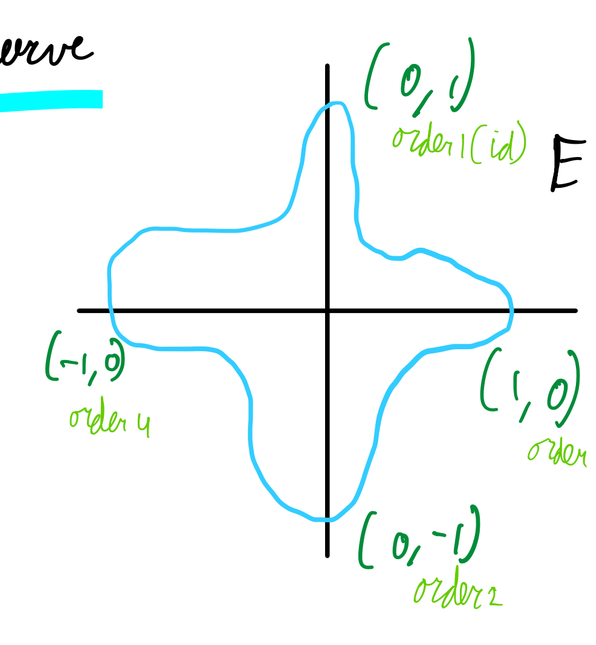
Lecture 3
Tuesday, 13 September 2022 13:28

Edwards curve



$E: x^2+y^2 = 1+dx^2y^2$
for $d<0$

these 4 points exist over any finite field
points (b, b) have order 8

also mod p these 4 points exist,
and they have the same order using the same addition formulas

$$(x_1,y_1)+(x_2,y_2) = \left(\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right)$$

A point P has order k if $k>0$ is the smallest integer with kP = identity; here identity $=(0,1)$

Oops, denominators! Is P_1+P_2 actually defined? Here; argument over $\mathbb{R}$;
watch ECC part I (video from last year) for the general proof.

If P_1 on curve, then x^2+y^2 (≥ 0) $= 1+dx^2y^2$ ($d>0$)

$dx^2y^2 < -1$

$0 < \sqrt{|d|}\ |x_1y_1| < 1$

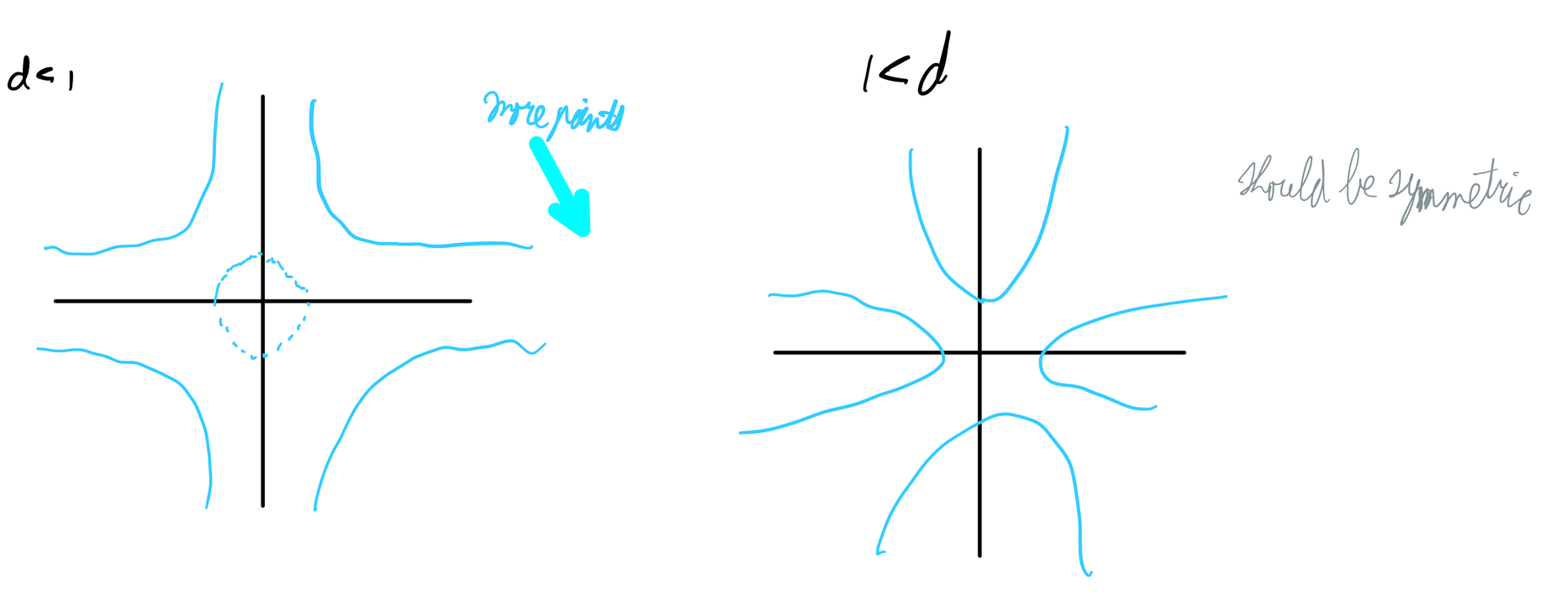
if x_1 or y_1 is 0, the denominators are equal to 1; else

