Zürcher Hochschule Winterthur

The Elliptic Curve Cryptosystem

Dr. Andreas Steffen

What are Elliptic Curves?

Zürcher Hochschule Winterthur

General form:

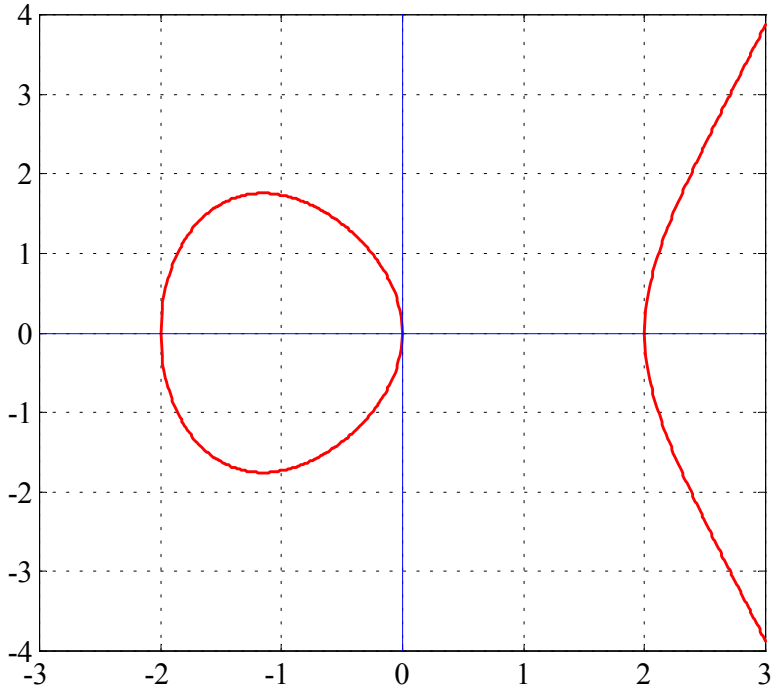
$$y^2 = x^3 + ax + b$$

Condition for distinct single roots:

$$4a^3 + 27b^2 \neq 0$$

Example:

$$y^2 = x^3 - 4x$$
$$= x(x-2)(x+2)$$



What is an Algebraic Group <G,∗> ?

A group is an algebraic system consisting of a set G and an operation ∗ such that for all elements a, b and c in G the following conditions must be fulfilled:

- Closure: $a * b$ must remain in G
- Associativity: $a * (b * c) = (a * b) * c$
- Neutral Element: $a * e = e * a = a$
- Inverse Element: $a * a' = a' * a = e$
- Commutativity: $a * b = b * a$ (Abelian Group)

Examples:

- Addition: $\langle R, + \rangle$ $e = 0$, $a' = -a$
- Multiplication: $\langle R-\{0\}, \cdot \rangle$ $e = 1$, $a' = a^{-1}$

Points P(x,y) on an Elliptic Curve form a Group

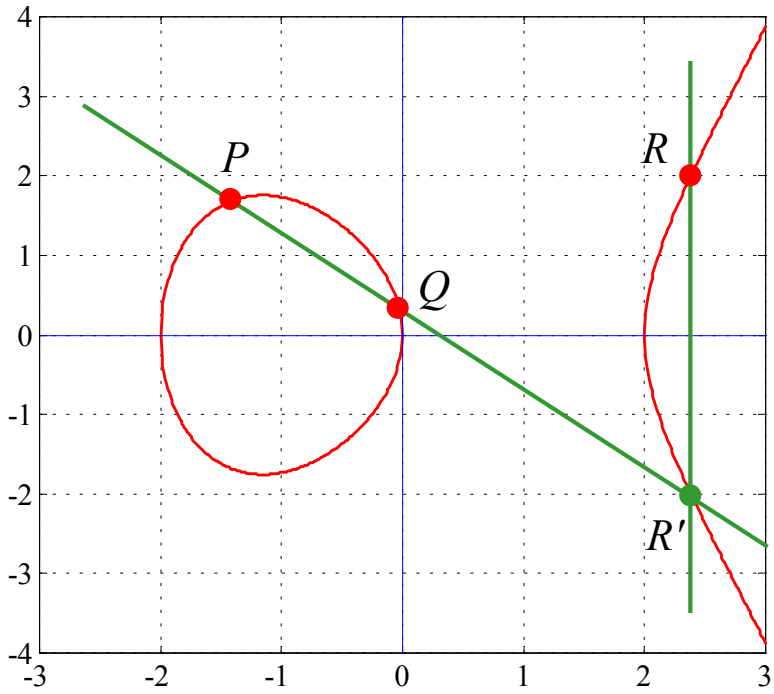
Group set:

All points P(x,y) lying on an elliptic curve

Group operation:

Point addition

$$R = P * Q$$



Neutral and Inverse Elements

Inverse element:

P'(x,-y) = P(x,y)

is mirrored on x-axis

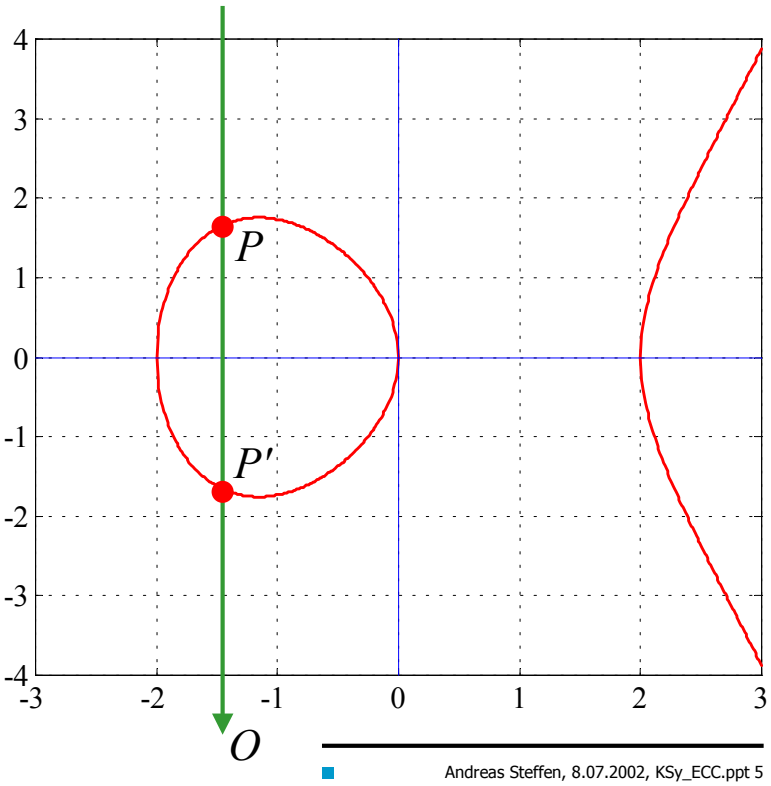
Point addition with inverse element:

P ∗ P' = O

results in a neutral element O(x,∞) at infinity

Neutral element:

P ∗ O = P

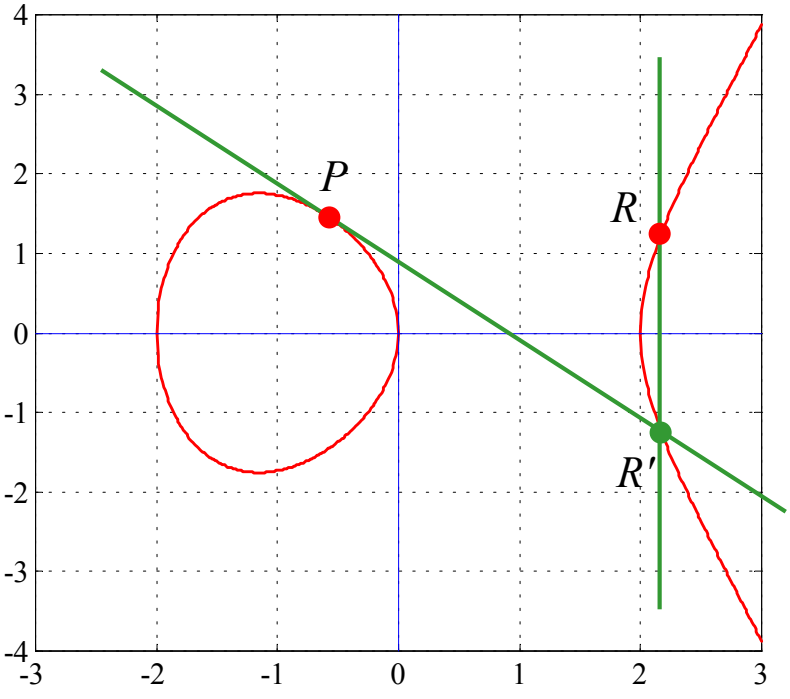


Point Doubling – Adding a point to itself

Point Doubling:

Form the tangent in Point P(x,y)

