Algorithmische Zahlentheorie*

Seminararbeit im Masterstudiengang Angewandte Informatik
WS 2015/16 Hochschule Hannover †

Marius Rhode‡
Hochschule Hannover
Fakultät IV - Wirtschaft und Informatik
[TODO PLZ] Hannover
Marius.Rohde@stud.HS-Hannover.de

Marcel Reichenbach§
Hochschule Hannover
Fakultät IV - Wirtschaft und Informatik
30459 Hannover
Marcel.Reichenbach@stud.HS-Hannover.de

ZUSAMMENFASSUNG
Zusammenfassung ... [TODO]

1. EINLEITUNG
Einleitung ... [TODO]

2. GRUNDLAGEN
Grundlagen ... [TODO]

2.1 Algebraische Strukturen
In diesem Kapitel werden die algebraischen Strukturen: Halbgruppen, Gruppen, Ringe und Körper vorgestellt. Diese werden für ein späteres Kapitel benötigt. Die algebraischen Strukturen beschreiben ein abstraktes Rechnen mit Zahlen. Dies ermöglicht gezielter nur die Rechenregeln an sich zu untersuchen, unabhängig von der Rechengröße und der jeweiligen Operation. Ein Anwendungsbereich ist u. a. in der Kryptographie zu finden. [4]

2.1.1 Halbgruppen
Eine Halbgruppe ist eine Menge M mit einer assoziativen Operation $\circ$, geschrieben mit (M, $\circ$) oder einfach nur M. Zur Erinnerung, das Assoziativgesetz besagt: $(a \circ b) \circ c = a \circ (b \circ c)$ für alle a, b, c $\in$ M. Es gilt für sämtliche Elemente einer Halbgruppe. Das Zeichen $\circ$ ist Platzhalter für eine beliebige Operation. Der Wertebereich von $\circ$ ist eine Teilmenge von M so dass, $a \circ b \in M$ für alle a, b $\in$ M. Für das Zeichen $\circ$ werden auch die folgenden Operationszeichen verwendet: $*$, $\cdot$, $+$. Auch muss die Menge nicht zwangsläufig M sein. [1]

Durch das Assoziativgesetz können also Klammern weggelassen werden. Zum besseren Verständnis konkrete Beispiele von Halbgruppen [1]:

- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Halbgruppen mit der Addition als Operation, ebenso wie mit der Multiplikation.
- Wenn $a \circ b = |b - a|$ für alle a, b $\in \mathbb{Z}$, dann ist ($\mathbb{Z}$, $\circ$) keine Halbgruppe. Da in diesem Fall $(1 \circ 2) \circ 3 = 1 \circ 3 = 2$ ist, aber $1 \circ (2 \circ 3) = 1 \circ 1 = 0$ ist. Ein verändern der Klammerung ergibt unterschiedliche Ergebnisse, somit ist das Assoziativgesetz nicht mehr gewährleistet, wodurch $\mathbb{Z}$ in diesem Fall keine Halbgruppe mehr sein kann.

Sobald es ein neutrales Element in einer Halbgruppe gibt heißt dieses **Monoid**. Ein neutrales Element ist immer dann gegeben wenn es ein e $\in$ M gibt, sodass für alle a $\in$ M gilt: $a \circ e = e \circ a = a$. Dieses weitere Axiom muss von jeder Halbgruppe erfüllt werden um ein Monoid zu sein. Als Zeichen für ein Monoid wird neben e oft auch 1 verwendet, bei den Operationszeichen $\circ$, $\cdot$, $*$. Wird das $+$ als Operationszeichen verwendet ist oft 0 das neutrale Element. [1]

Wenn ein Monoid auch das folgende Axiom erfüllt, ist es eine **Gruppe**. Existiert für alle a $\in$ G ein b $\in$ G, sodass $a \circ b = b \circ a = e$ gilt, so heißt b invers zu a. [1]

2.1.2 Ringe
In einem Ring als Algebraische Struktur sind mehr als nur eine Operation vorhanden. Eine Menge R mit den zwei Operationen $+$ und $\cdot$ auf R ist genau dann ein Ring wenn folgenden drei Bedingungen gelten [1]:

- (R, $+$) ist eine abelsche Gruppe. (Eine Operation $\circ$ auf einer Menge M heiß kommutativ oder abelsch, wenn: $a \circ b = b \circ a$ für alle a, b $\in$ M gilt.)
- (R, $\cdot$) ist ein Monoid
- Für alle a, b, c $\in$ R gilt: $a(b + c) = ab + ac$, $(a + b)c = ac + bc$ (Distributivgesetze)

*Genau Betrachtungen der Problemlösenden Algorithmen für ... [TODO]

†ATM ka was man hier noch beschreiben könnte erstmal [TODO]

‡Marius Rhode ... [TODO]

§Marcel Reichenbach ... [TODO]

ACM ISBN 978-1-4503-2138-9…15.00
DOI: http://dx.doi.org/10.1145/1235

Zusätzlich heißt ein Ring kommutativ, wenn die Operation $\cdot$ kommutativ ist. Ein Ring besitzt also immer eine kommutative Addition und eine nicht notwendigerweise kommutative Multiplikation. Die beiden Distributivgesetze verbinden diese beiden Operationen miteinander. Ein Ring heißt nullteilerfrei wenn $a \cdot b = 0$ ist und dadurch impliziert wird, dass $a = 0$ oder $b = 0$ sein muss, für alle $a, b \in R$. Wenn es für ein $a \in R$ ein b gibt, so dass $ab = ba = 1$ gilt, dann ist a invertierbar oder eine Einheit. Alle Elemente im Monoid $(R, \cdot)$ wo dies zutrifft sind in einer multiplikativen Gruppe zusammengefasst, bezeichnet wird diese mit R^X. [1]

Es gibt spezielle Ringe, die sogenannten Körper. Ist eine Menge $(K, +, \cdot)$ ein Ring und ist $(K - 0, \cdot)$ eine kommutative Gruppe, heißt K ein Körper. Alle von Null verschiedenen Elementen sind Einheiten und es gilt: $K^X = K^* = K - 0$. [1]

3. PRIMZAHLEN

Primzahlen ... [TODO]

4. DISKRETER LOGARITHMUS

Diskreter Logarithmus ... [TODO]

4.1 Elliptischen Kurven Grundlagen

In diesem Kapitel sollen nur die Grundlagen von elliptischen Kurven näher gebracht werden, um so die **E**lliptic **C**urve **C**ryptography, kurz ECC, verstehen zu können. Der Vorteil beim ECC-Verfahren im Vergleich zum RSA-Verfahren, liegt darin das die Schlüssellänge deutlich kürze ausfallen kann ohne dabei an Sicherheit zu verlieren. Ein RSA-Schlüssel mit 1024 Bit ist etwa so sicher wie ein Schlüssel aus einer elliptischen Kurve mit gerade mal ca. 160 Bit. Dazu kommt das der Rechenaufwand und Speicherbedarf beim ECC-Verfahren wesentlich geringer ist als beim RSA-Verfahren. So kann ECC in Smartcards und Mobiltelefonen genutzt werden.[2]

Um die Funktionsweise der elliptischen Kurven in ihrer vollen Breite und Tiefe zu verstehen ist dafür eine sehr komplexe Mathematik notwendig. Innerhalb dieser Seminararbeit kann dieses Thema nicht Breiter und Tiefer durchleuchtet werden und es sei ihr auf die folgende Literatur verwiesen: [2] und [3].

Eine Elliptische Kurve ist eine ebene Kurve wie in Abbildung 1 gezeigt. Sie wird durch eine Gleichung der Form: $y^2 = x^3 + ax + b$ beschrieben. Damit ist eine Menge Z aller Punkte P(x, y) die auf der elliptischen Kurve liegen definiert. Wichtig dabei ist das die Kurvenparameter a und b so gewählt sind das die partiellen Ableitungen nach x und nach y auf keinem Punkt der Kurve gleichzeitig null sind, dazu später mehr.