This holds for P_1 and P_2, so $i \in \{1,2\}$ ($0<\sqrt{|d|}\ |x_iy_i|<1$)

The the denominators are $1 \pm dx_1y_1x_2y_2 = 1 \pm \sqrt{|d|}^2\ |x_1y_1|\,|x_2y_2|$
ignore absolute values, to get $\pm$? $= 1 \pm$ something in $(-1,1)$

Hence the denominator is unequal to 0.

This fails for $d>0$ at the first step $dx_1^2y_1^2<1$



no exceptions to the addition law for $d<0$, else there are exceptions
Over $\mathbb{F}_p$, the condition becomes d is not a square

Note: over $\mathbb{F}_p^*$ (without 0), there are $\frac{p-1}{2}$ squares, $\frac{p-1}{2}$ non-squares (and 0 for $\mathbb{F}_p$)

Edwards curves form a group, with
addition works for any P_1, P_2 for d is not a square
associativity (ask Sagemath)
neutral element / identity: $(0,1)$ see homework
$-P = -(x,y) = (-x,y)$ because

$$(x,y)+(-x,y) = \left(\frac{xy+(-x)y}{\cdots}, \frac{yy-x(-x)}{1-dx(-x)yy}\right)$$

$$= \left(0, \frac{y^2+x^2}{1+dx^2y^2}\right)$$

1, because $x^2+y^2 = 1+dx^2y^2$ for points on an Edwards curve

$= (0,1)$ = identity / neutral element ✓

This means we get a group.
This group is commutative, because I can flip (x_1,y_1) and (x_2,y_2) (every expression is symmetric)