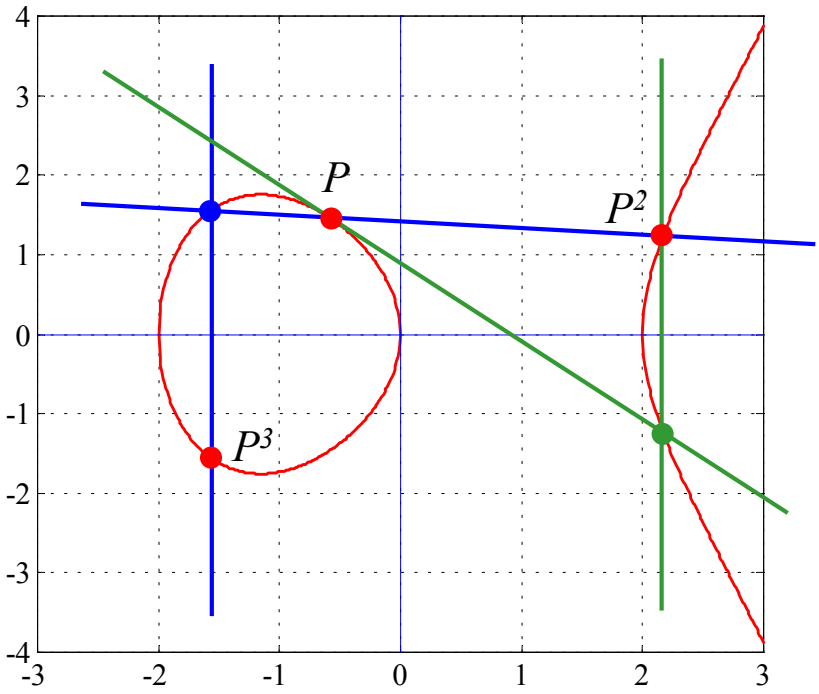
$$R = P * P$$



Point Iteration – Adding a point k-1 times to itself

Point Iteration:

$$P^k = P * P * \ldots * P$$



Mathematical Description of Geometrical Transform

Line g: $y = s \cdot x - y_0$

with $$s = \frac{y_Q - y_P}{x_Q - x_P}$$

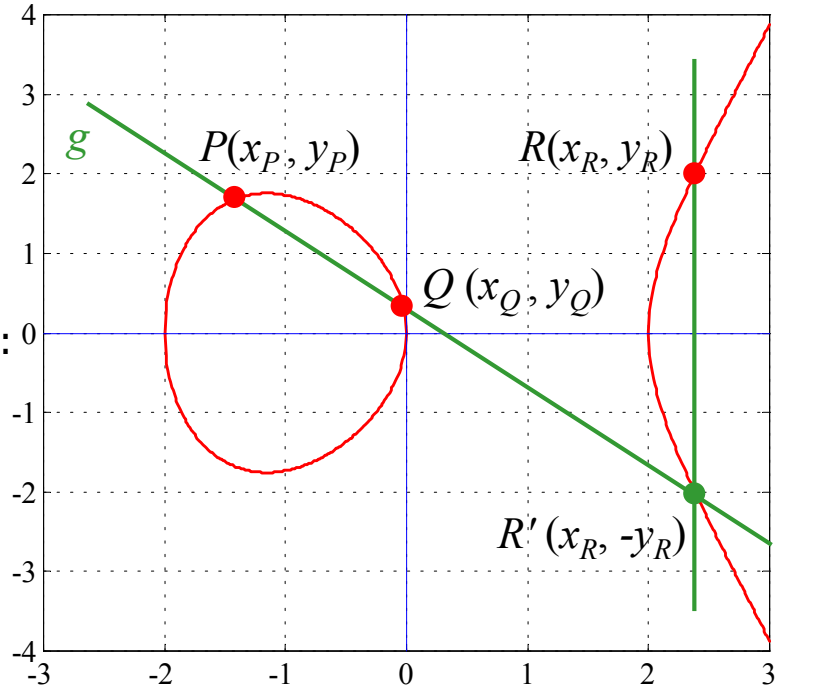
$$y_0 = y_P - s \cdot x_P$$

Intersection with curve:

$$(s \cdot x - y_0)^2 = x^3 + ax + b$$

Coordinates of point R:

$$x_R = s^2 - x_P - x_Q$$
$$y_R = -(s \cdot x_R + y_0)$$



Mathematical Description of Geometrical Transform

Tangent g: $y = s \cdot x - y_0$

$$s = \frac{dy}{dx} = \frac{3x_P^2 + a}{2y_P}$$

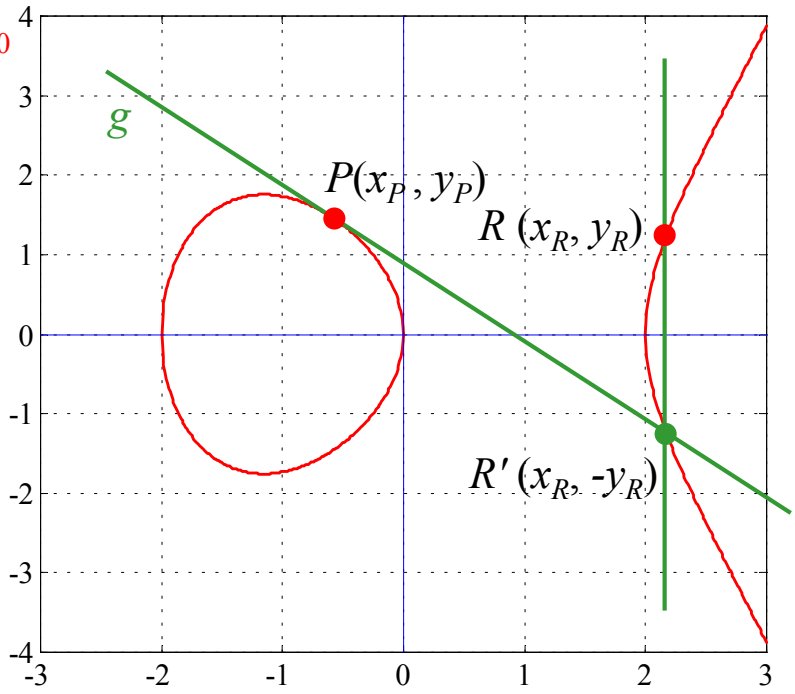
$$y_0 = y_P - s \cdot x_P$$

Intersection with curve

$(s \cdot x - y_0)^2 = x^3 + ax + b$

Coordinates of point R:

$$x_R = s^2 - 2x_P$$
$$y_R = -(s \cdot x_R + y_0)$$



How can Geometry be useful for Cryptography?

Elliptic curves can be defined in a finite or Galois field GF_p:

$$y^2 = x^3 + ax + b \mod p$$

where the field size p is a prime number and

{0,1, ..., p-1} is an abelian group under addition mod p

and

{1, ..., p-1} is an abelian group under multiplication mod p.

Task 1 - Multiplication c = a·b in GF_{11}

- Compile a multiplication table for $c = a \cdot b \mod 11$
- Determine the solutions of the equation $x^2 = 5 \mod 11$
- You have about 10 minutes for this task

Solution 1 - Multiplication c = a·b in GF_{11}

·	0	1	2	3	**4**	5	6	**7**	8	9	10	*a*
0	0	0	0	0	0	0	0	0	0	0	0	
1	0	1	2	3	4	5	6	7	8	9	10	
2	0	2	4	6	8	10	1	3	5	7	9	
3	0	3	6	9	1	4	7	10	2	5	8	
4	0	4	8	1	5	9	2	6	10	4	7	
5	0	5	10	4	9	3	8	2	7	1	6	
6	0	6	1	7	2	8	3	9	4	10	5	
7	0	7	3	10	6	2	9	5	1	8	4	
8	0	8	5	2	10	7	4	1	9	6	3	
9	0	9	7	5	3	1	10	8	6	4	2	
10	0	10	9	8	7	6	5	4	3	2	1	*c*

b

$x^2 = 5 \mod 11$?

$x_1 = 4, x_2 = 7$

Task 2 – Points on an Elliptic Curve

- Which points P(x,y) with x and y in GF_{11} fulfill the elliptic curve equation:

  $y^2 = x^3 + x + 6 \mod 11$

- You have about 10 minutes for this task

Solution 2 – Points on an Elliptic Curve

x	y^2	$y_{1,2}$	P(x,y)	P'(x,y)
0	6	-		
1	8	-		
2	5	4,7	(2,4)	(2,7)
3	3	5,6	(3,5)	(3,6)
4	8	-		
5	4	2,9	(5,2)	(5,9)
6	8	-		
7	4	2,9	(7,2)	(7,9)
8	9	3,8	(8,3)	(8,8)
9	7	-		
10	4	2,9	(10,2)	(10,9)

There are 12 points lying on the elliptic curve.

Together with the point O at infinity, the points on the elliptic curve form a group with n=13 elements.

n is called the order of the elliptic curve group and depends on the choice of the curve parameters a and b.

