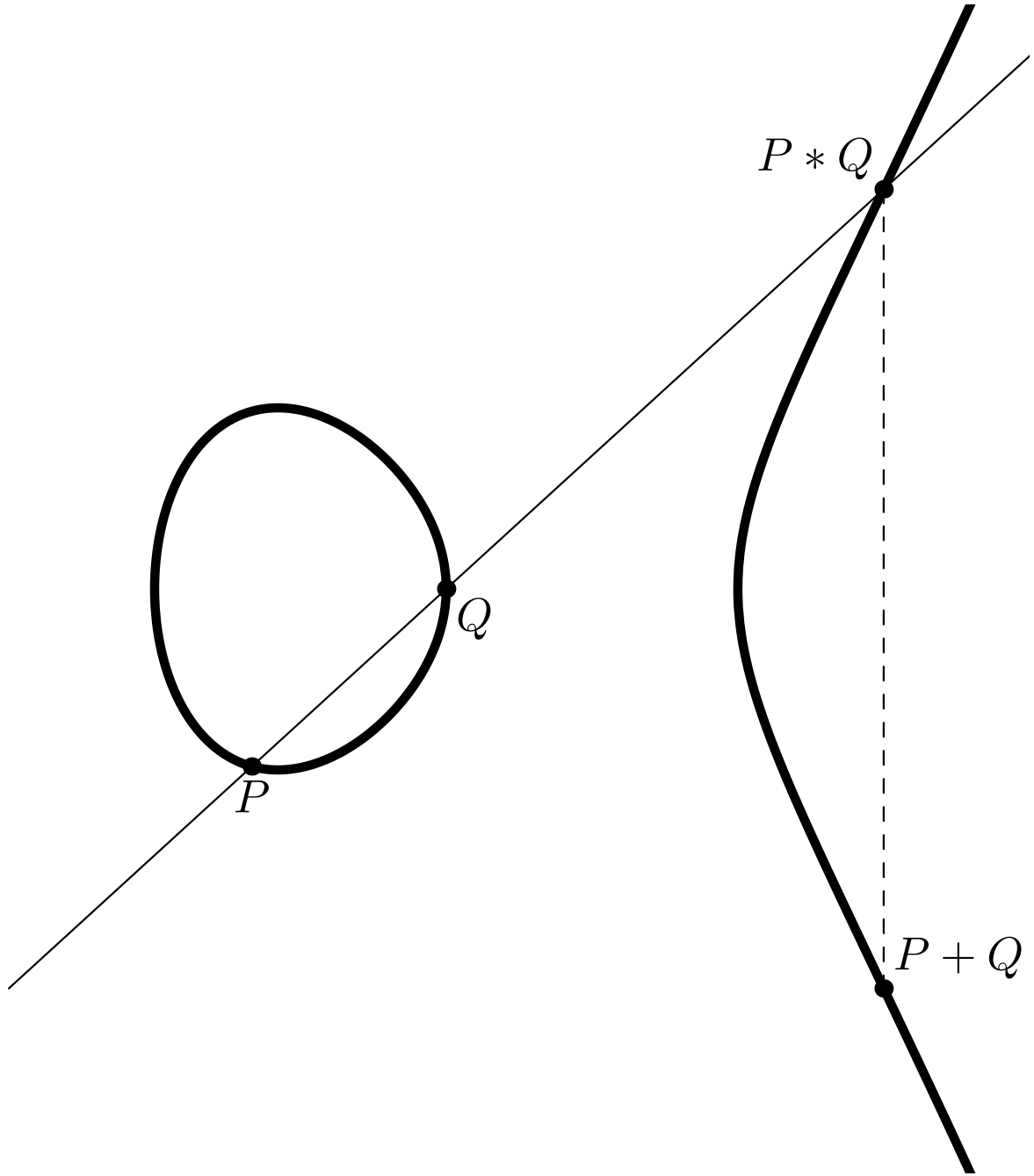
Rational points on elliptic curves

part II – Points of orders 2 and 3

Jakub Opršal

Spring school of the Department of algebra 2010

Outline


$P * Q$
Q
P
$P + Q$

A point P of an elliptic curve $C(\mathbb{F})$ is said to be of order n if

$$nP = P + P + \cdots + P = \mathcal{O}$$

and for any $k < n$ holds $kP \neq \mathcal{O}$. If such n exists P is said to have finite order.

