Schottengymnasium

Freyung 6, 1010 Wien

Vorwissenschaftliche Arbeit

Der Satz von Euler-Fermat und seine Anwendung in der Kryptographie

Leopold Karl

8C

Betreuer: Mag. Markus Kiesenhofer

Vorgelegt im Februar 2021

Abstract

Der Satz von Euler-Fermat ist eine zahlentheoretische Erkenntnis, die zwei teilerfremde natürliche Zahlen im Rahmen der Kongruenzrechnung zueinander in Bezug setzt. Dieser Lehrsatz ist Grundlage zahlreicher weiterführender Überlegungen in der Zahlentheorie und findet konkrete Anwendung in der modernen Kryptographie in Form der RSA-Verschlüsselung. Dieses innovative kryptographische Verfahren sichert in der heutigen Zeit, in der Cyber-Schutz eine zentrale Rolle spielt, eine abhörsichere Schlüsselübermittlung und ermöglicht die Erstellung von digitalen Signaturen.

In der vorliegenden vorwissenschaftlichen Arbeit werden einleitend ein historischer Überblick der Zahlentheorie und eine mathematische Einführung in zahlentheoretische Grundlagen gegeben. Die zentralen Elemente dieser Arbeit sind die mathematische Erschließung des Kleinen Satzes von Fermat sowie insbesondere die nachvollziehbare Herleitung dessen Verallgemeinerung, des Satzes von Euler-Fermat. Dies geschieht anhand der Erläuterung zahlentheoretischer Grundlagen, anhand theoretischer Beweisführungen und konkreter Beispiele, die den Leserinnen und Lesern die abstrakte Mathematik greifbar machen sollen.

Abgerundet wird die Arbeit mit einer Einführung in die moderne Kryptographie sowie mit einer verständlich aufbereitete Erklärung des RSA-Verfahrens, welche die Anwendbarkeit und Nützlichkeit dieses zahlentheoretischen Lehrsatzes in der Praxis belegt.

Vorwort

Schon im Kindergartenalter begeisterte ich mich für die Mathematik, auch wenn damals noch das Rechnen an sich im Vordergrund stand. Aufgrund vieler toller Persönlichkeiten, die mich im Laufe meines (Schul-)Lebens auf dem Gebiet der Mathematik förderten, ist diese Begeisterung bis heute erhalten geblieben. Gerade deswegen ist es mir nicht zuletzt auch ein persönliches Anliegen, mich in meiner vorwissenschaftlichen Arbeit einem mathematischen Thema zu widmen.

Den konkreten thematischen Anstoß für meine Arbeit gab Prof. Markus Fulmek von der Universität Wien. Während weiterer Lektüre zum Thema fiel mir die Anwendung des Satzes von Euler-Fermat in der Kryptographie, das RSA-Verfahren, auf. Obwohl ich der Behandlung einer Verschlüsselungstechnik aufgrund mangelnden kryptographischen Vorwissens zuerst skeptisch gegenüberstand, zog mich die Thematik beim Einlesen in Bann. Dabei wurde mir erst bewusst, wie aktuell und relevant diese Verschlüsselung für jede und jeden heutzutage ist. Zugegebenermaßen war ich tatsächlich erstaunt darüber, auf welch logischem und greifbarem Fundament die Kryptographie, die oftmals als für Laien zu komplex dargestellt wird, aufbaut.

An dieser Stelle möchte ich einigen Personen, die mich im Laufe des Schreibprozesses unterstützt haben, meinen herzlichsten Dank aussprechen:

allen voran meiner Familie für tägliche Motivation und Unterstützung,

meinem Betreuer, Mag. Markus Kiesenhofer, der mich trotz der heurigen schulischen Ausnahmesituation aufgrund von Covid-19 stets beratend begleitet hat,

Oskar Schmölz und Rossen Nenov, die mir bei Frage- und Problemstellungen bezüglich des verwendeten Textverarbeitungsprogramms LaTeX zur Seite gestanden sind,

Ao. Univ.-Prof. Mag. Dr. Markus Fulmek, der mir bei der Themenfindung geholfen hat und Mag. Bernhard Krauskopf, meinem Professor in der Mathematikolympiade, der es mit seinem Enthusiasmus über die letzten Jahre hinweg geschafft hat, meine Begeisterung für die Mathematik weiter zu entfalten.

Leopold Karl, Wien, Jänner 2021

Inhaltsverzeichnis

1 Einleitung **6**

2 Einführung in die Zahlentheorie **7**
2.1 Geschichte der Zahlentheorie 8
2.2 Zahlentheoretische Grundlagen 11
2.2.1 Die Kongruenzrelation 11
2.2.2 Rechnen mit Kongruenzen 13
2.2.3 Das inverse Element 14
2.2.4 Der Euklidische Algorithmus 15
2.2.5 Der erweiterte Euklidische Algorithmus 16

3 Der Kleine Satz von Fermat **18**
3.1 Der Satz 18
3.2 Beweis 19

4 Der Satz von Euler-Fermat **20**
4.1 Historisches zu Leonhard Euler 20
4.2 Die Euler'sche Phi-Funktion $\Phi(n)$ 23
4.3 Eigenschaften der Phi-Funktion $\Phi(n)$ 25
4.4 Der Satz 28
4.5 Beweis 29

5 Anwendung in der Kryptographie **30**
5.1 Kryptographie – Was ist das? 31
5.2 Das RSA-Verfahren 32
5.2.1 Die Schlüsselerzeugung 33
5.2.2 Verschlüsseln und Entschlüsseln 34
5.2.3 Das Signaturverfahren 34
5.2.4 Sicherheit des RSA-Verfahrens 35
5.2.5 Angriffe auf das RSA-Verfahren 37

6 Fazit **39**

Literaturverzeichnis **40**

Abbildungsverzeichnis **44**

Tabellenverzeichnis **44**

Glossar **45**

Eidesstattliche Selbstständigkeitserklärung **52**

1 Einleitung

Vor wenigen Jahrhunderten wurde die Zahlentheorie noch als „Zahlenspielerei“ abgetan, doch heute wissen wir es besser: Sie ist Grundlage vieler mathematischer Erkenntnisse, findet aber auch in der Praxis Verwendung.

Die vorliegende Arbeit beschäftigt sich mit einem konkreten Satz der elementaren Zahlentheorie, dem Satz von Euler-Fermat, und dessen spezifischer Anwendung in der Kryptographie, dem RSA-Verfahren. Dabei verfolgt sie das Anliegen, den mathematischen Lehrsatz verständlich aufzubereiten und dessen praktischen Nutzen darzustellen. Um dies umfassend zu ermöglichen, wird anfänglich auf die Zahlentheorie selbst sowie auf ausgewählte grundlegende Überlegungen dieser eingegangen. Des Weiteren wird der Kleine Satz von Fermat behandelt, der Vorläufer des Satzes von Euler-Fermat ist. Daraufhin wird das Kernthema dieser vorwissenschaftlichen Arbeit, der Satz von Euler-Fermat, ausführlich dargestellt und die dazu notwendige Euler'sche Phi-Funktion eingeführt. Anschließend geht die vorliegende Arbeit auf die wichtigste praktische Anwendung des behandelten Satzes, das RSA-Verfahren, ein. Darüber hinaus ist am Ende der Arbeit ein Glossar zu finden, um womöglich unbekannte Fachbegriffe zu erklären.

Grundsätzlich erhebt diese vorwissenschaftliche Arbeit nicht den Anspruch, einen vollständigen Überblick über die Disziplin der Zahlentheorie und jene der Kryptographie zu geben. Die Arbeit ist vielmehr darauf fokussiert, nur so weit in die jeweiligen Fachgebiete vorzudringen, wie es eine nachvollziehbare Erklärung der erwähnten Hauptthemen verlangt, um den Rahmen der Arbeit nicht zu sprengen. Deswegen ist auch ein historischer Abriss der Kryptographie, die Erklärung weiterer kryptographischer Verfahren und die Darstellung der Gesamtheit aller zahlentheoretischen Grundlagen nicht Teil dieser vorwissenschaftlichen Arbeit.

Die Grundlage der vorliegenden Arbeit bildet eine fundierte Lektüre zahlreicher literarischer Werke, die im Literaturverzeichnis zu finden sind, sowie ein im Zuge der Österreichischen Mathematikolympiade erworbenes Vorwissen des Autors auf dem Gebiet der Zahlentheorie.

2 Einführung in die Zahlentheorie

„Alles ist Zahl“, soll schon Pythagoras im sechsten Jahrhundert vor Beginn unserer Zeitrechnung gesagt und damit gemeint haben, dass sich unsere Natur durch Zahlen beschreiben lässt und uns die Beschäftigung mit ihnen zu einem besseren Naturverständnis verhilft.[1] Als Teilgebiet der Mathematik beschäftigt sich die Zahlentheorie genau mit diesem Thema – den Eigenschaften von Zahlen und den mit ihnen durchgeführten Rechenoperationen.

Historisch betrachtet ist die Zahlentheorie ursprünglich durch das Bedürfnis der Menschen motiviert, gleichartige Objekte (z. B. Vieh) zu zählen und die resultierenden Werte zu vergleichen. So beschränkt sie sich in den Anfängen auf das Untersuchen von natürlichen Zahlen $\mathbb{N}$. Bedingt durch neue mathematische Problemstellungen entstand im Laufe der Zeit immer wieder die Notwendigkeit, die Grundmenge der Zahlen zu erweitern, sodass man sich heutzutage in der Menge der komplexen Zahlen $\mathbb{C}$ bewegt. Entsprechend der größeren Zahlenmenge hat sich das Gebiet der Zahlentheorie fortlaufend nicht nur um die Grundmenge der Zahlen, sondern auch um neu entstandene Rechenoperationen und Ansätze aus anderen mathematischen Teilgebieten erweitert. So ist sie mittlerweile zu einem für einzelne Mathematikerinnen und Mathematiker kaum zu überblickenden Teilgebiet der Mathematik angewachsen, das sich nochmals in zahlreiche kleinere Teilgebiete aufsplitten lässt. Um die drei größten davon zu nennen, seien hier die elementare, die algebraische und die analytische Zahlentheorie angeführt. Die elementare Zahlentheorie beschäftigt sich vorwiegend mit dem ursprünglichen Grundgedanken der Zahlentheorie: den Eigenschaften der natürlichen Zahlen $\mathbb{N}$, der ganzen Zahlen $\mathbb{Z}$ und der rationalen Zahlen $\mathbb{Q}$. Das Gebiet der algebraischen Zahlentheorie geht über $\mathbb{Q}$ hinaus und betrachtet algebraische Zahlenkörper. Die analytische Zahlentheorie beschäftigt sich hingegen hauptsächlich mit dem Zahlenkörper $\mathbb{C}$, mit dem Ziel arithmetische Eigenschaften zu finden und zu betrachten.

Da der in dieser Arbeit behandelte Satz von Euler-Fermat Aussagen über eine Eigenschaft von natürlichen Zahlen $\mathbb{N}$ trifft, ist er in erster Linie der elementaren Zahlentheorie zuzuordnen.[2]

[1] Vgl. **Oswald/Steuding** (2015), S. 3.
[2] Vgl. **Forster** (2015), S. 1; **Magidin** (2011); **Oswald/Steuding** (2015), S. 3; **Walz** (2017).

2.1 Geschichte der Zahlentheorie

Vor über 40.000 Jahren kommt unter den Menschen das Verlangen auf, Gegenstände zu zählen. Heute bezeichnen wir diesen Zeitpunkt als Ursprung der Mathematik. Denn auch wenn der genaue Beginn von Rechen- und Zähltätigkeiten nicht bekannt ist, haben wir doch Artefakte, die eine frühe Zähltätigkeit der Menschheit belegen.

Dem für diese Arbeit interesssanten Teilgebiet der Mathematik, der Zahlentheorie, wird dann im Altertum aus wirtschaftlichen Gründen Beachtung geschenkt, was sie zu einem der ältesten Zweige der Mathematik macht. Das Bewerten von Gütern ist in dieser Zeit sowohl im Handel als auch bei rechtlichen Angelegenheiten, wie einer Erbschaft, von großer Bedeutung. Um eine solche Bewertung exakt und korrekt durchzuführen, müssen die Betroffenen mit Mengenverhältnissen umgehen können und ein gewisses Zahlenverständnis aufweisen. Diese Fähigkeiten werden heute zum Gebiet der Zahlentheorie gezählt.

Den ersten Fund, der das Vorhandensein zahlentheoretischer Überlegungen belegt, stellt die babylonische Tafel „Plimpton 322“ dar, die eine Tabelle pythagoräischer Tripel zeigt. Ihre Entstehung wird auf ca. 1800 v. Chr. geschätzt, womit in Folge der Beginn der Zahlentheorie festgelegt ist. Etwas später im Verlauf der Geschichte beschäftigen sich vor allem die Pythagoräer mit der Zahlentheorie, wobei diese sich besonders für pythagoräische Tripel, Teilbarkeiten, die Parität, sowie vollkommene und figurierte Zahlen interessieren.[3] Ein noch heute bekannter Mathematiker und Zahlentheoretiker der damaligen Zeit ist Euklid von Alexandria, der um 300 v. Chr. im heutigen Ägypten lebt. Er verfasst die „Elemente“[4], ein dreizehnbändiges Werk, das einen ausführlichen Überblick über die mathematischen Errungenschaften der „alten Griechen“ (vorwiegend auf dem Gebiet der Geometrie und Zahlentheorie) gibt und sogar schon die Art und Weise, in der heutzutage Mathematik betrieben wird, verwendet – es wird mit Definitionen, Sätzen und Beweisen gearbeitet.

Im dritten Jahrhundert n. Chr. verfasst Diophant von Alexandria das nächste große zahlentheoretische Werk, seine „Arithmetica“. Die „Arithmetica“ ist eine Sammlung von Gleichungen und Gleichungssystemen, für deren Lösung nur die Menge von $\mathbb{Q}^+$ zugelassen ist.[5]

[3] Vgl. **Walz** (2017).
[4] Vgl. **Thaer/Schreiber** (2010).
[5] Vgl. **Brückler** (2017), S. 137–140; **Ziegenbalg** (2015), S. 6–9.

