Elliptic Curve Cryptography (ECC)

Michael Reyer: reyer@ti.rwth-aachen.de

Institute for Theoretical Information Technology
Prof. Dr. Rudolf Mathar

RWTH AACHEN

The Discrete Logarithm

Comparison between Classical Case und Elliptic Curves

Classical case	Elliptic curves
multiplicative group	additive group
$(Z_n^*, \cdot)$	$(E(K), +)$
a prim. element (PE)	G generator
$\mathbb{Z}_n^* = \{a^k \mid k = 1, \ldots, \varphi(n)\}$	$E(K) = \{k\,G \mid k = 1, \ldots, \lvert E(K)\rvert\}$
for $y \in \mathbb{Z}_n^*\ \exists k \in \{1, \ldots, \varphi(n)\}$	für $P \in E(K)\ \exists k \in \{1, \ldots, \lvert E(K)\rvert\}$
$y = a^k \mod n$	$P = k\,G$
$k = \log_a y$	$k = \log_G P$
k is DL of y to basis a	k is DL of P to basis G
a^k with Square-and-Multiply	$k\,G$ with Double-and-Add
Infeasible: Calculation of k	Infeasible: Calculation of k

Elliptic Curves over the Reals

Elliptic curves over the reals

- Simple graphical representation
  - of the curve as well as
  - addition (and doubling) of points.

Elliptic Curves over the Reals

Elliptic curves over the reals

- Simple graphical representation
  - of the curve as well as
  - addition (and doubling) of points.

$$f(x,y) = y^2 - (x^3 + ax + b) = g(y) - h(x) = 0,\ a,b,x,y \in \mathbb{R}$$

Elliptic Curves over the Reals

Elliptic curves over the reals

- Simple graphical representation
  - of the curve as well as
  - addition (and doubling) of points.

$$f(x,y) = y^2 - (x^3 + ax + b) = g(y) - h(x) = 0,\ a, b, x, y \in \mathbb{R}$$

- Preliminaries
  - The curve is symmetric to x-axis
  - Interesting: Nulls of cubic curve $h(x)$

Elliptic Curves over the Reals

Elliptic curves over the reals

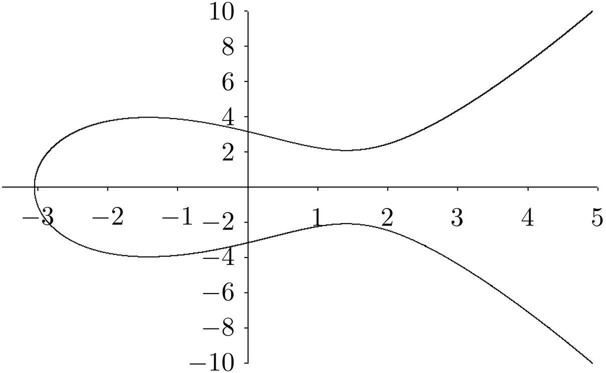
- Simple graphical representation
  - of the curve as well as
  - addition (and doubling) of points.

$$f(x,y) = y^2 - (x^3 + ax + b) = g(y) - h(x) = 0,\ a,b,x,y \in \mathbb{R}$$

- Preliminaries
  - The curve is symmetric to x-axis
  - Interesting: Nulls of cubic curve $h(x)$
  - Known: if for the discriminant $\Delta = 4a^3 + 27b^2$ of h holds:
    - $\Delta > 0$: h has one null in the reals
    - $\Delta < 0$: h has three nulls in the reals
    - $\Delta = 0$: it ex. double or triple null in the reals

