

# Kryptographie mit elliptischen Kurven

Dr. Dirk Feldhusen

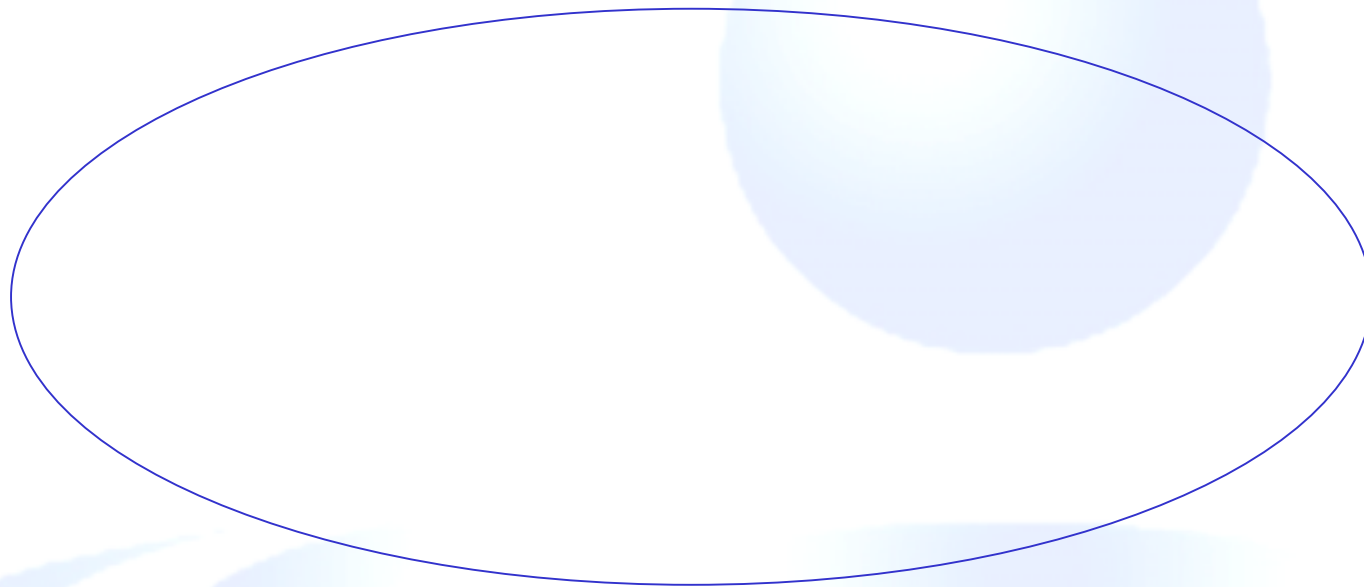
SRC Security Research & Consulting GmbH

Bonn - Wiesbaden

- Elliptische Kurven
  - ▶ Grafik
  - ▶ Punktaddition
  - ▶ Implementation
- Kryptographie
  - ▶ Asymmetrische Verfahren (Public Key)
  - ▶ Überblick über herkömmliche Verfahren
  - ▶ Verfahren mit elliptischen Kurven
- Vergleich

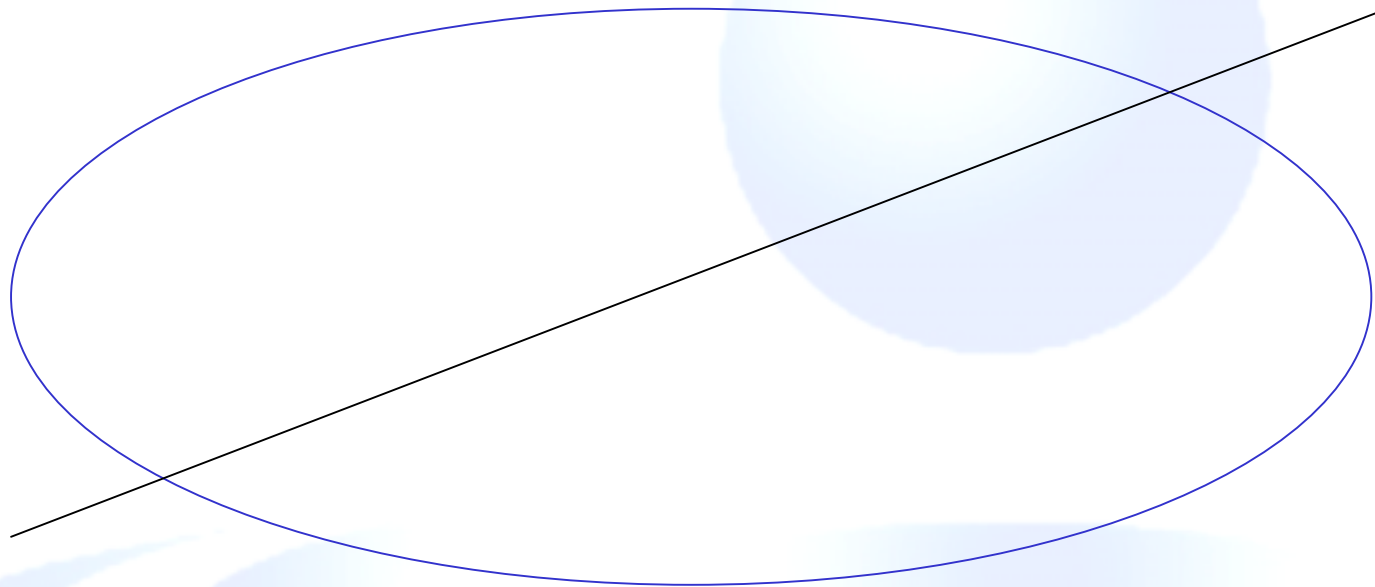
# Elliptische Kurven

Was ist eine elliptische Kurve?



Eine Ellipse ?

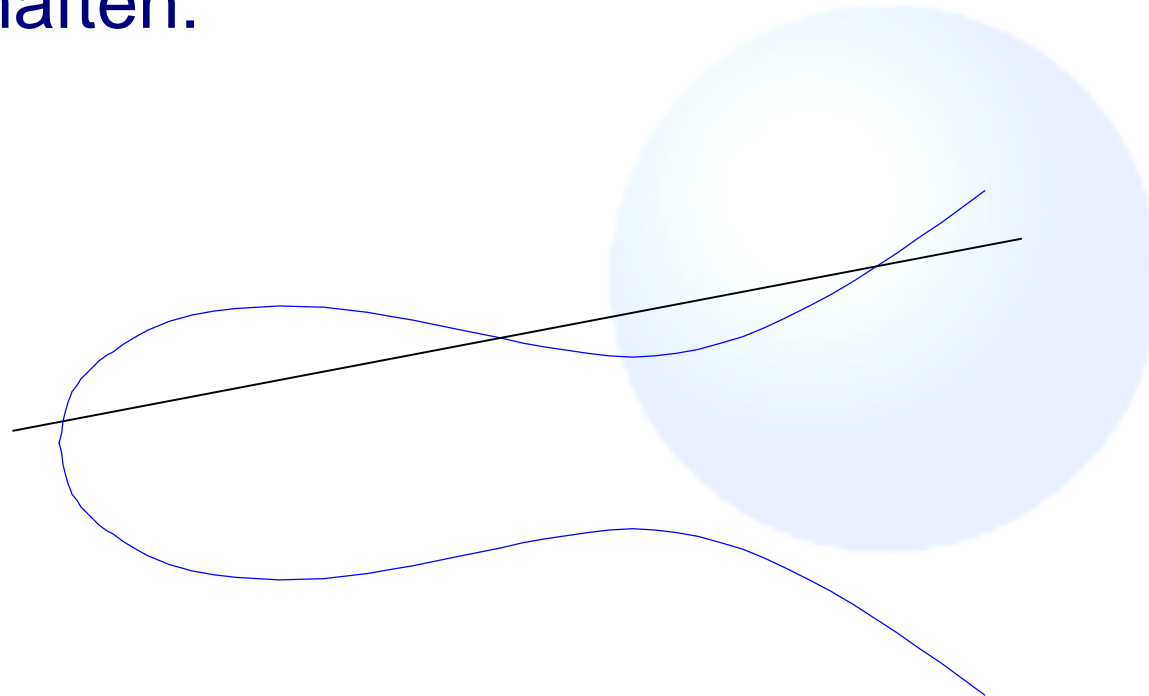
Was ist eine elliptische Kurve?



Eine Ellipse ist **keine** elliptische Kurve!

# Elliptische Kurven

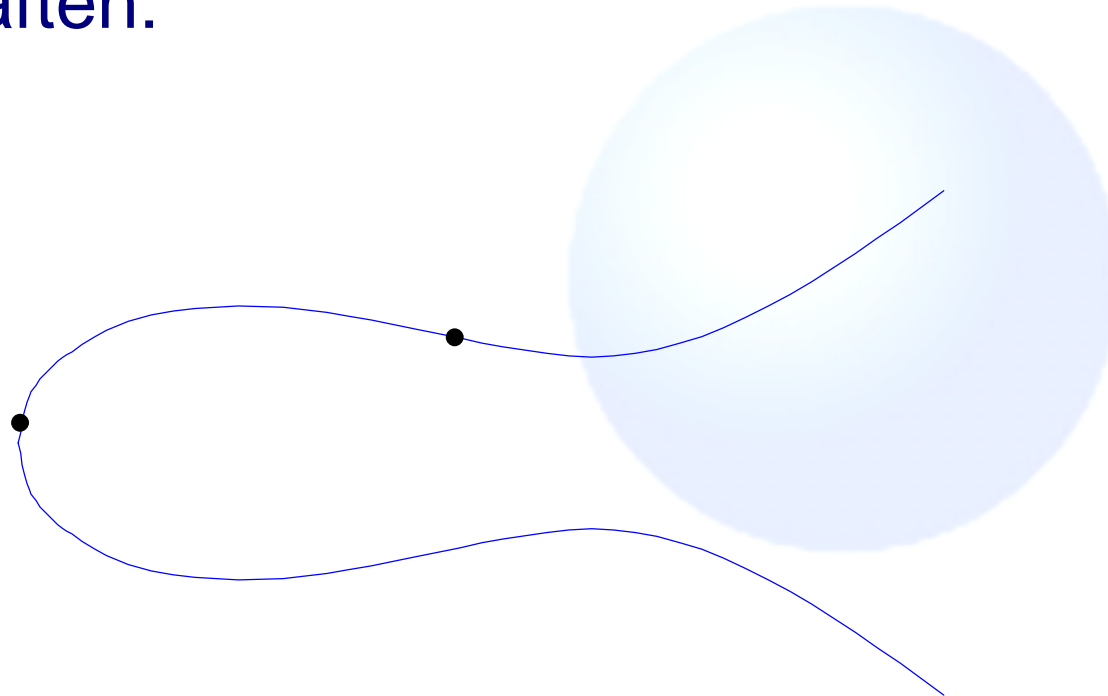
Eigenschaften:



Eine Gerade schneidet eine elliptische  
Kurve in **drei** Punkten.

# Elliptische Kurven

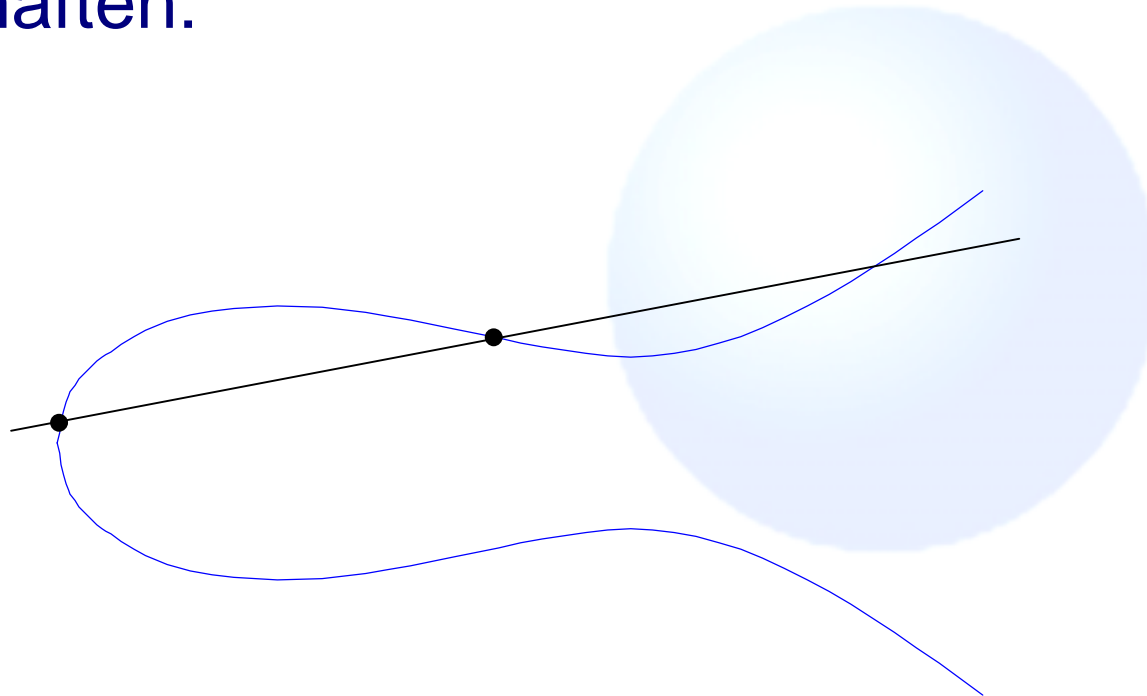
Eigenschaften:



Zwei Punkte auf der Kurve ...

# Elliptische Kurven

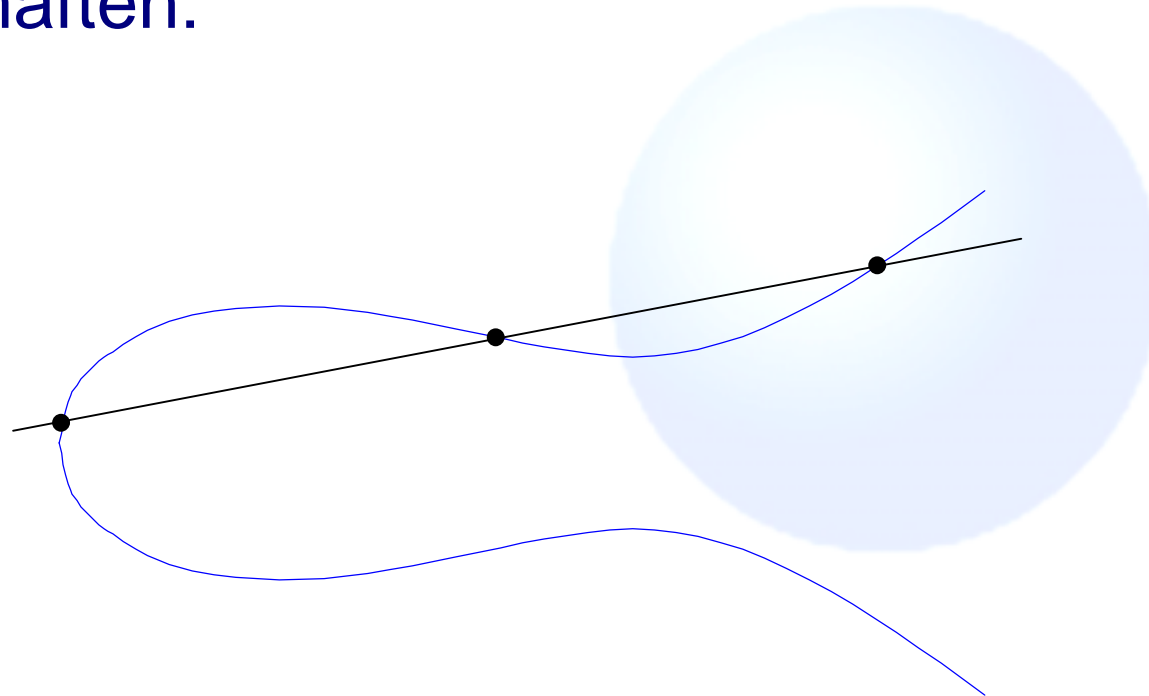
Eigenschaften:



Zwei Punkte auf der Kurve lassen sich durch eine Gerade verbinden.

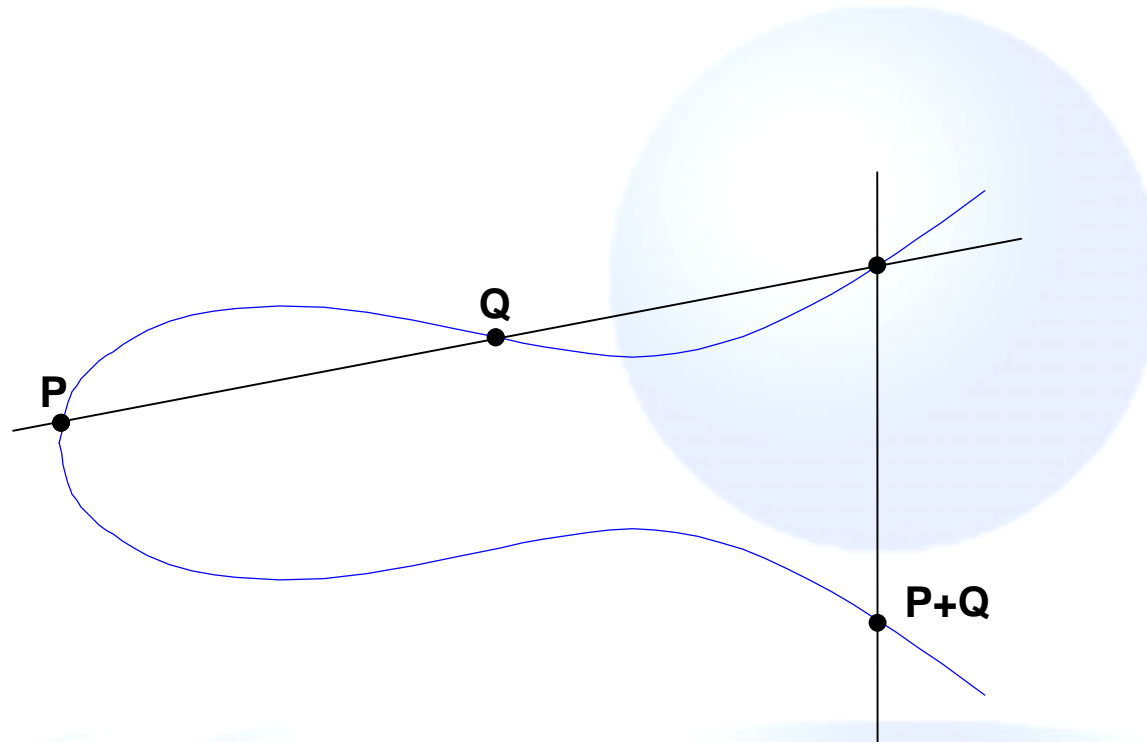
# Elliptische Kurven

Eigenschaften:

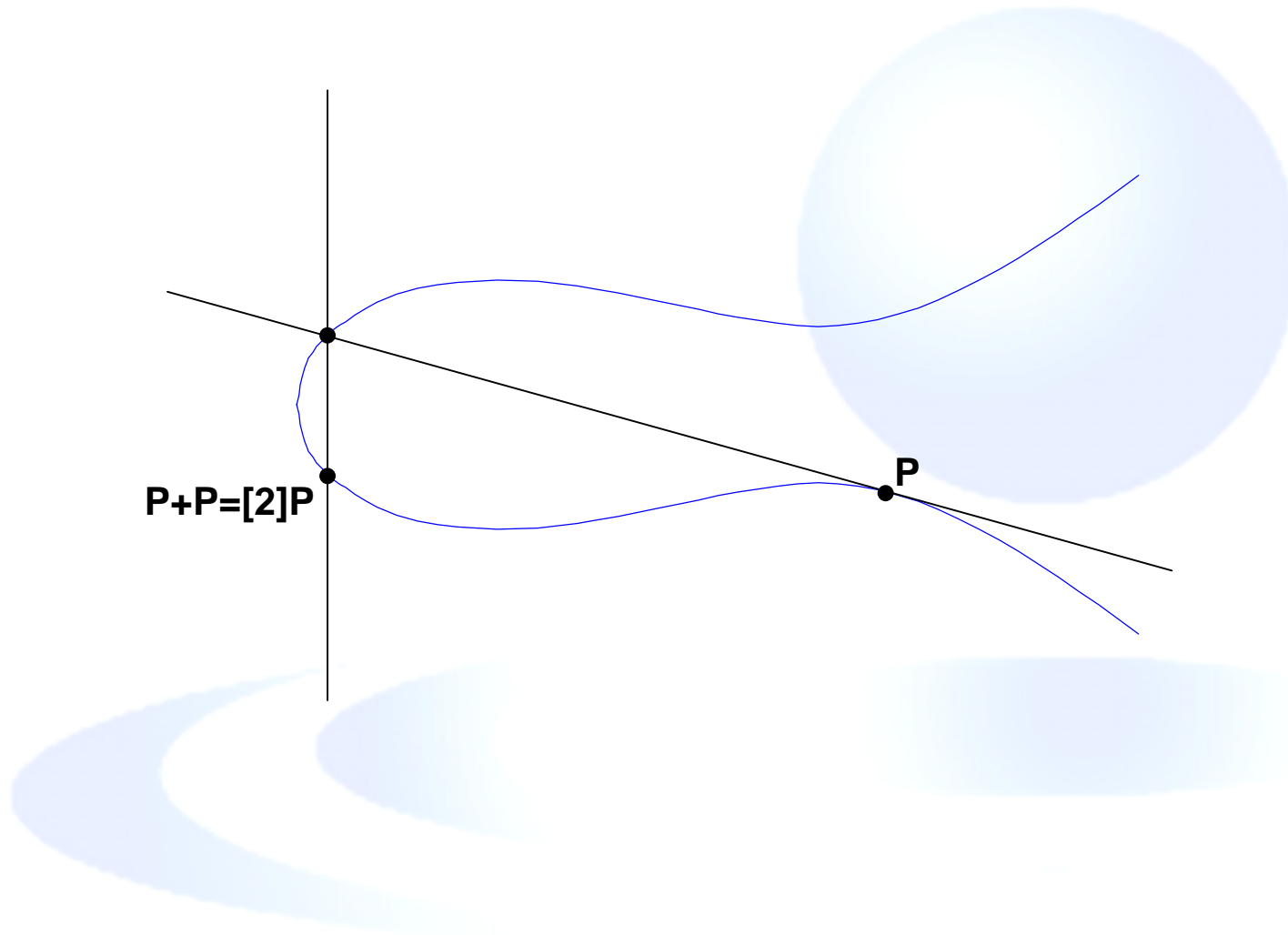


Die Gerade trifft die Kurve in einem weiteren Punkt.

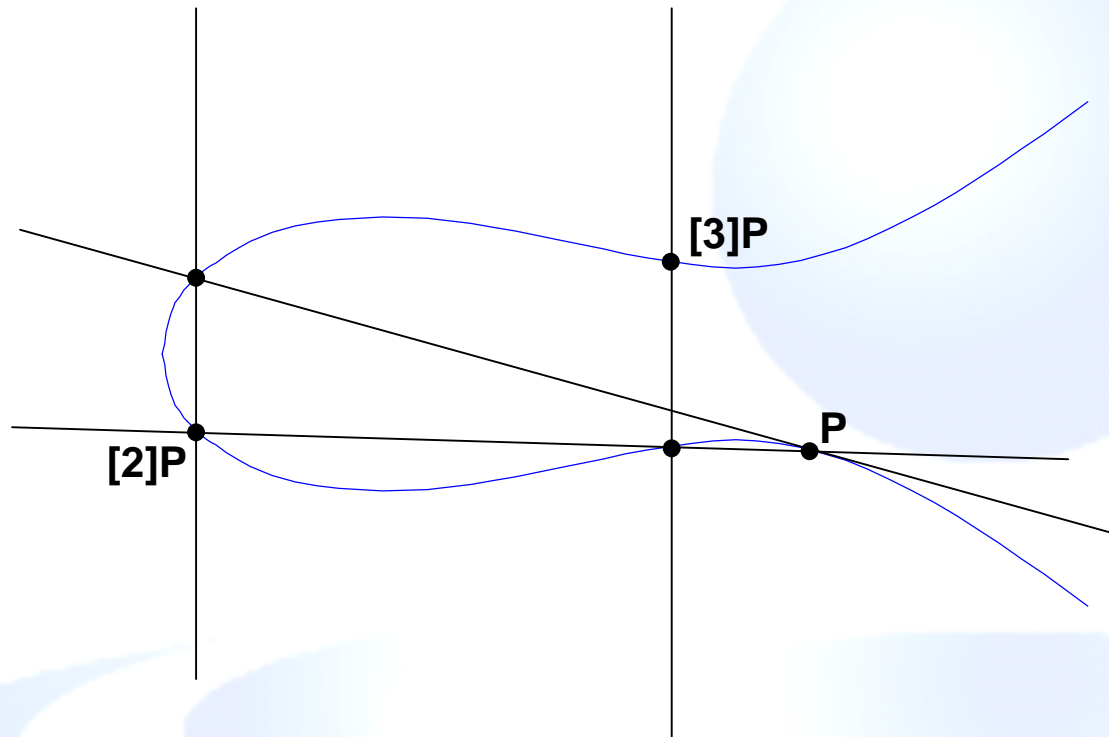
# Punktaddition



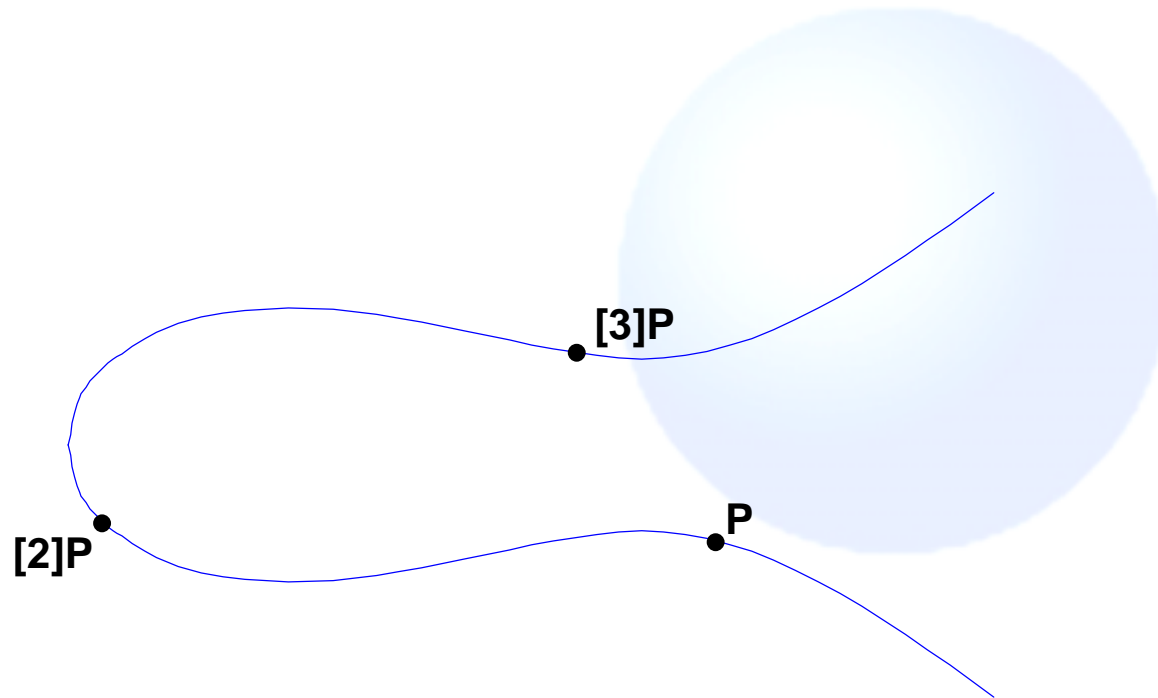
# Punktverdopplung



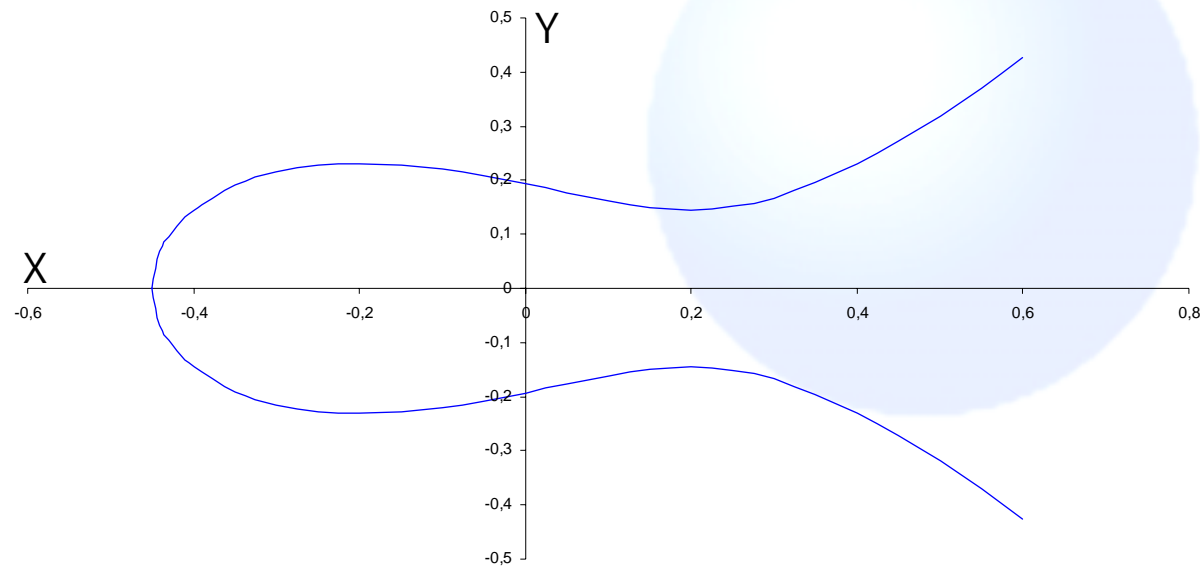
# Skalare Vielfache



# Skalare Vielfache



Was ist eine elliptische Kurve?



Gleichung: 
$$Y^2 = X^3 + 0,12 X + 0,037125$$

Berechnung der Punktezuordnung:

- P und Q zwei Punkte auf der Kurve
- $P = (x_1, y_1)$  und  $Q = (x_2, y_2)$
- $\lambda = (y_2 - y_1) / (x_2 - x_1)$  Steigung der Gerade
- $x_3 = \lambda^2 - x_1 - x_2$  und  $y_3 = y_1 + (x_3 - x_1) * \lambda$   
Koordinaten des dritten Punktes
- $P + Q = (x_3, -y_3)$

- Eine elliptische Kurve ist die Lösungsmenge einer geeigneten kubischen Gleichung.
- Eine Gerade schneidet die Kurve in drei Punkten.
- Zwei Punkten auf der Kurve lässt sich ein dritter zuordnen.
- Diese Zuordnung lässt sich einfach berechnen.
- Durch Iteration dieser Zuordnung werden Punkte scheinbar zufällig über die Kurve verteilt.

Übertragung auf ganze Zahlen:

- eine große Primzahl  $p$
- Stichwort:  $GF(p)$
- eine Gleichung der Form  $y^2 = x^3 + a x + b$  mit ganzen Zahlen  $a$  und  $b$
- Elliptische Kurve:  $4 a^3 + 27 b^2 \neq 0$
- Punkte der Kurve sind Lösungen dieser Gleichung modulo  $p$

# Implementation

Beispiel:  $p = 5$ ,  $a = 2$ ,  $b = 1$

4	○					
3		○		○		
2		○		○		
1	○					
0						
y	x	0	1	2	3	4

Alternative zu einer großen Primzahl  $p$ :

- Statt ganzen Zahlen in Binärdarstellung: Bitvektoren
- Addition und Multiplikation ohne Übertrag
- Beispiel:  $1 + 1 = 0$ ,  $11 * 111 = 1001$
- Arithmetik ähnelt der ganzer Zahlen
- Modulus: prim, Länge  $n + 1$
- Stichwort:  $GF(2^n)$
- Die elliptische Kurve wird durch eine Gleichung der Form  $y^2 + x y = x^3 + a x^2 + b$  definiert

- Symmetrische Verfahren
  - ▶ Effizient in der Performance
  - ▶ Problem: Übermittlung und Geheimhaltung des Schlüssels
- Asymmetrische Verfahren (Public Key)
  - ▶ öffentlicher Schlüssel / geheimer Schlüssel
  - ▶ Sicherheit durch mathematisches Problem
  - ▶ größere Schlüssellänge, schlechtere Performance

Weit verbreitete Verfahren:

- RSA (1977)
- Diffie-Hellman (1976)
- ElGamal (1984)
- DSA : Digital Signature Algorithm (1991)

## RSA-Verfahren:

- Primzahlen  $p, q$
- Produkt  $N = p * q$
- Schlüsselpaar  $e, d$
- Verschlüsselung:  $M \rightarrow M^e \text{ modulo } N$
- Sicherheit:  $e \rightarrow d$  erfordert  $N \rightarrow p, q$ 
  - ▶ Faktorisierungsproblem
  - ▶ Zahlkörpersieb: 512 bit geknackt

Andere Verfahren (DH, ElGamal, DSA)

- Parameter: Primzahl  $p$ , ganze Zahl  $g$
- Geheim: Exponent  $e$
- Öffentlich:  $h = g^e$  modulo  $p$
- Sicherheit:  $p, g, h \rightarrow e$ 
  - Diskreter Logarithmus
  - Zahlkörpersieb

## Diskrete Logarithmus-Problem:

- Beispiel:
  - ▶  $p=11, g=2$
  - ▶  $\{ 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 \}$   
Menge aller Potenzen  $g^e$  modulo  $p$  für  $e = 1, 2, 3, \dots$
- Problem:
  - ▶ finde zu einer Potenz den Exponenten !
- Kryptographische Anwendung:
  - ▶  $p$  eine 300-stellige Primzahl

# ECC

Problem	DL	ECDL
Parameter	Primzahl $p$	$p$ und Kurvenparameter $(a, b)$
Basis	Rest $g$	Punkt $P$ auf der Kurve
Öffentlich	$g^e$ modulo $p$	Punkt $[n] P$
Geheim	Exponent $e$	Vielfachheit $n$
Größe von $p$	1024 bit	160 bit
Operation	1 modulare Multiplikation	2 modulare Multiplikationen 1 modulare Division

Es existieren zu den Verfahren

- Diffie-Hellman
- ElGamal
- DSA

Varianten mit elliptischen Kurven.

## Sicherheit der Verfahren:

- RSA, DH, ElGamal, DSA:
  - ▶ subexponentielles Verfahren: Zahlkörper-Sieb
- ECC:
  - ▶ „Goldenes Schild“ (Neal Koblitz) schützt gegen bekannte Attacken
  - ▶ exponentielle Verfahren: Pollard rho
  - ▶ Empfehlungen für Kurven beachten
  - ▶ Punkteanzahl bestimmen

# Vergleich

Bei vergleichbarer Sicherheit zu RSA sind bei ECC kürzere Schlüssellängen nötig:

RSA	512	1024	2048
ECC	108	160	210

Im Vergleich zu RSA benötigt ECC kürzere  
Bitlängen bei

- Öffentlichen / privaten Schlüssel
- Modulus der modularen Arithmetik
- Signaturen
- Zertifikaten

# Vergleich

(Bits)	RSA	DSA	ECC
Parameter	0	2208	481
Öffentlicher Schlüssel	1088	1024	161
Privater Schlüssel	2048	160	160
Signatur	1024	320	320

- iX 9/2001 : Einführender Artikel über ECC
- [www.elliptische-kurven.de](http://www.elliptische-kurven.de) : Online-Einführung
- [www.ecc-brainpool.org](http://www.ecc-brainpool.org) : Interessengemeinschaft

SRC Security Research & Consulting GmbH  
Graurheindorfer Str. 149a  
53117 Bonn

Tel. +49-(0)228-2806-0

Fax: +49-(0)228-2806-199

E-mail: [info@src-gmbh.de](mailto:info@src-gmbh.de)

WWW: [www.src-gmbh.de](http://www.src-gmbh.de)