Aber auch außerhalb der europäischen Hochkulturen werden zahlentheoretische Überlegungen angestellt, die wesentlich für das heutige Gebiet der Zahlentheorie sind. So verdanken wir den Indern u. a. unser heutiges Dezimalsystem der Zahlen und den ersten Algorithmus zum Lösen von Pell'schen Gleichungen, den Brahmagupta im Jahr 628 fand. Ebenso tragen chinesische und arabische Mathematiker seinerzeit wesentlich zur Weiterentwicklung der Zahlenteorie bei: Das Volk der Chinesen untersucht unabhängig von externen Einflüssen die Eigenschaften der Zahlen und gelangt zu einigen interessanten Erkenntnissen, wie dem Chinesischen Restsatz. Die Araber setzen sich im Gegensatz dazu intensiv mit dem Gedankengut benachbarter und eroberter Kulturkreise auseinander und entwickeln dieses weiter, woraus u. a. der Satz von befreundeten Zahlen von Tabit ibn Qurra und das später als Satz von Wilson bekannt gewordene Theorem von Al-Haytam resultieren.[6]

Während sich der stete Fortschritt der Zahlentheorie in moslemischen und anderen nichteuropäischen Ländern im Verlauf des Mittelalters weiterhin vollzieht, stagniert er im römisch und katholisch geprägten Europa. Das damalige Standardwerk im europäischen Raum ist die lateinische Übersetzung der „Arithmetik" des Nikomachos, das trotz seines mathematisch deutlich niedrigeren Niveaus als die „Elemente" des Euklid große Bekanntheit erlangt.[7] Im Zuge der Renaissance und der wissenschaftlichen Revolution werden in Europa die zahlentheoretischen Werke der Antike systematisch erschlossen, wodurch eine neue Blütezeit der Zahlentheorie beginnt, in der zahlreiche bekannte Zahlentheoretiker wirken: Pierre de Fermat (1601–1665) versieht einerseits die „Arithmetica" des Diophant von Alexandrien mit Randbemerkungen, unter denen u. a. die Fermatsche Vermutung zu finden ist, andererseits formuliert er den Kleinen Satz von Fermat, auf den im Kapitel 3 eingegangen wird, sowie zahlreiche weitere zahlentheoretische Theoreme und Vermutungen. Um seine Erkenntnisse mit ihm zu teilen und einen Austausch von Ideen und Ansätzen zu ermöglichen, pflegt Pierre de Fermat einen Briefwechsel mit Marin Mersenne (1588–1648), der auch mit zahlreichen anderen Mathematikern seiner Zeit wie Huygens, Pell, Galilei und Toricelli vorwiegend per Brief in Kontakt steht und für seine Beschäftigung mit den nach ihm benannten Mersenne-Primzahlen bekannt ist.[8] Diese stehen in engem Zusammenhang mit den vollkommenen Zahlen, deren Form, nachdem sie schon

[6] Vgl. **Brückler** (2017), S. 141–145; **Ziegenbalg** (2015), S. 10–13.
[7] Vgl. **Ziegenbalg** (2015), S. 14.
[8] Vgl. **Brückler** (2017), S. 145–146; **Ziegenbalg** (2015), S. 18.

Jahrhunderte zuvor von Euklid ergründet worden ist, Leonhard Euler (1707–1783) exakter bestimmt. Außerdem führt Euler die Phi-Funktion, die im Kapitel 4.2 definiert wird, ein und stellt neben vielen anderen Theoremen den Satz von Euler-Fermat auf, der eine Verallgemeinerung des Kleinen Satzes von Fermat darstellt. Genaueres zu diesen beiden Sätzen ist in den Kapiteln 3 und 4 zu finden.[9]

Ein weiterer wichtiger und überaus bekannter Zahlentheoretiker ist Carl Friedrich Gauß (1777–1855). Er soll schon als kleiner Bub die Methode des Kleinen Gauß gefunden haben, die es ermöglicht, die Summe beliebig vieler aufeinanderfolgender Glieder einer arithmetischen Folge zu summieren. Um zum Beispiel die (natürlichen) Zahlen von 1 bis 100 zu addieren (beim Lösen dieser Aufgabe entdeckt der damals 8-jährige Gauß der Legende nach diese Methode), addiert man die kleinste und die größte Zahl und multipliziert das Ergebnis mit der halben Anzahl der zu summierenden Zahlen. Das bedeutet konkret: $(1 + 100) \cdot \frac{100}{2} = 101 \cdot 50 = 5050$.[10] Carl Friedrich Gauß ist aber nicht nur im Jugendalter schon genial, sondern bleibt sein ganzes Leben über ein begnadeter Mathematiker. Sein zahlentheoretisches Hauptwerk „Disquisitiones arithmeticae“ (1801), das u. a. den Fundamentalsatz der Arithmetik beinhaltet, der die Existenz und Eindeutigkeit der Primfaktorenzerlegung einer jeden Zahl $n > 1 \in \mathbb{N}$ behandelt, gilt heute als Beginn der modernen Zahlentheorie.[11] Von diesem Zeitpunkt an wird die Zahlentheorie als eigenes, systematisch geordnetes Teilgebiet der Mathematik angesehen, legt eine rasante Entwicklung bis heute hin und bietet die Grundlagen für eine Reihe von modernen Technologien und Anwendungen.[12] Gerade deswegen ist auch folgendes Bonmot von Gauß so treffend:

> *„Die Mathematik ist die Königin der Wissenschaft und die Arithmetik ($\widehat{=}$ Zahlentheorie) ist die Königin der Mathematik.“*[13]

[9] Vgl. **Brückler** (2017), S. 147; **Ziegenbalg** (2015), S. 20.
[10] Vgl. **Strick** (2017), S. 26–27.
[11] Vgl. **Karpfinger/Meyberg** (2010), S. 65.
[12] Vgl. **Brückler** (2017), S. 149; **Ziegenbalg** (2015), S. 21–23.
[13] Vgl. **Ziegenbalg** (2015), S. 23.

2.2 Zahlentheoretische Grundlagen

Um auf die Beweisführungen des Kleinen Satzes von Fermat und des Satzes von Euler-Fermat bestmöglich vorzubereiten, finden sich in diesem Kapitel zahlentheoretische Grundlagen, die für das Verständnis folgender Beweise hilfreich sind. Auf die Darstellung sonstiger zahlentheoretischer Grundlagen wird verzichtet und Grundkenntnisse der Schulmathematik werden vorausgesetzt, um den Fokus auf das eigentliche Thema zu gewährleisten.

2.2.1 Die Kongruenzrelation

Bei der Division natürlicher Zahlen a_i durch $m \in \mathbb{N}$ erhält man einen gewissen Rest $r \in \mathbb{N}$. Mithilfe der Kongruenzrelation werden die Zahlen a_i zueinander bezüglich des bestehenden Rests beim Teilen durch eine festegelegte Zahl m in Bezug gesetzt. Da eine einfache Notation dieser Beziehung der Zahlen a_i untereinander bei vielen zahlentheoretischen Sachverhalten, wie auch beim Satz von Euler-Fermat, hilfreich für deren Beschreibung und Beweis ist, wird die heute übliche Darstellung in Folge näher erläutert.

Man nehme die Menge $\mathbb{M} = \{a_i \in \mathbb{N} \mid a_i = i\} = \{0; 1; 2; 3; ...\}$. Nun teilen wir die Zahlen a_i z. B. durch $m = 3$ und betrachten den Rest r_i vom jeweiligen a_i. Dazu werden alle a_i in folgende Form gebracht, die hier allgemein formuliert ist:

$$a_i = i = x_i \cdot m + r_i \text{ mit } x, r \in \mathbb{N}.$$

Nun wird der Reihe nach für i eingesetzt. Dafür erhalten wir:

$$\begin{aligned}
a_0 &= 0 = 0 \cdot 3 + 0 \\
a_1 &= 1 = 0 \cdot 3 + 1 \\
a_2 &= 2 = 0 \cdot 3 + 2 \\
a_3 &= 3 = 1 \cdot 3 + 0 \\
&... \\
a_{98} &= 98 = 32 \cdot 3 + 2 \\
a_{99} &= 99 = 33 \cdot 3 + 0 \\
a_{100} &= 100 = 33 \cdot 3 + 1 \\
&...
\end{aligned}$$

Wie zu erkennen ist, gleicht der Rest $r_0 = 0$ der Zahl a_0 dem von a_3, aber auch dem von a_{99}. Die Zahlen a_1 und a_{100} besitzen ebenfalls denselben Rest, nämlich 1. Ebenso beträgt sowohl für a_2 als auch für a_{98} der Rest 2. Es lässt sich allgemein festhalten, dass für einen Rest r_k einer Zahl $k \in \mathbb{M}$ mit $n \in \mathbb{N}$ Folgendes gilt:

(1) Wenn $k = 3n$, dann ist $r_k = r_{3n} = 0$.

(2) Wenn $k = 3n + 1$, dann ist $r_k = r_{3n+1} = 1$.

(3) Wenn $k = 3n + 2$, dann ist $r_k = r_{3n+2} = 2$.

Um diese Relationen einfach zu notieren, wird das Kongruenzzeichen „ $\equiv$ “ und der Begriff „modulo“, kurz „mod“, eingeführt. Mit dem Unterschied, dass die zueinander in Bezug gesetzten Zahlen bzw. Terme nicht ident sind, sondern sich nur ihr Rest beim Teilen durch eine bestimmte Zahl m gleicht, wird das Kongruenzzeichen grundsätzlich wie das Gleichheitszeichen verwendet, auch wenn diese sich bezüglich der möglichen Umformungsschritte voneinander unterscheiden, wie im Kapitel 2.2.2 erläutert wird. Das Setzen des Ausdrucks „$mod\ m$“ nach einer Kongruenzgleichung oder einem Term bestimmt, durch welches m ein a_i geteilt wird, bevor der zugehörige Rest r_i betrachtet wird. Ein Beispiel wäre $6 \equiv 99\ (mod\ 3)$, da $r_6 = 0 = r_{99}$ beim Teilen durch $m = 3$ gilt.[14]

Ein weiterer wichtiger Begriff in diesem Zusammenhang ist jener der „Restklasse“. Eine Restklasse $\mathbb{K} = \{a_i \in \mathbb{Z} \mid a_i \equiv a_k\ (mod\ m)\}$ bezeichnet die Menge der zu $a_k\ (mod\ m)$ kongruenten ganzen Zahlen. Es gibt m voneinander verschiedene Restklassen modulo m, da $a_i \equiv 0 \vee 1 \vee 2 \vee ... \vee (m-1)$ sein kann. Modulo 3 existieren also die drei paarweise voneinander verschiedenen Restklassen 0, 1 und 2.[15]

[14] Vgl. **Padberg/Büchter** (2018), S. 29–30; **Ziegenbalg** (2015), S. 85.
[15] Vgl. **Bartholomé/Rung/Kern** (2008), S. 44; **Ziegenbalg** (2015), S. 86.

2.2.2 Rechnen mit Kongruenzen

Im Folgenden werden die Grundrechenarten innerhalb der Kongruenzrechnung definiert und anhand von Beispielen (Bsp.) veranschaulicht. Wir setzen dafür $a, b \in \mathbb{Z} \wedge m \in \mathbb{N}$.

I) Addition:

$$(a \ mod \ m) + (b \ mod \ m) := (a + b) \ mod \ m.$$

Bsp: $(87 \ mod \ 5) + (34 \ mod \ 5) \equiv (87 + 34) \ mod \ 5 \equiv 121 \ mod \ 5 \equiv 1 \ mod \ 5.$

II) Subtraktion:

$$(a \ mod \ m) - (b \ mod \ m) := (a - b) \ mod \ m.$$

Bsp: $(76 \ mod \ 7) - (37 \ mod \ 7) \equiv (76 - 37) \ mod \ 7 \equiv 39 \ mod \ 7 \equiv 4 \ mod \ 7.$

III) Multiplikation:

$$(a \ mod \ m) \cdot (b \ mod \ m) := (a \cdot b) \ mod \ m.$$

Bsp: $(64 \ mod \ 13) \cdot (3 \ mod \ 13) \equiv (64 \cdot 3) \ mod \ 13 \equiv 192 \ mod \ 13 \equiv 10 \ mod \ 13.$

IV) Division:

Die Division ist innerhalb der Kongruenzrechnung nicht möglich, da die ganzen Zahlen gegenüber der Division nicht abgeschlossen sind, also $\frac{a}{b}$ nicht zwingend eine ganze Zahl sein muss, und man sich bei der Kongruenzrechnung nur im Zahlenraum der ganzen Zahlen $\mathbb{Z}$ bewegt. Um trotzdem eine Äquivalenzumformung zu haben, die das Gegenstück zur Multiplikation bildet, wurde das Multiplizieren mit dem inversen Element gefunden, auf das im folgenden Kapitel 2.2.3 näher eingegangen wird.[16]

[16] Vgl. **Bartholomé/Rung/Kern** (2008), S. 44–47; **Oswald/Steuding** (2015), S. 123.

2.2.3 Das inverse Element

Grundsätzlich existiert für das Rechnen mit Kongruenzen ein inverses Element der Addition und eines der Multiplikation[17]. Da für diese Arbeit ausschließlich das multiplikative Inverse relevant ist, wird nur dieses angeführt und in weiterer Folge der Arbeit als „das Inverse“ bzw. „inverses Element“ bezeichnet.

Ein inverses Element j von a ist eine Zahl, für die mit $a, j \in \mathbb{Z} \ \wedge \ m \in \mathbb{N}$ gilt:

$$a \cdot j \equiv 1 \ (mod \ m).$$

Satz: Für $a \in \mathbb{Z} \ \wedge \ m \in \mathbb{N}$ besitzt a genau dann ein inverses Element j modulo m, wenn $ggT(a, m) = 1$ gilt. [18]

Beweis: Sei j ein inverses Element von a modulo m, dann lässt sich dies per Definition der Kongruenznotation auch als $j \cdot a \equiv 1 \ (mod \ m)$ schreiben, was ebenfalls laut Definition $j \cdot a = 1 + k \cdot m$ mit $k \in \mathbb{Z}$ entspricht. Dies kann in $j \cdot a + (-k) \cdot m = 1$ umgeformt werden, woraus resultiert, dass $ggT(a, m) = 1$ ist. Wäre $ggT(a, m)$ nicht 1, sondern $d \in \mathbb{N}$ ohne 1, dann könnte $j \cdot a + (-k) \cdot m$ nur ein Vielfaches von d sein, da Folgendes gilt, wobei $\frac{a}{d}, \frac{m}{d} \in \mathbb{N}$ sind, weil $d = ggT(a, m)$:

$$\begin{aligned} & j \cdot a + (-k) \cdot m = \\ &= j \cdot \frac{a}{d} \cdot d + (-k) \cdot \frac{m}{d} \cdot d = \\ &= d \cdot \left(j \cdot \frac{a}{d} + (-k) \cdot \frac{m}{d} \right). \end{aligned}$$

□

Da bei der Kongruenzrechnung, wie im vorherigen Kapitel erläutert, nicht einfach dividiert werden darf, dient das Multiplizieren mit dem Inversen j einer Zahl a als Gegensatz zur Äquivalenzumformung der Multiplikation. Selbstverständlich darf dieser Divisionsersatz der Kongruenzrechnung nur dann verwendet werden, wenn auch ein inverses Element j zu a existiert, wofür, wie oben bewiesen, $ggT(a, m) = 1$ die Voraussetzung ist.[19]

[17] Vgl. **Bartholomé/Rung/Kern** (2008), S. 47.
[18] ggT = größter gemeinsamer Teiler
[19] Vgl. **Bundschuh** (2008), S. 83–84; **Ziegenbalg** (2015), S. 47–48.

