What is an elliptic curve?

An elliptic curve is a smooth projective plane of genus one with at least one point.

This information together with the theorem of Riemann Roch is enough to derive that any elliptic curve admits an affine equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in k$, where k is the field where the point is defined.

This equation is the general form of a Weierstrass curve.
[The indices actually make sense if you give y weight 3, x weight 2 and ask that the weight + index equals 6.]

In algebraic geometry, smooth means that the curve does not have singularities. Now that we have an equation for the curve we can define singular using the Jacobi criterion: For fields of characteristic larger than 3

A point $P = (x_P, y_P)$ on E is singular if (x, y) also satisfies the two partial derivatives, $2y + a_1x + a_3 = 0$ and $a_1y = 3x^2 + 2a_2x + a_4$.

Note that "point on E" means that the point satisfies the curve equation. Note also that you need to check this for all points over any extension field of k.

Short Weierstrass curves

For fields of characteristic larger than 3 we can transform this equation to one with fewer variables, called *short Weierstrass form*.

Valid transformations are those that keep the curve shape the same, so y^2 and x^3 are monic and no other degrees than in the long equation appear.

This means we can change $y \leftarrow \alpha^3 y + \beta x + \gamma, x \leftarrow \alpha^2 x + \delta$, and divide both sides by α^6. Such transforms are called *curve isomorphisms*.

Short Weierstrass curves

For fields of characteristic larger than 3 we can transform this equation to one with fewer variables, called *short Weierstrass form*.

Valid transformations are those that keep the curve shape the same, so y^2 and x^3 are monic and no other degrees than in the long equation appear.

This means we can change $y \leftarrow \alpha^3 y + \beta x + \gamma, x \leftarrow \alpha^2 x + \delta$, and divide both sides by α^6. Such transforms are called *curve isomorphisms*.

Our first target is to get rid of the $a_1xy + a_3y$ term. If the characteristic is not 2 we can use $y \leftarrow y - (a_1x + a_3)/2$ to reach the form $y^2 = x^3 + a'_2x^2 + a'_4x + a'_6$.

If the characteristic is not 3 we can similarly get rid of the a'_2x^2 term by using $x \leftarrow x - a'_2/3$.

The curve equation $y^2 = x^3 + c_4x + c_6$ is called short Weierstrass form. (In the lecture we used the also common notation $y^2 = x^3 + ax + b$).

Singularities

Let's look for singularities in this form, so we look for points on the curve that satisfy $y = 0$ and $3x^2 + c_4 = 0$.

A singular point on a curve in short Weierstrass form thus has the form $(\, , 0)$. Being on the curve means $0 = x^3 + c_4 x + c_6$, so we have two equations for x.

Let's see whether we have a common root by computing the gcd:
$x^3 + c_4 x + c_6 = (x/3)(3x^2 + c_4) + (2c_4/3)x + c_6$
$3x^2 + c_4 = (9/(2c_4)x - (27c_6/4c_4))((2c_4/3)x + c_6) + c_4 - 27c_6^2/(4c_4^2)$
A singularity exists if and only if the remainder is 0, i.e. if
$c_4 - 27c_6^2/(4c_4^2) = 0$, i.e.

$$4c_4^3 - 27c_6^2 = 0.$$

This was the condition given in class (as $4a^3 - 27b^2$)

How about double roots?

