrow$ but 2 is not a square mod 3

$\therefore \overline{C}(\mathbb{F}_3) = \{\mathcal{O}\}$

$\therefore C(\mathbb{Q})^{tors} = \{\mathcal{O}\}$.

$C(p)$ is torsion free.

If $(x,y) \in C(\mathbb{Q})^{tors}$, then $x,y \in \mathbb{Z}$.

Let p be a prime such that $p \nmid 2\Delta$

$\therefore \quad \overline{C} : y^2 \equiv x^3 + ax^2 + bx + c \quad (p)$, then

$\overline{C}$ is an elliptic curve over $\mathbb{F}_p$.

There is a homomorphism

$$\Phi : C(\mathbb{Q}) \longrightarrow \overline{C}(\mathbb{F}_p)$$

$$\mathrm{Ker}(\Phi) = C(p)$$

$$\Phi : C(\mathbb{Q})^{tors} \longrightarrow \overline{C}(\mathbb{F}_p) \text{ is injective.}$$

$$\therefore \quad C(\mathbb{Q})^{tors} \cong \text{subgroup of } \overline{C}(\mathbb{F}_p)$$

Example: $\quad C: y^2 = x^3 + x.$

$$\Delta(x^3 + ax + b) = -27b^2 - 4a^3 \Rightarrow \Delta = -4$$

We can reduce C modulo all $p > 2$.

Take $p = 3$

x	$x^3 + x$	points
0	0	$(0,0)$
1	2	—
2	1	$(2,1), (2,-1)$ order 4
		$\mathcal{O}$

$\overline{C}(\mathbb{F}_3) \cong C_4 = \mathbb{Z}/4$

take: $p = 5$

x	$x^3 + x$ (5)	point
0	0	$(0,0)$
1	2	—
2	0	$(2,0)$
3	0	$(3,0)$
4	3	—
		$\mathcal{O}$

$$\overline{C}(\mathbb{F}_5) \cong \mathbb{Z}/2 \times \mathbb{Z}/2 .$$

$\therefore$ $C(\mathbb{Q})^{tors}$ is a subgroup of both $\mathbb{Z}/4$ and $\mathbb{Z}/2 \times \mathbb{Z}/2$ so it is either $\{\mathcal{O}\}$ or $\mathbb{Z}/2$.

But $(0,0) \in C(\mathbb{Q})$ and this is a 2-torsion point so $C(\mathbb{Q})^{tors} = \{\mathcal{O}, (0,0)\} \cong \mathbb{Z}/2$.

$\Rightarrow$ End of proof of Nagel - Luta Theorem

Remark: It's obvious that if $(x,y) \in C(\mathbb{Q})^{tors}$ then unless $y = 0$, then the only primes which divide y are factors of 2Δ.

Proof: Let $y \neq 0$. Choose a prime $p | y$, $p \nmid 2\Delta$.
The reduction map $\Phi : C(\mathbb{Q})^{tors} \longrightarrow C(\mathbb{F}_p)$ is injective.

$$(x, y) \longmapsto (x \bmod p, 0)$$

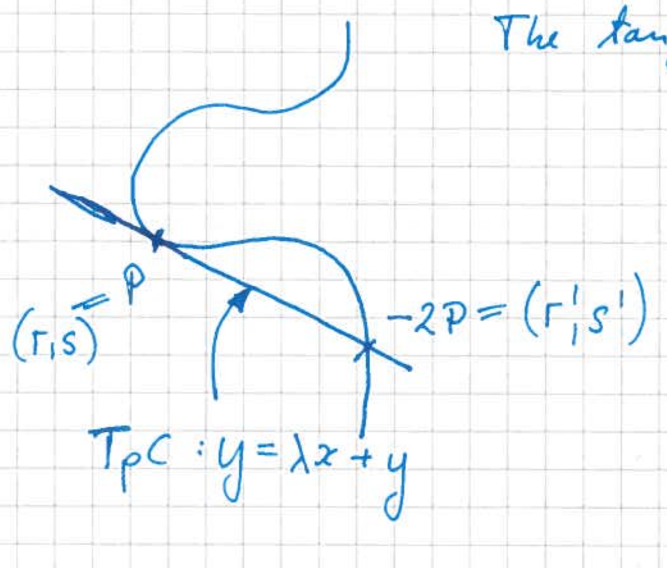
$\therefore$ $\Phi(x,y)$ is 2-torsion
$\therefore$ (x,y) is 2-torsion
$\therefore$ $y = 0$ ↯ contradiction.

Proposition:
Let $C : y^2 = x^3 + ax^2 + bx + c$; $a, b, c \in \mathbb{Z}$.

$P = (r, s)$, $-2P = (r', s')$.
if $r, s, r', s' \in \mathbb{Z}$, then $s^2 | \Delta$.

(this finishes the proof of Nagel–Lutz Theorem).

Proof Of Proposition:



The tangent line at P is $y = \lambda x + \mu$

$$\lambda = \frac{f'(r)}{2s}$$

On $C \cap T_pC$ we have $(\lambda x + \mu)^2 = x^3 + ax^2 + bx + c$

$$x^3 + (a - \lambda^2)x^2 + \dots = 0$$

The roots of this are r, r, r'.

$$\Rightarrow \quad 2r + 2r' = \lambda^2 - a$$

where $r, r', a \in \mathbb{Z}$, $\lambda \in \mathbb{Q}$

$$\lambda^2 \in \mathbb{Z}$$

$$\therefore \lambda \in \mathbb{Z}.$$

$$\Rightarrow \boxed{\begin{aligned} f'(r) &\equiv 0 \quad (2s) \\ f(r) &\equiv 0 \quad (s^2) \end{aligned}}$$

$\Rightarrow$ want: $\Delta(f) \equiv 0 \ (s^2)$

Proof now follows from:

<u>Lemma:</u>

Let f be a cubic monic polynomial over $\mathbb{Z}$, and $r, s \in \mathbb{Z}$ such that

$$f(r) \equiv 0 \quad (s^2)$$

$$f'(r) \equiv 0 \quad (2s)$$

Then $\Delta(f) \equiv 0 \quad (s^2)$.

Proof of Lemma

Let $g(x) = f(x+r)$

$\Delta(g) = \Delta(f)$ and $g(0) \equiv 0 \ (s^2)$

$$g'(0) \equiv \ (2s)$$

$$g(x) = h(x) \qquad (s^2),$$

where $h(x) = x^3 + ax^2 + 2sx \cdot b$

but then $\Delta(h) \equiv \Delta(g) \quad (s^2)$

so sufficient to prove $\Delta(h) \equiv 0 \ (s^2)$

$$h(x) = x\underbrace{(x^2 + ax + 2sb)}_{(x-\alpha)(x-\beta)} \qquad \begin{aligned} \alpha + \beta &= -a \\ \alpha\beta &= 2sb \end{aligned}$$

$$\Delta(h) = \begin{vmatrix} 1 & 1 & 1 \\ 0 & \alpha & \beta \\ 0 & \alpha^2 & \beta^2 \end{vmatrix}^2 = \begin{vmatrix} \alpha & \beta \\ \alpha^2 & \beta^2 \end{vmatrix}^2 = \left(\alpha\beta \begin{vmatrix} 1 & 1 \\ \alpha & \beta \end{vmatrix}\right)^2$$

$$= 4s^2 \ b^2(\beta - \alpha)^2 =$$

$$= 4s^2b^2 \quad \left((\alpha+\beta)^2 - 4\alpha\beta\right) =$$

$$= 4s^2b^2\left(a^2 - 8sb\right) \equiv 0 \quad (s^2) \qquad \square$$

5 Mordell's Theorem

Mordell's Theorem

Let C be an elliptic curve over $\mathbb{Q}$. Then $C(\mathbb{Q})$ is a finitely generated abelian group, i.e. there is a finite set $\{P_1, \dots, P_N\} \subseteq C(\mathbb{Q})$ such that every element in $C(\mathbb{Q})$ is of the form

$$\sum_{i=1}^{N} a_i P_i \quad , a_i \in \mathbb{Z}.$$

$\Rightarrow$ We'll only prove this in the case $C(\mathbb{Q})$ has at least one 2-torsion point $(r,0)$.

$y^2 = f(x) \ \therefore \ f(r) = 0.$

We can replace f by $g(x) = f(x+r)$ to get an isomorphic curve, so w.l.o.g. $C: y^2 = x^3 + ax^2 + bx$.
(if we know algebraic number theory then there is no loss of generality in this version of the proof).

$\Rightarrow$ Every finitely generated abelian group is of the form

$A = \mathbb{Z}^r \times A^{tors}$ (A^{tors} is finite).

$$\therefore \ A/_{2A} \cong (\mathbb{Z}/_2)^r \times \frac{A^{tors}}{2A^{tors}}.$$

$\therefore \ A/_{2A}$ is a finite group.

Mordell's Theorem $\Rightarrow$ <u>Weak Mordell Theorem:</u> $C(\mathbb{Q})/_{2C(\mathbb{Q})}$ is finite.

We'll first prove the Weak Mordell Theorem and then use that to prove Mordell's Theorem.

<u>Aim:</u> Prove that $C(\mathbb{Q})/_{2C(\mathbb{Q})}$ is finite.

<u>Assume</u> $C: y^2 = x^3 + ax^2 + bx \quad (a, b \in \mathbb{Z})$

Let $T = (0,0)$ a 2-torsion point.

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[rr, "\times 2"] & & C(\mathbb{Q}) \\
P \arrow[rr, mapsto] \arrow[dr, "\varphi"] & & 2 \cdot P \\
& \bar{C}(\mathbb{Q}) \arrow[ur, "\psi"] &
\end{tikzcd}$$

rather than looking directly at the map $P \mapsto 2P$, we'll factorise this into map

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\varphi"] \arrow[rr, bend right, "\times 2"'] & \bar{C}(\mathbb{Q}) \arrow[r, "\psi"] & C(\mathbb{Q})
\end{tikzcd}$$

Given $C: y^2 = x^3 + ax^2 + bx$

let $\overline{C}: y^2 = x^3 + \overline{a}x^2 + \overline{b}x$, where

$$\overline{a} = -2a$$
$$\overline{b} = a^2 - 4b$$

$\overline{C}$ is called the "isogenous curve".

<u>Remark:</u>

$$\overline{\overline{a}} = -2\overline{a} = 4a$$

$$\overline{\overline{b}} = \overline{a}^2 - 4\overline{b} = 4a^2 - 4(a^2 - 4b) = 16b.$$

$$\Rightarrow \overline{\overline{C}}: y^2 = x^3 + 4ax^2 + 16bx$$

so $\overline{\overline{C}}$ is isomorphic to C by the map

$$(x, y) \longmapsto \left(\frac{x}{4}, \frac{y}{8}\right)$$

The map $\varphi: C \longrightarrow \overline{C}$ is defined by $\varphi(x,y) = (\overline{x}, \overline{y})$

where $\overline{x} = \dfrac{y^2}{x^2}$ & $\overline{y} = \dfrac{y(x^2 - b)}{x^2}$ $\quad x \neq 0.$

We still need to define $\varphi(\mathcal{O})$ and $\varphi(T)$ (where $x = 0$).

