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:	sXXXXXX@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

Abkürzungsverzeichnis

Abbildungsverzeichnis

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.

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

$$\mathbb{N}^+ = \{1, 2, 3, 4, 5, ...\}$$

und $\mathbb{N}_0$ inklusive der Zahl 0 als Teilmenge mit

$$\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, ...\}.$$

Die Primzahlen $\mathbb{P}$ sind hierbei etwas ganz besonderes. Sie unterscheiden sich von anderen Zahlen. Sie sind eine Teilmenge der natürlichen Zahlen und die Kardinalität ihrer Elemente ist 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. Auf die unendlichkeit der

Primzahlen sowie deren bestimmung wird später in 1.1.2 eingegangen.

Doch wie genau sind Primzahlen definiert? Dafür muss erst geklärt werden, was zusammengesetzte Zahlen sind. Dadurch können die Primzahlen klarer von anderen natürlichen Zahlen abgegrenzt werden. Eine natürliche Zahl mit $n \geq 2$ ist eine zusammengesetzte Zahl, falls es zwei natürliche Zahlen m und k mit den Eigenschaften:

$$m, k \geq 2 \text{ oder } m, k \neq n, \text{ für die gilt: } m \cdot k = n.$$

Zusammengesetzte natürliche Zahlen können also immer als Produkt zweier natürlicher Zahlen ≥ 2 beschrieben werden. Primzahlen bilden hierzu das Gegenstück. Eine Primzahl p ist eine natürliche Zahl mit $p \geq 1$, wobei p nur durch 1 und sich selbst teilbar sein darf. Durch diese Eigenschaft sind Primzahlen nicht zusammengesetzt. Sie können weder als Produkt von natürlichen Zahlen n mit $n \geq 2$ noch als Produkt von zwei Primzahlen beschrieben werden. Man nehme als Beispiel die Primzahl 7. Sie lässt sich nicht als Produkt von natürlichen Zahlen oder als Produkt von Primzahlen darstellen. Als Gegenbeispiel nimmt man die zusammengesetzte natürliche Zahl 28. Sie kann durch Multiplikation aus den Zahlen 2 und 14 gebildet werden:

$$2 \cdot 14 = 28.$$

Eine weitere Eigenschaft von Primzahlen ist, dass sie das Grundgerüst zur Bildung von Zahlen sind, da man aus ihnen alle natürlichen Zahlen bilden kann. Eine zusammengesetzte natürliche Zahl n mit $n \geq 2$ kann wie bereits beschrieben immer als Produkt von mindestens zwei weiteren natürlichen Zahlen dargestellt werden. Die einzelnen Faktoren können wiederum ebenfalls als Produkt von zwei weiteren natürlichen Zahlen dargestellt werden. Diese Aufteilung geht rekursiv so lange weiter, bis die Faktoren lediglich Primzahlen sind. Die übrig gebliebenen Faktoren dieses Produktes heißen Primfaktoren. Die Zerlegung einer zusammengesetzten natürlichen Zahl in ihre Primfaktoren nennt man Primfaktorzerlegung. Zweck dieser Primfaktorzerlegung ist es Zahl als Produkt von mehreren Primzahlen darzustellen. Nehmen wir als Beispiel die Zahl 28. Im vorigen Absatz stellten wir diese zusammengesetzte natürliche Zahl durch die Multiplikation von 2 und 14 dar. Die Zahl 2 ist eine Primzahl. Die Zahl 14 ist noch nicht in ihre Primzahlfaktoren zerlegt. Sie lässt sich als folgendes Produkt darstellen:

$$2 \cdot 7 = 14.$$

Da 7 auch eine Primzahl ist, wurden alle Primfaktoren gefunden. Die Zahl 28 lässt

sich in ihrer Primfaktorzerlegung also wie folgt darstellen:

$$2 \cdot 2 \cdot 7 = 28.$$

Die Mehrfachheit von Primzahlen lässt sich auch als Potenz schreiben. Somit wird daraus

$$2^2 \cdot 7 = 28.$$

Der Vorteil durch die Potenzen zeigt sich besonders bei großen Zahlen, da diese oft eine große Anzahl an Primfaktoren haben können. Nimmt man als Beispiel die Zahl 5281250000. Diese setzt sich mit ihren Primfaktoren wie folgt zusammen:

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 13 \cdot 13 = 5281250000.$$

Man erkennt rasch, dass sich die Primfaktoren mit der Potenzschreibweise zusammenfassen lassen und man so die Primfaktorzerlegung wie folgt darstellen kann:

$$2^4 \cdot 5^9 \cdot 13^2 = 5281250000.$$

Die Vorteile der Potenzschreibweise liegt hier auf der Hand, da man erheblich Zeit beim Aufschreiben und Platz auf dem Papier spart.

1.1.2. Bestimmung von Primzahlen

Nachdem die grundlegenen Eigenschaften der Primzahlen angeführt wurden, muss auf die Bestimmung von Primzahlen eingegangen werden. Paulo Ribenboim geht in seinem Buch „*Die Welt der Primzahlen: Geheimnisse und Rekorde*“der Frage auf den Grund, ob primzahldefinierende Funktionen existieren. An einer Stelle des Buches geht er auf diese möglichen Funktionen und ihre Eigenschaften ein [**Ribenboim.2011**]. Solch eine Funktion müsse laut ihm eine der folgenden drei Eigenschaften aufweisen, damit man sie zur Bestimmung von Primzahlen nutzen könne:

(a) $f(n) = p_n$ (die n-te Primzahl) für alle n ≥ 1;

(b) $f(n)$ ist immer prim und wenn n $\neq$ m, dann gilt: $f(n) \neq f(m)$;

(c) der positive Wertebereich der Funktion ist identisch mit der Menge der Primzahlen

Ribenboin erklärt, dass die Bedingung, um (a) zu erfüllen schärfer sei als (b) und als (c). Die bisher erzielten Resultate zur Findung einer Formel zur Bestimmung

von Primzahlen seien außerdem eher enttäuschend. Doch wenn die Funktionen zur Bestimmung von Primzahlen bisher enttäuschend waren, wie wurden diese bisher bestimmt?

Eine der simpelsten und sicher auch eine der ältesten Methoden ist das „Sieb des Eratosthenes“. Der Übersetzer Kai Brodersen beschreibt in seiner Übersetzung aus dem Jahre 2021 eines Buches aus dem Griechischen von Nikomachos von Gerasa, wie dieser sehr simpel die Funktionsweise des Siebes erläuterte [**Nikomachos+2021+7+7**]. Die Richtigkeit dieses Verfahrens wurde von Nikomachos im frühen 2. Jh. n. Chr. belegt. Bei dem Verfahren schreibt man alle natürlichen Zahlen von 2 bis zu einer gewählten Zahl n in eine Liste. Um die Primzahlen zu erhalten, siebt man jetzt die zusammengesetzten natürlichen Zahlen aus, indem man Vielfache streicht. Man beginnt bei der kleinsten Zahl, der 2. Man schreitet in der Liste fort und streicht alle Vielfachen der 2 bis zur höchsten gewählten Zahl n durch. Anschließend beginnt man mit der nächstgrößeren Zahl, welche nicht durchgestrichen ist respektive ausgesiebt wurde und streicht von dieser ebenfalls alle Vielfachen bis zur höchsten Zahl n durch. Den simplen Algorithmus führt man nun solange fort, bis man keine Vielfachen mehr streichen kann. Die übriggebliebenen Zahlen sind die Reihe der Primzahlen bis n. Die Darstellung in einer Tabelle ist heutzutage geläufig, da dies übersichtlicher ist. In der folgenden Tabelle wurde der Algorithmus des Siebes des Eratosthenes von 2 bis 100 angewandt:

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Das Sieb des Eratosthenes ist eine Möglichkeit, Primzahlen genau zu bestimmen. Problematisch wird es jedoch bei großen Zahlen. Für jede Zahl müssen je alle anderen Zahlen durchgegangen werden und es muss eine Teilbarkeitsprüfung durchgeführt werden. Umso größer die Zahlen werden, desto rechenaufwendiger wird die Anwendung

des Sieb des Eratosthenes, um Primzahlen zu finden. Dieses ist also kein optimaler Ansatz, große Primzahlen zu bestimmen. Neben dem Sieb des Eratosthenes gibt es viele weitere Methoden, Primzahlen zu bestimmen.

