technische universität
dortmund

Vorlesung (WS 2014/15)

Sicherheit: Fragen und Lösungsansätze

Dr. Thomas P. Ruhroth

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Agenda und Ziele

- Genutzte math. Schreibweisen
- Algebraische Strukturen
- Elliptische Kurven
- Zufallszahlen
- Komplexitätsklassen

- Genutzte Schreibweisen zuordnen und nutzen können.
- Gruppen, Ringe und elliptische Kurven verstanden und nutzen können.
- Die Hierarchie der Komplexitätsklassen kennen

Einfach Notationen

- Grundlagen, die bekannt sind
- Notationen für die VL festlegen
  - Häufig verschieden verwendet
  - Ist die 0 (Null) in den natürlichen Zahlen?

Schreibweisen

- Schreibweise von Mengen:
  - M = { a ∈ A | zusätzliche Bedingungen }
  - „M ist die Menge aller a, die ein Element von A sind, und die alle Bedingungen erfüllen“
- Schreibweise von Quantoren:
  - ∀ … = „Für alle“ …
  - ∃ … = „Es existiert“ …
- Schreibweise von Funktionen:
  - f: M → N, mit f(x)=y
  - „f ist eine Abbildung (Funktion) von der Menge M in die Menge N, wobei jedes x ∈ M wie angegeben auf ein y ∈ N abgebildet wird.“
  - M heißt dann Definitionsmenge, N Werte- oder Zielmenge

Eigenschaften von Funktionen

- Injektiv:

  Jedes Element der Wertemenge wird höchstens einmal als Funktionswert eines Elementes der Definitionsmenge angenommen.
  $\forall\ x1,x2 \in A:\ f(x1) = f(x2) \Rightarrow x1 = x2$

- Surjektiv:

  Jedes Element der Wertemenge wird mindestens einmal als Funktionswert eines Elementes der Definitionsmenge angenommen.
  $\forall\ y \in A: \exists\ x \in B:\ f(x) = y$

- Bijektiv:

  Jedes Element der Wertemenge wird genau einmal als Funktionswert eines Elementes der Definitionsmenge angenommen.
  Oder: Die Funktion ist injektiv und surjektiv.

- Invertierbar:

  Wenn $f : A \rightarrow B$ eine bijektive Funktion ist, so existiert eine Funktion $f^{-1} : B \rightarrow A$ sodass $f^{-1}(f(x)) = x\ \forall\ x \in A$

- Logarithmus
  - $\log_b(x)=y \Leftrightarrow x = b^y$
  - Lässt man b weg, so ist in der Informatik der binäre Logarithmus gemeint, das heißt die inverse Abbildung zu 2^y.
- Matrixmultiplikation:
  - Abbildung $R^{m\times n} \times R^{n\times l} \rightarrow R^{m\times l}$
  - Beispiel:

$$c_{22}=a_{21}\cdot b_{12}+ a_{22}\cdot b_{22}+ \ldots + a_{2n}\cdot b_{n2}$$

$$\underline{A\cdot B=C}$$

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & & \ddots & \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1l} \\ b_{21} & b_{22} & \ldots & b_{2l} \\ \vdots & & \ddots & \\ b_{n1} & b_{n2} & \ldots & b_{nl} \end{pmatrix} = \begin{pmatrix} \ldots & \ldots & \ldots & \ldots \\ \ldots & c_{22} & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix}$$

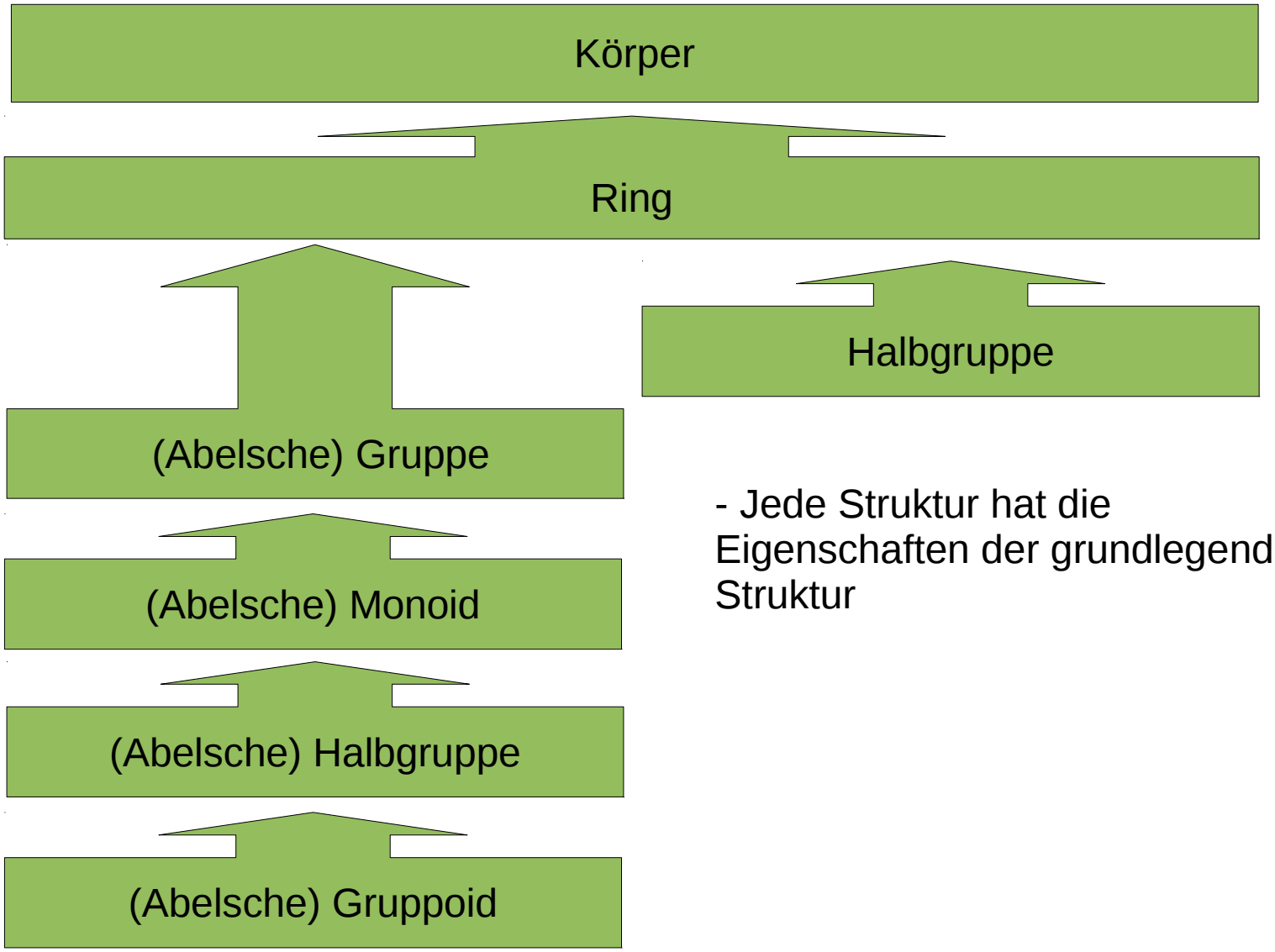
- Berechnung des grösten gemeinsamen Teilers ggT nach Euklid:

[...] Wenn CD nicht Teiler von AB ist, subtrahiert man, von den beiden Zahlen AB und CD ausgehend, immer die kleinere von der größeren bis die entstandene Zahl Teiler der ihr vorhergehenden ist, der dann der größte gemeinsame Teiler von AB und CD ist. [...]

Nach Euklid, Die Elemente, Buch VII, Proposition 2
http://www.opera-platonis.de/euklid/eb7/eb703.htm

Algebraische Strukturen

Algebraische Strukturen



- Jede Struktur hat die Eigenschaften der grundlegenden Struktur

Gruppe

Eine Gruppe $(G,*)$ ist eine Menge G mit einer darauf definierten Verknüpfung $* : G \times G \to G$, für die die folgenden Axiome gelten:

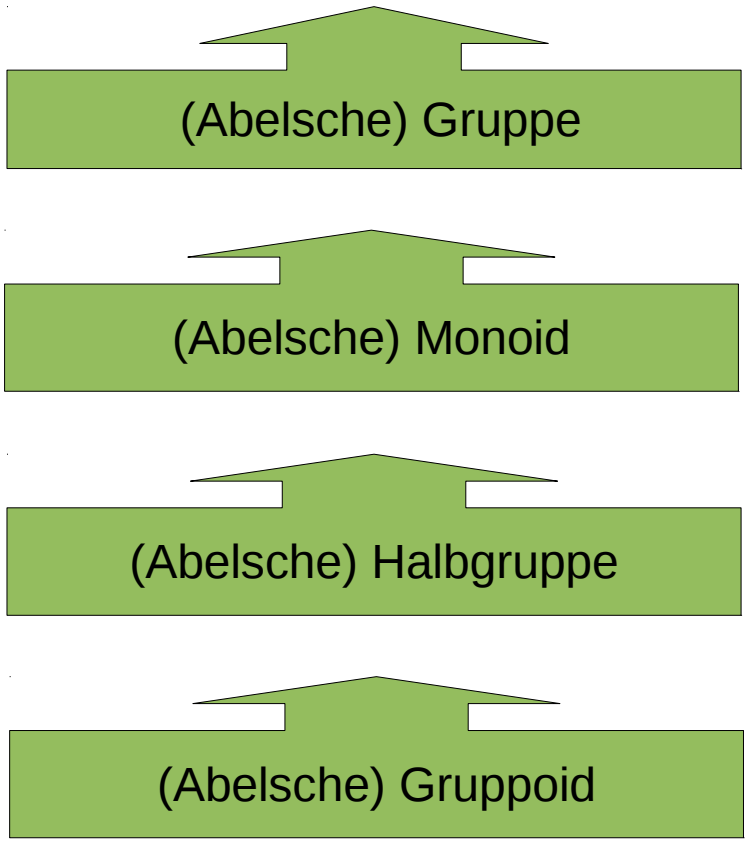
- $\forall\, a,b,c \in G$ gilt: $(a * b) * c = a * (b * c)$ — Assoziativität
- $\exists\, e \in G$ sodass $\forall\, a \in G$ gilt: $a * e = e * a = a$ — Neutrales Element
- $\forall\, a \in G\ \exists\, a^{-1} \in G$ sodass: $a * a^{-1} = a^{-1} * a = e$ — Inverses Element

Erfüllt eine Gruppe noch das Axiom

- $\forall\, a,b \in G$ gilt: $a * b = b * a$
  Kommutativ

so nennt man sie kommutative oder Abelsche Gruppe.

Algebraische Strukturen



+ inverses Element

+ neutrales Element

+ Assoziativität

Binäre Struktur (G,*)

Ring

Ein Ring $(R,+,*)$ ist eine Menge R mit zwei darauf definierten Verknüpfungen $+ : R \times R \to R$ und $* : R \times R \to R$, für die die folgenden Axiome gelten:

- $(R,+)$ ist eine abelsche Gruppe
- $(R,*)$ ist eine Halbgruppe
- $\forall$ a,b,c $\in$ R gilt: Distributivgesetz
  - $a * (b + c) = a * b + a * c$
  - $(a + b) * c = a * c + b * c$

Man bezeichnet dabei das neutrale Element von $(R,+)$ als Nullelement 0.

Ring II

Falls $(R,*)$ kommutativ ist, bezeichnet man den Ring als kommutativ, falls $(R,*)$ ein neutrales Element 1 besitzt, so bezeichnet man den Ring als unitär.

