ELLIPTIC CURVE CRYPTOGRAPHY

Winter term 2009/10

MICHAEL NÜSKEN

October 27, 2009

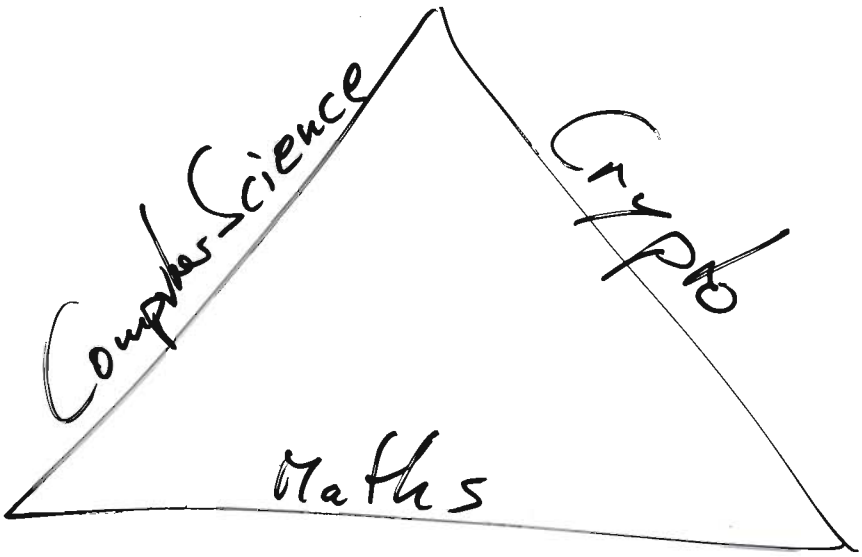
1. Introduction

We consider elliptic curves from three different sides:

- Mathematics view: defines and analyzes their structure and properties.
- Computer science view: asks for efficient implementation of operations and properties.
- Cryptography view: requires some things to be intractable.

It is an interplay between the three areas and we will have to consider them all again and again.

As our main interest is cryptography, let's start here with two examples.



El Gamal type Signatures (x' [redacted] 89)

ecc
27.10.09
7

Global setup

We fix a group G, (finite, commutative, additively written)

an element P of finite order ℓ, ($\ell = \min\{j \in \mathbb{N}_{>0} \mid jP = 0\}$)

a hash function (collision-resistant, & one-way)

$$\text{hash}: \{0,1\}^* \longrightarrow \mathbb{Z}_\ell, \text{ and}$$

a structureless ~~map~~ type cast

$$^*: G \longrightarrow \mathbb{Z}_\ell$$

User setup „Alice"

Choose $\alpha \in_R \mathbb{Z}_\ell$ randomly. ← private key of Alice

Compute $A := \alpha P$. ← public key of Alice

Signature verification:

Input: Public key A, document $m \in \{0,1\}^*$,

signature $\sigma = (B, \gamma)$

Output: Accept or reject.

1. Verify

$$B^* A + \gamma B = \text{hash}(m) \cdot P \text{ in } G.$$

2. Return $\begin{cases} \text{Accept if true} \\ \text{Reject if false.} \end{cases}$

El Gamal ~~signature~~ signing?

Input: private key α,
document $m \in \{0,1\}^*$

Output: $\sigma = (B, \gamma)$ signature.

[Observe $A = \alpha P$
$B = ? \cdot P$

then:...
$$\beta^* A + \gamma B = \text{hash}(m)\, P$$
can be written by multiples of P:...]

1. Choose $\beta \in_R \mathbb{Z}_\ell$,
compute $B := \beta P$ (temporary key pair)

2. Solve for γ:

$$\beta^* \alpha P + \gamma \beta P = \text{hash}(m)\, P \text{ in } G.$$

ie.
$$\beta^* \alpha + \gamma \beta = \text{hash}(m) \text{ in } \mathbb{Z}_\ell$$

3. Return (B, γ).

Need a nice group:

In our examples we need

$$\exp_P : \mathbb{Z}_\ell \longrightarrow \langle P \rangle \subseteq G$$
$$a \longmapsto \alpha P$$

$\exp_P$ = scalar$_P$

<u>easy</u>

and its inverse "dlog_P" is <u>difficult.</u>

<u>Groups candidates</u>

$\mathbb{Z}_\ell^+$ cyclic groups, addition of $\mathbb{Z}_\ell$.

e.g. with $P = 1$.

BAD choice: both maps are easy.

$\mathbb{Z}_p^\times$ (prime) e.g. with $P = 2$.

Here $\alpha \longmapsto P^\alpha = 2^\alpha$ in $\mathbb{Z}_p$ (n = bitsize of p)

is still easy. (Runtime $O(n^3)$)

How fast can I compute α from P^α?

Elliptic curves over $\mathbb{F}_q$ ....

the finite field with q elements, q prime power

Definition

An <u>elliptic curve</u> E over $\mathbb{F}_q$ (a field k) is a <u>smooth</u> <u>cubic</u> curve in the plane [with a ~~the~~ rational flex point].

Cubic curves:

$y^2 = x^3$ over $\mathbb{F}_{27}$

$y^2 = x^3$ over $\mathbb{R}$

$y^2x + y^3 + x^3 - 3xy + x - 10 = 0$ over $\mathbb{F}_{13}$

$x^3 + y^3 + 1 = 0$ over $\mathbb{Q}$

$(\Leftrightarrow \quad a^3 + b^3 + c^3 = 0$ over $\mathbb{Z})$

$y^2 = x^3 - x$

General cubic polynomial has 10 coefficients:

$$x^3,\ x^2y,\ xy^2,\ y^3,\ x^2,\ xy,\ y^2,\ x,\ y,\ 1.$$

(This is why a cubic is determined generically by 9 points.)

$$\sum_{i+j\le 3} a_{ij}\, x^i y^j$$

$$\left(P_r = (x_r, y_r) \right.$$

$$\sum_{i+j\le 3} (x_r^{\,i}\, y_r^{\,j})\, a_{ij} = 0$$

ie. with 9 points, $r \in \{1, \dots, 9\}$:

$$\begin{array}{c} P_1 \\ P_2 \\ \\ 9 \end{array} \underbrace{\begin{bmatrix} 1 & x_1 & y_1 & \cdots \\ 1 & x_2 & y_2 & \cdots \\ \vdots & & & \\ & & & \end{bmatrix}}_{\sim 10} \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ \vdots \\ a_{30} \end{bmatrix} = 0.$$

→ at least 1-dim kernel

→ at least 1 curve has the given 9 points.

Completing the definition:

a cubic polynomial f in two variables x, y defines a cubic curve over k $(= \mathbb{F}_q)$

$\mathcal{C} = \{ (x,y) \in k^2 \mid f(x,y) = 0 \}$ ...

The curve is smooth if all of its points

have a non-zero normal vector:

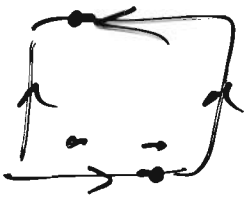
the set $\{ (x,y) \in k^2 \mid f(x,y)=0,$
$f_x(x,y)=0,$
$f_y(x,y)=0 \}$

is empty (and also at infinity....).

[Tricky candidate: $f(y,z) = y^2 z - 1$]

$y^2 - x^3$
$\rightsquigarrow$
$y^2 z - x^3$
$\rightsquigarrow$
$y^2 z - 1$.]

Guess:
$\langle F, F_x, F_y, F_z \rangle$,
...



Definition

An elliptic curve is a smooth cubic curve ...

---

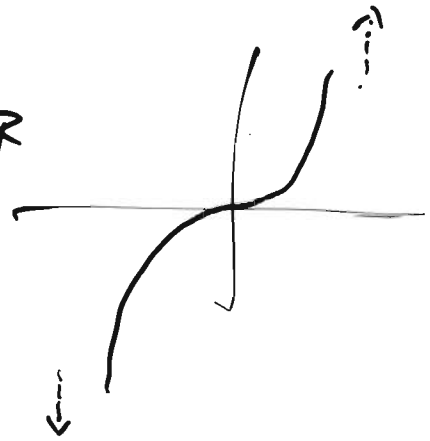
* cubic curve:

(a) This is the set of solutions of a cubic polynomial in two variables x, y ...

(b) including 'points at infinity'.

simple examples:

- $f = y - x^3$ over $\mathbb{R}$

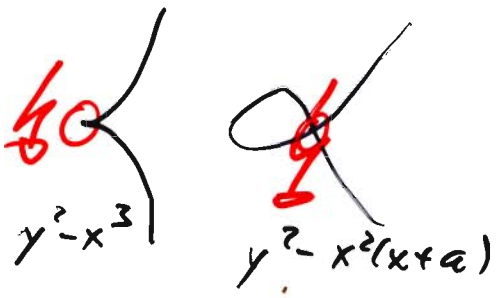


points at infinity

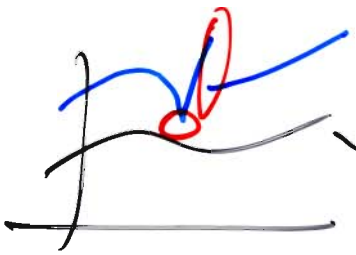
Here: one point $\mathcal{O}$.

* smooth

NOT:



School:



graph of $g : k \to k$

$$\text{graph } g = \{ (x, g(x)) \mid x \in k \}$$
$$= \{ (x, y) \mid y = g(x) \}$$

This considers

$$f = y - g(x).$$

ecc
3.11.09
2

We have seen that here the tangent to a point of $\{f=0\} := \{(x,y)\in k \mid f(x,y)=0\}$ is given by

$$\left\{ (x,y)\in k^2 \;\middle|\; \begin{bmatrix} f_x(x_0,y_0) & f_y(x_0,y_0) \end{bmatrix} \begin{bmatrix} x-x_0 \\ y-y_0 \end{bmatrix} = 0 \right\},$$

actually/obviously, this is not a line if this is a line! if $f_x(x_0,y_0)=0$ and $f_y(x_0,y_0)=0$.

Now, an affine curve
<u>without points at infinity</u>
is smooth if

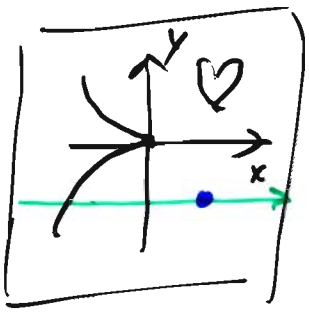
$$\{ f=0,\ f_x=0,\ f_y=0 \}$$

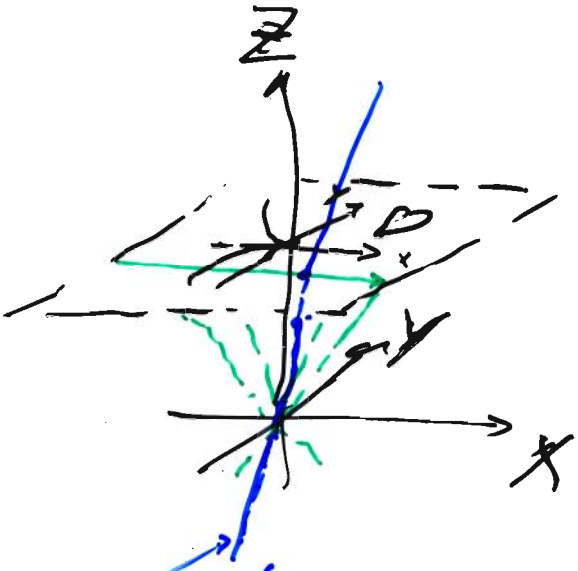
is empty.

In other words: for every point (x_0,y_0) of the curve, that is $f(x_0,y_0)=0$, either $f_x(x_0,y_0)\neq 0$ or $f_y(x_0,y_0)\neq 0$.

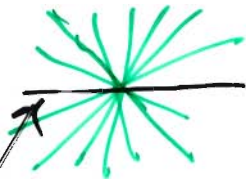
Interludium: Projective space

ecc
3.11.09
3





affine plane



projective point
(it is a line in k^3 through the origin)

this proj. point is the point "in direction x", it is the point at infinity of the green line.

$$k^2 \hookrightarrow k^3 \qquad \mathbb{P}^2 k = \mathbb{P}(k^3)$$

$$(x,y) \longmapsto (x,y,1) \qquad X:Y:Z$$

where $(X,Y,Z) \neq (0,0,0)$.
$\in k^3$

$$k^2 \hookrightarrow \mathbb{P}^2 k$$

$$(x,y) \longmapsto x:y:1 \qquad = \{(\alpha X, \alpha Y, \alpha Z) \mid \alpha \in k^\times\}.$$

affine points — proj. points

Side question: given $X:Y:Z$, to which affine point does this correspond (if so)?

If $Z \neq 0$ then $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$.

If $Z = 0$ then it is a point at infinity!

Actually we are interested in sets/curves

$$\{ f = 0 \}.$$

We want that – in case $Z \neq 0$ –

$$\underbrace{Z^{\deg f} f\left(\frac{X}{Z}, \frac{Y}{Z}\right)}_{=: F(X,Y,Z)} = 0 \quad \text{for } \cancel{\text{our points}} \text{ projective solutions.}$$

↑ this is a homogeneous polynomial of the same degree as f.

<u>Example</u>

$$f = y - x^3 \rightsquigarrow F = Z^3\left(\frac{Y}{Z} - \left(\frac{X}{Z}\right)^3\right)$$
$$= YZ^2 - X^3.$$

Now, since we are back to <u>polynomials</u>, we can ask for <u>all</u> solutions of $\{ X:Y:Z \in \mathbb{P}^2_k \mid F(X,Y,Z) = 0 \}$

A polynomial F is homogeneous if

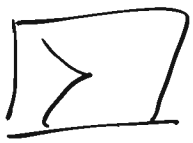
(i) all its monomials have the same degree

(ii) for all X, Y, Z, ~~and~~ $\alpha \in k$ we have

$$F(\alpha X, \alpha Y, \alpha Z) = \alpha^{\deg F} \cdot F(X, Y, Z)$$

Obviously, by construction:

$$\begin{array}{ccc} k^2 & \longrightarrow & \mathbb{P}^2 k \\ \cup & & \cup \\ \{f=0\} & \longrightarrow & \{F=0\} \end{array}$$



Side remark: NOTE that we only use $+, -, \cdot, /$.

non-smooth (singular) affine

$f(x_0, y_0) = 0$
$f_x(x_0, y_0) = 0$
$f_y(x_0, y_0) = 0$

non-smooth (singular) projective

$F(X_0, Y_0, Z_0) = 0$
$F_X(X_0, Y_0, Z_0) = 0$?
$F_Y(X_0, Y_0, Z_0) = 0$
$F_Z(X_0, Y_0, Z_0) = 0$?

Example

- $f = y - x^3$, $F = YZ^2 - X^3$

Now which solutions are seen by F but not small f? Which solutions at infinity do we find?

$\rightsquigarrow$ Need $Z=0$: $F(X,Y,0) = 0$

$$\overset{\shortparallel}{-X^3}$$

(~~Next~~ - since we are allowed to scale -)

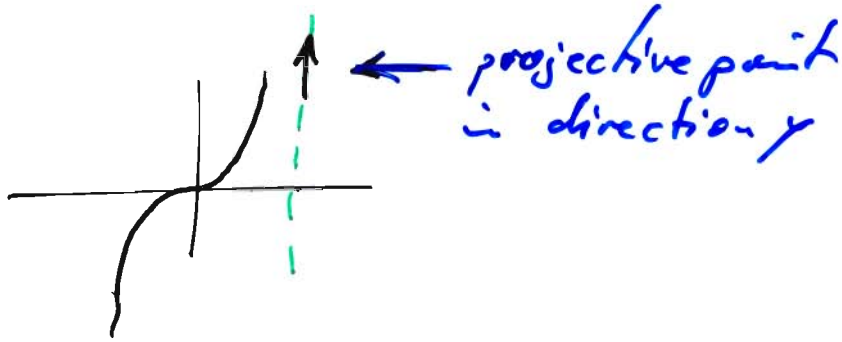
~~we put $Y = 1$.~~

~~and~~ find $-X^3 = 0$

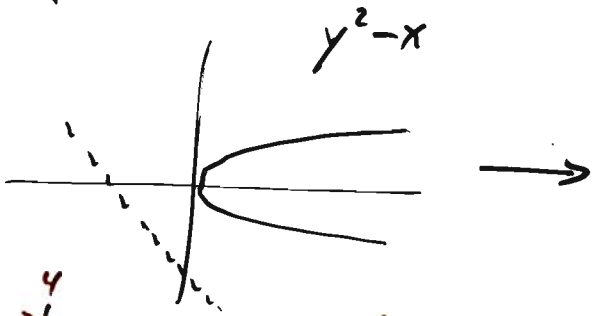
so $X = 0$, and $Y \neq 0$.

Thus $0:1:0 \in \{F = 0\}$.

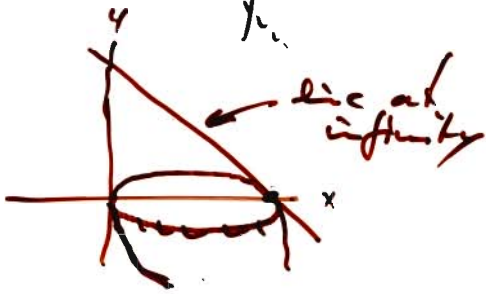
In picture:



another example:



Preview



Transformations?

It may be helpful to rewrite equations.
What is allowed?
Probably best to use only polynomial transformation.

$$f = (x+y)^3 - y^3 = x^3 + 3xy^2 + 3x^2y$$

$$h = u^3 - v^3 .$$

and identify $u = x+y$, $v = y$.

Affine space

$$k^2 \longrightarrow k^2$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} ax+by+e \\ cx+dy+f \end{pmatrix}$$

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ invertible!

Projectively?

$$\mathbb{P}^2 k \longrightarrow \mathbb{P}^2 k$$

$$X:Y:Z \longmapsto U:V:W$$

$$\begin{bmatrix} U \\ V \\ W \end{bmatrix} = A \cdot \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \text{ with } A \in k^{3\times 3} \text{ invertible.}$$

How to determine A ?

Well ... linear algebra ...

and give the images of

$1:0:0$ = 'infinite' point in direction of the x-axis

$0:1:0$ = 'infinite' point in y-direction

$0:0:1$ = affine origin $(0,0)$

Let's take

$$1:0:0 \longmapsto 1:0:1$$
$$0:1:0 \longmapsto 0:1:1$$
$$0:0:1 \longmapsto 0:0:1$$

this defines

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \quad A^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & -1 & 1 \end{bmatrix}$$

Say we consider $f = y^2 - x$, $F = Y^2 - XZ$

$$\begin{bmatrix} U \\ V \\ W \end{bmatrix} = \begin{bmatrix} X \\ Y \\ X+Y+Z \end{bmatrix} = A \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}$$

$U = X, \quad V = Y, \quad W = X+Y+Z$

$X = U, \quad Y = V, \quad Z = -U-V+W$

~~So $H = F($~~

ecc
3.11.09
9

90

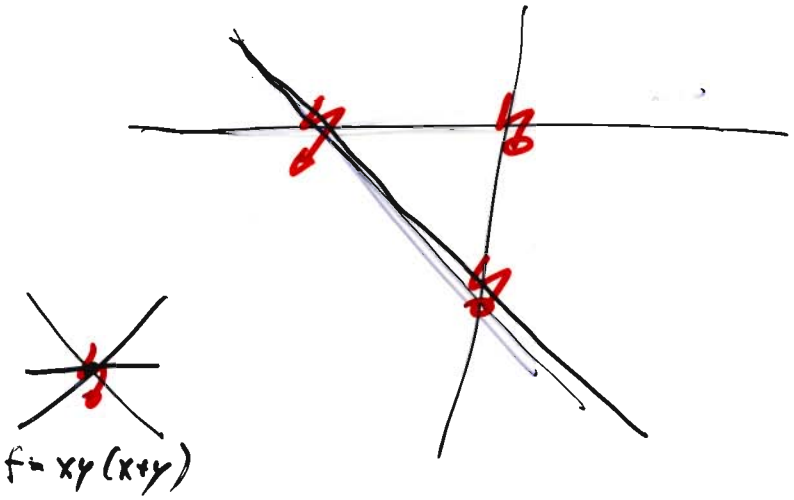
$$\underline{\underline{H(U,V,W)}} = F(X,Y,Z)$$
$$= F(U,V,-U-V+W)$$
$$= V^2 - U(-U-V+W)$$
$$= V^2 + U^2 + UV - UW$$

$$(U+\tfrac{1}{2}V)^2 + \tfrac{3}{4}V^2 - UW$$

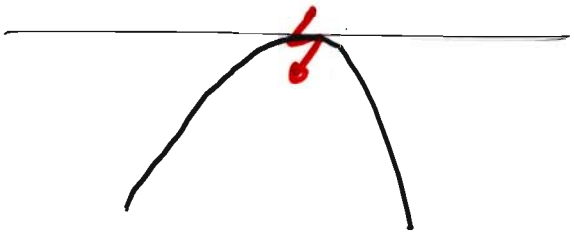
and

$$\underline{\underline{h(u,v,\cancel{w})}} = H(u,v,1)$$
$$= u^2 + uv + v^2 - u\,.$$

ecc
9.11.09
4

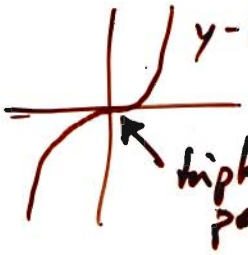


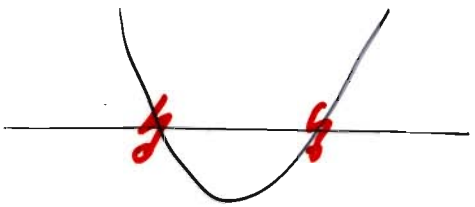
$f = xy(x+y)$



$f = xy(x+y+1)$

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





$f = (y-1)(2y-x^2)$

over $\mathbb{R}$

But over $\mathbb{Q}$ the singular points do not exist!

Def

An elliptic curve over a field k is a smooth, irreducible, cubic, projective curve.

including points at infinity

with $\underbrace{\text{a rational point}}$.

that is, the curve is non-empty.

Degree

Assume we have a cubic polynomial

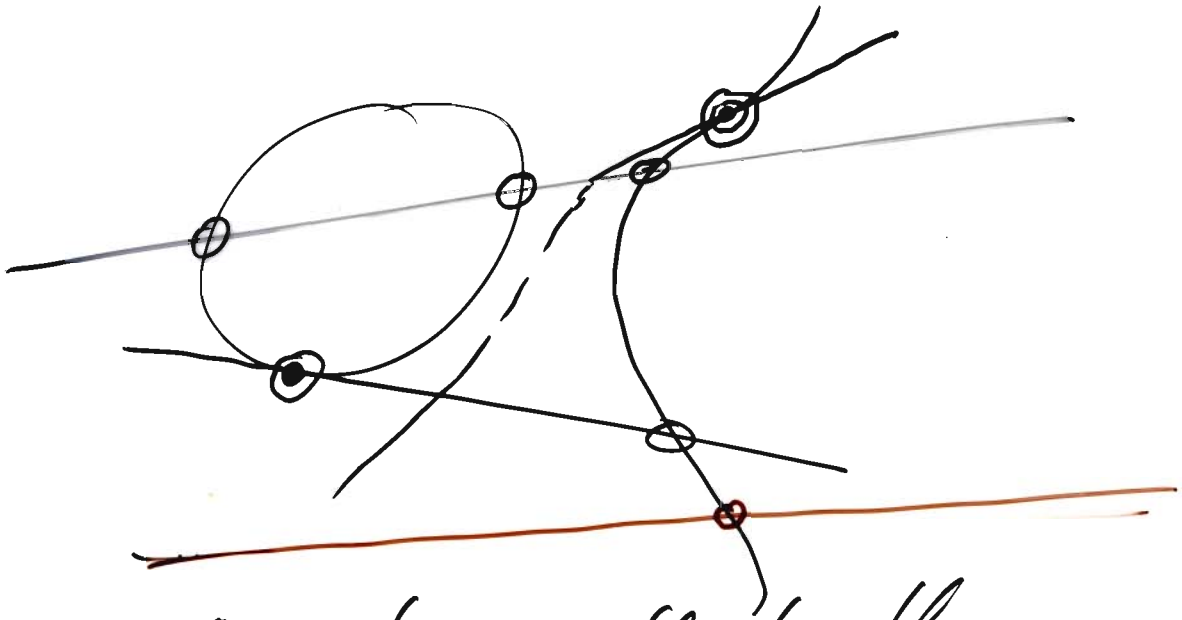
$$f(x,y)$$

and a line, say, $y = \alpha x + \beta$.