Die Besprechung aller dieser Verfahren und Algorithmen soll nicht Thema dieser Arbeit sein, jedoch soll noch eine gängige Methode erläutert werden. Über Probabilistische Verfahrne kö
WEITERSCHREIBEN

1.1.3. Rolle der Primzahlen in der Kryptografie

Primzahlen haben einen effektiven Nutzen in der Kryptografie. Bevor man sich fragt, wie Primzahlen in der Kryptografie genutzt werden, sollte man die Kryptografie vorher definieren. Dietmar Wätjen beschreibt diesne Begriff seinem Buch „*Kryptographie: Grundlagen, Algorithmen, Protokolle*“aus dem Jahr 2018 [**Watjen.2018**]. Kryptografie ist die Wissenschaft vom geheimen Schreiben. Kernziel ist es dabei, einen unverschlüsselten Text, genannt Klartext in einen Chiffretext überführt. Dieser Vorgang heißt *chiffrieren*. Der Vorgang, bei welchem der Chiffretext wieder in den Klartext überführt wird, heißt *dechiffrieren*. Für beide Vorgänge werden Schlüssel notwendig. Die Abbildung 1.1 stellt dies übersichtlich dar:

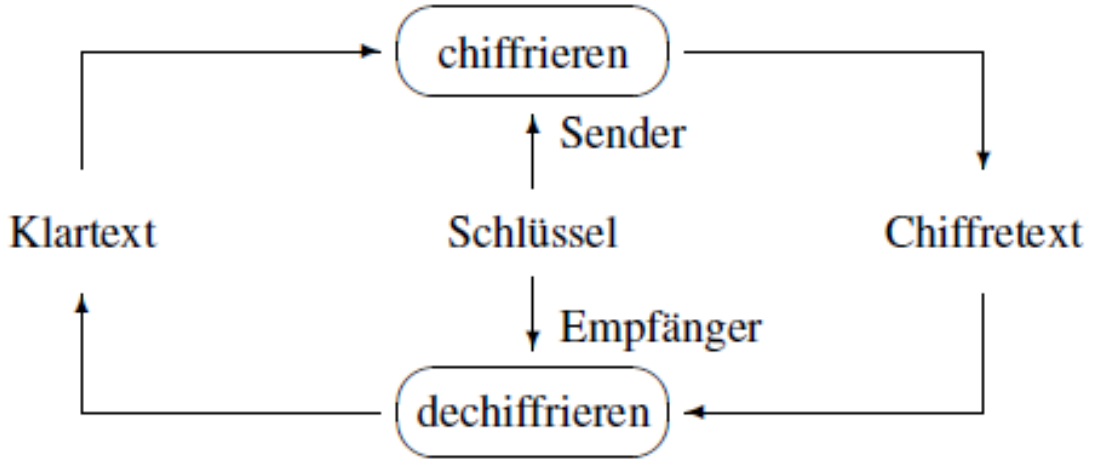

Abbildung 1.1.: Kryptografische Verschlüsselung
Quelle: [**Watjen.2018**]

Wätjen beshreibt Kryptografische System, auch Kryptosystem genannt, als ein System aus fünf Komponenten:

1. Klartextraum M
2. Chiffretextraum C
3. Schlüsselraum K
4. Familie von Chiffriertransformationen $E_k : M \to C$ mit $k \in K$
5. Familie von Dehiffriertransformationen $D_k : C \to M$ mit $k \in K$

Laut Watjen sind M, C und K höchstens, abzählbare Mengen. Eine Chiffriertransformation E_K wird durch einen Schlüssel K und einen Chiffrieralgorithmus E definiert, welcher für jede Familie gleich ist. Eine Dechiffriertransformation D_K wird ebenfalls durch einen Schhlüssel K bestimmt. Desweiteren sollen die Kryptografischen Systeme nach Watjen die folgenden drei Eigenschaften aufweisen:

(1) Klartextraum M

(2) Chiffretextraum C

(3) Schlüsselraum K

Laut
Durch die Kryptografie können dadurch Übertragungen von sensiblen Informationen zum einen sicherer als auch privater ablaufen, da ein abgefangenes Chiffrat nicht direkt lesbar ist.
Primzahlen sind aufgrund ihrer hervorragenden Eigenschaften für die Kryptologie nützlich. Viele Verfahren, welche den Klartext in einen Chiffretext überführen, benötigen für ihren Algorithmus Primzahlen. Ein gutes Beispiel ist der Diffie-Hellmann-Schlüsselaustausch
hier diffie-hellmann

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 $(M, c_1, \ldots, c_m, f_1, \ldots, f_n)$ 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 $f_i : M \to M$ im Fall $s = 1$ und $f_i : M^{s_i} \to M$ im Fall $s_i > 1$, genannt die (inneren) **Operationen**. Die lineare Liste$(0, \ldots, 0, s_1, \ldots, s_n)$ 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 heiß $(M, e, \cdot)$ 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 $x^n = x_1 \cdot x_2 \cdot \cdots \cdot x_n$ ergibt. Betrachtet man jedoch den Monoid $(\mathbb{N}, 0, +)$, so ergibt analog dazu für ein $x \in \mathbb{N}$ die Potenzierung $x^n = x_1 + x_2 + \cdots + x_n = x \cdot n$, 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) $e \cdot x = x$
- (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** oder Abelsche Gruppe.
In jeder Gruppe $(G, e, \cdot, inv)$ gelten für alle $x \in G$ folgende Formeln:

- $x \cdot x = x \Rightarrow x = e$
- $x \cdot e = x$
- $x \cdot inv(x) = e$
- $(\forall z \in G : x \cdot z = z) \Rightarrow x = e$
- $x \cdot y = e \Rightarrow x = inv(y)$
- $inv(x \cdot y) = inv(x) \cdot inv(y)$
- $inv(inv(x)) = x$

- $inv(e) = e$

Um Gruppen ein wenig anschaulicher zu machen, betrachten wir im Folgenden ein paar Beispiele:

- $(\mathbb{Z}, +)$ ist eine Gruppe. $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$ ist die Menge der ganzen Zahlen, welche zusammen mit der Addition als Gruppenoperation eine abelsche Gruppe bildet, wobei $e = 0$ das neutrale Element und $-a$ das Inverse eines beliebigen Elements $a \in \mathbb{Z}$ ist.

- Ein Gegenbeispiel ist $(\mathbb{Z} \setminus \{0\}, \cdot)$. Die Menge der ganzen Zahlen (ohne die 0) mit der Multiplikation als Gruppenoperation bildet keine Gruppe, da es kein Inverses Element $a^(- 1)$ für jedes Element $a \in \mathbb{Z}$ gibt.

1.2.3. Zyklische Gruppe

Die eben eingeführten Gruppen besitzen unendlich viele Elemente. Für die Kryptographie interessant sind jedoch endliche algebraische Strukturen, weshalb im Folgenden die endlichen Gruppen eingeführte werden.

Definition: Endliche Gruppe Eine Gruppe $(G, \circ)$ ist *endlich*, wenn sie eine endliche Anzahl an Elementen hat. Die Anzahl der Elemente der Gruppe wird als *Kardinalität* oder *Ordnung* der Gruppe G mit $|G|$ bezeichnet.
Beispiele für endliche Gruppen sind:

- $(\mathbb{Z}_n, +)$: Die Kardinalität von $\mathbb{Z}_n$ ist $|\mathbb{Z}_n| = n$, da $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$.

- $(\mathbb{Z}_n^*, \cdot)$: Die Menge $\mathbb{Z}_n^*$ besteht aus den positiven Zahlen kleiner n, die teilerfremd zu n sind, d.h. es gilt $ggt(a, n) = 1$ für jedes $a \in \mathbb{Z}_n^*$. Die Kardinalität ist daher durch die eulersche Phi-Funktion gegeben, d.h. $|\mathbb{Z}_n^*| = \Phi(n)$. So hat beispielsweise die Gruppe $\mathbb{Z}_9^*$ eine Kardinalität von $\Phi(9) = 3^2 - 3^1 = 6$. Die sechs Gruppenelemente sind $1, 2, 4, 5, 7, 8$.

Für die Konstruktion eines DLPs wird eine weitere Spezialisierung der endlichen Gruppen benötigt, die sogenannten zyklischen Gruppen. Einleitend dazu wollen wir zunächst den Begriff der Ordnung eines Elements definieren.