Points of order 2

Assume we have non-singular elliptic curve $C(\mathbb{C})$ given by Weierstrass equation

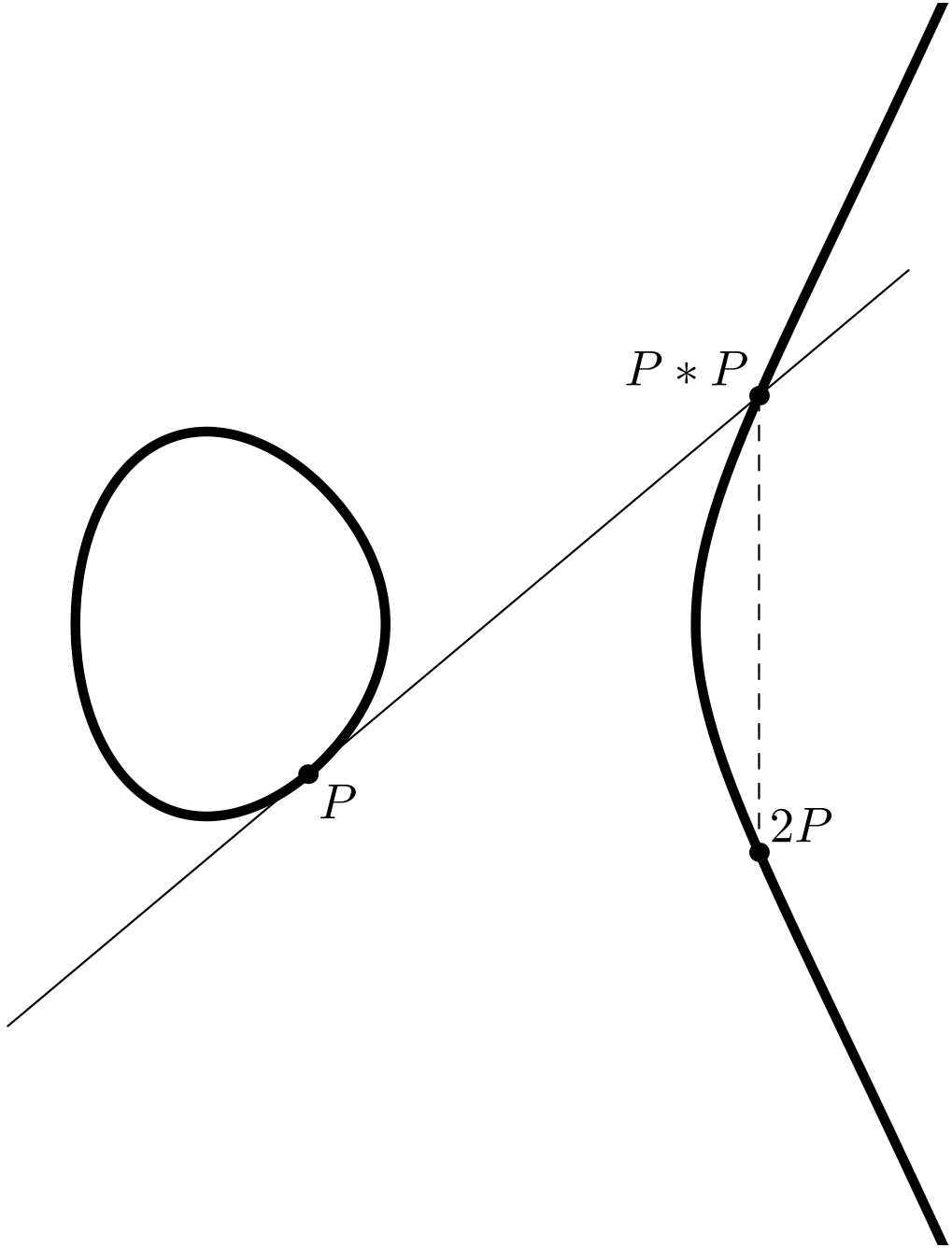
$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