To find the points of intersection of the curve $\{f=0\}$ and the line just plug in:

$$\varphi(x) := f(x, \alpha x + \beta) = 0,$$
$$y = \alpha x + \beta.$$

We expect at most three solutions, because φ is a polynomial in x of degree 3.



This picture reflects the geometric degree.

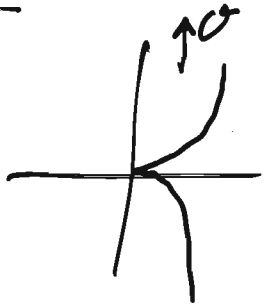
Def (generalized Weierstraß equation)

For $a_1, \dots, a_6 \in k$ the equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

describes a cubic curve in <u>generalized Weierstraß form</u>.

Eg. $a_1 = \dots = a_6 = 0$ yields $y^2 = x^3$



For any choice of $\underline{a}$ there is exactly one point at infinity:

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

Moreover, note that $\mathcal{O}$ is always regular on these curves.

We can further simplify the equation by coordinate changes.

Eg. $u = x + \frac{a_2}{3}$,

$x = u - \frac{a_2}{3}$.

Plugging in:

$$x^3 + a_2 x^2 + a_4 x + a_6$$

$$= \left(u - \frac{a_2}{3}\right)^3 + a_2 \left(u - \frac{a_2}{3}\right)^2 + a_4 \left(u - \frac{a_2}{3}\right) + a_6$$

$$= u^3 + \underbrace{\left(-a_2 + a_2\right)}_{=0} u^2 + ? \cdot u + ?$$

Of course, we can use this only if our field k allows division by $3 \cdot 1_k$, that is, if $3 \cdot 1_k \neq 0$ in k.

$$3 \cdot 1_k = 1_k + 1_k + 1_k$$

Recall $\operatorname{char} k = \min \{ j \in \mathbb{N}_{>0} \mid j \cdot 1_k = 0 \text{ in } k \}$

(with $\min \emptyset := \infty$ (or 0)).

and for the previous we need $\operatorname{char} k \neq 3$.

Let's try that trick on the left of a generalized Weierstraß equation:

$$y^2 + (a_1 x + a_3)\, y - r(x) = 0$$

So replace $\quad y = v - \dfrac{a_1 x + a_3}{2 \cdot 1_k}$

(provided you can, ie. char $k \neq 2$.)

Now plugging in:

$$0 = \left(v - \frac{a_1 x + a_3}{2}\right)^2 + (a_1 x + a_3)\left(v - \frac{a_1 x + a_3}{2}\right) - r(x)$$

$$= v^2 + \underbrace{\left(-2 \cdot \frac{a_1 x + a_3}{2} + a_1 x + a_3\right)}_{=0} v - \tilde{r}(x)$$

still of degree ≤ 3.

By this trick we obtain an equation of the form

$$v^2 = \tilde{r}(x)$$

and playing the first trick now we find

$$v^2 = u^3 + au + b \,.$$

Where the connection is given by: $\quad y = v - \frac{a_1}{2} x - \frac{a_3}{2}$

$$x = u - \tilde{a}_2/3 \,.$$

For short:

<u>Theorem</u>

If the characteristic of k is neither 2 nor 3 then ~~by~~ a coordinate change we can bring ~~the~~ any elliptic curve in Weierstraß form, that is,

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

Note that we ~~have~~ only proved this under the assumption that the curve was in generalized Weierstraß form.
(From cubic to generalized Weierstraß you get by applying the algorithm of Nagell (see the notes of Connell).)

Let's consider our questions here: points at infinity?
smooth?

Points at infinity

Projective version is

$$Y^2 Z = X^3 + a X Z^2 + b Z^3$$

So plugging in $Z=0$ gives $0 = X^3$,

so $X=0$ and $Y \neq 0$,

thus $O = 0:1:0$ is

the only point at infinity.

Plugging in $Y=1$ yields

$$Z = X^3 + a X Z^2 + b Z^3$$

Now, call

$$h(x,z) = x^3 + a x z^2 + b z^3 - z$$

and ~~consider~~ examine O for smoothness:

$$h(0,0) = 0$$

$$h_x(x,z) = 3x^2 + a z^2 + \cancel{3b z^2}$$

$$h_x(0,0) = 0$$

$$h_z(x,z) = 2axz + 3bz^2 - 1$$

$$h_z(0,0) = -1 \neq 0 \; !$$

Thus O is a regular point.

When are the affine points all regular?

4.11.09
ecc
8

Consider
$$f(x,y) = -y^2 + x^3 + ax + b.$$

The curve now is $f = 0$.

Compute:
$$f_x(x,y) = 3x^2 + a,$$
$$f_y(x,y) = -2y.$$

A point is singular if all three terms f, f_x, f_y vanish.

In particular: $y = 0$. (since $f_y = -2y$ and char $k \neq$ [redacted] 2).

Thus we are looking for solution of

$$f = 0 \quad : \quad r(x) := x^3 + ax + b = 0$$
$$f_x = 0 \quad : \quad 3x^2 + a = 0$$

This has a solution iff the polynomial r has a multiple zero!

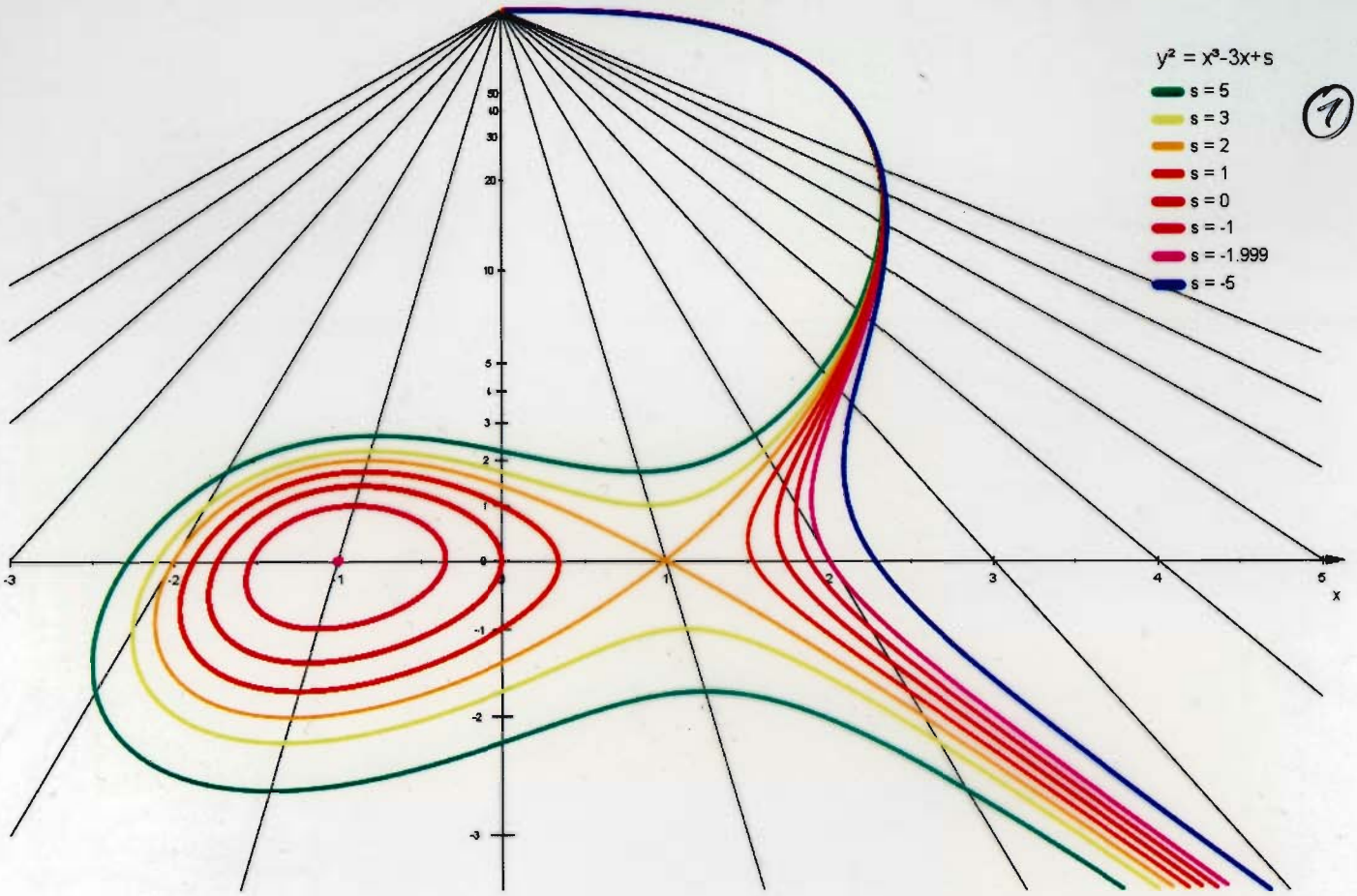
Assume $r(x) = (x - x_0)(x - x_1)(x - x_2)$,

Then $r'(x) = (x - x_1)(x - x_2) + (x - x_0)(x - x_2) + (x - x_0)(x - x_1)$

so $r'(x_0) = (x_0 - x_1)(x_0 - x_2)$

Thus x_0 is a common solution iff $x_0 = x_1$ or $x_0 = x_2$,

ie. x_0 is a double or triple root of r.



1

$$y^2 = x^3 - 3x + s$$

This 'proves' that the point O at infinity is the y-direction!

Let's try to characterize the cases where $r(x) = x^3 + ax + b$ has multiple roots.
We run the PEEA:

					t
$r_0 = r(x)$:	$x^3 + ax + b$	3			
$r_1 = r'(x)$:	$3x^2 + a$	2^2a^2	x		
	$2ax + 3b$		$6ax - 9b$		
	$4a^3 + 27b^2$				

$$3\,(x^3 + ax + b) = (x + 0)(3x^2 + a) + (2ax + 3b)$$

$$\begin{array}{r} 3x^3 + ax \\ \hline 2ax + 3b \end{array}$$

$$2^2a^2\,(3x^2 + a) = (3x\,2a + -9b)(2ax + 3b) + 4a^3 + 27b^2$$

$$\begin{array}{r} 2a\,(6a\,x^2 + 9bx) \\ \hline 2a\,(-9bx + 2a^2) \\ -18abx - 27b^2 \\ \hline 4a^3 + 27b^2 \end{array}$$

Thus: r, r' have a common root iff $4a^3 + 27b^2 = 0$.

<u>Thm</u> Assume that char $k \neq 2, 3$.
A cubic curve

$$y^2 = x^3 + ax + b =: r(x)$$

has the only point O at infinity, where $O = 0:1:0$, and its tangent is the line at infinity which in turn has a triple intersection with the curve at O, in other words: O is a flex.

The curve is smooth iff

(a) $r(x)$ has no multiple root, or equiv.

(b) $r(x)$ and $r'(x)$ have no common root, or equiv.

(c) $4a^3 + 27b^2 \neq 0$.

Remark: to consider O and its tangent change to the chart/map $Y = 1$:

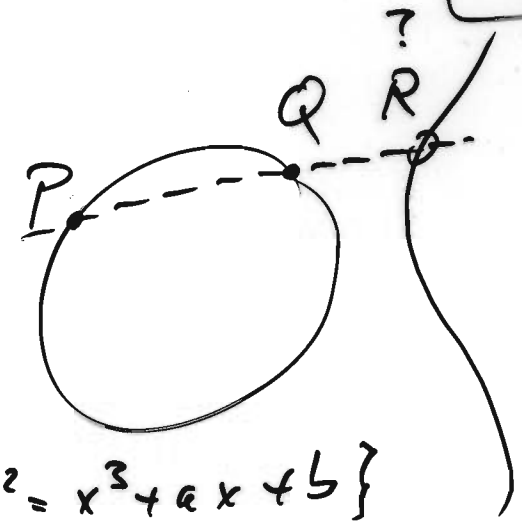
$$z = x^3 + axz^2 + bz^3.$$

Here $(x,z) = (0,0)$ is a solution and you'll find that $z = 0$ is the tangent, which has no further intersection...

The operation

We are looking for a map

$$E \times E \longrightarrow E$$



where $E = \{ (x,y) \in k^2 \mid y^2 = x^3 + ax + b \}$
$\cup \{ \mathcal{O} \}$.

Now observe that any given line has three points of intersection – provided you count with multiplicities and the field is large enough.

In projective coordinates, we have

$$F(X,Y,Z) = -Y^2 Z + X^3 + aXZ^2 + bZ^3,$$

~~and the~~ which defines the curve $F=0$, and the line is given by

$$L_{\lambda:\mu} = \begin{bmatrix} \lambda P_x + (\mu-\lambda) Q_x \\ \lambda P_y + (\mu-\lambda) Q_y \\ \lambda P_z + (\mu-\lambda) Q_z \end{bmatrix}$$

for some $P, Q \in \mathbb{P}^2 k$ different. Now we obtain

$$h(\lambda,\mu) = F(\lambda P_x + (\mu-\lambda) Q_x, \lambda P_y + (\mu-\lambda) Q_y, \lambda P_z + (\mu-\lambda) Q_z)$$

is a homogeneous polynomial of degree 3.

thus either

$h \equiv 0$

or h has three roots in some extension of k.

That is, either the line intersect three times or the line is entirely part of the curve.

The ~~former~~ latter would mean that the curve splits into a line and a quadratic curve, i.e. the curve would be reducible.

By assumption however it is irreducible!

So: every line intersects an elliptic curve exactly three times - well at least over $\bar{k}$.

Next: assume $P, Q \in E$.

Then $h(0,\mu) = \cancel{F(\mu Q) = 0}$

$$\overset{\shortparallel}{F(\mu Q_x, \mu Q_y, \mu Q_z)} = \mu^3 F(Q) = 0.$$

and

$$h(\mu,\mu)$$

$$\overset{\shortparallel}{F(\mu P_x, \mu P_y, \mu P_z)} = \mu^3 F(P) = 0.$$

Thus $h(\lambda, 1)$

has $\lambda = 0$ and $\lambda = 1$ as zeroes,

ie. $h(\lambda,1)$ is a multiple of $\lambda(\lambda - 1)$.

Using division with remainder we can write

$$h(\lambda,\mu) = \lambda \cdot (\lambda - \mu) \cdot \ell(\lambda,\mu)$$

with ℓ linear homogeneous.

We conclude that the third point now has rational coordinates!

$$\ell(\lambda,\mu) = \ell_1 \lambda + \ell_2 \mu$$

so

$$\lambda = \ell_2, \quad \mu = -\ell_1 \text{ is a solution}$$

and

$$L_{-\ell_2 : \ell_1} \quad \text{is the third point}$$

and obviously has coordinates in k because P and Q do and $-\ell_2$ and ℓ_1 are in k.

So we could define

$$P \boxplus Q := R = \text{third intersection point}$$

The operation

We define

$$P \boxplus Q := \text{third point on the line } (PQ) \text{ and the curve.}$$

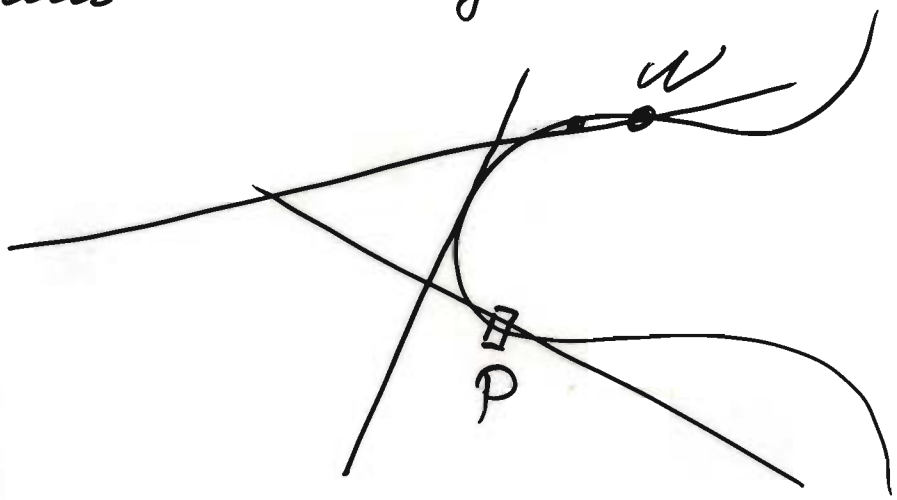
This is of course a well-def'd map

$$E \times E \longrightarrow E.$$

Say $N \in E$ was a neutral element wrt. to $\boxplus$.

Then $$P \boxplus N = P.$$

thus every line through such point P and N must be tangent at P.



Thus $\boxplus$ has no neutral element.

Observe also that with

$$R = P \boxplus Q$$

we have

$$P = Q \boxplus R,$$

and

$$Q = R \boxplus P$$

<u>Idea</u>

$$x + y + z = 0$$

has a similar symmetry.

Try to define an operation such that

$$P + Q + R = 0$$

where

$$P, \quad Q, \quad R$$

are three on a line and the curve.

Thus we should define

$$P + Q := -R$$

What's this?

We need that $-(-R) = R$.

We try to define

$$-R = R \boxplus \mathcal{A}$$

for some fixed point $\mathcal{A}$.

Then $-(-R) = R$.

If we want that $\mathcal{A}$ is neutral then we need $-\mathcal{A} = \mathcal{A}$, i.e.

$$\mathcal{A} = \mathcal{A} \boxplus \mathcal{A}.$$

In other words, $\mathcal{A}$ must be a flexpoint.

Assume that $\mathcal{N}$ is neutral w.r.t. $+$.

Then

$$\mathcal{N} + \mathcal{N} = \mathcal{N}$$

$$\mathcal{N} = -\mathcal{N}$$

i.e.

$\mathcal{N}, \mathcal{N}, -\mathcal{N}$ are on a line & the curve

$\mathcal{N}, -\mathcal{N}, \mathcal{A}$ — " —

then $\mathcal{A} = \mathcal{N}$.

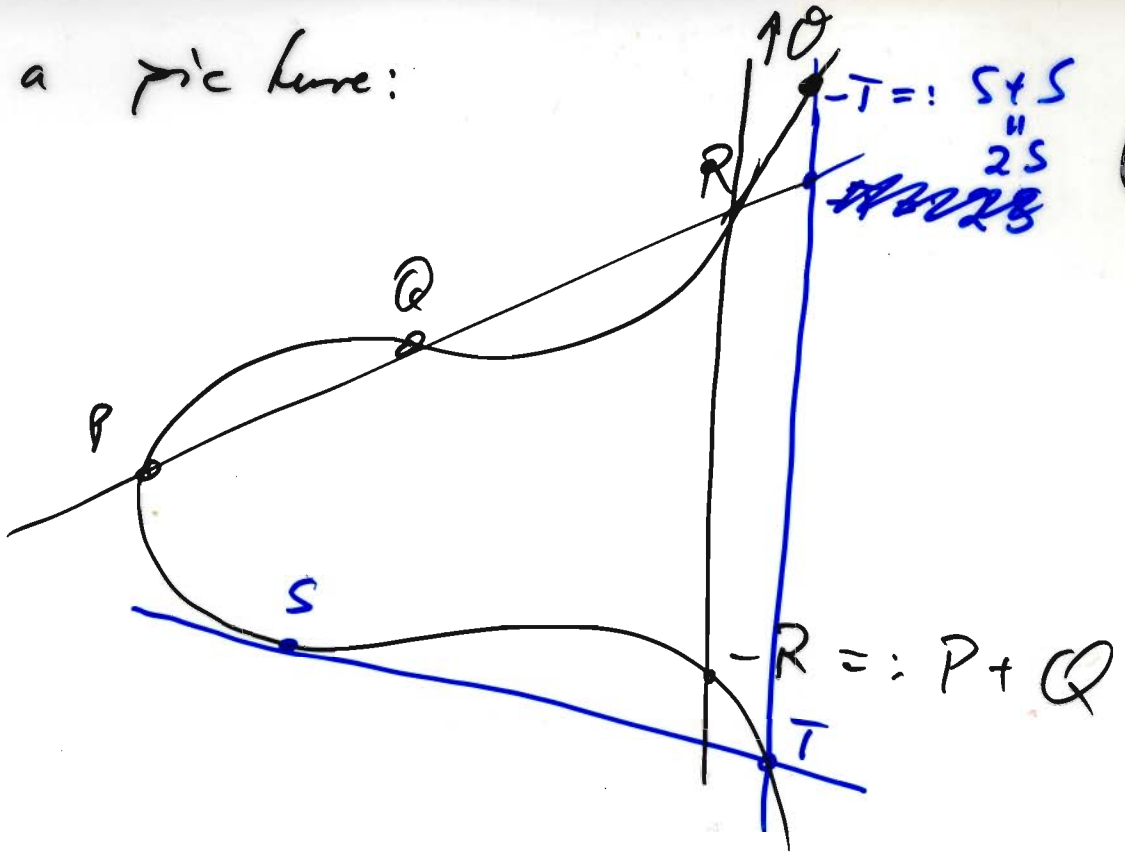
Thus $\mathcal{A}$ must be a flex and is neutral.

So take $\mathcal{A} = \mathcal{O}$ in our Weierstraß form:

$$\bar{E} \times \bar{E} \longrightarrow \bar{E}$$

$$(P, Q) \longmapsto P+Q := (P \boxplus Q) \boxplus \mathcal{O}$$

In a picture:



We already said that $P \boxplus P$ asks for the third point on the tangent at P.

Properties?

(Proper) This is a well defined map $E \times E \to E$.

Ⓐ … defer … $(P+Q)+S \overset{?}{=} P+(Q+S)$

Ⓝ Now, $\mathcal{O}$ is neutral: $P + \mathcal{O} = P$
$\qquad \shortparallel$
$\mathcal{O} + P$

Ⓘ Obviously: $P + (-P) = \mathcal{O}$

Ⓒ Clearly: $P + Q = Q + P$

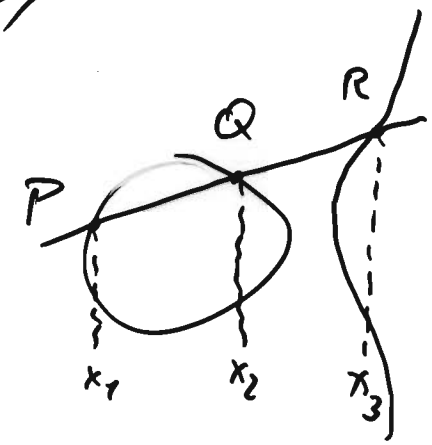
Can we derive formulas for

$P + Q$?

Say $P = (x_1, y_1)$, Assume $x_1 \neq x_2$.
$Q = (x_2, y_2)$.