We'll extend the definition by continuity.

First define $\varphi(T)$, if $(x,y) \in C$, $x \neq 0$, then

$$y^2 = x^3 + ax^2 + bx = x\underbrace{(x^2 + ax + b)}_{\frac{1}{u(x)}}, \quad u(0) = \frac{1}{b} \neq 0.$$

for (x,y) near T, we have $\quad (x = y^2 u)$

$$\varphi(x,y) = \left(\frac{y^2}{y^4u^2}, \frac{y(y^4u^2-b)}{y^4u^2} \right)$$

$$= \left(y : y^4u^2 - b : y^3u^3 \right)$$

$$\xrightarrow[(x,y) \longmapsto T]{} (0 : -b : 0) = \mathcal{O}$$

$\Rightarrow \varphi(T) = \mathcal{O}$.

Next work out $\varphi(\mathcal{O})$; $\mathcal{O}$ is in the (x,z)-plane.

$$z = x^3 + ax^2z + bxz^2$$

$$z\underbrace{(1 - ax^2 - bxz)}_{v(x,z)} = x^3$$

$$v(0,0) = 1.$$

$$z = \frac{x^3}{v}$$

$$\varphi(x : 1 : z) = \varphi\left(\frac{x}{z}, \frac{1}{z}\right) = \left(\frac{\left(\frac{1}{z}\right)^2}{\left(\frac{x}{z}\right)^2}, \frac{\frac{1}{z}\left(\left(\frac{x}{z}\right)^2 - b\right)}{\left(\frac{x}{z}\right)^2} \right)$$

$$= \left(\frac{1}{x^2} , \frac{x^2 - b\,z^2}{x^2 z} \right)$$

$$= \left(\frac{1}{x^2} , \frac{x^2 - b\frac{x^6}{v^2}}{\frac{x^5}{v}} \right)$$

$$= \left(\frac{1}{x^2} , \frac{1 - \frac{b x^4}{v^2}}{\frac{x^3}{v}} \right)$$

$$= \left(\frac{1}{x^2} , \frac{v^2 - b x^4}{v x^3} \right)$$

$$= \left(vx : v^2 - bx^4 : vx^3 \right)$$

$$\xrightarrow[(x,z) \to (0,0)]{} (0 : 1 : 0) = \mathcal{O}$$

$\Rightarrow$ so $\varphi(\mathcal{O}) = \mathcal{O}$.

There is a similar map

$$\overline{\varphi} : \overline{C} \longrightarrow \overline{\overline{C}}$$

composing with the isomorphism $\overline{\overline{C}} \to C$

we get a map $\quad \hat{\varphi} : \overline{C} \longrightarrow C$

$$(\overline{x}, \overline{y}) \longmapsto \left(\frac{\overline{y}^2}{4\overline{x}^2} , \frac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2} \right)$$

$$\mathcal{O}, T \longmapsto \mathcal{O}.$$

Lemma:

(i) if $P \in C$ then $\varphi(P) \in \overline{C}$.

(& if $P \in \overline{C}$ then $\psi(P) \in C$)

ii) φ, ψ are group homomorphisms.

iii) for $P \in C$,

$$\psi(\varphi(P)) = 2P.$$

Proof:

(i)

Let $P(x,y)$. w.l.o.g assume $x \neq 0$.

$$\bar{x} = \frac{y^2}{x^2}, \quad \bar{y} = \frac{y(x^2-b)}{x^2} \qquad \Big| \quad \bar{a} = -2a$$

$$y^2 = x^3 + ax^2 + bx \qquad \Big| \quad \bar{b} = a^2 - 4b.$$

Want to use these formulas to prove.

$$\bar{y}^2 = \bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x}$$

$$\bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x} = \frac{y^6}{x^6} - 2a\frac{y^4}{x^4} + (a^2-4b)\frac{y^2}{x^2}$$

$$= \frac{y^2}{x^2}\left(\left(\frac{y}{x}\right)^4 - 2a\left(\frac{y}{x}\right)^2 + a^2 - 4b\right)$$

$$= \frac{y^2}{x^2}\left[\left(\frac{y^2}{x^2} - a\right)^2 - 4b\right]$$

$$= \frac{y^2}{x^6}\left(\left(y^2 - ax^2\right)^2 - 4bx^4\right)$$

$$= \frac{y^2}{x^6}\left(\underbrace{(x^3+bx)^2}_{\text{from curve}} - 4bx^4 \right)$$

$$\therefore \bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x} = \frac{y^2}{x^6}\left((x^3+bx)^2 - 4bx^4 \right)$$

$$= \frac{y^2}{x^4}\left(x^4 + 2bx^2 + b^2 - 4bx^2 \right)$$

$$= \frac{y^2}{x^4}\left((x^2-b)^2 \right)$$

$$= \bar{y}^2 \quad \square$$

12.03.2014

Elliptic

Recall: Mordell's Theorem: $C(\mathbb{Q})$ is a finitely generated abelian group.

Assume $C(\mathbb{Q})$ has at least 1 2-torsion point.
W.l.o.g this is the point $T=(0,0)$ so.

$$C: y^2 = x^3 + ax^2 + bx.$$

Weak Mordell Theorem

$C(\mathbb{Q}) / 2C(\mathbb{Q})$ is a finite group.

$$C(\mathbb{Q}) \xrightarrow{\varphi} \overline{C}(\mathbb{Q}) \xrightarrow{\psi} C(\mathbb{Q})$$

$$\psi(\varphi(P)) = 2P.$$

We'll actually prove $\overline{C}(\mathbb{Q}) / \varphi(C(\mathbb{Q}))$

and $C(\mathbb{Q}) / \psi(\overline{C}(\mathbb{Q}))$ are finite.

$$\overline{C}: y^2 = x^3 + \overline{a}x^2 + \overline{b}x \qquad \overline{a} = -2a \qquad \overline{b} = a^2 - 4b$$

$$\varphi(x,y) = (\overline{x},\overline{y}) \qquad \overline{x} = \frac{y^2}{x^2} \qquad \overline{y} = \frac{y(x^2-b)}{x^2}$$

Lemma:

① $\varphi : C \to \overline{C}$

$\psi : \overline{C} \to C$

② φ, ψ are group homomorphisms

$Ker(\varphi) = \{ \mathcal{O}, T \}$

$Ker(\psi) = \{ \mathcal{O}, T \}$

③ $\psi(\varphi(P)) = 2P$

$\varphi(\psi(P)) = 2P$.

Proof:

① We need to show that

$\varphi(\mathcal{O}) = \mathcal{O}$ (by way defined φ)

and in $P + Q + R = \mathcal{O}$ in C

then $\varphi(P) + \varphi(Q) + \varphi(R) = \mathcal{O}$ in $\overline{C}$.

Suppose $P + Q + R = \mathcal{O}$ in C

$\therefore \exists$ line L such that $L \cap C = \{P, Q, R\}$

Sufficient to prove, there is a line $\bar{L}$ such that

$$\bar{L} \cap \bar{C} = \{\varphi(P), \varphi(Q), \varphi(R)\}$$

Assume L is not vertical, (otherwise $\{P, Q, R\} = \{P, -P, \mathcal{O}\}$

& we just have to show

$$\varphi(-P) = -\varphi(P).$$

$L: \; y = \lambda x + \mu.$

define $\bar{L} : y = \bar{\lambda} \bar{x} + \bar{\mu}$

$$\bar{\lambda} = \frac{\mu\lambda - b}{\mu}, \quad \bar{\mu} = \frac{\mu^2 - a\mu\lambda + b\lambda^2}{\mu}$$

Suppose $P = (x, y) \in L \cap C$

$$\varphi(P) = (\bar{x}, \bar{y})$$

We want $\varphi(p) \in \bar{L} \cap \bar{C}$,

i.e. want $\bar{y} = \bar{\lambda}\bar{x} + \bar{\mu}$

$$\bar{\lambda}\bar{x} + \bar{\mu} = \frac{\mu\lambda - b}{\mu} \frac{y^2}{x^2} + \frac{\mu^2 - a\mu\lambda + b\lambda^2}{\mu}$$

$$= \frac{1}{\mu x^2}\Big((\mu\lambda - b)y^2 + \mu^2 x^2 - a\mu\lambda x^2 + b\lambda^2 x^2\Big).$$

$$= \frac{1}{\mu x^2}\Big(\mu\lambda\underbrace{(y^2 - ax^2)}_{x^3+bx} + b\underbrace{(\lambda^2 x^2 - y^2)}_{=(\lambda x + y)\underbrace{(\lambda x - y)}_{=-\mu}} + \mu^2 x^2\Big)$$

$$= \frac{1}{\mu x^2}\left(\mu\lambda(x^3+bx) - b\mu(\lambda x + y) + \mu^2 x^2\right)$$

$$= \frac{1}{x^2}\left(\lambda x^3 + b\lambda x - b\lambda x - by + yx^2\right)$$

$$\therefore \lambda\bar{x} + \bar{\mu} = \frac{1}{x^2}\underbrace{\left(\lambda x^3 - by + \mu x^2\right)}_{x^2\underbrace{(\lambda x + \mu)}_{=y} - by}$$

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

$\Rightarrow \varphi(\mathcal{O}) = \varphi(T) = \mathcal{O}$

if x, y is any other point (i.e. $x \neq 0$), then

$$\varphi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) \neq \mathcal{O}$$

$\therefore \operatorname{Ker}(\varphi) = \{\mathcal{O}, T\}$.

(3) want $\varphi(\psi(P)) = 2P$.

We actually just need to know

$\varphi(\psi(P)) = 2P$ or $-2P$

i.e. $\varphi(\psi(P))$, $2P$ have the same x-coordinate.

Let $P = (x_0, y_0) \in C$.