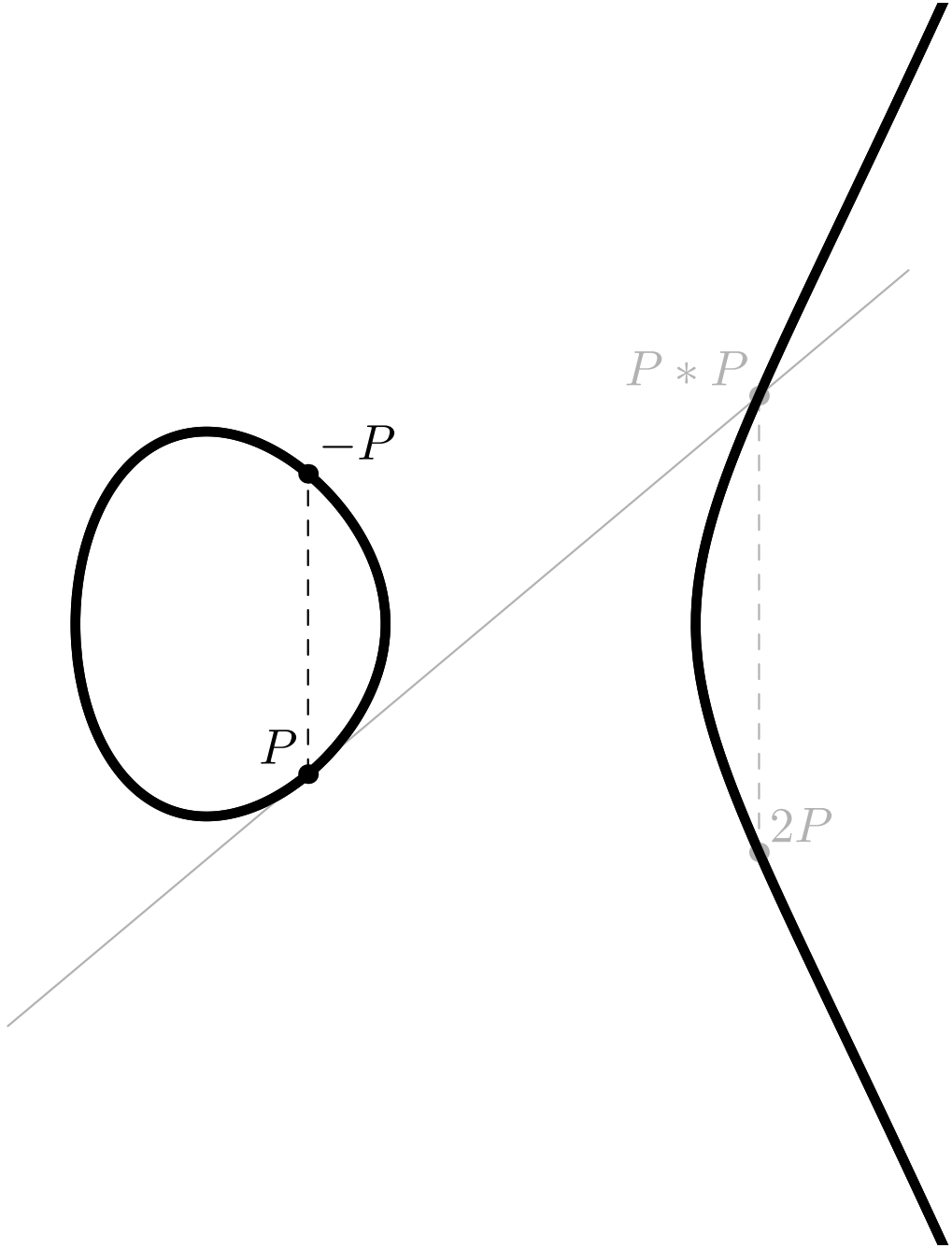
We'll find points of order two. I.e. such points P of the curve, that $2P = \mathcal{O}$ and $P \neq \mathcal{O}$.