Definition: Ordnung eines Elements Die *Ordnung* $ord(a)$ eines Elements a einer Gruppe $(G, \circ)$ ist die kleinste positive ganze Zahl k mit

$$a^k = \underbrace{a \circ a \circ \cdots \circ a}_{k \text{ mal}} = e$$

wobei e neutrales Element von G ist.
Nachfolgend wollen wir ein Beispiel betrachten:
Wir suchen die Ordnung von $a = 3$ in der Gruppe $\mathbb{Z}_{11}^*$. Dazu berechnen wir die Potenzen von a bis wir das neutrale Element 1 erhalten.

$$\begin{aligned}
a^1 &= 3 \\
a^2 &= a \cdot a = 9 \\
a^3 &= a^2 \cdot a = 27 \equiv 5 \bmod 11 \\
a^4 &= a^3 \cdot a = 15 \equiv 4 \bmod 11 \\
a^5 &= a^4 \cdot a = 12 \equiv 1 \bmod 11
\end{aligned}$$

Aus der letzten Zeile folgt $\text{ord}(3) = 5$ in $\mathbb{Z}_{11}^*$.
Es ist interessant zu sehen, was passiert, wenn man weiter mit a multipliziert:

$$\begin{aligned}
a^6 &= a^5 \cdot a = 1 \cdot a \equiv 3 \bmod 11 \\
a^7 &= a^5 \cdot a^2 = 1 \cdot a^2 \equiv 9 \bmod 11 \\
a^8 &= a^5 \cdot a^3 = 1 \cdot a^3 \equiv 5 \bmod 11 \\
a^9 &= a^5 \cdot a^4 = 1 \cdot a^4 \equiv 4 \bmod 11 \\
a^{10} &= a^5 \cdot a^5 = 1 \cdot a^5 \equiv 1 \bmod 11 \\
a^{11} &= a^{10} \cdot a = 1 \cdot a \equiv 3 \bmod 11 \\
&\vdots
\end{aligned}$$

Wie zu sehen ist, durchlaufen die Potenzen von a nach Erreichen des neutralen Elements e immer wieder die Sequenz $\{3, 9, 5, 4, 1\}$. Mit diesem Wissen können wir jetzt eine zyklische Gruppe definieren.

Definition: Zyklische Gruppe Eine Gruppe G, die ein Element α mit der maximalen Ordnung $\text{ord}(\alpha) = |G|$ enthält nennt man *zyklisch*. Elemente mit maximaler Ordnung nennt man *primitive Elemente* oder *Generatoren*.

Der Name *Generator* kommt daher, dass durch die Potenzierung $\alpha^i = a$ des primitiven Elements jedes andere Gruppenelement a dargestellt werden kann, also die gesamte Gruppe *generiert* wird. Das folgende Beispiel zeigt die Erzeugung der zyklischen

Gruppe $\mathbb{Z}_{11}^*$ durch das primitive Element $\alpha = 2$.

$$\begin{aligned} a &= 2 & a^6 &\equiv 9 \bmod 11 \\ a^2 &= 4 & a^7 &\equiv 7 \bmod 11 \\ a^3 &= 8 & a^8 &\equiv 3 \bmod 11 \\ a^4 &\equiv 5 \bmod 11 & a^9 &\equiv 6 \bmod 11 \\ a^5 &\equiv 10 \bmod 11 & a^{10} &\equiv 1 \bmod 11 \end{aligned}$$

Aus der letzten Gleichung folgt, dass $\text{ord}(a = 2) = 10 = |\mathbb{Z}_{11}^*|$. Damit ist gezeigt, dass das Element $a = 2$ wirklich ein Generator der zyklischen Gruppe $\mathbb{Z}_{11}^*$ ist.
Wie man aus den eben gezeigten Beispielen erkennen kann, sind einige Gruppenelemente Generatoren der Gruppe und andere nicht. Welche Ordnungen der Elemente in einer zyklischen Gruppe vorkommen hängt davon ab, welche natürlichen Zahlen die Gruppenkardinalität teilen. Betrachten wir nun wieder die Gruppe $\mathbb{Z}_{11}^*$, deren Kardinalität $|\mathbb{Z}_{11}^*| = 10$ ist, so ergeben sich mögliche Ordnungen der Elemente von $1, 2, 5$ und 10, da diese die einzigen natürlichen Zahlen sind die 10 teilen. Folgende Veranschaulichung zeigt dies.

$$\begin{aligned} \text{ord}\ (1) &= 1 & \text{ord}\ (6) &= 10 \\ \text{ord}\ (2) &= 10 & \text{ord}\ (7) &= 10 \\ \text{ord}\ (3) &= 5 & \text{ord}\ (8) &= 10 \\ \text{ord}\ (4) &= 5 & \text{ord}\ (9) &= 5 \\ \text{ord}\ (5) &= 5 & \text{ord}\ (10) &= 2 \end{aligned}$$

Satz: Primitive Elemente in einer zyklischen Gruppe G Ist G eine zyklische Gruppe, dann gilt:

1. Die Anzahl der primitiven Elemente in G ist $\Phi(|G|)$.
2. Ist $|G|$ prim, dann sind alle Elemente $a \neq 1 \in G$ primitiv.

Die erste Eigenschaft kann leicht gezeigt werden durch, $\Phi(10) = (5-1)(2-1) = 4$. Es muss also vier primitive Elemente in $\mathbb{Z}_{11}^*$ geben, welche konkret die Elemente $2, 6, 7$ und 8 sind. Die zweite Eigenschaft folgt implizit aus der ersten, da bei einer primen Kardinalität der Gruppe keine natürliche Zahl außer der 1 und der Kardinalität selber die Gruppenkardinalität teilt, und diese somit die einzigen möglichen

Elementordnungen sind. Da nur das Element 1 die Ordnung 1 haben kann, haben alle anderen Elemente die Ordnung $|G|$, sind also Generatoren der Gruppe.

1.2.4. Untergruppen

Untermengen innerhalb zyklischer Gruppe können wiederum selbst Gruppen sein. Solche werden als Untergruppen bezeichnet. Im Fall von zyklischen Gruppen ist die Anzahl der jeweiligen Untergruppen leicht zu ermitteln. Sie entspricht nämlich genau der Anzahl an natürlichen Teilern der Gruppenkardinalität, wie aus dem folgenden Satz von Lagrange hervorgeht.

Satz: Satz von Lagrange Sei H eine Untegruppe von G. Dann teilt $|H|$ die Gruppenkardinalität $|G|$.
Das *Finden* zyklischer Untergruppen innerhalb einer zyklischen Gruppe wird durch folgenden Satz gezeigt.

Satz: zyklische Untergruppen Sei $(G, \circ)$ eine zyklische Gruppe. Dann ist jedes Element $a \in G$ mit $\text{ord}(a) = s$ ein primitives Element einer zyklischen Untergruppe mit s Elementen.
Die Kernaussage dieses Satzes ist, dass jedes Element einer zyklischen Gruppe Generator einer zyklischen Untergruppe ist. Wir betrachten erneut die zyklische Gruppe $\mathbb{Z}_{11}^*$. Wie oben bereits gezeigt hat das Gruppenelement $a = 3$ die Ordnung 5, ist also Generator einer Untergruppe mit mit 5 Elementen. Die Elemente dieser Untergruppe sind eben jene, welche durch die Potenzierung von 3 mod 11 erzeugt werden können, also $\{3, 9, 5, 4, 1\}$. So kann für jedes Element verfahren werden, alle Untergruppen von $\mathbb{Z}_{11}^*$ gezeigt werden können. Folgende Aufstellung zeigt beispielhaft alle Untergruppen von $\mathbb{Z}_{11}^*$.

Ordnung: 1 Generatoren: $\{1\}$ Elemente: $\{1\}$

Ordnung: 2 Generatoren: $\{10\}$ Elemente: $\{1, 10\}$

Ordnung: 5 Generatoren: $\{3, 4, 5, 9\}$ Elemente: $\{1, 3, 4, 5, 9\}$

Ordnung: 10 Generatoren: $\{2, 5, 7, 8\}$ Elemente: $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Wie zu erkennen ist, kann es mehrere Generatoren der selben Untergruppe geben. Außerdem interessant ist die Tatsache, dass Untergruppen primer Ordnung p abgesehen von dem neutralen 1 keine Überschneidungen mit anderen Untergruppen primer Ordnung aufweisen, da jedes Element die Ordnung p hat und somit Generator

der Untergruppe ist. Dies verdeutlicht, dass der Satz *Primitive Elemente in einer zyklischen Gruppe* auch für zyklische Untergruppen gilt.
Der folgende Satz fasst die Erkenntnisse des letzten Abschnitts zusammen und gibt eine Methode zur Konstruktion einer Untergruppe für eine gegebene zyklische Gruppe.

Satz: Konstruktion einer zyklischen Untergruppe Sei G eine endliche zyklische Gruppe der Ordnung n und sei α ein Generator von G. Dann existiert für jede ganze Zahl k, die n teilt, genau eine zyklische Untergruppe H von G mit der Ordnung k. Diese Untergruppe wird erzeugt von $\alpha^{n/k}$. H besteht genau aus den Elementen $a \in G$, die die Bedingung $a^k = 1$ erfüllen. Es gibt keine weiteren Untergruppen.
Mit anderen Worten sagt dieser Satz, dass lediglich ein primitives Element α und die Ordnung einer zyklischen Gruppe $|G|$ benötigt wird, um alle Untergruppen von G zu konstruieren. Im folgenden Beispiel wollen wir dies zu Konstruktion einer Untergruppe anwenden.
Betrachten wird erneut die zyklische Gruppe $\mathbb{Z}_{11}^*$ und das primitive Element $\alpha = 6$. Wenn wir nun eine Generator β der Untergruppe mit der Ordnung $k = 5$ finden möchten, berechnen wir:

$$\beta = \alpha^{n/k} = 6^{10/5} = 6^2 = 36 \equiv 3 \bmod 11$$

Wie wir oben schon gezeigt haben ist 3 tatsächlich ein Generator der Untergruppe $\{1, 3, 4, 5, 9\}$ mit $k = 5$ Elementen.

1.2.5. Ring

Ein **Ring** ist eine algebraische Struktur $(R, 0, 1, +, \cdot, -)$ des Typs $(0, 0, 2, 2, 1)$ mit den folgenden Eigenschaften:

1. Es ist $(R, 0, +, -)$ eine kommutative Gruppe
2. Es ist $(R, 1, \cdot)$ ein Monoid.
3. Für alle $x, y, z \in R$ gelten die Distributivgesetze $x(y + z) = xy$ und $(y + z)x = yx + zx$

Ist $(R, 1, \cdot)$ ein kommutatives Monoid, so nennt man $(R, 0, 1, +, \cdot, -)$ einen kommutativen Ring.

1.2.6. Körper

1.3. Allgemeines zur Verschlüsselung

XXX

1.3.1. Symmetrische und Asymmetrische Verschlüsselung

x

1.4. Das diskrete Logarithmusproblem

Das DLP bildet die mathematische Grundlage für viele asymmetrische Kryptosysteme, wie den DHKE oder die Elgamal-Verschlüsselung. Etwas legere ausgedrückt könnte man das DLP als Baukasten für asymmetrische Kryptosysteme betrachten, da es für zyklische Gruppen verallgemeinert werden kann. Im Folgenden wollen wir zunächst das DLP in Primzahlkörpern betrachten. Hierzu greifen wir auf die in Kapitel XY erläuterten Eigenschaften zyklischer Gruppen zurück.

Definition: Diskretes Logarithmusproblem (DLP) in $\mathbb{Z}_p^*$ Gegeben sind die endliche zyklische Gruppe $\mathbb{Z}_p^*$ der Ordnung $p-1$, ein primitives Element $\alpha \in \mathbb{Z}_p^*$ und ein weiteres Element $\beta \in \mathbb{Z}_p^*$. Das DLP ist das Problem, eine ganze Zahl x im Bereich $1 \leq x \leq p-1$ zu finden, sodass:

$$\alpha^x \equiv \beta \bmod p$$

Wie in Kapitel XY gezeigt, muss ein solches x existieren, da α ein primitives Element ist, was bedeutet dass jedes andere Gruppenelement durch die Potenzierung α^x dargestellt werden kann. Das gesuchte x wird als *diskreter Logarithmus* von β zur Basis α bezeichnet. Formal beschrieben als:

$$x = \log_\alpha \beta \bmod p.$$

Anders als der gewöhnliche Logarithmus in $\mathbb{R}$ ist der diskrete Logarithmus in einer endlichen zyklischen Gruppe nicht effizient zu berechnen. Grund dafür sind die Eigenschaften endlicher zyklischer Gruppen. Denn wie in Kapitel XY gezeigt, generiert die Potenzierung eines primitiven Elements α die jeweilige zyklische Gruppe bzw.

Untergruppe in einer nicht absehbaren Reihenfolge.

Für kleinere Gruppen lässt sich x natürlich durch stumpfes Ausprobieren sog. *brute Force* in einer kurzen Zeit ermitteln. Diskrete Logarithmen in ausreichend großen Gruppen sind jedoch sehr schwer zu ermitteln.

Um den diskreten Logarithmus x von $\alpha^x \equiv \beta \bmod p$ zu ermitteln muss ein potenzieller Angreifer jedes x zwischen 1 und $p-1$ als möglichen Exponenten ausprobieren. Der Erzeuger kann zum effizienten berechnen von β, jedoch den Square-and-Multiply-Algorithmus verwenden, was das DLP zu einer Einwegfunktion macht.

Neben dem trivialen brute Force Angriff auf das DLP gibt es weitere Verfahren, welche die Menge an möglichen x Werten einschränken. Der Babystep-Giantstep-Algorithmus reduziert die Komplexität des DLPs von $O(n)$ auf $O(\sqrt{n})$. Noch weiter kann die Komplexität durch den Pohling-Hellman-Algorithums eingeschränkt werden. Durch diesen Angriff kann bei bekannter Primfaktorzerlegung der Gruppenordnung n, die Komplexität des DLPs auf $O(\sqrt{q})$ reduzieren, wobei q der größte Faktor von n ist. Aus diesem Grund wählt man in der Praxis eine Gruppe mit primer Ordnung für das DLP. Da die Ordnung von Gruppen $\mathbb{Z}_p^*$ dem Wert $p-1$ entspricht, der offensichtlich nicht prim ist, greift man auf Untergruppen von $\mathbb{Z}_p^*$ mit primer Ordnung zurück.

1.4.0.1. Das verallgemeinerte diskrete Logarithmusproblem

Wie oben bereits erwähnt kann das DLP in jeglichen zyklischen Gruppen definiert werden. Bis jetzt haben wir immer die zyklische Gruppe $\mathbb{Z}_p^*$ betrachtet. Das DLP kann folgendermaßen verallgemeinert werden:

Definition: Verallgemeinertes diskretes Logarithmusproblem Gegeben sei eine endliche zyklische Gruppe G mit der Gruppenoperation $\circ$ und der Kardinalität n. Wir betrachten ein primitives Element $\alpha \in G$ und ein weiteres Element $\beta \in G$. Das diskrete Logarihtmusproblem liegt darin, eine ganze Zahl x im Bereich $1 \leq x \leq n$ zu finden, sodass:

$$\beta = \underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{x \text{ mal}} = \alpha^x$$

Auch hier ist die Existenz von x sicher, da α als primitives Element die gesamte Gruppe generiert. Das DLP lässt sich zwar in jeglichen zyklischen Gruppen definieren, jedoch ist es in einigen nicht *schwierig* zu lösen, wodurch es keine Einwegfunktion

mehr darstellt. Ein Beispiel dafür sind additive Gruppen $G = (\mathbb{Z}_p, +)$. Die x-fache Anwendung der Gruppenoperation auf einen Generator α zur Erzeugung eines Elements β kann als *Multiplikation* mod p dargestellt werden. Der gesuchte Faktor x lässt sich dann leicht durch die Multiplikation von β und inv(α) berechnen. Letzteres lässt sich effizient mittels des EEAs ermitteln.
Gruppen auf denen ein DLP für kryptografische Zwecke definiert werden kann sind:

1. Multiplikative Gruppen des Primkörpers $\mathbb{Z}_p$ oder Untergruppen davon. Der DHKE nutz klassischerweise diese Gruppen. Auch die Elgamal-Verschlüsselung und der digitale Signaturalgorithmus (DSA) nutzen diese Gruppen.

2. Zyklische Gruppen welche über elliptischen Kurven gebildet werden. Das DLP ist in diesen Gruppen besonders schwer zu lösen, da kein Algorithmus bekannt ist, der die Komplexität des DLPs stark reduziert, wie dies beispielsweise beim DLP in $\mathbb{Z}_p^*$ durch den Babystep-Giantstep-Algorithmus möglich ist. Deshalb werden diese Gruppen in modernen Kryptosystemen zunehmend eingesetzt, mit dem Effekt, dass gleiche Sicherheit mit deutlich geringerer Schlüssellänge erzielt werden kann.

3. Multiplikative Gruppen von endlichen Körpern $GF(2^m)$ oder Untergruppen davon. Sie sind in der Praxis weniger verbreitet, und es nicht vollständig geklärt ob Angriffe auf das DLP in $GF(2^m)$ nicht effizienter sind als jene gegen das DLP in Primkörpern.

4. Hyperelliptische Kurven oder algebraische Varietäten, die auch Verallgemeinerungen von elliptischen Kurven sind. Trotz einiger Vorteile gegenüber den klassischen elliptischen Kurven, sind die hyperelliptischen Kurven in der Praxis nicht sehr verbreitet.

Es gab im Laufe der Zeit einige weitere Vorschläge für mögliche Gruppen gegeben, welche jedoch nicht weiter verfolgt wurden, da sich meist herausstellte, dass das DLP einfacher zu lösen ist.

1.4.1. Diffie-Hellmann Key Exchange

x

1.5. Ziel der Arbeit

XXX

1.6. Geplante Vorgehensweise

XXX

2. Elliptische Kurven

Als Basis für asymmetrische Kryptosysteme können elliptische Kurven dazu genutzt werden, die verschlüsselungstechnische Effektivität mathematischer Probleme, wie das des diskreten Logarithmus, zu erhöhen. Bei der Kryptographie unter Verwendung elliptischer Kurven bei deutlich kürzerer Schlüssellänge ein gleichwertigers Ergebnis erzielt werden. Dieser Effekt wird durch die spezielle Arithmetik auf elliptischen Kurven erzielt, deren mathematische Grundlage, konkrete Eingenschaften und Funktionsweise im folgenden Kapitel erörtert werden soll.