If the curve has the form

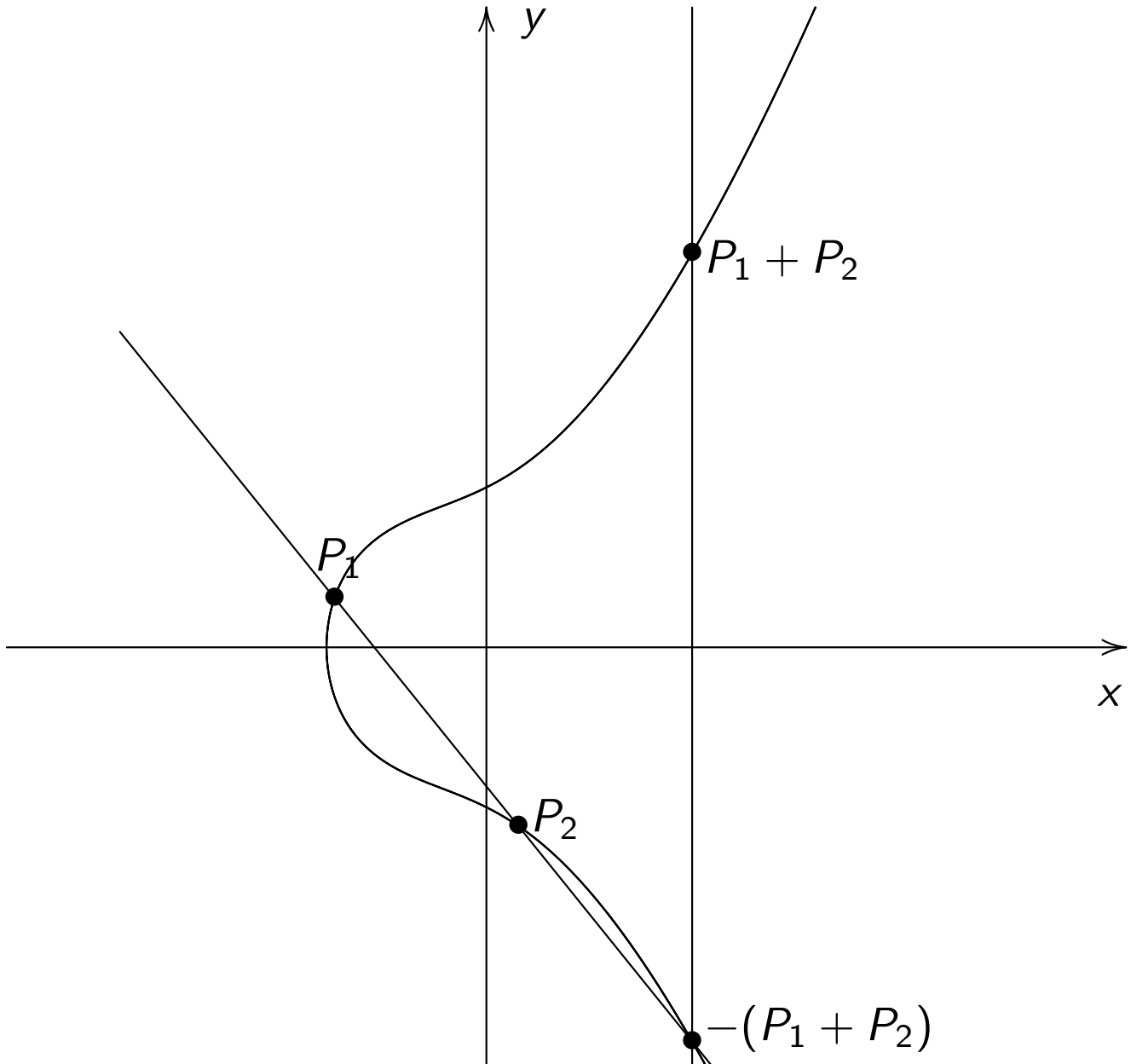
$$y^2 = (x - x_0)(x - x_1)^2$$

then the partial derivatives are $y = 0$ and
$0 = (x - x_1)^2 + 2(x - x_0)(x - x_1)$ using the chain law and $(x_1, 0)$ is a point on the curve that satisfies both partial derivatives, thus is a singular point.

Since an elliptic curve is non singular, the case of two identical roots cannot appear.