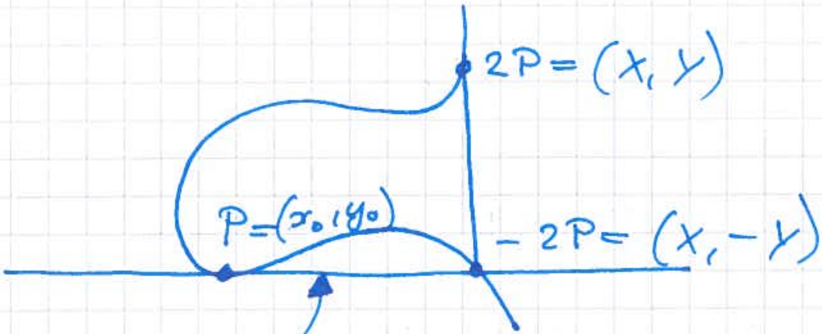
We'll calculate $\psi(\varphi(P))$.

$$\psi(\varphi(P)) = \psi\left(\frac{y_0^2}{x_0^2}, \frac{y_0(x_0^2-b)}{x_0^2}\right)$$

$$= \left(\frac{\left(\frac{y_0(x_0^2-b)}{x_0^2}\right)^2}{4\left(\frac{y_0^2}{x_0^2}\right)^2}, ?\right)$$

$$= \left(\frac{y_0^2(x_0^2-b)^2}{4y_0^4}, ?\right)$$

$$= \left(\frac{(x_0^2-b)^2}{4y_0^2}, ?\right).$$



$T_pC:\ y = \lambda x + \mu$

$$\lambda = \frac{f'(x_0)}{2y_0}$$

<u>On $T_pC \cap C$:</u>

$$(\lambda x + \mu)^2 = x^3 + ax^2 + bx$$

$$\therefore\ x^3 + (a - \lambda^2)x^2 + \dots = 0$$

→ roots are x_0, x_0, X

$$\therefore\ 2x_0 + X = \lambda^2 - a$$

$$\begin{aligned}
X &= \lambda^2 - a - 2x_0 \\
&= \left(\frac{f'(x_0)}{2y_0}\right)^2 - a - 2x_0 \\
&= \left(\frac{3x_0^2 + 2ax_0 + b}{2y_0}\right)^2 - a - 2x_0. \\
&= \frac{1}{4y_0^2}\Big(9x_0^4 + 12ax_0^3 + (6b + 4a^2)x_0^2 + 4abx_0 + b^2 \\
&\qquad - 4\underbrace{(a + 2x_0)(x_0^3 + ax_0^2 + bx_0)}_{= 2x_0^4 + 3ax_0^3 + (a^2 + 2b)x_0^2 + abx_0}\Big).
\end{aligned}$$

$$X = \frac{1}{4y_0^2}\Big(9x_0^4 + \cancel{12a\,x_0^3} + (6b+\cancel{4a^2})x_0^2 + \cancel{4ab\,x_0} + b^2$$
$$- 8x_0^4 - \cancel{12a\,x_0^3} - (\cancel{4a^2}+8b)x_0^2 - \cancel{4ab\,x_0}\Big)$$

$$= \frac{1}{4y_0^2}\left(x_0^4 - 2b\,x_0^2 + b^2\right)$$

$$= \frac{1}{4y_0^2}\left(x_0^2 - b\right)^2$$

This is the x-coordinate of $\psi(\varphi(p))$ $\square$

<u>Plan</u>: We'll show that $\overline{C}(\mathbb{Q}) \big/ \varphi(C(\mathbb{Q}))$

$C(\mathbb{Q}) \big/ \psi(\overline{C}(\mathbb{Q}))$ are both finite

$\Rightarrow$ $C(\mathbb{Q}) \big/ 2C(\mathbb{Q})$ is finite

To do this we'll define a map

$$\alpha : C(\mathbb{Q}) \big/ \psi(\overline{C}(\mathbb{Q})) \longrightarrow \mathbb{Q}^* \big/ \mathbb{Q}^{*2}$$

$$\overline{\alpha}: \frac{\overline{C}(\mathbb{Q})}{\varphi(C(\mathbb{Q}))} \longrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$$

$$\alpha(x,y) = \begin{cases} x & , (x,y) \neq T \\ b & , (x,y) = T \end{cases}$$

$$\alpha(\mathcal{O}) = 1$$

These are injective homomorphisms.

$\mathrm{Im}(\alpha) \subseteq \{ d \in \mathbb{Z} \mid d \mid b \}$
This is finite.

So $\frac{C(\mathbb{Q})}{\psi(\overline{C}(\mathbb{Q}))}$ is finite.

Elliptic

14.03.2014

$C: \ y^2 = x^3 + ax^2 + bx$

$\bar{C}: \ y^2 = x^3 + \bar{a}x^2 + \bar{b}x$

$\bar{a} = -2a$

$\bar{b} = a^2 - 2b$

$\varphi: C \longrightarrow \bar{C} \ ; \ \psi: \bar{C} \longrightarrow C$

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

$$\psi(\bar{x},\bar{y}) = \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{\bar{x}^2} \right)$$

φ, ψ are homomorphisms $\quad T = (0,0)$

$\varphi(T), \psi(T) = \mathcal{O}$

$\varphi(\mathcal{O}), \psi(\mathcal{O}) = \mathcal{O}$

$\mathrm{Ker} = \{\mathcal{O}, T\} \ ; \ \varphi(\psi(P)) = 2P.$

$\psi(\varphi(P)) = 2P.$

<u>Define</u>: $\quad \alpha: C(\mathbb{Q}) \longrightarrow \mathbb{Q}^* / \mathbb{Q}^{*2}$

$$\mathbb{Q}^{*2} = \{ x^2 : x \in \mathbb{Q}^* \}$$

(elements of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ can be thought of as square-free, non-zero integers

$$\mathbb{Q}^* \ni x = \pm \prod p_i^{n_i} \underset{\text{in } \mathbb{Q}^*/\mathbb{Q}^{*2}}{=} \pm \prod p_i^{(n_i \bmod 2)}$$

$$\alpha(x,y) = \begin{cases} x & \text{if } x \neq 0 \\ b & \text{if } x = 0 \end{cases}$$

$$\alpha(\mathcal{O}) = 1$$

<u>Proposition</u>

α is a homomorphism.

<u>Proof</u>: want: $\alpha(\mathcal{O}) = 1$ ✓ by def.
and if $P + Q + R = \mathcal{O}$ then

$$\alpha(P)\alpha(Q)\alpha(R) = 1 \quad \text{in } \mathbb{Q}^*/\mathbb{Q}^{*2}$$

Suppose $P + Q + R = \mathcal{O}$. Assume $P, Q, R \neq \mathcal{O}, T$

Let L be the line such that $L \cap C = \{P, Q, R\}$

$L: y = \lambda x + \mu$

Let $P, Q, R = (x_i, y_i)$, $i = 1, 2, 3$.

We want to show that $\alpha(P)\alpha(Q)\alpha(R) = 1$ in $\frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$

i.e. $x_1 x_2 x_3$ is a square.

$\cancel{y_i = \lambda x_i + \mu_i}$

On $L \cap C$, we have

$$(\lambda x+\mu)^2 = x^3+ax^2+bx$$

$$x^3 + \ldots - \mu^2 = 0$$

The roots are x_1, x_2, x_3.

$\therefore \; x_1 x_2 x_3 = \mu^2$. $\square$

<u>Proof:</u> $\operatorname{Ker}(\bar{\alpha}) = \varphi(\bar{C}(\mathbb{Q}))$

<u>Remark:</u> We also define $\bar{\alpha} : \bar{C}(\mathbb{Q}) \to \mathbb{Q}^* / \mathbb{Q}^{*2}$

$$(\bar{x}, \bar{y}) \longmapsto \bar{x}$$
$$(0,0) \longmapsto \bar{b}$$
$$\mathcal{O} \longmapsto 1$$

This is also a homomorphism &

$\operatorname{Ker}(\bar{\alpha}) = \varphi(C(\mathbb{Q}))$ (by the same proof)

<u>Proof:</u> $\varphi(C(\mathbb{Q})) \subseteq \operatorname{Ker}(\bar{\alpha})$

Let $p = (x, y) \in C(\mathbb{Q})$

$$\varphi(p) = \left(\frac{y^2}{x^2}, - \right)$$

$\bar{\alpha}(\varphi(p)) = \frac{y^2}{x^2} = 1$ in $\mathbb{Q}^* / \mathbb{Q}^{*2}$,

i.e. $\varphi(p) \in \operatorname{Ker}(\bar{\alpha})$.

(note the cases $P = T, O$ are trivial).

$\Rightarrow$ <u>now</u>: $\quad \mathrm{Ker}(\bar\alpha) \subseteq \varphi(C(\mathbb{Q}))$

Let $(\bar x, \bar y) \in \mathrm{Ker}(\bar\alpha)$.

for the moment assume $(\bar x, \bar y) \neq T$, so $x \neq 0$.

$\bar\alpha(\bar x, \bar y) = \bar x$, so $\bar x = w^2 \quad (w \in \mathbb{Q}^*)$.

We'll write down a preimage of $(\bar x, \bar y)$ in $C(\mathbb{Q})$

Let $x_1 = \frac{1}{2}\left(w^2 - a - \frac{\bar y}{w}\right) \quad , y_1 = x_1 w$

$x_2 = \frac{1}{2}\left(w^2 - a - \frac{\bar y}{w}\right) \quad , y_2 = -x_2 w$

<u>Claim</u>: let $p_i = (x_i, y_i)$, then

$p_i \in C(\mathbb{Q})$ and

$\varphi(p_i) = (\bar x, \bar y)$

$$x_1 x_2 = \frac{1}{4}\left((w^2 - a)^2 - \frac{\bar y^2}{w^2}\right)$$

$$= \frac{1}{4}\left((\bar x - a)^2 - \frac{\bar y^2}{\bar x}\right) = \frac{1}{4\bar x}\left(\bar x^3 \underbrace{- 2a}_{=\bar a} \bar x^2 + \underbrace{a^2}_{\bar b + 4b} \bar x - \bar y^2\right)$$

$$\Rightarrow x_1 x_2 = \frac{1}{4\bar x}\left(\cancel{\bar x^3 + \bar a x^2 + \bar b \bar x} + 4b\bar x \cancel{- \bar y^2}\right)$$

$$= \frac{1}{4\bar x}(4b\bar x) = b.$$

$x_1 + x_2 = w^2 - a$

So the x_i's are solutions of $x_i^2 + (a - w^2)x_i + b = 0$

$\therefore \; x_i^3 + a x_i^2 + b x_i = w^2 x_i^2 = y_i^2$

so $(x_i, y_i) \in C(\mathbb{Q})$

$$\varphi(x_1, y_1) = \left(\frac{y_1^2}{x_1^2}, -\right) = \left(w^2, -\right)$$
$$= (\bar{x}, -)$$

$\therefore \; \varphi(P_1) = \pm(\bar{x}, \bar{y})$ so $\varphi(\pm P_1) = (\bar{x}, \bar{y})$.

so $(\bar{x}, \bar{y})$ has a preimage

Now suppose $T = (0,0) \in \mathrm{Ker}(\bar{\alpha})$

i.e. $\bar{\alpha}(0,0) = 1$

i.e. b is a square.

$a^2 - 4b$ is a square.