Falls für ein Element $a \in R$ ein kleinstes n existiert mit $a^n=1$, so hat a die Ordnung n.

Restklassenring

- Wähle natürliche Zahl n größer 1.
- Dividiere die ganzen Zahlen jeweils durch n, betrachte den Rest.
- Fasse die ganzen Zahlen nun zu Äquivalenzklassen bezüglich des Restes zusammen.

Diese Restklassen bilden nun mit den folgenden Verknüpfungen einen Ring, den Restklassen- oder Moduloring Z/nZ, „Z modulo n“

- $+ : Z/nZ \times Z/nZ \rightarrow Z/nZ$ mit $\forall$ a,b $\in$ Z/nZ: $[a]_n + [b]_n = [a+b]_n$
- $* : Z/nZ \times Z/nZ \rightarrow Z/nZ$ mit $\forall$ a,b $\in$ Z/nZ: $[a]_n * [b]_n = [a*b]_n$

Üblicherweise nutzt man als Vertreter der Restklassen die Zahlen 0,1,...,n-1; in diesem Fall lässt man die eckigen Klammern weg.

Beispiel: Restklassenring Z/5Z

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

∗	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Offensichtlich ist 0 das neutrale Element der Addition, 1 das der Multiplikation.

Andere Eigenschaften lassen sich nicht ganz so leicht ablesen, so hat zum Beispiel das Element 3 die Ordnung 4, wegen $3 * 3 = 4$, $3^2 * 3 = 2$, $3^3 * 3 = 1$.

Auch gilt zum Beispiel $2^{-1}=3$, denn $1/2=x \Rightarrow 1=2x \Rightarrow x=3$.

Körper

Ein Körper $(K,+,*)$ ist ein Ring,
bei dem $(K\backslash\{0\},*)$ eine abelsche Gruppe ist.
Ist die einem Körper zugrundeliegende Menge endlich,
so bezeichnet man ihn als Galoisfeld.

Klasse = Ring + neutrales Element $*$ + inverses Element $*$

Vektorraum

Ein Vektorraum $(V,\oplus,\cdot)$ über einem Körper $(K,+,*)$

ist eine Menge, für die $(V,\oplus)$ eine abelsche Gruppe ist,

und die Verknüpfung $\cdot : K \times V \to V$ die folgenden Eigenschaften erfüllt:

$\forall\ \alpha,\beta \in K$, $\forall\ u,v \in V$, 1 Einselement von K

- $(\alpha \cdot (\beta \cdot u) = (\alpha * \beta) \cdot u$
- $\alpha \cdot (u \oplus v) = \alpha \cdot u \oplus \alpha \cdot v$
- $(\alpha + \beta) \cdot u = \alpha \cdot u \oplus \beta \cdot u$
- $1 \cdot u = u \cdot 1 = u$

Man nennt dann $\cdot$ Skalarmultiplikation, die Elemente von V Vektoren, und die Elemente von K Skalare.

Irreduzible Elemente

- Ein Element eines Ringes R (und damit eines Körpers, Vektorraumes...) heißt Einheit, falls es innerhalb dieses Ringes ein Teiler der 1 ist.
- Jedes Element des Ringes, das weder eine Einheit ist, noch sich als Produkt zweier beliebiger Nichteinheiten darstellen lässt, heißt irreduzibel.

Primelemente

- Falls ein Element p $\in$ R keine Einheit ist, die 0 keine Einheit ist, und für beliebige a,b $\in$ R gilt, das aus *„p teilt a∗b“* folgt *„p teilt a“* oder *„p teilt b“*, so ist p ein Primelement.
  - In einem Körper sind alle Elemente, die nicht die 0 sind, Einheiten, es existieren also keine Primelemente.
- Ist der Ring R nullteilerfrei, kommutativ und unitär (und auch nicht der Nullring), so sind Primelemente irreduzibel, besitzt auch noch jedes Element eine eindeutige Zerlegung in irreduzible Elemente, so sind diese mit den Primelementen identisch.

Primzahlen

- Eine Primzahl ist ein Primelement des Ringes der ganzen Zahlen.
- Betrachtet werden meist nur positive Primzahlen, also jene, die Teil der natürlichen Zahlen sind.
- Es lässt sich jede natürliche Zahl eindeutig als ein Produkt aus Primzahlen darstellen, die sogenannte Primfaktorzerlegung.
  - Nützlich ist dies vorallem bei der Berechnung des ggT, oder bei der Bruchrechnung
  - Es ist kein effizientes Verfahren bekannt, mithilfe dessen sich eine Zahl in ihre Primfaktoren zerlegen lässt.

Primzahlsuche

- Es existieren verschiedene Verfahren, um Primzahlen vorauszusagen:
  - Euler nutze die Formeln n^2+n+17 und n^2-n+41. Diese liefern für n<16 bzw. für n<41 immer Primzahlen.
  - Euklid wiederum summierte alle schon bekannten Primzahlen, und addierte 1.
  - Sehr beliebt ist gerade für große Zahlen auch $M_n=2^n-1$, die sogenannte Mersenne-Zahl. Zusätzlich lässt sich relativ effizient testen, ob das Ergebnis tatsächlich eine Primzahl ist.
- Es ist zu beachten, das diese und alle anderen bekannten Formeln im Allgemeinen keine Primzahl berechnen, lediglich ist die Wahrscheinlichkeit viel höher, als beispielsweise bei einer zufallsbasierten Suche.

Primzahltest

Überprüfe, ob es sich bei einer gegeben Zahl n um eine Primzahl handelt:

- Primitiv: Teste für alle Zahlen von 2 bis n, ob n sich teilen lässt. Sehr ineffizient.
- Deshalb werden oft Algorithmen eingesetzt, die nur mit einer gewissen Wahrscheinlichkeit korrekt arbeiten, dafür aber effizienter.
- Gerade für große Zahlen sehr effektiv: Miller-Rabin

Miller-Rabin

- Berechne d,j sodass $2^j d = n-1$ und d ungerade.
- Berechne für beliebiges a, $1<a<n$, die Folge $(a^d, a^{2d}, a^{4d}, \ldots, a^{2^{j-1}d}, a^{2^j d})$, jeweils modulo n
- Ist n eine Primzahl, so endet die Folge garantiert auf 1. Man kann dies sogar schon beim ersten Auftauchen einer 1 oder -1 vorhersehen, da in Folge nur quadriert wird.
- Ist n keine Primzahl, so ist es relativ unwahrscheinlich $\left(< \frac{1}{4} \right)$, dass die Folge auf 1 endet.
- Durch wiederholtes Anwenden mit anderen Werten für a kann diese Wahrscheinlichkeit noch verringert werden.

Polynome

- Ein Polynom, oder auch eine Polynomfunktion besteht aus einer Menge von Koeffizienten a_i und wird dargestellt als:

$$P(x)=\sum_{i=0}^{n} a_i x^i = a_n x^n + \dots a_2 x^2 + a_1 x + a_0$$

- Dabei bestimmt der Größte vorkommende Exponent n den Grad des Polynoms. Voraussetzung ist, das a_n nicht null ist. Man bezeichnet a_n dann als Leitkoeffizient.
- Die Multiplikation von Polynomen verläuft nach folgendem Schema:

$$P(x)=\sum_{i=0}^{n} a_i x^i \, , Q(x)=\sum_{i=0}^{m} b_i x^i$$

$$P(x)\cdot Q(x)=\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{m+n} c_i x^i$$

$$mit\ c_i = \sum_{j\ +\ i=k} a_j b_i$$

Polynomdivision

Die Division von Polynomen ist etwas anspruchsvoller als die Multiplikation:

- Gegeben sind Polynome *P* und *Q*, wobei *P* vom gleichem oder höheren Grad als *Q* ist.
- Gesucht werden Polynome *S* und *R*, sodass *P=SQ+R* gilt, und *R* von kleinerem Grad als *Q* ist.
- Beispiel mit $P(x)=-3x^6+2x^5-3x4-2x3+4x2+2x+4$, $Q(x)=x^3+x+2$:

$$
\begin{array}{rrrrrrrrrrrrrrrrr}
(- & 3x^6 & + & 2x^5 & - & 3x^4 & - & 2x^3 & + & 4x^2 & + & 2x & + & 4) & :(x^3+x+2)=-3x^3+2x^2+2 \\
- & 3x^6 & & & - & 3x^4 & - & 6x^3 & & & & & & & \\
\hline
 & & & 2x^5 & & & + & 4x^3 & + & 4x^2 & + & 4x & + & 4 & \quad Rest:\ 2x \\
 & & & 2x^5 & & & + & 2x^3 & + & 4x^2 & & & & & \\
\hline
 & & & & & & & 2x^3 & & & + & 4x & + & 4 & \\
 & & & & & & & 2x^3 & & & + & 2x & + & 4 & \\
\hline
 & & & & & & & & & & & 2x & & &
\end{array}
$$

Beispiel: GF(2^8)

- GF(2^8) bezeichnet das Galoisfeld der Polynome von maximal siebten Grad, die als Koeffizienten nur 0 und 1 besitzen.
- Deshalb werden diese Polynome meist als achtstellige Folge von 0 und 1 dargestellt, welche dann entweder als Binär- oder als Hexadezimalzahl interpretiert wird.
- Ein einzelnes Polynom lässt sich so als ein Byte speichern.

$A(x) = x^5 + x^4 + x^3 + 1$

00111001

0x39

Addition und Multiplikation in GF(2^8)

Addition:

$C(x) = A(x) + B(x) = c_7x^7 + c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$ mit

$c_i = a_i + b_i \; mod \; 2 = a_i \; XOR \; b_i$

Multiplikation

$C(x) = A(x) * B(x) = (A(x) \cdot B(x))\%P(x)$ mit einem irreduziblen Polynom P(x) vom Grad 8, später in der Vorlesung verwendet:

$P(x) = x^8 + x^4 + x^3 + x + 1$

Hierbei sei $\cdot$ die Polynommultiplikation, % die Modulorechnung.

- Für inverse Elemente in GF(2^8) gilt:

  $A^{-1}(x) * A(x) = 1 \bmod P(x)$ mit P(x) irreduzibel wie oben.
- Ein Beispiel für ein Polynom P = 9
  - $(09)_{16} = (00001001)_2 \Rightarrow P(x) = x^3 + 1$
  - $P + 7 = (00001001)_2$ XOR $(00000111)_2 = (00001110)_2 = (0E)_{16}$
  - $P * 3 = (x^3 + 1) * (x + 1) = (x^4 + x^3 + x + 1) \% (x^8 + x^4 + x^3 + x + 1)$

    $= x^4 + x^3 + x + 1 = (00011011)_2 = (1B)_{16} = 27$

Funktionen im Körper bzw. Vectorraum

- Eine Abbildung $f : V \to V'$ zwischen den Vektorräumen V,V' heißt linear, wenn die Reihenfolge von der Anwendung der Abbildung und einer Verknüpfung auf V bzw. der passenden Verknüpfung auf V' keinen Unterschied macht:

  $\forall\ \alpha,\beta \in K, \forall\ u,v \in V$ gilt

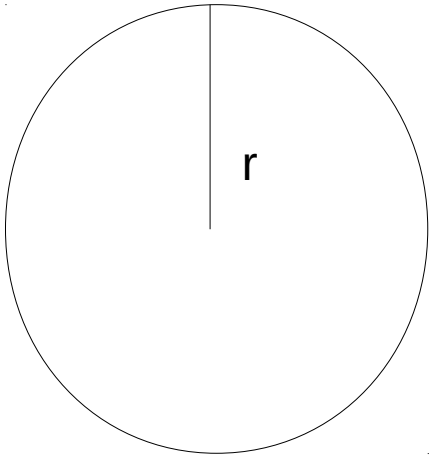
  $f(\alpha \cdot u \oplus \beta \cdot v) = \alpha \cdot f(u) \oplus \beta \cdot f(v)$

- Eine Abbildung $f : V \to V$ heißt selbstinvers, wenn sie zugleich ihre eigene inverse Abbildung ist, wenn also $f \circ f = id$ ist, wobei id die Identität ist, die jedes Element auf sich selbst abbildet. Insbesondere ist eine selbstinverse Abbildung immer bijektiv, und sie bildet einen Körper in sich selbst ab.

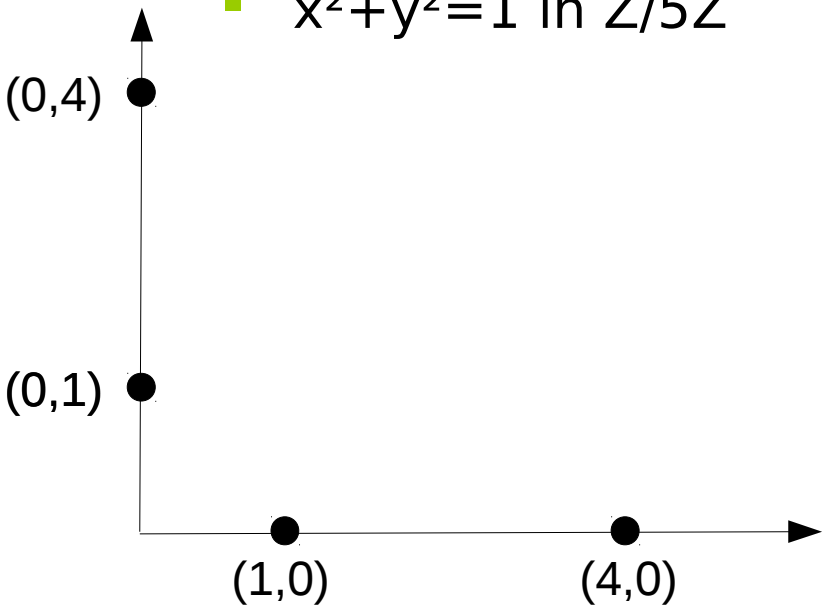
Elliptische Kurven

Algebraische Kurven

- $x^2+y^2=r$ in R^2

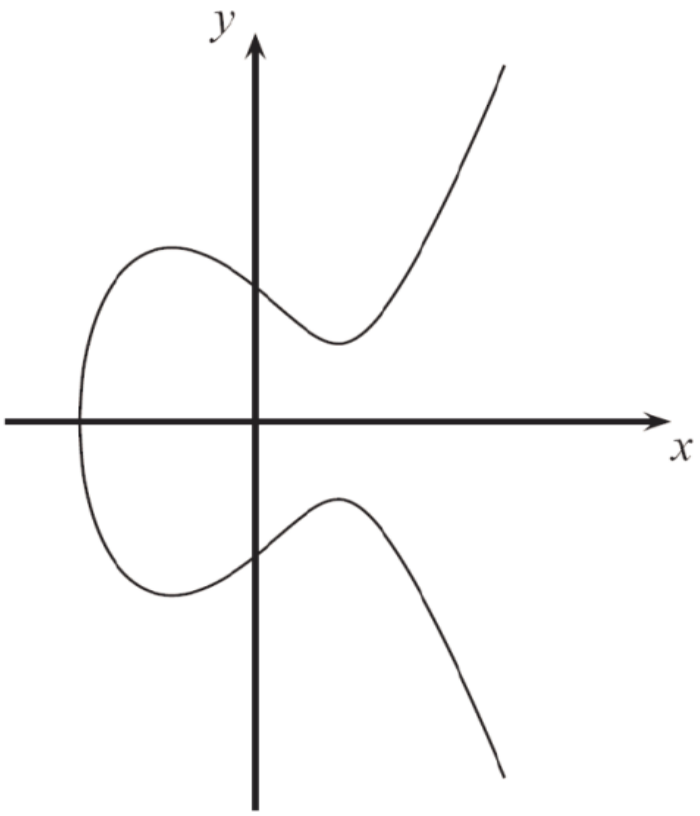


- $x^2+y^2=1$ in $Z/5Z$



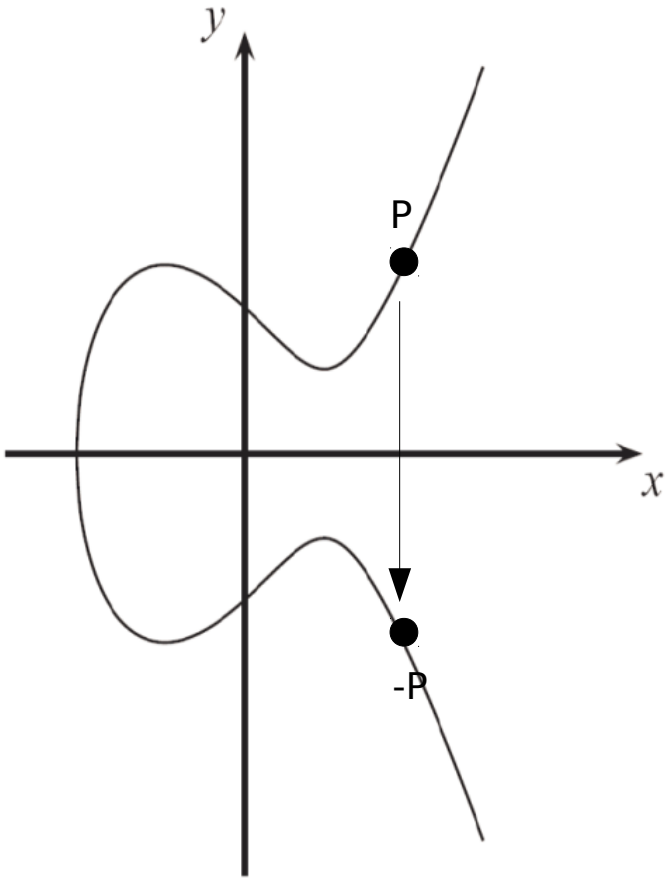
Definition: Elliptische Kurve

Die Elliptische Kurve über Z/pZ, p>3,
ist die Menge von allen Paaren $(x,y) \in Z/pZ$ mit
$y^2 = x^3 + ax + b \bmod p$
Zusammen mit einem imaginären Punkt O
in der Unendlichkeit, wobei
$a,b \in Z/pZ$ und $4a^3+27b^2 \neq 0 \bmod p$ gilt.



Beispiel in R^2: $y^2 = x^3 - 3x + 3$

Inverses Element



Das inverse Element zu

P=(x,y)

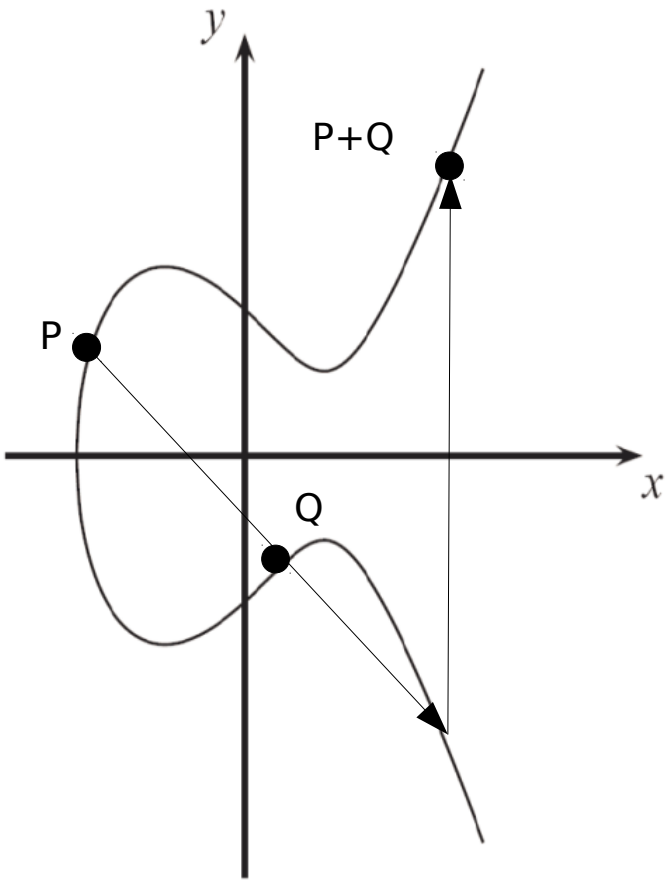
ist aufgrund der x-Achsen-Symmetrie einer elliptischen Kurve

-P=(x,-y).

Wichtig:

Jede Operation in einer elliptischen Kurve bleibt in der Kurve!

Addition $P \neq -Q$ und $P \neq Q$



- $P \neq -Q$ und $P \neq Q$
- Die Addition führt immer in die Kurve
- Addition funktioniert auch, falls die Kurve nicht zusammenhängt
- Wenn $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ nicht invers zueinander und nicht gleich sind sind, gilt

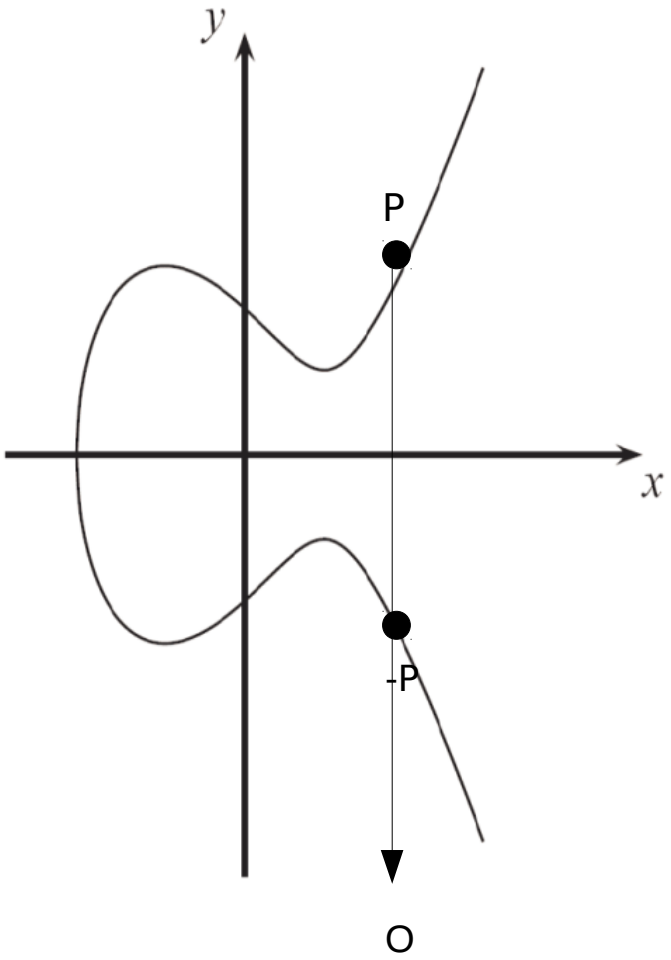
  $P + Q = R$ mit

  $s = (y_P - y_Q) / (x_P - x_Q)$

  $x_R = s^2 - x_P - x_Q$ und

  $y_R = -y_P + s(x_P - x_R)$

Addition P = – Q

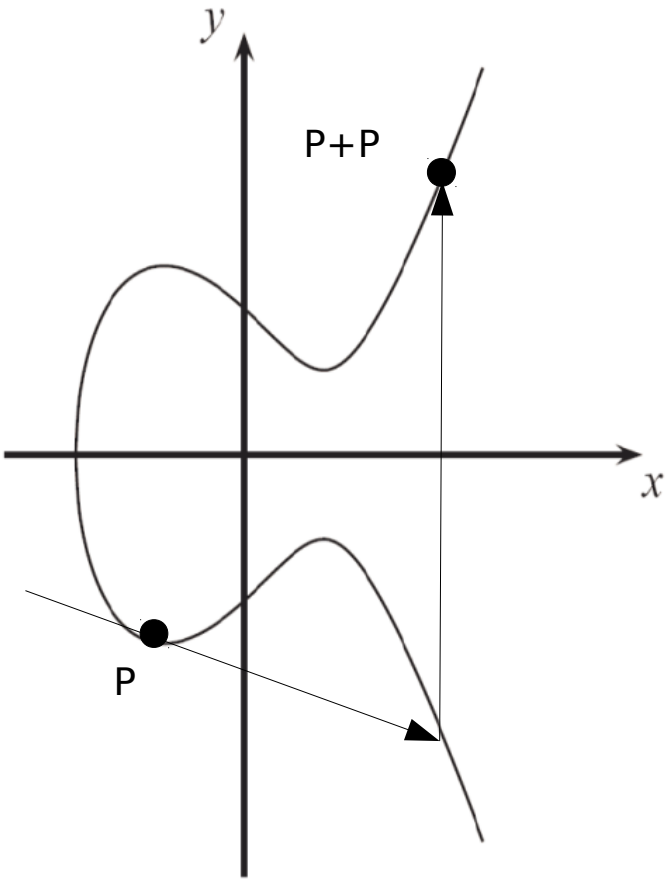


- P + (-P) = O

  (O war der imaginäre Punkt im Unendlichen)
- O ist damit das neutrale Element der Addition:

  P + O = P

P+P oder 2P



- P+P wird mit der Tangente berechnet
- Es wird kurz nP für
  P+P+ ... +P (n-mal)
  geschrieben

Wenn y_P nicht 0 ist, gilt

2P = R mit

$s = (3 x_P^2 + a) / (2y_P)$

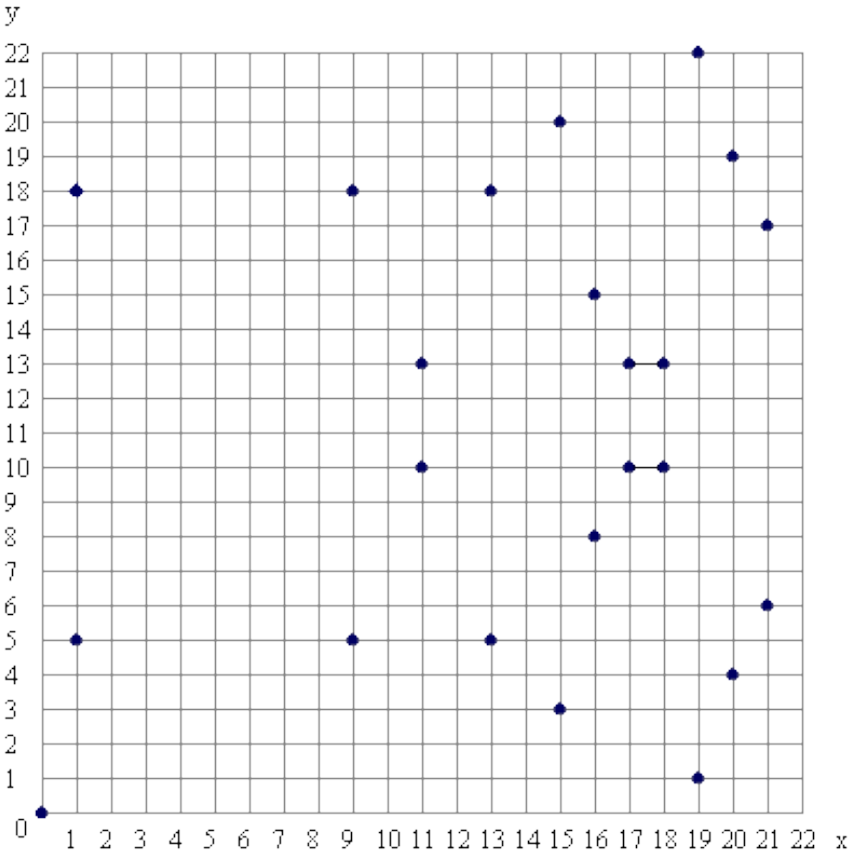
$x_R = s^2 - 2x_P$

$y_R = -y_P + s(x_P - x_R)$

Abelsche Gruppe

- Elliptische kurven bilden mit der Addition eine abelsche Gruppe:
- $\forall$ P,Q,R $\in$ EC gilt: (P + Q) + P = P + (Q + R)
  Assoziativität
- $\exists$ P $\in$ EC sodass $\forall$ P $\in$ EC gilt: P + O = O + P = P
  Neutrales Element
- $\forall$ P $\in$ EC $\exists$ -P $\in$ EC sodass: P + (-P) = (-P) $*$ P = O
- $\forall$ P,Q $\in$ EC: P + Q = Q + P

$y^2 = x^3 + x$ über Z/23Z



Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

- $y^2 = x^3 + x$ über Z/23Z

  EC= { (0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5) (13,18) (15,3) (15,20) (16,8) (16,15) (17,10) (17,13) (18,10) (18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17) }

Das Diskrete Logarithmus Problem

- Sind ein Punkt P und ein Skalar n gegeben, so lässt sich der Punkt

  T = nP leicht berechnen.
- Sind dagegen die Punkte P und T gegeben, so ist das verwendete Skalar n nicht effizient zu berechnen.
- Somit ist die so entstandene Abbildung s(P , n) = (P , nP) eine Einwegfunktion, also eine Funktion, die in Polynomialzeit berechenbar ist, deren Inverse aber entweder nicht bekannt ist, oder für die alle bekannten Inversen nur sehr ineffizient sind.

Zufallszahlen

Zufallszahlen

- Echte Zufallszahlen sind technisch sehr aufwändig zu bestimmen:
  - Strahlung einer radioaktiven Quelle
  - Atmosphärisches Rauschen
- Daher werden in der Kryptographie sogenannte Pseudozufallszahlen verwendet, also Zahlen(-folgen), die zufällig wirken, in Wirklichkeit aber deterministisch bestimmt sind.
  - Mit dem gleichen Startwert (Seed) kann die Zahlenfolge beliebig reproduziert werden.
  - Es existieren verschiedene Gütekriterien für die Zufälligkeit einer Folge.
- Damit die Kryptographie einen Pseudozufallszahlengenerator akzeptiert, muss dieser gewisse Kriterien erfüllen, die Wichtigsten sind:
  - ein Beobachter kann die Zahlenfolge nicht als „nichtzufällig“ erkennen.
  - selbst wenn der Generator bekannt ist, sollte er ohne korrekten Seed nutzlos sein.

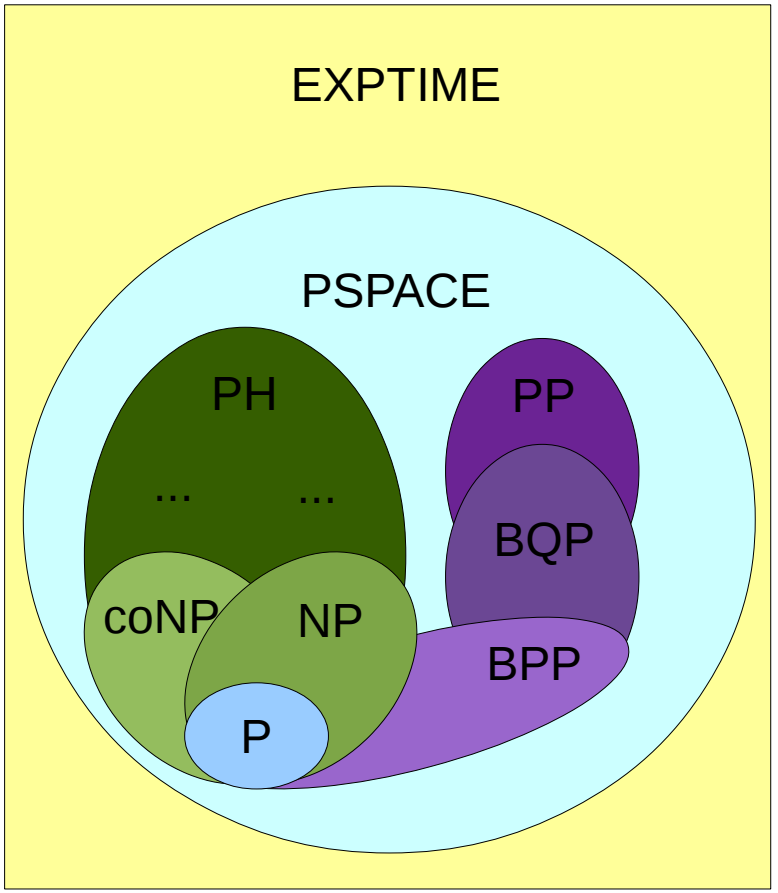
Komplexität

Effizienz

- Um die Effizienz eines Algorithmus zu bewerten, werden die Laufzeit oder der Speicherplatz im Verhältnis zur Länge der Eingabe betrachtet.
- Je nach Anwendung werden meist der Worst-Case oder der Average-Case betrachtet.
- In der Kryptographie ist es für ein effizient zu lösendes Problem wünschenswert, das ein Algorithmus mit höchstens polynomialer Laufzeit bekannt ist.
- Dagegen kann es für ein nicht effizient zu lösendes Problem verschiedene Anforderungen geben:
  - Er sollte keine Algorithmen geben, die in polynomialer Laufzeit das Ergebnis finden.
  - Es sollte keine Algorithmen geben, die in polynomialer Laufzeit ein Ergebnis finden, das mit hoher Wahrscheinlichkeit richtig ist.
  - Bestenfalls sollte es komplett unmöglich sein, für ein beliebiges Ergebnis zu bestimmen, ob es das richtige ist.

Wichtige Komplexitätsklassen

Klasse	Informelle Bedeutung
P	Probleme in polynomieller Zeit lösbar
NP	Lösungen in polynomieller Zeit bestätigbar
coNP	Lösungen in polynomieller Zeit widerlegbar
PH	enthält verschiedene Erweiterungen von P,NP,coNP
BPP	Probleme in polynomieller Zeit mit einer konstanten Fehlerwahrscheinlichkeit $<1/2$ lösbar
BQP	Wie BPP, aber nur auf Quantencomputern
PP	Probleme in polynomieller Zeit mit einer dynamischen Fehlerwahrscheinlichkeit $<1/2$ lösbar
PSPACE	Probleme mit maximal polynomiellem Speicherplatzbedarf lösbar
EXPTIME	Probleme in exponentieller Zeit lösbar



- Bei manchen dieser Komplexitätsklassen steht noch nicht sicher fest, ob sie nicht identisch sind.
- Es existieren noch weitere, schwierigere Komplexitätsklassen.

Nächste Woche:
Kryptographie