2.2.4 Der Euklidische Algorithmus

Der Euklidische Algorithmus ist eine systematische Folge von Rechenoperationen, die schlussendlich zum ggT zweier Zahlen $a, b \in \mathbb{N}$ führt.

Bei der Durchführung des Euklidischen Algorithmus setzt man die Zahlen a, b in die Gleichung $a = x_0 \cdot b + y_0$ mit $x_0, y_0 \in \mathbb{Z} \ \wedge \ a, b \in \mathbb{N} : a > b$ ein. Daraufhin wird b durch $b = x_1 \cdot (a - x_0 \cdot b) + y_1 = x_1 \cdot y_0 + y_1$ ausgedrückt. Der fortlaufende Algorithmus ergibt sich durch erneutes Einsetzen in eine Gleichung derselben Form, wobei der Einfachheit halber $a = a_0;\ b = a_1;\ y_0 = a_2$ gesetzt wird, sodass die Ausgangsgleichung folgendermaßen aussieht: $a_0 = x_0 \cdot a_1 + a_2$. Der durchlaufende Algorithmus hat mit $k, z \in \mathbb{N}$, wobei a_k ein beliebiges Glied der Folge a_i, die sich aus dem Algorithmus ergibt, darstellt und das z-te Glied $a_z = 0$ ist, die folgende Form:

$$
\begin{aligned}
a_0 &= x_0 \cdot a_1 + a_2 \\
a_1 &= x_1 \cdot a_2 + a_3 \\
a_2 &= x_2 \cdot a_3 + a_4 \\
&\ldots \\
a_k &= x_k \cdot a_{k+1} + a_{k+2} \\
a_{k+1} &= x_{k+1} \cdot a_{k+2} + a_{k+3} \\
&\ldots \\
a_{z-3} &= x_{z-3} \cdot a_{z-2} + a_{z-1} \\
a_{z-2} &= x_{z-2} \cdot a_{z-1} + a_z.
\end{aligned}
$$

Die letzte Zeile des Euklidischen Algorithmus liefert den $ggT(a, b)$, der a_{z-1} beträgt.

Angewandt auf $a = 255; b = 57$ sehen die obigen, allgemein formulierten Zeilen so aus:

$$
\begin{aligned}
255 &= 4 \cdot 57 + 27 \\
57 &= 2 \cdot 27 + 3 \\
27 &= 9 \cdot 3 + 0.
\end{aligned}
$$

Daher ist der $ggT(255, 57) = 3$.

Beweis: Der gesicherte Erfolg des Euklidischen Algorithmus, also die Tatsache, dass er am Ende wirklich den ggT zweier Zahlen $a, b \in \mathbb{N}$ liefert, beruht auf der Tatsache, dass für die früher erwähnten a_i mit $a = a_0; b = a_1$ der $ggT(a_0, a_1) = ggT(a_1, a_2) = ... = ggT(a_k, a_{k+1})$ ist. Dies folgt aus der umgeformten ersten Zeile des Euklidischen Algorithmus $a_2 = a_0 - x_0 \cdot a_1$, da der $ggT(a_0, a_1)$ sowohl a_0 als auch a_1, folglich auch $x_0 \cdot a_1$ und somit die Differenz $a_0 - x_0 \cdot a_1 = a_2$ teilt. Analoges gilt für alle weiteren a_i.

Da jede Teilmenge der natürlichen Zahlen $\mathbb{N}$ ein kleinstes Element besitzt, gelangt der für a_i gegen 0 konvergierende Euklidische Algorithmus nach einer endlichen Anzahl von äquivalenten Rechenoperationen an ein Ende der Form $a_{z-2} = x_{z-2} \cdot a_{z-1} + a_z$ mit $a_z = 0$, woraus der $ggT(a, b) = a_{z-1}$ abgelesen werden kann.[20] □

2.2.5 Der erweiterte Euklidische Algorithmus

Der erweiterte Euklidische Algorithmus baut auf dem Euklidischen Algorithmus auf, indem er an dessen umgeformter vorletzten Zeile ansetzt und ihn in entgegengesetzter Richtung bis zu den beiden Anfangsgliedern $a = a_0$ und $b = a_1$ wieder zurückverfolgt. Schlussendlich erhält man durch den Erweiterten Euklidischen Algorithmus eine Vielfachsummendarstellung des $ggT(a, b)$, aus der u. a. das inverse Element j einer Zahl $a \in \mathbb{N}$ $(mod\ m)$ bestimmt werden kann.

Die vorletzte Zeile des Euklidischen Algorithmus $a_{z-3} = x_{z-3} \cdot a_{z-2} + a_{z-1}$, in der a_{z-1} dem $ggT(a, b)$ gleichzusetzen ist, wird in $ggT(a, b) = a_{z-3} - x_{z-3} \cdot a_{z-2}$ umgeformt. Anhand der drittletzten Zeile des Euklidischen Algorithmus $a_{z-4} = x_{z-4} \cdot a_{z-3} + a_{z-2}$ wird der Ausdruck $a_{z-4} - x_{z-4} \cdot a_{z-3}$ für a_{z-2} gefunden und in vorherige Gleichung eingesetzt:

$$\begin{aligned} ggT(a, b) &= a_{z-3} - x_{z-3} \cdot a_{z-2} = \\ &= a_{z-3} - x_{z-3} \cdot (a_{z-4} - x_{z-4} \cdot a_{z-3}) = \\ &= -x_{z-3} \cdot a_{z-4} + (1 + x_{z-3} \cdot x_{z-4}) \cdot a_{z-3}. \end{aligned}$$

Nun wird stets ein a_i durch a_{i-1} und a_{i-2} ausgedrückt, wodurch man schlussendlich zu einem Ausdruck der Form $ggT(a, b) = g \cdot a_0 + h \cdot a_1$ mit $g, h \in \mathbb{Z}$ gelangt.

[20] Vgl. **Bundschuh** (2008), S. 22; **Oswald/Steuding** (2015), S. 67–68; **Reiss/Schmieder** (2014), S. 119–121.

Anhand des konkreten Beispiels $a = 60; b = 23$ wird jetzt der erweiterte Euklidische Algorithmus durchgeführt. Dafür wendet man zuerst den Euklidische Algorithmus zur Bestimmung der Startzeile an:

$$\begin{aligned} 60 &= 2 \cdot 23 + 14 \\ 23 &= 1 \cdot 14 + 9 \\ 14 &= 1 \cdot 9 + 5 \\ 9 &= 1 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

Der $ggT(a, b)$ beträgt also 1, und ist Startpunkt für den erweiterten Euklidischen Algorithmus. Dieser ergibt sich, wie beschrieben, aus einer Umformung der vorletzten Zeile des Euklidischen Algorithmus. In diesem konkreten Fall lautet sie $5 = 1 \cdot 4 + 1$, umgeformt $1 = 5 - 1 \cdot 4$. Die konkrete Durchführung des erweiterten Euklidischen Algorithmus anhand des Zahlenbeispiels sieht also wie folgt aus:

$$5 = 1 \cdot 4 + 1 \;\Leftrightarrow\; 1 = 1 \cdot 5 + (-1) \cdot 4$$

$$\begin{aligned} ggT(60, 23) = 1 &= 1 \cdot 5 + (-1) \cdot 4 \\ 1 &= (-1) \cdot 9 + 2 \cdot 5 \\ 1 &= 2 \cdot 14 + (-3) \cdot 9 \\ 1 &= (-3) \cdot 23 + 5 \cdot 14 \\ 1 &= 5 \cdot 60 + (-13) \cdot 23. \end{aligned}$$

Aus der Vielfachsummendarstellung der letzten Zeile kann man u. a. das inverse Element $j_a \equiv 5 \ (mod\ 23)$ von $a = 60$ sowie $j_b \equiv -13 \equiv 47 \ (mod\ 60)$ von $b = 23$ ablesen – eine für die weitere Arbeit, insbesonders für die Anwendung des Satzes von Euler-Fermat in der Kryptographie, das RSA-Verfahren, wichtige Tatsache.[21]

[21] Vgl. **Beutelspacher/Schwenk/Wolfenstetter** (2015), S. 159–160; **Bundschuh** (2008), S. 30–32; **Waldecker/Rempe-Gillen** (2016), S. 22–23; **Ziegenbalg** (2015), S. 46–47.

3 Der Kleine Satz von Fermat

Dieses Kapitel behandelt den Kleinen Satz von Fermat, der dem Satz von Euler-Fermat vorangegangen ist. Sein Entdecker Pierre de Fermat lebte im 17. Jahrhundert, galt als genialer Hobby-Mathematiker auf den verschiedensten Gebieten der Mathematik und befasste sich darüber hinaus mit physikalischen Phänomenen. Auch verfasste er die sogenannte Fermat'sche Vermutung, die ebenso als Großer Satz von Fermat bezeichnet wird, weshalb der Kleine Satz von Fermat als für die heutige Zahlentheorie unwichtigerer der beiden Lehrsätze die Bezeichnung „Klein" trägt.[22]

3.1 Der Satz

1640 formulierte Pierre de Fermat in einem Brief an seinen Freund und Mathematikerkollegen Bernard Frènicle de Bessy zum ersten Mal den Kleinen Satz von Fermat, jedoch ohne diesen zu beweisen. Deshalb gilt ein von Leonhard Euler 1736 veröffentlichter Beweis dieses Satzes durch vollständige Induktion als erster.[23]

Satz: Sei p eine Primzahl und $a \in \mathbb{N}$. Dann gilt:

(1) $a^p \equiv a \ (mod\ p)$.

Sei außerdem $ggT(a,p) = 1$. Dann gilt:

(2) $a^{p-1} \equiv 1 \ (mod\ p)$.

Betrachten wir nun zum besseren Verständnis das konkrete Beispiel $a = 8, p = 3$:

ad (1) $8^3 = 512 \equiv 8 \equiv 2 \ (mod\ 3)$.

ad (2) $8^{3-1} = 64 \equiv 1 \ (mod\ 3)$.

[22] Vgl. **Brückler** (2017), S. 146; **Mahoney** (2020); **Strick** (2008).
[23] Vgl. **Brückler** (2017), S. 146.

3.2 Beweis

Der Fall $p \mid a$ für (1) ist trivial: $0^p \equiv 0\,(mod\,p)$. Folglich werden die Beweise für (1) und (2) mit $a \not\equiv 0\,(mod\,p)$ geführt. Dazu seien $x_1, x_2, ..., x_{p-1}$ definiert als:

$$\begin{aligned} x_1 &= 1 \cdot a \\ x_2 &= 2 \cdot a \\ &... \\ x_{p-1} &= (p-1) \cdot a. \end{aligned}$$

Nun ist zu zeigen, dass $x_1, x_2, ..., x_{p-1}$ modulo p paarweise verschieden sind und in Folge alle Restklassen modulo p, ausgenommen der Restklasse K_0, für deren Elemente k_i $(\in K_0) \equiv 0\,(mod\,p)$ gilt, abbilden:

Seien also $l, m \in \mathbb{N}$ mit $1 \leq l, m \leq p-1 \wedge l \neq m$. Die Annahme des indirekten Beweises laute $x_l \equiv x_m\ (mod\ p)$, also $l \cdot a \equiv m \cdot a\ (mod\ p)$. Da aus $a \not\equiv 0\,(mod\,p)$ folgt, dass der $ggT(a, p) = 1$ ist, gilt somit außerdem $l \equiv m\ (mod\ p)$.

Dies steht jedoch im Widerspruch zu den Bedingungen $1 \leq l, m \leq p-1 \wedge l \neq m$, da die Zahlen $1, 2, ..., l, m, ..., (p-2), (p-1)$ modulo p betrachtet paarweise verschieden sind. Folglich existieren keine zwei Zahlen l und m, für die x_l und x_m in der gleichen Restklasse modulo p liegen. Deswegen stellen die $(p-1)$ Zahlen $x_1, x_2, ..., x_{p-1}$ alle primen Restklassen modulo p dar. Daher gilt:

$$\begin{aligned} x_1 \cdot x_2 \cdot ... \cdot x_{p-1} &\equiv 1 \cdot 2 \cdot ... \cdot (p-1) \quad (mod\ p) \\ 1a \cdot 2a \cdot ... \cdot (p-1)a &\equiv 1 \cdot 2 \cdot ... \cdot (p-1) \quad (mod\ p) \\ a^{p-1} \cdot (p-1)! &\equiv (p-1)! \quad (mod\ p). \end{aligned}$$

Da weiters jeder einzelne Faktor von $(p-1)!$ zu p teilerfremd ist und somit auch $(p-1)!$ keinen gemeinsamen Teiler mit p besitzt, gilt $a^{p-1} \equiv 1\,(mod\,p)$ und damit $a^p \equiv a\ (mod\ p)$.[24]

□

[24] Vgl. **Reiss/Schmieder** (2014), S. 188–189.

4 Der Satz von Euler-Fermat

In diesem Kapitel wird der Satz von Euler-Fermat, das Herzstück dieser Arbeit, behandelt. Dazu wird nach einer historischen Betrachtung Leonhard Eulers zuerst die Euler'sche Phi-Funktion $\Phi(n)$ eingeführt und danach der Satz von Euler-Fermat selbst sowie ein Beweis dessen angeführt.