Suppose T is in the image of φ.

$$\varphi(x, y) = (0,0)$$

i.e. $\frac{y^2}{x^2} = 0, \; \frac{y(x^2 - b)}{x^2} = 0$

i.e. $y = 0$

so T is in $\varphi(C(\mathbb{Q}))$ iff $\exists$ a point $(x,0) \in C(\mathbb{Q})$ with $x \neq 0$.

i.e. $x^3 + ax^2 + bx = 0$

$\therefore x^2 + ax + b = 0$

This has rational solutions

$\Leftrightarrow a^2 - 4b \in \mathbb{Q}^{*2}$

$\Leftrightarrow T \in \mathrm{Ker}(\bar{\alpha})$.

$\square$

<u>Weak Mordell</u>

$C(\mathbb{Q}) / 2C(\mathbb{Q})$ is finite

$\Uparrow$ (easy)

$\bar{C}(\mathbb{Q}) / \varphi(C(\mathbb{Q}))$, $C(\mathbb{Q}) / \alpha(\bar{C}(\mathbb{Q}))$

are both finite

$\Uparrow$ (trivial)

$\mathrm{Im}(\bar{\alpha})$, $\mathrm{Im}(\alpha)$ are finite

Proposition

$\operatorname{Im}(\alpha) \subset \{ b_1 \in \mathbb{Z} \mid b_1 | b \}$, b_1 is square free.

(So $|\operatorname{Im}(\alpha)| \leq \left| \begin{matrix} \text{square-free} \\ \text{factors of } b \end{matrix} \right|$

Proof:

Recall that $\alpha(x,y) = x$

want to show that if p is a prime such that $v_p(x)$ is odd then $p | b$. (note $\alpha(T) = b$, which is a factor of b)

Suppose for a moment $(x,y) \in C(\mathbb{Q}_p)$, i.e.

$v_p(x), v_p(y) < 0$ and

$2v_p(y) = 3v_p(x)$

$\therefore v_p(x)$ is even $\lightning$

$\therefore x, y \in \mathbb{Z}_{(p)}$.

let $n = v_p(x)$, so $n \geq 0$, odd.

so $n \geq 1$

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

$\underbrace{2v_p(y)}_{\text{even}} = \underbrace{n}_{\text{odd}} + v_p(x^2 + ax + b)$ $\therefore v_p(x^2 + ax + b)$ is odd.

but $x, a, b \in \mathbb{Z}_{(p)}$ so

$$v_p(x^2 + xa + b) \geq 0$$

$$\therefore \quad v_p(x^2 + ax + b) \geq 1$$

so $p \mid x^2 + ax + b$

and $p \mid x$

$\therefore \; p \mid b$ $\square$

<u>Corollary</u>

$$\frac{\bar{C}(\mathbb{Q})}{\varphi(C(\mathbb{Q}))} \text{ and } \frac{C(\mathbb{Q})}{\psi(\bar{C}(\mathbb{Q}))}$$

are finite.

<u>Proof</u>: by 1st Isomorphism Theorem,

$$\frac{C(\mathbb{Q})}{\psi(\bar{C}(\mathbb{Q}))} = \frac{C(\mathbb{Q})}{\operatorname{Ker}(\alpha)} \cong \operatorname{Im}(\alpha).$$

$\square$

Homomorphisms

Lemma

Let A, B be two abelian groups with maps
$\varphi : A \to B$, $\psi : B \to A$
such that $\psi(\varphi(a)) = 2a$.

Then $\left|\frac{A}{2A}\right| \leq \left|\frac{A}{\psi(B)}\right| \times \left|\frac{B}{\varphi(A)}\right|$

Proof:

Let $\{a_i\}$ be coset reps. for $\frac{A}{\psi(B)}$.
let $\{b_j\}$ be coset representatives for $\frac{B}{\varphi(A)}$

<u>Claim</u>: $\{a_i + \psi(b_j)\}$ represent all the cosets of $A/2A$

Choose $a \in A$.

Want $a = a_i + \psi(b_j) + 2a'$ $(a' \in A)$

First we have

$a = a_i + \psi(b)$ for some $b \in B$.

$b = b_j + \varphi(a')$ $(a' \in A)$

$\therefore$ $a = a_i + \psi(b_j) + \underbrace{\psi(\varphi(a'))}_{= 2a'}$ $\square$

Corollary:

$C(\mathbb{Q})/2C(\mathbb{Q})$ is finite.

The Rank of a Curve

For the moment, we'll assume we'll proved Mordell's Theorem

i.e. $C(\mathbb{Q})$ is finitely generated.

$$\therefore \quad C(\mathbb{Q}) \cong C(\mathbb{Q})^{tors} \oplus \mathbb{Z}^r$$

The number r is called the rank of the curve C.

We'll now try to calculate the rank of a curve.

Obviously,

$$\frac{C(\mathbb{Q})}{2C(\mathbb{Q})} \cong \frac{C(\mathbb{Q})^{tors}}{2C(\mathbb{Q})^{tors}} \oplus \left(\frac{\mathbb{Z}}{2}\right)^r$$

So to calculate r, we need to know

$$\left| \frac{C(\mathbb{Q})}{2C(\mathbb{Q})} \right| \text{ and } \left| \frac{C(\mathbb{Q})^{tors}}{2C(\mathbb{Q})^{tors}} \right|$$

Lemma:

$$\left| \frac{C(\mathbb{Q})^{tors}}{2C(\mathbb{Q})^{tors}} \right| = \begin{cases} 2, \text{ if } a^2-4b \text{ is not a square} \\ 4, \text{ if } a^2-4b \text{ is a square.} \end{cases}$$

Proof:

let $A = C(\mathbb{Q})^{tors}$

$$A \xrightarrow{\times 2} A$$

By 1st Isomorphism theorem,

$$2A \cong A / A[2]$$

$$|A[2]| = \begin{cases} 2 & , a^2-4b \text{ is not a square.} \\ 4 & , a^2-4b \text{ is a square.} \end{cases}$$

$$\left| A/2A \right| = \frac{|A|}{|2A|} \quad ; \quad |2A| = \frac{|A|}{|A[2]|}$$

$$\therefore \left| A/2A \right| = |A[2]|$$

$\square$

Proposition

$$2^r = \frac{|\mathrm{Im}(\alpha)| \, |\mathrm{Im}(\bar{\alpha})|}{4}$$

Proof:

$$\left|\frac{C(\mathbb{Q})}{2C(\mathbb{Q})}\right| = \underbrace{\left|\frac{C(\mathbb{Q})}{\psi(\overline{C}(\mathbb{Q}))}\right|}_{=|\mathrm{Im}(\alpha)|} \cdot \left|\frac{\psi(\overline{C}(\mathbb{Q}))}{2C(\mathbb{Q})}\right|$$

so we want to calculate

$$\left|\frac{\psi(\overline{C}(\mathbb{Q}))}{2C(\mathbb{Q})}\right|$$

We have a homomorphism

$$\Psi : \frac{\overline{C}(\mathbb{Q})}{\varphi(C(\mathbb{Q}))} \longrightarrow \frac{\psi(\overline{C}(\mathbb{Q}))}{\psi(\varphi(C(\mathbb{Q})))}$$

$$p + \varphi(C(\mathbb{Q})) \longmapsto \psi(p) + \psi(\varphi(C(\mathbb{Q})))$$

The map Ψ is surjective.

We need to calculate $\ker \Psi$.

If $\Psi(p + \varphi(C(\mathbb{Q}))) = \psi(\varphi(C(\mathbb{Q})))$

then $\vartheta(p) \in \vartheta(\varphi(C(\mathbb{Q})))$.

$\therefore \vartheta(p) = \vartheta(\varphi(q))$, for some $q \in C(\mathbb{Q})$

$\vartheta(p - \varphi(q)) = 0$

so $p - \varphi(q) \in \mathrm{Ker}(\vartheta) = \{\mathcal{O}, T\}$.

so $\mathrm{Ker}(\Psi) = \{\varphi(C(\mathbb{Q})), T + \varphi(C(\mathbb{Q}))\}$

i.e. $|\mathrm{Ker}(\Psi)| = \begin{cases} 1, & \text{if } T \in \varphi(C(\mathbb{Q})), \\ 2, & \text{if } T \notin \varphi(C(\mathbb{Q})). \end{cases}$

$$= \begin{cases} 1, & \text{if } \bar{\alpha}(T) = 1 \\ 2, & \text{if } \bar{\alpha}(T) \neq 1. \end{cases}$$

$$= \begin{cases} 1, & a^2 - 4b \in \mathbb{Q}^{*2} \\ 2, & a^2 - 4b \notin \mathbb{Q}^{*2} \end{cases}$$

So to summarise, we have

$$\left| \frac{\vartheta(\bar{C}(\mathbb{Q}))}{2C(\mathbb{Q})} \right| = \begin{cases} \left| \frac{\bar{C}(\mathbb{Q})}{\varphi(C(\mathbb{Q}))} \right|, & \text{if } \bar{b} \in \mathbb{Q}^{*2} \\ \frac{1}{2} \left| \frac{\bar{C}(\mathbb{Q})}{\varphi(C(\mathbb{Q}))} \right|, & \text{if } \bar{b} \notin \mathbb{Q}^{*2} \end{cases}$$

$$= \begin{cases} |\mathrm{Im}\,\bar{\alpha}|, & \bar{b} \in \mathbb{Q}^{*2} \\ \frac{1}{2}|\mathrm{Im}\,\bar{\alpha}|, & \bar{b} \notin \mathbb{Q}^{*2} \end{cases}$$

$$\therefore \left| \frac{C(\mathbb{Q})}{2C(\mathbb{Q})} \right| = \begin{cases} |\mathrm{Im}\,\alpha|\,|\mathrm{Im}\,\bar{\alpha}|, & \text{if } b \in \mathbb{Q}^{*2} \\ \frac{1}{2}|\mathrm{Im}\,\alpha|\,|\mathrm{Im}\,\bar{\alpha}|, & \text{if } b \in \mathbb{Q}^{*2} \end{cases}$$

but $$\frac{C(\mathbb{Q})}{2C(\mathbb{Q})} = \frac{C(\mathbb{Q})^{tors}}{2C(\mathbb{Q})^{tors}} \oplus \left(\mathbb{Z}/_2\right)^r$$

So $$\left| \frac{C(\mathbb{Q})^{tors}}{2C(\mathbb{Q})^{tors}} \right| \cdot 2^r = \begin{cases} |\mathrm{Im}\,\alpha|\,|\mathrm{Im}\,\bar{\alpha}|, & b \in \mathbb{Q}^{*2} \\ \frac{1}{2}|\mathrm{Im}\,\alpha|\,|\mathrm{Im}\,\bar{\alpha}|, & b \notin \mathbb{Q}^{*2} \end{cases}$$

So using the previous Lemma,

$$2^r = \frac{|\mathrm{Im}(\alpha)|\,|\mathrm{Im}(\bar{\alpha})|}{4}$$

$\square$

Elliptic 19.03.2014

$C: y^2 = x^3 + ax^2 + bx \quad , a, b \in \mathbb{Z}$

$C(\mathbb{Q}) = C(\mathbb{Q})^{tors} \oplus \mathbb{Z}^r$

r is called the rank of C.