Das Addieren von zwei Punkten, die auf der elliptischen Kurve liegen, ergibt wieder einen Punkt welcher ebenfalls auf der Kurve liegt.[2] Mit Addition ist das Verknüpfen von zwei Punkten gemeint, man könnte es auch als Multiplikation bezeichnen. In beiden fällen hat es nichts mit den bekannten Operationen auf Zahlen zu tun. Das Addieren von zwei Punkten ist vielmehr geometrisch definiert, siehe dazu auch Abbildung 1:

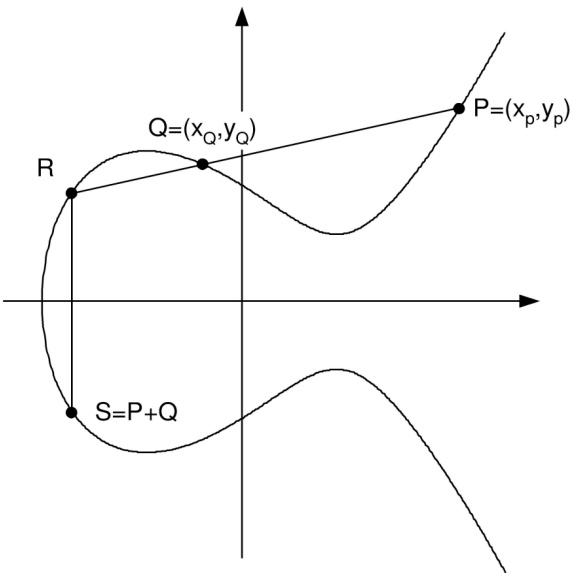

Abbildung 1: Addition von zwei Punkten auf einer elliptischen Kurve [2]

DEFINITION 1. *Durch die gegebenen Punkte P und Q wird eine Gerade gelegt, welche die Kurve in einem dritten Punkt R schneidet. Dieser wird anschließend an der x-Achse gespiegelt. Als Ergebnis erhält man den Punkt S, welcher als Addition von P und Q bezeichnet wird.[2]*

Die so definierte Addition ist kommutativ, zur Erinnerung: $P + Q = Q + P$. Nicht für alle elliptischen Kurven kann eine Addition von Punkten durchgeführt werden. Wie oben bereits erwähnt dürfen die partiellen Ableitungen nach x und nach y auf keinem Punkt der Kurve gleichzeitig null sein. Anders ausgedrückt die Kurve darf sich nicht selbst schneiden, ansonsten kann die Additionsoperation nicht für beliebige Punkte durchgeführt werden. Zusätzlich muss beachtet werden, dass bei einer Addition von zwei Punkten die nachfolgenden Spezialfälle auftreten können[2]:

- Wenn für die beiden zu Addierenden Punkten $Q = P$ gilt, wird die Tangente an der Kurve im Punkt P verwendet. Dabei entsteht der der Schnittpunkt mit der Kurve in R und durch Spiegelung resultiert daraus $S = P + P = 2P$.

- Sollten die X-Koordinaten beider zu addierender Punkte gleich sein, so dass ($Q_X = P_X$) gilt, entsteht eine vertikale Gerade und die Kurve wird kein weiteres mal geschnitten. Für diesen Fall wird die elliptische Kurve um einen weiteren Punkt ∞, welcher im Unendlichen liegt, ergänzt. Die Addition von Punk P mit ∞ ist so definiert das man wiederum P als Ergebnis erhält ($P + \infty = P$). Somit ist ∞ das neutral Element der Addition. Es gilt also: $P + Q = \infty$ wenn die x-Koordinaten von P und Q gleich sind. Daraus folgt das Q das inverse Element vo P ist und es gilt: $Q = -P$.

Das Addieren eines Punktes P mit einem Skalar k ∈ {1, 2, 3 ...} wird als wiederholte Addition definiert:

$$kP = P1 + P2 + ... + Pk$$

4.2 Asymmetrische Verschlüsselung mit Elliptischen Kurven

Um Elliptischen Kurven für Asymmetrische Verschlüsselung einsetzen zu können muss in einem endlichen Körper gerechnet werden um Rundungsfehler zu vermeiden. Bei der Addition und Multiplikation in endlichen Körpern sind diese so definiert, dass das Ergebnis immer wider ein Element des endlichem Körpers ist. Aufgrund dessen muss eine weitere Operation durchgeführt werden: *mod* $|Z|$. Dies stellt sicher das der resultierende Rest ist in jedem Fall wieder ein Element aus Z ist. Für die Addition besitzt jedes Element ein inverses Element -a, damit gilt für die Subtraktion: $b - a = b + (-a)$. Bei der Multiplikation ist das inverse Element a^{-1}, damit gilt für die Division: $b/a = b \cdot a^{-1}$. Für ein konkretes Beispiel sei an dieser Stelle auf S. 154 - 257 in [2] verwiesen.