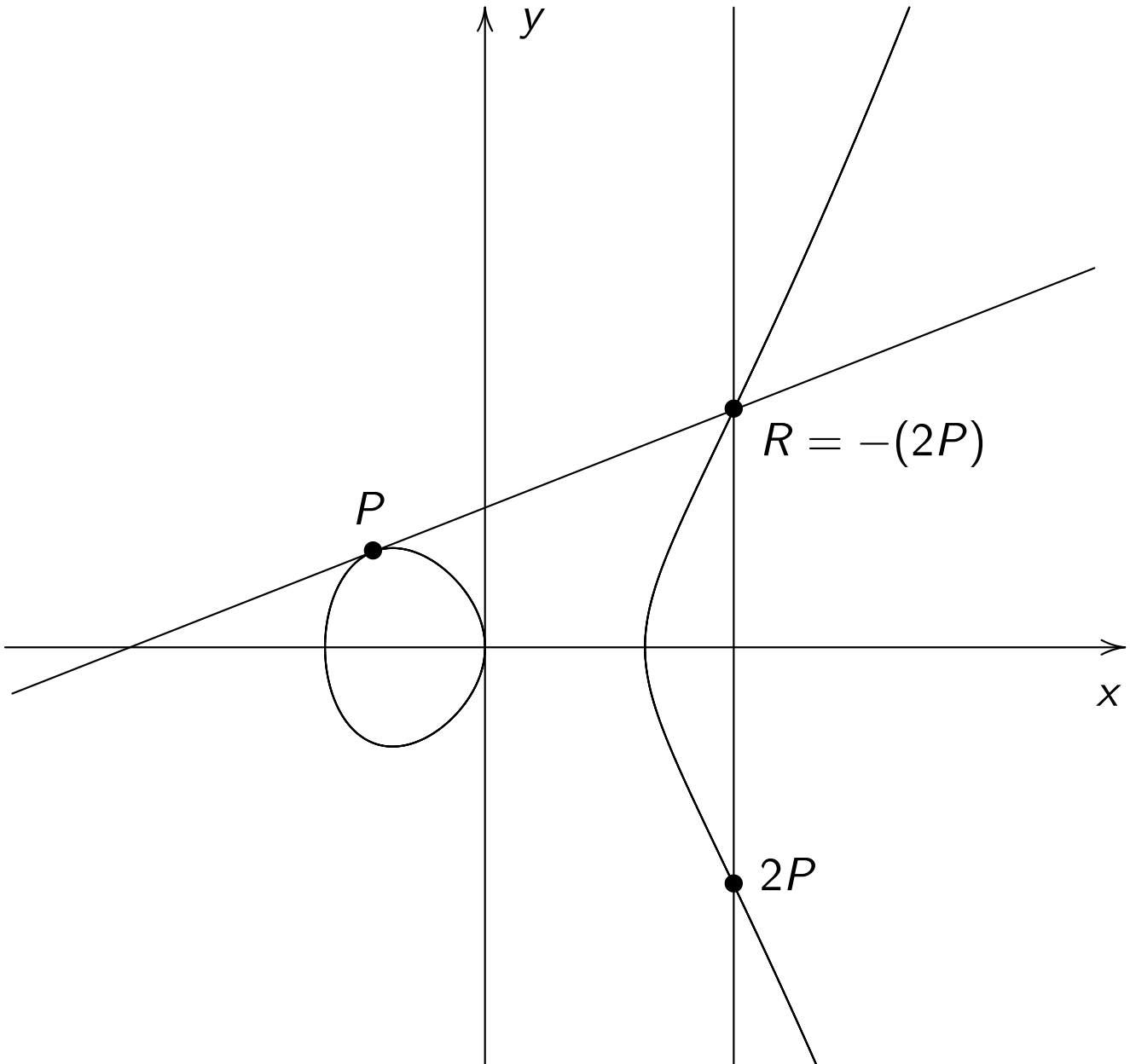
Tangents to the curve and points with multiplicity

Definition: If P, Q, R are on a line then $P + Q + R = \infty$.



Tangents to the curve and points with multiplicity

Definition: If P, Q, R are on a line then $P + Q + R = \infty$.



Optimization

When using cyrptosystems in practice, they need to be implemented and users want fast formulas.

For fields of large characteristic (typically prime fields) and rings modulo integers (like for RSA), inversions/divisions are a lot more expensive than multiplications. The EFD uses a ratio of I = 100 M for the ranking of different formulas (scroll a bit down to see the tables).

The relative cost of multiplication to squaring is less clear: If implementations use the same code for both, they take the same time. If there is separate code then ratios of S= 0.8M or S= 0.6M are reasonable.

If the designer can choose the constants (under the condition that the system is secure) they can typically achieve that the constants are much smaller – sometimes small enough to just do additions, essentially always at most one word (this matters as most moduli require multi-precision arithmetic).

Montgomery curves

Montgomery curves are a special form of elliptic curves which can be written in the form

$$Bv^2 = u^3 + Au^2 + u.$$

This almost matches the Weierstrass equation given above and the addition law is very similar.