$\Rightarrow \quad 2^r = \dfrac{|\operatorname{Im}(\alpha)| \cdot |\operatorname{Im}(\bar{\alpha})|}{4}$, where

$\alpha : C(\mathbb{Q}) \longrightarrow \mathbb{Q}^* / \mathbb{Q}^{*2}$

$\mathcal{O} \longmapsto 1$

$(0,0) = T \longmapsto b$

$(x, y) \longmapsto x$

$\operatorname{Im}(\bar{\alpha}) \subseteq \{ b_1 \in \mathbb{Z} \setminus 0 : b_1$ is square-free and $b_1 | b \}$

Example:

$C: y^2 = x^3 + x \quad ; \quad b = 1.$

$\alpha(\mathcal{O}) = 1$

if $\alpha(x,y) = -1$, then $x < 0$

$\therefore x^3 + x < 0$

$\therefore y^2 < 0$ ⚡

$|\operatorname{Im}(\alpha)| = 1.$

$\overline{C}: x^3 + \overline{a}x^2 + \overline{b}x = y^2 \Rightarrow \overline{C}: y^2 = x^3 - 4x$

$= x(x+2)(x-2)$

$\overline{a} = -2a = 0$

$\overline{b} = a^2 - 4b = -4$

$(0,0), (-2,0), (2,0)$

α

$\downarrow \quad \downarrow \quad \downarrow$

$-1 \quad -2 \quad 2$

b_1	$\mathrm{Im}(\overline{\alpha})$
1	✓
2	✓ $\overline{\alpha}(2,0)$
-1	✓ $\overline{\alpha}(T)$
-2	✓ $\overline{\alpha}(-2,0)$

$$|\mathrm{Im}(\overline{\alpha})| = 4$$

$$\Rightarrow 2^r = \frac{|\mathrm{Im}\,\alpha| \cdot |\mathrm{Im}\,\overline{\alpha}|}{4} = \frac{1 \cdot 4}{4} = 1$$

$\Rightarrow r = 0.$, i.e the rank of C is 0.

<u>Proposition</u>

Let $b = b_1 b_2$, where $b_1, b_2 \in \mathbb{Z}$ and b_1 is square-free.

(1) $b_1 \in \mathrm{Im}(\alpha)$ iff the following equation has a solution $(N, M, e) \in \mathbb{Z}^3$
$\neq (0,0,0)$

$$(*) \quad N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4$$

(2) If there is a solution to (*), then there is a solution such that $hcf(M, e) = 1$ and $hcf(b_1, e) = 1$.

To calculate $\mathrm{Im}(\alpha)$ list all factorizations $b = b_1 b_2$ with b_1 square-free.

For each factorization, write down equation (*). We have to decide whether (*) has solutions. If we find a solution then there are solutions so $b_1 \in \mathrm{Im}(\alpha)$.
If there are no real solutions or no solutions mod R, then there are no solutions.

Proof (of Proposition):
(assume $b_1 \neq b$; note: $\alpha(T) = b$)
and (*) has solutions.

Suppose $\alpha(x, y) = b_1$.

$$x = \frac{m}{e^2} \; ; \; y = \frac{n}{e^3} \; ; \; n, m, e \in \mathbb{Z}$$

$$\alpha(x, y) = b_1 \Rightarrow m = b_1 M^2. \; (M \in \mathbb{Z})$$

$$y^2 = x^3 + ax^2 + bx$$

$$\frac{n^2}{e^6} = \frac{b_1^3 M^6}{e^6} + a \frac{b_1^2 M^4}{e^4} + b \frac{b_1 M^2}{e^2}$$

$$n^2 = b_1^3 M^6 + a b_1^2 M^4 e^2 + b_1^2 b_2 M^2 e^4$$
$$= b_1^2 M^2 \underbrace{\left(b_1 M^4 + a M^2 e^2 + b_2 e^4 \right)}_{\text{RHS of } (*)}$$

$b_1^2 M^2 \mid n^2$

so $b_1 M \mid n$, let $n = b_1 M N$

$\therefore N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4 \quad (*)$

Conversely if (N, M, e) is a solution to $(*)$
if $e = 0$, then $N^2 = b_1 M^4$, so $b_1 = 1 = \alpha(\mathcal{O})$

assume $e \neq 0$

$$\left(\frac{b_1 M^2}{e^2}, \frac{b_1 N M}{e^3} \right) \in C(\mathbb{Q})$$

and $\alpha\left(\frac{b_1 M^2}{e^2}, \frac{b_1 N M}{e} \right) = \frac{b_1 M^2}{e^2} = b_1$ in $\mathbb{Q}^* / \mathbb{Q}^{*2}$

Assume $(N, M, e) \neq (0, 0, 0)$ is a solution
if $p \mid M$ & $p \mid e$.

$$\boxed{N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4}$$

then $p^4 \mid$ RHS of $(*)$

$\therefore p^4 \mid N^2$

so $p^2 \mid N$

but $\left(\frac{N}{p^2}, \frac{M}{p}, \frac{e}{p}\right)$ is a smaller solution.

Suppose (N, M, e) is a solution with $hcf(M, e) = 1$

Suppose $p | b_1$ & $p | e$.

$\therefore$ $p |$ RHS of ⊛

$\therefore$ $p | N^2$

$\therefore$ $p | N$ (p prime).

$\therefore$ $p^2 |$ LHS of ⊛

$$\therefore \quad b_1 M^4 + \underbrace{a M^2 e^2}_{=0} + \underbrace{b_2 e^4}_{=0} \equiv 0 \ (p^2)$$

$$\Rightarrow \quad b_1 M^4 \equiv 0 \ (p^2)$$

Since b_1 is square-free, $p^2 \nmid b_1$ so $p | M^4$ ※ contradiction $hcf(M, e) = 1$

$\therefore$ $p \nmid b_1$ so $hcf(b_1, e) = 1$ $\square$

Example: $y^2 = x^3 + \underbrace{2}_{b}x$

b_1	$\mathrm{Im}(\alpha)$
1	✓ $\alpha(O)$
2	✓ $\alpha(T)$
−1	× $(\mathbb{R})$
−2	× (deduced from group structure).

$N^2 = -M^4 - 2e^4$

no solutions

$\overline{C}: y^2 = x^3 - 8x$

$\overline{a} = -2a = 0$

$\overline{b} = a^2 - 4b = -8$

b_1	$\mathrm{Im}(\overline{\alpha})$
1	✓ $\overline{\alpha}(O)$
2	× (2)
−1	× deduced
−2	✓ $\overline{\alpha}(T)$

$N^2 = 2M^4 - 4e^4$

N is even

e is odd

$2M^4 - 4e^4 \equiv 0 \ (4)$

$M^4 \equiv 0 \ (2)$

M is even.

$N^2 \equiv -4e^4 \ (32)$

$\left(\frac{N}{2}\right)^2 \equiv -e^4 \ (8)$

$e^4 \equiv 1 \ (8)$

$\Rightarrow \left(\frac{N}{2}\right)^2 \equiv -1 \ (8)$. ✗

$\Rightarrow$ -1 is not a square mod 8.

$$\Rightarrow \quad 2^r = \frac{2 \cdot 2}{4} = 1 \quad \Rightarrow \quad \underline{\underline{r = 0}}$$

$$\Rightarrow \quad C(\mathbb{Q}) = C(\mathbb{Q})^{tors} = \{ \mathcal{O}, T \}.$$

21.03.2014

Elliptic

$C(\mathbb{Q}) = C(\mathbb{Q})^{tors} \oplus \mathbb{Z}^r$, r is called the rank of C.

$$2^r = \frac{|\mathrm{Im}(\alpha)| \cdot |\mathrm{Im}(\overline{\alpha})|}{4} \; ; \; \alpha : C(\mathbb{Q}) \to \mathbb{Q}^* / \mathbb{Q}^{*2}$$

$$\overline{\alpha} : \overline{C}(\mathbb{Q}) \to \mathbb{Q}^* / \mathbb{Q}^{*2}$$

$\mathrm{Im}(\alpha) \subseteq \{b_1 \mid b\}$; $C : y^2 = x^3 + ax^2 + bx$.

Proposition

Let $b_1 \mid b$ (square free). Then $b_1 \in \mathrm{Im}(\alpha)$ iff $(*)\; N^2 = b_1 M + aM^2 e^2 + b_2 e^4$ $(b = b_1 b_2)$ has a solution $(N, M, e) \in \mathbb{Z}^3 \setminus (0,0,0)$.

If $(*)$ has a solution, then there is a solution with $\mathrm{hcf}(M, e) = 1$.
$\mathrm{hcf}(e, b_1) = 1$

Remark:

If p is prime & $p \mid b_2$ but $p^2 \nmid b_2$, then $p \nmid M$.

Example:

$C: y^2 = x^3 - 3x$

$b = -3$

b_1	$\mathrm{Im}(\alpha)$	
1	✓	$\alpha(\mathcal{O})$
3	✗	(3)
-1	✗	deduced
-3	✓	$\alpha(T)$

$b_1 = 3$: $N^2 = 3M^4 - e^4$

$b_2 = -1$:

e is invertible mod 3.

$$\frac{N^2}{e^4} \equiv -1 \ (3) \ ✗.$$

$\overline{C}: y^2 = x^3 + 12x$

$\overline{a} = -2a = 0$

$\overline{b} = a^2 - 4b = 12$

b_1	$\mathrm{Im}(\overline{\alpha})$	
1	✓	$\overline{\alpha}(\mathcal{O})$
2	✗	deduced.
3	✓	$\overline{\alpha}(T)$
6	✗	(3)
-1	✗ no real solution	
-2		
-3		
-6		

eg. $b_1 = -1$: $N^2 = -M^4 - 12e^4$

$\underline{b_1 = 6}$

$N^2 = 6M^4 + 2e^4$, e is coprime to 6.
i.e. is invertible mod 3.

$$\frac{N^2}{e^4} \equiv 2 \quad (3) \quad \times$$

$$\Rightarrow \quad 2^r = \frac{2 \cdot 2}{4} = 1 \therefore \text{rank} = 0.$$

$\therefore$ $C(\mathbb{Q})$ has only torsion points

$\Delta = -4 \cdot (-3)^3$

$5 \nmid \Delta$ so we can reduce mod 5.

x mod 5	$x^3 - 3x$	$C(\mathbb{F}_5)$
0	0	$(0,0) = T$
1	3	$\times$
2	2	$\times$
−2	3	$\times$
−1	2	$\times$

$C(\mathbb{F}_5) = \{\mathcal{O}, T\}$

but $C(\mathbb{Q}) = C(\mathbb{Q})^{\text{tors}}$, which is isomorphic to a subgroup of $C(\mathbb{F}_5)$.

