ECC:
Elliptic Curve Cryptography

Teil1: Einführung, Elliptische Kurven

Universität Bremen

Albert Diner
Kilian Krys

kurzer Exkurs zur Kryptographie (1)

- Symmetrische Kryptographie
  - gemeinsames Geheimnis (Schlüssel)
  - vertraulicher Informationskanal wird vorrausgesetzt

  Lösung des Schlüsselverteilungsproblem:
- Asymmetrische (Publik Key-) Kryptographie
  - Einwegfunktion, Einwegfunktion mit Falltür
    - Diffie-Hellman
    - ElGamal-Verfahren

Universität Bremen

Quelle:
• BORMANN, Carsten; SOHR, Karsten. *IT-Sicherheit: Kryptographie - Asymmetrische Kryptographie*, Vorlesung Informationssicherheit, 2012-11-26.

kurzer Exkurs zur Kryptographie (2)

- Asymmetrische Krypto mit Diffie-Hellman

  p: große Primzahl

  g: primitiv Wurzel von p

Alice

Wählt zufällig eine Zahl **a**.
Berechnet $\boldsymbol{\alpha := g^a \bmod p}$.

Bob

Wählt zufällig eine Zahl **b**.
Berechnet $\boldsymbol{\beta := g^b \bmod p}$.

Alice $\xrightarrow{\alpha}$ Bob

Bob $\xrightarrow{\beta}$ Alice

Alice: Berechnet $\boldsymbol{\beta^a \bmod p}$

Bob: Berechnet $\boldsymbol{\alpha^b \bmod p}$

$$\boldsymbol{\beta^a \bmod p} = (g^b)^a \bmod p = g^{ba} \bmod p = g^{ab} \bmod p = (g^a)^b \bmod p = \boldsymbol{\alpha^b \bmod p} =: K_{AB}$$

Quelle:
• BORMANN, Carsten; SOHR, Karsten. *IT-Sicherheit: Kryptographie - Asymmetrische Kryptographie*, Vorlesung Informationssicherheit, 2012-11-26.

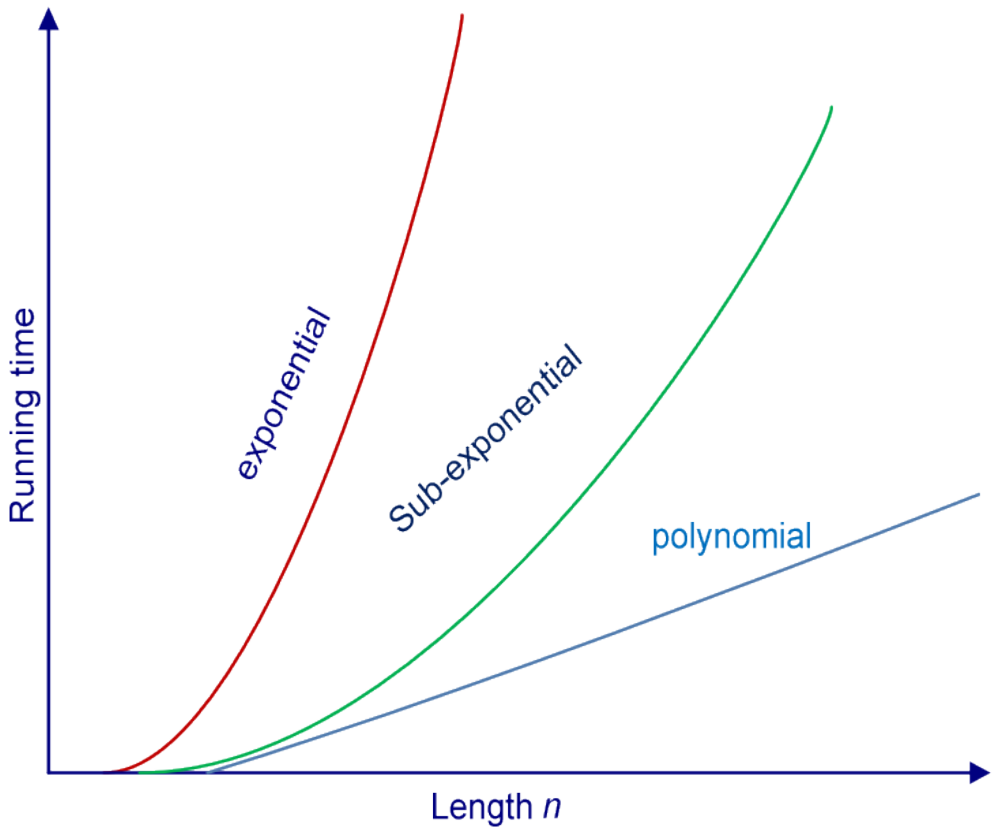
Sicherheit & Aufwand

- Wie sicher ist das zugrunde liegende Problem der Kryptographie-Verfahren?
  - RSA: Faktorisierungsproblem
  - Diffie-Hellman: Diskreter Logarithmus
- Asymetrische Kryptographie (RSA)
  - Die 232-stellige Zahl RSA-768 wurde 2009 in Primfaktoren zerlegt. Aufwand: ca. 2,5 Jahre mit mehreren hundert Rechnern.
  - aktuell "sicher": 1024 / 2048 Bit Schlüssel
  - Schlüsselgenerierung und ver-/entschlüsselung recht aufwendig

Quellen:
• Wikipedia. *RSA Factoring Challenge*, 2013-04-04, URL: de.wikipedia.org/wiki/RSA_Factoring_Challenge (Aufruf 2013-05-25)
• KLEINJUNG, Thorsten, et al. Factorization of a 768-bit RSA modulus. In: *Advances in Cryptology–CRYPTO 2010*. Springer Berlin Heidelberg, 2010. S. 333-350.
• MEIER, Willi; STAFFELBACH, Othmar. Kryptographie und elliptische Kurven. *Elemente der Mathematik*, 1997, 52. Jg., Nr. 4, S. 137-151.

Komplexität von Algorithmen

Laufzeit	Formel
konstant	$O(1)$
logarithmisch	$O(\log n)$
linear	$O(n)$
n-log-n	$O(n \log n)$
quadratisch	$O(n^2)$
polynomial	$O(n^k)$ für $k \geq 1$
sub-exponential	$O(2^{(n\text{^}s)})$ für $s > 0$
exponential	$O(d^n)$ für $d > 1$



Quellen:
• Wikipedia. *Komplexitätstheorie*, 2013-04-27, URL: de.wikipedia.org/wiki/Komplexitätstheorie (Aufruf 2013-05-24).
• LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).

Sicherheit der Krypto-Algorithmen

- RSA: Faktorisierungsproblem
  - Das Faktorisierungsproblem kann mit dem Zahlkörpersieb (GNFS: general number field sieve) gelöst werden.
    - Der zeitlicher Aufwand ist **subexponentiell**:

$$O(e^{1.923(\log n)^{1/3}(\log\log n)^{2/3}})$$

- Diffie-Hellman: Diskreter Logarithmus Problem
  - Auch hier ist das schnellste bekannte Verfahren GNFS mit **subexponentieller** Laufzeit.