If $u_1 \neq u_2$ then $\lambda = (v_1 - v_2)/(u_1 - u_2)$;
if $u_1 = u_2$ and $v_1 = v_2 \neq 0$ then $\lambda = (3u_1^2 + 2Au_1 + 1)/(2Bv_1)$.
In both cases

$$u_3 = B\lambda^2 - A - u_1 - u_2, v_3 = \lambda(u_1 - u_3) - v_1$$

As on Weierstrass curves:
$-(u_1, v_1) = (u_1, -v_1)$ and ∞ is the neutral element.

Montgomery curves always have a point $(0, 0)$ of order 2 and at least one of the following

- $u^2 + Au + 1 = (u - u_1)(u - u_2)$, giving $(u_1, 0), (u_2, 0)$ of order 2;
- there is a point of order 4.

Hence, the group order is always divisible by 4.

Every Montgomery curve can be transformed to a twisted Edwards curve and vice versa.

Birational equivalences

Two curves are *birationally equivalent* if there exust maps between the curves given by fractions of polynomials (rational maps) which map almost all points on one curve to the other and almost all points of the other to the frist and which are compatible with the group law, i.e.

$$\phi_1 : E_1 \to E_2, \phi_2 : E_2 \to E_1, \phi_i(P+Q) = \phi_i(P) + \phi_i(Q),$$

where ϕ_i are rational maps and for all $P, Q, P+Q$ on E_i where ϕ_i is defined.

Twisted Edwards cuve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to Montgomery curve $M_{A,B} : Bv^2 = u^3 + Au^2 + u$ for

$$A = 2(a+d)/(a-d), B = 4/(a-d) \Leftrightarrow a = (A+2)/B, d = (A-2)/B$$

mapping

$$u = (1+y)/(1-y), v = u/x \Leftrightarrow x = u/v, y = (u-1)/(u+1).$$

These have exceptions at

Birational equivalences

Two curves are *birationally equivalent* if there exust maps between the curves given by fractions of polynomials (rational maps) which map almost all points on one curve to the other and almost all points of the other to the frist and which are compatible with the group law, i.e.

$$\phi_1 : E_1 \to E_2, \phi_2 : E_2 \to E_1, \phi_i(P+Q) = \phi_i(P) + \phi_i(Q),$$

where ϕ_i are rational maps and for all $P, Q, P+Q$ on E_i where ϕ_i is defined.

Twisted Edwards cuve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to Montgomery curve $M_{A,B} : Bv^2 = u^3 + Au^2 + u$ for

$$A = 2(a+d)/(a-d), B = 4/(a-d) \Leftrightarrow a = (A+2)/B, d = (A-2)/B$$

mapping

$$u = (1+y)/(1-y), v = u/x \Leftrightarrow x = u/v, y = (u-1)/(u+1).$$

These have exceptions at $(0,0), (u_1,0), (u_2,0), (-1, \pm\sqrt{(A-2)/B}), \infty$ on $M_{A,B}$ and

Birational equivalences

Two curves are *birationally equivalent* if there exust maps between the curves given by fractions of polynomials (rational maps) which map almost all points on one curve to the other and almost all points of the other to the frist and which are compatible with the group law, i.e.

$$\phi_1 : E_1 \to E_2, \phi_2 : E_2 \to E_1, \phi_i(P+Q) = \phi_i(P) + \phi_i(Q),$$

where ϕ_i are rational maps and for all $P, Q, P+Q$ on E_i where ϕ_i is defined.

Twisted Edwards cuve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to Montgomery curve $M_{A,B} : Bv^2 = u^3 + Au^2 + u$ for

$$A = 2(a+d)/(a-d), B = 4/(a-d) \Leftrightarrow a = (A+2)/B, d = (A-2)/B$$

mapping

$$u = (1+y)/(1-y), v = u/x \Leftrightarrow x = u/v, y = (u-1)/(u+1).$$

These have exceptions at $(0,0), (u_1,0), (u_2,0), (-1, \pm\sqrt{(A-2)/B}), \infty$ on $M_{A,B}$ and $(0,1), (0,-1)$ and any points at infinity on $E_{a,d}$ if those points exist.