Elliptische Kurven können über beliebigen Körpern definiert werden. Für die Kryptographie interessant sind elliptische Kurven über Primkörpern.
Um das weitere Verständnis zu verbessern, wollen wir erst eine uns schon bekannte Kurve ansehen. In Abbildung XY ist das Polynom $x^2 + y^2 = r^2$ über $\mathbb{R}$ dargestellt. Wie zu sehen ist, handelt es sich hierbei um die Kreisgleichung. Der zu sehende Kreis ist nichts anderes als die Menge aller Punkte, welche die Kreisgleichung erfüllen. Ein Beispiel für eine solchen ist der Punkt $(r, 0)$. Wenn x den Wert r hat, muss y folglich den Wert 0 haben. Ein Gegenbeispiel ist der Punkt $(r, r/2)$. Dieser erfüllt die Kreisgleichung nicht. Die Kreisgleichung kann verallgemeinert werden, indem

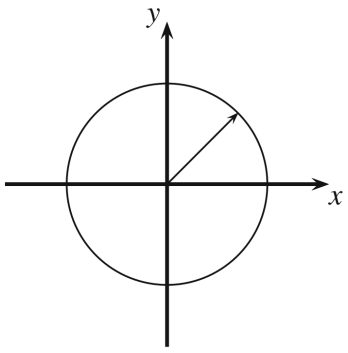

Abbildung 2.1.: r

den Termen x^2 und y^2 Koeffizienten voran gesetzt werden. Eine solche Gleichung, $ax^2 + by^2 = c$ erzeugt über $\mathbb{R}$ eine Ellipse, wie in Abbildung XY zu sehen.

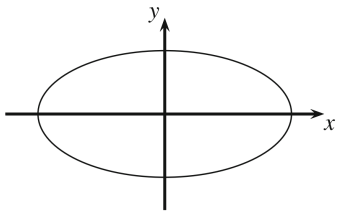

Abbildung 2.2.: r

Eine elliptische Kurve ist nun eine spezielle Polynomgleichung, der Form $y^2 = x^3+ax+b$, unter der Bedingung $4a^3+27b^3 \neq 0$. Eine solche Gleichung über $\mathbb{R}$ ist in Abbildung XY dargestellt. Damit elliptische Kurven sinnvoll in der Kryptologie eingesetzt werden

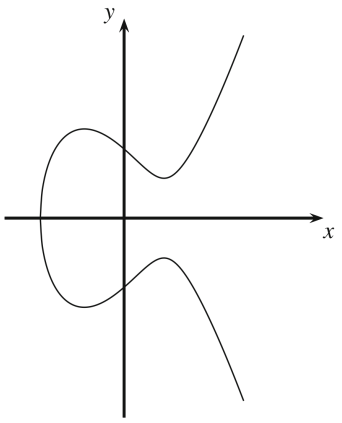

Abbildung 2.3.: r

können, muss die Polynomgleichung über einem Primkörper betrachtet werden. Das heißt einfach gesprochen, alle Berechnungen werden modulo p durchgeführt.

Definition: Elliptische Kurven über Primkörpern Die *elliptische Kurve* über $\mathbb{F}_{\text{|}}$, ist die Menge aller Punkte (x, y) mit $x, y \in \mathbb{F}_{\text{|}}$, welche die folgende Gleichung erfüllen:

$$y^2 \equiv x^3 + ax + b \bmod p, \text{ wobei } a, b \in \mathbb{F}_{\text{|}}$$

und die Bedingung

$$4a^3 + 27b^3 \neq 0$$

gelten müssen. Zu der elliptischen Kurve gehört des Weiteren auch der imaginäre *Punkt im Unendlichen* $\mathcal{O}$.

Durch die Bedingung XY werden sog. Singularitäten ausgeschlossen. Andernfalls gäbe es Punkte, deren Tangente nicht wohldefiniert ist, was für das Rechnen auf elliptischen Kurven jedoch erforderlich ist.

Nachdem elliptische Kurven nun definiert wurden, stellt sich die Frage, wie diese in der Kryptographie eingesetzt werden können. Wenn wir uns an das in Kapitel XY zurückerinnern, wird für die Konstruktion eines **DLP**s eine zyklische Gruppe benötigt. Eine eben solche findet sich in der Punktmenge der elliptischen Kurve wieder. Offen bleibt wie die Gruppenoperation definiert ist. Diese muss die in Kapitel XY geforderten Gruppengesetze erfüllen.

Als Symbol für die Gruppenoperation wird das Additionszeichen + verwendet. Durch die Gruppenoperation muss aus zwei Punkten $P = (x_1, y_2)$ und $Q = (x_2, y_2)$ der Kurve ein dritter Punkt R auf der Kurve berechnet werden.

$$P + Q = R$$

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

Am verständlichsten lässt sich diese Operation grafisch zeigen.
Elliptische Kurven über endlichen Körpern können grafisch nicht sinnvoll dargestellt werden. Ihre Form und Arithmetik lassen sich jedoch gut veranschaulichen wenn man sie auf $\mathbb{R}$ abbildet. Im Folgenden betrachten wir eine Elliptische Kurve, dargestellt in einem kartesischen Koordinatensystem, um die Gruppeneigenschaften bezüglich der Punktaddition zu zeigen. Hierbei sind nun zwei Fälle zu unterscheiden.

Punktaddition $P + Q$: Falls $P \neq Q$ erfolgt die geometrische Konstruktion, indem zunächst eine Grade durch die beiden Punkte gelegt wird. Aufgrund der Kurveneigenschaften hat diese immer einen dritten Schnittpunkt mit der Kurve. Dieser wird an der x-Achse gespiegelt um den gesuchten Punkt R zu erhalten. Abbildung XY zeigt die beschriebene Konstruktion.

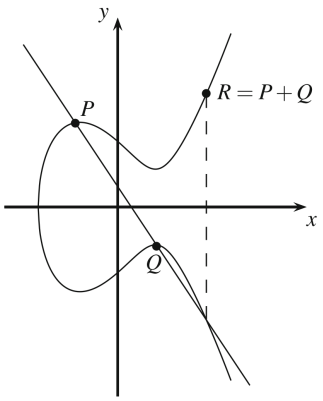

Abbildung 2.4.: r

Punktverdopplung $P + P$: Falls P und Q identisch sind erfolgt die geometrische Konstruktion, indem eine Tangente an den Punkt P angelegt wird. Diese liefert wieder einen weiteren Schnittpunkt mit der Kurve, welcher an der x-Achse gespiegelt wird um den Punkt R zu erhalten. Anstatt $R = P + Q$ schreibt man in diesem Fall $R = P + P = 2P$ Abbildung XY zeigt die beschriebene Konstruktion.

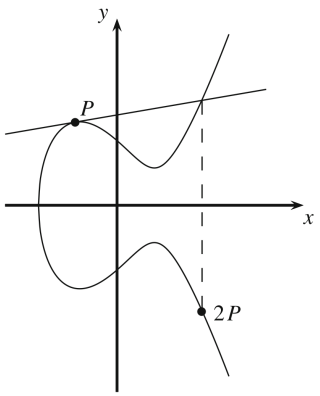

Abbildung 2.5.: r

Nach dieser grafischen Veranschaulichung sollte es leichter fallen die folgenden Formeln für die Punktaddition bzw. Punktverdopplung nachvollziehen zu können. Die Gruppenoperation existiert in jedem Körper, weshalb die Berechnung von R, wie grade gezeigt über den reellen Zahlen $\mathbb{R}$, als auch über einem Primkörper $\mathbb{F}_p$ durchgeführt werden kann.

Die Formeln für die Punktaddition und - verdopplung auf elliptischen Kurven können anhand der grade gezeigten Veranschaulichung hergeleitet werden. Das Vorgehen hierbei ist prinzipiell recht simpel.