Then the line (PQ) is given by

$$y = m x + c$$



with

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

so

$$y = m(x - x_1) + y_1.$$

is our line.
Now intersect with the curve $E: y^2 = x^3 + ax + b$.
Thus we must have x_3 a solution of:

$$0 = x^3 + ax + b - (m(x - x_1) + y_1)^2.$$

Assume we have it then the rhs is

$$(x - x_1)(x - x_2)(x - x_3)$$
$$\parallel$$
$$x^3 - (x_1 + x_2 + x_3)x^2 + \dots$$

Also the rhs evaluates to

$$x^3 - m^2 x^2 + \dots$$

So we necessarily have

$$x_3 = m^2 - x_1 - x_2.$$

So

$$R = (x_3, y_3)$$

with

$$x_3 = m^2 - x_1 - x_2, \qquad m = \frac{y_2 - y_1}{x_2 - x_1}.$$
$$y_3 = m(x_3 - x_1) + y_1$$

and so

$$P + Q = (x_3, -y_3)$$

because

$$-R = (x_3, -y_3)$$

as $y^2 = x_3^3 + a x_3 + b$
has the solutions $y = y_3$ and $y = -y_3$
and is the intersection of the line $x = x_3$
through R and O.

So we are happy?
No, what if $x_1 = x_2$?
In case $P = Q$ we need to determine
the line $y = m(x - x_1) + y_1$ as
the tangent at P:

$$f(x, m(x-x_1)+y_1) = x^3 + ax + b - (m(x-x_1)+y_1)^2$$

where

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

To get a tangent we have to determine m such that

$$f(x, m(x-x_1)+y_1)$$

has a double root at $x = x_1$.
Thus also its derivative at $x = x_1$ must vanish:

$$0 = \underbrace{f_x(x_1, y_1)}_{3x_1^2+a} \cdot 1 + \underbrace{f_y(x_1, y_1)}_{-2y_1} \cdot m$$

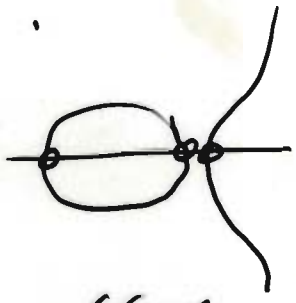
thus we must have

$$m = \frac{3x_1^2 + a}{2y_1}.$$

This is of course only possible if $y_1 \neq 0$.
So then we find

$$P + Q = (x_3, -y_3) \qquad \begin{aligned} x_3 &= m^2 - 2x_1 \\ y_3 &= m(x_3 - x_1) + y_1 \\ m &= \frac{3x_1^2+a}{2y_1}. \end{aligned}$$

In case $P = Q$ and $y_1 = 0$



we necessarily have $3x_1^2 + a \neq 0$,
because the curve is smooth.
So we expect $m = \infty$ to be the right thing...
Actually, we can see that now

$x = x_1$ is the tangent.

Thus $P + Q = O$ here.

We have:

- $P \neq Q \to x_1 \neq x_2$
  $\to x_1 = x_2$ i.e. $Q = -P$.
  $\hookrightarrow P + (-P) = \mathcal{O}$
- $P = Q \to y_1 \neq 0$
  $\hookrightarrow y_2 = 0$

Altogether:

$$P + Q = (x_4, y_4)$$

with

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_2 \neq x_1 \\[2ex] \dfrac{3x_1^2 + a}{2y_1} & \text{if } P = Q,\ x_1 = x_2,\ y_1 = y_2 \neq 0 \\ y_1 \neq 0. \end{cases}$$

and

$$x_4 = m^2 - x_1 - x_2$$

$$y_4 = -m(x_4 - x_1) - y_1$$

in these cases.

Else:

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

$$P + P = \mathcal{O} \quad \text{if } P = -P \text{ i.e. } y_1 = 0,$$

and

$$P + \mathcal{O} = P,$$

$$\mathcal{O} + Q = Q,$$

$$\mathcal{O} + \mathcal{O} = \mathcal{O}.$$

How to prove associativity?

Solution 1: computationally.

Assume that P, Q, R are sufficiently generic (i.e. we never to deal with $\mathcal{O}$ and never add a point to itself).

Then we have formulas for

$$P + Q$$

$$(P+Q) + R$$

$$Q + R$$

$$P + (Q + R)$$

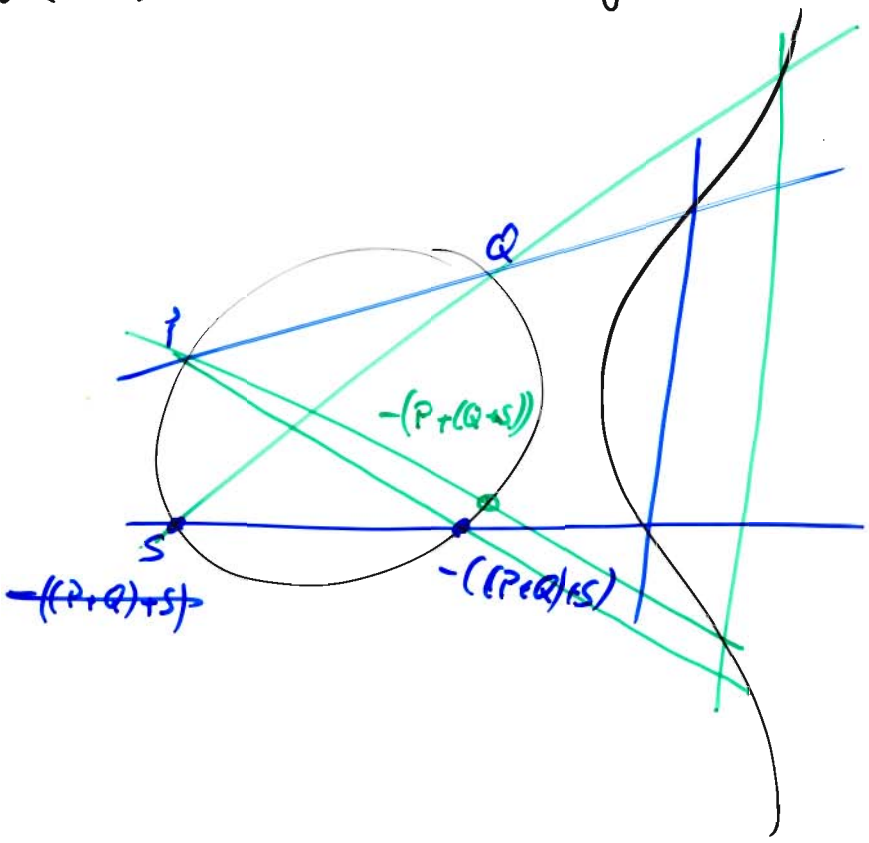
in terms of $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $S = (x_3, y_3)$

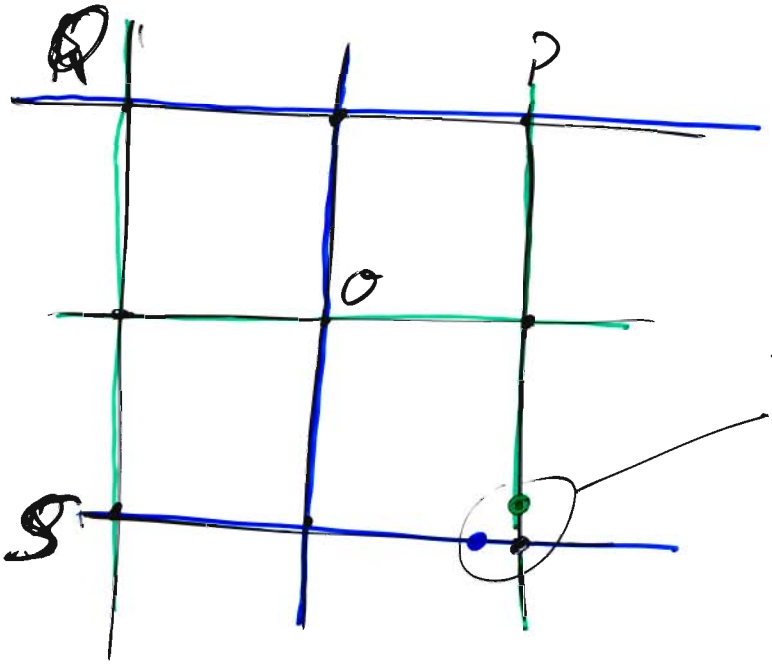
noting that
$$y_1^2 = x_1^3 + a x_1 + b,$$
$$y_2^2 = x_2^3 + a x_2 + b,$$
$$y_3^2 = x_3^3 + a x_3 + b.$$

One finds $(P+Q) + S = P + (Q + S)$

By 'closure' arguments this proves associativity in all cases.

Solution 2: Prove it geometrically.





Theorem: This is one point!

Solution 3: Prove it algebraically.

Construct a completely different group $\mathrm{Div}^0(E)/\mathrm{Princ}(E) =: \mathrm{Pic}(E)$

Then prove that the map

$$E \longrightarrow \mathrm{Pic}(E)$$
$$P \longmapsto [(P)-(O)]$$

is an isomorphism.

Riemann-Roch

Singular cubics

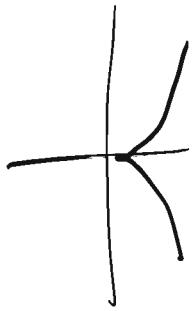
Assume Weierstraß form:

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

- Then either the rhs has a triple zero:

$$y^2 = (x - x_0)^3 \rightsquigarrow y^2 = x^3$$

$$z^2 = x^3$$



It turns out that

$$(\{y^2 = x^3\} \setminus \{(0,0)\}) \cup \{\mathcal{O}\} \cong (k, +).$$

$$(x,y) \longmapsto x/y$$

$$\mathcal{O} \longmapsto 0$$

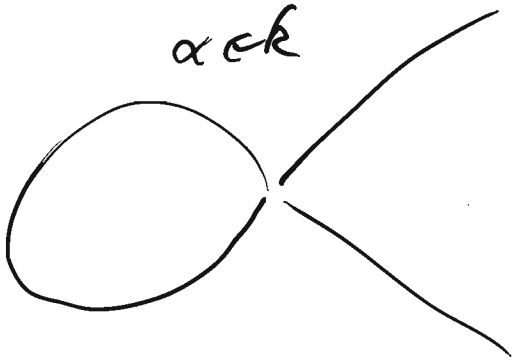
- Or the rhs has a double zero:

$$y^2 = x^2(x + a).$$

And there two cases:

$$a = \alpha^2 \quad \text{with} \quad \begin{cases} \alpha \in k, \\ \alpha \notin k. \end{cases}$$

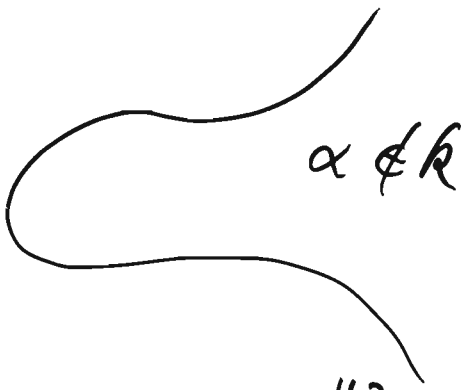
$\alpha \in k$



$\cong$

$\{u + \alpha v \mid u, v \in k,\ v^2 - av^2 = 1\}$

$\alpha \notin k$



$\cong$

$k^\times$.

Other equations: Legendre form.

Assume we have curve $y^2 = x^3 + ax + b$.

Say: $x^3 + ax + b = (x - e_0)(x - e_1)(x - e_2)$

Map $e_0 \mapsto 0$, $e_1 \mapsto 1$ by a linear transform on x:

$$u = \frac{x - e_0}{e_1 - e_0}, \quad v = (e_1 - e_0)^{3/2} \cdot y$$

we find:

$$\boxed{v^2 = u(u-1)(u-\lambda).}$$

with

$$\lambda = \frac{e_2 - e_0}{e_1 - e_0}$$

$$1 - \frac{\lambda}{\lambda - 1} = \frac{\lambda - 1 - \lambda}{\lambda - 1} = \frac{1}{1-\lambda}$$

Actually, the set

$$\left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}, \frac{1}{1-\lambda} \right\}$$

usually has six elements and each describes an isomorphic variant of the curve. Only if $\lambda = -1, 2, \frac{1}{2}$, or $\lambda^2 - \lambda + 1 = 0$ the set is smaller.

(over $\mathbb{C}$: $\lambda = e^{\pm 2\pi i/6}$,
i.e. primitive sixth roots of unity)

ecc
17.11.09
5 ~~6~~

~~Isom~~ morphisms?

projectively

$$\beta: \quad \mathbb{P}^2 k \longrightarrow \mathbb{P}^2 k$$

$$X_0 : X_1 : X_2 \longmapsto F_0(X) : F_1(X) : F_2(X)$$

where

$$F_0(\lambda X) : F_1(\lambda X) : F_2(\lambda X)$$
$$\shortparallel$$
$$\cancel{F_1(\lambda X)} \quad F_0(X) : F_1(X) : F_2(X).$$
$$\cancel{F_2(\lambda X)}$$

We require that $F_i(\lambda X) = \lambda^d F_i(X)$

for some d.

Moreover, let's require that F_i is a polynomial, homogeneous of same ~~homogen~~ degree d.

We further need that

~~affine~~

$$(F_0(X), F_1(X), F_2(X)) \neq (0, 0, 0)$$

for all $X_0 : X_1 : X_2$ that we are interested in.

affinely

$$k^2 \longrightarrow k^2$$

$$(x_0, x_1) \longmapsto (f_0(x), f_1(x))$$

where f_0, f_1 are ~~quad~~ polynomials in x_0, x_1.

Def Given $E, F \subset \mathbb{P}^2 k$ two elliptic curves then a map

$$\varphi : E \longrightarrow F$$

is called a <u>morphism</u>

if (1) φ is algebraic, i.e.

$$\varphi(X_0 : X_1 : X_2) = F_0(X) : F_1(X) : F_2(X)$$

for some polynomials F_0, F_1, F_2 in variables X_0, X_1, X_2 which homogeneous and of same degree.

(2) φ is a group morphism, i.e.

$$\varphi(O_E) = O_F$$

$$\varphi(P +_E Q) = \varphi(P) +_F \varphi(Q)$$

An isomorphism is a morphism φ which has an inverse $\bar{\varphi}$: $\varphi \circ \bar{\varphi} = id_F$, $\bar{\varphi} \circ \varphi = id_E$.

Theorem (cf Silverman '86)

If E and F are two curves in general Weierstraß form and

$$\varphi : E \to F$$

is an isomorphism, then there exists $\mu \in k^\times$, $r, s, t \in k$ such that

$$\varphi(x,y) = (\mu^2 x + r,\ \mu^3 y + s\mu^2 x + t)$$

Pf see Silverman, uses Riemann Roch $\square$

Corollary

If E, F are even in Weierstraß form then

$$\varphi(x,y) = (\underbrace{\mu^2 x}_{u},\ \underbrace{\mu^3 y}_{v}).$$

~~$F: y^2 = x^3 + ax + b$,~~

~~$F: y$~~

Now if $\varphi(x,y) \in F$ that means

$$(\mu^3 y)^2 = (\mu^2 x)^3 + a(\mu^2 x) + b$$

Assume

$$E: \quad y^2 = x^3 + ax + b$$

Thus for $(x,y) \in E$ we have

$u = \mu^2 x$
$v = \mu^3 y.$

$$\underbrace{\mu^6 y^2}_{u} = \underbrace{\mu^6 x^3}_{} + a\mu^4 \underbrace{\mu^2 x}_{} + b\mu^6$$

$$F: \quad v^2 = u^3 + c\,u + d$$

where $\quad c = a\mu^4, \quad d = b\mu^6.$

Now, define the j-invariant.
Given a curve $E: \; y^2 = x^3 + ax + b$.
Define

$$j(E) := 1728 \, \frac{4a^3}{4a^3 + 27b^2}.$$

Easy: if $E \xrightarrow[\psi]{\simeq} F$ then

$$j(E) = j(F).$$

$$j(F) = 1728 \, \frac{4c^3}{4c^3 + 27d^2} = 1728 \, \frac{4a^3\mu^{12}}{4a^3\mu^{12} + 27b^2\mu^{12}} = j(E)$$

<u>Theorem</u> char $k \neq 2, 3$.

Given E, F in Weierstraß form with same j-invariant.

Then there exists μ such

$$E \longrightarrow F$$
$$(x, y) \longmapsto (\mu^2 x, \mu^3 y)$$

is an isomorphism from E to F.

<u>Pf</u> We have

$$E: \; y^2 = x^3 + ax + b,$$
$$F: \; v^2 = u^3 + cu + d,$$

and

$$j(E) = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2}$$
$$\|$$
$$j(F) = 1728 \cdot \frac{4c^3}{4c^3 + 27d^2}.$$

<u>Case $a \neq 0$</u>

Thus $j(E) \neq 0$, and $c \neq 0$.

We want $c = a\mu^4$.

Pick $\mu \in k$ such that $\mu^4 = c/a$.

Then $\dfrac{27b^2}{4a^3} = \dfrac{27d^2}{4c^3}$ so $b^2\mu^{12} = d^2$.

Thus either $d = b\mu^6$ or $d = -b\mu^6$.

In the second case replace μ with $i\mu$ where $i^2 = -1$.

then $c = a(i\mu)^4$ and $d = b(i\mu)^6$.

Case $a=0$

Thus $j(E)=0$ and $c=0$.

Now pick $\mu \in \bar{k}$ such that $d = b\mu^6$.

Then also $a \overset{!}{=} c\mu^4$. ✓ $\square$

A few special cases

$j=0 \to a=0$, ie $E_{0,b}: y^2 = x^3+b$.

For example: $x^3+y^3+1=0$ over $\mathbb{Q}$. $3 \mid xyz$, $3 \nmid xyz$

this is isomorphic to $y^2 = x^3 - 432$.

$j=1728 \to b=0$, ie. $E_{a,0}: y^2 = x^3+ax$

For example: over $\mathbb{Q}$ $a=-25$, $a=-4$.

are nice examples.

By our theorem $E_{-25,0} \underset{\mathbb{C}}{\cong} E_{-4,0}$.

However: $E_{-25,0}$ has infinitely many $\mathbb{Q}$-rational points,

whereas

$E_{-4,0}$ has exactly 4 $\mathbb{Q}$-rational points.

For defining μ we need $\sqrt{10}$ here which explains this discrepancy.

We say that

$E_{-25,0}(\mathbb{Q})$ is a <u>twist</u> of $E_{-40}(\mathbb{Q})$

<u>Def</u> Two elliptic curves E, F over a field k are called <u>twists</u> of each other iff $E(\bar{k}) \cong F(\bar{k})$.

(but not necessarily $E(k) \cong F(k)$.)

By $E(K) = \{(x,y) \in K^2 \cap E\} \cup \{O\}$.

Finally note that the j-invariant of

$$E: y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}$$

has j-invariant j, provided $j \neq 0, 1728$.

$$\Delta = \frac{2^2 \cdot 3^3 j^3}{(1728-j)^3} + \frac{3^3 \cdot 2^2 j^2 (2^6 3^3 - j)}{(1728-j)^3}$$

$$= \frac{2^2 3^3}{(1728-j)^3}\left(\cancel{j^3} + 2^6 3^3 j^2 - \cancel{j^3}\right).$$

so

$$j(E) = 2^6 \cdot 3^3 \cdot \frac{2^2 \cdot 3^3 \cdot j^3}{\cancel{(1728-j)^3}} \cdot \frac{\cancel{(1728-j)^3}}{2^2 \cdot 3^3 \cdot 2^6 \cdot 3^3 \cdot j^3} = j.$$

Endomorphisms

examples:

identity: $(x,y) \longmapsto (x,y)$

negation $(x,y) \longmapsto (x,-y)$

zero : $(x,y) \longmapsto \mathcal{O}$

$\ulcorner\ X:Y:Z \longmapsto 0:1:0\ .\ \lrcorner$

doubling: $\underset{(x,y)}{\overset{\shortparallel}{P}} \longmapsto \underset{\left(\left(\frac{3x^2+a}{2y}\right)^2-2x,\ -\left(\frac{3x^2+a}{2y}\right)\left(\left(\frac{3x^2+a}{2y}\right)^2-2x-x\right)-y\right)}{\overset{\shortparallel}{2P}}$

Generalizing:

scalar multiplication $E \longrightarrow E$

$[n] : P \longmapsto n \cdot P$

for any $n \in \mathbb{Z}$ is an endomorphism.

Over a finite field of course

$$[n] = [n + \#E]\ .\ .$$

Sometimes

$(x,y) \longmapsto (\zeta x, -y)$ $\quad \zeta^3 = 1,\ \zeta \neq 1$

or $(x,y) \longmapsto (-x, iy)$ $\quad i^2 = -1$.

make sense.

Further?

18.11.09
ecc
8

Frobenius automorphism of $\mathbb{F}_q$:

$$\varphi: \begin{array}{ccc} \overline{\mathbb{F}_q} & \longrightarrow & \overline{\mathbb{F}_q} \\ x & \longmapsto & x^q \end{array}.$$

Observe that for $x \in \mathbb{F}_q$ we have $x^q = x$.
Lagrange.

Notice further that φ is a field automorphism.

So define

$$E: y^2 = x^3 + ax + b \longrightarrow F: v^2 = u^3 + cu + d$$

$$(x, y) \longmapsto (x^q, y^q).$$

We know $(y^q)^2 = (x^q)^3 + a^q x^q + b^q$

so $c = a^q$, $d = b^q$.

If want an endomorphism then $F = E$, i.e. we need $a = a^q$, $b = b^q$.

i.e. $a \in \mathbb{F}_q$, $b \in \mathbb{F}_q$.

If a, b are in $\mathbb{F}_q$ but look at E over $\mathbb{F}_q$ or $\overline{\mathbb{F}_q}$.

then $\varphi: \begin{array}{c} E \to E \\ (x,y) \mapsto (x^q, y^q) \end{array}$

is indeed an endomorphism.

Excursion:
automorphism of fields

$$\begin{array}{ll} F & \text{large field} \\ | & \\ k & \text{small field} \end{array}$$

We consider field morphism

$$\varphi : F \longrightarrow F$$

fixing k pointwise.

As the set

$$\{ x \in F \mid \varphi x = x \}$$

always is a subfield of F
we do not loose anything.

Over $k = \mathbb{Q}$ there many fields with even the vector space dimension over $\mathbb{Q}$ being finite:
the automorphism of $F \mid \mathbb{Q}$ form a group: $\mathrm{Gal}(F \mid \mathbb{Q})$.

Over $\mathbb{Q}$: $\mathrm{Gal}(F \mid \mathbb{Q})$ can be very complicated, in particular, it can be non-commutative.

Over $\mathbb{F}_q$: $\mathrm{Gal}(\mathbb{F}_{q^m} \mid \mathbb{F}_q) = \{1, \phi_q, \phi_q^2, \dots, \phi_q^{m-1}\}$
ie. it is not only commutative but even cyclic.

Back to endomorphisms of elliptic curve:

Consider [2]:

$$P \mapsto 2P = \left(\frac{(3x^2+a)^2}{4y^2} - 2x \,,\; -\frac{(3x^2+a)y}{2y^2}\left(\frac{(3x^2+a)^2}{4y^2} - 3x\right) - y \right)$$

Can we simplify this?

$$= \left(\frac{p_1(x,y)}{q_1(x,y)} \,,\; \frac{p_2(x,y)}{q_2(x,y)} \right)$$

Observe that $P \in E$, i.e. $y^2 = x^3 + ax + b$.

$$= \left(\frac{(3x^2+a)^2}{4(x^3+ax+b)} - 2x \,,\; \left(-\frac{(3x^2+a)}{2(x^3+ax+b)} \left(\frac{(3x^2+a)^2}{4(x^3+ax+b)} - 3x \right) - 1 \right) y \right)$$

That's nice :). Can we have "that" for any endomorphism?