4.1 Historisches zu Leonhard Euler

Leonhard Euler ist eine Persönlichkeit, die sowohl für ihre wissenschaftlichen Leistungen als auch für ihren Charakter gerühmt wurde und wird. So soll er neben seinen weit gefächerten Tätigkeiten auf dem Gebiet der Wissenschaft ein ruhiges und ausgeglichenes Temperatment gehabt haben, stets heiter, gesellig und mit einem offenen Gemüt ausgestattet. Einzig bei Diskussionen um und über die Religion reagierte er aufgrund seiner Strenggläubigkeit manchmal aufbrausend. Zeitzeuginnen und Zeitzeugen berichten darüber hinaus von der einzigartigen Konzentrationsfähigkeit Eulers, der laut diesen sogar mit einem Kleinkind auf dem Schoß arbeiten konnte.[25]

1707 wird Leonhard Euler als Erstgeborener und Sohn des protestantischen Pfarrers Paul Euler und Margaretha Brucker geboren. Er genießt zuerst elementaren Unterricht bei seinen Vater, lernt dann an der Lateinschule in Basel und wird nebenbei privat von Johannes Burckhardt, der laut Daniel Bernoulli großen Einfluss auf den kleinen Euler gehabt haben soll, in der Kunst der Mathematik unterwiesen. Im Alter von zarten 13 Jahren immatrikuliert er an der Basler Universität, was für damalige Verhältnisse jedoch normal ist, um die „prima laurea“, einen in etwa der heutigen Matura bzw. Hochschulreife entsprechenden Abschluss, zu erwerben. Danach studiert er nach Abbruch eines Theologie-Studiums Mathematik, wobei er beim damals sehr berühmten Mathematikprofessor Johann Bernoulli lernt und sich durch seine mathematischen Arbeiten dessen Wohlwollen und Respekt erwirbt.[26]

[25] Vgl. **Fellmann** (1995), S. 9; **Wußing** (2008), S. 45.
[26] Vgl. **Bernoulli** (1743); **Calinger** (2016), S. 14–37; **Fellmann** (1995), S. 16–25; **Wußing** (2008), S. 47–48.

Im Jahre 1726 erfolgt ein Ruf der Petersburger Akademie an Leonhard Euler, dem er 1727 folgt. Dort bekommt er 1731 eine Stelle als Professor der Physik und 1733 zusätzlich eine Professur für Mathematik. In der Zeit seiner Professur in Petersburg[27] verfasst er seine ersten Hauptwerke, die zweiteilige „Mechanica“ (1736), die ebenfalls zweibändige „Rechenkunst“ (1738/1740) und das „Tentamen novae theoriae musicae“ (1739), ein musiktheoretisches Werk. Aber auch die nach ihm benannte Euler'sche Zahl $e \approx 2,7182818$ erforscht und bestimmt er in seiner ersten Petersburger Schaffensphase.

Im Jahr 1735 leidet Leonhard Euler an einer lebensgefährdenden Infektionskrankheit, die ihn, dem heutigen Wissenstand nach, 1738 erneut heimsucht und ihn des Augenlichts seines rechten Auges beraubt.[28]

Nach dem Tod Anna Iwanownas kommt es in Russland zu politischen Unsicherheiten, woraufhin Euler 1741 beschließt, Petersburg zu verlassen, und nach Berlin zu gehen, um dort zuerst der Sozietät, einer Vorgängerin der Berliner Akademie, beizutreten und sich 1746 letzterer anzuschließen. So verlegt Leonhard Euler sein Lebenszentrum für das nächste Vierteljahrhundert nach Preußen, das unter der Führung Friedrich II. steht. Hier beschäftigt er sich mit zahlreichen, vorwiegend mathematischen und physikalischen Problemen und schafft weitere Werke, die wesentlich zur Entwicklung der Wissenschaft beitrugen. Auf dem Gebiet der Zahlentheorie kann er viele Vermutungen anderer Mathematikerinnen und Mathematiker widerlegen und andere, wie u. a. auch den zentralen Satz dieser Arbeit, den Satz von Euler-Fermat und zuvor den Kleinen Satz von Fermat, beweisen. Aufgrund von ausufernden Meinungsverschiedenheiten zwischen Euler und Friedrich II. sowie der Tatsache, dass Friedrich II. Euler als bedeutendsten Mathematiker seiner Zeit nicht zum Präsidenten der Berliner Akademie ernennen will, entschließt sich Euler 1766 Berlin in Richtung Petersburg zu verlassen.[29]

An der Petersburger Akademie verbringt der nahezu erblindete Leonhard Euler in finanzieller Sicherheit sein restliches Leben und vervollständigt sein dem Fortschritt der Wissenschaft so dienliches Lebenswerk, bis er am 18. September 1783 an einem Schlaganfall verstirbt.[30]

[27] heute: Sankt Petersburg
[28] Vgl. **Calinger** (2016), S. 88–89; **Fellmann** (1995), S. 30; **Wußing** (2008), S. 48–51.
[29] Vgl. **Fellmann** (1995), S. 57–102; **Wußing** (2008), S. 65–66.
[30] Vgl. **Calinger** (2016), S. 451–532; **Fellmann** (1995), S. 103–119.

Leonhard Eulers Tod war ein großer Verlust für die Wissenschaft, da er als insbesonders auf dem Gebiet der Mathematik und der Physik brillanter Wissenschaftler die Forschung der Menschheit wesentlich vorangetrieben und zahlreiche Wege für zukünfitge Entwicklungen in verschiedenen wissenschaftlichen Teilbereichen geebnet hat. Neben den schon genannten seien nun noch ein paar ausgewählte Entdeckungen seiner Genialität erwähnt: Euler ergründet neben seiner Entdeckung der Euler'schen Gerade, die durch den Höhenschnittpunkt, den Schwerpunkt und den Umkreismittelpunkt eines Dreiecks verläuft, auch das Königsberger Brückenproblem, stellt den Euler'schen Polyedersatz auf, der die Anzahl der Ecken, Flächen und Kanten eines Polyeders zueinander in Bezug setzt und entdeckt, nachdem er die schon erwähnte Euler'sche Zahl e bestimmt hat, die in der Natur und folglich in den Naturwissenschaften eine essentielle Rolle spielt, eine Beziehung zwischen den für die Mathematik wichtigsten Zahlen $0, 1, \pi, i$ *und* e, die Euler'sche Identität, die häufig als schönste Formel der Mathematik gepriesen wird. Sie lautet $e^{i\pi} + 1 = 0$.[31]

[31] Vgl. **Vollrath**.

4.2 Die Euler'sche Phi-Funktion $\Phi(n)$

Die Euler'sche Phi-Funktion $\Phi(n)$ ist eine von Leonhard Euler eingeführte von $n \in \mathbb{N}$ abhängige Funktion, welche die Anzahl der zu n teilerfremden Zahlen zwischen 1 und n angibt, was der Anzahl primer Restklassen modulo n entspricht. Er führte sie ein, um den Satz von Euler-Fermat in der Art und Weise, in der wir ihn kennen, formulieren zu können.

Für $n \in \mathbb{N}$ sei $R_n := \{1; 2; ...; (n-1)\}$ die Menge aller positiven Reste beim Teilen durch n und $R'_n := \{k \in \mathbb{N} \mid k \in R_n \ \wedge \ ggT(n,k) = 1\}$ die Menge aller zu n teilerfremden Zahlen aus R_n.
Die Euler'sche Phi-Funktion ist wie folgt definiert:

$$\Phi(n) = \lfloor R'_n \rfloor.$$

Dies entspricht der Mächtigkeit, also der Anzahl an Elementen der Menge R'_n.[32]

Zur Veranschaulichung sei ein konkretes Beispiel angeführt. Wir untersuchen $\Phi(n)$ mit $n = 12$. Dabei ergibt sich $R_{12} = \{1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11\}$ und $R'_{12} = \{1; 5; 7; 11\}$. Da R'_{12} vier Elemente enhält, ist $\lfloor R'_{12} \rfloor = \Phi(12) = 4$.

In der nun folgenden Abbildung (Abb. 1) sind die Werte der Phi-Funktion für die ersten 99 natürlichen Zahlen $\mathbb{N}\backslash\{0\}$ enthalten. Dabei gibt die Zeile eines Werts $\Phi(n)$ die Zehnerstelle und die Spalte die Einerstelle von n an. Auch graphisch lässt sich die Phi-Funktion $\Phi(n)$ darstellen. In der im Anschluss zu sehenden Graphik (Abb. 2) wurden die natürlichen Zahlen $1 \leq n \leq 1000$ gegen ihren $\Phi(n)$-Wert aufgetragen. Anhand der oberen Punkte, die man zu einer Geraden verbinden könnte und die in ihrer Gesamtheit wie eine Diagonale durch den gezeigten Ausschnitt der graphisch dargestellten Phi-Funktion verlaufen, kann man sehr schön erkennen, dass für eine Primzahl $\Phi(p) = (p-1)$ gilt.

[32] Vgl. **Bundschuh** (2008), S. 48; **Strick** (2020), S. 278–279.

φ(n)	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
00+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Abbildung 1: Werte von $\Phi(n)$ für $1 \leq n \leq 99$

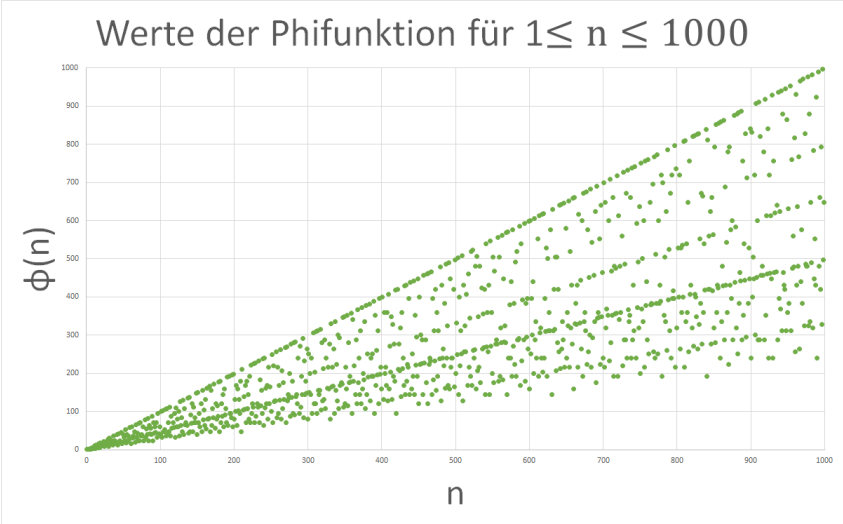

Abbildung 2: Graphische Darstellung der Phi-Funktion

4.3 Eigenschaften der Phi-Funktion $\Phi(n)$

Nun sollen die Eigenschaften der Euler'schen Phi-Funktion genau beleuchtet werden, um mit diesem Wissen die Bedeutung und Folgen des Satzes von Euler-Fermat verstehen zu können. Nach der allgemeinen Beschreibung jeder Eigenschaft der Phi-Funktion wird stets ein Beispiel (Bsp.) zur Veranschaulichung angeführt. Ein Blick auf die Abbildung 1, die alle Werte der Phi-Funktion von 1 bis 99 zeigt, kann zum Vergleichen hilfreich sein. Die inhaltlich zitierte Literatur dieses Unterkapitels ist am Ende dieses Absatzes vermerkt, um eine klare Unterscheidung zwischen Hochzahlen und Fußzeilenverweisen zu gewährleisten.[33]

- $\Phi(p) = p - 1$ mit $p \in \mathbb{P}$ (= Menge der Primzahlen).

  Dies gilt, da für alle Zahlen $l \in \mathbb{N}\backslash\{0\} < p$ laut Definition einer Primzahl $ggT(l, p) = 1$ gilt. □

  Bsp: $\Phi(7) = 6$ mit $R_n = R'_n = \{1; 2; 3; 4; 5; 6\}$.

- $\Phi(p^k) = p^k - p^{k-1}$ für $\forall\ k \in \mathbb{N}$ mit $p \in \mathbb{P}$.

  Die Begründung hierfür lautet: $p^k = p \cdot p^{k-1} \Rightarrow$ Es gibt p^{k-1} paarweise voneinander verschiedene $z_i \in \mathbb{N}$ mit $1 \leq z_i \leq p^k$, für die $z_i \equiv 0\ (mod\ p)$ gilt. Die restlichen z_i sind nicht kongruent 0 $(mod\ p)$ und folglich teilerfremd zu p^k. □

  Bsp: $\Phi(3^4) = 81 - 27 = 54$.

- $\Phi(p \cdot q) = (p-1) \cdot (q-1) = \Phi(p) \cdot \Phi(q)$ für $p, q \in \mathbb{P}$.

  Zur Beweisführung betrachten wir folgende $p \times q$ - Tabelle, die alle Zahlen $z_i \in \mathbb{N}$ nach ihrer Form $z_i = v_i \cdot p + r_i$ mit $v_i, r_i \in \mathbb{N} : 1 \leq r_i \leq p \wedge 1 \leq v_i \leq q-1$ ordnet. Wie der Tabelle zu entnehmen ist, liegen alle Zahlen einer Spalte in derselben Restklasse modulo p, weil gilt: $ggT(v_i \cdot p + r_i, p) = ggT\left((v_i - 1) \cdot p + r_i, p\right) = ... = ggT(r_i, p)$. Außerdem bildet eine Zeile die Restklassen modulo p exakt so ab, dass jede genau einmal vorkommt. Da für alle Zahlen z_i, die nicht kongruent 0 modulo p sind, der $ggT(z_i, p) = 1$ ist, gibt es $(p-1) = \Phi(p)$ Spalten, deren Zahlen allesamt teilerfremd zu p sind.

[33] Vgl. **Bundschuh** (2008), S. 48–49; **Ziegenbalg** (2015), S. 109–111.

1	2	3	...	p
$p+1$	$p+2$	$p+3$	...	$2p$
$2p+1$	$2p+2$	$2p+3$	...	$3p$
$3p+1$	$3p+2$	$3p+3$	...	$4p$
...	...	...	...	...
$(q-1)\cdot p+1$	$(q-1)\cdot p+2$	$(q-1)\cdot p+3$	...	$q\cdot p$

Tabelle 1: Tabellarische Anordnung der $z_i \in \mathbb{N}$ nach den Parametern p und q

Außerdem sind die z_i einer Spalte modulo q paarweise verschieden, woraus folgt, dass sie exakt alle Restklassen modulo q abbilden. Denn wäre $v_1 \cdot p + r_1 \equiv v_2 \cdot p + r_2 \ (mod\ q)$ mit $v_1 \neq v_2$, woraus $v_1 \cdot p \equiv v_2 \cdot p \ (mod\ q)$ folgt, ergäbe sich daraus wegen der Teilerfremdheit von p und q das Kongruenzverhältnis $v_1 \equiv v_2 \ (mod\ q)$, weswegen $v_1 = v_2$ gelten müsste, da diese beiden Zahlen zwischen 0 und $(q-1)$ liegen. Dies steht jedoch im Widerspruch zu der anfänglichen Annahme, dass $v_1 \neq v_2$.