Herleitung: Formeln für Punktaddition bzw. Punktverdopplung Gegeben ist die Gleichung der elliptischen Kurve $y^2 = x^3 + ax + b$ und die Punkte $P = (x_1, y_1)$ und $Q = (x_2, y_2)$. Zunächst ist die Geradengleichung der Sekante durch P und Q zu ermitteln. Eine Grade im Allgemeinen hat die Form

$$g : y = sx + m.$$

Der Parameter s ist dabei die Steigung der Geraden und m ist der Schnittpunkt mit der y-Achse. Die Steigung s lässt sich (im Fall der Punktaddition) wie gewohnt

durch Anlegen des Steigungsdreiecks berechnen, also mit der Formel

$$s = \frac{y_2 - y_1}{x_2 - x_1}.$$

. Im Falle einer Punktverdopplung muss s über die Tangente der Elliptischen Kurve im entsprechenden Punkt ermittelt werden. Dazu leiten leiten wir die Kurvengleichung der elliptischen Kurve nach x ab. Es ergibt sich

$$\frac{\delta y}{\delta x} = \frac{3x^2 + a}{2\sqrt{x^3 + ax + b}}$$

Bei genauerer Betrachtung fällt auf, dass der Nenner genau $2y$ entspricht, weshalb auch

$$\frac{\delta y}{\delta x} = \frac{3x^2 + a}{2y}$$

geschrieben werden kann. Da die erste Ableitung die Steigung der elliptischen Kurve in jedem Punkt beschreibt, haben wir somit eine Formel mit welcher wird durch einsetzen eines Punktes $P = (x_1, y_1)$, die jeweilige Tangentensteigung ermitteln können. Es gilt also

$$s = \frac{3x_1^2 + a}{2y_1}.$$

Zur Bestimmung des Schnittpunkts mit der y-Achse kann nun einer der beiden Punkte P oder Q in die Geradengleichung $y = s * x + m$ eingesetzt werden. Durch Einsetzen des Punkts $P = (x_1, y_1)$ erhalten wir die folgende Gleichung

$$y_1 = s * x_1 + m,$$

welche nach m aufgelöst folgendermaßen aussieht:

$$m = y_1 - s * x_1$$

Durch Einsetzten aller Parameter in die obige Geradengleichung ergibt sich

$$y = \frac{y_2 - y_1}{x_2 - x_1} * x + y_1 - \frac{y_2 - y_1}{x_2 - x_1} * x_1$$

für die gesuchte Gerade g durch die Punkte P und Q. Um den dritten Schnittpunkt dieser Geraden g mit der elliptischen Kurve E zu ermitteln, sind beide Kurven gleichzusetzen. Da es für das weitere Vorgehen keine Rolle spielt und es der Übersichtlichkeit dient, werden im Folgenden wieder die Parameter s und m statt eben

gezeigten Konkretisierungen verwendet. Es ergibt sich die Gleichung

$$(sx + m)^2 = x^3 + ax + b.$$

Nach ausmultiplizieren der Gleichung erhalten wir

$$0 = x^3 - s^2x^2 + (a - 2sm) \cdot x - m^2 + b.$$

Im Normalfall ist das allgemeine Lösen eines solchen kubischen Polynoms nicht trivial. Wir haben hier jedoch den Vorteil, dass zwei der drei Schnittpunkte von g mit E schon bekannt sind. Fassen wir das Polynom als Funktion

$$f(x) = x^3 - s^2x^2 + (a - 2sm) \cdot x - m^2 + b$$

auf, so sind wir Im Grunde auf der Suche nach den Nullstellen dieser kubischen Funktion. Da die Punkte P und Q auf der Geraden g sowie auf der elliptischen Kurve E liegen, lösen sie die obige F Gleichung, sind also Nullstellen der Funktion $f(x)$. Daraus folgt, dass die Funktion $f(x)$ restlos durch $(x - x_1)$ und $(x - x_2)$ geteilt werden kann um den Funktionsgrad zu verringern.

$$f(x) \div (x - x_1) \cdot (x - x_2) = l(x) \text{ Rest } 0$$

Aufgrund dessen, dass $f(x)$ den Grad 3 hat, muss $l(x)$ den Grad 1 haben und durch $l(x) = ux + v$ beschrieben werden können. Da

$$l(x) + (x - x_1) \cdot (x - x_2) = g(x),$$

muss auch gelten

$$u \cdot x \cdot x \cdot x = x^3,$$

weshalb $u = 1$ gelten muss. Daraus ergibt sich

$$l(x) = x + v.$$

Somit ist $x_3 = -v$ eine weitere Nullstelle von $f(x)$. Es folgt also

$$g(x) = (x - x_1) \cdot (x - x_2) \cdot (x - x_3),$$

woraus durch ausmultiplizieren

$$f(x) = x^3 - (x_1 + x_2 + x_3) \cdot x^2 + (x_1x_2 + x_1x_3 + x_2x_3) * x - x_1x_2x_3$$

entsteht. Vergleicht man nun diese Darstellung mit der obigen also

$$f(x) = x^3 - s^2x^2 + (a - 2sm) \cdot x - m^2 + b,$$

so folgt durch Koeffizientenvergleich

$$s^2 = x_1 + x_2 + x_3$$

also

$$x_3 = x^2 - x_1 - x_2$$

Um die Formel für y_3 zu ermitteln kann nun der Punkt R in die Formel für s eingesetzt werden. Dies ist möglich, da der Punkt R auf der gleichen Geraden wie P und Q liegt, weshalb auch die Steigung s identisch ist. Es gilt also

$$s = \frac{y_2 - y_1}{x_2 - x_1} = \frac{y_3 - y_1}{x_3 - x_1}.$$

Aufgelöst nach y_3 ergibt sich

$$y_3 = s \cdot (x_3 - x_1) + y_1.$$

Da der Schnittpunkt an der x-Achse gespiegelt wird um R zu erhalten müssen die Vorzeichen in der Formel für y noch gedreht werden. Final ergeben sich für den Punkt $R = (x_3, y_3)$ also die Formeln:

$$x_3 = s^2 + x_1 - x_2$$

$$y_3 = s \cdot (x_1 - x_3) - y_1$$

Formel: Punktaddition und -verdopplung auf elliptischen Kurven:

$$x_3 = s^2 - x_1 - x_2$$

$$y_3 = s(x_1 - x_3) - y_1$$

, wobei

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{, falls } P \neq Q \text{ (Punktaddition)} \\ \frac{3x_1^2 + a}{2y_1} & \text{, falls } P = Q \text{ (Punktverdopplung)} \end{cases}$$

Zur Erfüllung der Gruppeneigenschaften wird außerdem ein neutrales Element $\mathcal{O}$ benötigt. Alle Punkte P der elliptischen Kurve müssen die Eigenschaft $P + \mathcal{O} = P$. Da kein Punkt der elliptischen Kurve diese Eigenschaft erfüllen kann, wird der imaginäre *unendlich ferne Punkt* als neutrales Element $\mathcal{O}$ definiert. Dieser Punkt liefert den dritten *Schnittpunkt* mit der Kurve im Falle, dass ein Punkt P und der bezüglich der x-Achse gegenüberliegende Punkt $-P$ addiert werden. Abbildung XY zeigt den Fall grafisch.
Die Existenz eines neutralen Elements ermöglicht die Definition eines Inversen $-P$ für jeden Punkt P auf der Kurve, für welches $P + (-P) = \mathcal{O}$. Wie Abbildung XY entnommen werden kann, ist für den Punkt $P = (x_p, y_p)$ das Inverse also $-P = (y_p, -y_p)$ zu definieren. In einem Primkörper berechnet sich die negative y-Koordinate durch $-y_p = p - y_p$.

2.1. Punktbestimmung

Die Arithmetik für Elliptische Kurven wurde bereits besprochen. Nun wird erarbeitet, wie man die Punkte einer elliptischen Kurve bestimmt. Doch was ist ein Punkt einer elliptischen Kurve? Im Foglenden wird erklärt, was ein Punkt auf einer elliptischen Kurve ist und wie diese berehcnet werden können. Die Erklärungen werden anschließend anhand einiger Beispiele näher erläutert. Anschließend wird Python-Code präsentiert, welcher die Punktbestimmung für eine elliptische Kurve mit p > 3 durchführt und die Punkte anschließend in der Konsole ausgibt.

2.1.1. Rechnerische Grundlagen

Viele Mathematiker suchten eine Formel, mit denen sich die Anzahl der Punkte einer elliptischen Kurve schätzen lässt, ohne dass man diese vorher aus- oder berechnen muss. Joseph H. Silverman beweist in seinem Buch einen mathematischen Satz aus der Zahlentheorie, welcher eine allgemeine Aussage über die Anzahl der rationalen Punkte auf einer elliptischen Kurve trifft [**silverman**]. Dieser Satz kann also herangezogen werden, um eine ungefähre Abschätzung über die Anzahl der Punkte auf einer elliptischen Kurve über einem Primkörper p zu treffen. Bei dem mathematischen Satz handelt es sich um die Hasse–Weil–Schranke. Diese wird im allgemeinen dafür benutzt, um die Anzahl der Lösungen der Gleichung und der Bedingungen aber auch

für die Einschränkung des Lösungsraums. Die Hasse-Weil-Schranke wird angelehnt an [**reinholdhuebl**] wie folgt beschrieben. Sei k = $\mathbb{F}_p$ ein endlicher Körper und $\overline{E}$ eine elliptische Kurve über k, dann gilt

$$p + 1 - 2 \cdot \sqrt{p} \leq |\overline{E}| \leq p + 1 + 2 \cdot \sqrt{p}$$

Was ist jedoch die Hauptaussage der Hasse-Weil-Schranke? Sie besagt, dass sich bei großen p die Anzahl der Elemente der elliptischen Kurve in der Größenoprdnung von p bewegen. Diese Schranke bildet hierbei eine obere und untere Grenze. Die Anzahl der Punkte bewegt sich also innerhalb dieser Schranke. Dies ist für elliptische Kurven mit kleinem p uninteressant, jedoch wird diese Schranke für elliptische Kurven mit großem gewählten p, was in der Kryptographie gängig ist, relevant.

Doch wie lassen sich die Punkte konkret berechnen? Um diese Frage zu beantworten, müssen wir noch einmal die Grundlagen für elliptische Kurven aufgreifen. Wie Reinhold Hübl in seinem Manuskript der Kryptologie [**reinholdhuebl**] erläutert, ist eine elliptische Kurve mit den Charakteristiken char(k) = 0 oder char(k) > 3 eine Kurve, die durch ein Polynom der Form

$$F(X, Y) = Y^2 - X^3 - aX - b$$

mit $a, b \in k$ dargestellt ist, für die $4a^3 + 27b^2 \neq 0 \in k$ gilt.

Stellt man die Gleichung der Funktion nach y^2 um, dann erhält man folgende Gleichung in zwei Variablen:

$$y^2 = x^3 + \text{ax} + \text{b mod(p)},$$

wobei $a, b \in \mathbb{F}_p$. Diese Gleichung ist der Schlüssel für die im Voraus aufgeworfene Frage, was ein Punkt einer elliptischen Kurve ist. Diese sind nämlich alle Punkte (x, y), welche die Gleichung lösen.

Um die Punkte auf einer Kurve zu berechnen, prüft man zunächst, ob es sich bei der betrachteten Kurve um eine elliptische Kurve mit p > 3 handelt. Dafür arbeitet man mit der Formel $4a^3 + 27b^2 \neq 0$. Man setzt die Parameter a und b der vermeintlichen elliptischen Kurve ein. Wenn die linke Seite $\neq 0$ ist, dann handelt es sich bei der besagten Kurve tatsächlich um eine elliptische Kurve mit p > 3. Rechnen wir dies nun einmal schematisch durch. Gegeben ist eine Funktion F mit

$$F(X, Y) = Y^2 - X^3 + 3X - 3 \in \mathbb{F}_{13}$$

Wie man der Funktion entnehmen kann ist a = - 3 = 10 und b = 3 in $\mathbb{F}_{13}$. Diese setzen wir nun in die Formel ein.

$$4 \cdot 10^3 + 27 \cdot 3^2 = 6 \neq 0 \bmod(13)$$

Da $6 \neq 0$ ist definiert die Funktion eine elliptische Kurve in $\mathbb{F}_{13}$. Die Abbildung 2.6 zeigt die Zeichnung der Funktion dieser elliptischen Kurve über den reellen Zahlen im kartesischen Koordinatensystem:

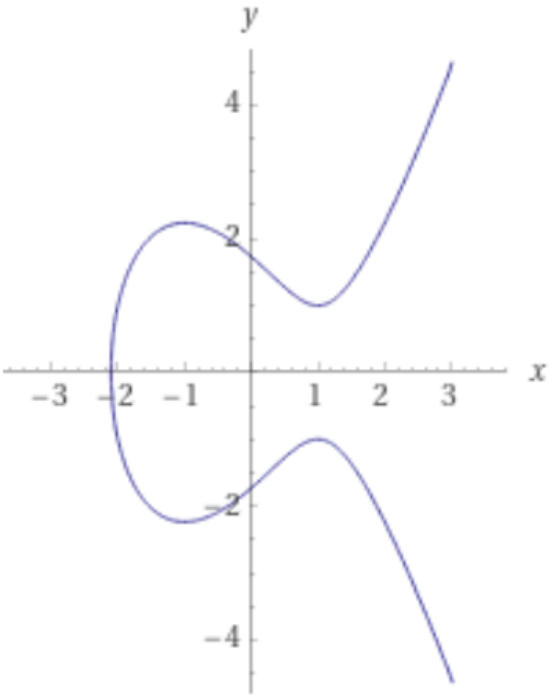

Abbildung 2.6.: Zeichnung der elliptischen Kurve
Quelle: Wolframalpha

Nachdem man allgemein geprüft hat, ob es sich bei der besagten Funktion um eine elliptische Kurve handelt, geht es jetzt um die Findung der Lösungen der umgestellten Gleichung, um alle Punkte zu finden. Dafür gibt es mehrere Möglichkeiten. Die Möglichkeiten haben unterschiedliche Zeit- und Rechenkomplexitäten, wodurch sich die Lösungsmöglichkeiten differenzieren lassen. Je nach Anwendungsfall lohnt sich die Implementierung einer anderen Lösung. Im Folgenden sind drei Möglichkeiten zur Berechnung aller Punkte auf elliptischen Kurven aufgezählt:

- Brute-Force
- Punktaddition und Punktverdopplung
- Algorithmischer Brute-Force

Neben dieser drei gängigen Methoden werden in der Mathematik und in der Kryptografie auch die Barrett-Reduktion und weiterhin auch eine Methode, bei welcher sich die Symmetrie zur x-Achse der elliptischen Kurve zur Berechnung zunutze gemacht wird, genutzt. Um diese soll es jedoch nicht gehen. In den folgenden zwei Unterkapiteln wird die Berechnung der Punkte über Brute-Force mit zwei Methoden sowie über die Punktaddition und -verdopplung erläutert und mittels Beispielen verständlich erklärt.

2.1.2. Punktberechnung: Brute-Force-Methode

Wie bereits erläutert wurde, ist die umgestellte Gleichung der elliptischen Kurve in zwei Variablen folgende:

$$y^2 = x^3 + \mathrm{ax} + \mathrm{b} \in \mathbb{F}_p$$

Da die linke Seite mit y^2 offensichtlich quadratisch ist, muss am Ende auf beiden Seiten der Gleichung die Quadratwurzel gezogen werden, um die Gleichung zu lösen und im weiteren Sinne Punkte auf der Kurve zu finden. Da dies umständlich und im endlichen Körper $\mathbb{F}_p$ schwer zu realisieren ist, wird die rechte Seite bis zu einem Quadrat aufgelöst. Dafür muss man als erstes alle Punkte $\mathrm{x} \in \mathbb{F}_p$ bestimmen, für die $x^3 + ax + b$ ein Quadrat in $\mathbb{F}_p$ sind. Die Quadratprüfung ist dabei simpel: Man geht jedes Element in $\mathbb{F}_p$ von 0 bis p-1 durch und prüft, ob das quadrierte Element in der Restklasse ein Quadrat ist. Hierbei geht es um keine komplexe Rechnung, sondern lediglich um stupides ausprobieren. Zur Verdeutlichung folgendes Beispiel: Wir haben den Körper $\mathbb{F}_5$. Der Körper beinhaltet die Elemente $\mathbb{F}_5 = 0, 1, 2, 3, 4$. Die Quadrate mitsamt ihrer Wurzeln sind folgende:

$$0 = 0^2 \qquad 1 = 1^2 = 4^2 \qquad 4 = 2^2 = 3^2$$

Die Zahlen 0, 1 und 4 sind demnach in $\mathbb{F}_5$ Quadrate. Die Wurzeln wurden der Vollständigkeit halber ebenfalls obig rechts des Quadrates notiert. Man berechnet die Quadrate nach folgendem Schema:

1. Man hat k mit $\mathrm{k} \in \mathbb{F}_p$
2. Man beginnt bei $\mathrm{k} = 0$
3. Es wird quadriert mit k^2
4. Der Wert von k^2 in $\mathbb{F}_p$ wird ermittelt, dafür rechnet man k^2 mod(p)
5. Die ermittelte Zahl ist ein Quadrat in $\mathbb{F}_p$

6. Man wiederholt alle Schritte mit allen k von 0 bis p-1
7. Am Ende hat man alle Quadrate und ihre zugehörigen Wurzeln

Dies wird anhand eines ausführlichen Beispiels deutlich. Sei p = 11 und somit $\mathbb{F}_p = \mathbb{F}_{11}$.