Um elliptische Kurven für kryptologische Anwendungsfälle zu nutzen, muss die Ordnung eines Punktes der elliptischen Kurve berechnet werden.

DEFINITION 2. *Die Ordnung eines Punktes ist die Anzahl der Punkte, die durch fortwährender Addition dieses Punktes, erzeugt werden.[2]*

Dazu folgendes Beispiel:

$$P + P = 2P \Rightarrow 2P + P = 3P \Rightarrow ... \Rightarrow xP + P = (x + 1)P$$

P ist dabei immer ein Punkt auf der elliptischen Kurve. Irgendwann ist $x_i P = \infty$, somit kein Punkt mehr auf der Kurve, und damit hat der Punkt P die Ordnung x_i, im weiteren verlauf als n bezeichnet.

4.2.1 Schlüsselaustausch mit elliptischen Kurven

Zuerst muss der Körper bestimmt werden und eine elliptische Kurve, dazu wählt man ein große Primzahl und die Kurvenparameter a und b. Weiter wird nun ein Erzeugerpunkt G vereinbart, dabei soll die Ordnung des Punktes G möglichst groß und eine Primzahl sein. A wählt eine geheime ganze Zahl n_A welche kleiner sein muss als n und berechnet daraus den öffentlichen Schlüssel $P_A = n_A \cdot G$. Teilnehmer B mach das gleich jeweils mit n_B und P_B. P_A und P_B können nun über eine unsichere Leitung ausgeschaut werden. Nun kann Teilnehmer A den Schlüssel $K = n_A \cdot P_B$ berechnen. B berechnet ebenfalls K mit n_B und P_A. So habe dabei ein und das selbe geheime K berechnet.

Es folgt der Beweis das A und B wirklich das gleiche K berechnet haben müssen:

BEWEIS 1. *A berechnet $K = n_A \cdot P_B$. P_B wurde ursprünglich von Teilnehmer B berechnet mit $n_B \cdot G$. Dies kann in die Berechnung für K von A an stelle von P_B eingesetzt werden so das daraus folgt: $K = n_A \cdot P_B = n_A \cdot (n_B \cdot G)$. Das gleiche Prinzip angewendet für die Berechnung von K durch Teilnehmer B ergibt: $K = n_B \cdot P_A = n_B \cdot (n_A \cdot G)$. Unter Berücksichtigung des Assoziativgesetzes können diese beiden Gleichungen, gleich gesetzt werden:*

$$n_A \cdot (n_B \cdot G) = n_B \cdot (n_A \cdot G)$$

Asymmetrische Verschlüsselungsverfahren basieren auf Einwegfunktionen. Wobei es nicht allzu schwierig ist k · P zu Berechnen allerdings ist das Berechnen von k aus k · P und P sehr aufwendig. Anzumerken ist das diese aussage allerdings bis heute noch nicht bewiesen wurde.

5. FAZIT

Fazit ... [TODO]

6. REFERENCES

[1] O. Deiser and C. Lasser. *Erste Hilfe in Linearer Algebra.* Springer Spektrum, Berlin Heidelberg, 2015.

[2] M. Hufschmid. *Information und Kommunikation.* Teubner Verlag, Wiesbaden, 2006.

[3] S. Spitz, M. Pramateftakis, and J. Swoboda. *Kryptographie und IT-Sicherheit.* Vieweg + Teubner Verlag and Springer Fachmedien, Wiesbaden, 2011.

[4] P. D. F. Sprengel. Kryptographie und algorithmen. Technical report, Hochschule Hannover, 2012.

7. ANHANG

Anhang ... [TODO]