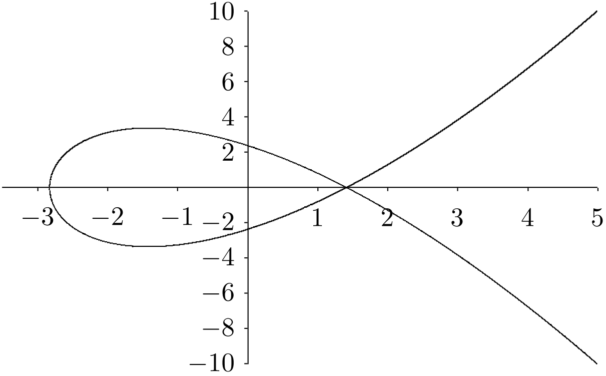
Elliptic Curves over the Reals

Graphical Representation



$$y^2 = x^3 - 6x + 10,\ \Delta = 4 \cdot (-6)^3 + 27 \cdot 10^2 = 1836$$

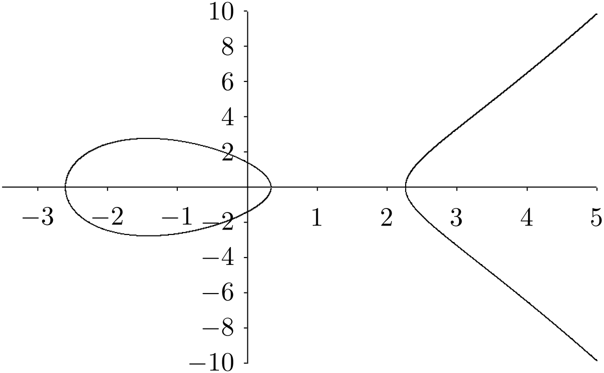
Elliptic Curves over the Reals
Graphical Representation



$$y^2 = x^3 - 6x + 4\sqrt{2},\ \Delta = 0$$

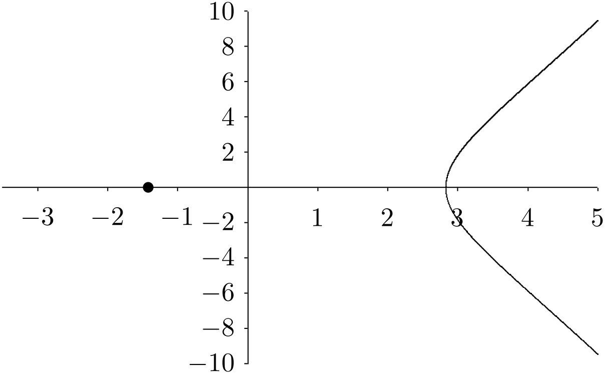
Elliptic Curves over the Reals

Graphical Representation

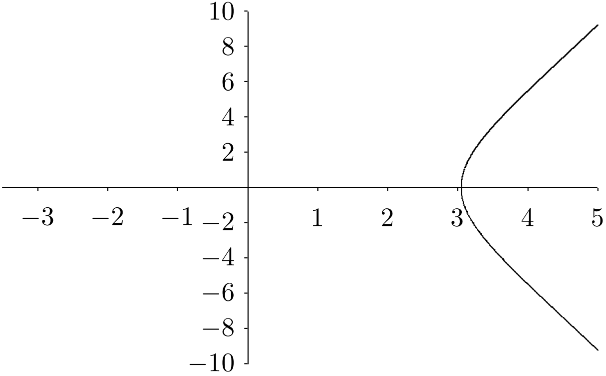


$$y^2 = x^3 - 6x + 2,\ \Delta = -756$$

Elliptic Curves over the Reals
Graphical Representation



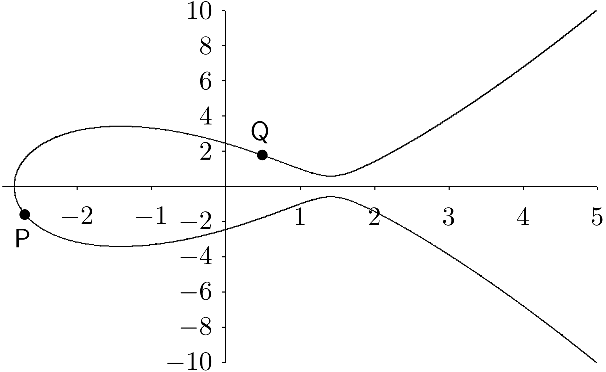
$$y^2 = x^3 - 6x - 4\sqrt{2},\ \Delta = 0$$



$$y^2 = x^3 - 6x - 10,\ \Delta = 1836$$

Elliptic Curves over the Reals

Graphical Representation of Addition

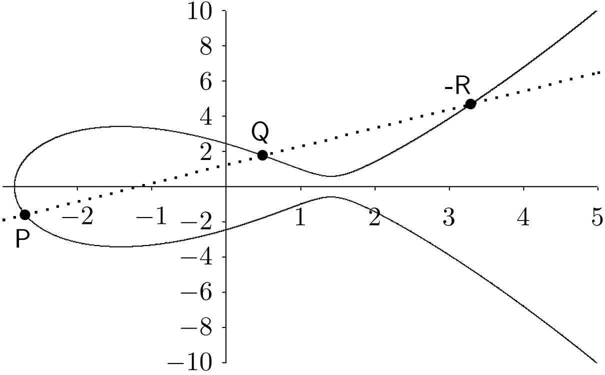


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Representation of Addition

- Define a line through P and Q.
- The third intersecting point on the curve is $-R$.