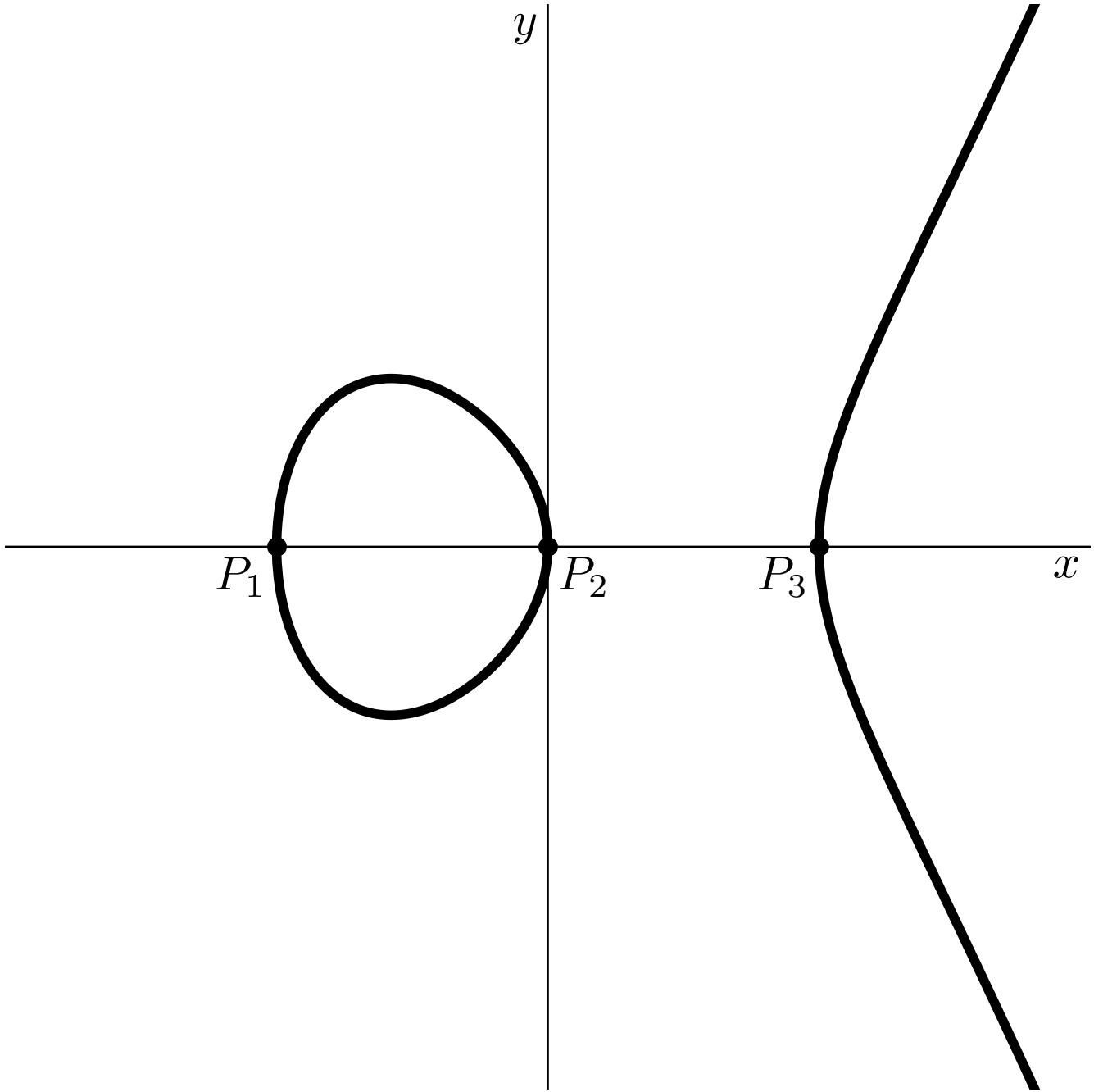
Holds

$$2P = \mathcal{O} \iff P = -P$$

We have a simple formula for $-P$. If $P = (x, y)$ then $-P = (x, -y)$.

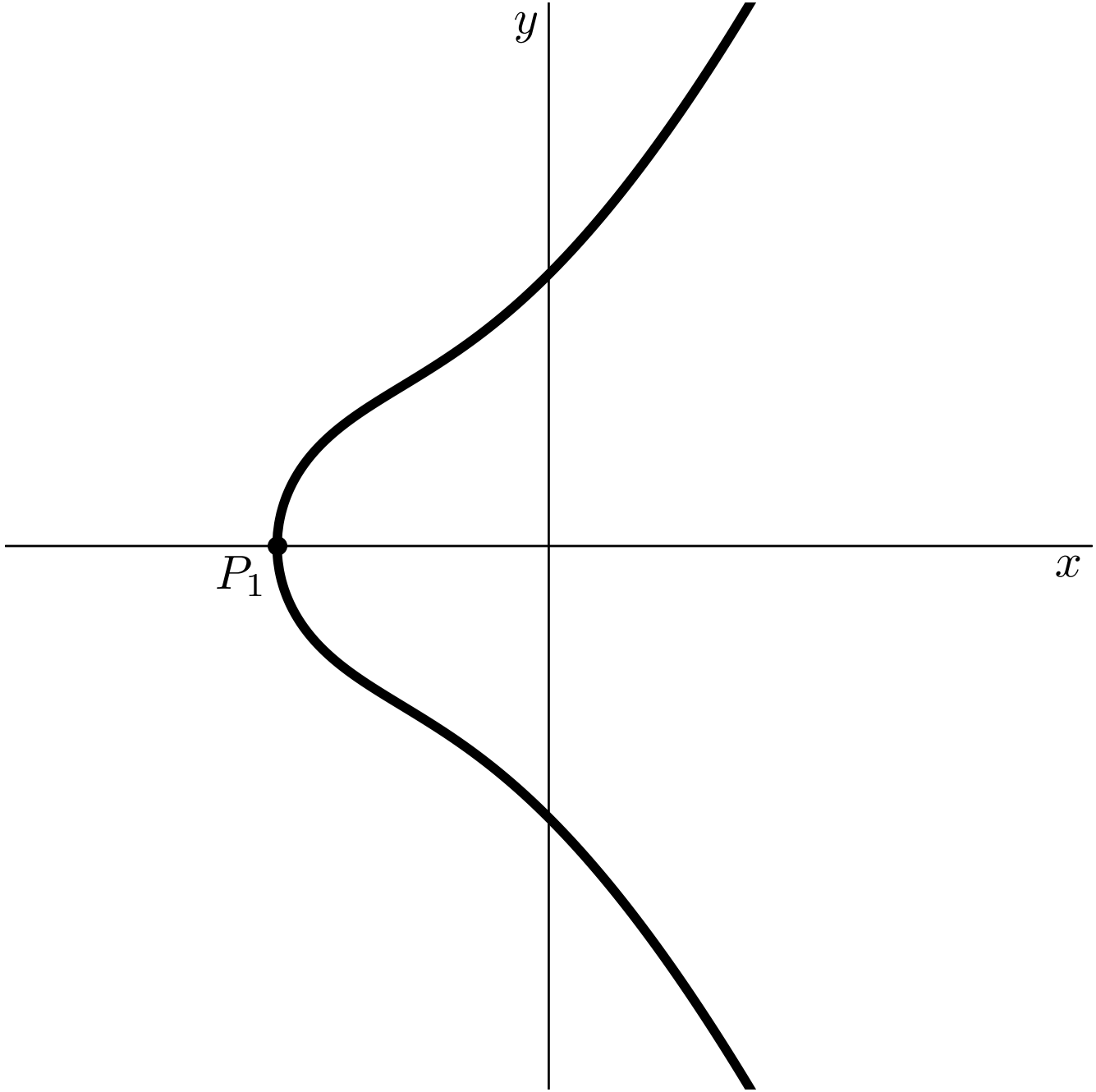

$P * P$
P
$2P$


$P * P$
$-P$
P
$2P$


y
x
P_1
P_2
P_3

Points of order 2

In any abelian group points, which satisy $2P = \mathcal{O}$, form a subgroup. In case of elliptic curves this subgroup is isomorphic to the Klein four group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.


y
x
P_1

Points of order 3

As in the case of order two, we'll find solutions to $2P = -P$ rather than $3P = \mathcal{O}$.

Recall the formula for the sum of two points $A = (x_1, y_1)$, $B = (x_2, y_2)$. We have $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

$$x(A + B) = \lambda^2 - a - x_1 - x_2$$
$$y(A + B) = \lambda x(A + B) + \nu$$

This formula for the $2P$ (if $P = (x, y)$) looks like

$$\lambda = \frac{f'(x)}{2y}$$
$$x(2P) = \lambda^2 - a - 2x$$

The point $P = (x, y)$ is of order three iff

$$x = x(2P) = \lambda^2 - a - 2x$$

As $f''(x) = 6x - 2a$, this condition is equivalent to

$$\psi_3(x) := 2f(x)f''(x) - f'(x)^2 = 0$$

The polynomial ψ_3 has four distinct roots.