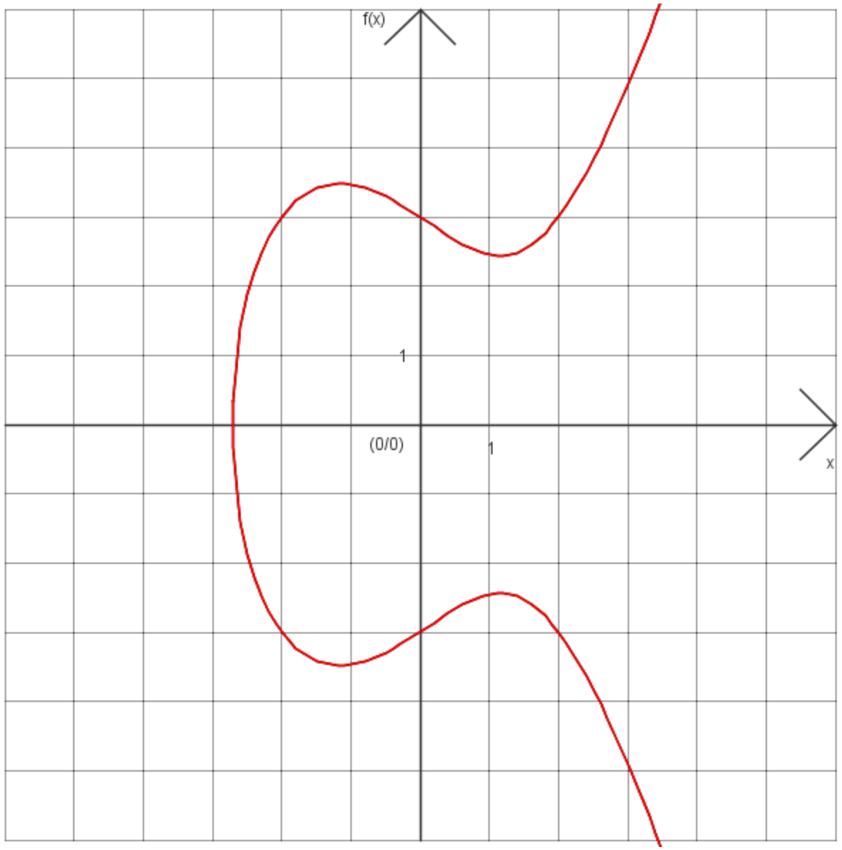
Quellen:
• MEIER, Willi; STAFFELBACH, Othmar. Kryptographie und elliptische Kurven. *Elemente der Mathematik*, 1997, 52. Jg., Nr. 4, S. 137-151.
• LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).

Elliptische Kurven

- Theorie der elliptischen Kurven ist Teil der arithmetischen Geometrie
- Mit elliptischen Kurven kann man
  - Primfaktoren großer Zahlen finden
  - berechnen von Quadratwurzeln modulo p
  - Kryptographie durchführen
- Halfen bei der Lösung des Gaußschen Klassenzahlproblems
- Entstanden aus der Idee, den Umfang einer Ellipse zu berechnen

Quellen: • NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
• LEMMERMEYER, Franz. *Elliptische Kurven I*. 1999, URL: http://www.zum.de/Faecher/Materialien/rubin/texte/elliptic_curve.pdf (Aufruf 2013-05-27).
• SCHWEIZER, Patrick. *Berechnung elliptischer und hyperelliptischer Kurven für paarungsbasierte Kryptografie*, Diplomarbeit, Institut für Mathematik, Technische Universität Berlin, 2008, URL: www.math.tu-berlin.de/~kant/publications/diplom/schweitzer.pdf (Aufruf 2013-05-27).

Elliptische Kurven allgemein (1)



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

Kurve mit

$a = -4$

$b = 9$

Elliptische Kurven allgemein (2)

Polynom:

$F(x,y) = x^3 - a_1xy + a_2x^2 - a_3y + a_4x + a_5 - y^2$

Elliptische Kurve (Weierstraßsche Normalform)

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \qquad a_i \in K$

keine Singularität

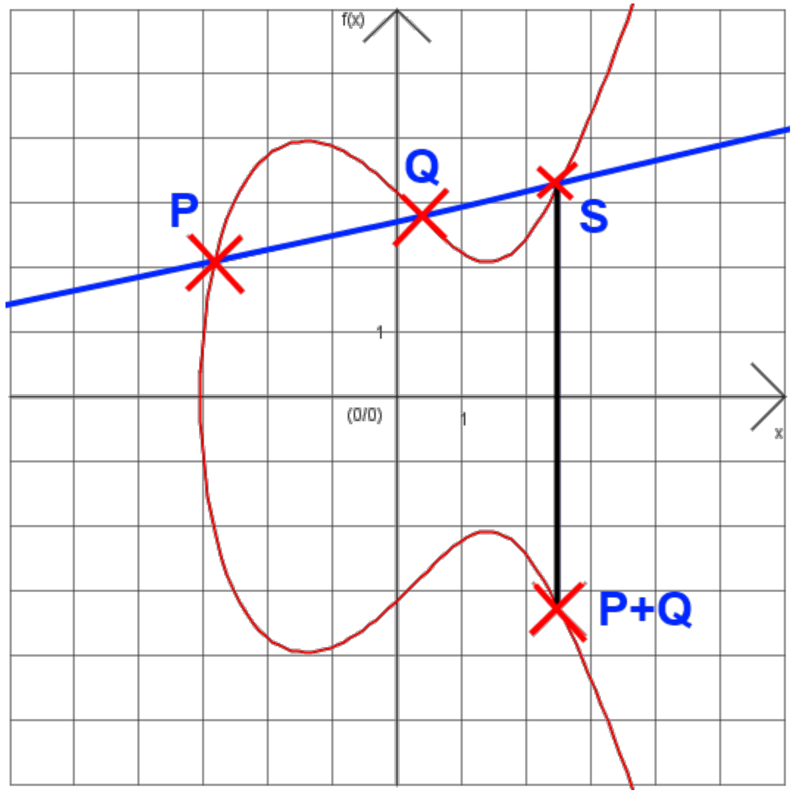
$y^2 = x^3 + a_4x + a_5$

Vereinfachte Weierstraßsche Normalform

$y^2 = x^3 + ax + b \qquad \text{mit } 4a^3 + 27b^2 \neq 0$

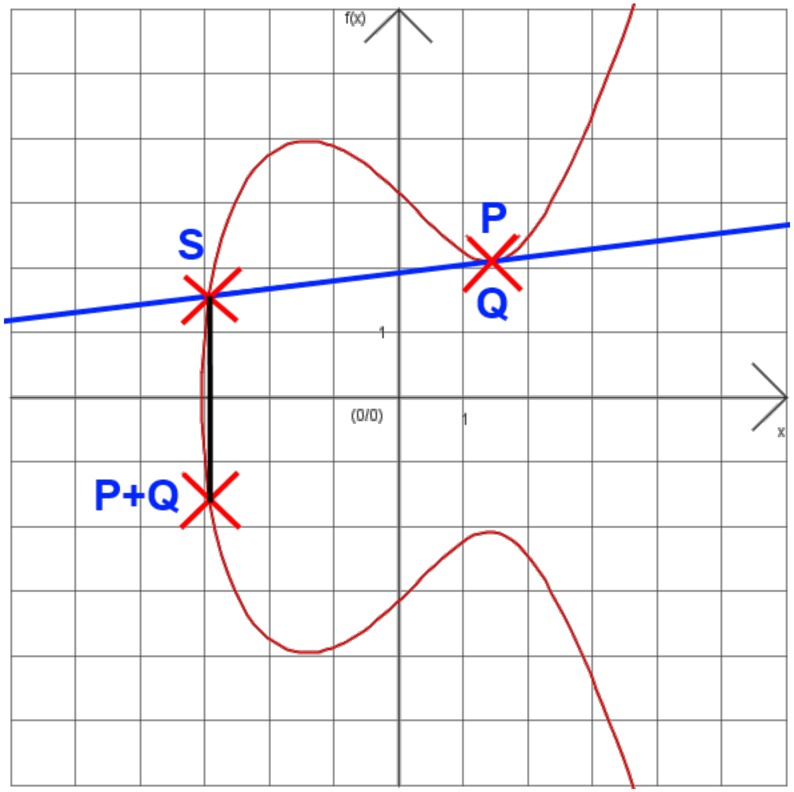
Quelle:
• MÜHLENFELD, Björn. *Einführung in Elliptische Kurven*. Ausarbeitung im Rahmen des Proseminars Public-Key Kryptographie, Universität Paderborn, 2006-01-10, URL: http://www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Muehlenfeld_Ausarbeitung.pdf (Aufruf 2013-05-27).

Rechnen mit Punkten auf elliptischen Kurven (1)



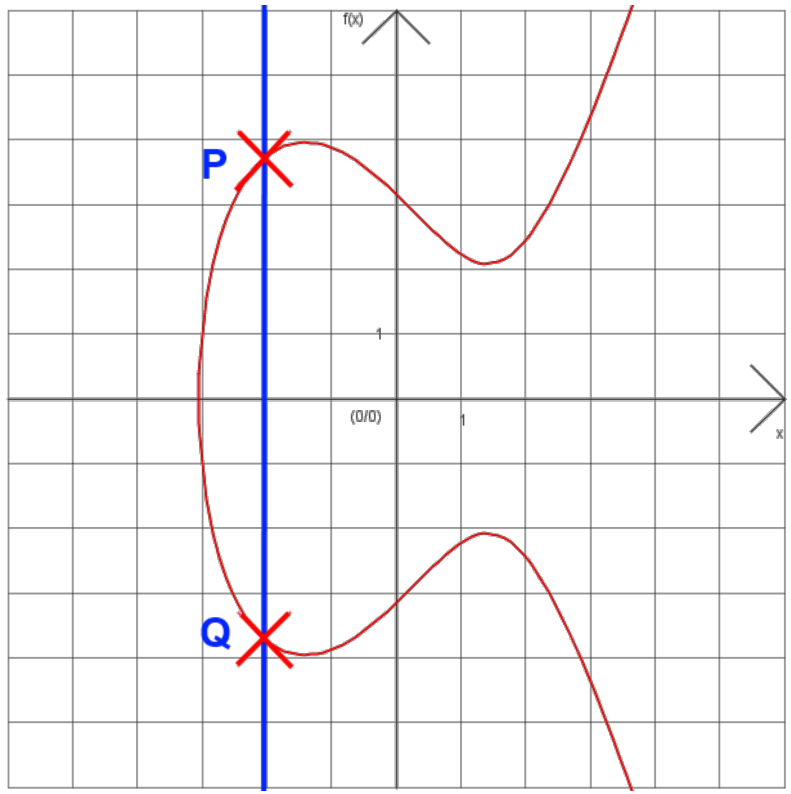
Quelle:
• STIBOR, Thomas; ECKERT, Claudia. *Kapitel 11 Eliptische Kurven*, Vorlesung Kryptographie, Präsentation, Technische Universität München, 2009-06-24, URL: www.sec.in.tum.de/assets/lehre/ss09/kryptographie/Kapitel.11.pdf (Aufruf 2013-05-27).

Rechnen mit Punkten auf elliptischen Kurven (2)



Quelle:
• MÜHLENFELD, Björn. *Einführung in Elliptische Kurven*. Ausarbeitung im Rahmen des Proseminars Public-Key Kryptographie, Universität Paderborn, 2006-01-10, URL: http://www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Muehlenfeld_Ausarbeitung.pdf (Aufruf 2013-05-27).

Rechnen mit Punkten auf elliptischen Kurven (3)



Quelle:
- MÜHLENFELD, Björn. *Einführung in Elliptische Kurven*. Ausarbeitung im Rahmen des Proseminars Public-Key Kryptographie, Universität Paderborn, 2006-01-10, URL: http://www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Muehlenfeld_Ausarbeitung.pdf (Aufruf 2013-05-27).

Rechnen mit Punkten auf elliptischen Kurven (4)

- Zusätzlicher Punkt für „Unendlich“

- Punkte bilden eine (abelsche) Gruppe
  - Operation: + mit P + Q = R
    - Assoziativität: P+(Q+R) = (P+Q)+R
    - Kommutativität: P+Q = Q+R
  - neutrales Element: ∞ mit P + ∞ = ∞ + P = P
  - inverses Element: (x,-y) mit P+(-P) = -P + P = ∞

Universität Bremen

Quellen:
• MÜHLENFELD, Björn. *Einführung in Elliptische Kurven*. Ausarbeitung im Rahmen des Proseminars Public-Key Kryptographie, Universität Paderborn, 2006-01-10, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Muehlenfeld_Ausarbeitung.pdf (Aufruf 2013-05-27).
• STIBOR, Thomas; ECKERT, Claudia. *Kapitel 11 Eliptische Kurven*, Vorlesung Kryptographie, Präsentation, Technische Universität München, 2009-06-24, URL: www.sec.in.tum.de/assets/lehre/ss09/kryptographie/Kapitel.11.pdf (Aufruf 2013-05-27).

Rechnen mit Punkten auf elliptischen Kurven (5)

Addition von Punkten auf einer elliptischen Kurve mit $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$

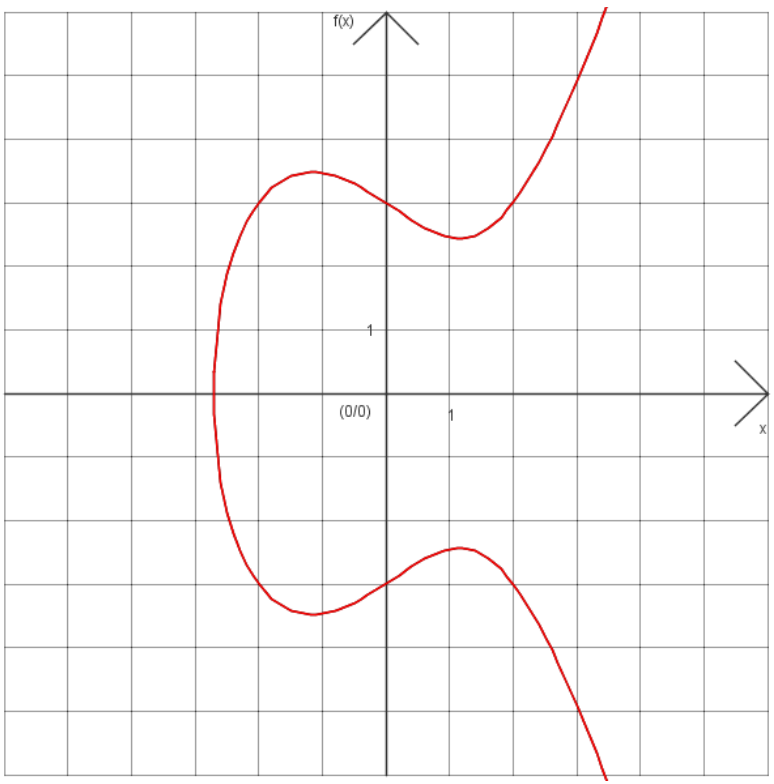
- für $P = \infty$ — $P+Q = Q+P = Q$
- für $x_P = x_Q$ und $y_P = -y_Q$ — $P+Q = \infty$

  sonst: (s: Steigung der Gerade durch P und Q)
- $P+Q = (x_R, y_R)$ — $s = (y_P - y_Q) / (x_P - x_Q)$

  $x_R = s^2 - x_P - x_Q$ — $y_R = s \cdot (x_P - x_R) - y_P$
- für $P = Q$ — $s = (3 \cdot x_P^2 + a) / (2y_P)$

Quellen:
• MENEZES, Alfred J.; VANSTONE, Scott A. Elliptic curve cryptosystems and their implementation. *Journal of Cryptology*, 1993, 6. Jg., Nr. 4, S. 209-224.
• KÖHLER, Günter; GREINER, Richard. *Elliptische Kurven in der Kryptographie*, Skript, Projekttage Mathematik 2002, 2002, URL: www.mathematik.uni-wuerzburg.de/~greiner/Download/MathSpiel/PT2002-ellku-scr.pdf (Aufruf 2013-05-25).
• BRIEDEMANN, M.; BUSCH, A.;HEIER, M.; HÜBNER, S.; KRAUS, S.; ZÜRN, A.; KÖHLER, G.; GREINER, R.; HEUBECK, B. *Elliptische Kurven in der Kryptographie*, Arbeitsbericht der Arbeitsgruppe, Projekttage 2002, 2002, URL: www.mathematik.uni-wuerzburg.de/~greiner/Download/MathSpiel/PT2002-ellku-abr.pdf (Aufruf 2013-05-25).

Rechnen mit Punkten auf elliptischen Kurven (6)



$\mathbf{y^2 = x^3 + ax + b}$

Kurve mit a = -4, b = 9

gewählte Punkte:

P = (-2, 3), Q = (0, 3)

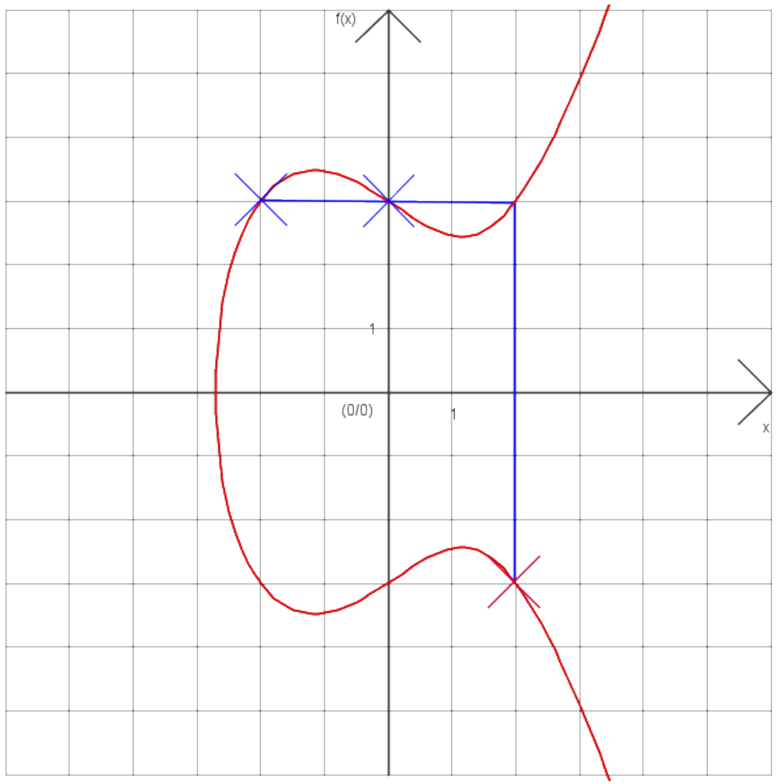
Berechnung:

s = (3 - 3) / ((-2) - 0) = 0 / (-2) = 0

$x_R = 0^2 - (-2) - 0 = -2$

$y_R = 0 \cdot ((-2) - (-2)) - 3 = -3$

Rechnen mit Punkten auf elliptischen Kurven (7)



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

Kurve mit a = -4, b = 9

gewählte Punkte:

P = (-2, 3), Q = (0, 3)

Berechnung:

s = (3 - 3) / ((-2) - 0) = 0 / (-2) = 0

$x_R = 0^2 - (-2) - 0 = -2$

$y_R = 0 \cdot ((-2) - (-2)) - 3 = -3$

R = (-2, -3)

Elliptische Kurve aus einzelnen Punkten

- Ziel: Elliptische Kurven als Krypto-Verfahren
- Problem bei Graphen über $\mathbb{R}$: z.T. unendlich viele Nachkommastellen!

  $\Rightarrow$ Zahlen werden gerundet!

$\Rightarrow$ Endliche (ganzzahlige) Körper verwenden

Quelle:
• MÜHLENFELD, Björn. *Einführung in Elliptische Kurven*. Ausarbeitung im Rahmen des Proseminars Public-Key Kryptographie, Universität Paderborn, 2006-01-10, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Muehlenfeld_Ausarbeitung.pdf (Aufruf 2013-05-27).

Elliptische Kurve in Z_P (1)

- P: Primzahl
- Z_P ist ein Restklassenkörper

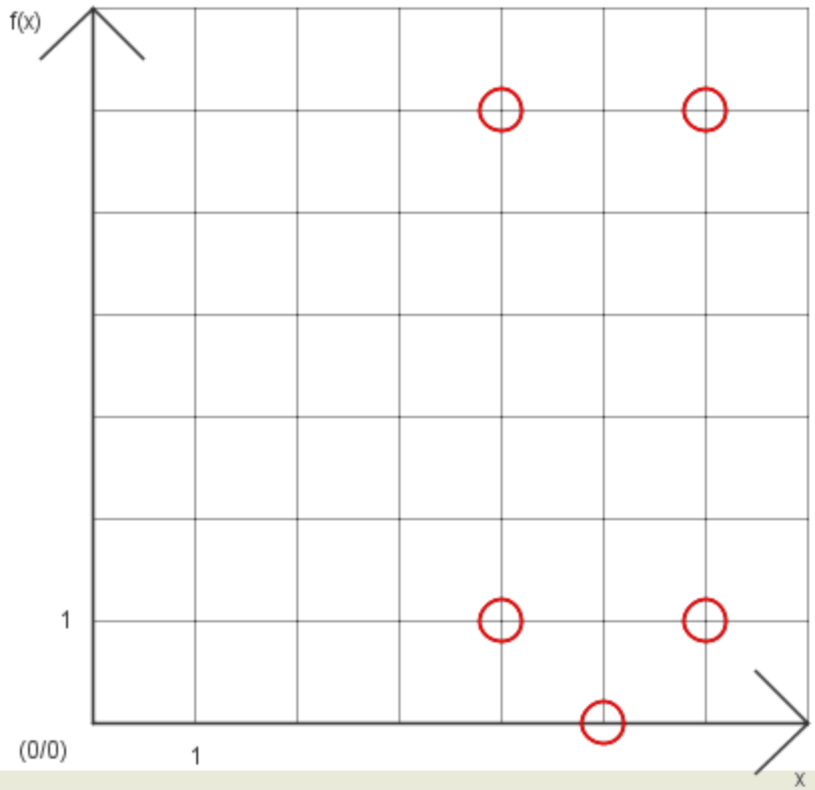
  statt unendliche viele Punkte in $\mathbb{R}$

  beschränkten Zahlenbereich von 0 bis p-1
- statt $y^2 = x^3 + ax + b$
- jetzt: $(y^2) \bmod p = (x^3 + ax + b) \bmod p$

Quellen:
• DEMYTKO, N. A new elliptic curve based analogue of RSA. In: *Advances in Cryptology—EUROCRYPT'93*. Springer Berlin Heidelberg, 1994. S. 40-49.
• MÜHLENFELD, Björn. *Einführung in Elliptische Kurven*. Ausarbeitung im Rahmen des Proseminars Public-Key Kryptographie, Universität Paderborn, 2006-01-10, URL: http://www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Muehlenfeld_Ausarbeitung.pdf (Aufruf 2013-05-27).

Elliptische Kurve in Z_P (2)

a = 1, b = 3, p = 7 $\qquad$ $y^2 = x^3 + ax + b$



Berechnung der Kurve in Z_P (1)

a = 1, b = 3, p = 7 $y^2 = x^3 + ax + b$

x	**(x^3+x+3) mod p**	**y**	**Punkte**
0			
1			
2			
3			
4			
5			
6			

zuerst eine Tabelle mit x-Werten von 0 bis p-1 erstellen

Quellen:
• NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
• STIBOR, Thomas; ECKERT, Claudia. *Kapitel 11 Eliptische Kurven*, Vorlesung Kryptographie, Präsentation, Technische Universität München, 2009-06-24, URL: www.sec.in.tum.de/assets/lehre/ss09/kryptographie/Kapitel.11.pdf (Aufruf 2013-05-27).

Berechnung der Kurve in Z_P (2)

$a = 1, b = 3, p = 7$ $\qquad$ $y^2 = x^3 + ax + b$

x	**$(x^3+x+3) \bmod p$**	**y**	**Punkte**
0	3		
1	5		
2	5		
3	5		
4	1		
5	0		
6	1		

den rechten Teil der Formel **(x^3+x+3) mod p** berechnen

Quellen:
• NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
• STIBOR, Thomas; ECKERT, Claudia. *Kapitel 11 Eliptische Kurven*, Vorlesung Kryptographie, Präsentation, Technische Universität München, 2009-06-24, URL: www.sec.in.tum.de/assets/lehre/ss09/kryptographie/Kapitel.11.pdf (Aufruf 2013-05-27).

Berechnung der Kurve in Z_P (3)

$a = 1, b = 3, p = 7$ $y^2 = x^3 + ax + b$

x	$(x^3+x+3) \bmod p$	y	Punkte
0	3	-	
1	5	-	
2	5	-	
3	5	-	
4	1	± 1	
5	0	0	
6	1	± 1	

bei dem y-Wert muss die Wurzel aus y^2 eine ganze Zahl sein

Quellen:
• NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
• STIBOR, Thomas; ECKERT, Claudia. *Kapitel 11 Eliptische Kurven*, Vorlesung Kryptographie, Präsentation, Technische Universität München, 2009-06-24, URL: www.sec.in.tum.de/assets/lehre/ss09/kryptographie/Kapitel.11.pdf (Aufruf 2013-05-27).

Berechnung der Kurve in Z_P (4)

a = 1, b = 3, p = 7 $y^2 = x^3 + ax + b$

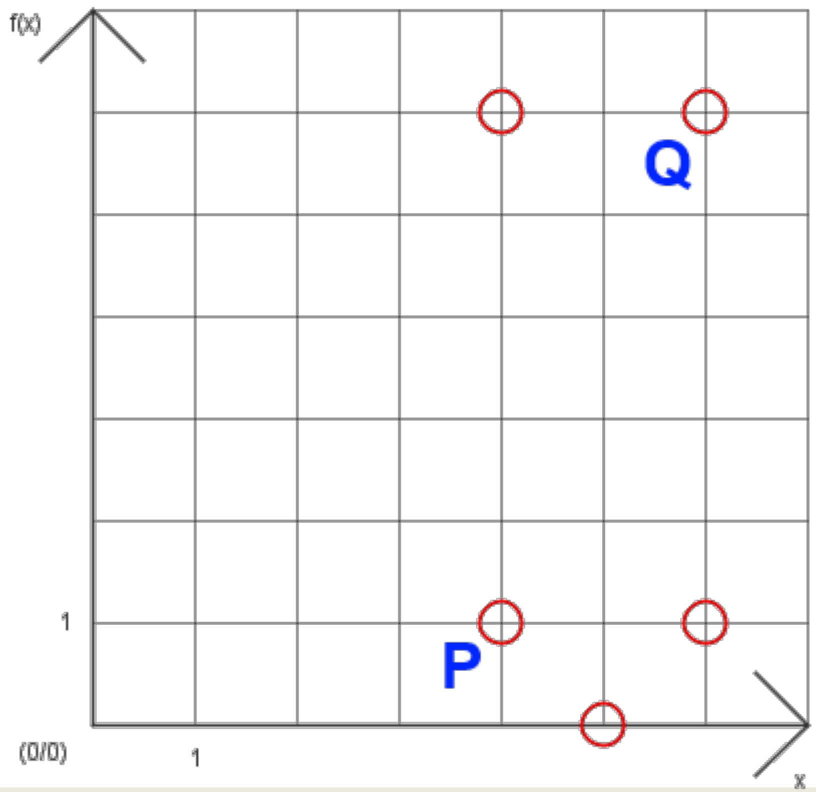
x	**(x^3+x+3) mod p**	**y**	**Punkte**
0	3	-	
1	5	-	
2	5	-	
3	5	-	
4	1	± 1	(4,1) ; (4,6)
5	0	0	(5,0)
6	1	± 1	(6,1) ; (6,6)

bei ganzzahligen Ergebnissen mit y ungleich Null, gibt es immer zwei Lösungen und somit auch zwei Punkte

Quellen:
• NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
• STIBOR, Thomas; ECKERT, Claudia. *Kapitel 11 Eliptische Kurven*, Vorlesung Kryptographie, Präsentation, Technische Universität München, 2009-06-24, URL: www.sec.in.tum.de/assets/lehre/ss09/kryptographie/Kapitel.11.pdf (Aufruf 2013-05-27).

Addition von Punkten in Z_P (1)

a = 1, b = 3, p = 7 P = (4, 1) Q = (6, 6)



Addition von Punkten in Z_P (2)

für $x_P = x_Q$ und $y_P = - y_Q$ $\Rightarrow$ $P + Q = \infty$

für $P = (x_P, 0)$ $\Rightarrow$ $P + P = \infty$

sonst

$x_R = (s^2 - x_P - x_Q) \bmod p$

$y_R = s \cdot (x_P - x_R) - y_P \bmod p$

für $P \neq Q$ $\Rightarrow$ $s = ((y_P - y_Q) / (x_P - x_Q)) \bmod p$

sonst $\Rightarrow$ $s = ((3 \cdot x_P{}^2 + a) / (2 \cdot y_P)) \bmod p$

Quellen:
• DEMYTKO, N. A new elliptic curve based analogue of RSA. In: *Advances in Cryptology—EUROCRYPT'93*. Springer Berlin Heidelberg, 1994. S. 40-49.
• KÖHLER, Günter; GREINER, Richard. *Elliptische Kurven in der Kryptographie*, Skript, Projekttage Mathematik 2002, 2002, URL: www.mathematik.uni-wuerzburg.de/~greiner/Download/MathSpiel/PT2002-ellku-scr.pdf (Aufruf 2013-05-25).
• BRIEDEMANN, M.; BUSCH, A.;HEIER, M.; HÜBNER, S.; KRAUS, S.; ZÜRN, A.; KÖHLER, G.; GREINER, R.; HEUBECK, B. *Elliptische Kurven in der Kryptographie*, Arbeitsbericht der Arbeitsgruppe, Projekttage 2002, 2002, URL: www.mathematik.uni-wuerzburg.de/~greiner/Download/MathSpiel/PT2002-ellku-abr.pdf (Aufruf 2013-05-25).

Addition von Punkten in Z_P (3)

Beispiel: **P = (4, 1)** **Q = (6, 6)** **P + Q = ?**

$s = ((y_P - y_Q) / (x_P - x_Q)) \bmod p$

$s = ((1 - 6) / (4 - 6)) \bmod 7 = ((-5) / (-2)) \bmod 7$

$= (5/2) \bmod 7 = (5 \cdot 2^{-1}) \bmod 7$

NR: Multiplikativinverse von 2 bestimmen

$(x \cdot 2) \bmod 7 = 1 \quad \Rightarrow \quad x = 4$

$s = (5 \cdot 4) \bmod 7 = 20 \bmod 7 = 6$

$\mathbf{x_R} = (6^2 - 4 - 6) \bmod 7 = 26 \bmod 7 = \mathbf{5}$

$\mathbf{y_R} = 6 \cdot (4 - 5) - 1 \bmod 7 = -6 - 1 \bmod 7 = -7 \bmod 7 = \mathbf{0}$

P + Q = (5, 0)

Addition von Punkten in Z_P (4)

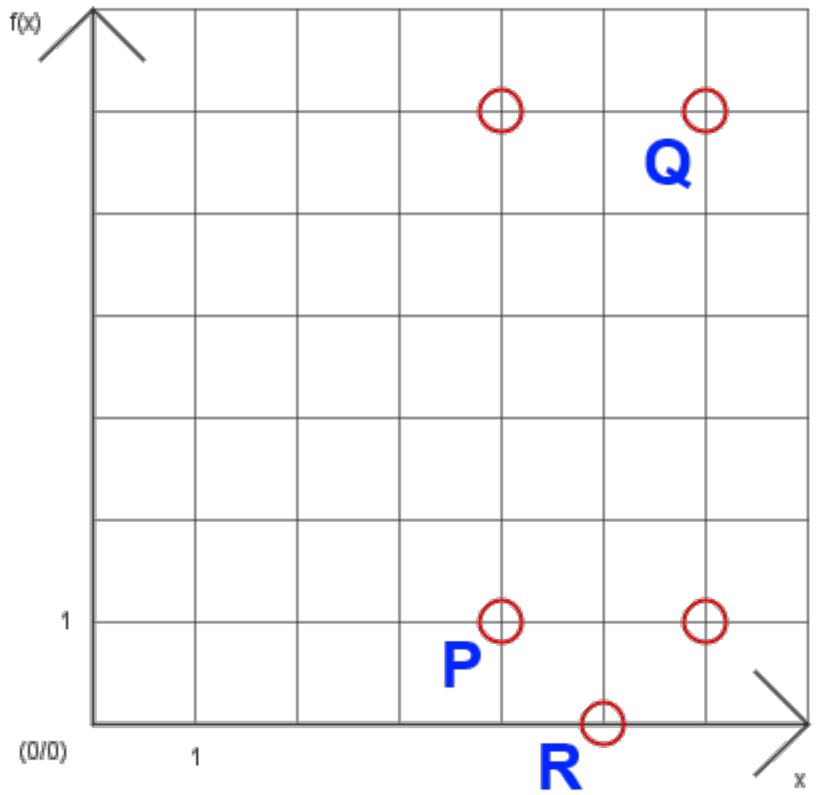
a = 1, b = 3, p = 7

P = (4,1)

Q = (6,6)

P + Q = R

R = (5, 0)



Skalare Multiplikation von Punkten in Z_P (1)

Multiplikation von c · P = mehrfache Addition

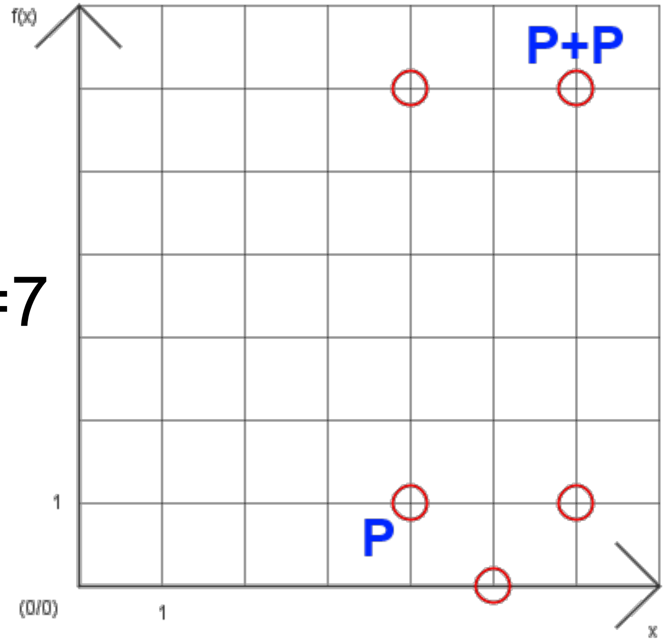
Beispiel:

P = (4, 1)

a = 1, b = 3, p =7

c = 3

P + P = (6, 6)



P + P

$s = ((3 \cdot x_P^2 + a) / (2 \cdot y_P)) \bmod p$

$x_R = (s^2 - x_P - x_P) \bmod p$

$y_R = s \cdot (x_P - x_P) - y_P \bmod p$

Berechnung:

$s = ((3 \cdot 4^2 + 2) * (2 \cdot 1)^{-1}) \bmod 7 = 0$

$\mathbf{x_R} = (0^2 - 4 - 4) \bmod 7 = -8 \bmod 7 = \mathbf{6}$

$\mathbf{y_R} = 0 \cdot (4 - 4) - 1 \bmod 7 = \mathbf{6}$

2P = P + P = (6, 6)

Skalare Multiplikation von Punkten in Z_P (2)

Multiplikation von c · P = mehrfache Addition

Beispiel:

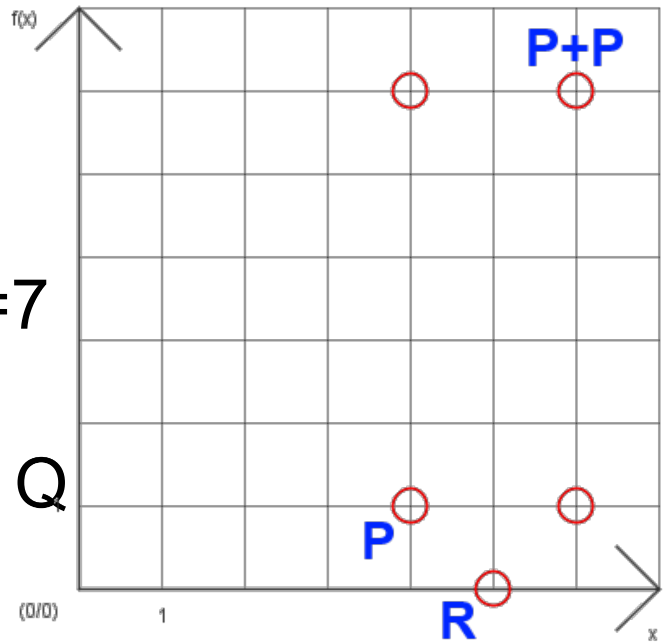
P = (4, 1)

a = 1, b = 3, p =7

c = 3

P + P = (6, 6) = Q

P + Q = (5, 0)



P + Q

$s = ((y_P - y_Q) / (x_P - x_Q)) \bmod p$

$x_R = (s^2 - x_P - x_Q) \bmod p$

$y_R = s \cdot (x_P - x_R) - y_P \bmod p$

Berechnung:

$s = ((1 - 6) * (4 - 6)^{-1}) \bmod 7 = 6$

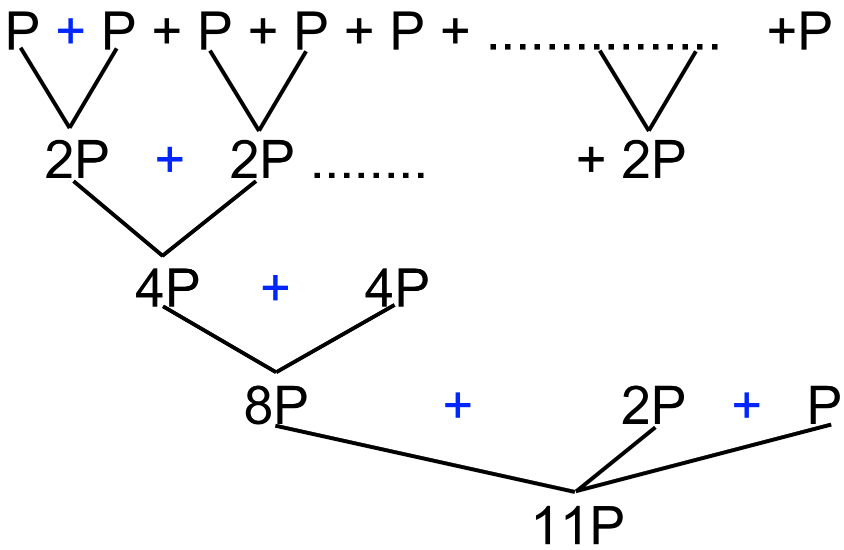
$\mathbf{x_R} = (6^2 - 4 - 6) \bmod 7 = 26 \bmod 7 = \mathbf{5}$

$\mathbf{y_R} = 6 \cdot (4 - 5) - 1 \bmod 7 = \mathbf{0}$

3 · P = P + Q = (5, 0)

Skalare Multiplikation von Punkten in Z_P (3)

- Double and Add Methode

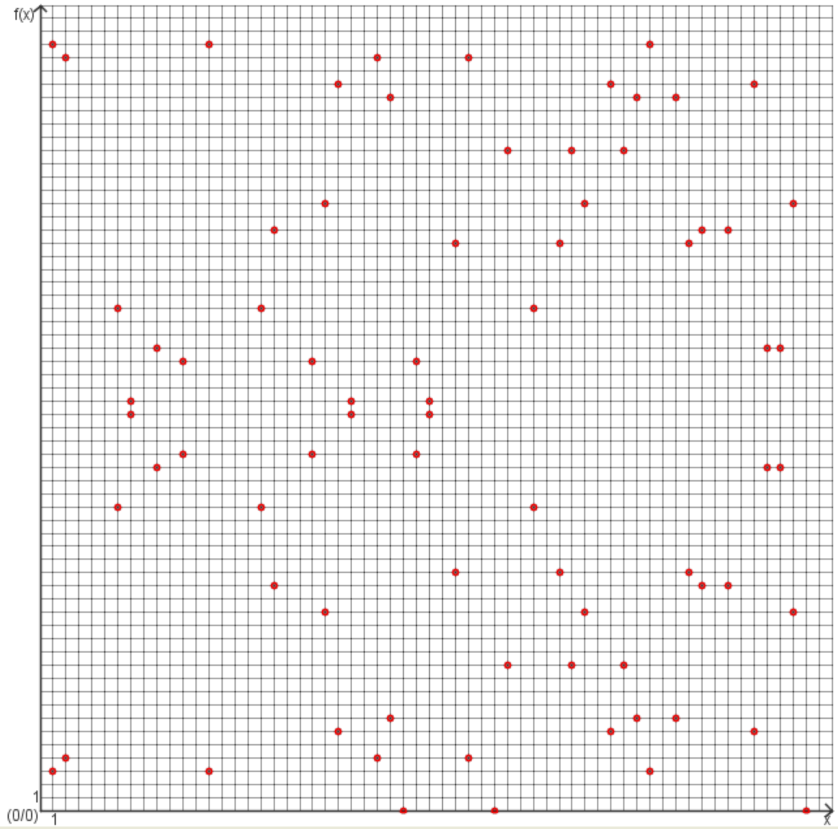


- Für c = 11 sind 5 Gruppenoperationen nötig
- Aufwand: im Mittel (3/2) $\log_2(c)$ Gruppenoperationen

Quellen:
• DOPATKA, Frank. *Ausarbeitung zu dem Thema Elliptische Kurven in der Kryptologie*, 2003, URL: www.frankdopatka.de/studium/koeln/mathe.pdf (Aufruf 2013-05-25)
• MEIER, Willi; STAFFELBACH, Othmar. Kryptographie und elliptische Kurven. *Elemente der Mathematik*, 1997, 52. Jg., Nr. 4, S. 137-151.
• MÜHLENFELD, Björn. *Einführung in Elliptische Kurven*. Ausarbeitung im Rahmen des Proseminars Public-Key Kryptographie, Universität Paderborn, 2006-01-10, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Muehlenfeld_Ausarbeitung.pdf (Aufruf 2013-05-27).

Warum ist es wichtig, zu wissen, wie viele Punkte eine Kurve hat?

- je mehr Punkte, desto unvorhersehbarer sieht das Ergebnis der Addition aus und somit auch das Ergebnis der skalaren Multiplikation
- die Wahrscheinlichkeit sinkt durch Zufall herauszufinden welche Punkte bei der Addition verwendet wurden



Anzahl der Punkte (Ordnung) einer elliptischen Kurve über Z_P (1)

- Satz von Hasse

  $p + 1 - 2 \cdot \sqrt{p} \leq |\#E(Z_P)| \leq p + 1 + 2 \cdot \sqrt{p}$

  $7 + 1 - 2 \cdot \sqrt{7} \leq |\#E(Z_P)| \leq 7 + 1 + 2 \cdot \sqrt{7}$

  $2{,}7 \leq |6| \leq 13{,}3$ **(Sichtbare Punkte + neutr. Element)**

- p = 762.821

  $761.075 \leq |\#E(Z_P)| \leq 764.569$ Δ3.494

- p = 8.999.051

  $8.993.052 \leq |\#E(Z_P)| \leq 9.005.052$ Δ12.000

Quellen:
• GRÜßIEN, Berit. *Einführung: Elliptische Kurven in der Kryptologie*, Seminar "Moderne Kryptosysteme", 2006-10-15, URL: www.ki.informatik.hu-berlin.de/algorithmenII/Lehre/ss06/modern_krypt/EllipstischeKurven.pdf (Aufruf 2013-05-25).
• KREITZ, Christoph. *Einheit 5.4: Elliptische Kurven*, Vorlesung Kryptographie und Komplexität, Universität Potsdam, 2009, URL: www.cs.uni-potsdam.de/ti/lehre/09ws-Kryptographie/slides/slides-5.4.pdf (Aufruf 2013-05-27).

Anzahl der Punkte (Ordnung) einer elliptischen Kurve über Z_P (2)

- Explizites Punktezählen mit Hilfe des Legendre-Symbols (s. folgende Folie)
- nur für kleine Primzahlen (p < 1000)
- Aufwand: O(p ln p)

$$\#E = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right)_L$$

Quelle:
- STIBOR, Thomas; ECKERT, Claudia. *Kapitel 11 Eliptische Kurven*, Vorlesung Kryptographie, Präsentation, Technische Universität München, 2009-06-24, URL: www.sec.in.tum.de/assets/lehre/ss09/kryptographie/Kapitel.11.pdf (Aufruf 2013-05-27).

Das Legendre-Symbol

- Für alle v aus Z_P gilt:
  v ist ein Quadrat in Z_P gdw. $v^{(p-1)/2}$ mod p = 1

$$\left(\frac{\mathbf{v}}{p}\right) = \begin{cases} 1 & \text{wenn } \mathbf{v} \text{ ein Quadrat in } Z_p, \\ -1 & \text{wenn } \mathbf{v} \text{ kein Quadrat in } Z_p, \text{ und} \\ 0 & \text{wenn } \mathbf{v} \equiv 0 \bmod p \text{ ist.} \end{cases}$$

Quelle:
• Wikipedia. *Legendre-Symbol*, 2013-04-03, URL: de.wikipedia.org/wiki/Legendre-Symbol (Aufruf 2013-05-27).

Anzahl der Punkte (Ordnung) einer elliptischen Kurve über Z_P (3)

- Schoofs Algorithmus
  - effizient (benötigt polynomielle Zeit)
  - Idee:
    - Ordnung mod p für viele kleine Primzahlen p berechnen
    - Über Chinesischen Restsatz auf #E schließen

Quelle:
• Wikipedia. *Schoof's algorithm*, 2013-03-15, URL: en.wikipedia.org/wiki/Schoof's_algorithm (Aufruf 2013-05-27).

Elliptische Kurven über Z_{2^m}

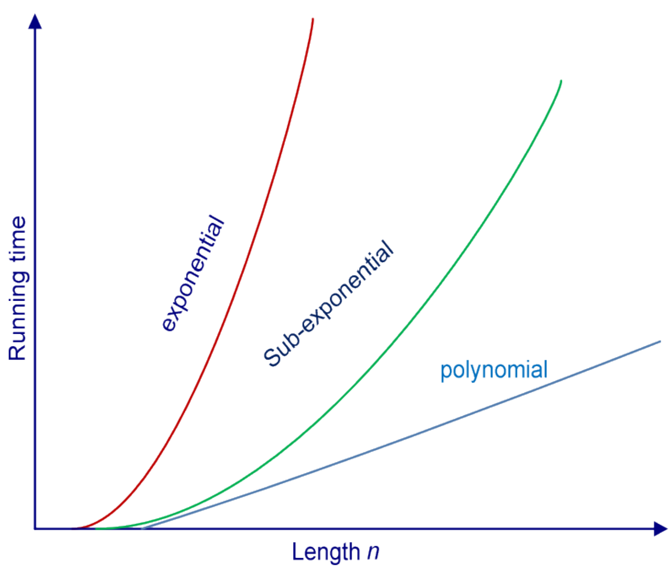
Zur Optimierung der Rechenoperationen am Computer, gibt es den effizienteren Körper Z_{2^m}.

Hier wird die Arithmetik entsprechend angepasst und arbeitet mit den XOR-Funktionen.

- Z_P hat Vorteile beim Softwareeinsatz
- Z_{2^m} hat Vorteile beim Hardwareeinsatz

Quellen:
• KREITZ, Christoph. *Einheit 5.4: Elliptische Kurven*, Vorlesung Kryptographie und Komplexität, Universität Potsdam, 2009, URL: www.cs.uni-potsdam.de/ti/lehre/09ws-Kryptographie/slides/slides-5.4.pdf (Aufruf 2013-05-27).
• GREBE, Ingo. *Elliptische Kurven in der Kryptographie*, Seminar Kryptographie und Datensicherheit, Präsentation, Universität Potsdam, 2005-07-07, URL: www.cs.uni-potsdam.de/ti/lehre/05-Kryptographie/slides/Elliptische_Kurven.pdf (Abruf 2013-05-26).

Zusammenfassung / Überblick



- Mathematik hinter EC ist recht komplex (im vgl. zu RSA / DH)

- Vergleich Kryptographie auf EC mit RSA & DH nötig
- Schwierigkeit bei der Verwendung (Patente)
- Einsatz von ECC

Quellen:
• LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).
• NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
• GRUßIEN, Berit. *Einführung: Elliptische Kurven in der Kryptologie*, Seminar "Moderne Kryptosysteme", 2006-10-15, URL: www.ki.informatik.hu-berlin.de/algorithmenII/Lehre/ss06/modern_krypt/ElliptischeKurven.pdf (Aufruf 2013-05-25).

Literatur (1)

- BORMANN, Carsten; SOHR, Karsten. *IT-Sicherheit: Kryptographie - Asymmetrische Kryptographie*, Vorlesung Informationssicherheit, 2012-11-26.
- Wikipedia. *RSA Factoring Challenge*, 2013-04-04, URL: de.wikipedia.org/wiki/RSA_Factoring_Challenge (Aufruf 2013-05-25)
- KLEINJUNG, Thorsten, et al. Factorization of a 768-bit RSA modulus. In: *Advances in Cryptology–CRYPTO 2010*. Springer Berlin Heidelberg, 2010. S. 333-350.
- MEIER, Willi; STAFFELBACH, Othmar. Kryptographie und elliptische Kurven. *Elemente der Mathematik*, 1997, 52. Jg., Nr. 4, S. 137-151.
- Wikipedia. *Komplexitätstheorie*, 2013-04-27, URL: de.wikipedia.org/wiki/Komplexitätstheorie (Aufruf 2013-05-24).
- LIU, Fuwen. *A tutorial of elliptic curve cryptography (ECC)*, 2010, URL: www-rnks.informatik.tu-cottbus.de/de/node/1131 (Aufruf 2013-05-24).
- NILLIES, Frank. *Kryptographie auf elliptischen Kurven am Beispiel von ElGamal und Menezes-Vanstone*, Proseminar Public-Key Kryptographie, 2006, URL: www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Nillies_Ausarbeitung.pdf (Aufruf 2013-05-25).
- LEMMERMEYER, Franz. *Elliptische Kurven I*. 1999, URL: http://www.zum.de/Faecher/Materialien/rubin/texte/elliptic_curve.pdf (Aufruf 2013-05-27).
- SCHWEIZER, Patrick. *Berechnung elliptischer und hyperelliptischer Kurven für paarungsbasierte Kryptografie*, Diplomarbeit, Institut für Mathematik, Technische Universität Berlin, 2008, URL: www.math.tu-berlin.de/~kant/publications/diplom/schweitzer.pdf (Aufruf 2013-05-27).
- MÜHLENFELD, Björn. *Einführung in Elliptische Kurven*. Ausarbeitung im Rahmen des Proseminars Public-Key Kryptographie, Universität Paderborn, 2006-01-10, URL: http://www2.cs.uni-paderborn.de/cs/ag-bloemer/lehre/proseminar_WS2005/material/Muehlenfeld_Ausarbeitung.pdf (Aufruf 2013-05-27).
- STIBOR, Thomas; ECKERT, Claudia. *Kapitel 11 Eliptische Kurven*, Vorlesung Kryptographie, Präsentation, Technische Universität München, 2009-06-24, URL: www.sec.in.tum.de/assets/lehre/ss09/kryptographie/Kapitel.11.pdf (Aufruf 2013-05-27).

Literatur (2)

- MENEZES, Alfred J.; VANSTONE, Scott A. Elliptic curve cryptosystems and their implementation. *Journal of Cryptology*, 1993, 6. Jg., Nr. 4, S. 209-224.
- KÖHLER, Günter; GREINER, Richard. *Elliptische Kurven in der Kryptographie*, Skript, Projekttage Mathematik 2002, 2002, URL: www.mathematik.uni-wuerzburg.de/~greiner/Download/MathSpiel/PT2002-ellku-scr.pdf (Aufruf 2013-05-25).
- BRIEDEMANN, M.; BUSCH, A.;HEIER, M.; HÜBNER, S.; KRAUS, S.; ZÜRN, A.; KÖHLER, G.; GREINER, R.; HEUBECK, B. *Elliptische Kurven in der Kryptographie*, Arbeitsbericht der Arbeitsgruppe, Projekttage 2002, 2002, URL: www.mathematik.uni-wuerzburg.de/~greiner/Download/MathSpiel/PT2002-ellku-abr.pdf (Aufruf 2013-05-25).
- GRUßIEN, Berit. *Einführung: Elliptische Kurven in der Kryptologie*, Seminar "Moderne Kryptosysteme", 2006-10-15, URL: www.ki.informatik.hu-berlin.de/algorithmenII/Lehre/ss06/modern_krypt/ElliptischeKurven.pdf (Aufruf 2013-05-25).
- DEMYTKO, N. A new elliptic curve based analogue of RSA. In: *Advances in Cryptology—EUROCRYPT'93*. Springer Berlin Heidelberg, 1994. S. 40-49.
- DOPATKA, Frank. *Ausarbeitung zu dem Thema Elliptische Kurven in der Kryptologie*, 2003, URL: www. frankdopatka.de/studium/koeln/mathe.pdf (Aufruf 2013-05-25).
- KREITZ, Christoph. *Einheit 5.4: Elliptische Kurven*, Vorlesung Kryptographie und Komplexität, Universitär Potsdam, 2009, URL: www.cs.uni-potsdam.de/ti/lehre/09ws-Kryptographie/slides/slides-5.4.pdf (Aufruf 2013-05-27).
- GREBE, Ingo. *Elliptische Kurven in der Kryptographie*, Seminar Kryptographie und Datensicherheit, Präsentation, Universität Potsdam, 2005-07-07, URL: www.cs.uni-potsdam.de/ti/lehre/05-Kryptographie/slides/Elliptische_Kurven. pdf (Abruf 2013-05-26).
- Wikipedia. *Legendre-Symbol*, 2013-04-03, URL: de.wikipedia.org/wiki/Legendre-Symbol (Aufruf 2013-05-27).
- Wikipedia. *Schoof's algorithm*, 2013-03-15, URL: en.wikipedia.org/wiki/Schoof's_algorithm (Aufruf 2013-05-27).