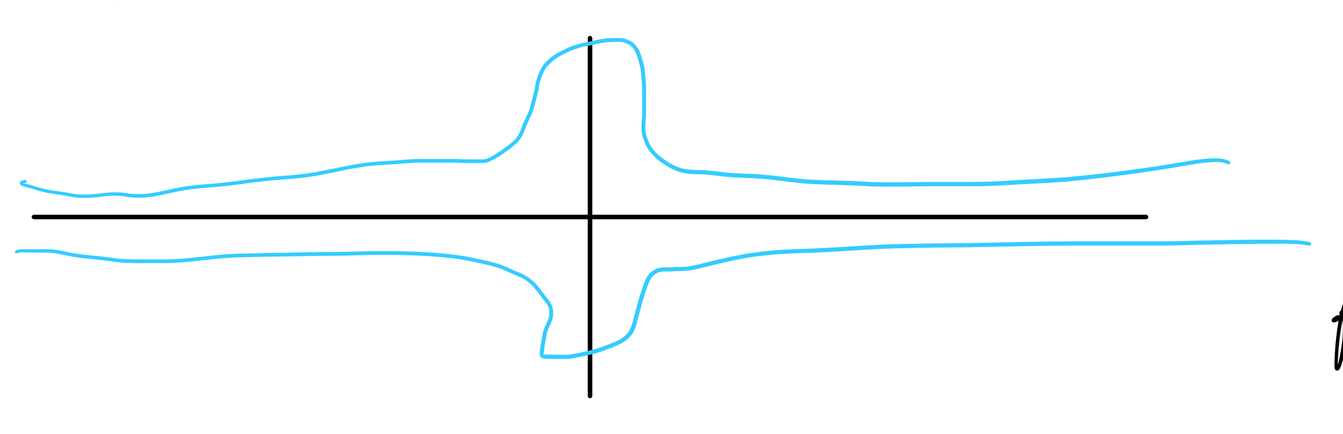
Note: because of the symmetry (and hence $(0,\pm 1)$ and $(\pm 1, 0)$) we get that the number of points on E over $\mathbb{F}_p$ is a multiple of 4.

In general, the number of points is in $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.

Generalization: twisted Edwards curves

$ax^2+y^2 = 1+dx^2y^2$ (no brackets: we have $(ax^2)+y^2$!) with $a, d \neq 0$ and $a \neq d$

This gives, for example



for $a, d<0$

over $\mathbb{F}_p$ ($p>2$), these still have group order divisible by 4 ~ from points of order 4 or more points of order 2

$$(x_1,y_1)+(x_2,y_2) = \left(\frac{x_1y_2+x_2y_1}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-ax_1x_2}{1-dx_1x_2y_1y_2}\right)$$