Somit verkörpern auch die Zahlen z_i einer jeden der $(p-1)$ Spalten, deren Zahlen teilerfremd zu p sind, genau alle Restklassen modulo q, woraus folgt, dass pro Spalte $q-1 = \Phi(q)$ Zahlen z_i vorhanden sind, für die $ggT(z_i, q) = 1$ gilt. Deswegen gibt es genau $(p-1)\cdot(q-1) = \Phi(p)\cdot\Phi(q)$ Zahlen $z_i \leq p \cdot q$, die teilerfremd zu $p \cdot q$ sind, was wiederum $\Phi(p \cdot q)$ entspricht. □

Bsp: $\Phi(35) = \Phi(5 \cdot 7) = 4 \cdot 6 = \Phi(5) \cdot \Phi(7) = 24$.

- $\Phi(m \cdot n) = \Phi(m) \cdot \Phi(n)$ für $m, n \in \mathbb{N}$ mit $ggT(m, n) = 1$.

  Diese Eigenschaft der Phi-Funktion ist eine Erweiterung der zuvor beschriebenen. Um sie zu belegen, sehen wir uns noch einmal etwas modelliert die obige Tabelle an. Es gilt fortan: $z_i = v_i \cdot n + r_i$ mit $v_i, r_i \in \mathbb{N} : 1 \leq r_i \leq n \ \wedge \ 1 \leq v_i \leq m-1$.

1	2	3	...	n
$n+1$	$n+2$	$n+3$	...	$2n$
$2n+1$	$2n+2$	$2n+3$	...	$3n$
$3n+1$	$3n+2$	$3n+3$	...	$4n$
...	...	...	...	...
$(m-1)\cdot n+1$	$(m-1)\cdot n+2$	$(m-1)\cdot n+3$	...	$m\cdot n$

Tabelle 2: Tabellarische Anordnung der $z_i \in \mathbb{N}$ nach den Parametern m und n

Die Beweise der Tatsachen, dass jede Zeile exakt die Restklassen modulo n und jede Spalte genau jene modulo m beinhaltet, sind (mit n statt $p \ \wedge \ m$ statt q) analog zum Beweis der vorhergehenden Eigenschaft zu führen. Der Unterschied in der Beweisführung besteht darin, dass nicht alle bis auf eine ($z_i \equiv 0$) dieser Restklassen teilerfremd zu n bzw. m sind, da n, m nicht zwingend prim sind:
Da alle Zahlen z_i einer Spalte modulo n kongruent zueinander sind und die Zahlen der ersten Zeile die Restklassen modulo n exakt wiederspiegeln, existieren genau $\Phi(n)$ Spalten, deren Zahlen z_i teilerfremd zu n sind. Analoges gilt für die Zeilen modulo m: Es gibt $\Phi(m)$ Zeilen, deren Zahlen z_i alle teilerfremd zu m sind. Daraus folgt, dass es $\Phi(m)\cdot\Phi(n)$ Zahlen z_i in der gesamten Tabelle und somit unter den ersten $m\cdot n$ natürlichen Zahlen ohne 0 gibt, für die $ggT(z_i, n) = 1 = ggT(z_i, m)$ gilt, was $\Phi(m\cdot n)$ entspricht. $\square$

Bsp: $\Phi(60) = \Phi(4 \cdot 15) = \Phi(4) \cdot \Phi(15) = (2^2 - 2^1) \cdot ((3^1 - 3^0) \cdot (5^1 - 5^0)) = 2 \cdot 8 = 16.$

- Allgemein kann die Anzahl der primen Restklassen einer beliebigen Zahl $a \in \mathbb{N}$, für die $a \geq 2$ gilt, anhand ihrer Primfaktoren $p_1, p_2, ..., p_n$ mit $n \in \mathbb{N}$ wie folgt berechnet werden:

$$\begin{aligned}\Phi(a) &= \Phi\left(p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_n^{k_n}\right) = \\ &= \Phi\left(p_1^{k_1}\right) \cdot \Phi\left(p_2^{k_2}\right) \cdot ... \cdot \Phi\left(p_n^{k_n}\right) = \\ &= \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdot \left(p_2^{k_2} - p_2^{k_2-1}\right) \cdot ... \cdot \left(p_n^{k_n} - p_n^{k_n-1}\right).\end{aligned}$$

Bsp: $\Phi(60) = \Phi(2^2 \cdot 3^1 \cdot 5^1) = \Phi(2^2) \cdot \Phi(3^1) \cdot \Phi(5^1) = (2^2 - 2^1) \cdot (3^1 - 3^0) \cdot (5^1 - 5^0) = 2 \cdot 2 \cdot 4 = 16.$

4.4 Der Satz

Leonhard Euler beweist 1736 nicht nur als erster allgemein den Kleinen Satz von Fermat, sondern kann dieses Kongruenzverhältnis, das von Fermat erstmals entdeckt und für einige einzelne Zahlenwerte gezeigt wurde, von der Beschränkung auf Primzahlen hin zu den ganzen Zahlen verallgemeinern.[34]

Eulers Verallgemeinerung des Kleinen Satzes von Fermat lautet:

$$a^{\Phi(m)} \equiv 1 \ (mod \ m)$$

$$\text{mit } a \in \mathbb{Z} \wedge m \in \mathbb{N}\backslash\{0\} \wedge ggT(a,m) = 1.$$

Zur Veranschaulichung seien in Folge Beispiele (Bsp.) gegeben.

Bsp. 1 $(a = 3; m = 4)$: $3^{\Phi(4)} = 3^2 \equiv 1 \ (mod \ 4)$.

Bsp. 2 $(a = 2; m = 7)$: $2^{\Phi(7)} = 2^6 \equiv 1 \ (mod \ 7)$.

[34] Vgl. **Brückler** (2017), S. 146.

4.5 Beweis

Seien $x_1, x_2, ..., x_{\Phi(m)}$ die zu m teilerfremden Zahlen von 1 bis m mit $x_1 < x_2 < ... < x_{\Phi(m)}$. Für a und m gelte weiterhin: $a \in \mathbb{Z}$, $m \in \mathbb{N}\backslash\{0\}$ und Teilerfremdheit.
Man setze nun $y_1 := a \cdot x_1;\ y_2 := a \cdot x_2;\ ...;\ y_{\Phi(m)} := a \cdot x_{\Phi(m)}$.

Behauptung 1: $ggT(y_j, m) = 1$ mit $1 \leq j \leq \Phi(m)$.

Direkter Beweis: $ggT(y_j, m) = ggT(a \cdot x_j, m) = 1$
wegen: $ggT(a, m) = ggT(x_j, m) = 1$.

Behauptung 2: Für $j \neq k$ mit $j, k \in \mathbb{N} : 1 \leq j, k \leq \Phi(m)$ gilt $y_j \not\equiv y_k \ (mod\ m)$.

Indirekter Beweis mit folgender Annahme:

$$\begin{aligned} y_j &\equiv y_k \ (mod\ m) \\ a \cdot x_j &\equiv a \cdot x_k \ (mod\ m) \\ x_j &\equiv x_k \ (mod\ m). \end{aligned}$$

Da ein Inverses j zu a $(mod\ m)$ existiert, ergibt sich ein Widerspruch zu $x_j \neq x_k \wedge 1 \leq x_j, x_k \leq m$.

Wir wissen also, dass $y_1, y_2, ..., y_{\Phi(m)}$ genauso wie $x_1, x_2, ..., x_{\Phi(m)}$ exakt alle Repräsentanten primer Restklassen modulo m widerspiegeln. Daraus folgt:

$$\begin{aligned} y_1 \cdot y_2 \cdot ... \cdot y_{\Phi(m)} &\equiv x_1 \cdot x_2 \cdot ... \cdot x_{\Phi(m)} \ (mod\ m) \\ (a \cdot x_1) \cdot (a \cdot x_2) \cdot ... \cdot (a \cdot x_{\Phi(m)}) &\equiv x_1 \cdot x_2 \cdot ... \cdot x_{\Phi(m)} \ (mod\ m) \\ a^{\Phi(m)} \cdot x_1 \cdot x_2 \cdot ... \cdot x_{\Phi(m)} &\equiv x_1 \cdot x_2 \cdot ... \cdot x_{\Phi(m)} \ (mod\ m). \end{aligned}$$

Weil $x_1, x_2, ..., x_{\Phi(m)}$ teilerfremd zu m sind, ist auch $x_1 \cdot x_2 \cdot ... \cdot x_{\Phi(m)}$ teilerfremd zu m. Folglich existiert ein inverser Rest für $x_1 \cdot x_2 \cdot ... \cdot x_{\Phi(m)}$ $(mod\ m)$. Nach Multiplikation mit dem Inversen von $x_1 \cdot x_2 \cdot ... \cdot x_{\Phi(m)}$ folgt schlussendlich $a^{\Phi(m)} \equiv 1 \ (mod\ m)$.[35] $\square$

[35] Die Beweisführung basiert auf einer Mitschrift des Autors bei einem Online-Vortrag zum Thema „Zahlentheorie – Der Satz von Euler Fermat“ von Clemens Heuberger im April 2020. Für ähnliche Beweisführungen aus der Literatur siehe: **Bartholomé/Rung/Kern** (2008), S. 127; **Bundschuh** (2008), S. 97–98; **Löh/Kilbertus/Krauss** (2019), S. 127; **Ziegenbalg** (2015), S. 113–114.

5 Anwendung in der Kryptographie

Neben der Tatsache, dass der Satz von Euler-Fermat wesentlich zur Weiterentwicklung der Zahlentheorie beigetragen hat, da einige mathematische Erkenntnisse, wie der Satz von Wilson oder das Quadratische Reziprozitätsgesetz, auf ihm aufbauen, liegt auch eine kryptographische Anwendung des Lehrsatzes vor: das RSA-Verfahren.

Um in diese Methode der Verschlüsselung bestmöglich einzuführen, wird in Folge auf die Mittel und Ziele der Kryptographie eingegangen sowie eine Einteilung dieser vorgenommen. Daraufhin wird das RSA-Verfahren selbst behandelt.

Die mathematischen Grundlagen dieses Kapitels sind zu einem Großteil schon in den zuvorgegangenen Kapiteln erläutert worden. Falls im Laufe dieses Kapitels jedoch mathematische Prinzipien oder kryptographische Begrifflichkeiten erläuterungsbedürftig erscheinen, sind deren Erklärungen im Glossar zu finden.

Auf eine historische Betrachtung der Kryptographie, aber auch auf Betrachtungen anderer kryptographischer Verfahren wird verzichtet, um den Rahmen dieser vorwissenschaftlichen Arbeit nicht zu sprengen. Interessierten ist die in der Fußnote angegebene Literatur zur historischen Entwicklung der Verschlüsselungstechniken sowie ein Blick ins Literaturverzeichnis zu empfehlen.[36]

[36] Vgl. **Beutelspacher** (2015); **Beutelspacher** (2013); **Pincock/Frary** (2007); **Schmeh** (2010).

5.1 Kryptographie – Was ist das?

Der Begriff „Kryptographie“ leitet sich von den griechischen Wörtern „kryptein“ und „graphein“ ab und bedeutet somit wörtlich übersetzt „Verstecktes Schreiben“. Man versteht darunter die Lehre der Verschlüsselung von Daten.[37]

Etwas ausführlicher beschrieben, bezeichnet die Kryptographie die Wissenschaft, die versucht Methoden zu finden, um Unbefugten den Zugriff auf vertrauliche Daten zu verwehren. Dabei greift sie auf die beiden Hilfsmittel Mathematik und Computertechnologie zurück, um derartige Verschlüsselungsverfahren zu ergründen und sieht von physikalischen oder steganographischen Maßnahmen zur Geheimhaltung einer Kommunikation ab.[38]

Der Gegenbegriff zur Kryptographie ist die Kryptoanalyse. Sie verfolgt das Ziel, geheime, verschlüsselte Nachrichten abzufangen und zu entschlüsseln. Der Überbegriff dieser beiden Fachgebiete ist die Kryptologie.[39]

Die Kryptographie lässt sich abermals nach verschiedenen Kriterien unterteilen. Eine mögliche Unterteilung ist jene nach der Art der Verschlüsselung. Hierbei werden die symmetrischen Chiffren, die asymmetrischen Chiffren und die Protokolle, eine Mischung aus den beiden zuvor erwähnten, unterschieden.[40] Eine weitere Möglichkeit der Unterteilung ist die Einteilung der Kryptographie nach den verfolgten Sicherheitszielen, die auch als Sicherheitsdienste bezeichnet werden. Dazu zählen die Vertraulichkeit, die Integrität, die Authentizität, die Verbindlichkeit, die Anonymität und die Zugriffskontrolle.[41]

[37] Vgl. **Schmeh** (2016), S. 9.
[38] Vgl. **Schmeh** (2016), S. 9–10.
[39] Vgl. **Paar/Pelzl** (2016), S. 2; **Schmeh** (2016), S. 11.
[40] Vgl. **Buchmann** (2016), S. 73–77; **Schmeh** (2016), S. 427–429.
[41] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 2–10; **Spitz/Pramateftakis/Swoboda** (2011), S. 14–19; **St. Denis/Johnson** (2017), S. 25–31.

5.2 Das RSA-Verfahren

In diesem Kapitel wird die Anwendung des Satzes von Euler-Fermat im Konkreten behandelt. Dazu werden nach einer kurzen Einführung die Schlüsselerzeugung, der Ver- und Entschlüsselungsvorgang, das Signaturverfahren und die Sicherheit des RSA-Verfahrens sowie Angriffe darauf beleuchtet.

