

# **Seminarvortrag Modulare Arithmetik**

Hendrik Annuth

8289

# Inhaltsverzeichnis

1.	<b>Definition einer algebraischen Struktur</b> .....	3
1.1	Die ganzen Zahlen.....	3
1.2	Restklassen.....	3
2.	<b>Operationen in dieser algebraischen Struktur</b> .....	7
2.1.	Potenzieren.....	7
2.1.1	Beispiele.....	7
2.1.2	Kleiner Satz von Fermat.....	8
2.2.	Radizieren.....	9
2.2.1	Beispiele.....	9
2.2.1	Struktur.....	9
2.3.	Logarithmieren.....	11
2.2.1	Beispiele.....	11
2.2.1	Struktur.....	12

3.	<b>Praktische Anwendungen dieser Operationen im Bereich der Kryptographie</b> .....	13
3.1.	Authentifizierung.....	13
3.1.1	Das Dilemma der Authentifizierung.....	13
3.1.2	Schritte der Authentifizierung.....	13
3.1.3	Fiat-Shamir-Protokoll.....	14
3.2.	Schlüsselaustausch.....	15
3.2.1	Das Problem des Schlüsselaustausches.....	15
3.2.2	Diffie-Hellman-Schlüsselaustausch.....	15
4.	<b>Quellenangaben</b> .....	16
5.	<b>Vertiefendes Material</b> .....	17
5.1	RSA-Kryptosysteme.....	17
5.2	Primzahlen.....	17
5.3	Quantencomputer.....	17

# 1. Definition einer algebraischen Struktur

In diesem Kapitel geht es um das Verständnis des Restklassenkörpers. Es soll gezeigt werden, dass eine Vielzahl von Möglichkeiten in ihm bestehen, die uns der gewöhnliche Zahlenraum  $\mathbb{Z}$  so nicht bietet. Hier wird auch eine einfache Einführung in die Rechnung im Bereich der Restklassen gegeben.

## 1.1 Die ganzen Zahlen

Eine einfache Gleichung wie

$$X \cdot 5 = 10$$

ist im Bereich der ganzen Zahlen bereits nicht mehr durch eine Operation lösbar. Um die Gleichung zu lösen, bedürfte es einer Invertierung der Operation „ $\cdot 2$ “, d.h. einer Zahl, die mit 2 multipliziert 1 ergibt. Die 1 ist neutrales Element der Multiplikation. So wäre nach Multiplikation mit 1 unser  $x$  in dieser Gleichung unverändert.

## 1.2 Restklassen

Für eine freiere Bewegung im Zahlenraum der algebraischen Struktur, wird nun eine Restklassenmenge gewählt, da diese einen zyklischen Charakter hat, kann im Zahlenraum wieder zurückgekehrt werden, ohne dabei den Bereich der ganzen Zahlen verlassen zu müssen.

Die bekannteste Restklassenmenge ist die Uhr. Die Uhrzeiten der späteren Stunden des Tages bilden zwölf Äquivalenzklassen.

$$\mathbb{Z}_{12} = \{ [0]_{12}; [1]_{12}; [2]_{12}; [3]_{12}; [4]_{12}; [5]_{12}; [6]_{12}; [7]_{12}; [8]_{12}; [9]_{12}; [10]_{12}; [11]_{12} \}$$

So bezeichnen die Uhrzeiten 0, 12 und 24 Uhr die gleiche Uhrzeit, die Zahlen sind in einer Äquivalenzklasse und bilden ein Element der Restklassenmenge.

Hier ein paar Rechenbeispiele zur Restklassenarithmetik:

$$|\mathbb{Z}_{12}| = 12$$

$$\mathbb{Z}_{12} = \{[0]_{12}; [1]_{12}; [2]_{12}; [3]_{12}; [4]_{12}; [5]_{12}; [6]_{12}; [7]_{12}; [8]_{12}; [9]_{12}; [10]_{12}; [11]_{12}\}$$

$$[0]_{12} = \{\dots; -24; -12; 0; 12; 24; \dots\}$$

$$[8]_{12} = \{\dots; -16; -4; 8; 20; 32; \dots\}$$

$$[8]_{12} + [11]_{12} = [7]_{12}, \text{ denn } 8 + 11 = 19 = 12 \cdot 1 + \underline{7} \Rightarrow 19 \in [7]_{12}$$

$$[4]_{12} \cdot [8]_{12} = [8]_{12}, \text{ denn } 4 \cdot 8 = 32 = 12 \cdot 2 + \underline{8} \Rightarrow 32 \in [8]_{12}$$

Nun wird versucht, in dieser Restklassenmenge unsere Gleichung zu lösen:

$$[2]_{12} \cdot [x]_{12} = [10]_{12}$$

Wie bereits beschrieben, wird dafür nach dem Element gesucht, dass die Operation „ $\cdot$ “ invertiert:

$$[2]_{12} \cdot [0]_{12} = [0]_{12}$$

$$[2]_{12} \cdot [1]_{12} = [2]_{12}$$

$$[2]_{12} \cdot [2]_{12} = [4]_{12}$$

$$[2]_{12} \cdot [3]_{12} = [6]_{12}$$

$$[2]_{12} \cdot [4]_{12} = [8]_{12}$$

$$[2]_{12} \cdot [5]_{12} = [10]_{12}$$

$$[2]_{12} \cdot [6]_{12} = [0]_{12}$$

$$[2]_{12} \cdot [7]_{12} = [2]_{12}$$

$$[2]_{12} \cdot [8]_{12} = [4]_{12}$$

$$[2]_{12} \cdot [9]_{12} = [6]_{12}$$

$$[2]_{12} \cdot [10]_{12} = [8]_{12}$$

$$[2]_{12} \cdot [11]_{12} = [10]_{12}$$

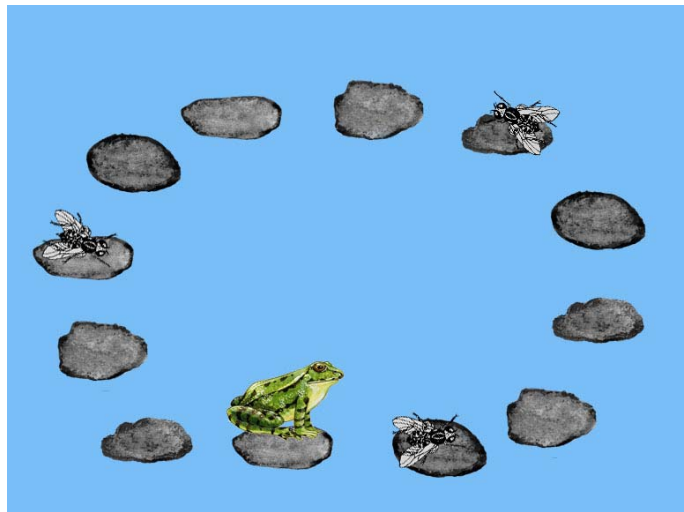
Das Element existiert nicht, jedoch sind zwei Lösungen erkennbar. Diese durch Probieren herausgefundenen Lösungen sind allerdings unbefriedigend, denn die Gleichung

$$[2]_{12} \cdot [x]_{12} = [7]_{12}$$

kann so nicht gelöst werden, da die Operation innerhalb dieser Restklassenmenge nicht wirklich invertierbar ist.

Wo liegen nun die Ursachen für dieses Problem?

Sei folgendes Beispiel gegeben: In einem Teich befinden sich zwölf Steine. Auf einem sitzt ein Frosch, auf anderen befinden sich Fliegen, die der Frosch gerne fressen möchte. Hat unser Frosch eine Sprungweite von zwei Steinen, so gelingt es ihm nie, die Fliegen zu fangen, da er nie auf die ungeraden Steine gelangt. Der ggT von 2 und 12 ist nämlich 2.



Eine triviale Lösung für das Problem wäre es, dem Frosch eine Sprungweite von 1 zu geben, denn so würde er nacheinander alle

Steine erreichen. Dies hilft aber für die Definition der algebraischen Struktur nicht weiter, da auch andere Zahlen als 1 gebraucht werden. Ist die Sprungweite des Frosches 7, so erreicht er auch alle Steine, da der ggT von 7 und 12 auch 1 ist. Wird für die Restklassenmenge als Basis nun eine Primzahl gewählt, sind logischerweise alle kleineren Zahlen, also die Elemente dieser Restklassenmenge, teilerfremd zu der Basis und der Frosch gelangt in der Struktur mit jeder Sprungweite auf alle Steine.

Zur Betrachtung dieser Tatsache wird nun die Primzahl 7 als Basis der Restklassenmenge gewählt.

Beispiel  $\mathbb{Z}_p$ ,  $p=7$

$(\mathbb{Z}_7, +)$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$(\mathbb{Z}_7, *)$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Nun ist es möglich, die anfangs gestellte Gleichung durch eine Operation zu lösen, da nun das inverse Element zu 2 bekannt ist.

$$2 * x \equiv 10 \pmod{7}$$

$$a \equiv 2 \pmod{7}$$

$$a^{-1} \equiv 4 \pmod{7}$$

Nun kann man dieses Element in die Gleichung einsetzen.

$$2 * x \equiv 10 \pmod{7} \quad | *4$$

$$4 * 2 * x \equiv 4 * 10 \pmod{7}$$

$$1 * x \equiv 40 \equiv 5 * 7 + \underline{\underline{5}} \pmod{7}$$

Bei der so definierten algebraischen Struktur handelt es sich um einen Körper, in dem, wie gezeigt, eine Vielzahl an Möglichkeiten besteht, die der Bereich der ganzen Zahlen nicht bietet.

Die modulare Arithmetik arbeitet in dieser algebraischen Struktur.

Die beschriebenen Körper, auch Galoisfelder genannt, gehen auf den französischen Mathematiker Galois (1811-1832) zurück.

## 2. Operationen in dieser algebraischen Struktur

In diesem Kapitel sollen Operationen betrachtet werden, die in den in Kapitel 1 beschriebenen Körpern möglich sind. Es wird hier das Potenzieren, das Radizieren insbesondere in Hinblick auf Quadratwurzeln und das Logarithmieren betrachtet.

### 2.1. Potenzieren

#### 2.1.1 Beispiele

Berechnung von Potenzen am Beispiel von  $\mathbb{Z}_7$ :

$$5^1 \equiv 5$$

$$5^2 \equiv 25 \equiv 3 \cdot 7 + \underline{4}$$

$$5^3 \equiv 5^2 \cdot 5 \equiv 4 \cdot 5 \equiv 20 \equiv 2 \cdot 7 + \underline{6}$$

$$5^4 \equiv 5^3 \cdot 5 \equiv 6 \cdot 5 \equiv 30 \equiv 4 \cdot 7 + \underline{2}$$

$$5^5 \equiv 5^4 \cdot 5 \equiv 2 \cdot 5 \equiv 10 \equiv 7 + \underline{3}$$

$$5^6 \equiv 5^5 \cdot 5 \equiv 3 \cdot 5 \equiv 15 \equiv 2 \cdot 7 + \underline{1}$$

Betrachtet man die Potenzen von  $\mathbb{Z}_7$ , so fällt dabei einiges auf:

$1^1 \equiv 1$	$2^1 \equiv 2$	$3^1 \equiv 3$	$4^1 \equiv 4$	$5^1 \equiv 5$	$6^1 \equiv 6$
$1^2 \equiv 1$	$2^2 \equiv 4$	$3^2 \equiv 2$	$4^2 \equiv 2$	$5^2 \equiv 4$	$6^2 \equiv 1$
$1^3 \equiv 1$	$2^3 \equiv 1$	$3^3 \equiv 6$	$4^3 \equiv 1$	$5^3 \equiv 6$	$6^3 \equiv 6$
$1^4 \equiv 1$	$2^4 \equiv 2$	$3^4 \equiv 4$	$4^4 \equiv 4$	$5^4 \equiv 2$	$6^4 \equiv 1$
$1^5 \equiv 1$	$2^5 \equiv 4$	$3^5 \equiv 5$	$4^5 \equiv 2$	$5^5 \equiv 3$	$6^5 \equiv 6$
$1^6 \equiv 1$	$2^6 \equiv 1$	$3^6 \equiv 1$	$4^6 \equiv 1$	$5^6 \equiv 1$	$6^6 \equiv 1$

Innerhalb der Potenzen von 2 und 1 ist feststellbar, dass nicht mehr alle Elemente der Restklassenmenge erreicht werden können.

Die Potenzen von 3 und 5 erreichen jedoch jedes Element und werden daher als „erzeugende Elemente“ bezeichnet.

Die Potenz  $(p-1)$ , also  $7-1=6$ , ergibt für alle Elemente der Restklassenmenge 1. Dies soll genauer untersucht werden.

## 2.1.2 Kleiner Satz von Fermat

$$x^{(p-1)} \equiv 1 \pmod{p}$$

$p$  sei eine Primzahl.

Beweis durch Induktion:

1.  $x^{(p-1)} \equiv 1 \pmod{p} \mid *x$

Behauptung:  $x^p \equiv x \pmod{p}$

2. Verankerung:  $x$  sei 0  $0^p \equiv 0 \pmod{p}$

3. Zu zeigen:  $(x+1)^p \equiv x+1$

$$(x+1)^p \equiv x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \dots + \binom{p}{p-1}x^1 + 1 \pmod{p}$$

$$\binom{p}{k} = \frac{p!}{(p-k)!*k!} = \frac{p*(p-1)*...*(p-k)}{k*(k-1)*...1}$$

$$(x+1)^p \equiv x^p + p * \left( \frac{(p-1)!}{(p-1)!*1!}x^{p-1} + \frac{(p-1)!}{(p-2)!*2!}x^{p-2} + \dots + \frac{(p-1)!}{1!*(p-1)!}x^1 \right) + 1 \pmod{p}$$

Da eine mit  $p$  multiplizierte Zahl immer durch  $p$  teilbar ist, entfällt der gesamte mittlere Term.

$$(x+1)^p \equiv x^p + 1 \pmod{p} \wedge x^p \equiv x \pmod{p} \Rightarrow \underline{\underline{(x+1)^p \equiv x+1 \pmod{p}}}$$

q.e.d.

## 2.2 Radizieren

Auch innerhalb von Restklassen können Wurzel gezogen werden. Diese Abbildung hat bestimmte Charakteristiken, auf die in diesem Kapitel eingegangen wird.

### 2.2.1 Beispiele

Quadratwurzeln am Beispiel von  $\mathbb{Z}_7$ :

$$\begin{aligned}\sqrt{4} &\equiv 2 \pmod{7} \quad \wedge \quad \sqrt{4} \equiv (7-2) \equiv 5 \pmod{7} \\ 5^2 &= 25 = 3 \cdot 7 + \underline{4} \\ -2 &\in [5]_7\end{aligned}$$

Dieses zweite Ergebnis erklärt die Gleichung.

$$x^2 \equiv (x-p)^2 \equiv x^2 - 2xp + p^2 \equiv x^2 - p(x-p) \equiv x^2 \pmod{p}$$

$$\sqrt{1} \equiv \{1;6\}; \sqrt{2} \equiv \{3;4\}; \sqrt{3} \equiv ?; \sqrt{4} \equiv \{2;5\}; \sqrt{5} \equiv ?; \sqrt{6} \equiv ? \pmod{7}$$

### 2.2.2 Struktur

Eine wichtige Frage ist: Wann treten modulare Quadratwurzeln auf?

$1^1 \equiv 1$	$2^1 \equiv 2$	$3^1 \equiv 3$	$4^1 \equiv 4$	$5^1 \equiv 5$	$6^1 \equiv 6$
$1^2 \equiv 1$	$2^2 \equiv 4$	$3^2 \equiv 2$	$4^2 \equiv 2$	$5^2 \equiv 4$	$6^2 \equiv 1$
$1^3 \equiv 1$	$2^3 \equiv 1$	$3^3 \equiv 6$	$4^3 \equiv 1$	$5^3 \equiv 6$	$6^3 \equiv 6$
$1^4 \equiv 1$	$2^4 \equiv 2$	$3^4 \equiv 4$	$4^4 \equiv 4$	$5^4 \equiv 2$	$6^4 \equiv 1$
$1^5 \equiv 1$	$2^5 \equiv 4$	$3^5 \equiv 5$	$4^5 \equiv 2$	$5^5 \equiv 3$	$6^5 \equiv 6$
$1^6 \equiv 1$	$2^6 \equiv 1$	$3^6 \equiv 1$	$4^6 \equiv 1$	$5^6 \equiv 1$	$6^6 \equiv 1$

$$a^{(p-1)/2} \equiv (p-1) \pmod{p} \Rightarrow a \text{ hat keine modulare Quadratwurzel}$$

$$a^{(p-1)/2} \equiv 1 \pmod{p} \Rightarrow a \text{ hat eine modulare Quadratwurzel}$$

Bei der Potenz  $(p-1)/2$  liegt entweder die Potenz 1 oder  $(p-1)$  vor, und dieses Ergebnis scheint in direkter Korrelation zu der Existenz der Wurzeln zu stehen.

Zunächst ist interessant warum bei dem Exponenten  $(p-1)/2$  immer nur 1 und  $(p-1)$  heraus kommt.

Das Element 1 wird in den Potenzen jedes Elements definiert,

$$\text{denn: } 1 \equiv 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \pmod{7}$$

Da der Exponent 6 gerade ist, kann die Wurzel gezogen werden:  $\sqrt{1} \equiv \{1; -1\} \wedge -1 \in [p-1]_p$

Warum ist nun dieses Ergebnis für die Existenz einer Wurzel interessant?

Dazu wird nun eines der erzeugenden Elemente betrachtet:

$$3^1 \equiv 3$$

Erzeugende Elemente enthalten sich selbst und alle anderen erzeugenden Elemente, bzw. das letzte Element nur mit einem ungeraden Exponenten, d.h. man kann aus ihnen nie die Wurzel ziehen.

$$3^2 \equiv 2$$

$$3^3 \equiv 6$$

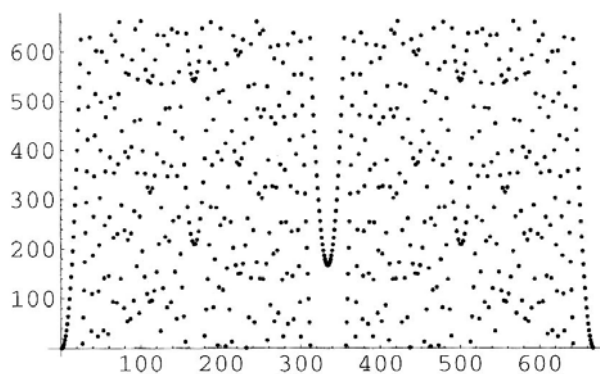
$$3^4 \equiv 4$$

Wiederum enthalten erzeugende Elemente alle vorhandenen Wurzeln, zumindest eines der beiden möglichen Ergebnisse.

$$3^5 \equiv 5$$

$$3^6 \equiv 1$$

Quadrate am Beispiel von  $\mathbb{Z}_{667}$   $f(x)=x^2$



Am Anfang ist gewohnte Parabelform erkennbar. Es ist eine Spiegelsymmetrie zu erkennen, die aus der Gleichung

$$x^2 \equiv (x - p)^2 \pmod{p}$$

folgt.

Es gibt auch mächtigere Lösungsmengen als 2, wenn  $\mathbb{Z}_n$  wie hier  $n=p*q$   $667=23*29$

$$\sqrt{506} = \{62;315;352;602\}$$

Die modulare Quadratwurzel berechnen:

Innerhalb einer Restklassenmenge mit genau einer einzigen Primzahl als Basis gibt es effiziente Berechnungsschemata.

Ist  $n=p*q$  zu einer Restklassenmenge entsprechend groß (200stellig), ist auch für moderne Rechensysteme

$$\sqrt{a} \equiv x \pmod{n}$$

nur noch in extrem langer Zeit (Jahren) zu berechnen.

Natürlich muss hierbei  $a^2 > p$  sein.

Es gibt bis jetzt keinen Algorithmus, der das Problem auf andere Weise löst, als die einzelnen Kombinationen durchzuprobieren.

Auf der anderen Seite ist die Umkehrfunktion, das Quadrieren, extrem einfach zu berechnen:

$$a^2 \equiv x \pmod{n}$$

## 2.3. Logarithmieren

Auch innerhalb von Restklassen können Logarithmen berechnet werden. Die Eigenschaften der Logarithmusfunktion sollen hier im Speziellen betrachtet werden.

### 2.3.1 Beispiele

Logarithmen am Beispiel von  $\mathbb{Z}_7$ :

Frage: Mit welchem Element muss 2 potenziert werden, damit 4 herauskommt?

Oder  $2^x \equiv 4 \pmod{7}$

Antwort:  $\log_2 4 \equiv 2 \pmod{7}$

denn  $2^2 \equiv 4 \pmod{7}$

Aber auch:

$\log_2 4 \equiv 5 \pmod{7}$

denn  $2^5 \equiv 32 \equiv 4 \cdot 7 + 4 \equiv 4 \pmod{7}$

Nicht nur, dass bei der Abbildung zwei Ergebnisse entstehen,

$2^x \equiv 5 \pmod{7}$

hat z.B. gar kein Ergebnis:

$\log_2 5 \equiv ? \pmod{7}$

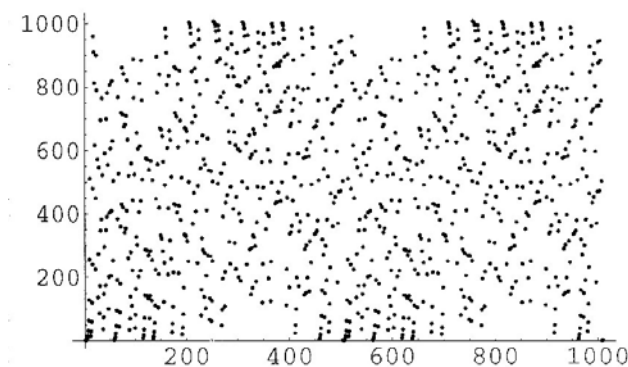
## 2.3.2 Struktur

Logarithmen am Beispiel von  $\mathbb{Z}_7$ :

Das Element 2 ist innerhalb der Restklassenmenge 7 ein zyklisches Element, daher ergibt sich für den Logarithmus dieses Elements eine Relation. Da innerhalb der Potenzierung von dem Element 2 auch nicht alle Elemente vorkommen, ist die Abbildung nicht surjektiv. Es gibt also für bestimmte Elemente von 2 kein Ergebnis, da man sie mit einer Potenzierung von zwei nicht erreicht.

Für die erzeugenden Elemente 3 und 5 in Bezug auf die Restklassenmenge 7 ergibt sich eine eindeutige Abbildung, da jedes Element erreicht werden kann.

Potenzen am Beispiel von  $\mathbb{Z}_{1009}$   $f(x)=2^x$ :



Am Anfang ist die bekannte Exponentialsteigung sichtbar.

Der Graph ist hier periodisch zu einem Teiler von  $(p-1)=(1009-1)$  (hier  $1008/2=504$ ).

Den modularen Logarithmus berechnen:

Ist  $p$  entsprechend groß (200stellige Primzahl), ist auch für moderne Rechensysteme

$$\log_b a \equiv x \pmod{p}$$

nur noch in extrem langer Zeit (Jahren) zu berechnen.

Natürlich muss hierbei  $b^x > p$  sein

Es gibt bis jetzt keinen Algorithmus, der das Problem auf andere Weise löst, als die einzelnen Kombinationen durchzuprobieren.

Auf der anderen Seite ist die Umkehrfunktion, die Potenz, extrem einfach zu berechnen:

$$a^b \equiv x \pmod{p}$$

### 3. **Praktische Anwendungen dieser Operationen im Bereich der Kryptographie**

Die in Kapitel 2 vorgestellten Verfahren finden in der modernen Kryptographie vielfältige Anwendungen. In diesem Kapitel werden zwei dieser Verfahren exemplarisch vorgestellt.

#### 3.1. Authentifizierung

##### 3.1.1 Das Dilemma der Authentifizierung

Angenommen, man hat sich nachts verlaufen und begegnet der rechts abgebildeten Person. Diese behauptet, sie sei Batman. Da die Person nicht unbeschränkt vertrauenswürdig aussieht, stellt sich die Frage, ob es sich wirklich um Batman handelt.

Batman steckt nun in einem Dilemma: Nimmt er seine Maske ab und sagt uns, dass es sich bei ihm um Bruce Wayne handelt, hat er alle seine Geheimnisse preisgegeben. Tut er dies nicht, kann er nicht beweisen, dass er Batman ist - oder etwa doch?



##### 3.1.2 Schritte der Authentifizierung

In Hinblick auf die Authentifizierung müssen 3. Schritte durchgeführt werden:

1. Ich weiß etwas, das mich authentifiziert  
Authentifizierung durch eine Information, die nur ich haben kann und darum ein eindeutiger Beweis für meine Identität ist.
2. Diese Information gebe ich nicht heraus  
Würde ich diese Information preisgeben, so könnten sich auch andere Personen als mich ausgeben.
3. Ich kann beweisen, dass ich die Information habe  
Ich muss einen Weg finden zu beweisen, dass ich die Information habe, ohne diese preiszugeben.

### 3.1.3 Fiat-Shamir-Protokoll

1. Ich wähle ein  $n=p*q$  für meine Restklassenmenge und ein Element  $s$  in dieser und quadriere  $s$ .
2. Die Zahl  $s$  gebe ich unter keinen Umständen preis.
3. Authentifizierungsprozess
  1. Ich gebe allgemein  $s^2$  und  $n$  bekannt.
  2. Ich gebe zusätzlich zu  $s^2$  und  $n$  ein frei gewähltes  $r^2$  bekannt.  
Nun darfst du fragen:  
entweder was ist  $s*r \rightarrow$  deine Prüfung  $(s*r)^2 \equiv s^2 * r^2 \pmod{n}$ ?  
oder was ist  $r \rightarrow$  deine Prüfung  $r_{neu}^2 \equiv r^2 \pmod{n}$
  3. Wüsste jemand die Fragen im Voraus, könnte er mogeln und sich als mich ausgeben. Darum wird Schritt 2 vielfach durchgeführt.

Wie könnte man mogeln?

- a) Wenn ich weiß, es wird nach  $r$  gefragt,  
gebe ich dir irgendein von mir berechnetes  $r^2$   
und auf deine Frage dann das gewählte  $r$   
Wichtig: Die Frage nach  $s*r$  könnte ich nicht beantworten, da ich  $s$  nicht kenne.
- b) Wenn ich weiß, es wird nach  $s*r$  gefragt,  
nehme ich eine Zahl  $a$  und quadriere sie, multipliziere das  
inverse Element von  $s^2$  mit  $a^2$  und gebe dir das Ergebnis.  
Fragst du nach  $s*r$ , gebe ich dir  $a$ . Da  $r^2 = (s^2)^{-1} * a^2$ ,  
ist  $s^2 * (s^2)^{-1} * a^2 = a^2$   
Wichtig: Die Frage nach  $r$  könnte ich nicht beantworten.

## 3.2. Schlüsselaustausch

### 3.2.1 Das Problem des Schlüsselaustausches

Beim Schlüsselaustausch handelt es sich um ein recht offensichtliches Problem. Der Schlüssel wird zur Sicherung der Übertragung genutzt. Zum Zeitpunkt des Schlüsselaustauschs ist die Übertragung also ungesichert. Die Frage ist also: Wie kann ich sicher einen Schlüssel übertragen auf einem ungesicherten Datenkanal?



### 3.2.2 Diffie-Hellman-Schlüsselaustausch

1. Es sei ein  $p$  für eine Restklassenmenge und ein Element  $s$  in dieser allgemein bekannt.
2. Zwei Kommunikationspartner A und B wollen einen gemeinsamen Schlüssel verwenden.  
A wählt geheim eine natürliche Zahl  $a$  und berechnet  $s^a \equiv \alpha \pmod{p}$  B wählt geheim eine natürliche Zahl  $b$  und berechnet  $s^b \equiv \beta \pmod{p}$
3. A und B schicken sich gegenseitig  $\alpha$  und  $\beta$  zu
4. A berechnet nun  $\alpha^b \equiv s^{ab} \equiv k \pmod{p}$   
und B berechnet nun  $\beta^a \equiv s^{ba} \equiv k \pmod{p}$

Wenn jemand  $\alpha$  und  $\beta$  abfängt, wie errechnet er dann  $a$  oder  $b$ ?

$$\log_s \beta \equiv ? \vee \log_s \alpha \equiv ?$$

Da hier allerdings die in 2.3.2 beschriebene Problematik zum Tragen kommt, ist das Problem nicht in angemessener Zeit lösbar.

## 4. Quellenangaben

Diskrete Mathematik für Einsteiger, Albrecht Beutelspacher, Kapitel 5 Zahlentheorie  
(Als Einleitung in die Zahlentheorie)

Kryptologie, Albrecht Beutelspacher, Kapitel 5 Die Zukunft hat schon begonnen oder  
Asymmetrische Kryptosysteme  
(Als Einleitung in moderne, insbesondere asymmetrische Kryptosysteme)

Wolfram Koepf: *Computeralgebra*, Kapitel 4 *Modulare Arithmetik*  
(Kernquelle zum Thema modulare Quadratwurzeln und modulare Logarithmen)

Wolfram Koepf: *Computeralgebra*, Kapitel 5 *Codierungstheorie und Kryptographie*  
(Information zu Kryptosystemen)

<http://www-dm.informatik.uni-tuebingen.de/lehre/kryptoVL/ws0607/Quadratwurzeln.pdf>  
(Informationen zum Thema modulare Quadratwurzeln)

[http://www.vkfco.homepage.t-online.de/Downloads/FIAT\\_04\\_08\\_2006.pdf](http://www.vkfco.homepage.t-online.de/Downloads/FIAT_04_08_2006.pdf)  
(Informationen zum Thema modulare Quadratwurzeln)

<http://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch>  
(Allgemeine Information zum Thema Diffie-Hellman-Protokoll)

<http://de.wikipedia.org/wiki/Fiat-Shamir-Protokoll>  
(Allgemeine Information zum Thema Fiat-Shamir-Protokoll)

## 5. Vertiefendes Material

Dieses Kapitel beschäftigt sich insbesondere mit Quellen, die im Zuge der Seminarvorbereitung betrachtet wurden und die zu dem Thema inspirierend und interessant sind, allerdings nicht in den Seminarvortrag aufgenommen wurden.

### 5.1 RSA-Kryptosysteme

Die RSA ist ein asymmetrisches Kryptosystem, das mit dem Wissen aus dem Vortrag gut verständlich sein sollte. Zusätzlich sollte zum Verständnis noch der erweiterte euklidische Algorithmus betrachtet werden.

Das Verfahren der RSA wird im heutigen Datenverkehr vielseitig eingesetzt.

Quellen:

Kryptologie, Albrecht Beutelspacher, Kapitel 5 Die Zukunft hat schon begonnen oder Asymmetrische Kryptosysteme

(Eine recht einfache Erklärung zum Thema mit teilweise recht irreführenden Beispielen)

<http://de.wikipedia.org/wiki/RSA-Kryptosystem>

(Allgemeine Information zum Thema RSA)

### 5.2 Primzahlen

Für das gesamte Thema der Kryptographie und der modularen Arithmetik spielen Primzahlen eine extrem wichtige Rolle.

Zudem faszinieren sie Mathematiker bereits seit den Anfängen der Mathematik.

Quellen:

Die Musik der Primzahlen, Marcus du Sautoy

(Das Buch ist kein Mathematik-Buch, sondern eine Abhandlung über die riemannsche Vermutung, der ersten Regelmäßigkeit, die in der Abfolge der Primzahlen bis jetzt gefunden wurde, aber bis heute nicht bewiesen ist, wenngleich heute kaum noch Zweifel an ihrer Korrektheit bestehen)

<http://www.primzahlen.de/>

(Diese Seite besitzt einen Primzahltester und viele andere interessante Informationen zum Thema)

### 5.3 Quantencomputer

Im Zusammenhang mit Kryptosystemen wird häufig von der Gefahr durch Quantencomputer gesprochen, die solche Systeme aufgrund ihrer Struktur knacken können, bzw. ein Ergebnis mit einer bestimmten Korrektheitswahrscheinlichkeit ermitteln können.

Tatsächlich ist man noch sehr weit davon entfernt, solche Rechensysteme im größeren Umfang zu verwirklichen. Ihr Konzept und ihr Potenzial ist allerdings für die Kryptographie äußerst interessant.

Quellen:

<http://de.wikipedia.org/wiki/Quantencomputer>

(Allgemeine Information zum Thema Quantencomputer)

<http://www.vossyline.de/artikel/multimedia/quantencomputer.htm>

(Eine Abhandlung, die sich insbesondere mit dem Knacken von Codes befasst)