addition law is complete, if and only if d is not square and a is a square

Elliptic curves in the dark ages, i.e. prior to 2007

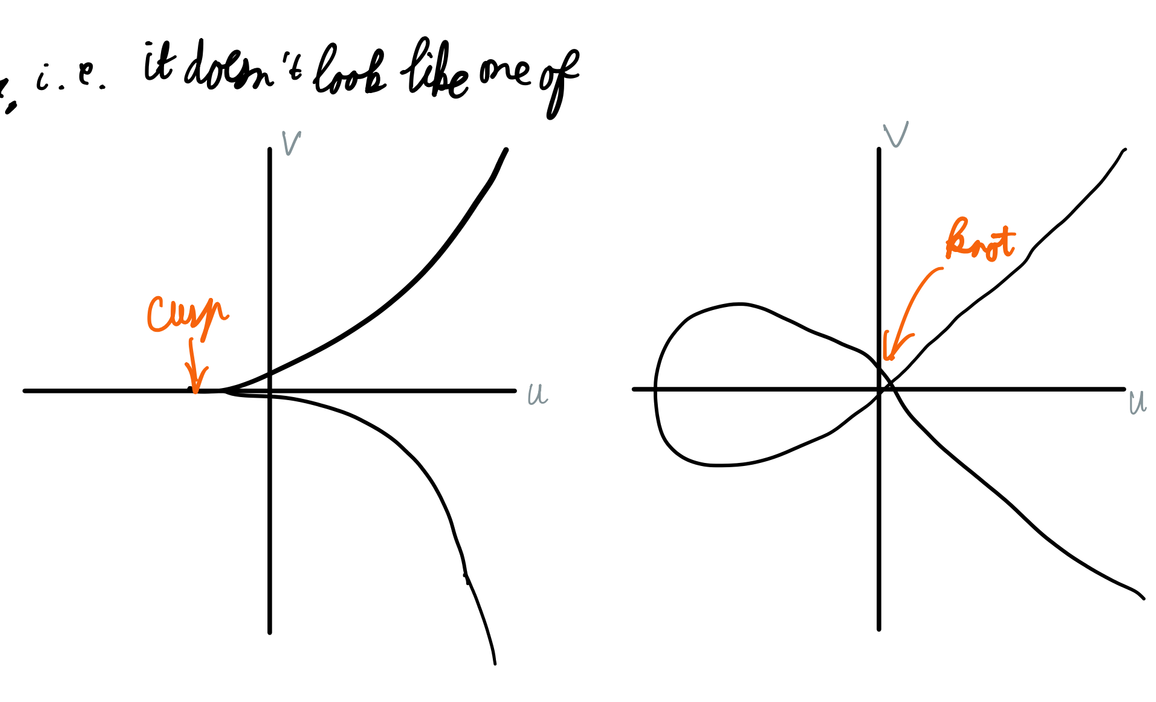
Weierstrass curves

over $\mathbb{R}$ and over $\mathbb{F}_p$, $p>3$, we can

write each elliptic curve as

$$v^2 = u^3 + c_4u + c_6$$
with $4c_4^3+27c_6^2 \neq 0$

The latter constraint ensures that the curve is non-singular, i.e. it doesn't look like one of



Most general form (works for any field)

$$v^2+a_1vu+a_3v = u^3+a_2u^2+a_4u+a_6$$
is an elliptic curve if it's not singular

for each term, give
v weight 3
u weight 2
then (index on a + power of $v \cdot 3$ + power of $u \cdot 2 = 6$)
Hence no a_5 (there is no combination of powers of u and v for which this is equal to 6).

Can do isomorphic transformations, e.g. $v \to v - \frac{a_1u+a_3}{2}$ for $p \neq 2$ (as in $\mathbb{F}_p$)

$u \to u$ is an invertible map and brings curve to $v^2 - 2\frac{a_1u+a_3}{2}v + \left(\frac{a_1u+a_3}{2}\right)^2 + a_1vu - a_1\frac{a_1u+a_3}{2} + a_3v - a_3\frac{a_1u+a_3}{2}$ ("a_1uv", "a_3v")

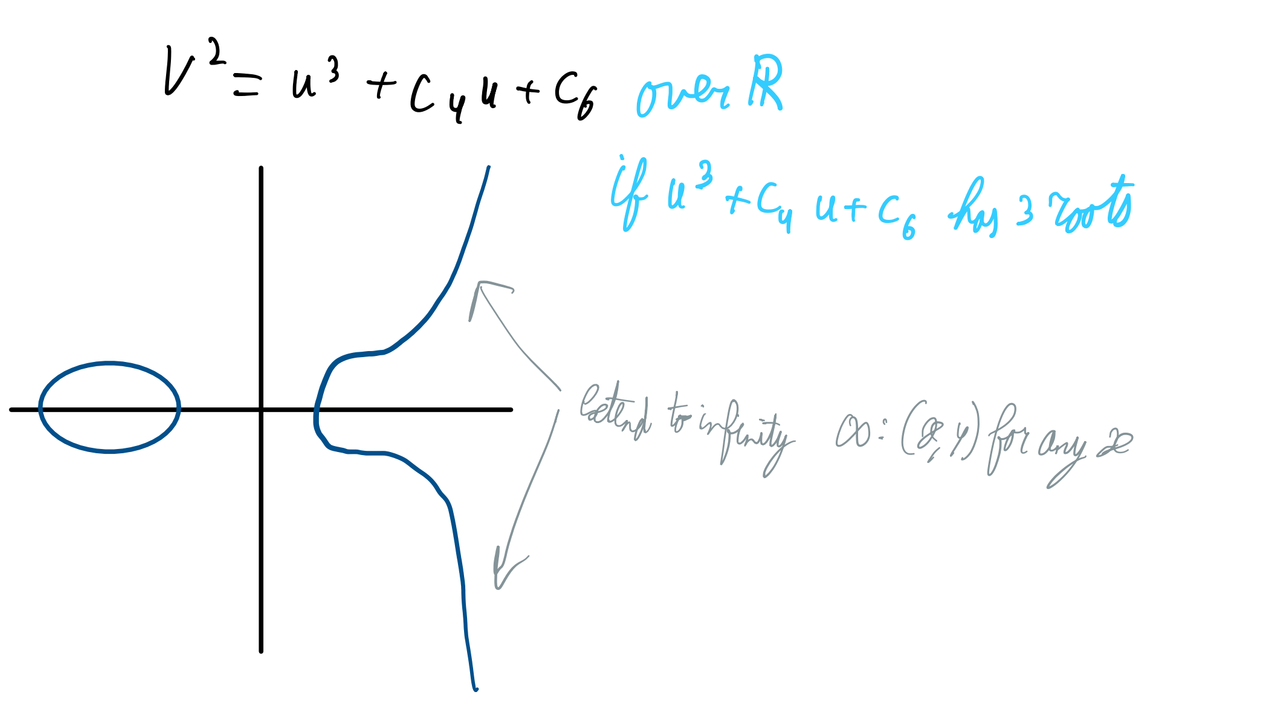
$$= v^2 + \left(\frac{a_1u+a_3}{2}\right)^2 - a_1\frac{a_1u+a_3}{2}u - a_3\frac{a_1u+a_3}{2}$$