Assume we have

$$E \longrightarrow E$$

$$\alpha : \quad (x,y) \longmapsto (R_1(x,y), R_2(x,y))$$

Now:

$$R_1(x,y) = \frac{p_1(x,y)}{q_1(x,y)} = \frac{p_1(x) + p_2(x)y}{q_1(x) + q_2(x)y}$$

with $p_1, p_2, q_1, q_2 \in k[x]$

by replacing y^2 with x^3+ax+b wherever possible.

Expanding with $q_1(x) - q_2(x)y$ allows to get the denominator 'y-free':

$$R_1(x,y) = r_1(x) + r_3(x)\cdot y$$

with $r_1, r_3 \in k(x)$.

Similarly, we can simplify R_2: (quotients in x)

$$R_2(x,y) = r_4(x) + r_2(x)\cdot y$$

with $r_2, r_4 \in k(x)$.

Now, note that α is endo, that is, in particular

$$\alpha(-P) = -\alpha(P).$$

$$\begin{array}{ccc} \| & & \| \\ \alpha(x,-y) & & (R_1(x,y), -R_2(x,y)) \\ \| & & \\ (R_1(x,-y), R_2(x,-y)) & & \end{array}$$

so

$$R_1(x,-y) = R_1(x,y),$$
$$R_2(x,-y) = -R_2(x,y).$$

thus $r_3 = 0$, $r_4 = 0$.

Thus we can always write an endomorphism in the form

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

$$\alpha(x,y) = \left(\frac{p(x)}{q(x)} , \frac{s(x)}{t(x)} \cdot y \right)$$

with $r_1, r_2 \in k(x)$, $p, q, s, t \in k[x]$,

$\gcd(p,q) = 1$, $\gcd(s,t) = 1$.

Now, we can fill in the 'gaps' by declaring

$$\alpha(x,y) := \mathcal{O} \quad \text{if} \quad q(x) = 0.$$

<u>Fact</u> Given E, α as above, $q(x_0) \neq 0$.

Then $t(x_0) \neq 0$.

<u>Pf</u> Since $\alpha(x,y) \in E$ we have

$$\frac{y^2 \, s(x)^2}{t(x)^2} = \frac{\overbrace{p(x)^3 + a p(x) q(x)^2 + b\, q(x)^3}^{=: u(x)}}{q(x)^3}$$

$(x,y) \in E \rightarrow \|$

$$\frac{(x^3 + ax + b)\, s(x)^2}{t(x)^2}$$

Thus $(x^3 + ax + b)\, s(x)^2 \, q(x)^3 = u(x)\, t(x)^2$

where $\gcd(u, q) = 1$.

Now assume $y(x_0) \neq 0$ and $t(x_0) = 0$.

Then x_0 is a double root of $(x^3 + ax + b) \cdot s(x)^2$.

Since x^3+ax+b has no double roots we obtain $s(x_0)=0$. But that is impossible because $\gcd(s,t)=1$. $\square$

For $\alpha=[2]$ we obtain

$$\alpha(P) = \left(\frac{(3x^2+a)^2 - 8x(x^3+ax+b)}{4(x^3+ax+b)} , \right.$$

$$\left. y \cdot \frac{-(3x^2+a)\left((3x^2+a)^2 + 12x(x^3+ax+b) - 8(x^3+ax+b)^2\right)}{8(x^3+ax+b)^2} \right).$$

We see that if $q(x) = 4(x^3+ax+b) = 0$

$$\Updownarrow$$

$$t(x) = 8(x^3+ax+b)^2 = 0,$$

so everything is fine.

For the Frobenius we get – if char $k \neq 2$ –

$$\phi_q(P) = (x^q, y^q)$$
$$= \left(x^q, y(x^3+ax+b)^{\frac{q-1}{2}}\right)$$

so $q(x)=1$, $t(x)=1$,

$p(x)=x^q$, $s(x) = (x^3+ax+b)^{\frac{q-1}{2}}$.

<u>Definition</u>

Degree of an endomorphism $\alpha \neq 0$:

$$\deg \alpha := \max\{\deg p, \deg q\}.$$

Fibers:

$$\alpha^{-1}(Q) = \{P \in E \mid \alpha(P) = Q\},$$

Kernel

$$\ker \alpha := \alpha^{-1}(O).$$

Intuition:

$$\boxed{\#\alpha^{-1}(Q) = \deg \alpha \quad \text{almost always.}}$$

But that's wrong!

$$\phi_q^{-1}(O) = \{O\}: \quad \# \ker \phi_q = 1.$$

but

$$\deg \phi_q = q.$$

<u>Definition</u>

We call α <u>separable</u> iff $\left(\frac{p(x)}{q(x)}\right)' \neq 0$ in $k(x)$.

also all other fibers have one element: if $x^q = a$ for $a \in \mathbb{F}_q$. then $a \in \mathbb{F}_{q^m}$ for some m. Thus $a^{q^m} = a$, now $x = a^{q^{m-1}}$ and unique...

For example, the Frobenius is <u>not</u> separable:

$$(x^q)' = \underbrace{q}_{=0} x^{q-1} = 0$$

On the other hand for $\alpha = [2]$.

Observe: α separable iff $p' \neq 0$ or $q' \neq 0$ in $k[x]$.

[Pf $\left(\frac{p}{q}\right)' = \frac{p'q - pq'}{q^2}$ ...]

For $\alpha = [2]$:

$$q'(x) = 4(3x^2 + a) = 12x^2 + 4a \neq 0.$$

Thus $[2]$ is separable if char $k \neq 2$.

25.11.09

<u>Theorem</u>

Let $\alpha \neq 0$ be a separable endomorphism of an elliptic curve E. Then

$$\# \ker \alpha = \# \alpha^{-1}(Q) = \deg \alpha$$

for $Q \in \operatorname{im} \alpha$. If $\alpha \neq 0$ is not separable then

$$\# \ker \alpha < \deg \alpha.$$

($\ker \alpha = \{ P \in E(\bar{k}) \mid \alpha(P) = \mathcal{O} \}$.

P1

First note that if $Q \in$ im α

$$\# \alpha^{-1}(Q) = \# \alpha^{-1}(\mathcal{O})$$

⌜Assume $Q = \alpha(P)$. Then

$$\begin{aligned} R \in \alpha^{-1}(Q) &\iff Q = \alpha(R) \\ &\iff \alpha(P) = \alpha(R) \\ &\iff \alpha(R-P) = 0 \\ &\iff R - P \in \alpha^{-1}(\mathcal{O}). \end{aligned}$$ ⌟

Write

$$\alpha(x) = (r_1(x), \; r_2(x)y), \quad r_1, r_2 \in k(x),$$

$$r_1(x) = \frac{p(x)}{q(x)}, \quad p, q \in k[x] \text{ coprime}.$$

Choose $(u,v) = \alpha(P)$ "generically", more precisely:

- $u \neq 0$, $v \neq 0$, $(u,v) \neq \mathcal{O}$.
- $\deg(p - uq) \overset{!}{=} \max\{\deg p, \deg q\} = \deg \alpha$.
- $u \notin r_1(S)$ where $S = \{x \in \bar{k} \mid (p'q - pq')(x) \cdot q(x) = 0\}$

Since $\bar{k}$ is infinite this leaves enough choices for (u,v), and S is finite since α is sep.

Note that we have $r_1' \neq 0$.

We actually try find all points in the preimage of (u,v), that is,

$$u = \frac{p(x)}{q(x)} \qquad\qquad v = r_2(x)\, y$$

$$\Updownarrow \qquad\qquad\qquad \Updownarrow$$

$$p(x) - u\, q(x) \overset{(*)}{=} 0 \qquad\qquad y = \frac{v}{r_2(x)}.$$

Thus every root of $(*)$ gives one point in the preimage. Note that since $(u,v) \neq 0$ we have always $q(x) \neq 0$. And since $v \neq 0$, $v^2 = u^3 + a u + b$ we must also have $r_2(x) \neq 0$. Thus we only need to determine the number of solutions of $(*)$. And

$$\deg(p - uq) = \deg \alpha,$$

thus we only need to check that $p - uq$ does not have multiple roots. So consider

$$(p - uq)(x) = 0 \quad , \quad (p' - u q')(x) = 0 .$$

This implies

$$(u\, p'\, q)(x) = (u\, p\, q')(x)$$

Since $v \neq 0$ this means $(p'q - pq')(x) \neq 0$, or $u \in r_1(S)$:

$u = r_1(x)$ with $(p'q - pq')(x) = 0$ i.e. $x \in S$ ↯

Thus $p - uq$ has no multiple roots and so $\alpha^{-1}(u,v)$ has exactly $\deg \alpha$ elements, i.e.

$$\# \alpha^{-1}(u,v) = \deg \alpha$$
$$\shortparallel$$
$$\# \ker \alpha \quad .$$

if α is not separable, we can do everything but $p' = q' = 0$. So

$$p - uq$$

always has multiple roots, and thus

$$\# \ker \alpha < \deg \alpha . \qquad \square$$

<u>Theorem</u>

If $\alpha \neq 0$ is an endo then α is surjective.

<u>Pf</u> Given $(u,v) \in E(\bar{k})$, we are looking for $x_T \in \bar{k}$ such that

$$p(x_T) - u\, q(x_T) = 0 .$$

Note that p or q is non-constant and $p \neq 0$. $\in k[x]$
Thus $p - uq$ is constant for at most one value of u!

In case $p - uq$ is not constant take a root x_1: $p(x_1) - uq(x_1) = 0$.

Necessarily, $q(x_1) \neq 0$ since $\gcd(p,q) = 1$.

Now, $u = \dfrac{p(x_1)}{q(x_1)}$. Then take a root y_1 of $y_1^2 = x_1^3 + ax_1 + b$. Now $\alpha(x_1, y_1) = (u, *)$

Thus $\alpha(x_1, y_1) = (u, v)$ or $\alpha(x_1, y_1) = (u, -v)$

$$\Downarrow$$

$$\alpha(x_1, -y_1) = (u, v).$$

If $p - uq$ is constant, choose

$(u_1, v_1) \in E(\bar{k})$

such that $u_1 \neq u$ (so we can find preimages for (u_1, v_1).)

and $(u,v) + (u_1, v_1) \neq (u, \pm v)$. ie. $(u_1, v_1) \neq -2(u,v)$.

(so we can find a preimage for $(u,v) + (u_1, v_1)$.)

Now, choose P_1 s.t. $\alpha(P_1) = (u_1, v_1)$

P_2 s.t. $\alpha(P_2) = (u, v) + (u_1, v_1)$.

Then $\alpha(P_2 - P_1) = (u, v)$. $\square$

So we now know that

$$\# \alpha^{-1}(Q) = \deg \alpha$$

for every separable $\alpha \neq 0$ for every point $Q \in E(\bar{k})$.

Let's see: which endomorphisms do we know:

scalar mult: $n \in \mathbb{Z}$ $\quad [n]: E(\bar{k}) \to E(\bar{k})$, $P \mapsto nP$

Frobenius: $\quad \phi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$, $(x,y) \mapsto (x^q, y^q)$.

So also $n \in \mathbb{Z}$ $\quad [n] \circ \phi_q = \phi_q \circ [n]$

and $r, s \in \mathbb{Z}$ $\quad r\phi_q + s[1]: E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$, $P \mapsto r\phi_q(P) + sP$

Even ϕ_q^2 would be possible...

but it turns that ϕ_q^2 is one of the endos $r\phi_q + s$

It turns out that these in many cases are all the endomorphisms.

(But not always.)

Repetition

(1) Every endo α is either zero or surjective.

(2) For every separable endo $\alpha \neq 0$ we have

$$\# \ker \alpha = \deg \alpha$$

and for every non-separable endo $\alpha \neq 0$ we have

$$\# \ker \alpha < \deg \alpha.$$

where $\alpha(x,y) = (r_1(x), r_2(x)y)$ is separable iff $r_1' \neq 0$.

and

$$\deg \alpha = \max\{\deg p, \deg q\}$$

where $r_1 = \frac{p}{q}$ with $\gcd(p,q) = 1$.

We have that

$$\alpha = r\varphi_q + s$$

are all endos.

Group endo: ✓

algebraic: Note that φ_q, $[1]$ are algebraic.

Note that

$$+ : \begin{array}{l} E \times E \to E \\ (P, Q) \mapsto P+Q \end{array}$$

is algebraic.

Composing is fine:

$$p\left(\frac{p_1(x,y,\dots)}{q_1(x,y,\dots)}, \dots\right)$$

Thus $[n]$ is algebraic:

$$[n](P) = [n-1](P) + [1](P).$$

$$[-n] = -[n] \text{ and } [0].$$

Now: $r\varphi_q + s = [r] \circ \varphi_q + [s]$.

Side remark:

$$\mathrm{End}(E) := \{\alpha : E \to E \text{ endo}\}$$

is a ring with unit element $[1]$.

under $+$, $\circ$

and also a $\mathbb{Z}$-module.

In many cases

Too many ell. curves.

To be shown later for any ell. curve E.

$$\mathrm{End}(E) = \mathbb{Z}[\varphi_q]$$

$$= \{ r\varphi_q + s \mid r, s \in \mathbb{Z} \}.$$

We are going to prove a criterion for separability of $r\varphi_q + s$:

<u>Theorem</u> Given an elliptic curve E defined over $\mathbb{F}_q$ and $p = \mathrm{char}\, \mathbb{F}_q$, then:

<u>1</u> $r\varphi_q + s$ separable iff $p \nmid s$

We need to have sufficient control about $r_1(x)$ in the endos $r\varphi_q + s$ to decide whether $r_1' = 0$ or not.

We define

$$c_\alpha := \frac{r_1'(x)}{r_2(x)}.$$

This turns out to be constant for all endos α of an ell. curve.

<u>Lemma</u> Let $E: y^2 = x^3 + ax + b$ be an elliptic curve and let $(u,v) \in E$ be any nonzero point. Write

$$(x,y) + (u,v) = (f(x,y), g(x,y))$$

with polynomials $f, g \in k(x,y)$.
Then

$$\frac{\frac{d}{dx} f(x,y)}{g(x,y)} = \frac{1}{y}.$$

This says that the differential

$$\frac{dx}{y} \quad \text{is translation-invariant.}$$

Additionally, one can show that any translation-invariant differential is a multiple of $\frac{dx}{y}$.

<u>Proof</u> (lemma)

We have

$$f(x,y) = m^2(x,y) - x - u$$

$$g(x,y) = -m(x,y)(f(x,y) - u) - v$$

with

$$m(x,y) = \frac{y-v}{x-u}.$$

Now compute

$$y \frac{d}{dx} f(x,y) - g(x,y)$$

$$= y\,(f_x(x,y) + f_y(x,y)\,y') - g(x,y).$$

Using $2y'y = 3x^2 + a$,

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

$$v^2 = u^3 + au + b,$$

this expression simplifies to zero. $\square$

<u>Lemma</u> Let $\alpha_1, \alpha_2, \alpha_{1+2}$ and $\alpha_{1\circ 2}$ be endomorphisms of an ell. curve with

$$\alpha_{1+2} = \alpha_1 + \alpha_2,$$

$$\alpha_{1\circ 2} = \alpha_1 \circ \alpha_2.$$

Assume that c_{α_1} and c_{α_2} are both constant. Then

$$c_{\alpha_{1+2}} = c_{\alpha_1} + c_{\alpha_2},$$

$$c_{\alpha_{1\circ 2}} = c_{\alpha_1} \cdot c_{\alpha_2}.$$

In particular, they are also constant.

By the above (unproven) remark any α has c_α constant:

$\frac{dx}{y} \circ \alpha$ is translation-invariant

and thus $\frac{dx}{y} \circ \alpha = \hat{c}_\alpha \cdot \frac{dx}{y}$ for some constant $\hat{c}_\alpha$. And $\hat{c}_\alpha = c_\alpha$.

<u>Proof</u> Write $\alpha_j(x,y) = (r_{1j}(x), \overbrace{r_{2j}(x)\,y}^{=y_j})$,

and $(x_j(x,y), y_j(x,y)) = \alpha_j(x,y)$,

so

$$\alpha_{1+2}(x,y) = (x_1, y_1) + (x_2, y_2).$$

$$\frac{\partial}{\partial x} x_{1+2} = \frac{\partial x_{1+2}}{\partial x_1} \cdot \frac{\partial x_1}{\partial x} + \frac{\partial x_{1+2}}{\partial x_2} \cdot \frac{\partial x_2}{\partial x}$$

by chain rule:

$$\begin{tikzcd} & E \arrow[dr, bend left, "\alpha_1"] & \\ E \arrow[ur, bend left, "\alpha_1"] \arrow[dr, bend right, "\alpha_2"'] & x & E \\ & E \arrow[ur, bend right, "+"'] & \end{tikzcd}$$

By the previous Lemma we have

$$\frac{\partial x_{1+2}}{\partial x_1} = \frac{y_{1+2}}{y_1}$$

taking $(v,v) = (x_2, y_2)$.

Similarly: $\frac{\partial x_{1+2}}{\partial x_2} = \frac{y_{1+2}}{y_2}$.

By assumption

$$\frac{\partial x_1}{\partial x} = \frac{\partial r_{11}(x)}{\partial x} = c_{\alpha_1} \cdot \underbrace{r_{21}(x)}_{\frac{y_1}{y}}$$

$$= c_{\alpha_1} \cdot \frac{y_1}{y}$$

thus

$$\frac{\partial x_{1+2}}{\partial x} = c_{\alpha_1} \cdot \frac{y_{1+2}}{y_1} \cdot \frac{y_1}{y} + c_{\alpha_2} \cdot \frac{y_{1+2}}{y_2} \cdot \frac{y_2}{y}$$

$$= (c_{\alpha_1} + c_{\alpha_2}) \cdot \frac{y_{1+2}}{y}$$

that is:

$$\underbrace{\frac{\frac{\partial}{\partial x} x_{1+2}}{y_{1+2}/y}}_{= c_{\alpha_{1+2}}} = c_{\alpha_1} + c_{\alpha_2}$$

For x_{102} we have $x_{102} = x_1 \circ x_2$.

$$\alpha_{102}(x, y) = \alpha_1(\underbrace{\alpha_2(x, y)}_{= (r_{12}(x), \dots)}) = (\overbrace{r_{11}(r_{12}(x))}^{x_{102}}, \dots)$$

x_1 x_2

We get

$$\frac{\partial x^*_{102}}{\partial x} = \frac{\partial x_{102}}{\partial x_2} \cdot \frac{\partial x_2}{\partial x}$$

We have $$\frac{\partial x_2}{\partial x} = c_{\alpha_2} \cdot \frac{y_2}{y}.$$

and

$$\frac{\partial x_{102}}{\partial x_2} = \frac{\partial x_1}{\partial x}\bigg|_{x = x_2}$$

$$= \left(c_{\alpha_1} \cdot \frac{y_1}{y} \right)\bigg|_{x = x_2}$$

$$= \underbrace{c_{\alpha_1}\big|_{x = x_2}}_{= c_{\alpha_1}} \cdot \frac{y_{102}}{y_2}$$

because it is constant.

so

$$\frac{\partial x_{102}}{\partial x} = c_{\alpha_1} \frac{y_{102}}{y_2} \cdot c_{\alpha_2} \cdot \frac{y_2}{y}$$

$$= \underbrace{c_{\alpha_1} \cdot c_{\alpha_2}}_{c_{\alpha_{102}}} \cdot \frac{y_{102}}{y}$$

$\square$

Now consider

$$\alpha = r\varphi_q + s.$$

Observe that

$$c_{[1]} = \frac{x'}{y/y} = 1,$$

and
$$c_{\varphi_q} = \frac{(x^q)'}{y^q/y} = \frac{q \cdot x^{q-1}}{y^{q-1}} = 0.$$
$= 0 \in k$.

Thus we conclude:

<u>Lemma</u> Let E be an ell. curve def'd over a field $\mathbb{F}_q$ of characteristic p, and $r, s \in \mathbb{Z}$. Then

- $r\varphi_q + s$ is an endo of E, and nonzero ~~iff~~ $(r,s) \neq (0,0)$.
- $c_{r\varphi_q + s} = s$.
- $r\varphi_q + s \cdot 1$ is separable iff $p \nmid s$.

<u>Pf.</u>
$$c_{r\varphi_q + s} = c_r \cdot \underbrace{c_{\varphi_q}}_{=0} + c_s = c_s \underset{\text{induction}}{=} s$$

and
$$c_{r\varphi_q + s} = \frac{r_1'(x)}{r_2(x)} \quad \text{for } (r\varphi_q + s)(x,y) = (r_1(x), r_2(x)y)$$

so $r_1' = 0$ iff $c_{r\varphi_q + s} = 0 \in \mathbb{F}_q$.
iff $p \nmid s$

$\square$

Torsion

The order of an element P of a group E is the smallest positive integer ℓ such that $\ell P = O$.

We define the ℓ-torsion

$$E[\ell] := \{ P \in E(\bar{k}) \mid \ell P = O \}.$$
$$= \ker[\ell]$$

Eg. $E[4]$ contains all 4-~~torsion~~ order, 2-~~torsion~~ order

a 1-order element

$$4P = O, \quad 2P = O, \quad P = O.$$

Our aim is the structure (and size) of $E(\mathbb{F}_q)$ for some field $\mathbb{F}_q$ over which E is defined.

Obviously:

$$E(\mathbb{F}_q)[\ell] \trianglelefteq E(\bar{\mathbb{F}}_q)[\ell].$$
$$\parallel$$
$$E[\ell].$$

Since $E(\mathbb{F}_q)$ is finite we can pick an appropriate ℓ to learn its entire structure. [Eg. $\ell = \# E(\mathbb{F}_q)$.]

As we do not get know the degree of $[\ell]$, we do not get know $\# E[\ell] = \# \ker[\ell] \underset{\uparrow}{=} \deg \ell$.

<u>1 - torsion</u> $E[1] = O = \{O\}$ if $p \nmid \ell$.

<u>2 - torsion</u>

$$E[2] = \{ P \in E \mid 2P = O \} \qquad E : y^2 = x^3 + ax + b$$

Now either $P = O$ or

$$2P = \left(m^2 - 2x \ , \ -m(m^2 - 3x) - y \right)$$

with $m = \dfrac{3x^2 + a}{2y}$.

so $2P = O$ iff $4y^2 = 0$ iff $y = 0$.

iff $x^3 + ax + b = 0$

Thus $E[2] = \{O\} \cup \{ (x,0) \in \bar{k}^2 \mid x^3 + ax + b = 0 \}$.

In particular. $\# E[2] = 4$

So $E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

UNLESS... char $k \neq 2, 3$.

Side remark:

<u>Fundamental theorem on finitely generated abelian groups</u>

If G is a finitely generated abelian group then

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_s} \times \mathbb{Z}^r$$

for some $r, s \in \mathbb{N}$, $m_i \in \mathbb{N}_{\geq 2}$, and ...

For char $k=3$ we can do the same as there every curve can be put the form

$$E: y^2 = x^3 + a_2 x^2 + a_4 x + a_6$$

and so

$$2P = \mathcal{O} \iff P = -P$$
$$\iff y = 0$$
$$\iff x^3 + a_2 x^2 + a_4 x + a_6 = 0.$$

$$\rightsquigarrow \quad E[2] = \{\mathcal{O}\} \cup \{(x,0) \mid \quad \}$$

$$\# E[2] = 4$$

$$\rightarrow \quad E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

For char $k=2$ the situation is different:

$\underline{y^2 + xy = x^3 + a_2 x^2 + a_6}$, ~~$\Delta = a_6 \neq 0$~~

$$-P = (x, x+y)$$

so $P = -P \iff x = 0$

$$\iff x = 0 \wedge y^2 = a_6.$$
$$\iff x = 0,\ y = \sqrt{a_6}$$

Thus $E[2] = \{\mathcal{O}, (0, \sqrt{a_6})\} \cong \mathbb{Z}_2.$

$\underline{y^2 + a_3 y = x^3 + a_4 x + a_6,\ a_3 \neq 0}$

$$-P = (x, a_3 + y)$$

so $P = -P \iff a_3 = 0$

Thus $E[2] = \{\mathcal{O}\} = 0$

<u>Proposition</u> E/k. Then

(i) char $k = 2$ we have $E[2] \cong 0$ or $E[2] \cong \mathbb{Z}_2$

(ii) char $k \neq 2$ we have $E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Actually, $\deg [2] = 4$ in all cases.