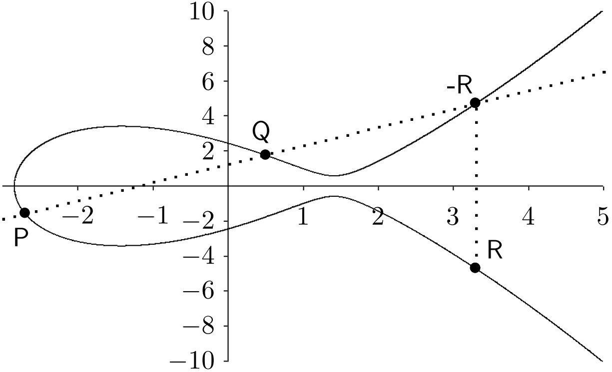


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Representation of Addition

- Define a line through P and Q.
- The third intersecting point on the curve is $-R$.
- Mirror $-R$ at x-axis to obtain $R = P + Q$.

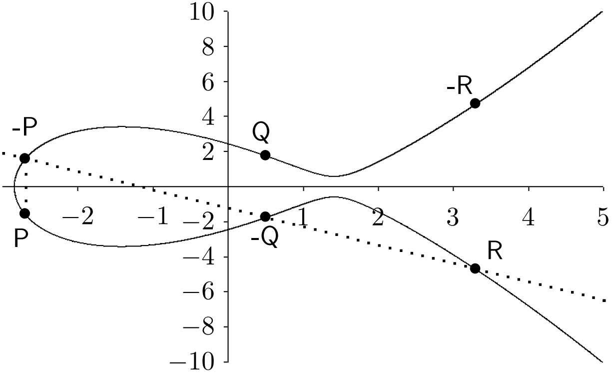


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Representation of Addition

- Define a line through P and Q.
- The third intersecting point on the curve is $-R$.
- Mirror $-R$ at x-axis to obtain $R = P + Q$, $R + (-Q) = P$.

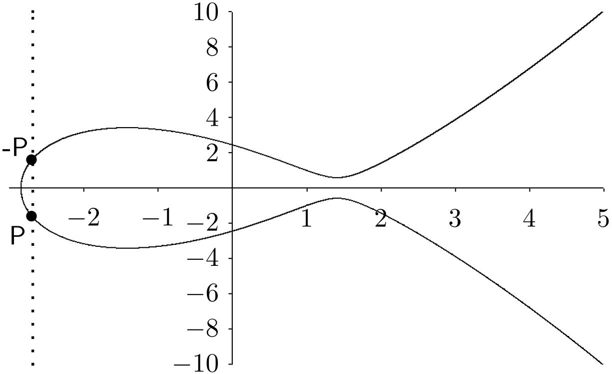


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Representation of Addition

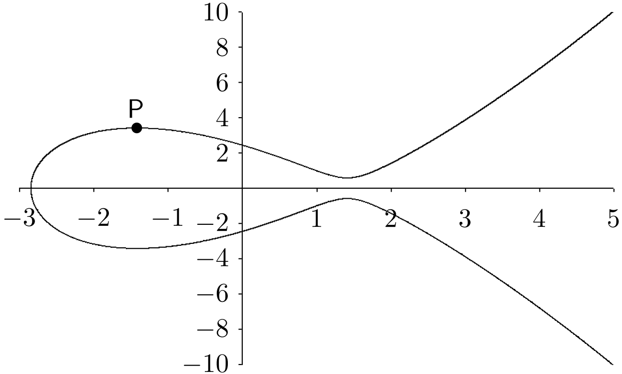
- Special case $P + (-P) = \mathcal{O}$
- $\mathcal{O}$ is neutral element w.r.t. addition.



$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Doubling of Point $P + P$

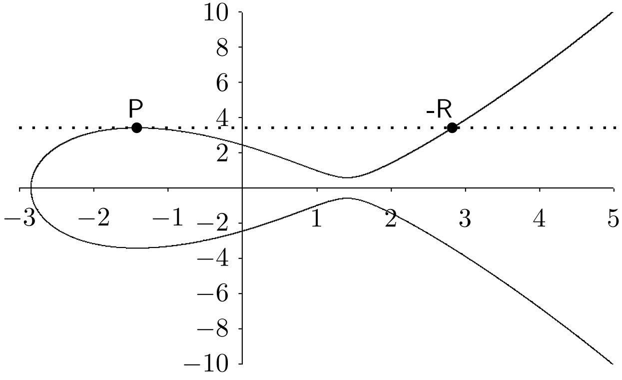


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Doubling of Point $P + P$

- Draw tangent at P.
- The second intersecting point of the tangent line defines $-R$.

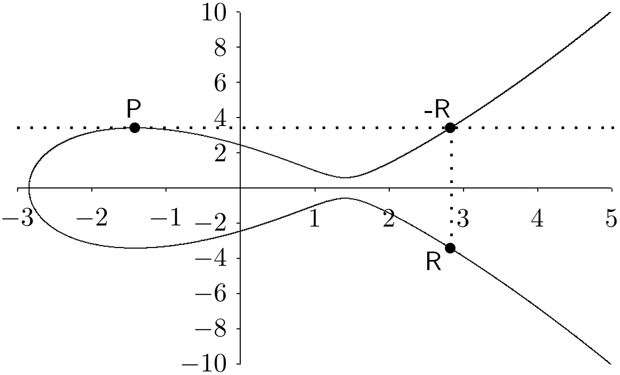


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Doubling of Point $P + P$

- Draw tangent at P.
- The second intersecting point of the tangent line defines $-R$.
- Mirroring $-R$ at x-axis defines $R = 2P$,

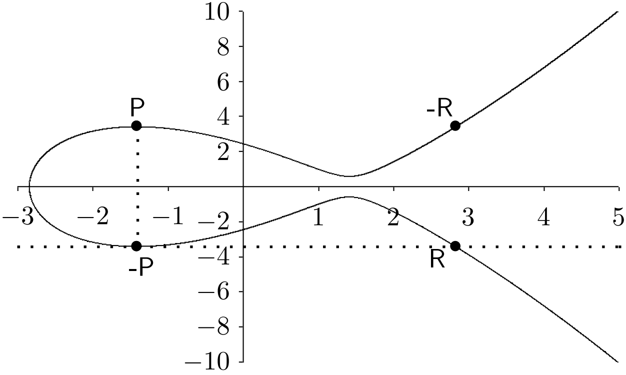


$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over the Reals

Graphical Doubling of Point $P + P$

- Draw tangent at P.
- The second intersecting point of the tangent line defines $-R$.
- Mirroring $-R$ at x-axis defines $R = 2P$, $R + (-P) = P$.



$$y^2 = x^3 - 6x + 6$$

Elliptic Curves over Finite Fields

In cryptography elliptic curves over finite fields are used.

- No floating points
- No rounding error, important for error-free decryption

Elliptic Curves over Finite Fields

In cryptography elliptic curves over finite fields are used.

- No floating points
- No rounding error, important for error-free decryption

Elliptic curves over $\mathbb{F}_p$

$y^2 \equiv x^3 + ax + b \pmod{p}$ mit $a, b, x, y \in \{0, 1, \ldots, p-1\} = \mathbb{Z}_p$

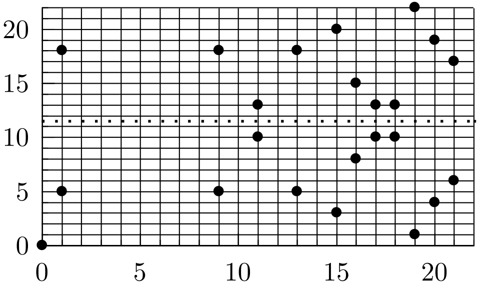
Elliptic Curves over Finite Fields

In cryptography elliptic curves over finite fields are used.

- No floating points
- No rounding error, important for error-free decryption

Elliptic curves over $\mathbb{F}_p$

$y^2 \equiv x^3 + ax + b \pmod{p}$ mit $a, b, x, y \in \{0, 1, \dots, p-1\} = \mathbb{Z}_p$



$y^2 = x^3 + x$ in $\mathbb{F}_{23}$

Algebraic Formulas as in the reals, but reduced modulo p