Der RSA-Algorithmus ist eine nach seinen Erfindern R. Rivest, A. Shamir und L. Adleman benannte Methode der Verschlüsselung nach dem Public-Key-Prinzip. Die drei Wissenschaftler erfanden ihn im Jahr 1978, als sie versuchten, die Unmöglichkeit eines asymmetrischen Verschlüsselungsverfahrens zu beweisen.[42]

Das RSA-Verfahren beruht auf dem Prinzip, jeder Teilnehmerin bzw. jedem Teilnehmer einer Kommunikation einen privaten und einen öffentlichen Schlüssel zuzuteilen. Mithilfe des öffentlichen Schlüssels einer Person Bob können alle eine an ihn adressierte Nachricht verschlüsseln. Entschlüsseln kann diese Botschaft anschließend nur noch Bob mit seinem privaten Schlüssel. Es bietet sich also ein Vergleich mit unserem Briefkastensystem an: Jede bzw. jeder kann in Bobs Briefkasten einen Brief einwerfen, aber nur er besitzt den Schlüssel, um den versperrten Briefkasten zu öffnen.[43]

Verwendung findet die RSA-Verschlüsselung hauptsächlich bei der Erstellung digitaler Signaturen und als sicherer Kanal zur Passwortübermittlung von symmetrischen Verfahren. Da der RSA-Algorithmus jedoch wesentlich mehr Rechenleistung benötigt als herkömmliche symmetrische Verschlüsselungsmethoden, wie der AES- oder der 3DES-Algorithmus[44], wird er nur bedingt zur Verschlüsselung ganzer Nachrichten verwendet.[45]

[42] Vgl. **Beutelspacher/Schwenk/Wolfenstetter** (2015), S. 19.
[43] Vgl. **Paar/Pelzl** (2016), S. 3–4; **Spitz/Pramateftakis/Swoboda** (2011), S. 2; **Wätjen** (2018), S. 4.
[44] Für weitere Informationen zu diesen Verfahren siehe folgende Literatur: **Buchmann** (2016), S. 135–153; **Manz** (2019), S. 32–51; **Paar/Pelzl** (2016), S. 63–140.
[45] Vgl. **Paar/Pelzl** (2016), S. 199–200; **Schmeh** (2016), S. 204.

5.2.1 Die Schlüsselerzeugung

Bevor jemand einer Person Bob eine mit dem RSA-Verfahren verschlüsselte Nachricht schicken kann, braucht dieser sowohl einen öffentlichen als auch einen privaten Schlüssel. Um diese beiden so zu erstellen, dass man vom öffentlichen Schlüssel nicht auf den privaten schließen kann, was eine Voraussetzung für dessen Sicherheit ist, greift der RSA-Algorithmus auf den Satz von Euler-Fermat zurück.

Für das Generieren von Bobs Schlüssel werden zwei sehr große Primzahlen p und q gewählt. Da es keine allgemeine Formel zur Berechnung von Primzahlen gibt, werden solange zufällig auserwählte Zahlen mithilfe von Primzahltests auf ihre Primzahleigenschaften überprüft, bis zwei Primzahlen gefunden sind. Daraufhin werden p und q miteinander multipliziert, sodass man die Zahl $p \cdot q = n \in \mathbb{N}$ erhält. Nun gilt mit den Voraussetzungen $m < n \ \wedge \ m, k \in \mathbb{N}$ laut dem Satz von Euler-Fermat Folgendes:

$$
\begin{aligned}
& m^{\Phi(n)} \equiv 1 \ (mod\ n) && / \ \hat{} k \\
& (m^{\Phi(n)})^k \equiv 1^k \ (mod\ n) && \\
& m^{\Phi(n) \cdot k} \equiv 1 \ (mod\ n) && / \cdot m \\
& m^{k \cdot \Phi(n) + 1} \equiv m \ (mod\ n). &&
\end{aligned}
$$

Da $\Phi(n) = \Phi(p \cdot q) = (p-1) \cdot (q-1) \wedge m < n$ ist, gilt $m^{k \cdot (p-1) \cdot (q-1) + 1} \ (mod\ n) = m$.

Um die Schlüsselerzeugung zu finalisieren, wird ein beliebiges $e \in \mathbb{N}$ gewählt, sodass $ggT(e, \Phi(n)) = 1$ ist, und mithilfe des erweiterten Euklidischen Algorithmus ein $d \in \mathbb{N}$ bestimmt, sodass $e \cdot d \equiv 1 \ (mod\ \Phi(n))$ gilt. Dies ist mit dem Ausdruck $e \cdot d = k \cdot \Phi(n) + 1 = k \cdot (p-1) \cdot (q-1) + 1$ gleichzusetzen. Eingesetzt in die vorherige Gleichung ergibt sich $m^{e \cdot d} \ (mod\ n) = m$. Dies kann auch als $(m^e)^d \ (mod\ n) = m$ formuliert werden.

Die beiden Zahlen e und n werden nun als öffentlicher Schlüssel bekanntgegeben und d und n als privater Schlüssel verwendet. Die Zahlen p, q und $\Phi(n)$ sind auf jeden Fall geheim zu halten oder zu vernichten, da eine angreifende Person aus ihnen sofort den privaten Schlüssel Bobs berechnen könnte und die Zahlen für den laufenden Verschlüsselungsbetrieb nicht mehr benötigt werden.[46]

[46] Vgl. **Beutelspacher/Schwenk/Wolfenstetter** (2015), S. 19–20; **Paar/Pelzl** (2016), S. 202–206; **Wätjen** (2018), S. 77.

5.2.2 Verschlüsseln und Entschlüsseln

Wie bereits erwähnt kann nach beschriebener Schlüsselerzeugung jede und jeder Bob eine RSA-verschlüsselte Nachricht schicken. Wie das funktioniert, wird in Folge anhand eines Ver- und Entschlüsselungsvorgangs erklärt.

Alice will Bob eine mithilfe des RSA-Logarithmus verschlüsselte Nachricht m schicken. Sie verwendet dazu Bobs öffentlichen Schlüssel $(e \mid n)$ und chiffriert den Klartext m, um den Geheimtext c zu erhalten: $c = (m)^e \ (mod\ n)$. Daraufhin schickt Alice den Geheimtext an Bob. Dieser benutzt seinen privaten Schlüssel $(d \mid n)$, um c zu entschlüsseln, und erhält wieder die ursprünglich von Alice verfasste Nachricht: $c^d \ (mod\ n) = (m^e)^d \ (mod\ n) = m$.

Damit ist nicht nur der Ver- und Entschlüsselungsvorgang detailliert beschrieben, sondern auch die Korrektheit des RSA-Verfahrens bewiesen.[47]

5.2.3 Das Signaturverfahren

Da der RSA-Algorithmus aktuell oft zur Erzeugung digitaler Signaturen verwendet wird, wird diese folgend erklärt.

Eine digitale Signatur hat zum Ziel, die Verfasserin Alice einer Nachricht eindeutig identifizieren zu können. Die Erstellung einer solchen ist mithilfe des RSA-Verfahrens möglich, in dem Alice den Klartext m zuerst mit ihrem eigenen privaten Schlüssel g verschlüsselt und danach einen normalen RSA-Chiffriervorgang mit Bobs öfffentlichem Schlüssel e durchführt: $c = (m^g)^e$. Nach Erhalten des Geheimtextes c dechiffriert Bob diesen mit seinem privaten Schlüssel d: $c^d = ((m^g)^e)^d = m^g$. Nun hat er die mit Alice' privatem Schlüssel chiffrierte Botschaft m^g vor sich. Diese entschlüsselt er mithilfe deren öffentlichen Schlüssels. Dabei erhält Bob den ursprünglichen Klartext m sowie den Nachweis, dass die Nachricht tatsächlich von Alice stammt, da nur diese ihren privaten Schlüssel kennt.[48]

[47] Vgl. **Beutelspacher/Schwenk/Wolfenstetter** (2015), S. 19; **Schmeh** (2016), S. 204–206; **Wätjen** (2018), S. 77–78.
[48] Vgl. **Beutelspacher** (2015), S. 134; **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 124.

5.2.4 Sicherheit des RSA-Verfahrens

Die Sicherheit des RSA-Verfahrens beruht auf seiner Public-Key-Eigenschaft, die sich aus dem Faktorisierungsproblem ergibt. Dieses bezeichnet die Schwierigkeit große natürliche Zahlen in ihre großen Primfaktoren zu zerlegen. Bislang wurde dafür noch kein effizienter Algorithmus gefunden. Weil jedoch auch dessen Nichtexistenz nicht bewiesen werden konnte, geht man davon aus, dass der RSA-Algorithmus eine Trapdoor-Einwegfunktion ist, der private Schlüssel also nicht aus dem öffentlichen berechnet werden kann. Auch hat die Vermutung, dass man, ohne den privaten Schlüssel zu kennen, eine Nachricht nicht entschlüsseln kann, bisher Bestand und wird als RSA-Annahme bezeichnet.[49]

Gerade aufgrund dieser zahlreichen ungeklärten Probleme und bestehenden Vermutungen ist das RSA-Verfahren sowohl aus kryptographischer als auch aus kryptoanalytischer Sicht höchstinteressant. Deswegen wird nun auf die Wahl der für die Schlüsselerzeugung gewählten Parameter und daraufhin auf kryptoanalytische Angriffe auf RSA-verschlüsselte Systeme eingegangen, wobei vom Kerckhoff'schen Prinzip ausgegangen wird.

Um möglichst gut gegen kryptoanalytische Angriffe gewappnet zu sein, gibt es bestimmte Empfehlungen, welche die Parameter p, q, e und d erfüllen sollten:

Für die Primzahlen p und q gilt, dass sie ausreichend groß sein müssen, damit n möglichst schwierig zu faktorisieren ist. Da sich die Geschwindigkeit ausgeführter Operationen pro Zeiteinheit der Computer laut dem Moor'schen Gesetz alle 18 Monate verdoppelt, muss die Größe des RSA-Moduls n regelmäßig angepasst werden. Dem EU-Projekt ECRYPT II zufolge sollte n mindestens die in folgender Tabelle angeführte Größe haben, um als sicher zu gelten.[50]

Sicher bis	2020	2030	2040	in absehbarer Zukunft
Mindestgröße (in Bits)	1776	2432	3248	15.424

Tabelle 3: Mindestgröße des RSA-Moduls n

[49] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 125–128; **Beutelspacher/Schwenk/Wolfenstetter** (2015), S. 20–21; **Buchmann** (2016), S. 172–174.
[50] Vgl. **Buchmann** (2016), S. 174–175; **Smart** (2012).

Außerdem sollten die Primzahlen p und q gewissen weiteren Kriterien genügen, um von den verschiedenen Faktorisierungsalgorithmen nicht schon nach kurzer Zeit gelöst werden zu können. So dürfen sich p und q nicht zu sehr unterscheiden, aber auch nicht allzu nah beisammen liegen. Darüber hinaus sollte auch die Primfaktorenzerlegung der direkt benachbarten Zahlen von p und q möglichst wenige kleine Primzahlen aufweisen.[51]

Für die Wahl von e müssen sowohl die Sicherheit als auch die Effizienz der Verschlüsselung beachtet werden. Denn je kleiner e gewählt wird, desto weniger Zeit benötigt ein Computer zum Chiffrieren. Da der $ggT(e, \Phi(n)) = ggT(e, (p-1) \cdot (q-1)) = 1$ sein muss und sowohl $(p-1)$ als auch $(q-1)$ gerade sind, weil die Primzahlen $p, q > 2$ nur ungerade sein können, ist die kleinstmögliche Wahl $e = 3$. Hiergegen spricht jedoch die verlangte Sicherheit, da ein Low-Exponent-Angriff ein derart verschlüsseltes RSA-System in kurzer Zeit entschlüsseln könnte. Deswegen wird oft $e = 2^{16} + 1$ gewählt. Diese Zahl besitzt in binärer Schreibweise (genau wie $e = 3$) nur zwei Einser, ermöglicht eine effiziente Verschlüsselung und ist wesentlich sicherer. Folglich findet man in heute implementierten RSA-verschlüsselten Systemen meistens den Exponenten $e = 2^{16} + 1$, der allgemein als sicher gilt.

Die Zahl e derart klein zu wählen, führt unweigerlich zu einem großen d, was aus sicherheitstechnischer Sicht gut ist, da d bewiesenermaßen größer als $n^{0,292}$ sein muss, um nicht als Schwachstelle des Verschlüsselungsverfahrens zu gelten.[52]

Werden alle diese Sicherheitshinweise bei der Implementierung des RSA-Verfahrens beachtet, geht man nach heutigem Stand der Wissenschaft davon aus, dass der RSA-Algorithmus sicher ist, da bisher kein effizienter (also polynomieller) Algorithmus zum Faktorisieren großer Zahlen bekannt ist. Trotzdem ist es nicht ausgeschlossen, dass ein solcher einmal gefunden wird, wodurch das RSA-Verfahren schlagartig unsicher wäre.[53]

[51] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 118.
[52] Vgl. **Buchmann** (2016), S. 175–176; **Paar/Pelzl** (2016), S. 210–211.
[53] Vgl. **Beutelspacher** (2015), S. 140; **Spitz/Pramateftakis/Swoboda** (2011), S. 125.

5.2.5 Angriffe auf das RSA-Verfahren

Weil unter den Menschen stets auch das Verlangen danach besteht, kryptographische Verfahren zu brechen, werden nun zuerst kryptoanalytische Angriffsarten und daraufhin mögliche Attacken auf das RSA-Verfahren beleuchtet.

- Seitenkanalangriffe basieren auf der Beobachtung unbeabsichtigter Seitenkanäle einer RSA-Implementierung wie z. B. dem Stromverbrauch. Diese Art von Angriffen setzt einerseits den Zugang zu den beobachteten Seitenkanälen voraus, andererseits existieren relativ leicht durchführbare Gegenmaßnahmen.
- Protokollangriffe setzen sich zum Ziel, Schwachstellen im Protokoll zu suchen, in dem das RSA-Verfahren eingesetzt wird. Durch Einhalten moderner Sicherheitsstandards und Richtlinien ist ein derartiger Angriff verhinderbar.
- Mathematische Angriffe zielen darauf ab, mathematische Schwachstellen eines Verfahrens – vor allem mithilfe von Algorithmen – auszunutzen. Beim RSA-Algorithmus besteht die beste kryptoanalytische Methode darin, den Modul n zu faktorisieren. Auch wenn die Effizienz dafür verwendeter Algorithmen schon wesentlich gesteigert wurde, gilt das RSA-Verfahren nach wie vor als mathematisch sicher.[54]

Nun folgt eine Auswahl konkreter Angriffsmethoden auf RSA-verschlüsselte Systeme:

- Vollständige Schlüsselsuche
  Dieser Angriff verfolgt das simple Ziel, alle möglichen privaten Schlüssel des Empfängers Bob einer Nachricht durchzuprobieren. Dabei ist die angreifende Person jedoch höchstwahrscheinlich nicht erfolgreich, da sie schon bei einer Schlüssellänge von nur 256 Bits im Schnitt 2^{255}, also die Hälfte aller 2^{256}, Schlüssel durchprobieren müsste. Dies entspricht in Dezimalschreibweise ungefähr 10^{76} Versuchen. Als Vergleichswert sei angeführt, dass selbst die Anzahl an Atomen im Universum geringer als diese Zahl ist. Darüber hinaus sind heute Schlüssellängen von 1.024 oder 2.048 Bits üblich. Der Angriff durch vollständige Schlüsselsuche scheitert also kläglich.[55]

[54] Vgl. **Paar/Pelzl** (2016), S. 221–224.
[55] Vgl. **Schmeh** (2016), S. 208.