$\therefore$ $C(\mathbb{Q}) = \{\mathcal{O}, T\}$.

Example:

$C: y^2 = x^3 + 3x$

$b = 3$

b_1	$\operatorname{Im}(\alpha)$
1	✓ $\alpha(O)$
3	✓ $\alpha(T)$
-1	× (deduced)
-3	× ($\mathbb{R}$)

$b_1 = -3$

$N^2 = -3M^4 - 1 \cdot e^4$

$\overline{C}: y^2 = x^3 - 12x$

b_1	
1	✓ $\bar{\alpha}(O)$
2	× (deduced)
3	× (deduced)
6	✓ $(2,1,1)$
-1	× (deduced)
-2	✓ (deduced)
-3	✓ $\bar{\alpha}(T)$
-6	× (3)

$b_1 = 6$, $N^2 = 6M^4 - 2e^4$

$(2,1,1)$ is a solution

$b_1 = -6$, $N^2 = -6M^4 + 2e^4$

e coprime to 6.

$\therefore$ invertible mod 3.

$\frac{N^2}{e^4} \equiv 2\ (3)$. ×

$$2^r = \frac{2 \cdot 4}{4} = 2 \Rightarrow r = 1 = \text{rank}.$$

Example:

$$y^2 = x^3 - 4x^2 - 14x$$

$b = -14$, $a = -4$

b_1	Im (α)
1	✓ $\alpha(O)$
2	✓ $(3,2,1)$
7	✓
14	✓ $(3,1,1)$
-1	✓ (deduced)
-2	✓
-7	✓
-14	✓ $\alpha(T)$

$b_1 = 14$

$$N^2 = 14M^4 - 4M^2e^2 - e^4$$

$(3,1,1)$ is a solution.

$b_1 = 2$

$$N^2 = 2M^4 - 4M^2e^2 - 7e^4$$

e is coprime to 2.

$e^2 \equiv 1 \ (8)$

N is odd $\quad N^2 \equiv 1 \ (8)$

if M is even, then $2M^4 \equiv 0 \ (8)$

$$4M^2e^2 \equiv 0 \ (8)$$

$$N^2 \equiv -7 \ (8)$$

$\therefore$ $(3, 2, 1)$ is a solution.

$\bar{C}$: $\bar{a} = -2a = 8$

$\bar{b} = \bar{a}^2 - 4b = 16 + 4 \cdot 14 = 72 = 2^3 3^2$

b_1	$\mathrm{Im}(\bar{\kappa})$
1	✓ $\alpha(\Theta)$
2	✓ $\alpha(T)$
3	✗ deduced.
6	✗ (2)
−1	✗
−2	✗ ($\mathbb{R}$
−3	✗
−6	✗ ($\mathbb{R}$)

$b_1 = 6$

$N^2 = 6M^4 + 8M^2e^2 + 12e^4$

$\mathrm{hcf}(6, e) = 1$

$\therefore$ e is odd

$e^2 \equiv 1 \ (8)$

$\boxed{e^4 \equiv 1 \ (16)}$

$\left[(8n+1)^2 = 64n^2 + 16n + 1 \equiv 1 \ (16) \right]$

N is even.

$$0 \equiv 6M^4 \ (4) \quad ; \quad M^4 \equiv 0 \ (2).$$

$\therefore M$ is even.

$$\Rightarrow \quad 6M^4 \equiv 0 \ (32).$$

$$8M^2e^2 \equiv 0 \ (32)$$

$$\therefore \quad N^2 \equiv 12e^4 \quad (32)$$

$$\left(\frac{N}{2}\right)^2 \equiv 3e^4 \ (8)$$

$$\equiv 3 \ (8) \quad \therefore \text{X} \therefore$$

only 1 is an odd square mod 8.

$b_1 = -6$

$$N^2 = -6M^4 + 8M^2e^2 - 12e^4$$

$$= -6\left(M^4 - \frac{8}{6}M^2e^2 + 2e^4\right)$$

$$= -6\left(\underbrace{\left(M^2 - \frac{2}{3}e^2\right)^2}_{\geq 0} + \underbrace{\left(2 - \frac{4}{9}\right)}_{>0} e^4\right)$$

$$\leq 0 \quad \therefore \text{X} \therefore$$

$b_1 = -2$

$$N^2 = -2M^4 + 8M^2e^2 - 36e^4$$

$$= -2\left(M^4 - 4M^2e^2 + 18e^4\right)$$

$$= -2\left(\left(M^2 - 2e^2\right)^2 + 14e^4\right) \leq 0.$$

$$2^{\text{rank}} = \frac{8 \cdot 2}{4} = 4$$

$\Rightarrow$ $\underline{\text{rank} = 2}$

<u>Mordell's Theorem</u>

$C(\mathbb{Q})$ is finitely generated.

<u>Weak Mordell Theorem</u>

$\frac{C(\mathbb{Q})}{2C(\mathbb{Q})}$ is finite

But Weak Mordell $\not\Rightarrow$ Mordell.

eg. $(\mathbb{Q}, +)$ is not finitely generated.

but $2\mathbb{Q} = \mathbb{Q}$, so $\mathbb{Q}/2\mathbb{Q} = 0$, which is finite

To prove Mordell's Theorem we need something else

<u>Heights & Descent</u>

Let $x = \frac{n}{m} \in \mathbb{Q}$, with n, m coprime,

the <u>height of x</u> is $H(x) = \max\{|n|, |m|\}$

eg: $H(-1) = 1$; $H(100) = 100$

$H(0) = 1$; $H\left(\frac{7}{3}\right) = 7$.

For any N, there are only finitely many rational numbers with height $\leq N$!

This allows us to prove facts about $\mathbb{Q}$ by induction on the height. This kind of proof is called proof by descent.

The logarithmic height $h(x)$ is defined by

$$h(x) = \log(H(x)).$$

If $P(x,y) \in C(\mathbb{Q})$, we define $h(P) = h(x)$.
and $h(\mathcal{O}) = 0$.

Lemma 1:

Let $P_0 \in C(\mathbb{Q})$. $\exists\, c_1$ such that $\forall P \in C(\mathbb{Q})$

$$h(P + P_0) \leq 2h(P) + c_1$$

(c_1 depends only on P_0 and C).

Lemma 2

$\exists\, c_2$ s.t. $\forall P \in C(\mathbb{Q}) \quad h(2P) \geq 4h(P) - c_2$

Proof of Mordell's Theorem:

$\frac{C(\mathbb{Q})}{2C(\mathbb{Q})}$ is finite.

Let $Q_1, \dots, Q_r$ be a set of coset reps. for $2C(\mathbb{Q})$ in $C(\mathbb{Q})$.
Since this set is finite, Lemma 1 gives us a constant c_1 such that $\forall P \in C(\mathbb{Q})$

$$h(P+Q_i) \leq 2h(P) + c_1.$$

Let $N \in \mathbb{N}$ and let $R_1, \dots, R_s$ be the points on $C(\mathbb{Q})$ with height $\leq N$.

Claim:
$S = \{Q_1, \dots, Q_r, R_1, \dots, R_s\}$ generates $C(\mathbb{Q})$ when N is big enough.

We'll do this by a descent argument.
Let $P \in C(\mathbb{Q})$

if $h(P) \leq N$, then $P \in S$.

so P is in the subgroup generated by S.

Now assume $h(P) > N$, ~~and~~ and any point with smaller height than P is in the subgroup generated by S.

$P \equiv Q_i \mod 2\,C(\mathbb{Q})$, for some $Q_i \in S$.

i.e. $P = Q_i + 2P'$.

$\cancel{h(P) \leq 2h(2P') + c_1}$
~~(by Lemma 1)~~.

$\cancel{h(2P')} \Rightarrow \quad h(2P') \leq 2h(P) + c_1$

$$h(2P') \geq 4h(P') - c_2$$

$$4h(P') - c_2 \leq 2h(P) + c_1$$

$$\therefore \; h(P') \leq \frac{1}{2}h(P) + c_3$$

$$h(P') - h(P) = c_3 - \frac{1}{2}h(P)$$

$$h(P) > N$$

$\therefore \; h(P') < h(P)$ if $c_3 - \frac{N}{2} < 0$.

The constant c_3 depends only on the curve C_1, so we take $2N > c_3$ and $h(P') < h(P)$

$\therefore$ P' is in the subgroup generated by S.

$P = Q_i + 2P'$ is also in this subgroup.

$\therefore$ S ~~generated~~ generates $C(\mathbb{Q})$

$\therefore$ $C(\mathbb{Q})$ is finitely generated. $\square$

Elliptic 26.03.2014.

$$H\left(\frac{n}{m}\right) = \max(|n|, |m|)$$

$$h(x) = \log H(x)$$

$$h(P = h(x) \quad , \quad P = (x, y)$$

Lemma 1, $\forall P_0 \in C(\mathbb{Q})$, $\exists c_1$ s.t.

$$\forall P \in C(\mathbb{Q}) \quad , \quad h(P + P_0) \leq 2h(P) + c_1$$

Lemma 2

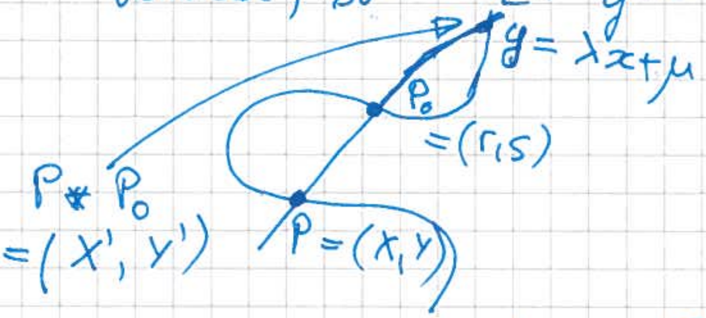
$\exists c_2$ such that

$$h(2P) \geq 4h(P) - c_2$$

Lemma 1:

Proof: Assume $P \neq P_0, -P_0, O$

Let L be the line through P, P_0 then L is not vertical, so $L: y = \lambda x + \mu$.



so $C \cap L: \quad (\lambda x + \mu)^2 = x^3 + ax^2 + bx + c$

$$x^3 + (a - \lambda^2)x^2 + \dots = 0.$$

$$X + X' + r = \lambda^2 - a.$$

$$\lambda = \cancel{\quad} \frac{y-s}{x-r}$$

$$\Rightarrow \quad x + x' + r = \lambda^2 - a$$

$$\Rightarrow \quad x' = \lambda^2 - a - x - r$$

$$= \frac{(y-s)^2 - (a+r)(x-r)^2 - x(x-r)^2}{(x-r)^2}$$

$$= \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

$A, \ldots, G$ are constants $\in \mathbb{Z}$

$$P = (x, y) = \left(\frac{n}{e^2}, \frac{m}{e^3} \right)$$

$$x' = \frac{Ame + Bn^2 + Cne^2 + De^4}{En^2 + Fne^2 + Ge^4}$$

$$|n| \leq H(P)$$

$$|e| \leq H(P)^{1/2}$$

since $(x,y) \in C(\mathbb{Q})$

~~the~~ $m^2 = n^3 + a n^2 e^2 + b n e^4 + c e^6$

$$|n|^3 \le H(P)^3$$
$$|n^2 e^2| \le H(P)^3$$
$$|e^6| \le H(P)^3$$

$m^2 \ll H(P)^3$

(i.e. $\le$ const. $H(P)^3$).

$|m| \ll H(P)^{3/2}$

$\therefore$ $|A\underbrace{me}_{\ll H(P)^2} + B\underbrace{n^2}_{\le H(P)^2} + C\underbrace{ne^2}_{\ll H(P)^2} + D\underbrace{e^4}_{\le H(P)^2}| \ll H(P)^2$

same for denominator

$\therefore$ $\underset{\substack{\| \\ H(P+P_0)}}{H(x')} \ll H(P)^2$

$\therefore$ $h(P+P_0) \le 2h(P) + \text{const.}$ $\square$

Lemma

Let $\varphi, \psi \in \mathbb{Z}[x]$ s.t. φ, ψ are coprime in $\mathbb{Q}[x]$. Let $d = \max(\deg(\varphi), \deg(\psi))$.

Then $\exists\, c$ such that $\operatorname{hcf}\left(n^d \varphi\left(\frac{m}{n}\right), n^d \psi\left(\frac{m}{n}\right)\right)$

$$\leq c$$

for all rationals $\frac{n}{m}$ (n, m coprime)

Proof:

Let $\Phi(n,m) = n^d \varphi\left(\frac{m}{n}\right)$

$\Psi(n,m) = n^d \psi\left(\frac{m}{n}\right)$

$\exists\, h, k \in \mathbb{Q}[x]$ s.t. $h\varphi + k\psi = 1$.

Choose $c' \in \mathbb{Z}$ s.t. ~~...~~ $\bar{h} = c'h$, $\bar{k} = c'k$ $\in \mathbb{Z}[x]$

$\bar{h}\varphi + \bar{k}\psi = c'$

let $H(n,m) = n^D \bar{h}\left(\frac{m}{n}\right)$

$K(n,m) = n^D \bar{k}\left(\frac{m}{n}\right)$

$D = \max(\deg(\bar{h}), \deg(\bar{k}))$

$\therefore H(n,m)\Phi(n,m) + K(n,m) \cdot \Psi(n,m) = c' n^{d+D}$

$$\mathrm{hcf}(\Phi(n,m),\Psi(n,m)) \leq \mathrm{hcf}(\Phi(n,m), c'n^{d+D})$$

(w.l.o.g $\deg(\Phi)=d$.)

$$\leq c'\,\mathrm{hcf}(\Phi(n,m), n^{d+D})$$

$$\leq c'\,\mathrm{hcf}(\Phi(n,m)^{d+D}, n^{d+D})$$

$$\leq c'\,\mathrm{hcf}(\Phi(n,m), n)^{d+D}$$

$$\Phi(n,m) = a_0 m^d + a_1 m^{d-1} n + \dots + a_d n^d$$

$$\mathrm{hcf}(\Phi(n,m), n) = \mathrm{hcf}(a_0 m^d, n)$$

$$\leq \mathrm{hcf}(a_0, n)\,\underbrace{\mathrm{hcd}(m,n)^d}_{=1}$$

$$\leq a_0 .$$

$$\mathrm{hcf}(\Phi(n,m), \Psi(n,m)) \leq c' a_0^{d+D}$$

$\square$

__Lemma:__

Let φ, ψ be as before, then $\exists\, c$ such that

$$h\left(\frac{\varphi(x)}{\psi(x)}\right) \geq d \cdot h(x) - c$$

where $d = \max(\deg(\varphi), \deg(\psi))$.

Proof:

Let $\Phi(n,m) = n^d\varphi\left(\frac{m}{n}\right)$

$\Psi(n,m) = n^d\psi\left(\frac{m}{n}\right)$.

$$\frac{\varphi\left(\frac{m}{m}\right)}{\psi\left(\frac{m}{n}\right)} = \frac{\Phi(n,m)}{\Psi(n,m)}$$

by the previous lemma,

$$H\left(\frac{\varphi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \gg \max\left(|\Phi(n,m)|, |\Psi(n,m)|\right)$$

$$\gg |n^d| \max\left(\left|\varphi\left(\frac{m}{n}\right)\right|, \left|\psi\left(\frac{m}{n}\right)\right|\right)$$

$$\gg |n^d| \left(\left|\varphi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|\right)$$

since φ, ψ have no common zeros

$$|\varphi| + |\psi| \gg 1.$$

since one of φ, ψ has degree d.

$$|\varphi(x)| + |\psi(x)| \gg |x|^d$$

$$|\varphi(x)| + |\psi(x)| \gg \max(1, |x|^d)$$

$$\therefore H\left(\frac{\varphi(\frac{m}{n})}{\psi(\frac{m}{n})}\right) \gg |n^d| \max\left(1, \left|\frac{m}{n}\right|^d\right)$$

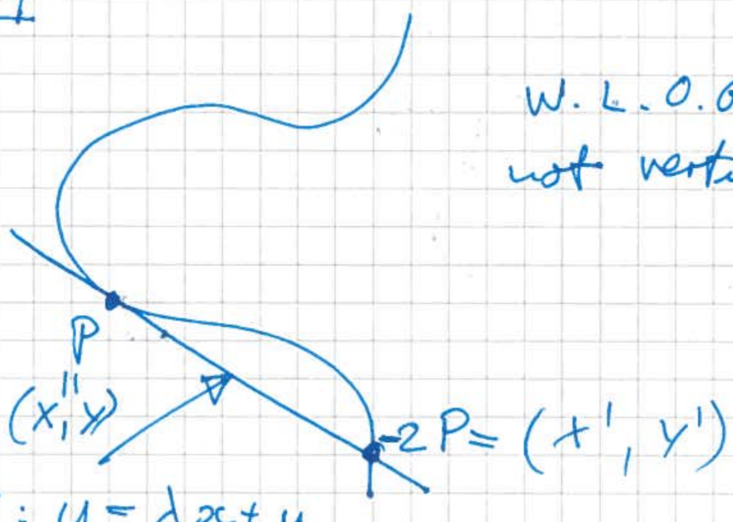
$$\gg \max(|n|, |m|)^d \gg H\left(\frac{m}{n}\right)^d$$

$$h\left(\frac{\varphi(\frac{m}{n})}{\psi(\frac{m}{n})}\right) \geq d\, h\left(\frac{m}{n}\right) - \text{constant}.$$

□

$\Rightarrow$ <u>Lemma 2</u>: $h(2P) \geq 4h(P) - \text{constant}.$

<u>Proof</u>:



W.L.O.G. T_pC is not vertical.

$T_pC: y = \lambda x + \mu$

on $C \cap T_pC$: $(\lambda x + \mu)^2 = x^3 + ax^2 + bx + c$

$$2X + X' = \lambda^2 - a$$

$$= \left(\frac{f'(X)}{2Y}\right)^2 - a$$

$$= \frac{f'(X)^2 - a f(X)}{4 f(X)}$$

denominator has degree 3, ~~num~~ numerator has degree 4.

if h is a common factor of $f(x)$ and of $f'(x)^2 - a\,f(x)$

$\therefore \quad h \mid f, (f')^2.$

any zero of h is a common zero of f, f'.

but f has no repeated roots

$\therefore \quad f$ & f' have no common zero

$\therefore \quad h$ is constant, by previous lemma,

$$\underbrace{h(x')}_{= h(2P)} \geq \underbrace{4h(x)}_{= h(P)} - c$$

$\square$

Open problems in elliptic curves

28th Mar

L-functions

First consider the quadratic equation $x^2 = d$ where $d > 0$, $d \in \mathbb{Z}$ and $d \equiv 1 \bmod (4)$. For any prime p, let:

$$a_p = \# \{ x \in \mathbb{F}_p : x^2 \equiv d \bmod (p) \}$$

On average, a_p is usually 0 or 2, but it is possible that a_p is 1.

Let $\chi(p) = a_p - 1$

Reciprocity law: $\chi(p)$ depends only on $p \bmod d$:

$$\chi : (\mathbb{Z}/d)^\times \longrightarrow \{\pm 1\}$$

is a homeomorphism. The L-function of $x^2 = d$ is:

$$\underset{s \in \mathbb{C}}{L(\chi, s)} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p) p^{-s}}$$

Simple example: If $d = 1$ then $\chi(p) = 1$ $\forall p$. Therefore $L(\chi, s) = \sum n^{-s} = \zeta(s) \leftarrow$ the Riemann-Zeta function.

Theorem: $\zeta(s)$ has a meromorphic continuation to $\mathbb{C}$. It has only a simple pole at $s = 1$.

$$\operatorname{Res}_{s=1} \zeta(s) = 1$$

Theorem: If $d \neq 1$ then $L(\chi, s)$ has an analytic continuation to $\mathbb{C}$. There is a simple formula relating $L(\chi, s)$ to $L(\chi, 1-s)$. This is called the functional equation.

Theorem: $L(\chi, 1) \neq 0$. More precisely, there is a formula for $L(\chi, 1)$.

Let k be $\mathbb{Q}(\sqrt{d})$ - the splitting field of the quadratic equation $x^2 - d$.

There is $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathbb{Q}(\sqrt{d}) = k$. Cl_k is the class group of k, it tells us how far $\mathcal{O}$ is from having unique factorisation.

$$Cl_k = \text{Ideals}/\text{Principal ideals}.$$

Cl_k is finite.

$\mathcal{O}^\times \cong \{\pm 1\} \times \mathbb{Z}$. Let v be a generator $\mathcal{O}^\times/\{\pm 1\}$. If $v = x + y\sqrt{d}$ then $x^2 - dy^2 = \pm 1$.

This v corresponds to the fundamental solution to Pell's equation.

$$\operatorname{Reg}_k = |\log|v||$$

Class number formula is given by:

$$L(1,\chi) = \frac{4|Cl_k|\,Reg_k}{|\mathcal{O}_{k}^{\times}{}_{tors}|\,|\sqrt{d}|}$$

Now let C be an elliptic curve over $\mathbb{Q}$. Let $N_p = \#|C(\mathbb{F}_p)|$
$= 1 + \#$ affine points
$y^2 \equiv f(x) \bmod p$.

If we fix an x, then the number of solutions is:

$$1 + \left(\frac{f(x)}{p}\right)$$

$$N_p = 1 + \sum_{x\in\mathbb{F}_p}\left(\left(\frac{f(x)}{p}\right)+1\right) = p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{f(x)}{p}\right)$$

Let $a_p = p+1-N_p$

Hasse's Theorem $|a_p| < 2\sqrt{p}$. More precisely:

$$\frac{a_p}{2\sqrt{p}} = \cos(\Theta_p) \quad \text{where } 0<\Theta_p<\pi$$

How are these distributed?

The Sato-Tate conjecture Θ_p is distributed like

$$\frac{2}{\pi}\sin^2(\Theta)\,d\Theta$$

The L-function of an elliptic curve The L-function of C is

$$L(C,S) = \prod_p \frac{1}{1-a_p p^{-S}+p^{1-2S}}$$

$$\underbrace{L(C,S+\tfrac{1}{2})}_{L(C,s)} = \prod_p \frac{1}{(1-e^{i\Theta_p}p^{-S})(1-e^{-i\Theta_p}p^{-S})}$$

This converges for $Re(S) > \frac{3}{2}$

Theorem (Wiles, Breuil, Conrad, Diamond, Taylor) $L(C,s)$ has an analytic continuation to $\mathbb{C}$ and a functional equation relating $L(C,S)$ to $L(C,2-S)$.

The Birch-Swinnerton-Dyer Conjecture

This is the next big conjecture in this field... Prove it and get a million pounds!!!

Conjecture $L(C,1)=0$ if and only if $C(\mathbb{Q})$ is infinite, i.e. if $rank(C)>0$.

There is a more precise version of this. Precisely:

$$rank(C) = ord_{s=1}(L(C,S)).$$

To describe the conjectured leading term, we need some definitions. When calculating $rank(C)$ we actually calculate $C(\mathbb{Q})/2C(\mathbb{Q})$. To calculate this, we decide whether certain equations have solutions. Sometimes this is difficult because there are no solutions, but there exists solutions in $\mathbb{R}$ and in $\mathbb{Z}/n$ $\forall N$.

This happens when there is a 2-torsion element in a certain group: Ш.

Similarly, 3-torsion elements in Ш make it difficult to calculate $|C(\mathbb{Q})/3C(\mathbb{Q})|$.

Major conjecture Ш is finite. This is a long way from being proven.

Recall $h(p)$, the height of a curve at point p. It turns out that:

$$\hat{h}(p) = \lim_{n\to\infty}\frac{h(2^n p)}{4^n}$$

(This is called the canonical height – this limit always exists). Then:

$$\hat{h}: C(\mathbb{Q})/C(\mathbb{Q})_{tors} \longrightarrow \mathbb{R}^{>0}$$

is a quadratic form on $\mathbb{Z}^{rank}$. Let $P_1,\dots,P_r$ be the generators of $C(\mathbb{Q})/C(\mathbb{Q})_{tors} \cong \mathbb{Z}^r$. Then:

$$Reg(C) = |\det(B(P_i,P_j))_{i,j=1,\dots,r}|$$

where B is the corresponding bilinear form.

Birch-Swinnerton-Dyer conjecture

$$L(C,S) = \frac{|Ш(C)|\,\Omega_C\,Reg_C}{|C(\mathbb{Q})_{tors}|}\prod_{p|\Delta} c_p\,.\,(S-1)^{rank} + O((S-1)^{rank+1})$$

where c_p's tell you what happens to C when you reduce it mod p. They are numbers!

LAST YEARS EXAM SOLUTIONS

#1)c) $C: y^2 = x^2(x^2+1)$
$L: y = \lambda x$ over $\mathbb{C}$

Calculate $I(C,L,(0,0)) = \dim \mathbb{C}[x,y]_{(0,0)}/(y^2-x^2(x^2+1),\, y-\lambda x)$

$\cancel{= \dim \mathbb{C}[x,y]_{(0,0)}/}$ Eliminate y

$= \dim \mathbb{C}[x]_{(0)}/(\lambda x^2 - x^4 - x^2)$

$= \dim \mathbb{C}[x]_{(0)}/(-x^4-(1-\lambda^2)x^2)$

$$= \begin{cases} 2 & \lambda \neq \pm 1 \\ 4 & \lambda = \pm 1 \quad (\text{as } 1-\lambda^2 = 0)\end{cases}$$

#1) d) For which λ do C and L meet at more than 1 point?

If $\lambda \neq \pm 1$ then there are other points of intersection by Bézout's Theorem.

#1) e) Let P be any of other intersection point. Show that $I(C, L, P) = 1$

$\lambda \neq \pm 1$ as there is another point of intersection.

$$y^2 = x^2(x^2+1)$$
$$y = \lambda x$$

$\Rightarrow \lambda^2 x^2 = x^4 + x^2$
$\Rightarrow x^4 + (1-\lambda^2)x^2 = 0$

Since $P \neq (0,0)$ then $x \neq 0$ (as $y = \lambda x$). So we can divide by x^2.

$\Rightarrow x^2 + (1-\lambda^2) = 0$
$\Rightarrow x = \pm\sqrt{1-\lambda^2}$

There are 2 other points of intersection:

$$(\pm\sqrt{1-\lambda^2}, \pm\lambda\sqrt{1-\lambda^2})$$

call these P_1 and P_2.

Bézout's $\Rightarrow I(C, L, (0,0)) + I(C, L, P_1) + I(C, L, P_2) = 4$
$\therefore I(C, L, P_1) = I(C, L, P_2) = 1$. $\square$

#2) c) Find the Weierstrass normal form of $U^3 + 2V^3 = 1$ given the point $\mathcal{O} = (1, 0)$.

$$F(U, V, W) = U^3 + 2V^3 - W^3$$

$$\frac{\partial F}{\partial U} = 3U^2, \quad \frac{\partial F}{\partial V} = 6V^2, \quad \frac{\partial F}{\partial W} = -3W^2$$

at $\mathcal{O} = (1:0:1)$: $T_{\mathcal{O}}C$: $3U - 3W = 0$, i.e. $U - W = 0$ $(Z = U - W)$.

On the intersection: $C \cap T_{\mathcal{O}}C$: $U^3 + 2V^3 - U^3 = 0$
$\Rightarrow 2V^3 = 0 \Rightarrow V^3 = 0$ and $U = W$.

Therefore $\mathcal{O} = (1:0:1)$ is a point of inflection.

Let $L_1 = T_{\mathcal{O}}C$. Choose L_2 to be any other line through $\mathcal{O}$. Let $L_2 = V = 0$. Let L_3 to be a line not going through $\mathcal{O}$. Let L_3: $U = 0$

$$X = V$$
$$Y = U$$
$$Z = U - W$$

Then $U = Y$, $V = X$, $W = Y - Z$

so $F = U^3 + 2V^3 - W^3$
$= Y^3 + 2X^3 - (Y-Z)^3$
$= Y^3 + 2X^3 - Y^3 + 3Y^2Z - 3YZ^2 + Z^3$
$= 2X^3 + 3Y^2Z - 3YZ^2 + Z^3$

Now change to affine coordinates: $(Z = 1)$

$$2x^3 + 3y^2 - 3y + 1 = 0$$

$$3y^2 - 3y = -2x^3 - 1$$
$$y^2 - y = -\tfrac{2}{3}x^3 - \tfrac{1}{3}$$

complete the square:

$$(y - \tfrac{1}{2})^2 - \tfrac{1}{4} = -\tfrac{2}{3}x^3 - \tfrac{1}{3}$$

Substitute y with $y - \frac{1}{2}$ to get:

$$y^2 = -\tfrac{2}{3}x^2 - \tfrac{1}{12}$$

Multiply x by $-\frac{3}{2}$ and multiply y by $-\frac{3}{2}$. Then:

$$\tfrac{9}{4}y^2 = -\tfrac{9}{4}x^3 - \tfrac{1}{12}$$

$$\Leftrightarrow y^2 = x^3 - \tfrac{1}{27}$$

#4) c) Calculate $C(\mathbb{Q})^{tors}$ where $C: y^2 = x^3 + 4x$ and $\Delta(C) = -28$

Let's reduce mod 3: $y^2 \equiv x^3 + x \bmod (3) \equiv 2x \bmod (3)$ by Fermat's little theorem.

x	x^3+x	$C(\mathbb{F}_3)$
0	0	$(0,0)$ ← order 2
1 } mod 3	2	
2	1	$(2,1)$, $(2,-1)$ ← must be order 4. $\mathcal{O}$

So $C(\mathbb{F}_3) \cong \mathbb{Z}/4$.
– $C(\mathbb{Q})^{tors}$ is a subgroup of $C(\mathbb{F}_3) \cong \mathbb{Z}/4$ so it has 1, 2 or 4.

It must have at least 2: $(0,0) \in C(\mathbb{Q})$, $C(\mathbb{Q})^{tors}$ has either 2 or 4 elements as $(0,0)$ is 2-torsion.

Let's reduce mod 5:

$x \bmod (5)$	$x^3 - x \bmod (5)$	$C(\mathbb{F}_5)$
0	0	$(0,0)$
1	0	$(1,0)$
2	1	$(2,1)$ and $(2,-1)$
3	4	$(3,2)$ and $(3,-2)$
4	0	$(4,0)$
		$\mathcal{O}$

$C(\mathbb{F}_5) \cong \mathbb{Z}/4 \times \mathbb{Z}/4$ or $\mathbb{Z}/2 \times \mathbb{Z}/8$

THIS DOESN'T HELP – Try a different method!

Find a formula for $-2P$ in terms of P.

$T_P C$: $y = \lambda x + \mu$. on $C \cap T_P C$:

$$(\lambda x + \mu)^2 = x^3 + 4x$$
$$\Rightarrow x^3 - \lambda^2 x^2 + (4 - 2\lambda\mu)x = 0$$

$$2X + X' = \lambda^2 = \left(\frac{f'(X)}{2Y}\right)^2 = \frac{(3X^2+4)^2}{4(X^3+4X)}$$

$$\Rightarrow X' = \frac{(3X^2+4)^2}{4(X^3+4X)} - 2X$$

If $(X,Y) \in C(\mathbb{Q})_{tors}$ then $Y = 0$ or $Y^2 \mid -2^8$. Therefore:

Y	X
0	$X^3+4X=0 \Rightarrow X=0$
± 1	$X^3+4X-1=0 \Rightarrow$ no solutions
± 2	$X^3+4X-4=0 \Rightarrow$ no solutions
± 4	$(2,4)$, $(2,-4)$
± 8	no solutions
± 16	no solutions.
	$\odot$

($X^3+4X-4=0$ $\Rightarrow$ roots are factors of 4 … 1, 2, 4 don't work $\Rightarrow$ no solutions)

If $X = 2$ then $X' = \frac{16^2}{4(16)} - 4 = \frac{16}{4} - 4 = 0$

$\Rightarrow$ $(2,4)$ and $(2,-4)$ are torsion points

$\Rightarrow$ $C(\mathbb{Q})_{tors} \cong \mathbb{Z}/4$.

#5) b) Calculate the rank of $C: y^2 = x^3 - 7x$

ANS: rank $= 1$.