<u>3-torsion</u>

We could calculate

$$[3]P = (\text{some polynomial in } x, \ldots)$$

but it's much easier to solve

$$2P = -P$$

$$x(2P) = m^2 - 2x \quad \text{with} \quad m = \frac{3x^2+a}{2y}$$

~~$y(2P) =$~~

Observe that $y(2P) \neq y(P)$ if $\underbrace{x(2P) = x(-P)}_{\Downarrow}$

$$2P = -P \Leftarrow 2P = \pm P$$

unless $P = O$.

So $2P = -P \wedge P \neq O$

$$\Leftrightarrow \quad \underset{\substack{\shortparallel \\ m^2 - 2x}}{x(2P)} = x$$

$$\Leftrightarrow \quad m^2 = 3x.$$

$$\Leftrightarrow \quad -(3x^2+a)^2 + 12x(x^3+ax+b) = 0$$

$$\Leftrightarrow \quad 3x^4 + 6ax^2 + 12bx - a^2 = 0$$

Unless char $k = 3$ (or 2) this is a degree 4 equation. Its discriminant is

$$\underbrace{-6912}_{2^8 \cdot 3^3} \cdot \Delta^2, \text{ so } \neq 0.$$

Thus there four solutions. For each such x_1 the term $x_1^3 + a x_1 + b \neq 0$. (Otherwise the curve is non-smooth.) So $y^2 = x_1^3 + a x_1 + b$ has two solution for every such x_1. Thus we find eight points of order 3:

$$\# E[3] = \{O\} \cup \left\{ (x,y) \;\middle|\; \begin{array}{l} -(3x^2+a) \\ +2x(x^3+ax+b) = 0, \\ y^2 = x^3 + ax + b \end{array} \right\}$$

$$\# E[3] = 9$$

and so

$$E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3 .$$

unless char $k \neq 2, 3$.

<u>Case char $k = 3$</u>

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6$$

$$\underset{P \neq O}{2P = -P} \iff m^2 - a_2 - 2x = x, \quad m = \frac{2a_2 x + a_4}{2y}$$

$$\iff a_2 x^3 + (a_2 a_6 - a_4^2) = 0$$

Since $\# E[3]$ must be a 3-power, this equation cannot have three solution. Actually, in case $a_2 \neq 0$:

$$a_2 \left(x + \sqrt[3]{\frac{a_2 a_6 - a_4^2}{a_2}} \right)^3 = 0$$

so we have a single solution.

and then $E[3] \cong \mathbb{Z}_3$

If however $a_2 = 0$ then $-a_4^2 = 0$

but this contradicts $\Delta \neq 0$.

and so $E[3] = \{O\}$ here.

$(x^p)' = p x^{p-1} = 0$ in char $k = p$.

<u>Proposition</u> E/k. Then

(i) char $k = 3$ we have $E[3] \cong 0$ or $E[3] \cong \mathbb{Z}_3$.

(ii) char $k \neq 3$ we have $E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

4-torsion $\to$ Exercise.

General case

<u>Def</u> We call an elliptic curve E/k

- <u>ordinary</u> iff $E[p] \cong \mathbb{Z}_p$, and
- <u>supersingular</u> iff $E[p] \cong O$,

where $p = \text{char } k$.

<u>Theorem</u> E/k, char $k = p$, $n \in \mathbb{N}_{>0}$.

Then

(i) if $p \nmid n$ then $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$.

(ii) If $p = n$ then $E[p] = O$ or $E[p] \cong \mathbb{Z}_p$.

In general, we write $n = p^r n'$ with $p \nmid n'$.

If E is ordinary: $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_{n'}$.

If E is supersingular: $E[n] \cong \mathbb{Z}_{n'} \times \mathbb{Z}_{n'}$.

CC
08.12.09
(7)

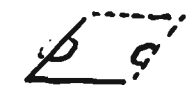
$$[n]P = \left(\frac{\varphi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3} \right)$$

Tricky! part!

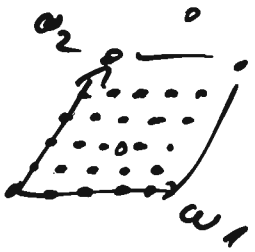
ψ_n is given by a recursion

$$\begin{cases} \psi_{2m} = f(\psi_m, \psi_{m\pm1}, \psi_{m\pm2}) \\ \psi_{2m+1} = g(\ \ \ \ \ \ \ \ ) \end{cases}$$

$$\varphi_n = h(\psi_m, \psi_{m\pm1})$$

$E|\mathbb{C}$: $\mathbb{C}^*/\omega_1\mathbb{Z}+\omega_2\mathbb{Z} \simeq$ 
Torus

for some $\omega_1, \omega_2 \in \mathbb{C}$ $\mathbb{R}$-lin. indep.



Here, 5-torsion is $\mathbb{Z}_5 \times \mathbb{Z}_5$

Trying to find meromorphic function that doubly periodic we find one particular: the Weierstraß $\wp$ - function

It has a double pole at 0
and single zeroes at $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$.

Now it turns out that

$$\wp'^2 = a_0 \wp^3 + a_2 \wp^2 + a_4 \wp + a_6 .$$

Thus

$$\mathbb{C}/\omega_1\mathbb{Z}+\omega_2\mathbb{Z} \longrightarrow E$$

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

This turns out to be an isomorphism of ~~groups~~ and algebraic....

ccc
~~08.12.09~~
~~9~~
09.12.09
1

The proof is long and will occupy us for some time.

For now:

Assume you have an endomorphism

$$\alpha : E \longrightarrow E .$$

It induces:

$$\alpha_n : E[n] \longrightarrow E[n]$$
$$P \longmapsto \alpha(P)$$

i.e.

$$nP = O \implies n\alpha(P) = \alpha(nP) = \alpha(O) = O$$

Now assume we already know the Theorem:

$$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$$

in case $p \nmid n$.

So we can choose $Q_1, Q_2 \in E[n]$ such that every point $P \in E[n]$ can be write uniquely as

$$P = \kappa_1 Q_1 + \kappa_2 Q_2$$

with $\kappa_1, \kappa_2 \in \mathbb{Z}/n = \mathbb{Z}_n$.

So $\alpha(\kappa_1 Q_1 + \kappa_2 Q_2) = \kappa_1 \alpha(Q_1) + \kappa_2 \alpha(Q_2)$

and $\alpha(Q_1) = a Q_1 + c Q_2$, $\alpha(Q_2) = b Q_1 + d Q_2$.

So

$$\alpha(r_1 Q_1 + r_2 Q_2) = (a r_1 + b r_2) Q_1 + (c r_1 + d r_2) Q_2$$

in other words:

$$\alpha_n = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

This will allow us to study, say,

$\operatorname{tr} \alpha_n$ and $\det \alpha_n$.

$\operatorname{tr} \alpha_n = a + d$

ecc $\rightarrow$ $\varphi_q^2 - t\varphi_q + q = 0$ ...

This will very helpful to study the Frobenius later on. ...

We can actually also use $\sigma \in \mathrm{Gal}(\bar{k}|k)$

this induces a group endo of E, which in turn induces a group endo of the n-torsion $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$.

Thus we obtain a <u>representation</u>

$$\mathrm{Gal}(\bar{k}|k) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_n} E[n] \cong \mathrm{Aut}_{\mathbb{Z}_n} \mathbb{Z}_n^2 = GL_2 \mathbb{Z}_n.$$

$$\sigma \longmapsto \sigma_n$$

It is clearly a group morphism.

Now observing that

$$E[n] = \ker [n].$$

we see that we need to know more about $[n]$. We know that this endo is separable iff $p \nmid n$.

So in essence we only need to know the degree of $[n]$.

By inspection we find

$$\deg [2] = 4,$$
$$\deg [3] = 9.$$

So we conjecture $\deg [n] = n^2$.

To prove this we need to determine polynomials such that

$$n \cdot (x,y) = \left(\frac{\varphi_n(x)}{q_1(x)}, \frac{\omega_n(x,y)}{q_2(x,y)} \right)$$

We also observed that if $q_1(x) = \psi_n(x,y)^2$ then we should find $q_2(x,y) = \psi_n(x,y)^3$.

These polynomials $\varphi_n, \omega_n, \psi_n$ will be defined now:

Def <u>Division polynomials</u>

"Given" $E: y^2 = x^3 + ax + b$
we define polynomials $\psi_n \in \mathbb{Z}[a, b, x, y]$.

$$\psi_0 = 0 \qquad \psi_{-n} = -\psi_n .$$

$$\psi_1 = 1$$

$$\psi_2 = 2y$$

$$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$$

$$\psi_4 = 4y\left(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3\right)$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \geq 2,$$

$$\psi_{2m} = \frac{1}{2y}\psi_m \cdot \left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right) \quad \text{for } m \geq 3.$$

$$\phi_n := x\psi_n^2 - \psi_{n+1}\psi_{n-1} \quad \text{for } n \in \mathbb{Z}.$$

$$\omega_n := \frac{1}{4y}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right) \quad \text{for } n \in \mathbb{Z}.$$

Notice $\omega_n = \dfrac{\psi_{2n}}{2\psi_n}$

Notice that this defines all the polynomials

ψ_n, ϕ_n, ω_n.

Lemma Denote $R := \mathbb{Z}[a, b, x, y^2]$

(i) $$\psi_n \in \begin{cases} 2yR & n \equiv_2 0, \\ R & n \equiv_2 1. \end{cases}$$

(ii) The weighted degree of ψ_n is $n^2 - 1$ where $\operatorname{wdeg} x = 2$, $\operatorname{wdeg} y = 3$.

(iii) $$\psi_n \in \begin{cases} 4yR & \text{if } n \equiv_4 0, \\ (x^2+a)^{\frac{n^2-1}{4}} + 2R & \text{if } n \equiv_4 1, \\ 2y(x^2+a)^{\frac{n^2-4}{4}} + 4yR & \text{if } n \equiv_4 2, \\ (x^2+a)^{\frac{n^2-1}{4}} + 2R & \text{if } n \equiv_4 3. \end{cases}$$

and the leading term is $y \times x^{\frac{n^2-1}{2}}$ if $n \equiv_2 0$, $x^{\frac{n^2-1}{2}}$ if $n \equiv_2 1$.

[Notice (iii) => (i).]

(iv) $\phi_n \in R$.

(v) $$\omega_n \in \begin{cases} R & \text{if } n \equiv_2 0, \\ yR & \text{if } n \equiv_2 1. \end{cases}$$

~~(vi)~~ Notice that ϕ_n and ψ_n^2 are in R, so we can rewrite them as polynomials in $\mathbb{Z}[a, b, x]$ by replacing y^2 with $x^3 + ax + b$.

(vi) For every $a, b \in k$ with $\Delta = -16(4a^3 + 27b^2) \neq 0$ we have that

$$\phi_n, \psi_n^2 \in k[x]$$

are coprime.

Proof ....

(ii) The claim is that

$$\text{let } \psi_n = \begin{cases} n\, y\, x^{\frac{n^2-4}{2}} & \text{if } n \equiv_2 0, \\ n\, x^{\frac{n^2-1}{2}} & \text{if } n \equiv_2 1. \end{cases}$$

We have to consider $n \leq 4$ ... done ✓

And now consider cases according to $n \bmod 4$:

$\underline{n \equiv_4 2}$, i.e. $n = 2m$ with $m \equiv_2 1$.

Now

$$\psi_n = \psi_{2m} = \frac{1}{2y}\, \psi_m \left(\psi_{m+2}\, \psi_{m-1}^2 - \psi_{m-2}\, \psi_{m+1}^2 \right)$$

let $\psi_m \psi_{m+2} \psi_{m-1}^2$

$$= m\, x^{\frac{m^2-1}{2}} \cdot (m+2)\, x^{\frac{(m+2)^2-1}{2}} \cdot (m-1)^2 y^2 x^{\frac{(m-1)^2-4}{1}}$$

$$= m\,(m+2)(m-1)^2 \cdot y^2\, x^{\frac{n^2-4}{2}}$$

let $\psi_m \psi_{m-2} \psi_{m+1}^2$

$$= m\, x^{\frac{m^2-1}{2}} \cdot (m-2)\, x^{\frac{(m-2)^2-1}{2}} \cdot (m+1)^2 y^2\, x^{\frac{(m+1)^2-4}{1}}$$

$$= m\,(m-2)(m+1)^2 \cdot y^2\, x^{\frac{n^2-4}{2}}$$

... $\square$

let $\left(\psi_m \left(\psi_{m+2}\, \psi_{m-1}^2 - \psi_{m-2}\, \psi_{m+1}^2 \right) \right)$

$$= \underbrace{m\left[(m+2)(m-1)^2 - (m-2)(m+1)^2 \right]}_{= 4m = 2n} \cdot y^2\, x^{\frac{n^2-4}{2}}$$

and so let ψ_n is as claimed.

Part (vi) of the Lemma is still open.

ECC
09.12.09
7

<u>Theorem</u> Give $E: y^2 = x^3 + ax + b$

then
$$n \cdot (x,y) = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)} \right).$$

By the lemma we see that

$$\phi_n \in R, \quad \psi_n^2 \in R$$

$$\frac{\omega_n}{\psi_n^3} \in y \cdot \text{Quot } R$$

so we get the form that we expect.
It is straightforward to check the theorem for some small n.

You may want to do induction on n.
Now we try to get

$$(n+1) \cdot (x,y)$$

from $n \cdot (x,y)$ and (x,y)

Distinguish cases $n \bmod 2$: $n \equiv_2 0$,
ie. $n = 2m$.

Actually

$$\psi_n^2 = n^2 \prod_{\substack{P \in E[n] \\ \neq \\ \mathcal{O}}} (x - x(P))$$

To prove Lemma (vi) Washington uses the Theorem.
Then he takes the smallest n such that ϕ_n and ψ_n^2 have a common zero.
In case $n = 2m$ we now write

$$(*) \qquad \frac{\phi_{2m}}{\psi_{2m}^2} = \frac{\phi_2}{\psi_2^2}\left(\phi_m / \psi_m^2\right)$$

explicit: $\dfrac{\phi_2}{\psi_2^2} = \dfrac{(3x^2+a)^2}{4(x^3+ax+b)} - 2x$

which should hold because of the Theorem!

I'd like to prove eg. $(*)$ only based on the defining recursions.

Cassels (1966): ... can be done with some trouble by induction..

Let's assume Lemma and Theorem are proved.

In particular:

$$n \cdot (x,y) = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \dots \right)$$

and

$$\deg \psi_n^2 = n^2 - 1, \qquad \operatorname{wdeg} \psi_n = n^2 - 1$$

$$\deg \phi_n = \deg\left(x\,\psi_n^2 - \psi_{n+1}\psi_{n-1} \right)$$

$$\text{wdegs: } \underbrace{2 \quad 2(n^2-1)}_{2n^2} \qquad \underbrace{(n+1)^2-1 \quad (n-1)^2-1}_{2n^2}$$

$$\text{lt } \phi_n: \quad \text{lt } x\psi_n^2 = n^2 \cdot x^{n^2} \longrightarrow \text{lt } \psi_n^2 = n^2 x^{n^2-1}$$

$$\text{lt } \psi_{n+1}\psi_{n-1} = (n+1)(n-1)\, x^{n^2}$$

$$\text{lt } \phi_n = x^{n^2}.$$

Thus $\deg \phi_n = n^2$.

Thus

$$\deg [n] \underset{\text{Lemma (vi)}}{=} \max\{ \underbrace{\deg \phi_n}_{n^2}, \underbrace{\deg \psi_n^2}_{n^2-1} \}$$

$$= n^2.$$

!

Corollary

$$\deg [n] = n^2. \qquad \square$$

Corollary

$$\# E[n] = \# \ker [n] = \deg [n] = n^2$$

in case $p \nmid n$

Proof (older Theorem, ~~ob~~ $p \nmid n$):

The claim is that
$$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n.$$

For n prime this is obvious using the previous Corollary.

Now, $E[n]$ is a finite abelian group in the general case:

$$E[n] \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_r}$$

with $n_r \mid n_{r-1} \dots n_2 \mid n_1$.

~~Then~~ take $\ell \mid n_r$ prime.

Then $E[\ell] \cong \underbrace{\mathbb{Z}_\ell \times \dots \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell}_{r \text{ factors.}}$

But we know $\# E[\ell] = \ell^2$ so $r = 2$.

So $E[n] = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $n_2 \mid n_1 \mid n$.

and $\# E[n] = n^2$ so $n_1 = n_2 = n$. $\square$

The Weil pairing

Assume $p \nmid n$.

Then $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$

say $\{T_1, T_2\}$ is a $\mathbb{Z}_n$-basis of $E[n]$.

Scalar product?

$$e : E[n] \times E[n] \longrightarrow G.$$

It is enough to fix

$$e(T_i, T_j)$$

Then – desiring bilinearity –

$$e(s_1 T_1 + s_2 T_2, t_1 T_1 + t_2 T_2)$$

$$= \sum_{i,j} s_i \, e(T_i, T_j) \, t_j$$

Moreover, we want that e is non-degenerate

$$\forall S: e(S, T) = 0 \Rightarrow T = 0.$$

Well... unfortunately, such a construction much about other properties of E... like algebraicity. Or, how behaves e with respect to endos?

ECC
15.12.09
2

In this light it's only a minor difficulty to switch to a multiplicatively written group G:

$$\mu_n := \{ x \in \bar{k} \mid x^n = 1 \}$$

Theorem

THEOREM 2.27 (Weil pairing). res:weil-exists *Let E be an elliptic curve defined over a field k and let n be a positive integer coprime to the characteristic of k. Then a* Weil pairing

$$e_n \colon E[n] \times E[n] \longrightarrow \mu_n$$

satisfying the following properties exists.

res:weil-bilinear *(i) e_n is bilinear, that is, for all $S, S_1, S_2, T, T_1, T_2 \in E[n]$*

$$e_n(S_1 + S_2, T) = e_n(S_1, T) \cdot e_n(S_2, T),$$
$$e_n(S, T_1 + T_2) = e_n(S, T_1) \cdot e_n(S, T_2).$$

res:weil-nondegenerate *(ii) e_n is non-degenerate, that is, for all $T \in E[n]$*

$$\forall S \in E[n] \colon e_n(S, T) = 1 \implies T = \mathcal{O},$$
$$\forall S \in E[n] \colon e_n(T, S) = 1 \implies T = \mathcal{O}.$$

res:weil-antisymmetric *(iii) e_n is antisymmetric, that is, for all T*

$$e_n(T, T) = 1.$$

In particular, $e_n(T, S) = e_n(S, T)^{-1}$.

res:weil-galoiscompatible *(iv) e_n is compatible with the Galois actions, that is, for every automorphism σ of $\bar{k}$ fixing k (in particular, for a curve in Weierstraß form this means that $\sigma(a) = a$ and $\sigma(b) = b$) we have*

$$e_n(\sigma S, \sigma T) = \sigma(e_n(S, T)).$$

res:weil-endocompatible *(v) For every endomorphism α of E we have*

$$e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg \alpha}.$$

We don't give a proof here.
To define it we need more information about functions living on the curve.
Given $S, T \in E[n]$.
One constructs an algebraic function g_T on the curve such that

each T' with $nT' = T$
is a single zero of g_T

and each T_0 with $nT_0 = O$
is a single pole of g_T,

and no other poles ~~or~~ zeroes.
Then we define

$$e_n(S, T) = \frac{g_T(S + P)}{g_T(O + P)}$$

for some P such that
$O + P$ and $S + P$ are neither
poles nor zeroes of g_T.

Tricky: $\exists g_T$? e_n well-def'd?

e_n bilinear?:

$$e_n(S_1 + S_2, T) = \frac{g_T(S_1 + (S_2 + P))}{g_T(S_2 + P)} \cdot \frac{g_T(S_2 + P)}{g_T(O + P)}$$

$$= e_n(S_1, T) \cdot e_n(S_2, T)$$

Other points are more tricky...

There is a different construction to obtain another pairing:
the Tate-Lichtenbaum pairing $\langle \cdot , \cdot \rangle_n$ which is bit easier to construct and evaluate. The connection is given by an equation of the form

$$e_n(S,T) \underset{\substack{\uparrow \\ \text{modulo} \\ n\text{th powers.}}}{\sim} \frac{\langle S,T\rangle_n}{\langle T,S\rangle_n}$$

In particular, we want and have

$$\langle T,T\rangle_n \neq 1.$$

<u>One consequence</u>: computing discrete logs in E is at most as difficult as computing discrete logs in μ_n:
If $Q = sP$ then

$$e_n(Q,T_i) = e_n(P,T_i)^s$$

so unless $e_n(P,T_i)$ is trivial solving the new equation provides information about s, probably modulo n.

In $\bar{k}$ one often has much faster dlog-algorithms. In particular in $\mathbb{Z}_p^\times$ we can find dlogs in time

$$2^{\leq 2} \uparrow c \cdot (\log_2 p)^{1/2} (\log_2 \log_2 p)^{1/2}$$

(even: $1/3$, $2/3$)

However, the 'size' of elements in μ_n is much larger than the 'size' of elements in $E(\mathbb{F}_q)$.

You need to embed $\mu_n \subset \mathbb{F}_{q^e}$.

For a random curve E we expect $e \in O(q)$

$x^n - 1 \mid x^{q^e} - x$

So already to store μ_n we would need $q \cdot \log_2 q$ bits. :(

But there some curves with small e

e.g. $e = 2, 3, 4, 6, 12, 24$.

Note that n depends on the curve because we want

$$E(\mathbb{F}_q)[n] \neq \{\mathcal{O}\} \text{ or even: } n \mid \# E(\mathbb{F}_q).$$

Corollary

Let $\{T_1, T_2\}$ be $\mathbb{Z}_n$-basis of $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$.

Then $e_n(T_1, T_2)$ is a primitive n-th root of unity.

"basis $\to$ basis".

Pf Consequence of the non-degeneracy:

Let $\zeta = e_n(T_1, T_2)$.

Clearly, $\zeta \in \mu_n$.

Assume $\zeta^d = 1$ for $d \mid n$.

We have to show $d = n$.

Consider $T = dT_2$.

Then $e_n(T_1, dT_2) = e_n(T_1, T_2)^d = \zeta^d = 1$.

and $e_n(T_2, dT_2) = 1^d = 1$.

Thus

$$e_n(s_1 T_1 + s_2 T_2, dT_2)$$
$$= e_n(T_1, dT_2)^{s_1} e_n(T_2, dT_2)^{s_2} = 1.$$

Thus $dT_2 = \mathcal{O}$.

Since T_1, T_2 generate $E[n]$ we must have $d = n$. $\square$

In particular, note that the Weil pairing is not unique.

Take r coprime to n.

Then with ζ also ζ^r is n-pru. (primitive root of unity)

And e_n is defined by fixing

$$e_n(T_1, T_2).$$

Thus with $e_n(S,T)$ is a Weil pairing

also $e_n(S,T)^r$ is a Weil pairing.

Te:
$$e_n(T_1, T_2) = \zeta.$$
$$e_n(T_1, T_2)^r = \zeta^r.$$

This may prove the existence theorem... Ex?

However, we later need a construction to <u>compute</u> e_n efficiently.

<u>Corollary</u>

If $E[n] \subseteq E(k)$ then $\mu_n \subseteq k$.

Notice that this applies also to extensions of k.

<u>Pf</u> $\underset{\substack{\uparrow \\ n\text{-prim}}}{\zeta} = e_n(T_1, T_2)$ as before.

Thus it is enough to show $\zeta \in k$.

~~Note~~ Notice that $k(\zeta) \,|\, k$ is Galois.

So take $\sigma_0 \in Gal(k(\zeta) \,|\, k)$

extend it to $\sigma \in Gal(\bar{k} \,|\, k)$

By the Weil pairing existence theorem we obtain

$$\zeta = e_n(T_1, T_2)$$
$$\parallel$$
$$e_n(\sigma T_1, \sigma T_2) = \sigma \zeta = \sigma_0 \zeta.$$

Thus – since this holds for any σ_0 – we obtain $\zeta \in k$. $\square$

For example, over a finite field $\mathbb{F}_q$ it is easy to decide when $\mu_n \subseteq \mathbb{F}_{q^e}$ because

$$\zeta^n = 1 \quad \text{and} \quad x^{q^e - 1} = 1 \text{ for any } x \in \mathbb{F}_{q^e}^\times.$$

i.e. $n \mid q^e - 1$ or $q^e \equiv_n 1$

Thus the smallest possible e is $e = \mathrm{ord}_{\mathbb{Z}_n} q$.

Since only μ_1 and μ_2 are in $\mathbb{Q}$ we immediately get:

<u>Corollary</u>

If $E \mid \mathbb{Q}$. Then for $n \geq 3$ we have

$$E[n] \not\subseteq E(\mathbb{Q}).$$

We can have $E[2] \subseteq E(\mathbb{Q})$,

e.g. $y^2 = x(x-1)(x-2)$ then

$$E[2] = \{ \mathcal{O}, (0,0), (1,0), (2,0) \}.$$

However:

for $n > 12$ or $n = 11$ we even have:

$$E(\mathbb{Q})[n] = \{\mathcal{O}\}.$$

for all other n one can construct curves with $E(\mathbb{Q})[n] \neq \{\mathcal{O}\}$.

Proposition

Let α an endo of E/k.
$n \in \mathbb{Z}$ coprime to char k.
Then
$$\deg \alpha \equiv_n \det(\alpha_n)$$

Pf Fix T_1, T_2 basis of $E[n]$,
then $\zeta = e_n(T_1, T_2)$ is n-prim.

Let $\alpha_n = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be the matrix of α on the n-torsion w.r.t. the basis T_1, T_2.

Now:
$$e_n(\alpha(T_1), \alpha(T_2))$$
$$= e_n(aT_1 + cT_2, bT_1 + dT_2)$$
$$= e_n(T_1, T_2)^{ad-bc}$$
$$= \zeta^{ad-bc}$$

On the other hand side:
$$e_n(\alpha(T_1), \alpha(T_2)) = e_n(T_1, T_2)^{\deg \alpha} = \zeta^{\deg \alpha}.$$

Thus $\zeta^{\deg \alpha} = \zeta^{ad-bc}$, and since ord $\zeta = n$ we obtain the claim

$\square$

<u>Proposition</u>

Let α, β be endos of $E|k$,
$a, b \in \mathbb{Z}$.

Then

$$\deg(a\alpha + b\beta)$$
$$= a^2 \deg \alpha$$
$$+ b^2 \deg \beta$$
$$+ ab\,(\deg(\alpha+\beta) - \deg\alpha - \deg\beta).$$

Pf Fix a number n coprime to char k.

Then
$$(a\alpha + b\beta)_n = a\,\alpha_n + b\,\beta_n.$$

Now check that for 2×2-matrices we have

$$\det(a\alpha_n + b\beta_n) = a^2 \det\alpha_n$$
$$+ b^2 \det\beta_n$$
$$+ ab\,(\det(\alpha_n+\beta_n) - \det\alpha_n - \det\beta_n)$$

(Enough to check the cases $a=0$, $b=0$, $a=b=1$.)

Thus by the previous proposition:

$$\deg(a\alpha + b\beta) \equiv_n a^2 \deg\alpha$$
$$+ b^2 \deg\beta$$
$$+ ab\,(\deg(\alpha+\beta) - \deg\alpha - \deg\beta).$$

Take $n = (p+1)^{\text{sth large}}$ then the equality even holds in $\mathbb{Z}$. $\square$

All about Frobenius

We already know the Frobenius

$$\phi_q : \begin{array}{ccc} E & \longrightarrow & E \\ (x,y) & \longmapsto & (x^q, y^q) \end{array}$$

so we immediately see $\deg \phi_q = q$.
We know that ϕ_q is not separable.
Further

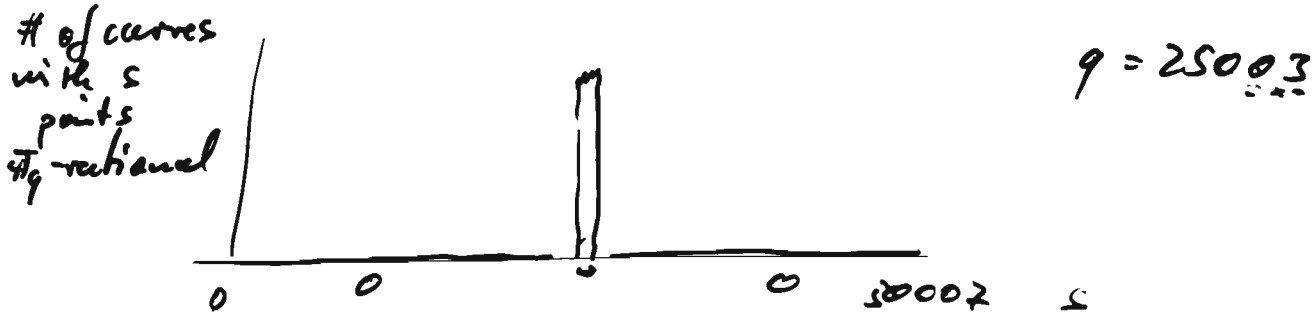
$$E(\mathbb{F}_q) = \ker(\phi_q - 1).$$

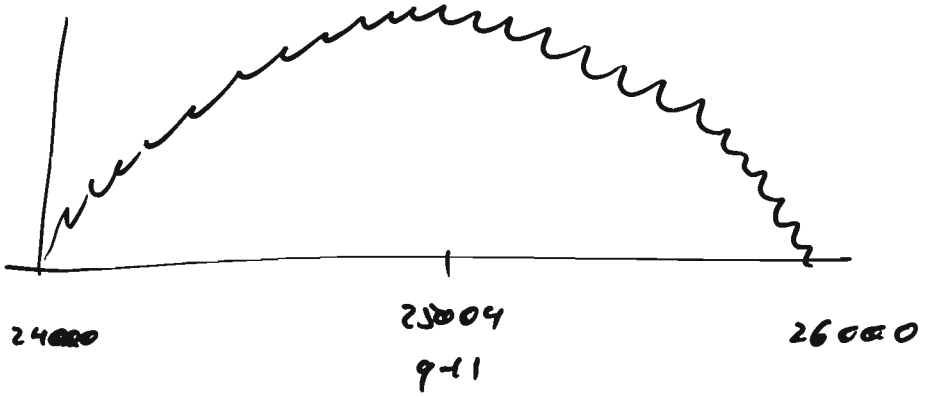
⌈ Note that $\mathrm{Gal}(\mathbb{F}_{q^e} | \mathbb{F}_q) = \langle \phi_q \rangle$! ⌋

What do we know about $\# E(\mathbb{F}_q)$?

Obviously:

$$0 \leq \# E(\mathbb{F}_q) \leq 2q+1$$





Theorem (Hasse)

If $E / \mathbb{F}_q$ then

$$\# E(\mathbb{F}_q) = q + 1 - t,$$

with

$$|t| \leq 2\sqrt{q}.$$

By reconsidering the proof of $\# E(\mathbb{F}_q) \leq 2q+1$ you see that for every x you look for the number of square roots of x^3+ax+b, for short:

$$\# E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+ax+b}{\mathbb{F}_q} \right)$$

If x^3+ax+b sees a random element of $\mathbb{F}_q^\times$ then the chance of being a square is 50%. Thus on average we expect one square root and so $\# E(\mathbb{F}_q) \approx q+1$.

Pf (Hasse)

Write $\deg(\varphi_q - 1) = \# E(\mathbb{F}_q)$
$= q+1-t$.

Recall that

$$\deg \varphi_q = q,$$

$$\deg -1 = 1.$$

Now:

$$\deg(r\varphi_q - s) = r^2 \overbrace{\deg \varphi_q}^{q} + s^2 \overbrace{\deg(-1)}^{1}$$

$$+ rs \underbrace{\left(\deg(\varphi_q - 1) - \deg \varphi_q - \deg(-1)\right)}$$

$$= q+1-t - q - 1$$

$$= -t.$$

$$= r^2 q + s^2 - rs\, t$$

$$= r^2 \left(\left(\frac{s}{r}\right)^2 - t\left(\frac{s}{r}\right) + q \right)$$

Of course, $\deg(r\varphi_q - s) \geq 0$ (unless $(r,s) = (0,0)$.)

That the polynomial $X^2 - tX + q \geq 0$ on $\mathbb{Q}$.

Thus $X^2 - tX + q \geq 0$ on $\mathbb{R}$, since $\mathbb{Q}$ is dense in $\mathbb{R}$.

Consequently, the discriminant $t^2 - 4q \leq 0$.

Thus

$$|t| \leq 2\sqrt{q}.$$

$\square$

<u>Theorem</u> (Characteristic polynomial of the Frobenius)

Let $E/\mathbb{F}_q$, $\#E(\mathbb{F}_q) = q+1-t$.

Then

$$\varphi_q^2 - t\varphi_q + q = 0 \text{ in } \mathrm{End}(E).$$

Moreover, if $\varphi_q^2 - k\varphi_q + q = 0$ then $k = t$.

Furthermore, $t \equiv_n \mathrm{trace}((\varphi_q)_n)$

and $q \equiv_n \det((\varphi_q)_n)$

for n coprime to $\mathrm{char}\, k$.

We call t = <u>trace of the Frobenius</u>

and $X^2 - tX + q$ the <u>characteristic polynomial of the Frobenius</u>.

Proof

We will show that

$$\varphi_q^2 - t\varphi_q + q$$

is the zero endo. We prove this by showing that its kernel is infinite.

Fix n coprime to char k.

Write

$$(\varphi_q)_n = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{Z}_n^{2\times 2}$$

wrt to some chosen basis T_1, T_2 of $E[n]$.

We want to find its characteristic polynomial:

By def. $\chi(X) = (-1)^2 \det((\varphi_q)_n - X)$ and hence it is a monic degree-2 polynomial.

Now

$$\chi(0) = \det(\varphi_q)_n \equiv_n \deg \varphi_q = q.$$

Further

$$\chi(1) = \det((\varphi_q)_n - 1) \equiv_n \deg(\varphi_q - 1) = \#E(\mathbb{F}_q)$$

$$= q + 1 - t.$$

Writing $\chi(X) = X^2 - kX + q$ we see $\chi(1) = 1 - k + q$ i.e. $k = t$. So $\chi = X^2 - tX + q$ and by Caley-Hamilton we obtain

$$\chi((\varphi_q)_n) = (\varphi_q)_n^2 - t(\varphi_q)_n + q = 0 \text{ in } \mathbb{Z}_n^{2\times 2}.$$

That is $\chi(\varphi_q) = \varphi_q^2 - t\varphi_q + q$ vanishes on $E[n]$.

Thus $\# \ker \chi(\varphi_q) \geq n^2$ for any n coprime to char k.

So $\chi(\varphi_q) = 0$ in $\mathrm{End}(E)$.

Finally assume

$$\varphi_q^2 - k\varphi_q + q = 0$$

Then

$$k\varphi_q = t\varphi_q$$

or

$$(k-t)\,\varphi_q = 0 \qquad \text{in } \mathrm{End}\,\bar{E}.$$

But φ_q is injective so

$$[k-t] = 0$$

Since its kernel ~~can be~~ is infinite we must have $k - t = 0$ in $\mathbb{Z}$.

Thus $k = t$! $\square$

This now implies a lot about the structure of the endomorphism ring:

If E is ordinary we have

$$\mathrm{End}\,E = \langle 1, \varphi_q \rangle = \mathbb{Z}[\varphi_q]/(\varphi_q^2 - t\varphi_q + q)$$

This is an order in a quadratic extension of $\mathbb{Q}$, namely in $\mathbb{Q}[X]/(X^2 - tX + q)$.

In case $t^2 = 4q$ the polynomial $X^2 - tX + q$ has a integer roots and $\varphi_q = [\sqrt{q}]$.

Structure & size

of $\mathbb{F}_q$-rational part of an elliptic curve $\Big\}$ $E(\mathbb{F}_q)$

What group is $E(\mathbb{F}_q)$?

It's a commutative, finite group.

Thus isomorphic to, say,

$$\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{m_r},$$

with $m_{i+1} \mid m_i$ for $i \in \{1, \dots, r-1\}$.

Now, the m_r-torsion is:

$$E(\mathbb{F}_q)[m_r] \cong \underbrace{\mathbb{Z}_{m_r} \oplus \mathbb{Z}_{m_r} \oplus \dots \oplus \mathbb{Z}_{m_r}}_{r \text{ summands}}$$

However, $E[m_r] \cong \mathbb{Z}_{m_r} \oplus \mathbb{Z}_{m_r}$

if $\gcd(q, m_r) = 1$

more general:

$$E(\mathbb{F}_q)[m_r] \lessdot E[m_r] \lessdot \mathbb{Z}_{m_r} \oplus \mathbb{Z}_{m_r}.$$

Thus $\# E(\mathbb{F}_q)[m_r] \leq m_r^2$.

And $\# E(\mathbb{F}_q)[m_r] = m_r^r$.

Thus $r \leq 2$.

<u>Theorem</u>

Given an elliptic curve E over a finite field $\mathbb{F}_q$. Then either

$$E(\mathbb{F}_q) \cong \mathbb{Z}_m \quad \text{for some } m \geq 1, \text{ or}$$

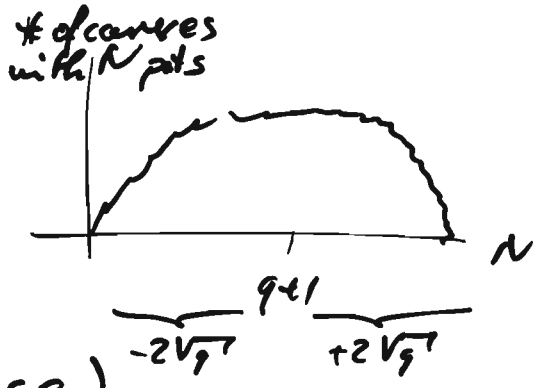
$$E(\mathbb{F}_q) \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \quad \text{for some } m_1, m_2, \; m_2 \mid m_1. \qquad \square$$

One can show that additionally

$$m_2 \mid q-1$$

or

$$t = \pm 2\sqrt{q}.$$



Even more:

<u>Theorem</u> (Rück, Waterhouse)

Assume $N = m_1 m_2$, $m_1 = p^e m_1'$, $p \nmid m_1'$, $m_2 \mid m_1'$, $|N-(q+1)| \leq 2\sqrt{q}$.

Then

there exists an elliptic curve E over $\mathbb{F}_q$ with N points and $E(\mathbb{F}_q) \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$

iff

$$\overset{q+1-N}{t} = \pm 2\sqrt{q}$$ (in particular, q must $N = q+1 \mp 2\sqrt{q}$, $m_1' = m_2$ be an <u>even</u> power)

or

$$m_2 \mid q-1.$$

Determining size

What do we already know?

$$0 \leq \# E(\mathbb{F}_q) \leq 2q+1$$

and even by Hasse

$$q+1-2\sqrt{q} \leq \# E(\mathbb{F}_q) \leq q+1+2\sqrt{q}.$$

This last inequality is optimal.

How to count $E(\mathbb{F}_q)$, if say

$$E: y^2 = x^3 + ax + b \quad ?$$

Brute force: check $O(q^2)$ points (x,y).

Next best solution: run through all x-values and ~~compute~~ find square roots of $y^2 = x^3 + ax + b$.

$\rightarrow O^{\sim}(q)$

A bit better is to only decide whether x^3+ax+b is a square, i.e. compute the Legendre symbol

$$\left(\frac{x^3+ax+b}{\mathbb{F}_q}\right).$$

Then $\# E(\mathbb{F}_q) = q+1+\sum_{x\in\mathbb{F}_q}\left(\frac{x^3+ax+b}{\mathbb{F}_q}\right).$

Runtime: $O^{\sim}(q)$

Further idea:

Use Lagrange:
pick a point $P \in E(\mathbb{F}_q)$ at random
and determine its order.

Determine order of P:

Brute force: try $m \cdot P$ for $m = 1, 2, \ldots$
until $m \cdot P = \mathcal{O}$.
runtime: $O^{\sim}(q)$.

Actually, if we find a point of order $> 4\sqrt{q}$
then – together with Hasse –
this determines the size.

Next best solution:
Just look for some m with $mP = \mathcal{O}$.
Only consider $m \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$.
Runtime: $O^{\sim}(\sqrt{q})$
Target down to the order:
factor m and consider – cleverly –
all its divisors.

Baby-step-giant-step

makes it even better:

We know that $mP = \mathcal{O}$

for some $m = q+1-t$

with $|t| \leq 2\sqrt{q}$.

Fix $B := \lceil \sqrt[4]{q} \rceil$.

Write $t = t_1 2B + t_0$

with $|t_0|, |t_1| < B$.

(That's always possible, $t_0 \equiv_{2B} t$.)

Now, compute the x-coordinates

of $P, 2P, \ldots, (B-1)\cdot P$.

and the x-coordinates of

$$(q+1 + t_1 \cdot 2B) \cdot P$$

for $t_1 \in \{-(B-1), \ldots, B-1\}$.

Then for the correct t_1, $\pm t_0$ we have

$$(q+1 + t_1 \cdot 2B \pm t_0)\, P = \mathcal{O}$$

or $$(q+1+t_1 \cdot 2B)\, P = \mp t_0 P.$$

or $$x\big((q+1+t_1 \cdot 2B)P\big) = x(t_0 P).$$

Then we now $m \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ with $mP = \mathcal{O}$.

Foram m determine the order by checking divisors of m.
Then we find the point's order, which gives information about the size of the curve.

In the lucky case:

runtime $O^{\sim}(q^{1/4})$.

Examples

$E: y^2 = x^3 + 2x + 1$ over $\mathbb{F}_{101}$.

Ψ

$P = (0, 1)$

Hasse interval: $82 .. 122$.

We find that $23 \cdot P = \mathcal{O}$.

Thus $\# E(\mathbb{F}_{101}) \in \{92, 115\}$.

We look for a point of order 2...
if there is one then $\# E(\mathbb{F}_{101}) = 92$
otherwise $\# E(\mathbb{F}_{101}) = 115$.

So look at:

$0 = x^3 + 2x + 1$ over $\mathbb{F}_{101}$.

Brute force: check all x.

Better: the zeroes of

$$x^{101} - x$$

are exactly the elements of $\mathbb{F}_{101}$.

Compute

$$\gcd(x^{101} - x, x^3 + 2x + 1)$$

$$\overset{\shortparallel}{\gcd}(x_{101} - x, x^3 + 2x + 1)$$

by computing

$$x_{101} := x^{101} \text{ rem } x^3 + 2x + 1$$

by square-and-multiply using $O(\log q)$ multiplications modulo $x^3 + 2x + 1$

Answer: $Q = (-13, 0)$ is on the curve. } On lg point of order 2!

Thus

$$\# E(\mathbb{F}_{101}) = 92.$$

Moreover:

$$E(\mathbb{F}_{101}) \cong \mathbb{Z}_{92} \in \begin{cases} \mathbb{Z}_{92} \\ \mathbb{Z}_{46} \oplus \mathbb{Z}_2. \end{cases}$$

Example

$$E: y^2 = x^3 - 33x - 22$$

over $\mathbb{F}_{101}$.

$P_1 = (36, -20)$ of order 11,

$P_2 = (37, -28)$ of order 9.

Thus $\#E(\mathbb{F}_q) = 99$

and $E(\mathbb{F}_q) \cong \mathbb{Z}_{99}$

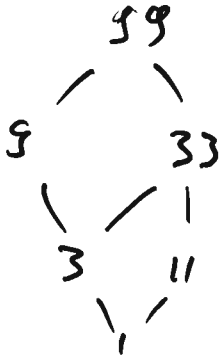
($\mathbb{Z}_{33} \times \mathbb{Z}_3$ has no point of order 9 and $3 \nmid 100$.)

~~Take s, t such that~~ $1 = s \cdot 11 + t \cdot 9$

~~then~~ $P = s P_1 + t P_2$

~~has order $11 \cdot 9$.~~

$P = P_1 + P_2$ is a generator.



Subfield curves

Over $\mathbb{F}_5$ choose $a, b \in \mathbb{F}_5$: $y^2 = x^3 + ax + b$,
grant $\Delta = 4a^3 + 27b^2 \neq 0$

So we'll have a small collection of curves to choose from. (At most 25.)

Now, consider

$$E: y^2 = x^3 + ax + b \quad \text{over} \quad \mathbb{F}_{5^m}$$

for some large m!

Clearly,

$$\left| \# E(\mathbb{F}_{5^m}) - (5^m + 1) \right| \leq 2 \cdot \sqrt{5^m}.$$

Here, additionally we can directly compute

$$\# E(\mathbb{F}_5) = 5 + 1 - t_5.$$

Observe further

$$\# E(\mathbb{F}_{5^m}) = 5^m + 1 - t_{5^m}$$

Note that

$$\varphi_{5^m}(x) = x^{5^m} = (\cdots((x^5)^5)^5 \cdots)^5 \quad (m \text{ times})$$

$$= \varphi_5^m(x)$$

Assume E is defined over $\mathbb{F}_q$.

We intend to compute $\# E(\mathbb{F}_{q^m})$.

Observe:

- $\varphi_{q^m} = (\varphi_q)^m$

- $\# E(\mathbb{F}_{q^m}) = q^m + 1 - t_{q^m}$

  $= \chi_{\varphi_{q^m}}(1)$

- $\chi_{\varphi_{q^m}}(T) = T^2 - t_{q^m} \cdot T + q^m$

  where $\chi_{\varphi_{q^m}}(\varphi_{q^m}) = 0$

Assuming q very small we can compute

$$\chi_{\varphi_q}(T) = T^2 - t_q T + q.$$

Write

$$\chi_{\varphi_q} = (T - \alpha)(T - \beta)$$

over $\mathbb{C}$.

Consider

$$f := (T^m - \alpha^m)(T^m - \beta^m)$$

$$= T^{2m} - (\alpha^m + \beta^m) T^m + q^m$$

ccc
13.1.10
3

Note that $f \in \mathbb{Z}[T]$.

(Either use Galois theory or check: $s_n = \alpha^n + \beta^n$, then

$$s_0 = 2, \quad s_1 = \alpha + \beta = t,$$

$$s_m = t\, s_{m-1} - q\, s_{n-2}.$$

Ex

(because: $\alpha^m = t\,\alpha^{m-1} - q\,\alpha^{m-2}$
$+$
$\beta^m = t\,\beta^{m-1} - q\,\beta^{m-2}$).)

Clearly, $\chi_{\varphi_q} \mid f$.

Thus $f(\varphi_q) = 0 \in \mathrm{End}(E)$.

Now, let

$$g := T^2 - (\alpha^m + \beta^m)\,T + q^m$$

and

$$g(\varphi_{q^m}) = f(\varphi_q)$$

$$\varphi_{q^m}^2 - (\alpha^m + \beta^m)\varphi_{q^m} + q^m \qquad \varphi_q^{2m} - (\alpha^m + \beta^m)\varphi_q^m + q^m$$

Thus

$$\chi_{\varphi_{q^m}} = g.$$

and $\# E(\mathbb{F}_{q^m}) = \chi_{\varphi_{q^m}}(1) = q^m + 1 - (\alpha^m + \beta^m)$.

Theorem

Count $\#E(\mathbb{F}_q)$ to get this!

Given a curve E defined over $\mathbb{F}_q$,

Write $\chi_{\varphi_q}(T) = T^2 - t\,T + q = (T-\alpha)(T-\beta)$.

over $\mathbb{C}$.

Then

$$\#E(\mathbb{F}_{q^m}) = q^m + 1 - \underbrace{(\alpha^m + \beta^m)}.$$

Can compute this fast using the recursion!

This allows computation of cardinalities for curves defined <u>small</u> fields.

Unfortunately, there only very few curves defined over small fields. And it may be that these are particularly weak in cryptographic setting.

Schoof (1985) found the first polynomial time point counting algorithm. It's runtime is something like $O(\log^8 q)$, but is has been improved considerably and can now deal with curves defined over fields $\mathbb{F}_q$ where q has several thousand bits.

Major improvements are due to

Elkies and

Atkin

resulting in the SEA algorithm.

Idea:

$$\varphi_q^2 - t\varphi_q + q = 0.$$

thus

$$\varphi_q^2(P) + q \cdot P = t\,\varphi_q(P).$$

That determines

$$t \mod \mathrm{ord}(P).$$

Unfortunately, we do not really the needed points P in our hands. And even if we take them in extensions of $\mathbb{F}_q$ we do not know their order...

You want a point of order ℓ?

Well, take the ℓ-torsion $E[\ell]$.

Warning: it may well be that $\ell \nmid E(\mathbb{F}_q)$.

Essentially we work over the ring, say ℓ odd:

$$R = \mathbb{F}_q[x,y] \big/ \langle -y^2+x^3+ax+b,\ \psi_\ell(x) \rangle,$$

noting that

$$(x,y) \in E[\ell] \iff \psi_\ell(x) = 0$$

ψ_ℓ: ℓ-division polynomial which is y-free (after reduction with $-y^2+x^3+ax+b$) since ℓ odd.

First, we pick a set

$$S$$

of primes such that

$$\prod_{\ell \in S} \ell > 4\sqrt{q}.$$

If we can determine $t \bmod \ell$ for all $\ell \in S$, then we know

$$t \bmod \prod_{\ell \in S} \ell$$

and together with $|t| \leq 2\sqrt{q}$ this determines t.

We do require $\underset{\text{char } \mathbb{F}_q}{p} \notin S$.

Case $\ell = 2$

If $x^3 + ax + b$ has a root x_1 in $\mathbb{F}_q$

then $(x_1, 0) \in E[2]$.

And thus $2 \mid q+1-t = \# E(\mathbb{F}_q)$.

Otherwise $2 \nmid q+1-t$

Thus we know $t \bmod 2$ then.

To make the decision compute

$$\gcd(x^q - x, x^3 + ax + b)$$
$$\parallel$$
$$\gcd(x_q - x, x^3 + ax + b)$$

where $x_q = x^q \text{ rem } x^3 + ax + b$

computed by square-and-multiply.

$\psi_2 = 2y \rightarrow E[2] =$ all points with $y = 0$.

Case ℓ odd, $\ell \neq p$

$\boxed{\text{Assume } q \text{ odd}}$

Aim:
$$(\varphi_q^2 P + qP) = t \cdot (\varphi_q P)$$

First, compute

$$\varphi_q^2(x,y) = (x^{q^2}, y^{q^2})$$ reduced modulo ψ_ℓ and $y^2 = x^3+ax+b$.

and

$$q_\ell \cdot (x,y)$$ reduced modulo ...

$\uparrow$
q rem ℓ

by using division polynomials

(because $\mathrm{ord}(x,y) = \ell$).

Note:
$$\boxed{\deg \psi_\ell = \frac{\ell^2-1}{2}}$$

Now, distinguish cases

(1) $\varphi_q^2(x,y) \neq \pm q_\ell \cdot (x,y)$.

Need the ordinary point addition to add them.

(2) $\varphi_q^2(x,y) = q_\ell \cdot (x,y)$

Need the point doubling ... or rather ~~oth~~ a few tricks to determine $t \bmod \ell$.

(3) $\varphi_q^2(x,y) = -q_\ell \cdot (x,y)$

Here the left hand side is $\mathcal{O}$ and

so $t \equiv_\ell 0$.

Case (G)

Let $(x', y') := \varphi_q^2(x,y) + q_e \cdot (x,y)$,
and abbreviate $(x_j, y_j) := j \cdot (x,y)$.
Then

$$x' = \left(\frac{y^{q^2} - y_{q_e}}{x^{q^2} - x_{q_e}} \right)^2 - x^{q^2} - x_{q_e} .$$

Write

$$(y^{q^2} - y_{q_e})^2 = y^2 \Big(y^{q^2-1} - \underbrace{\frac{y_{q_e}}{y}}_{} \Big)^2$$

even power even power

this is just a function of x given via division polynomials

$$= (x^3+ax+b) \Big((x^3+ax+b)^{\frac{q^2-1}{2}} - \frac{y_{q_e}}{y} \Big)^2$$

reduce mod ψ_e.

Thus we have

x' as a polynomial in x reduced modulo ψ_e.

Now, we want the x-coordinate of $j \cdot (x^q, y^q)$.
It is given by the division polynomials and we find

$$j \cdot (x^q, y^q) = (x_j^q, y_j^q)$$

So to find $\pm t \bmod \ell$
run through $j = 1, \dots, \frac{\ell+1}{2}$
and compare

$$x' \quad \text{with} \quad x_j^q$$

both reduced modulo y_ℓ.

Noting that $\ell \in O(\log q)$
(unless your choice of S was stupid),
we can do this in polynomial time.

Thus we get $\pm t \bmod \ell$ in poly time.

To determine the sign now consider
the y-coordinate:

$$\frac{y' - y_j^q}{y} \quad \text{is qualynomial in } x \text{ after reduction}$$

If this $= 0$ then $t \equiv_\ell j$
otherwise $t \equiv_\ell -j$.

<u>Case (2)</u> $\quad \varphi_q^2(x,y) = q_\ell \cdot (x,y)$

$$(x',y') = 2q_\ell \cdot (x,y)$$
$$\shortparallel$$
$$t \cdot \varphi_q(x,y)$$

Then
$$t\,\varphi_q(x,y) = \varphi_q^2(x,y) + q\cdot(x,y) = 2q\cdot(x,y)$$

Thus
$$\underbrace{t^2 q}\cdot(x,y) = t^2\varphi_q^2(x,y) = \underbrace{4q^2}\cdot(x,y)$$

Thus
$$t^2 \equiv_\ell 4q \quad .$$

Determine $w \in \mathbb{Z}_\ell$ such that $q \equiv_\ell w^2$.
Then either $t \equiv_\ell 2w$ or $t \equiv_\ell -2w$.
We now have
$$T^2 - tT + q = (T-w)(T+w) \quad .$$
Thus either $\quad (\varphi_q - w)(P) = \mathcal{O}$

or $\quad P' := (\varphi_q - w)(P)$,

$$(\varphi_q + w)(P') = \mathcal{O} \quad .$$

In any case there is a point $P \in E[\ell]$ with $\quad \varphi_q P = \pm w P$.

Assume $P \in E[\ell]$ with $\varphi_q P = wP$.

CCC
13.1.10
13

Then

$$0 = (\varphi_q^2 - t\varphi_q + q)P$$

$$= (q - tw + q)P$$

so

$$tw \equiv_\ell 2q \equiv_\ell 2w^2$$

and thus

$$t \equiv_\ell 2w.$$

~~Otherwise~~

We can check this as follows:

$$(x^q, y^q) = \pm w \cdot (x, y)$$

$$\| $$

$$(x_w, \pm y_w)$$

for <u>some</u> $(x, y) \in E[\ell]$.

So check

$$\boxed{\gcd(\text{numer}(x^q - x_w), \psi_\ell) \neq 1.}$$

Tricky:

$$(\varphi_q|_\ell : \underset{E[\ell]}{\underset{\cong}{\mathbb{Z}_\ell \times \mathbb{Z}_\ell}} \to \underset{E[\ell]}{\underset{\cong}{\mathbb{Z}_\ell \times \mathbb{Z}_\ell}}$$

$$\sim \begin{bmatrix} w & 1 \\ & w \end{bmatrix}$$

If this is so then there is a point in $E[\ell]$ such $\varphi_q P = wP$, and thus $t \equiv_\ell 2w$.

<u>Case (3)</u> Here $t \equiv_\ell 0$

Orders and divisors

Example $\mathbb{C}$ (the line), quotienpolynomials.

$$f = \frac{x(x-3)^3}{(x-2)^2} \longrightarrow$$

single zero at 0
triple zero at 3
double pole at 2.

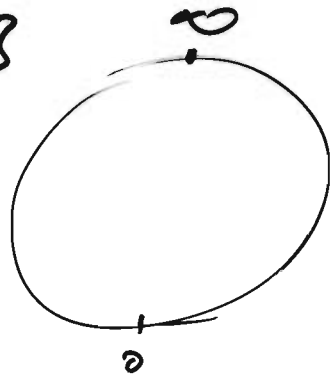
Is there a fn with

five-tuple zero at 5
double pole at 2 ? $\longrightarrow$ $g = \dfrac{17(x-5)^5}{(x-2)^2}$

Is it unique? No.
But it is unique up to a non-zero constant:
any other answer $\hat{g}$ to that question
is a non-zero multiple of g.

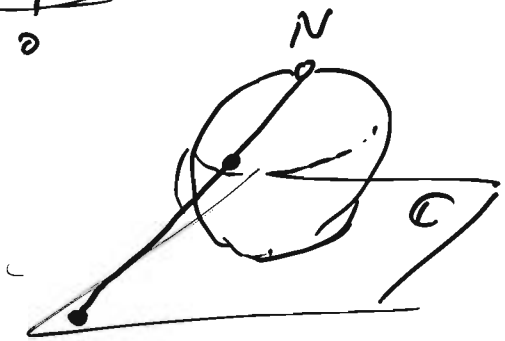
Equivalently:
The (non-zero) fns without zeros or poles
are precisely the constant functions.

Example 2 $\mathbb{P}^1\mathbb{C} = \mathbb{C} \cup \{\infty\}$



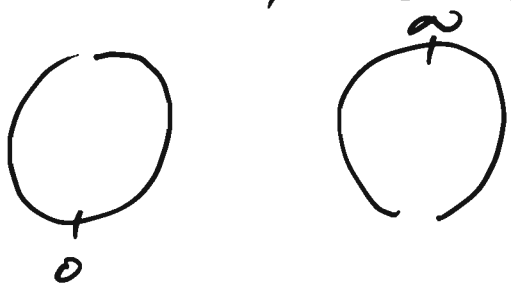
$$\mathbb{P}^1\mathbb{C} = \{ x:y \mid x,y \in \mathbb{C},\ (x,y) \neq (0,0) \}$$

$$x:y = ax : ay \quad \text{for } a \neq 0$$



$$\mathbb{C} \subset \mathbb{P}^1\mathbb{C} \supset \mathbb{C}$$

$$x \longmapsto x:1 \qquad 1:y \longleftarrow y$$



$$x:1 = 1:y$$
$$\Updownarrow$$
$$x = 1/y$$

$$2 \longmapsto 2:1 \longleftarrow \frac{1}{2}$$
$$2:1 = 1:\tfrac{1}{2}$$

Say, we consider

$$f = \frac{x(x-3)^3}{(x-2)^2} \longrightarrow$$

single zero at $0:1 = 0$
triple zero at $3:1 = 3$
double pole at $2:1 = 2$
double pole at $1:0 = \infty$

$$f(x:1) = \frac{(1-3y)^3}{y^2(1-2y)^2}$$

Same function! So the descriptions are fine around $x:1,\ x \neq 0$ $= 1:y,\ y \neq 0$.
Only the first description is fine around $0 = 0:1$,
the second around $\infty = 1:0$.

Is there a fn with
a five-triple zero at 5
a double pole at 2
and no further zeros
or poles ?

Already over $\mathbb{C}$ we get that <u>up to scalar</u>
<u>only</u>

$$g = \frac{17(x-5)^5}{(x-2)^2}$$

does this.

But

$$g = \frac{17(1-5y)^5}{y^3\,(1-2y)^2}$$

and so it has a triple pole at ∞
which was not required.

So : NO, there is no such function,
noting that g is unique up to scalar;
and such scalar does not change its
behavior at ∞.

Over $\mathbb{P}^1\mathbb{C}$ any fun is given as a quotient polynomial, so

$$h = \frac{f}{g} \quad \text{with} \quad f, g \in \mathbb{C}[x].$$

without common zeros.

Clearly,

$\deg f$ the (finite) zeros of h are the zeros of f with the same multiplicities.

$\deg g$ the (finite) poles of h are the zeros of g with the same multiplicities.

And what happens around infinity?

Now,

$$h = \frac{f|_{x=1/y} \cdot y^{\deg f}}{g|_{x=1/y} \cdot y^{\deg g}} \cdot y^{\deg g - \deg f}$$

We can now see that h at ∞, i.e. $y=0$,

has a

$(\deg g - \deg f)$-tuple zero

or a

$(\deg f - \deg g)$-tuple pole.

In total:

the multiplicities of zeros and poles (take negativity) add up to $\deg f - \deg g + (\deg g - \deg f) = 0$!

We'd like all that for an elliptic curve.

First: what kind of functions do we consider?

Notice that $E \subset \mathbb{P}^2\bar{k}$.

Well, as before $\bar{k}^2 \subset \mathbb{P}^2\bar{k}$

$$(x,y) \longmapsto x:y:1$$

We want functions given by quotients of polynomials somehow. So do this as follows:

consider $h = \dfrac{f}{g}$, $f,g \in \bar{k}[x,y]$

as a function on (most of) $\bar{k}^2$

and restrict to E.

We only require that f,g are coprime and that h is defined ~~at~~ at least at one point of $E(\bar{k})$.

In particular, if $E: y^2 = x^3+ax+b$

then $h = \dfrac{1}{-y^2+x^3+ax+b}$ is <u>not</u> a function on E.

There is one further problem:

$E: y^2 = x^3 - x$ over $\mathbb{Q}$.

$$f = \frac{x}{y}.$$

$y^2 = x^3 - x$

Clearly, f is a function on E, eg. $P = (2, \sqrt{6}) \in E$ and $f(P) = \frac{2}{\sqrt{6}} \in \bar{\mathbb{Q}}$.

But $Q = (0,0) \in E$, and at Q numerator and denominator of f vanish. :(

By the curve equation

$$f = \frac{x}{y} \underset{\substack{\uparrow \\ \text{curve} \\ \text{equation}}}{=} \frac{y}{x^2 - 1}.$$

This the same function on E, though given by a different quotient.

Now at Q we find $y = 0$, $x^2 - 1 = -1$, so

$$f(Q) = 0.$$

This resolves our problem in this example.

IN GENERAL: for every point P on E you can find a way to write a given function f such that at most one of numerator and denominator vanish.

Let's ease our life by introducing some notation:

<u>Definition</u>

Let E be an elliptic curve over some field k.

The <u>divisor group</u> $\mathrm{Div}(E)$ is the <u>free</u> abelian group generated by symbols $[P]$ for the points P of E, $\mathrm{Div}(E) = \bigoplus_{P \in E(\bar{k})} \mathbb{Z} \cdot [P]$, and its elements are called divisors. $\{(f: E \to \mathbb{Z})$ $f(P) \neq 0$ for at most finitely many $P.\}$

In other words, a <u>divisor</u> is a (formal) finite linear combination

$$D = \sum_{j \leq n} a_j \cdot [P_j]$$

with $a_j \in \mathbb{Z}$, $P_j \in E$ for $j \leq n \in \mathbb{N}$.

Further we define the <u>degree</u>

$$\deg D := \sum_{j \leq n} a_j \quad \in \mathbb{Z}$$

and the <u>sum</u>

$$\mathrm{sum}\, D := \sum_{j \leq n} a_j \cdot P_j \quad \in E.$$

<u>Examples</u>

- $D_1 = 1 \cdot [0] + 3 \cdot [3] - 2 \cdot [2]$.
- $D_2 = 5 \cdot [5] - 2 \cdot [2]$
- their sum is $D_1 + D_2 = 1 \cdot [0] + 3 \cdot [3] + 5 \cdot [5] - 4 \cdot [2]$.
- $\deg D_1 = 1 + 3 - 2 = 2$, $\mathrm{sum}\, D_1 = 5$.

Over $\mathbb{P}^1\mathbb{C}$ we had noticed that the sum of multiplicities of zeros and negative mult. of poles is always zero when we consider a "divisor coming from a function".

But we want to consider functions on an elliptic curve.

Consider a function on E.

Clearly, f has a zero at a point P if $f(P) = 0$,

i.e. multiplicity is at least one.

and a pole if $f(P) = \infty$.

(i.e. numerator $\neq 0$, denominator $= 0$),

i.e. multiplicity is at most -1.

With polynomials (on $\mathbb{C}$) we can capture the multiplicity (1) by the number of factors $x - b$ that we can take out, i.e.

$$f = \underbrace{(x-b)^r}_{?} \cdot g \qquad \text{with } g(b) \neq 0, \infty.$$

(1) of a zero b of f

Fact

Let E be an elliptic curve, and $P \in E$ some point.
Then there exists a <u>uniformizer</u> u_P <u>at P</u> with $u_P(P) = 0$.
such that

for every function f on E
there exists an integer $r \in \mathbb{Z}$
and a function g on E
such that

$$f = u_P^{\,r} \cdot g$$

and

$$g(P) \neq 0, \infty .$$

Moreover, this integer r is <u>uniquely</u> determined regardless of the choice of the uniformizer u_P.
We define the <u>order of f at P</u> by

$$\mathrm{ord}_P f := r .$$

Wanted property: $f = f_1 f_2$, both f_1, f_2 vanish at P.
then the zero multiplicity of f at P should be at least two.

This actually follows. So we're happy. :)

Corollary: $\operatorname{ord}_P u_P = 1$. $\square$

Lemma/Corollary

Given f_1, f_2 functions on a curve E and a point $P \in E$, we have

$$\operatorname{ord}_P f_1 f_2 = \operatorname{ord}_P f_1 + \operatorname{ord}_P f_2 .$$

$\square$

Let's consider the example

$$E: y^2 = x^3 - x,$$

$$f = x \quad \text{at} \quad P = (0,0).$$

Clearly, $f(P) = 0$.

But what is $\operatorname{ord}_P f$?

looks like $\operatorname{ord}_P f = 1$. :)

But no: $\operatorname{ord}_P f = 2$!

$$f = x \overset{\text{curve}}{=} \frac{y^2}{x^2-1} = (y)^2 \cdot \underbrace{\frac{1}{x^2-1}}_{\substack{\text{this is} \\ \text{neither } 0 \\ \text{nor } \infty \\ \text{at } P.}} .$$

this is zero at P

Thus $\operatorname{ord}_P f \geq 2$.

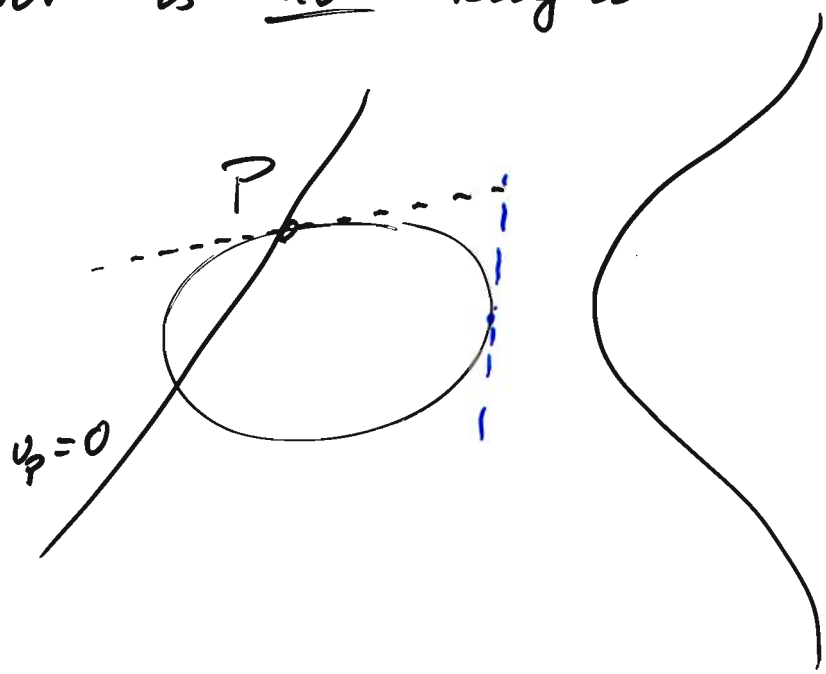
Actually, $u_P = y$ is a uniformizer at P.

Thus $\operatorname{ord}_P f = 2$.

Further, $\operatorname{ord}_P x = 2$ and $\operatorname{ord}_P \frac{x}{y} = 1$.

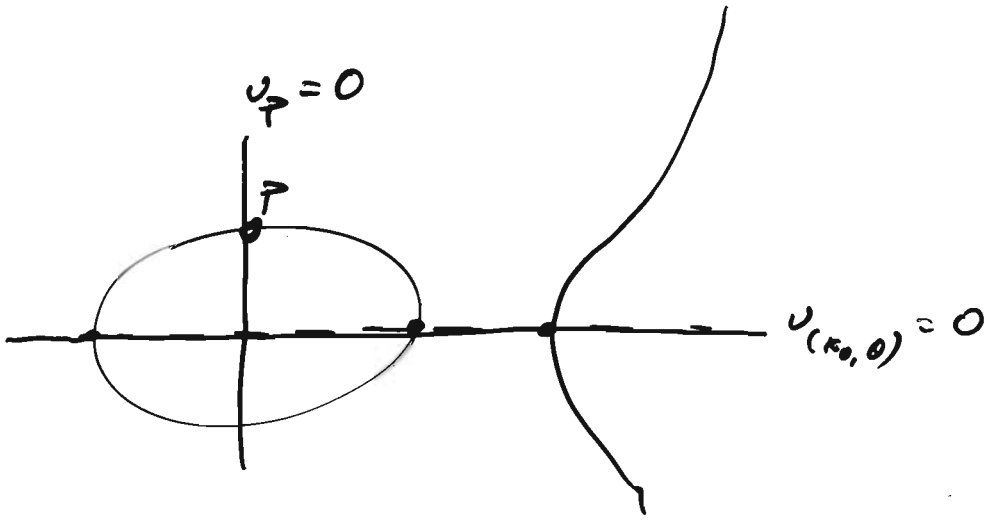
Fact

At any (finite) point of an elliptic curve E, the uniformizer u_P can be taken from the equation of a line that passes through P but is <u>not</u> tangent to E.



Given $E: y^2 = x^3 + ax + b$ then we can take

$$u_P = \begin{cases} x - x_0 & P = (x_0, y_0),\ y_0 \neq 0. \\ y & P = (x_0, y_0),\ y_0 = 0. \\ x/y & P = \mathcal{O} \end{cases}$$



Let's check $P = O$:

$$x : y : 1 = x' : 1 : z' \quad \text{with } x' = \frac{x}{y}, \quad z' = \frac{1}{y}$$

$$\rightsquigarrow$$

$$v_O = \frac{x}{y} = x'$$

Thus in the chart $\{ x' : 1 : z' \mid x', z' \in \bar{k} \}$.

$v_O = 0$ is a line passing through $O = 0:1:0$.

And it defines a line.

And it's not the tangent $z' = 0$ at O.

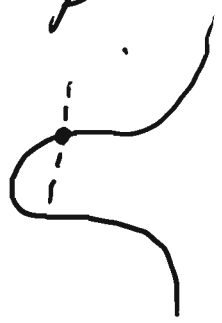
Thus v_O is fine under the previous fact.

<u>Example</u>

Consider $P = (-2, 8)$ on $y^2 = x^3 + 72$ over $\mathbb{C}$.

The line $x + 2 = 0$ passes through P.

So $v_P = x + 2$ is fine.



Consider $f = x + y - 6$.

It vanishes at P. Well, the curve equation can be rewritten as

$$(y+8)(y-8) = (x+2)^3 - 6(x+2)^2 + 12(x+2).$$

Thus

$$f = (x+2) + (y-8)$$

$$= (x+2)\left(1 + \frac{(x+2)^2 - 6(x+2) + 12}{y+8}\right)$$

Now, $(\dots)(P) \neq 0, \infty$. Thus $\operatorname{ord}_P f = \frac{1}{1}$.

Consider $t = \frac{3}{4}(x+2) \underbrace{- y + 8}_{-(y-8)}$

which is derived from the tangent.

We find $t(P) = 0$. Here:

$$t = (x+2)\underbrace{\left(\frac{3}{4} - \frac{(x+2)^2 - 6(x+2) + 12}{y+8}\right)}_{\text{vanishes at } P=(-2,8)}$$

$$= (x+2)^2 \underbrace{\frac{(-4(x+2)+24)(y+8) + 3(x+2)^2 - 18(x+2) + 36}{(y+8)^2}}_{\text{does not vanish at } P=(-2,8)}$$

Thus $\mathrm{ord}_P\, t = 2$.

<u>Definition</u>

For a non-zero function f on an elliptic curve E we define the <u>divisor of f</u> by

$$\mathrm{div}(f) := \sum_{P \in E} \mathrm{ord}_P(f) \cdot [P] \in \mathrm{Div}(E).$$

Note that by the following proposition the occurring sum is always finite.

Proposition

E ell. curve, f non-zero fn on E.

Then (i) f has only finitely many zeros and poles.

(ii) We have $\deg(\operatorname{div}(f)) = 0$.

(iii) If f has no zeros or poles, ie. $\operatorname{div}(f)=0$, then f is constant.

We have checked all this for $\mathbb{P}^1\mathbb{C}$ in place of E.
Actually, the proposition holds for any <u>smooth</u>, <u>irreducible</u>, <u>projective</u> curve.

(ii) fails for $\mathbb{C}$. $\mathbb{C}$ is a smooth, irreducible curve but it's not projective/complete.

(iii) fails for $(y-x)(y+x)=0$.

This curve is smooth (actually...), it's projective if you take it in $\mathbb{P}^2\mathbb{C}$.
but it is not irreducible.

Example:

$f = \frac{x}{y}$. $\operatorname{div} f = 0$!

$$\left.\begin{aligned} \operatorname{div} x &= [(0,0)] - [\infty], \\ \operatorname{div} y &= [(0,0)] - [\infty] \end{aligned}\right\} \to \operatorname{div} f = 0.$$

Parametrizations do not exist

ccc
26.1.10
1

Lemma a

Consider an elliptic curve $E: y^2 = x^3 + ax + b$ over a field k of characteristic different from 2. Assume that $X, Y \in \bar{k}(t)$ are quadratic functions in an indeterminate t such that

$$Y^2 = X^3 + aX + b$$

Then

$$X, Y \text{ are constant.}$$

Proof Write $x^3 + ax + b = (x - e_0)(x - e_1)(x - e_2)$ with $e_0, e_1, e_2 \in \bar{k}$ distinct.

Write

$$X = \frac{X_n}{X_d}, \quad Y = \frac{Y_n}{Y_d}$$

with $X_n, X_d, Y_n, Y_d \in \bar{k}[t]$

and X_n, X_d are coprime,

Y_n, Y_d are coprime.

The equation turns into

$$Y_n^2 X_d^3 = Y_d^2 (X_n^3 + a X_n X_d^2 + b X_d^3)$$

~~Since~~ By the coprimality assumptions:

$$Y_d^2 \mid X_d^3 .$$

Assume that X_d has a common root with $X_n^3 + a X_n X_d^2 + b X_d^3$. That would imply a common root for X_d and X_n. So we don't have that. Consequently, $X_d^3 \mid Y_d^2$. Wlog we have

$$X_d^3 = Y_d^2 ,$$

and so

$$Y_n^2 = X_n^3 + a X_n X_d^2 + b X_d^3$$

$$= (X_n - e_0 X_d)(X_n - e_1 X_d)(X_n - e_2 X_d)$$

<u>Claim</u> (1) X_d, $X_n - e_0 X_d$, $X_n - e_1 X_d$, $X_n - e_2 X_d$ are squares.

(2) ~~any~~ two of the vectors $(0,1)$, $(1,-e_0)$, $(1,-e_1)$, $(1,-e_2)$ are linearly independent.

(2) is clear by inspection

(1): X_d must be a square by looking at a prime factorization

To show that $X_n - e_i X_d$ is a square it suffices to show that for $i \neq j$

$$X_n - e_i X_d \quad \text{and} \quad X_n - e_j X_d$$

are coprime. Then since the product is a square each factor $X_n - e_i Y_d$ must be a square (via prime fact.).

Note

$$e_j (X_n - e_i X_d) - e_i (X_n - e_j X_d)$$

$$= (e_j - e_i) X_n$$

and

$$(X_n - e_i X_d) - (X_n - e_j X_d)$$

$$= (e_j - e_i) X_d .$$

Since $e_i \neq e_j$ a common root ~~would be~~ of $X_n - e_i X_d$ and $X_n - e_j X_d$ would be a common root of X_n and X_d. But these are coprime. So we have the claim.

The following lemma implies that this can only be if X_n and X_d are constant. Thus X is constant and thus also Y is constant. $\square$

Lemma

Assume P_1, P_2 are coprime polynomials in $\bar{k}[t]$, and there are four pairs $(a_i, b_i) \in \bar{k}^2$ such that

- any two pairs (a_i, b_i) are linearly independent in $\bar{k}^2$.
- each of the polynomials
$$a_i P_1 + b_i P_2$$
is a square.

Then P_1 and P_2 are constant polynomials.

Proof Assume P_1, P_2 is a minimal counterexample wrt.
$$\max(\deg P_1, \deg P_2) > 0.$$
Write
$$a_i P_1 + b_i P_2 = R_i^2 \quad \text{for some } R_i \in \bar{k}[t].$$

Then the R_i are pairwise coprime. Otherwise, $a_i P_1 + b_i P_2$ and $a_j P_1 + b_j P_2$ would have a common root and since (a_i, b_i) and (a_j, b_j) are linearly independent also P_1 and P_2 would have this root. But they are coprime.

Write (a_3, b_3) as a linear combination (a_1, b_1) and (a_2, b_2). Then for some $c_1, d_1 \in \bar{k}$ we get

ecc
26.1.10
5

$$R_3^2 = c_1^2 R_1^2 - d_1^2 R_2^2 .$$
$$= (c_1 R_1 + d_1 R_2)(c_1 R_1 - d_1 R_2)$$

Similarly,
$$R_4^2 = c_2^2 R_1^2 - d_2^2 R_2^2 .$$
$$= (c_2 R_1 + d_2 R_2)(c_2 R_1 - d_2 R_2) .$$

We will show that

(i) $c_i R_1 \pm d_i R_2$ is a square, and

(ii) Each two of the vectors $(c_i, \pm d_i)$ are linearly independent.

Then we are done: since

$$\max(\deg R_1, \deg R_2) \leq \tfrac{1}{2} \max(\deg P_1, \deg P_2)$$

and we would have a smaller counter-example. So R_1 and R_2 must be constant, but then since $a_i P_1 + b_i P_2 = R_i^2$ we would find that P_1 and P_2 are constant.

Note that c_i, d_i are all non-zero. Otherwise, R_3 or R_4 would be a multiple of R_1 or R_2 which would contradict their coprimality. But now we can see that $c_1 R_1 \pm d_1 R_2$ are coprime. (A common root would also be one of R_1, R_2.) Thus they are squares! This settles (i).

To prove (ii):

We have (c_1, d_1), $(c_1, -d_1)$ is lin. ind.

and (c_2, d_2), $(c_2, -d_2)$ is lin. ind.

Assume $(c_1, \pm d_1)$ and $(c_2, \pm d_2)$ is linearly dependent

then $(c_1, \pm d_1) = \lambda\,(c_2, \pm d_2)$ (or vice versa).

But then $(c_1^2, d_1^2) = \lambda^2\,(c_2^2, d_2^2)$

and so
$$R_3^2 = \lambda^2 R_4^2 .$$

But that cannot be since R_3, R_4 are coprime.
That settles (ii) and thus the lemma. $\square$

Back to divisors ...

Theorem

Consider an elliptic curve E and a divisor D. Then

$$\exists f \text{ on } E: \quad D = \mathrm{div}(f).$$

iff

$$\deg D = 0 \quad \text{and} \quad \mathrm{sum}\, D = \mathcal{O}.$$

First, note

$$\mathrm{sum}(D_1 + D_2) = \mathrm{sum}\, D_1 + \mathrm{sum}\, D_2.$$

(if we have associativity).

Denote

$$\mathrm{Div}^0(E) := \{ D \in \mathrm{Div}(E) \mid \deg D = 0 \}$$

degree-zero divisors

$$\mathrm{Princ}(E) := \{ \mathrm{div}(f) \mid f \text{ fn on } E, \text{ non-zero} \} \cup \{0\}.$$

principal divisors.

$$\mathrm{Princ}(E) \trianglelefteq \mathrm{Div}^0(E)$$

and

Picard group: $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E) / \mathrm{Princ}(E)$

Corollary

The map

$$\begin{array}{rcl} & & \mathrm{Pic}^0(E) \\ & & \| \\ \text{sum}: & & \mathrm{Div}^0(E)/\mathrm{Princ}(E) \longrightarrow E(\bar{k}), \\ & & D + \mathrm{Princ}(E) \longmapsto \text{sum}\, D \end{array}$$

is an isomorphism of groups.

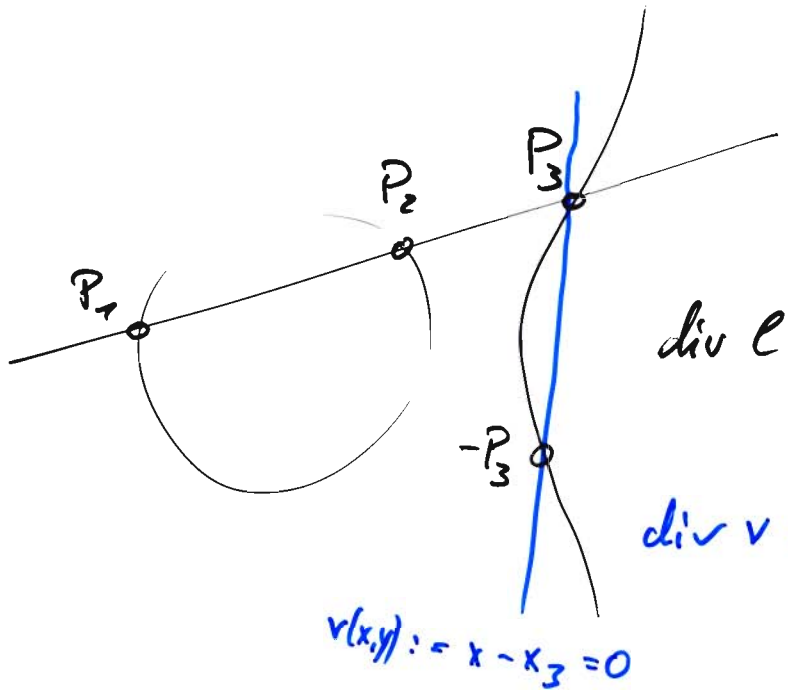
Proof

The map

$$\text{sum}: \mathrm{Div}^0(E) \longrightarrow E(\bar{k})$$

is surjective: $\text{sum}([P]-[O]) = P - O = P$.

The previous theorem tells us that its kernel is $\mathrm{Princ}(E)$. $\square$



$$\underbrace{ax+by+c}_{\ell(x,y)} = 0$$

$$\mathrm{div}\,\ell = [P_1]+[P_2]+[P_3] - 3[O].$$

$$\mathrm{div}\, v = [P_3] + \underset{\substack{\| \\ P_1+P_2}}{[-P_3]} - 2[O].$$

ecc
26.1.10
9

Thus

$$\operatorname{div}\left(\frac{\ell}{v}\right) = \operatorname{div}\left(\frac{ax+by+c}{x-x_3}\right) *$$

$$= [P_1] + [P_2] - [P_1+P_2] - [O]$$

So we can construct a function h on E such that

$$[P_1] + [P_2] = [P_1+P_2] + [O] + \operatorname{div}(h).$$

<u>Proof (Theorem)</u>

27.1.10
1

First, just take any divisor $D \in \operatorname{Div}(E)$,

$$D = \sum_{j \in J_0} a_j [P_j] - \sum_{j_0 \le j \le j_1} b_j [P_j] + z_0 [O]$$

with $a_j > 0$, $b_j > 0$, P_j pairwise different, $P_j \neq O$, $z_0 \in \mathbb{Z}$.

Inductively, we can replace $\sum a_j [P_j]$ by

$$\Big[\underbrace{\sum a_j P_j}_{P}\Big] + \left(\sum a_j - 1\right)[O] + \overbrace{\sum \operatorname{div}(h)}^{\operatorname{div}(\prod h)}$$

So we can find points P, Q, an integer $z \in \mathbb{Z}$ and a function h on E such that

$$D = [P] - [Q] + z[O] + \operatorname{div}(h).$$

Additionally, we observe that h is a product of function $\frac{ax+by+c}{x-x_3}$, each of which has sum $\mathcal{O}$:

$$\operatorname{div}\left(\frac{ax+by+c}{x-x_3}\right) = [P_1]+[P_2]-[P_1+P_2]-[\mathcal{O}],$$

$$\operatorname{sum}(\text{"}) = P_1+P_2-(P_1+P_2)-\mathcal{O} = \mathcal{O}.$$

Consequently,

$$\operatorname{sum}(h) = \mathcal{O}.$$

We get this:

for every divisor D ~~where~~ are points $P, Q \in E$, $z \in \mathbb{Z}$, h fn. on E with $\operatorname{sum}(\operatorname{div}(h)) = \mathcal{O}$ such that

$$D = [P]-[Q]+z[\mathcal{O}]+\operatorname{div}(h).$$

Observe:

$$\operatorname{sum} D = P - Q,$$

$$\deg D = 1-1+z+0 = z.$$

Assume now $\deg D = 0$ and $\operatorname{sum} D = \mathcal{O}$.
Writing D as above we find

$$z = \deg D = 0$$

and

$$P - Q = \operatorname{sum} D = \mathcal{O} \longrightarrow P = Q.$$

Thus

$$D = \underbrace{[P] - [P]}_{0} + \underbrace{0 \cdot [\mathcal{O}]}_{0} + \operatorname{div}(h)$$

$$= \operatorname{div}(h).$$

Conversely, assume $D = \operatorname{div}(f)$ for some function f.
Then $\deg D = \deg \operatorname{div}(f) = 0$,
and we can write D as above:

$$(*) \qquad \operatorname{div}(f) = D = [P] - [Q] + \underbrace{\operatorname{div}(h)}_{\operatorname{sum} = \mathcal{O}}.$$

So

$$\operatorname{sum} \operatorname{div}(f) = P - Q.$$

It suffices (and is necessary) that $\underline{\underline{P = Q}}$.
Then $\operatorname{sum} D = P - Q = \mathcal{O}$ as desired.
Rewrite $(*)$:

$$[P] - [Q] = \operatorname{div}\left(\frac{f}{h}\right).$$

This implies $P = Q$ by the following lemma.

$\square$

In $\mathbb{P}^1_{\mathbb{C}}$ we can easily find functions with divisor $[a]-[b]$:

$$f = \frac{x-a}{x-b}, \quad \operatorname{div}(f) = [a]-[b].$$

This however is impossible on an elliptic curve!

<u>Lemma</u>

Let $P, Q \in E(\bar{k})$ and there is a function h on E with $\operatorname{div}(h) = [P]-[Q]$. Then

$$P = Q.$$

<u>Proof</u> Suppose $P \neq Q$ and $\operatorname{div}(h) = [P]-[Q]$.
Thus h has a ~~single~~ simple pole at Q,
but also $h-c$ has a ~~single~~ simple pole at Q
and no other pole for any constant $c \in \bar{k}$.
Thus $h-c$ has ~~some~~ a ~~single~~ simple ~~pole~~ zero.
To be concrete take some point 1-fold $R \in E \setminus \{Q\}$:

$$\operatorname{div}(h - h(R)) = [R] - [Q].$$

Now, consider any fn f on E, and show that it is a polynomial function of h:

First, consider the case that f has neither zero or pole at Q. Now:

$$g := \prod_{\substack{R \in E \setminus \{Q\} \\ \mathrm{ord}_R f \neq 0}} \left(h - h(R)\right)^{\mathrm{ord}_R(f)}$$

This is only a finite product since $\mathrm{ord}_R f \neq 0$ only for finitely many points R.

Now, compute the divisor of g:

$$\mathrm{div}\, g = \sum_{R \in E \setminus \{Q\}} \mathrm{ord}_R f \cdot \underbrace{\mathrm{div}(h - h(R))}_{[R] - [Q]}$$

$$= \sum_{R \neq Q} \mathrm{ord}_R f \cdot [R] \underbrace{- \Big(\underbrace{\sum \mathrm{ord}_R f}_{\underbrace{\deg \mathrm{div} f}_{=0} - \mathrm{ord}_Q f}\Big) \cdot [Q]}$$

$$= \mathrm{div}\, f + \mathrm{ord}_Q f \cdot [Q]$$

Thus $\mathrm{div}(g/f) = 0$, and so $\frac{g}{f} = c$ constant.

So f is a rational fun of h.

Next, the general case:

$$\hat{f} := h^{\operatorname{ord}_Q f} \cdot f$$

Then $\operatorname{ord}_Q \hat{f} = \operatorname{ord}_Q f \cdot (-1) + \operatorname{ord}_Q f = 0$.

By the previous case $\hat{f}$ is a quotpolynomial fn of h, and so also $f = h^{-\operatorname{ord}_Q f} \cdot \hat{f}$.

In particular, we can write x and y as quotpolynomials in h. That is we have two quotpolynomials X, Y with

$$Y^2 = X^3 + aX + b.$$

($x = X \circ h$, $y = Y \circ h$, in h is a lat.)

But that is a parametrization. And so X, Y must be constant.

~~↯ h has a pole, thus many values~~

↯ $x = X \circ h$ takes on every x-value.

Thus our assumption $P \neq Q$ must be wrong.

$\square$

The Weil pairing

ecc
27.1.10
7

Recall: n coprime to char k,

$E[n]$ n-torsion of $\bar{E} = E(\bar{k})$,

μ_n n-th roots of unity in $\bar{k}$.

Aim: construct a pairing

$$e_n : E[n] \times E[n] \longrightarrow \mu_n$$

with nice properties.

Take $S, T \in E[n]$. Consider the divisor

$$\tilde{D} := \sum_{nT''=T} [T''] - \sum_{nR=O} [R]$$

Clearly, $\deg \tilde{D} = 0$. But also, taking $T' \in \bar{E}$: $nT' = T$,

$$\text{since } \tilde{D} = \sum_{R \in E[n]} [T'+R] - \sum_{nR=O} [R],$$

$$\text{so } \tilde{D} = \sum_{R \in E[n]} \big((T'+R) - R\big)$$

$$\overset{\#E[n]=n^2}{=} n^2 T' = nT = O,$$

noting $\{T'' \in \bar{E} \mid nT'' = T\} = \{T'+R \mid R \in E[n]\}$.

Thus there exists a function g_T such that

$$\operatorname{div}(g_T) = \tilde{D}$$

We will define $e_n(S,T) = \dfrac{g_T(S+P)}{g_T(P)}$.

To show that this is in μ_n we construct another function:
Namely, pick f_T such that

$$\operatorname{div}(f_T) = n \cdot D, \qquad D = [T] - [O].$$

Since $\deg nD = 0$ and $\operatorname{sum} D = nT - nO = O$ such a function f_T exists.
Compute the divisor of $f_T \circ [n]$:

$$\operatorname{div}(f_T \circ [n]) = \sum_{nT''=T} n \cdot [T''] - \sum_{nR=O} n \cdot [R].$$

$$= n \cdot \tilde{D} = n \cdot \operatorname{div}(g_T)$$

$$= \operatorname{div}(g_T^{\,n}).$$

Thus $f_T \circ [n]$ and $g_T^{\,n}$ are equal up to some constant and wlog we may assume

$$f_T \circ [n] = g_T^{\,n}.$$

Now,

$$g_T(S+P)^n = f_T(n(S+P))$$
$$= f_T(n\ P)$$
$$= g_T(P)^n$$

thus $$\left(\underbrace{\frac{g_T(S+P)}{g_T(P)}}\right)^n = 1$$

and so $\%$ is an n-th root of unity.

Next, the function

$$P \longmapsto \frac{g_T(S+P)}{g_T(P)}$$

is a fn on E. Since the curve is connected and μ_n is finite this function is actually constant. Thus we can define

$$e_n(S,T) := \frac{g_T(S+P)}{g_T(P)}$$

where $P, S+P \notin \operatorname{supp} \operatorname{div} g_T$.

Theorem part (i):

e_n is bilinear

Pf Linearity in S:

$$e_n(S_1, T) \cdot e_n(S_2, T)$$

$$= \frac{g_T(S_1+P)}{g_T(P)} \cdot \frac{g_T(S_2+S_1+P)}{g_T(S_1+P)}$$

$$= \frac{g_T((S_2+S_1)+P)}{g_T(P)} = e_n(S_1+S_2, T)$$

Linearity in T: let $T_1, T_2 \in E$, $T_3 := T_1 + T_2$.

We have fns; g_{T_i} and f_{T_i}

with $f_{T_i} \circ [n] = g_{T_i}^n$.

Compute:

$$\operatorname{div}\left(\frac{f_{T_1} \cdot f_{T_2}}{f_{T_3}}\right) = n[T_1] + n[T_2] - n[T_3] - n[O].$$

Also we have a function h such that

$$\operatorname{div}(h) = [T_1] + [T_2] - [T_3] - [O].$$

and so

$$\operatorname{div}(h^n) = \operatorname{div}\left(\frac{f_{T_1} \cdot f_{T_2}}{f_{T_3}}\right).$$

Thus $f_{T_1} \cdot f_{T_2} = c \cdot h^n \cdot f_{T_3}$

for some constant $c \in \bar{k}^\times$.

This implies

$$g_{T_1}^n \cdot g_{T_2}^n = c \cdot (h \circ [n])^n \cdot g_{T_3}^n$$

and so there is a constant $d \in \bar{k}^\times$ with $d^n = c$:

$$g_{T_1} \cdot g_{T_2} = d \cdot (h \circ [n]) \cdot g_{T_3} .$$

Now

$$e_n(S, T_1) \cdot e_n(S, T_2)$$

$$= \frac{g_{T_1}(S+P)}{g_{T_1}(P)} \cdot \frac{g_{T_2}(S+P)}{g_{T_2}(P)}$$

$$= \underbrace{\frac{d\, h(\overbrace{n(S+P)}^{=nP})}{d\, h(nP)}}_{1} \cdot \frac{g_{T_3}(S+P)}{g_{T_3}(P)}$$

$$= e_n(S, \underset{T_1+T_2}{\underset{\shortparallel}{T_3}}) .$$

$\square$

<u>Thm (ii)</u> e_n is non-degenerate:

$$\forall S: e_n(S,T) = 1 \quad \Rightarrow \quad T = \mathcal{O}$$

<u>Pf</u> By assumption

$$e_n(S,T) = \frac{g_T(S+P)}{g_T(P)} = 1 \quad \text{for every } S \in E[n]$$

I.e. for all $P \in E$ and $S \in E[n]$:

$$g_T(S+P) = g_T(P).$$