- Faktorisierungsangriff
  Ein Faktorisierungsangriff setzt daran an, n in p und q zu zerlegen. Den Zugang zu n hat die angreifende Person über den öffentlichen Schlüssel Bobs und mithilfe dieser Faktorisierung könnte sie problemlos dessen privaten Schlüssel berechnen. Da dem RSA-Verfahren jedoch eine Einwegfunktion zugrunde liegt, gestaltet sich die Suche nach p und q als äußerst aufwendig. Im Jahr 2016 lag der offizielle Weltrekord der Faktorisierung einer Zahl n in ihre beiden Primfaktoren bei einer Länge von 768 Bits, was 232 Dezimalstellen entspricht. Auch wenn sich in der Zwischenzeit Etliches auf diesem Gebiet getan haben mag und Geheimdienste ihre Möglichkeiten nicht publik machen, gilt auch heute eine Schlüssellänge von 2.048 Bits beim RSA-Verfahren als sicher.[56]

- Low-Exponent Attack
  Verschickt eine Absenderin Alice dieselbe Nachricht an mindestens e Personen und haben diese denselben geringen Wert für e gewählt, so kann eine angreifende Person aus dem Geheimtext c mithilfe des Chinesischen Restsatzes den Klartext m rekonstruieren. Gerade deswegen ist die Wahl von e, die im Kapitel 5.2.4 behandelt wurde, so wichtig.[57]

Nachdem nun einige konkrete Angriffe auf das RSA-Verfahren angeführt wurden, soll noch ein Ausblick in die zukünftige Sicherheit des RSA-Algorithmus gegeben werden. Dabei ist zu erwähnen, dass nicht Vieles für ein langes Fortbestehen der RSA-Verschlüsselung spricht. Neben der Möglichkeit der Auffindung eines effizienten Faktorisierungsalgorithmus gefährden auch die Entwicklung von Quantencomputern und anderen Apparaten, wie etwa TWINKLE oder TWIRL, die Sicherheit des RSA-Algorithmus. Doch ist es momentan das meist benutzte und intensivst erforschte asymmetrische Verschlüsselungsverfahren, gilt unter der Voraussetzung korrekter Implementierung als aktuell sicher und beruht trotz seiner Komplexität auf einer einfachen, mathematischen Erkenntnis: dem Satz von Euler-Fermat.[58]

[56] Vgl. **Schmeh** (2016), S. 208.
[57] Vgl. ebd. S. 209.
[58] Vgl. **Paar/Pelzl** (2016), S. 226–227; **Schmeh** (2016), S. 209–210.

6 Fazit

Abschließend lässt sich festhalten, dass der Satz von Euler-Fermat als Lehrsatz der elementaren Zahlentheorie einen wichtigen Zusammenhang zwischen zwei natürlichen Zahlen herstellt und damit grundlegend für weitere mathematische Erkenntnisse ist. Die vorliegende Arbeit zeigt den konkreten allgemeinen Nutzen dieser mathematischen Gesetzmäßigkeit auf und geht auf die Bedeutung des Satzes von Euler-Fermat für die Gesellschaft ein. Im Konkreten ist damit die Anwendung des Lehrsatzes in der Kryptographie, der Verschlüsselungswissenschaft, in Form des RSA-Verfahrens, welches einen wesentlichen Beitrag zum Schutz unser aller Privatsphäre leistet, gemeint.

Bei eingehender Beleuchtung von Angriffsversuchen auf ein RSA-verschlüsseltes System ist aufgefallen, dass jegliche mathematische Angriffe aktuell scheitern und ein Brechen eines solchen Kryptosystems bislang nur aufgrund schlechter Implementierung möglich ist. In Zukunft wird sich jedoch die spannende Frage stellen, ob es jemandem gelingt, das Faktorisierungsproblem zu lösen oder den RSA-Algorithmus mithilfe eines Quantencomputers oder anderer Apparate zu brechen.

Besonders erstaunlich während des gesamten Arbeitsprozesses war die Tatsache, dass der Satz von Euler-Fermat, der im 18. Jahrhundert als Teil der als unwichtig erachteten Zahlentheorie aufgestellt wurde, über 200 Jahre später als Grundlage für eine Anwendung dient, die Sicherheit und Privatsphäre, zwei Grundbedürfnisse des Menschen, sicherstellt. Dies wirft die weiterführende philosophische Frage auf, ob Forschung immer anwendungsorientiert vonstatten gehen muss oder eben nicht.

Zuletzt sei erwähnt, dass sich der Arbeitsprozess insofern zum Teil schwierig gestaltete, als es eine Herausforderung darstellt, die mathematischen Teile der Arbeit verständlich und nachvollziehbar zu gestalten, da die Behandlung eines mathematischen Themas selbstverständlich nicht ohne mathematische Notation auskommt. So wurde diese vorwissenschaftliche Arbeit in der Hoffnung verfasst, dass sich viele Leserinnen und Leser auf die aufbauende mathematische Hinführung zum Satz von Euler-Fermat einlassen.

Literaturverzeichnis

Printquellen

Bartholomé, Andreas; Rung, Josef; Kern, Hans: Zahlentheorie für Einsteiger. Eine Einführung für Schüler, Lehrer, Studierende und andere Interessierte. – 6., überarbeitete und erweiterte Auflage. – Wiesbaden: Vieweg + Teubner, 2008.

Bernoulli, Daniel: Magni Euleri praeceptor in mathematicis. Brief von Daniel Bernoulli an Leonhard Euler vom 4. September 1743. – Basel: 1743.

Beutelspacher, Albrecht: Geheimsprachen. Geschichte und Techniken. – 5., aktualisierte Auflage. – München: Verlag C.H. Beck, 2013.

Beutelspacher, Albrecht: Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. – 10. Auflage. – Wiesbaden: Springer Spektrum, 2015.

Beutelspacher, Albrecht; Neumann, Heike B.; Schwarzpaul, Thomas: Kryptografie in Theorie und Praxis. Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld. – 2., überarbeitete Auflage. – Wiesbaden: Vieweg + Teubner, 2010.

Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus-Dieter: Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge. – 8. Auflage. – Wiesbaden: Springer Spektrum, 2015.

Brückler, Franka Miriam: Geschichte der Mathematik kompakt. Das Wichtigste aus Arithmetik, Geometrie, Algebra, Zahlentheorie und Logik. – Berlin: Springer Spektrum, 2017.

Buchmann, Johannes: Einführung in die Kryptographie. – 6. Auflage. – Berlin, Heidelberg: Springer Spektrum, 2016.

Bundschuh, Peter: Einführung in die Zahlentheorie. – 6., überarbeitete und aktualisierte Auflage. – Berlin, Heidelberg: Springer, 2008.

Calinger, Ronald: Leonhard Euler. Mathematical genius in the Enlightenment. – Princeton: Princeton University Press, 2016.

Fellmann, Emil Alfred: Leonhard Euler. – Reinbek bei Hamburg: Rowohlt Taschenbuch, 1995.

Forster, Otto: Algorithmische Zahlentheorie. – 2., überarbeitete und erweiterte Auflage. – Wiesbaden: Springer Spektrum, 2015.

Karpfinger, Christian; Meyberg, Kurt: Algebra: Gruppen – Ringe – Körper. – 2. Auflage. – Heidelberg: Spektrum Akademischer Verlag, 2010.

Löh, Clara; Kilbertus, Niki; Krauss, Stefan (Hrsg.): Quod erat knobelandum: Themen, Aufgaben und Lösungen des Schülerzirkels Mathematik der Universität Regensburg. – Regensburg: Springer, 2019.

Manz, Olaf: Verschlüsseln, Signieren, Angreifen. Eine kompakte Einführung in die Kryptografie. – Berlin: Springer Spektrum, 2019.

Oswald, Nicola; Steuding, Jörn: Elementare Zahlentheorie. Ein sanfter Einstieg in die höhere Mathematik. – Berlin, Heidelberg: Springer Spektrum, 2015.

Paar, Christof; Pelzl, Jan: Kryptografie verständlich. Ein Lehrbuch für Studierende und Anwender. – Berlin, Heidelberg: Springer Vieweg, 2016.

Padberg, Friedhelm; Büchter, Andreas: Elementare Zahlentheorie. – 4., überarbeitete und aktualisierte Auflage. – Berlin: Springer Spektrum, 2018.

Pincock, Stephen; Frary, Mark: Geheime Codes: Die berühmtesten Verschlüsselungstechniken und ihre Geschichte. Übers. von Petra Trinkaus. – Bergisch Gladbach: Ehrenwirth, 2007.

Reiss, Kristina; Schmieder, Gerald: Basiswissen Zahlentheorie. Eine Einführung in Zahlen und Zahlbereiche. – 3., überarbeitete Auflage. – Berlin, Heidelberg: Springer Spektrum, 2014.

Schmeh, Klaus: Die Welt der geheimen Zeichen: Die faszinierende Geschichte der Verschlüsselung. – 2. Auflage. – Hamburg: Nikol, 2010.

Schmeh, Klaus: Kryptografie. Verfahren, Protokolle, Infrastrukturen. – 6., aktualisierte Auflage. – Heidelberg: dpunkt.verlag, 2016.

Smart, Nigel (Hrsg.): Yearly Report on Algorithms and Keysizes (2011-2012), ICT-2007-216676 ECRYPT II. – 2012.

Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim: Kryptographie und IT-Sicherheit. Grundlagen und Anwendungen. – 2., überarbeitete Aufl. – Wiesbaden: Vieweg + Teubner, 2011.

St. Denis, Tom; Johnson, Simon: Kryptografie für Entwickler. – Haar bei München: Franzis Verlag, 2017.

Strick, Heinz Klaus: Mathematik – einfach genial! Bemerkenswerte Ideen und Geschichten von Pythagoras bis Cantor. – Berlin: Springer Verlag, 2020.

Strick, Heinz Klaus: Mathematik ist schön. – Berlin: Springer, 2017.

Thaer, Clemens; Schreiber, Peter (Hrsg.): Die Elemente: Bücher I–XIII (Euklid). – Nachdruck der 4., erweiterten Auflage. – Frankfurt am Main: Deutsch, 2010.

Waldecker, Rebecca; Rempe-Gillen, Lasse: Primzahltests für Einsteiger. Zahlentheorie – Algorithmik – Kryptographie. – 2. Auflage. – Wiesbaden: Springer Spektrum, 2016.

Wätjen, Dietmar: Kryptographie. Grundlagen, Algorithmen, Protokolle. – 3., aktualisierte und erweiterte Auflage. – Wiesbaden: Springer Vieweg, 2018.

Wußing, Hans: 6000 Jahre Mathematik. Eine kulturgeschichtliche Zeitreise. Von Euler bis zur Gegenwart. – Berlin, Heidelberg: Springer, 2008.

Ziegenbalg, Jochen: Elementare Zahlentheorie. Beispiele, Geschichte, Algorithmen. – 2., überarbeitete Auflage. – Wiesbaden: Springer Spektrum, 2015.

Internetquellen

Hari, Markus: Folgen und Reihen – Figurierte Zahlen. https://meinstein.ch/math/folgen-und-reihen/ [12. 01. 2021].

Magidin, Arturo: Subjects studied in number theory. Mathematics Stack Exchange. https://math.stackexchange.com/questions/37648/subjects-studied-in-number-theory [03. 09. 2020].

Mahoney, Michael: Pierre De Fermat. https://www.encyclopedia.com/people/science-and-technology/mathematics-biographies/pierre-de-fermat [20. 12. 2020].

Strick, Heinz Klaus: Pierre de Fermat (1607/1608–1665). https://www.spektrum.de/wissen/pierre-fermat-1607-1608/962953 [20. 12. 2020].

Vollrath, Hans-Joachim: Entdeckungen Leonhard Eulers. http://www.history.didaktik.mathematik.uni-wuerzburg.de/ausstell/euler/perlen.html [28. 12. 2020].

Walz, Guido: Zahlentheorie. https://www.spektrum.de/lexikon/mathematik/zahlentheorie/11083 [31. 08. 2020].

Abbildungsverzeichnis

Abb. 1: Werte von $\Phi(n)$ für $1 \leq n \leq 99$ 24
Abb. 2: Graphische Darstellung der Phi-Funktion 24

Tabellenverzeichnis

Tab. 1: Tabellarische Anordnung der $z_i \in \mathbb{N}$ nach den Parametern p und q . . . 26
Tab. 2: Tabellarische Anordnung der $z_i \in \mathbb{N}$ nach den Parametern m und n . . 26
Tab. 3: Mindestgröße des RSA-Moduls n 35

Alle Abbildungen und Tabellen wurden vom Autor mit den Programmen Geogebra, Excel, Paint 3D und LaTeX erstellt.