Task 3 – Iterate a Point on the Elliptic Curve

- Iterate the point P(2,4) lying on $y^2 = x^3 + x + 6 \mod 11$:
- Compute $P^2 = P * P$ by doubling the point P

$$s = \frac{dy}{dx} = \frac{3x_P^2 + a}{2y_P} \qquad y_0 = y_P - s \cdot x_P \qquad \begin{aligned} x_R &= s^2 - 2x_P \\ y_R &= -(s \cdot x_R + y_0) \end{aligned}$$

- Compute $P^3 = P * P * P = P^2 * P$ by point addition

$$s = \frac{y_Q - y_P}{x_Q - x_P} \qquad y_0 = y_P - s \cdot x_P \qquad \begin{aligned} x_R &= s^2 - x_P - x_Q \\ y_R &= -(s \cdot x_R + y_0) \end{aligned}$$

- All operations are computed in GF_{11}

Solution 3 – Iterate a Point on the Elliptic Curve

- Compute $P^2 = P * P$ by doubling the point P(2,4)

$$s = \frac{3 \cdot 4 + 1}{2 \cdot 4} = \frac{13}{8} = 7 \cdot 2 = 3$$

$$y_0 = 4 - 3 \cdot 2 = -2 = 9$$

$$\begin{aligned} x_R &= 9 - 2 \cdot 2 = 5 \\ y_R &= -(3 \cdot 5 + 9) = -2 = 9 \end{aligned}$$

$P^2=(5,9)$

- Compute $P^3 = P * P * P = P^2 * P$ by point addition

$$s = \frac{9 - 4}{5 - 2} = \frac{5}{3} = 4 \cdot 5 = 9$$

$$y_0 = 4 - 9 \cdot 2 = -3 = 8$$

$$\begin{aligned} x_R &= 81 - 2 - 5 = 8 \\ y_R &= -(9 \cdot 8 + 8) = -3 = 8 \end{aligned}$$

$P^3=(8,8)$

Elliptic Curve Discrete Logarithm Problem (ECDLP)

k	P^k	s	y_0
1	(2,4)	3	9
2	(5,9)	9	8
3	(8,8)	8	10
4	(10,9)	2	0
5	(3,5)	1	2
6	(7,2)	4	7
7	(7,9)	1	2
8	(3,6)	2	0
9	(10,2)	8	10
10	(8,3)	9	8
11	(5,2)	3	9
12	(2,7)	∞	-
13	0	∞	-

Given an elliptic curve

$y^2 = x^3 + ax + b \mod p$

and a basis point P, we can compute

$Q = P^k$

through k-1 iterative point additions. Fast algorithms for this task exist. Unfortunately most of them are patented by Certicom and others.

Question: Is it possible to compute k when the point Q is known?

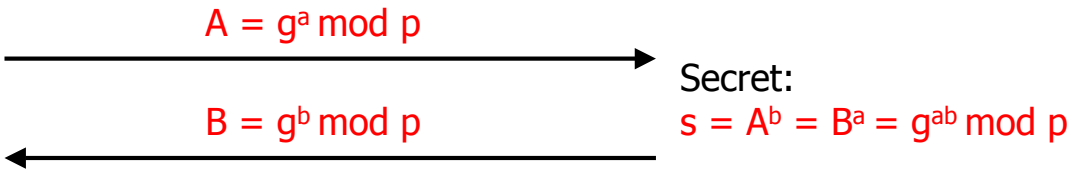
Answer: This is a hard problem known as the Elliptic Curve Discrete Logarithm.

Definition of an Elliptic Curve Cryptosystem

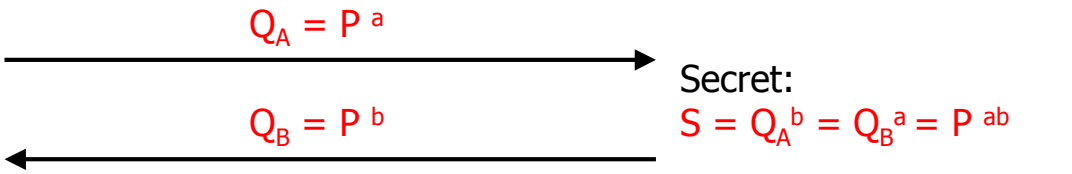
- version — is currently v1
- fieldID — identifies the finite field over which curve is defined
- curve — coefficients a and b of the elliptic curve
- base — specifies the base point P
- order — the order n of the base point

Cryptographic Application – Secret Key Exchange

- Diffie-Hellman: Basis g and prime p



- Elliptic Curve Cryptosystem: ECC, basis point P and prime p



Equivalent Cryptographic Strength

Symmetric	56	80	112	128	192	256
RSA n	512	1024	2048	3072	7680	15360
ECC p	112	161	224	256	384	512
Key size ratio	5:1	6:1	9:1	12:1	20:1	30:1