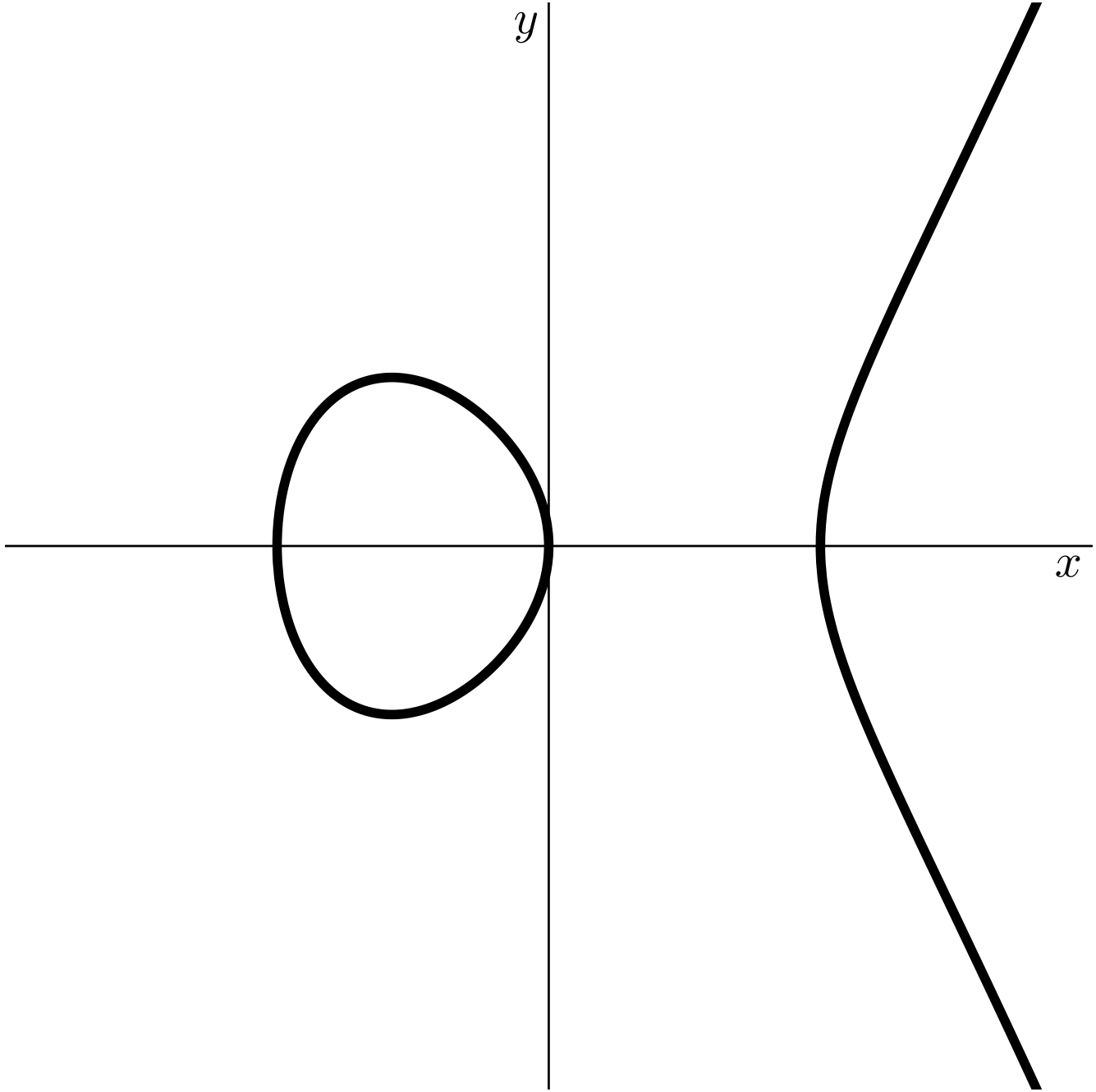
Points of order 3

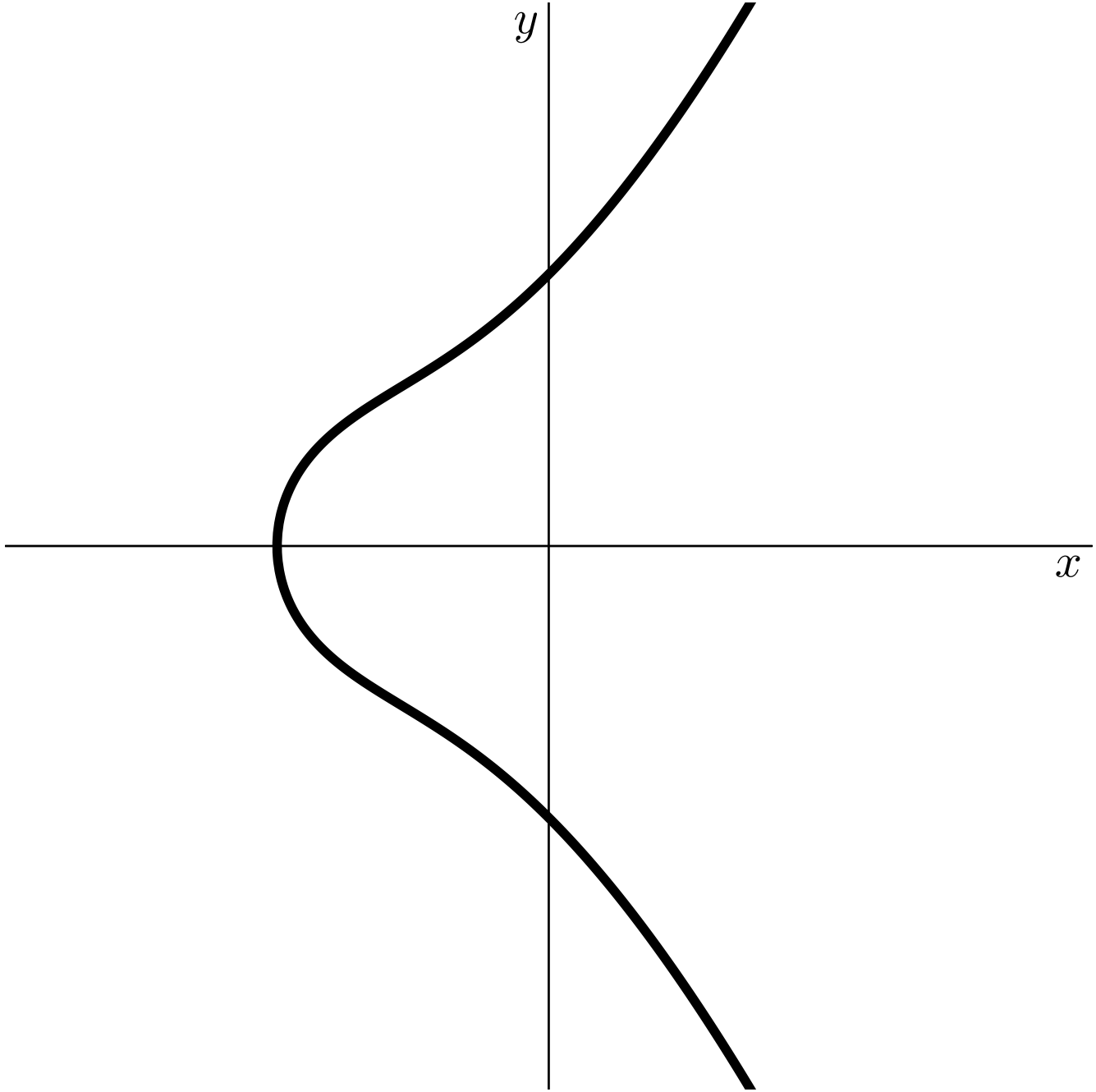
Theorem

A point P of an non-singular elliptic curve has order 3 if and only if x is the root of the polynomial

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$$

There are exactly eight such points and together with the point $\mathcal{O}$ they form a group isomorphic to $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.


y
x


y
x

Outline

Weierstrass $\wp$ function

A *lattice* L in the complex plane is a two-generated subgroup of additive group of complex numbers.

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

Weierstrass $\wp$ function is defined as

$$\wp(u) = \frac{1}{u^2} + \sum_{w \in L, w \neq 0} \left(\frac{1}{(u-w)^2} - \frac{1}{w^2} \right)$$

It is a meromorphic function with poles at lattice points of L. And it is L-periodic, that is $\wp(u + l) = \wp(u)$ for all $l \in L$.

Weierstrass $\wp$ function sattisfy the differential equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

Weierstrass $\wp$ function

A *lattice* L in the complex plane is a two-generated subgroup of additive group of complex numbers.

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

Weierstrass $\wp$ function is defined as

$$\wp(u) = \frac{1}{u^2} + \sum_{w \in L, w \neq 0} \left(\frac{1}{(u-w)^2} - \frac{1}{w^2} \right)$$

It is a meromorphic function with poles at lattice points of L. And it is L-periodic, that is $\wp(u + l) = \wp(u)$ for all $l \in L$.

Weierstrass $\wp$ function sattisfy the differential equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

Weierstrass $\wp$ function

A *lattice* L in the complex plane is a two-generated subgroup of additive group of complex numbers.