Glossar

Advanced Encryption Standard (AES)

Diese symmetrische Chiffre ist heutzutage die meist genutzte überhaupt und gilt als sehr sicher. Für eine detaillierte Beschreibung des AES siehe Literatur in der Fußnote.[59]

Algorithmus

Unter einem Algorithmus versteht man sowohl in der Kryptographie als auch in der Mathematik ein Verfahren, meistens einen Rechenvorgang, der nach einem bestimmten (sich wiederholenden) Schema abläuft und nach endlich vielen elementaren (also keine Erfindungskraft benötigenden und im Vorhinein schon wohl definierten) Schritten endet.[60]

Alice

Um kryptographische Vorgänge allgemein zu beschreiben, werden für die beiden miteinander kommunizierenden Personen allgemein die Namen Alice (A) und Bob (B) verwendet.[61]

Anonymität

Der Sicherheitsdienst der Anonymität bezeichnet das Unerkanntbleiben trotz Teilnahme an einer Kommunikation oder Durchführung eines Vorgangs. Ein Beispiel aus dem Alltag wäre das Bezahlen mit Bargeld, wobei die Anonymität gewahrt bleibt, und jenem mit Kredit- oder Bankomatkarte, bei dem die Identität der Kundschaft nachgewiesen werden kann.[62]

Asymmetrische Chiffre

Asymmetrische Chiffren bauen auf dem Grundgedanken auf, dass jede und jeder Teilnehmende einer Gruppe Kommunizierender einen privaten Schlüssel besitzt, den ausschießlich sie bzw. er selbst kennt. Zusätzlich wird ihr bzw. ihm ein öffentlicher Schlüssel zugeteilt, auf den man, wie der Name schon sagt, öffentlich zugreifen kann. Mithilfe des öffentlichen Schlüssels kann jede und jeder eine Nachricht verschlüsseln und dem Teilnehmenden Bob

[59] Vgl. **Buchmann** (2016), S. 145–153; **Paar/Pelzl** (2016), S. 103–140; **Schmeh** (2016), S. 137–148.
[60] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 45; **Buchmann** (2016), S. 17; **Waldecker/Rempe-Gillen** (2016), S. 29–31.
[61] Vgl. **Schmeh** (2016), S. 15–16.
[62] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 2; **Spitz/Pramateftakis/Swoboda** (2011), S. 17–18.

schicken. Nur dieser kann die Botschaft mithilfe seines privaten Schlüssels dechiffrieren. Im Grunde genommen ist das Prinzip also ähnlich, wie das der Briefkästen: Jede und jeder kann ein verschlossenes Briefkuvert in einen versperrten Briefkasten einwerfen, aber nur wer den Schlüssel für diesen besitzt, kann den Brief entgegennehmen und lesen. Derartige asymmetrische Verschlüsselungsmethoden sind allgemein auch unter dem Namen „Public-Key-Verfahren“ bekannt und werden seit ihrer Erfindung 1976 hauptsächlich auf dem Gebiet der digitalen Signatur, aber auch zum Übermitteln geheimer Schlüssel und für klassische Nachrichtenverschlüsselung benutzt.[63]

Authentizität

Wird von Authentizität gesprochen, ist damit die eindeutige Identifikation der Gesprächsbeteiligten gemeint. Sie setzt Integrität voraus, da eine abgeänderte Nachricht nicht mehr authentisch ist.[64]

Bob

Siehe *Alice*.

Chiffre

Die verwendete (geheime) Methode, die zum Verschlüsseln verwendet wird, wird als Chiffre bezeichnet.[65]

Chiffrieren

Die Tätigkeit den Klartext m in den Geheimtext c umzuwandeln wird im Fachjargon als Chiffrieren bezeichnet. [66]

Dechiffrieren

Die Tätigkeit den Geheimtext c in den Klartext m umzuwandeln wird Dechiffrieren genannt. [67]

[63] Vgl. **Paar/Pelzl** (2016), S. 3–4; **Spitz/Pramateftakis/Swoboda** (2011), S. 2; **Wätjen** (2018), S. 4.
[64] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 7–8; **Spitz/Pramateftakis/Swoboda** (2011), S. 15–17.
[65] Vgl. **Wätjen** (2018), S. 1.
[66] Vgl. ebd. S. 1.
[67] Vgl. ebd. S. 1.

Digitale Signatur

Um die absendende Person eines Dokuments, wie z. B. eines Briefs, verifizieren zu können, verwenden wir im Alltag unsere persönliche Unterschrift. In der digitalen Welt wird dafür die digitale Signatur benutzt. Die Echtheit einer solchen muss überprüfbar sein. Außerdem darf sowohl das ihr zugrunde liegende Dokument nicht unbemerkt verändert als auch die digitale Signatur selbst nicht heimlich von einem zum anderen Dokument übertragen werden können.[68]

Einwegfunktion

Als Einwegfunktion wird eine einfach ausführbare Funktion bezeichnet, die nur mit sehr großem Aufwand invertiert werden kann.[69]

Figurierte Zahlen

Unter figurierten Zahlen versteht man visualisierte Zahlenmuster, also eine natürliche Zahl, die sich als Figur darstellen lässt. Dabei werden gleichartige Gegenstände oftmals in Muster geometrischer Formen geordnet. Als Beispiel für eine Art von figurierten Zahlen seien die Quadratzahlen erwähnt. Dazu zählen all jene Zahle n, für die gilt, dass sich n gleichartige Gegenstäne in Form eines Quadrats auflegen lassen.[70]

Geheimtext

Der am Weg von Alice zu Bob verschlüsselte Klartext wird Geheimtext (c) genannt. Das Symbol c hat seinen Ursprung im englischen Wort „ciphertext“.[71]

Integrität

Integrität bezeichnet die Tatsache, dass eine Nachricht auf ihrem Weg von Alice zu Bob nicht verändert worden sein kann.[72]

---

[68] Vgl. **Schmeh** (2016), S. 215–216.
[69] Vgl. **Beutelspacher/Schwenk/Wolfenstetter** (2015), S. 12; **Schmeh** (2016), S. 198.
[70] Vgl. **Hari** (2017).
[71] Vgl. **Wätjen** (2018), S. 1.
[72] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 7–8; **Spitz/Pramateftakis/Swoboda** (2011), S. 15–17.

Kerckhoff'sches Prinzip

Das Kerckhoff'sche Prinzip besagt, dass ein kryptographisches System auch dann noch sicher sein muss, wenn die angreifende Person mit Ausnahme des verwendeten Schlüssls alle Informationen eines Kryptoverfahrens besitzt. Dieses Prinzip hat deswegen seine Berechtigung, da die Geschichte gezeigt hat, dass die Funktionsweise eines kryptographischen Systems nicht für immer geheimzuhalten ist und die Sicherheit nach Bekanntwerden dieser nur so gewährleistet werden kann.[73]

Klartext

Der unverschlüsselte Nachrichtentext, den Alice Bob übermitteln will, wird Klartext (m) genannt. Das Symbol m hat seinen Ursprung im englischen Wort „message".[74]

Öffentlicher Schlüssel

Der öffentliche Schlüssel, der passend zum privaten Schlüssel aller Teilnehmenden eines Systems erstellt wird und allen zugänglich ist, findet im asymmetrischen Verschlüsselungsverfahren beim Chiffriervorgang Verwendung.[75]

Parität

Die Parität bezeichnet die Eigenschaft einer ganzen Zahl, entweder ungerade oder gerade zu sein. Dies ist äquivalent zum Betrachten der ganzen Zahlen unter modulo 2 und der sich daraus ergebende Unterscheidungsmöglichkeit zwischen den Zahlen.[76]

Privater Schlüssel

Ein privater Schlüssel ist einer, den nur die adressierte Person einer Nachricht kennt und der in Kombination mit einem öffentlichen Schlüssel im asymmetrischen Verschlüsselungsverfahren Verwendung findet.[77]

Public-Key-Verfahren

Die Public-Key-Verschlüsselung ist ein Synonym zur asymmetrischen Verschlüsselung (siehe *asymetrische Chiffre*).[78]

[73] Vgl. **Beutelspacher** (2015), S. 19; **Paar/Pelzl** (2016), S. 12–13; **Schmeh** (2016), S. 40.
[74] Vgl. **Wätjen** (2018), S. 1.
[75] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 105; **Schmeh** (2016), S. 191.
[76] Vgl. **Ziegenbalg** (2015), S. 87.
[77] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 105; **Schmeh** (2016), S. 191.
[78] Vgl. **Paar/Pelzl** (2016), S. 176; **Schmeh** (2016), S. 191.

Quantencomputer

Ein Quantencomputer ist ein Computer, der nicht auf den Gesetzen der Klassischen Physik, sondern auf jenen der Quantenmechanik aufbaut. Er ist in der Lösung bestimmter Problemstellungen wesentlich effektiver als ein herkömmlicher Computer und würde somit nach kurzer Zeit eine RSA-Verschlüsselung brechen. Momentan ist die Existenz von Quantencomputern jedoch noch Zukunftsmusik.[79]

Schlüssel

Der Schlüssel (k von engl. „key“) trägt die Information, wie verschlüsselt wurde, und bezeichnet das Wissen, welches bei der symmetrischen Verschlüsselung Alice und Bob, bei der asymmetrischen nur der Empfänger der Nachricht Bob einem möglichen Angreifenden voraus haben müssen, um die Nachricht geheimzuhalten.[80]

Sicherer Kanal

Ein sicherer Kanal ist in der Kryptographie die Bezeichnung einer Leitung, die Abhörsicherheit garantieren und somit zur geheimen Passwort- bzw. Nachrichtenübermittlung verwendet werden kann.[81]

Steganographie

Unter Steganographie versteht man die Wissenschaft, die sich mit Maßnahmen zur geheimen Nachrichtenübermittlung beschäftigt, wobei die Existenz der Botschaft zu verbergen versucht wird. Ein Beispiel dafür wäre das Verfassen eines Briefes mit Zitronensaft, der über der Flamme einer Kerze sichtbar wird.[82]

Symmetrische Chiffre

Symmetrische Chiffren waren bis zur Entdeckung der *Asymmetrischen Chiffre* 1976 die einzig bekannten. Sie beruhen auf dem Prinzip, dass zwei Parteien eine gemeinsame Ver- und Entschlüsselungsmethode sowie den gleichen Schlüssel verwenden, wodurch das Antworten auf dieselbe Weise verschlüsselt werden kann wie die ursprüngliche Nachricht.[83]

---

[79] Vgl. **Schmeh** (2016), S. 311–318.
[80] Vgl. **Beutelspacher/Schwenk/Wolfenstetter** (2015), S. 6–7; **Wätjen** (2018), S. 1.
[81] Vgl. **Paar/Pelzl** (2016), S. 174.
[82] Vgl. **Spitz/Pramateftakis/Swoboda** (2011), S. 1.
[83] Vgl. **Paar/Pelzl** (2016), S. 3–4; **Spitz/Pramateftakis/Swoboda** (2011), S. 2; **Wätjen** (2018), S. 4.

Trapdoorfunktion

Existiert mit gegebener Zusatzinformation eine Abkürzung bzgl. der Berechnung der Umkehrfunktion einer Einwegfunktion, spricht man von einer Falltürfunktion.[84]

Triple Data Encryption Standard (3DES)

Diesem symmetrischen Verschlüsselungsverfahren liegt ein dreifach ausgeführter Data-Encryption-Standard-Algorithmus (DES) zugrunde. Er gilt als ebenbürtige Alternative zum AES-Verfahren, also als sehr sicher. Näheres zur Funktionsweise des 3DES ist in der, in der Fußnote angeführten, Literatur zu finden.[85]

TWINKLE

The Weizmann Institute Key Locating Engine (TWINKLE) ist eine von Adi Shamir 1999 präsentierte Idee zum Bau eines optisch-elektronischen Apparats, der Faktorisierungsvorgänge 100–1000-mal schneller als ein PC durchführen könnte und somit besser als ein solcher für einen Angriff auf ein RSA-verschlüsseltes System geeignet wäre.[86]

TWIRL

The Weizmann Institute Relation Locator (TWIRL) ist der Nachfolger von TWINKLE und eine bisher noch nicht realisierte Idee zum Bau einer Maschine, die einen RSA-Schlüssel von 1.024 Bits voraussichtlich innerhalb eines Jahres faktorisieren könnte.[87]

Verbindlichkeit

Verbindlichkeit, die auch als „Nicht-Abstreitbarkeit“ bezeichnet wird, meint die Tatsache, dass auch Dritten gegenüber stets die Person, welche eine Nachricht abgesandt hat, nachgewiesen werden kann, diese ihr Schreiben also nicht erfolgreich abstreiten kann. Dabei umfasst sie sowohl die Eigenschaften der Authentizität als auch die der Integrität.[88]

---

[84] Vgl. **Beutelspacher/Schwenk/Wolfenstetter** (2015), S. 12; **Schmeh** (2016), S. 198.
[85] Vgl. **Buchmann** (2016), S. 135–144; **Paar/Pelzl** (2016), S. 63–100; **Schmeh** (2016), S. 85–96.
[86] Vgl. **Schmeh** (2016), S. 209–210.
[87] Vgl. ebd. S. 210.
[88] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 2;
Spitz/Pramateftakis/Swoboda (2011), S. 17.

Vertraulichkeit

Das Ziel des Sicherheitsdienstes der Vertraulichkeit ist die geheime Kommunikation zweier Personen, also eine Nachrichtenübermittlung ohne ein mögliches Abhören durch Dritte.[89]

Zugriffskontrolle

Unter Zugriffskontrolle, die auch als Autorisierung bezeichnet wird, wird das kryptographische Ziel verstanden, variierende Zugriffsrechte verschiedener Personen zu verwalten und jedem nur jene Rechte zu genehmigen, die ihm zustehen.[90]

[89] Vgl. **Beutelspacher/Neumann/Schwarzpaul** (2010), S. 3–7; **Spitz/Pramateftakis/Swoboda** (2011), S. 15; **St. Denis/Johnson** (2017), S. 25.
[90] Vgl. **Spitz/Pramateftakis/Swoboda** (2011), S. 18.

Eidesstattliche Selbstständigkeitserklärung

„Ich, Leopold Karl, versichere, dass ich diese vorwissenschaftliche Arbeit selbstständig angefertigt, keine anderen als die angegebenen Hilfsmittel benutzt und alle aus ungedruckten Quellen, gedruckter Literatur oder aus dem Internet im Wortlaut oder im wesentlichen Inhalt übernommenen Formulierungen und Konzepte gemäß den Richtlinien wissenschaftlicher Arbeiten zitiert, durch Fußnoten gekennzeichnet bzw. mit genauer Quellenangabe kenntlich gemacht habe."

Wien, Februar 2021 U:

Zustimmung zur Aufstellung in der Schulbibliothek

„Ich bekunde hiermit mein Einverständnis damit, dass ein Exemplar dieser vorwissenschaftlichen Arbeit in meiner Schule, dem Öffentlichen Schottengymnasium der Benediktiner in Wien, aufgestellt wird."

Wien, Februar 2021 U: