Isogeny-basd cryptography I

Basics of elliptic curves

Tanja Lange

Eindhoven University of Technology

SAC – Post-quantum cryptography

What is an elliptic curve?

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

What is an elliptic curve?

An elliptic curve is a smooth projective plane curve 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.

In algebraic geometry, smooth means that the curve does not have singularities.

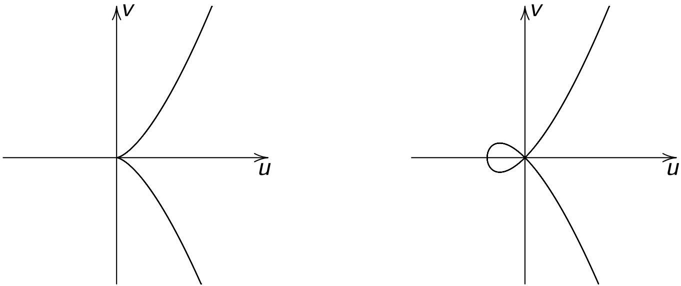
[The indices actually make sense if you give y weight 3, x weight 2 and ask that the weight + index equals 6.]

Singularities

Jacobi criterion:
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 $a_1y = 3x^2 + 2a_2x + a_4$.

A curve is non-singular (or smooth) if it does not have a singular point.

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.



Isomorphisms

An isomorphism is a map between elliptic curves that is defined everywhere, i.e., that is given by polynomials in x and y.

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.

Isomorphisms

An isomorphism is a map between elliptic curves that is defined everywhere, i.e., that is given by polynomials in x and y.

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.

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

Isomorphisms

An isomorphism is a map between elliptic curves that is defined everywhere, i.e., that is given by polynomials in x and y.

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.

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

Our first target is to get rid of the $a_1 xy + a_3 y$ term. If the characteristic is not 2 we can use $y \leftarrow y - (a_1 x + a_3)/2$ to reach the form $y^2 = x^3 + a_2' x^2 + a_4' x + a_6'$.

If the characteristic is not 3 we can similarly get rid of the $a_2' x^2$ term by using $x \leftarrow x - a_2'/3$.

The curve equation $y^2 = x^3 + c_4 x + c_6$ is called short Weierstrass form.

Short Weierstrass form $y^2 = x^3 + c_4x + c_6$

A singularity exists if and only if the right hand side has a double root, i.e. if its discriminant is zero:

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

Within this form the only isomorphisms possible are $y \leftarrow \alpha^3 y, x \leftarrow \alpha^2 x$, and divide both sides by α^6.

Short Weierstrass form $y^2 = x^3 + c_4x + c_6$

A singularity exists if and only if the right hand side has a double root, i.e. if its discriminant is zero:

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

Within this form the only isomorphisms possible are $y \leftarrow \alpha^3 y, x \leftarrow \alpha^2 x$, and divide both sides by α^6. This gives $c_4' = c_4/\alpha^4$ and $c_6' = c_6/\alpha^6$.

The j-invariant of a curve in short Weierstrass form is

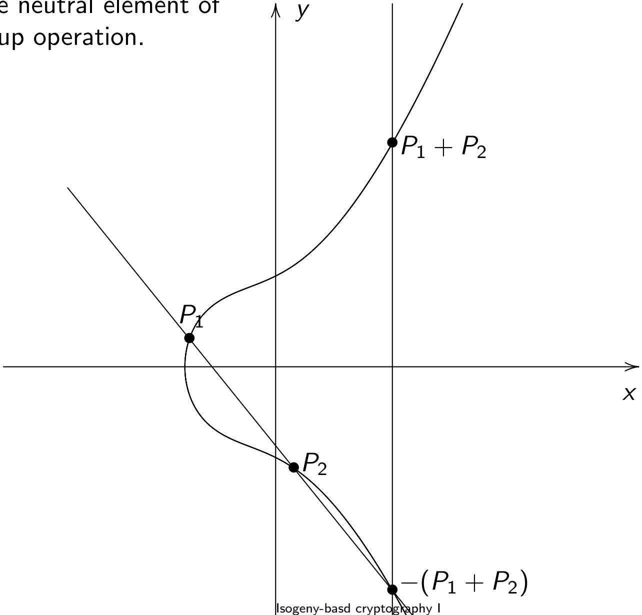
$$j = 1728 \cdot 4c_4^3/(4c_4^3 + 27c_6^2).$$

This is invariant under isomorphisms.

Addition law on the curve

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

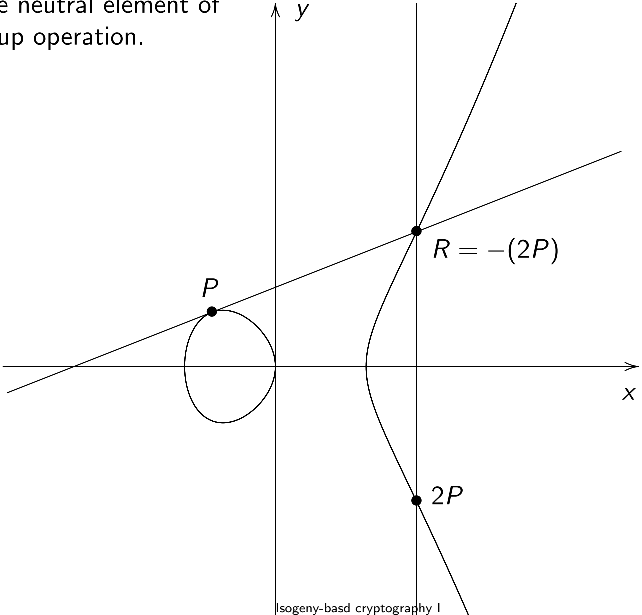
∞ is the neutral element of this group operation.



Tangents to the curve and points with multiplicity

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

∞ is the neutral element of this group operation.



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.

See the EFD for more curve shapes and efficient formulas.