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

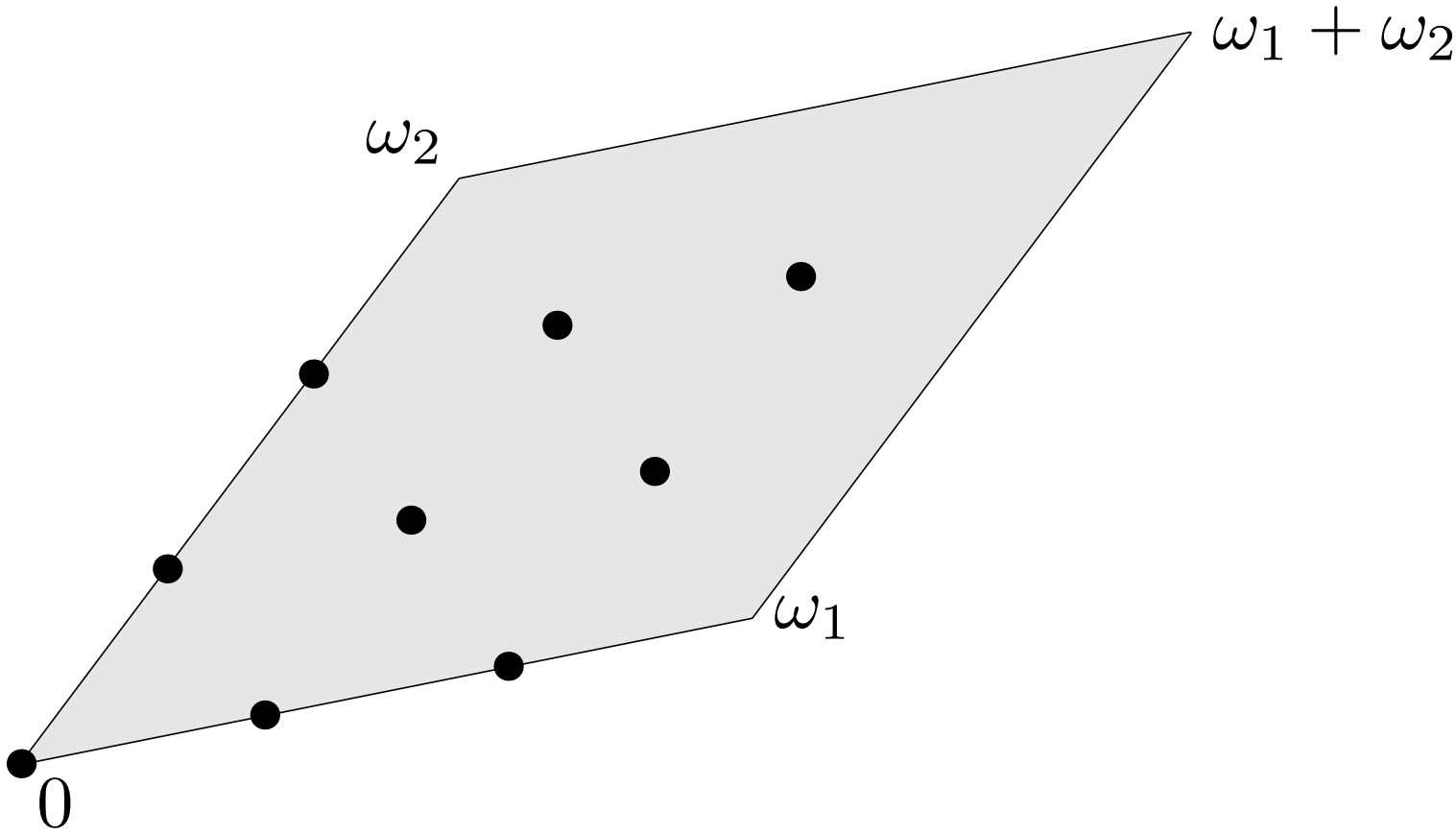
Weierstrass $\wp$ function is defined as

$$\wp(u) = \frac{1}{u^2} + \sum_{w \in L, w \neq 0} \left(\frac{1}{(u-w)^2} - \frac{1}{w^2} \right)$$

It is a meromorphic function with poles at lattice points of L. And it is L-periodic, that is $\wp(u + l) = \wp(u)$ for all $l \in L$.

Weierstrass $\wp$ function sattisfy the differential equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$


$\omega_1 + \omega_2$
ω_2
ω_1
0

Outline

Integer coeficients

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

By subtitution $X = d^2x$ and $Y = d^3y$ we get our equation to in the form

$$Y^2 = X^3 + d^2aX^2 + d^4bX + d^6c$$

and hence we can chose large integer d, such that this equation would have integer coeficients.

From now assume that the elliptic curve is given by an equation with integer coeficients.

The discriminant

The discriminant is the quantity

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

For $a = 0$, $D = -4b^3 - 27c^2$.

If we factor $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, the discriminant becomes of the form

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

The discriminant of a polynomial f with leading coeficient 1 is allways in the ideal of $\mathbb{Z}[x]$ generated by f and f'. Hence there are $r, s \in \mathbb{Z}[x]$, such that

$$D = r(x)f(x) + s(x)f'(x)$$

Lemma

Let $P = (x, y)$ be a point on elliptic curve such that both P and $2P$ have integer coordinates. Then either $y = 0$ or $y \mid D$