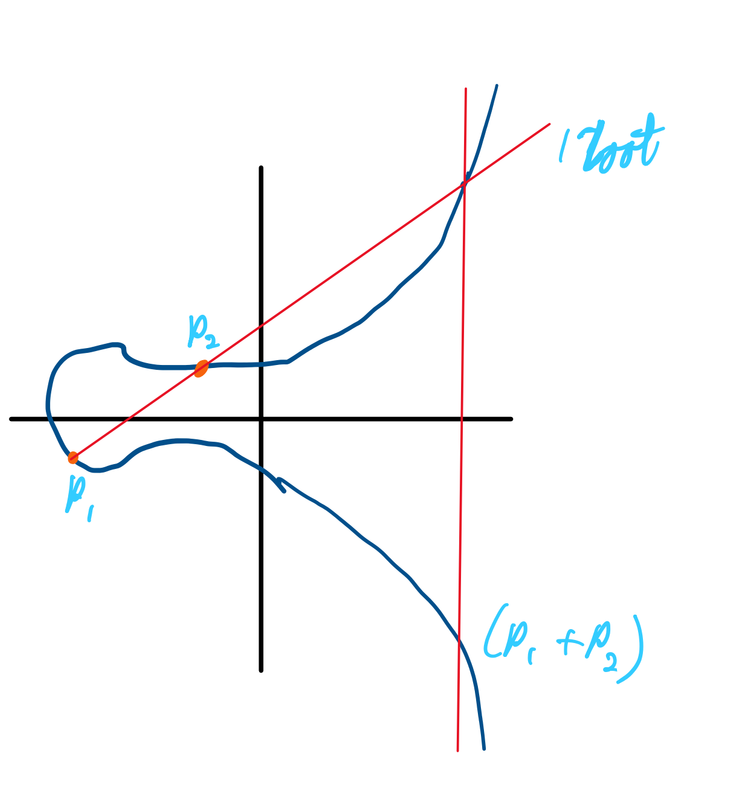
no more terms linear in v (got cancelled)
move the terms over to the right-hand side;
degree is at most 2, so RHS (right-hand side) stays with
monic u^3 (leading term has coefficient 1 (one)), rest changes to $v^2 = u^3+b_2u^2+b_4u+b_6$ for some b:
once more with $u \to u - \frac{b_2}{3}$ for $p>3$

gets to $v^2 = u^3+c_4u+c_6$

picture of short Weierstrass form:

$v^2 = u^3+c_4u+c_6$ over $\mathbb{R}$





Any Weierstrass curve has a point at infinity in v direction
This point P_∞ (or ∞) is the neutral element of addition on the Weierstrass curve

---

We add P_1 and P_2 by drawing the line through them, finding the third point of intersection and taking its mirror image with respect to the u-axis as P_1+P_2

Use tangent if points are equal.
For equal, but negative points, i.e. $Q+(-Q)$, we have $Q+(-Q) = P_\infty$ (point for v direction)