



# **Elliptische Kurven in der Charakteristik $p > 3$ und die Implementierung der Arithmetik in der Programmiersprache Python**

Studienarbeit T3\_3101

Hochschule: Duale Hochschule Baden-Württemberg Mannheim  
Kurs: TINF20IT2  
Name: Vorname Nachname  
Matrikelnummer: XXXXXX  
E-Mail: sXXXXXXX@student.dhbw-mannheim.de

Studiengangsleiter: Prof. Dr. Nathan Sudermann-Merx  
Betreuer: Prof. Dr. Reinhold Hübl  
Bearbeitungszeitraum: 18.10.2022 - XX.XX.2023

Unterschrift des Betreuers: \_\_\_\_\_



# Selbstständigkeitserklärung

Hiermit erkläre ich durch meine Unterschrift, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst und keine anderen Hilfsmittel als die angegebenen verwendet habe.

Insbesondere versichere ich, dass ich alle wörtlichen und sinngemäßen Übernahmen aus anderen Werken – dazu gehören auch Internetquellen – als solche kenntlich gemacht habe.

---

Ort, Datum

---

Unterschrift Student

## **Zusammenfassung**

Hier Text des Abstract in Deutsch.

## **Abstract**

Hier Text des Abstract in Englisch.

# Inhaltsverzeichnis

<b>Zusammenfassung</b>	<b>I</b>
<b>Abstract</b>	<b>II</b>
<b>1. Grundlagen</b>	<b>1</b>
1.1. Primzahlen . . . . .	1
1.1.1. Definition und Eigenschaften . . . . .	2
1.1.2. Bestimmung von Primzahlen . . . . .	2
1.1.3. Rolle der Primzahlen in der Kryptologie . . . . .	2
1.2. Algebraische Strukturen . . . . .	2
1.2.1. Monoid . . . . .	3
1.2.2. Gruppe . . . . .	4
1.3. Allgemeines zur Verschlüsselung . . . . .	4
1.3.1. Symmetrische und Asymmetrische Verschlüsselung . . . . .	4
1.3.2. Diffie-Hellmann . . . . .	5
1.4. Ziel der Arbeit . . . . .	5
1.5. Geplante Vorgehensweise . . . . .	5

# Abkürzungsverzeichnis

# Abbildungsverzeichnis

1.1. Hauptaufgaben der Ist-Analyse beim Redesign einer Netzwerkinfrastruktur	1
--	---



# 1. Grundlagen

Diese Studienarbeit befasst sich mit dem komplexen Thema der Elliptischen Kurven in der Kryptographie. Die Kryptographie ist ein mathematisches Thema, bei welchem es zu Anfang der Legung einer Grundlage für das Verständnis der Inhalte dieser Studienarbeit bedarf. In diesem Kapitel werden sowohl die mathematischen als auch die kryptographischen Grundlagen zum Verständnis der Inhalte dieser Studienarbeit gelegt.

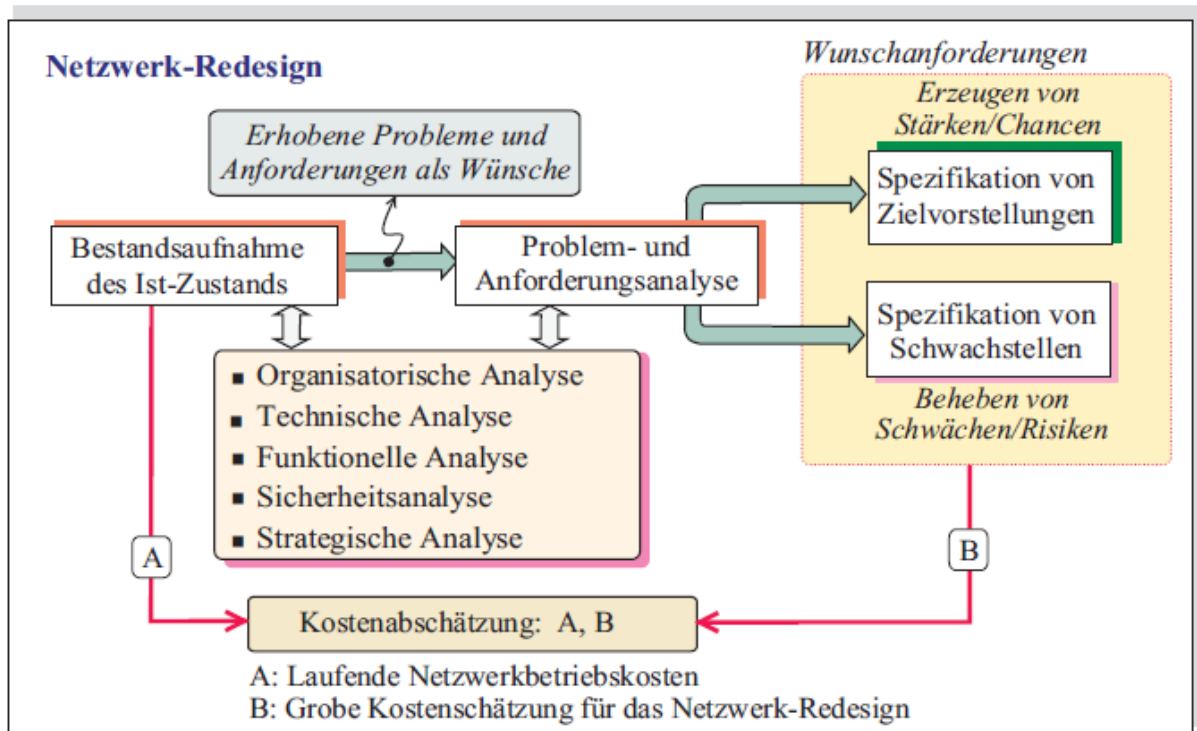


Abbildung 1.1.: Hauptaufgaben der Ist-Analyse beim Redesign einer Netzwerkinfrastruktur  
Quelle: [Berghammer.2021]

## 1.1. Primzahlen

In der Zahlentheorie, einem Teilbereich der Mathematik, werden viele unterschiedliche Eigenschaften von Zahlen untersucht. Durch die Untersuchung erhofft man sich neue Erkenntnisse für Wissenschaft und Technik. Die Primzahlen als mathematisches Forschungsgebiet sind hierbei ein Teilbereich der Zahlentheorie. Im Folgenden werden Primzahlen definiert und deren Eigenschaften erläutert. Anschließend wird untersucht, wie Primzahlen berechnet werden können. Am Ende wird erläutert, welche Rolle Primzahlen in der

Kryptologie und modernen Kryptosystemen innehaben.

### 1.1.1. Definition und Eigenschaften

Es gibt viele unterschiedliche Zahlenmengen. Beispielsweise gibt es die Menge der reellen Zahlen  $\mathbb{R}$ . Diese beinhalten als Teilmenge die rationalen und die irrationalen Zahlen. Die natürlichen Zahlen  $\mathbb{N}$  bilden hierbei alle positiven ganzen Zahlen ab. Dabei gibt es  $\mathbb{N}^+$  exklusive der Zahl 0 als Teilmenge mit  $\mathbb{N}^+ = \{1, 2, 3, 4, \dots, \infty\}$  und  $\mathbb{N}_0$  inklusive der Zahl 0 als Teilmenge mit  $\mathbb{N}_0 = \{0, 1, 2, 3, 4, \dots, \infty\}$ . Die Primzahlen  $\mathbb{P}$  sind hierbei etwas ganz besonderes. Sie unterscheiden sich von anderen Zahlen. Obwohl sie eine Teilmenge der natürlichen Zahlen sind ist die Kardinalität ihrer Elemente unendlich respektive die Anzahl der Primzahlen ist unendlich. Die Unendlichkeit der Primzahlen konnte schon mit mehreren mathematischen Sätzen bewiesen werden., unter anderem dem Satz von Euklid.

Doch wie genau sind Primzahlen definiert? Eine Primzahl  $p$  ist eine natürliche Zahl mit  $p > 0$ , wobei  $p$  nur durch 1 und sich selbst teilbar sein darf. Durch diese Eigenschaft können Primzahlen nicht durch Multiplikation von natürlichen Zahlen gebildet werden, jedoch können natürliche Zahl mit Ausnahme der Zahl 0 durch Primzahlen als Produkt gebildet werden. Die Primzahlen bilden also das Grundgerüst zur Bildung von Zahlen, da man aus ihnen alle anderen natürlichen Zahlen durch Multiplikation bilden kann. Teilt man eine Zahl so in ihr einzelnen Primfaktoren auf, dann nennt man dies Primfaktorzerlegung.

### 1.1.2. Bestimmung von Primzahlen

x

### 1.1.3. Rolle der Primzahlen in der Kryptologie

x

## 1.2. Algebraische Strukturen

Definiert durch die Zahlentheorie und als zentraler Untersuchungsgegenstand des mathematischen Teilgebietes der universellen Algebra, liefern algebraische Strukturen die Basis zur Realisierung komplexer symmetrischer und asymmetrischer Kryptosysteme, weshalb wir im folgenden Kapitel die Eigenschaften relevanter algebraischer Strukturen näher betrachten wollen. Darüber hinaus möchten wir Ihnen auch einige Werkzeuge zum Rechnen in der jeweiligen algebraischen Struktur an die Hand geben, welche zur späteren Realisierung

von Kryptosystemen benötigt werden.

Unter einer sehr allgemeinen Betrachtung ist eine mathematische Struktur eine Liste nichtleerer Mengen, genannt Trägermengen, mit Elementen aus den Trägermengen, genannt Konstanten, und mengentheoretischer Konstruktionen über den Trägermengen. Diese sind konkret Funktionen über den Trägermengen. Im Weiteren beschränken wir uns auf den Fall einer einzigen Trägermenge, wodurch die Strukturen als homogen bezeichnet werden können.

**Definition: Homogene algebraische Struktur** Eine homogene algebraische Struktur ist ein Tupel  $(M, c_1, \dots, c_m, f_1, \dots, f_n)$  mit  $m, n \in \mathbb{N}$  und  $n \geq 1$ . Dabei ist  $M$  eine nichtleere Menge, genannt **Trägermenge**, alle  $c_i$  sind Elemente aus  $M$ , genannt die **Konstanten**, und alle  $f_i$  sind  $s_i$ -stellige Funktionen  $f_i : M \rightarrow M$  im Fall  $s = 1$  und  $f_i : M^{s_i} \rightarrow M$  im Fall  $s_i > 1$ , genannt die (inneren) **Operationen**. Die lineare Liste  $(0, \dots, 0, s_1, \dots, s_n)$  mit  $m$  Nullen heißt **Typ** oder die **Signatur**.

Laut dieser Definition muss eine homogen algebraische Struktur nicht unbedingt Konstanten enthalten, jedoch mindestens eine Operation. Das Paar  $(\mathbb{N}, +)$  bildet beispielsweise eine homogene algebraische Struktur des Typs (2). Das 5-Tupel  $(\mathbb{N}, 0, 1, +, \cdot)$  bildet ebenfalls eine homogen algebraische Struktur des Typs (0,0,2,2).

Algebraische Strukturen unterscheiden sich grundsätzlich durch ihren Typ. Wirklich charakterisiert werden sie aber erst durch die jeweils geltenden Axiome, d.h. bestimmte Eigenschaften, welche für die Konstanten und Operationen gefordert werden. Durch die Hinzunahme immer weiterer Axiome, entsteht eine Hierarchie immer feinerer Strukturen, an deren Anfang der Monoid steht.

### 1.2.1. Monoid

**Definition: Monoid** Eine algebraische Struktur  $(M, e, \cdot)$  des Typs (0,2) heißt ein Monoid, falls für alle  $x, y, z \in M$  die folgenden Monoid Axiome gelten:

- (Ass)  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- (Neu)  $e \cdot x = x = x \cdot e$

Gilt zusätzlich noch für alle  $x, y \in M$  die Gleichung  $x \cdot y = y \cdot x$ , so heißt  $(M, e, \cdot)$  ein **kommutatives Monoid**.

Die erste und die letzte Gleichung bilden das Assoziativ- und Kommutativgesetz ab. Durch die mittlere Gleichung wird ein neutrales Element  $e$  bezüglich der Operation gefordert, wobei sowohl die **Linksneutralität** als auch die **Rechtsneutralität** spezifiziert wird.

Einfache Beispiele für Monoide sind  $(\mathbb{N}, 0, +)$ ,  $(\mathbb{N}, 1, \cdot)$  und  $(\mathbb{Z}, 0, +)$ . Die Potenzierung in solchen Monoiden ist folgendermaßen definiert.

**Definition: Potenzierung** In einem Monoid  $(M, e, \cdot)$  definiert man die  $n$ -te **Potenz**  $x^n$  von  $x \in M$  durch  $x^0 := e$  und  $x^{x+1} = x \cdot x^n$  für alle  $n \in \mathbb{N}$ .

Daraus ergibt sich für den Monoid  $(\mathbb{N}, 1, \cdot)$  die aus  $\mathbb{R}$  gewohnte Potenzierung. Nach welcher für ein  $x \in \mathbb{N}$  die Potenzierung  $x^n = x_1 \cdot x_2 \cdot \dots \cdot x_n$  ergibt. Betrachtet man jedoch den Monoid  $(\mathbb{N}, 0, +)$ , so ergibt analog dazu für ein  $x \in \mathbb{N}$  die Potenzierung  $x^n = x_1 + x_2 + \dots + x_n = x \cdot n$ , was also einer Multiplikation von  $x$  mit  $n$  entspricht.

## 1.2.2. Gruppe

**Definition: Gruppe** Eine algebraische Struktur  $(G, e, \cdot, inv)$  des Typs  $(0, 2, 1)$  heißt **Gruppe**, falls für alle  $x, y, z \in G$  die folgenden Axiome gelten:

- (Ass)  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- (Neu)  $e \cdot x = x \cdot e = x$
- (Inv)  $inv(x) \cdot x = e$

Gilt wiederum die Gleichung  $x \cdot y = y \cdot x$  für alle  $x, y \in G$ , so heißt  $(G, e, \cdot, inv)$  eine **kommutative Gruppe**.

### 1.2.2.1. Gruppe

### 1.2.2.2. Ring

### 1.2.2.3. Körper

## 1.3. Allgemeines zur Verschlüsselung

XXX

### 1.3.1. Symmetrische und Asymmetrische Verschlüsselung

x

### **1.3.2. Diffie-Hellmann**

x

### **1.4. Ziel der Arbeit**

XXX

### **1.5. Geplante Vorgehensweise**

XXX