Different forms of elliptic curves

Tanja Lange

Department of Mathematics and Computer Science

Technische Universiteit Eindhoven

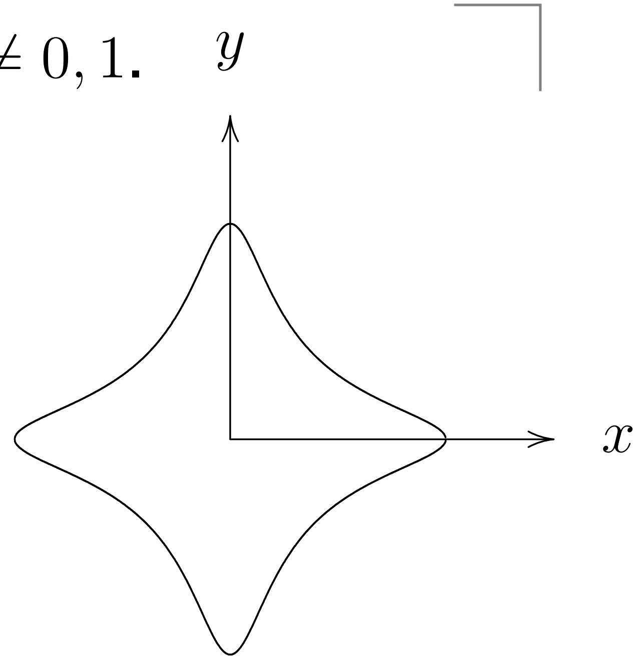
tanja@hyperelliptic.org

16.09.2008

How to add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Recap of Dan's talk and exercises:

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

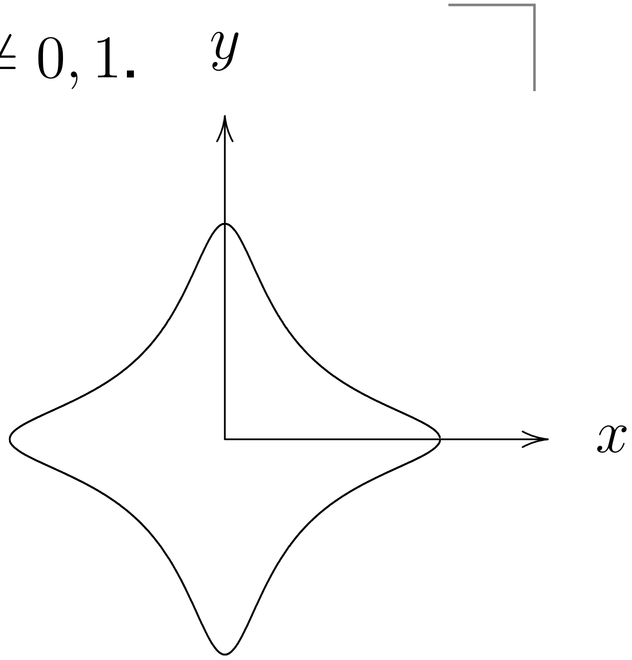
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$.
- $-(x_1, y_1) = (-x_1, y_1)$.
- $(0, -1)$ has order

How to add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x,y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Recap of Dan's talk and exercises:

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

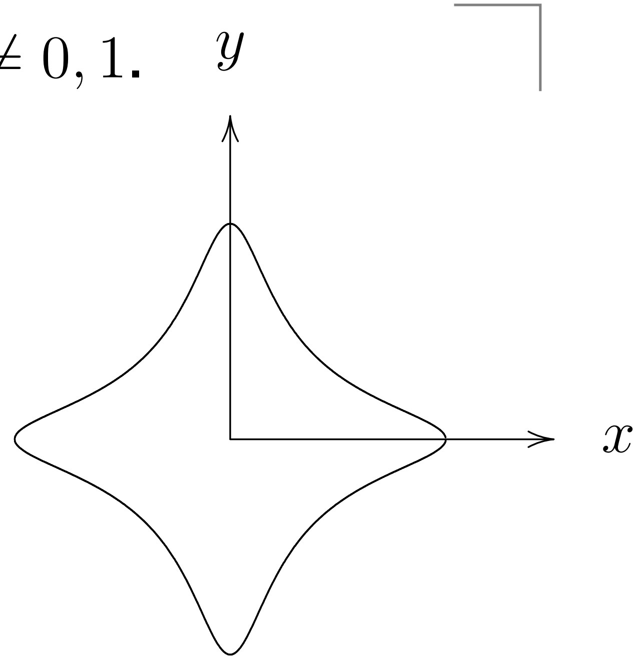
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$.
- $-(x_1, y_1) = (-x_1, y_1)$.
- $(0, -1)$ has order 2; $(1, 0)$ and $(-1, 0)$ have order

How to add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Recap of Dan's talk and exercises:

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$.
- $-(x_1, y_1) = (-x_1, y_1)$.
- $(0, -1)$ has order 2; $(1, 0)$ and $(-1, 0)$ have order 4.

Explicit formulas: addition

- $(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- Avoid inversions: Use $(X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$ to represent $(x_1, y_1) = (X_1/Z_1, Y_1/Z_1)$, i. e., $(X_1 : Y_1 : Z_1) = (\lambda X_1 : \lambda Y_1 : \lambda Z_1)$ for $\lambda \neq 0$.
- Addition formulas in projective coordinates:

$$\begin{aligned}
A &= Z_1 \cdot Z_2;\ B = A^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2;\\
E &= d \cdot C \cdot D;\ F = B - E;\ G = B + E;\\
X_3 &= A \cdot F \cdot ((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D);\\
Y_3 &= A \cdot G \cdot (D - C);\\
Z_3 &= F \cdot G.
\end{aligned}$$

- Needs 10M + 1S + 1D + 7A.

Doubling

- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$

Doubling

- $P + Q = \left(\dfrac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\dfrac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \dfrac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$

Doubling

- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1},\frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$
- No reason that the denominators should be 0. Actually, Dan Bernstein showed yesterday that they are never 0 for non-square d.
- Addition law produces correct result also for doubling.

Doubling

- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1}, \frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$
- No reason that the denominators should be 0. Actually, Dan Bernstein showed yesterday that they are never 0 for non-square d.
- Addition law produces correct result also for doubling.
- Unified group operations!

Doubling

- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1},\frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$
- No reason that the denominators should be 0. Actually, Dan Bernstein showed yesterday that they are never 0 for non-square d.
- Addition law produces correct result also for doubling.
- Unified group operations!
- Having addition law work for doubling removes some checks from the code.

Nice features of the addition law

- Addition law is symmetric in both inputs; easy to see that it is commutative.
- Neutral element of addition law is affine point, formulas handle correctly the addition of $(0, 1)$ to any point.
- Addition law works correctly for adding $P = (x_1, y_1)$ to its negative $(-x_1, y_1)$, producing $(0, 1)$ as output.
- Addition law produces correct result also for doubling.
- No need to distinguish addition and doubling in code. In double-and-add method (see Christophe Doche's talk yesterday) the doublings occur planned while an addition might accidentally be faced with two equal inputs.

Faster dedicated doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$
  $$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$

Faster dedicated doubling

- $$(x_1,y_1)+(x_1,y_1)=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1},\frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right)$$
  $$=\left(\frac{2x_1y_1}{1+d(x_1y_1)^2},\frac{y_1^2-x_1^2}{1-d(x_1y_1)^2}\right)$$

  Use curve equation $x^2+y^2=1+dx^2y^2$.

Faster dedicated doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$
$$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$
$$= \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)}\right)$$

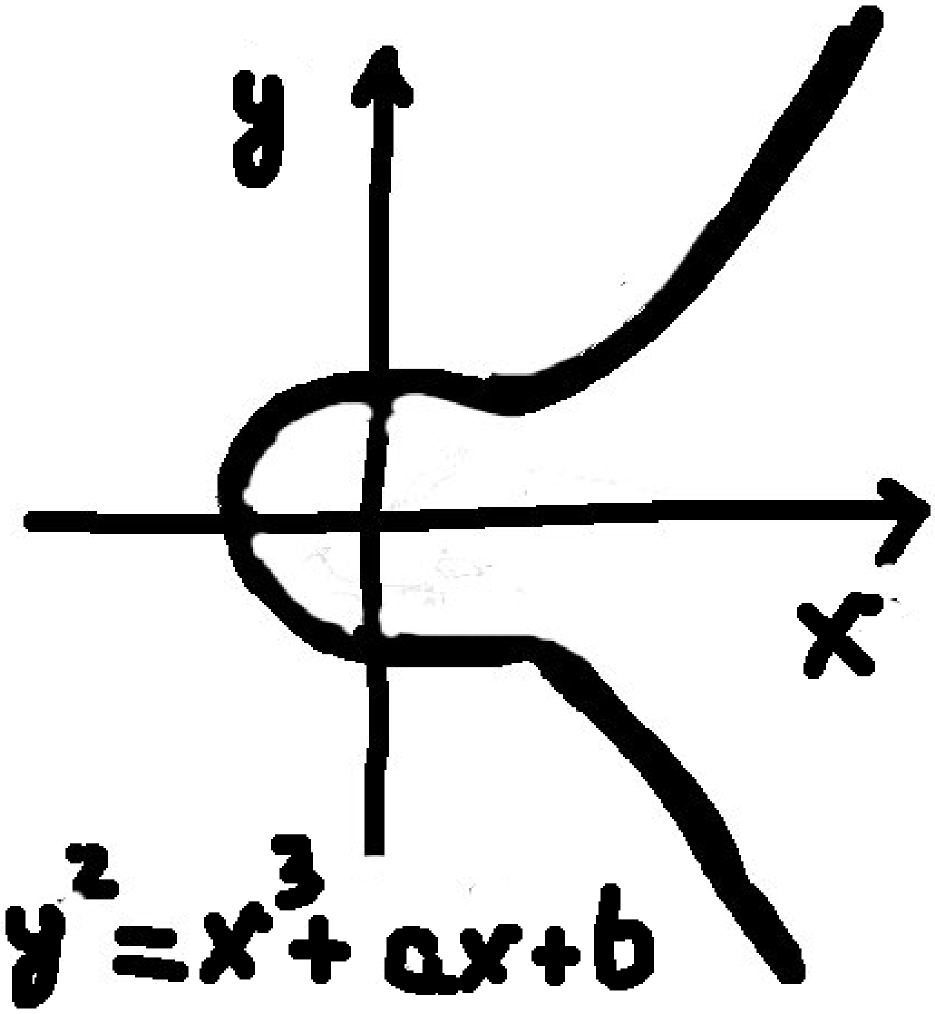
Faster dedicated doubling

- $$(x_1,y_1)+(x_1,y_1) = \left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1}, \frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right)$$
  $$= \left(\frac{2x_1y_1}{1+d(x_1y_1)^2}, \frac{y_1^2-x_1^2}{1-d(x_1y_1)^2}\right)$$
  $$= \left(\frac{2x_1y_1}{x_1^2+y_1^2}, \frac{y_1^2-x_1^2}{2-(x_1^2+y_1^2)}\right)$$
- Doubling formulas in projective coordinates:
  $$\begin{aligned} B &= (X_1+Y_1)^2;\ C = X_1^2;\ D = Y_1^2; \\ E &= C+D;\ H = Z_1^2;\ J = E-2H; \\ X_3 &= (B-E)\cdot J;\ Y_3 = E\cdot(C-D);\ Z_3 = E\cdot J. \end{aligned}$$
- Needs 3M + 4S + 6A.

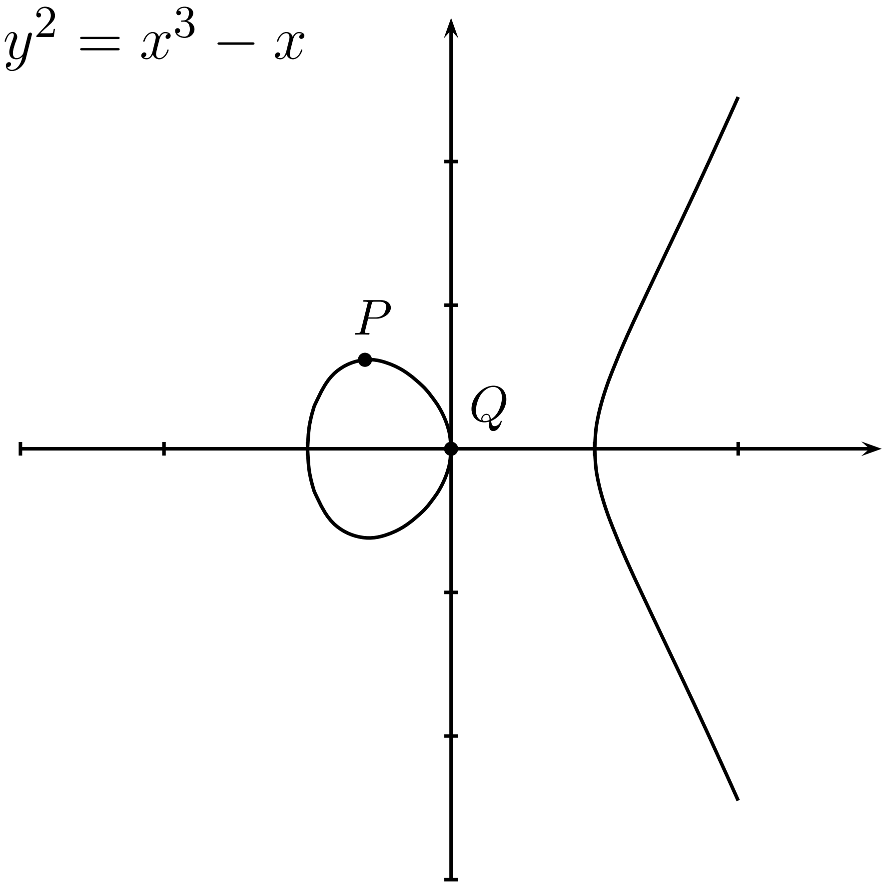
The dark ages . . .

...

• • •

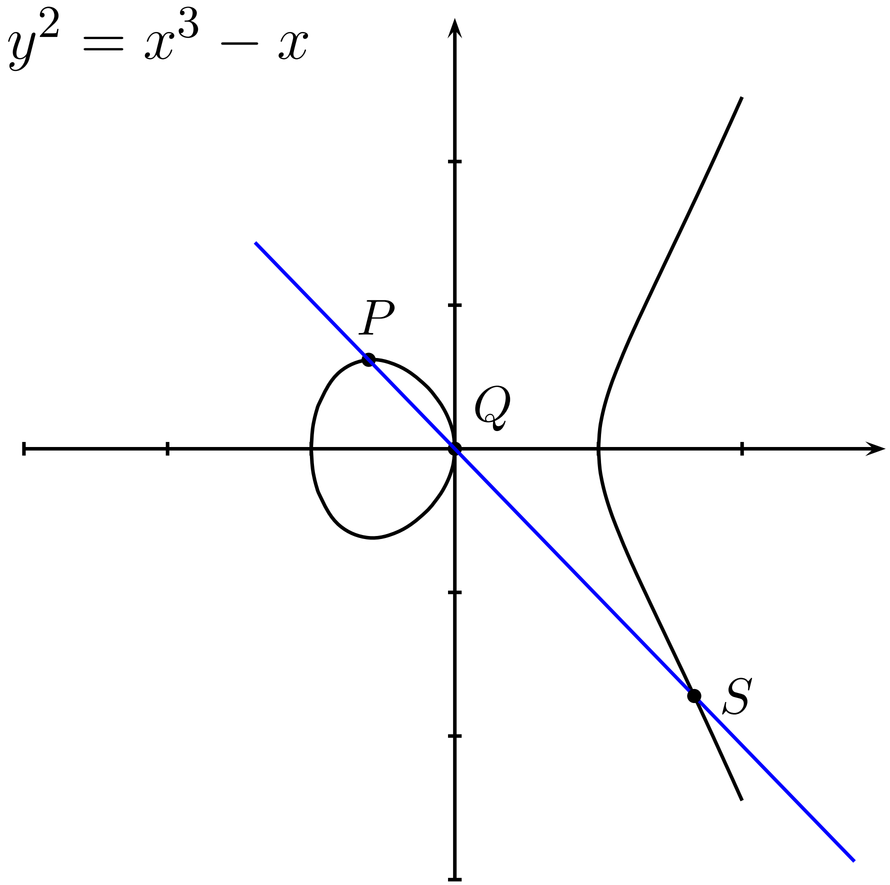

y
x
y²=x³+ax+b

Group Law in $E(\mathbb{R})$



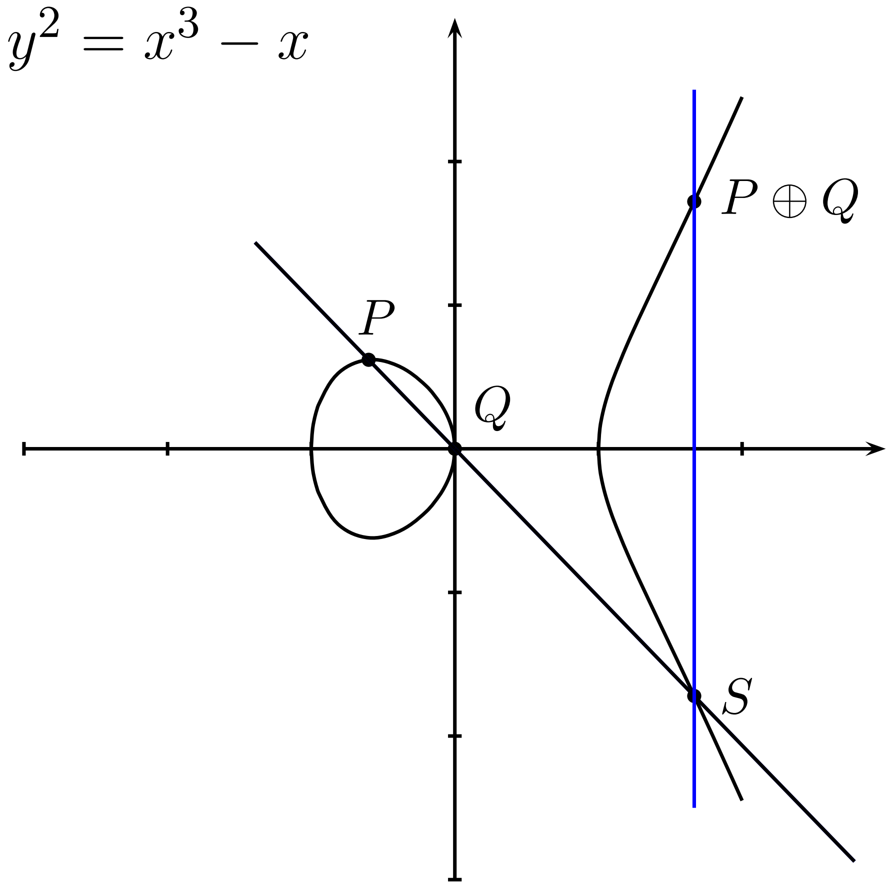
$P = (x_P, y_P), Q = (x_Q, y_Q)$ satisfy curve equation.

Group Law in $E(\mathbb{R})$



$P = (x_P, y_P), Q = (x_Q, y_Q)$ satisfy curve equation.

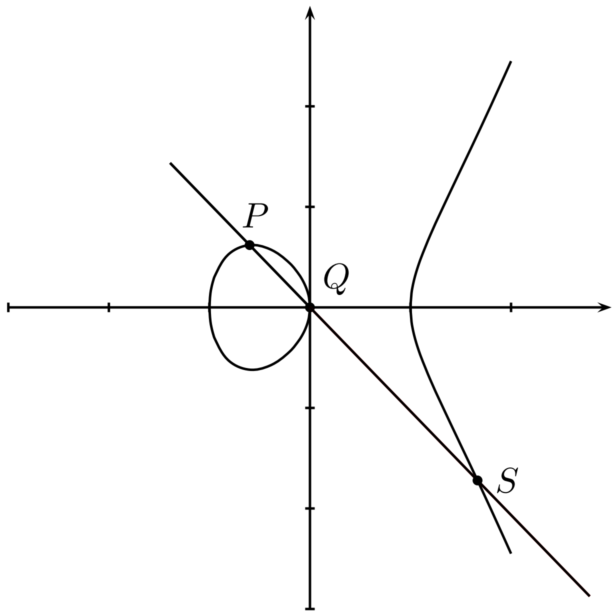
Group Law in $E(\mathbb{R})$



$P = (x_P, y_P), Q = (x_Q, y_Q)$ satisfy curve equation.

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



Line $y = \lambda x + \mu$ has slope

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}.$$

Equating gives

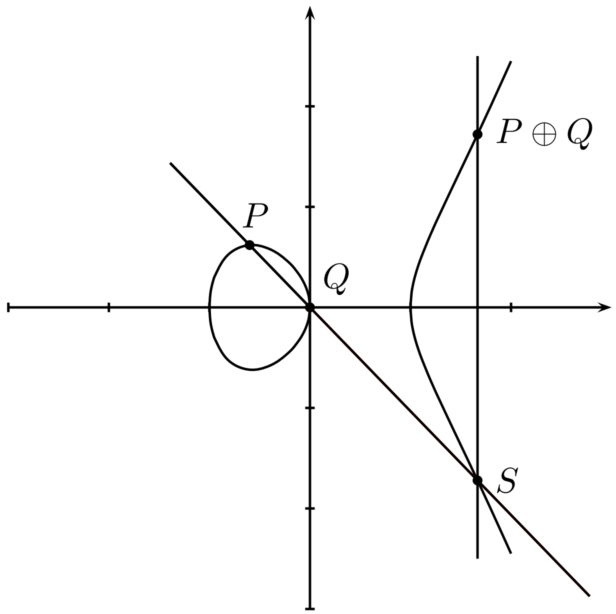
$$(\lambda x + \mu)^2 = x^3 + a_4 x + a_6.$$

This equation has 3 solutions, the x-coordinates of P, Q and S, thus

$$\begin{aligned}(x - x_P)(x - x_Q)(x - x_S) &= x^3 - \lambda^2 x^2 + (a_4 - 2\lambda\mu)x + a_6 - \mu^2 \\ x_S &= \lambda^2 - x_P - x_Q\end{aligned}$$

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



Point P is on line, thus

$$y_P = \lambda x_P + \mu, \text{ i.e.}$$
$$\mu = y_P - \lambda x_P,$$

and

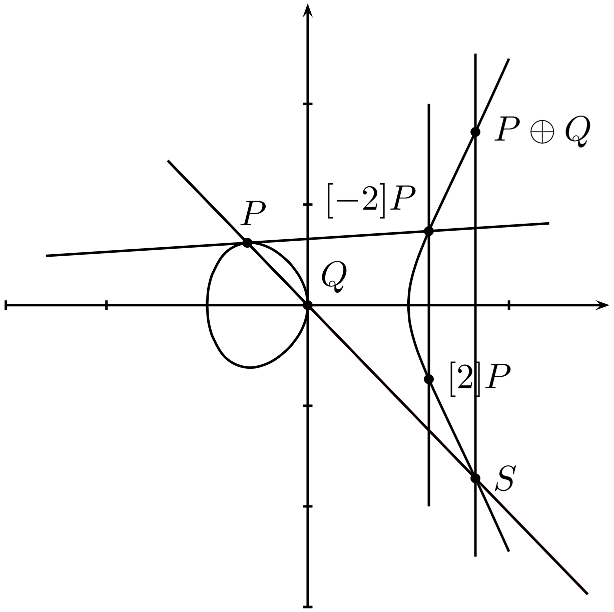
$$\begin{aligned} y_S &= \lambda x_S + \mu \\ &= \lambda x_S + y_P - \lambda x_P \\ &= \lambda(x_S - x_P) + y_P \end{aligned}$$

Point $P \oplus Q$ has the same x-coordinate as S but negative y-coordinate:

$$x_{P\oplus Q} = \lambda^2 - x_P - x_Q, \quad y_{P\oplus Q} = \lambda(x_P - x_{P\oplus Q}) - y_P$$

Group Law (q odd)

$$E : y^2 = x^3 + a_4x + a_6, \ a_i \in \mathbb{F}_q$$



When doubling, use tangent at P. Compute slope λ via partial derivatives of curve equation:

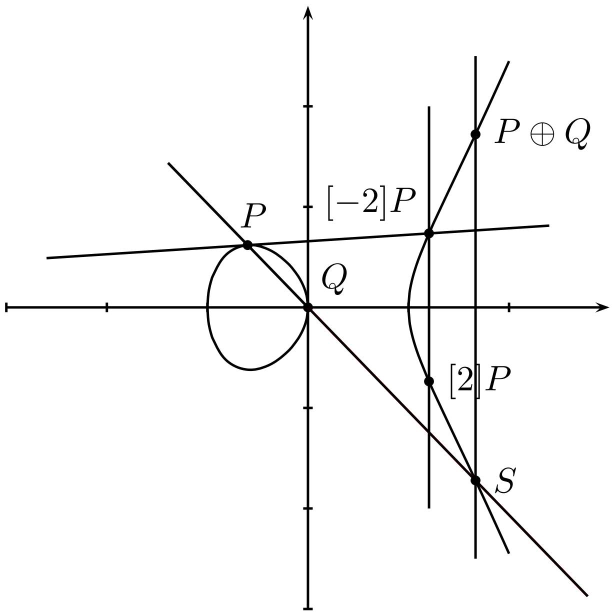
$$\lambda = \frac{3x_P^2+a_4}{2y_P}.$$

Remaining computation identical to addition.

$$x_{[2]P} = \lambda^2 - 2x_P, \quad y_{[2]P} = \lambda(x_P - x_{[2]P}) - y_P$$

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



Tangent at Q is vertical $x = x_Q$.
When adding $P \oplus Q$ and S, connecting line is vertical.

Third point online is P_∞, a point infinitely far up on the y-axis:

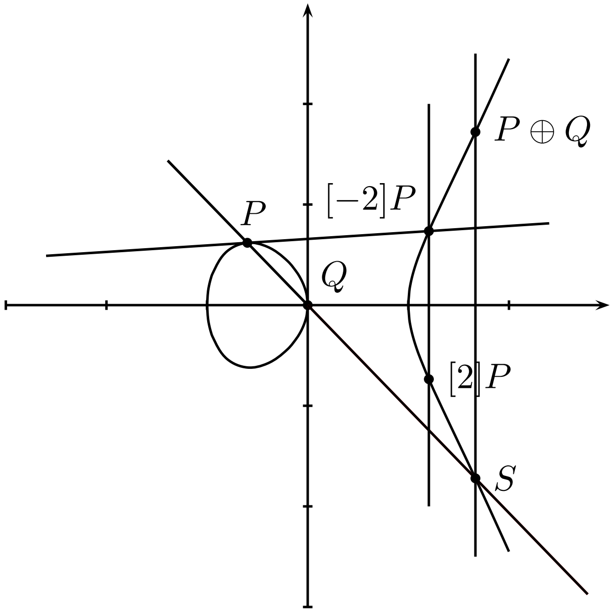
$$[2]Q = P_\infty; (P \oplus Q) \oplus S = P_\infty.$$

$$P \oplus P_\infty = P; P_\infty \oplus P_\infty = P_\infty.$$

P_∞ is neutral element; $-(x_1, y_1) = (x_1, -y_1)$.

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6, \; a_i \in \mathbb{F}_q$$



In general, for $(x_P, y_P) \neq (x_Q, -y_Q)$:

$$\begin{aligned}(x_P, y_P) \oplus (x_Q, y_Q) &= \\ &= (x_{P\oplus Q}, y_{P\oplus Q}) = \\ &= (\lambda^2 - x_P - x_Q, \lambda(x_P - x_{P\oplus Q}) - y_P),\end{aligned}$$

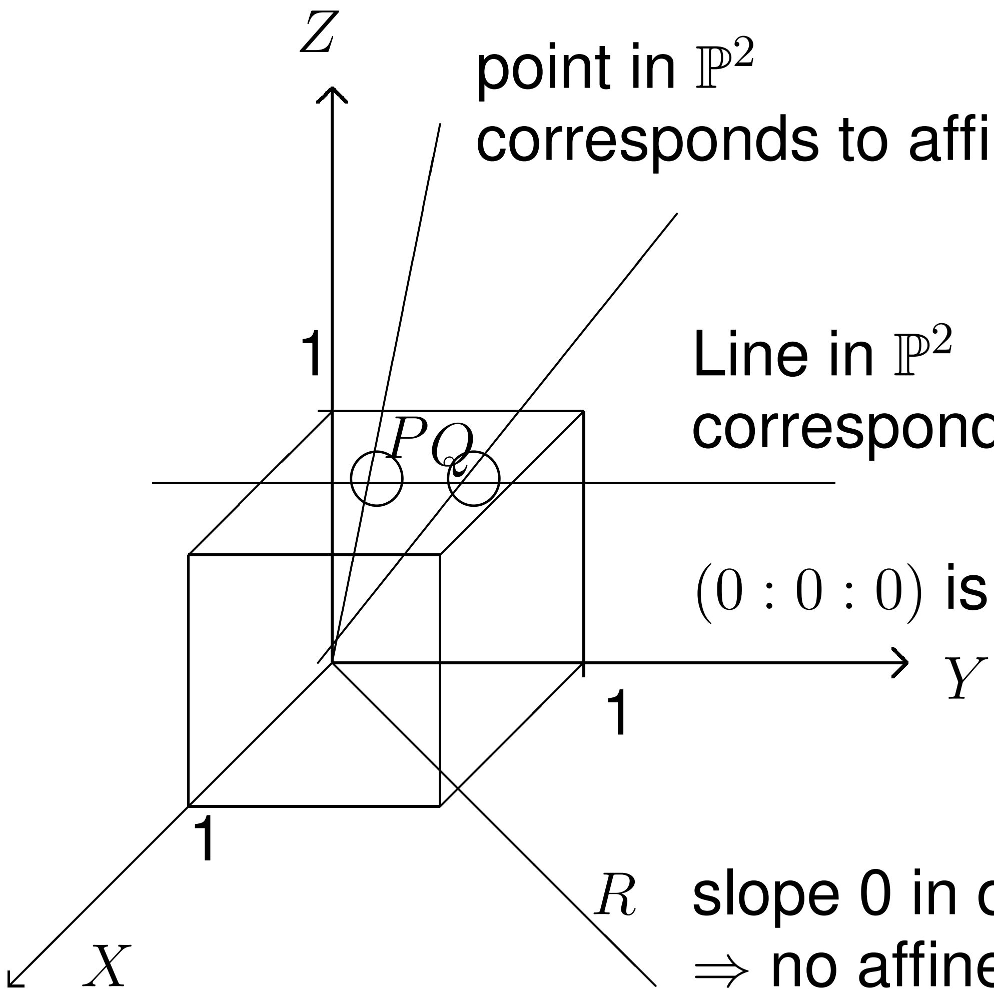
where

$$\lambda = \begin{cases} (y_Q - y_P)/(x_Q - x_P) & \text{if } x_P \neq x_Q, \\ (3x_P^2 + a_4)/(2y_P) & \text{if } P = Q \end{cases}$$

…and all the other cases …

Projective space $\mathbb{P}^2$

Let (x, y) correspond to $(X : Y : Z)$ if $x = X/Z, y = Y/Z$.
$(\lambda X : \lambda Y : \lambda Z)$ and $(X : Y : Z)$ represent same point ($\lambda \neq 0$).



point in $\mathbb{P}^2$
corresponds to affine point

Line in $\mathbb{P}^2$
corresponds to plane in $\mathbb{R}^3$

$(0 : 0 : 0)$ is excluded as point

slope 0 in direction Z
$\Rightarrow$ no affine point

Where does P_∞ come from?

Projective points $(X:Y:Z)$ correspond to affine points (x,y) if and only if $Z \neq 0$.
Replace x, y in Weierstrass equation $y^2 = x^3 + ax + b$ and multiply by Z^3:

$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3.$$

Each affine point (x_P, y_P) on the curve corresponds to a projective point $(\lambda x_P : \lambda y_P : \lambda)$. There might be additional solutions with $Z = 0$:

$$0 = X^3 + 0 \Rightarrow X = 0; Y \text{ arbitrary}$$

$(0:1:0)$ is additional projective point satisfying the projective equation. In this representation $P_\infty = (0:1:0)$.
This point is on the curve, thus all the special cases.

How about Edwards curves?

Projective equation:

$$X^2Z^2 + Y^2Z^2 = Z^4 + dX^2Y^2.$$

At $Z = 0$ we find

$$0 + 0 = 0 + dX^2Y^2 \Rightarrow X = 0 \text{ or } Y = 0.$$

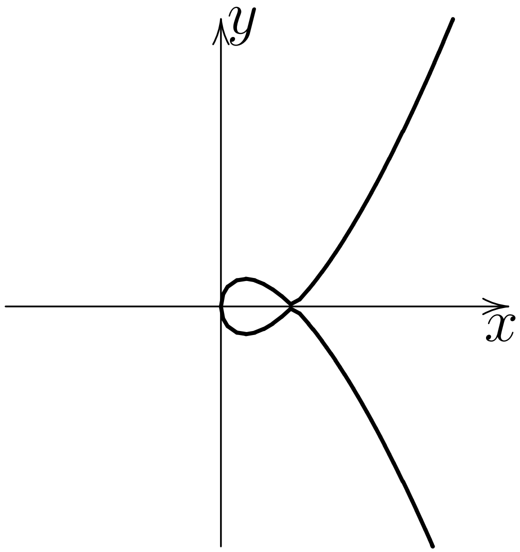
There are two points at infinity $(1 : 0 : 0)$ and $(0 : 1 : 0)$. So why no problems with exceptions????

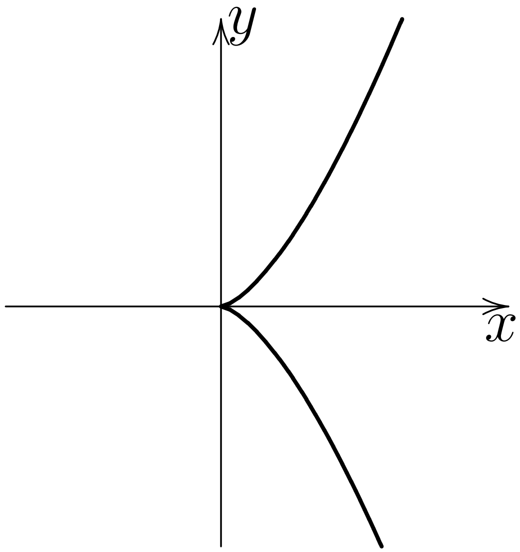
Let's look at $(1 : 0 : 0)$; the other point works the same with X and Y reversed.

So far ignored: singularities.

Singularities

Let $F(x,y)=0$ define a curve C and let $P=(x_P,y_P)$ be on the curve, i.e. $F(x_P,y_P)=0$. The curve is singular in P if both partial derivatives F_x and F_y vanish in P.
A curve is non-singular if there is no singular point P on the curve over the ground field and any extension field.





Study of Edwards curve at infinity I

Around $(1:0:0)$ we can describe the curve by

$$z^2 + y^2z^2 = z^4 + dy^2.$$

The point $(0,0)$ is on this curve. The partial derivatives

$$2yz^2 - 2dy, \quad 2z + 2y^2z - 4z^3$$

both vanish at $(0,0)$, so this is a singularity.

The group operation actually wants a non-singular curve. One can "blow-up" singularities. Locally this means introducing an extra dimension.

Study of Edwards curve at infinity II

$$z^2 + y^2z^2 = z^4 + dy^2.$$

Put $y = tz$, then

$$z^2 + y^2z^2 = z^4 + dy^2 \Leftrightarrow z^2 + t^2z^4 = z^4 + dt^2z^2$$

and the latter has z^2 as a factor. We can thus study the blow up with equation

$$1 + t^2z^2 = z^2 + dt^2.$$

For $z = 0$ we find a solution $dt^2 = 1$, i.e. $t = \pm 1/\sqrt{d}$, so the blow-ups of $(1 : 0 : 0)$ are defined where d is a square.
One can check that $(\pm 1/\sqrt{d}, 0)$ are nonsingular on the blow-up. Note that $(1 : 0 : 0)$ gave rise to 2 points.

Relationship between Weierstrass and Edwards curves

Birational equivalence

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.
- Let $P_4 = (u_4, v_4)$ have order 4 and shift u s.t. $2P_4 = (0,0)$. Then Weierstrass form:
$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u.$$
- Define $d = 1 - (4u_4^3/v_4^2)$.
- The coordinates $x = v_4 u/(u_4 v),\ y = (u - u_4)/(u + u_4)$ satisfy
$$x^2 + y^2 = 1 + dx^2y^2.$$
- Inverse map $u = u_4(1+y)/(1-y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points. Exceptional points have $v(u + u_4) = 0$.

Exceptional points of the map

- Points with $v(u + u_4) = 0$ on Weierstrass curve map to points at infinity on desingularization of Edwards curve.
- Reminder: $d = 1 - (4u_4^3/v_4^2)$.
- $u = -u_4$ is u-coordinate of a point iff

$$\begin{aligned} & (-u_4)^3 + (v_4^2/u_4^2 - 2u_4)(u_4)^2 + u_4^2(u_5) \\ = \; & v_4^2 - 4u_4^3 = v_4^2 d \end{aligned}$$

  is a square, i. e., iff d is a square.
- $v = 0$ corresponds to $(0, 0)$ which maps to $(0, -1)$ on Edwards curve and to solutions of $u^2 + (v_4^2/u_4^2 - 2u_4)u + u_4^2 = 0$. Discriminant is

$$(v_4^2/u_4^2 - 2u_4)^2 - 4u_4^2 = v_4^4 d,$$

  i. e., points defined over k iff d is a square.

Complete addition law

- Previous slide shows that for $d \neq \square$ in K all points of the Weierstrass curve map to the affine part of the Edwards curve; where we extend the map by $P_\infty \mapsto (0,1)$ and $(0,0) \mapsto (0,-1)$.
- Geometric description: The other missing points from the Weierstrass curve correspond to the blow-ups of $(1:0:0)$ and $(0:1:0)$ on the Edwards curve. They blow up to two points each on the desingularization of the curve. On both the Weierstrass and the Edwards side these points are defined over $K(\sqrt{d})$.
- Attention: Having no K-rational points at infinity does not guarantee that the formulas are complete:

$$(x_3,y_3) = ((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y_2), (x_1y_1 - x_2y_2)/(x_1y_2 - y_1x_2))$$

is addition on Edwards curve . . . and fails for doublings.

Hasse-Weil theorem

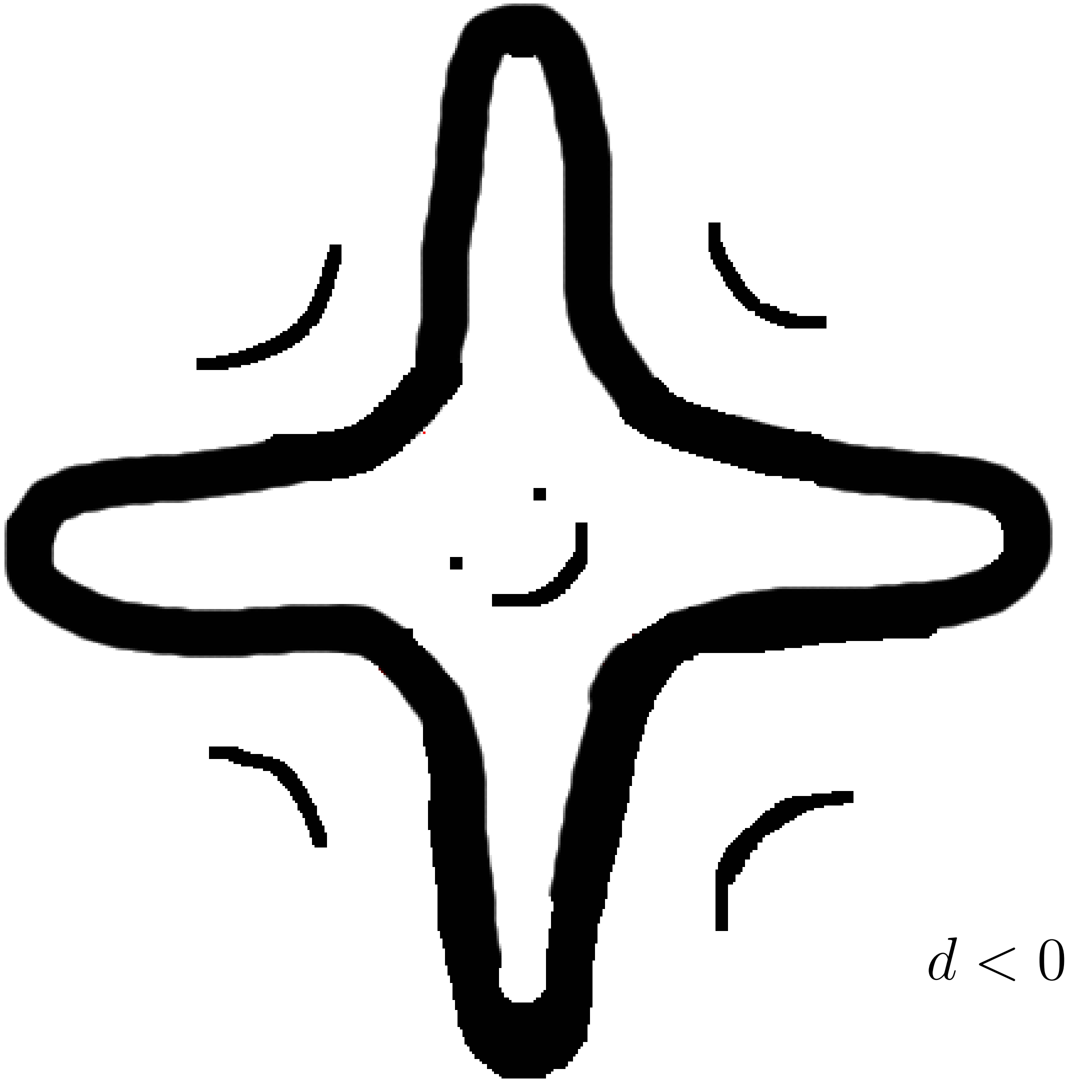
To get a finite group we consider the curves over finite fields; so there are q choices for values of x. In both cases, y satisfies a polynomial of degree 2, which on average will produce a solution for every second value of x. So we expect about q points.

The Hasse-Weil theorem refines this: Let E be an elliptic curve over $\mathbb{F}_q$. We have

$$|E(\mathbb{F}_q)| = q + 1 - t, \text{ where } |t| \leq 2\sqrt{q}.$$

Note that we do count the points at infinity in both cases (provided they are defined over the ground field).

Thank you for your attention!



$d < 0$, non-square!