- $0^2 \equiv 0 \mod(11)$
- $1^2 \equiv 1 \mod(11)$
- $2^2 \equiv 4 \mod(11)$
- $3^2 \equiv 9 \mod(11)$
- $4^2 \equiv 5 \mod(11)$
- $5^2 \equiv 3 \mod(11)$
- $6^2 \equiv 3 \mod(11)$
- $7^2 \equiv 5 \mod(11)$
- $8^2 \equiv 9 \mod(11)$
- $9^2 \equiv 4 \mod(11)$
- $10^2 \equiv 1 \mod(11)$

Wenn man die Null dazuzählt, hat $\mathbb{F}_{11}$ die Quadrate 0, 1, 3, 4, 5, 9. Im Folgenden sind die Quadrate mitsamt ihrer Wurzeln aufgeschrieben:

- Quadrat: 0 Wurzel 1: 0
- Quadrat: 1 Wurzel 1: 1 Wurzel 2: 10
- Quadrat: 3 Wurzel 1: 5 Wurzel 2: 6
- Quadrat: 4 Wurzel 1: 2 Wurzel 2: 9
- Quadrat: 5 Wurzel 1: 4 Wurzel 2: 7
- Quadrat: 9 Wurzel 1: 3 Wurzel 2: 8

Die berechneten Quadrate und Wurzeln sind nötig, um die Punkte zu bestimmen. Um dies zu bewerkstelligen, wird die Gleichung der elliptischen Kurve in zwei Variablen benötigt. Um die benötigte Formel zu erhalten, überführen wir die Ausgangsgleichung in zwei Variablen in eine Funktionsgleichung mit einer Variablen:

$$y^2 = x^3 + \text{ax} + \text{b} \in \mathbb{F}_p \qquad \Longrightarrow \qquad f(x) = x^3 + \text{ax} + \text{b} \in \mathbb{F}_p$$

Diese Funktionsgleichung ist der Ausgangspunkt für die Berechnung der Punkte. Man setzt nun alle x-Werte von 0 bis p-1 in die Funktionsgleichung ein. Jene x-Werte, welche die Quadrate ergeben, werden für die Punktbestimmung benötigt. Nehme als Beispiel p = 11. Wir haben die Quadrate und die Wurzeln oben bereits ausgerechnet. Sei weiterhin die Gleichung einer elliptischen Kurve E gegeben durch

$$F(X, Y) = Y^2 - X^3 + 10 \cdot X + 8 \in \mathbb{F}_{11}$$

Damit ist die umgestellte Gleichung in zwei Variablen und die Funktionsgleichung mit einer Variablen

$$y^2 = x^3 + \text{x} + 3 \qquad \Longrightarrow \qquad f(x) = x^3 + \text{x} + 3 \in \mathbb{F}_{11}$$

Setzen wir nun alle Elemente von 0 bis p-1 in die Funktionsgleichung ein und betrachten die Ergebnisse:

- $f(0) = 0^3 + 0 + 3 = 3 \in \mathbb{F}_{11} \qquad \Longrightarrow \qquad$ Quadrat
- $f(1) = 1^3 + 1 + 3 = 5 \in \mathbb{F}_{11} \qquad \Longrightarrow \qquad$ Quadrat
- $f(2) = 2^3 + 2 + 3 = 2 \in \mathbb{F}_{11}$
- $f(3) = 3^3 + 3 + 3 = 0 \in \mathbb{F}_{11} \qquad \Longrightarrow \qquad$ Quadrat
- $f(4) = 4^3 + 4 + 3 = 5 \in \mathbb{F}_{11} \qquad \Longrightarrow \qquad$ Quadrat
- $f(5) = 5^3 + 5 + 3 = 1 \in \mathbb{F}_{11} \qquad \Longrightarrow \qquad$ Quadrat
- $f(6) = 6^3 + 6 + 3 = 5 \in \mathbb{F}_{11} \qquad \Longrightarrow \qquad$ Quadrat
- $f(7) = 7^3 + 7 + 3 = 1 \in \mathbb{F}_{11} \qquad \Longrightarrow \qquad$ Quadrat
- $f(8) = 8^3 + 8 + 3 = 6 \in \mathbb{F}_{11}$
- $f(9) = 9^3 + 9 + 3 = 4 \in \mathbb{F}_{11} \qquad \Longrightarrow \qquad$ Quadrat
- $f(10) = 10^3 + 10 + 3 = 1 \in \mathbb{F}_{11} \qquad \Longrightarrow \qquad$ Quadrat

Die Ergebnisse zeigen dass für die folgenden x-Werte $f(x)$ ein Quadrat ist: 0, 1, 3, 4, 5, 6, 7, 9, 10. Bis jetzt wurde der einfache Brute-Force durchgeführt. Man muss nur noch wenige Schritte durchführen, um die Punkte auf der elliptischen Kurve zu bestimmen. Wir haben jetzt die Quadrate, die dazugehörigen Wurzeln sowie die x-Werte, welche Quadrate sind. Wie kombiniert man diese, um die Punkte auf der

elliptischen Kurve zu erhalten? Es gilt, die Informationen der Punkte P mit P = (x, y) der elliptischen Kurve zu erhalten. Für den x-Wert der Punkte nimmt man das Ergebnis des eingesetzten x von 0 bis p-1 in die Funktion. Man nimmt als x-Wert das vorhandene Quadrat. Die y-Werte der Punkte ergeben sich aus dem Ergebnis des eingesetzten x in die umgestellte Funktion mit einer Variablen. Man nimmt die Wurzeln des zugehörigen Quadrates zum Ergebnis. Daraus ergeben sich die folgenden Punkte auf der obig eingeführten elliptischen Kurve E:

- $f(0) = 3 \implies$ Punkt 1: $(0, 5)$ Punkt 2: $(0, 6)$
- $f(1) = 5 \implies$ Punkt 1: $(1, 4)$ Punkt 2: $(1, 7)$
- $f(3) = 0 \implies$ Punkt 1: $(3, 0)$
- $f(4) = 5 \implies$ Punkt 1: $(4, 4)$ Punkt 2: $(4, 7)$
- $f(5) = 1 \implies$ Punkt 1: $(5, 1)$ Punkt 2: $(5, 10)$
- $f(6) = 5 \implies$ Punkt 1: $(6, 4)$ Punkt 2: $(6, 7)$
- $f(7) = 1 \implies$ Punkt 1: $(7, 1)$ Punkt 2: $(7, 10)$
- $f(9) = 4 \implies$ Punkt 1: $(9, 2)$ Punkt 2: $(9, 9)$
- $f(10) = 1 \implies$ Punkt 1: $(10, 1)$ Punkt 2: $(10, 10)$

Die Berechnung der Punkte über die Brute-Force-Methode ist sehr umständlich. Insbesondere, wenn das gewählte p groß ist, dann ist diese Brute-Force-Methode sehr aufwendig. Es müssen alle Quadrate in $\mathbb{F}_p$ und deren zugehörigen Wurzeln berechnet werden. Weiterhin entsteht Zeit- und Rechenaufwand beim Einsetzen in die Funktionen. In der Kryptografie ist jedoch die Wahl besonders großer p gängig, um ein hohes Sicherheitsniveau zu erreichen. Aus diesem Grund werden im Folgenden die beiden anderen angeführten Lösungsmöglichkeiten angeführt.

2.1.3. Punktberechnung: Punktaddition und -verdopplung

Eine weitere Methode zur Berechnung von Punkten auf einer elliptischen kurve ist die Punktaddition und die Punktverdopplung. Dies ist eine elegante Methode, da man über einen simplen Algorithmus alle Punkte auf einer elliptischen Kurve bestimmen kann. Der Nachteil dieser Methode ist jedoch, dass im Vorfeld ein Punkt auf der elliptischen Kurve bekannt sein muss. Dieser muss über die Brute-Force-Methode oder einem anderen Ansatz berechnet werden oder ein Punkt ist gegeben. Die offene

Frage ist jedoch, ob jeder beliebige Punkt als Ausgangsobjekt genutzt werden kann, um auf seiner Grundlage alle anderen Punkte zu erzeugen.

Um dies herauszufinden, müssen noch einmal die Gruppeneigenschaften von elliptischen Kurven über $\mathbb{F}_p$ betrachtet werden. Hankerson, Menezes und Vanstone beschreiben in ihrem Buch „*Guide to Elliptic Curve Cryptography*“diese Gruppeneigenschaften und erklären damit, wie man herausfindet, ob es sich um eine zyklische Gruppe handelt und damit in welterem Sinne, welche Punkte auf der elliptischen Kurve Generatoren sind [**Hankerson2004**]. Sei E eine elliptische Kurve über $\mathbb{F}_p$. Die Anzahl der Punkte in E($\mathbb{F}_p$), bezeichnet als $\overline{E}(\mathbb{F}_p)$, wird als die Ordnung von E über $\mathbb{F}_p$ bezeichnet. Dabei ist der imaginäre Punkt im Unendlichen inkludiert. Im Folgenden ist es wichtig herauszufinden, ob E eine zyklische Gruppe ist. Eine elliptische Kurve E über $\mathbb{F}_p$ ist eine zyklische Gruppe, wenn $\overline{E}(\mathbb{F}_p)$ eine Primzahl ist. Die bereits angeführte Hasse-Weil-Schranke hilft dabei, eine Abschätzung darüber abzugeben.

$$p + 1 - 2 \cdot \sqrt{p} \leq |\overline{E}| \leq p + 1 + 2 \cdot \sqrt{p}$$

Diese gibt eine obere und untere Schranke für $\overline{E}$ an. Liegt innerhalb dieser Schranke eine Primzahl, so ist die Wahrscheinlichkeit dafür, dass E eine zyklische Gruppe über $\mathbb{F}_p$ definiert, sehr hoch. Ist eine elliptische Kurve E eine zyklische Gruppe, dann hat sie genau ein Element, welches ein Erzeuger der Gruppe ist. Mit diesem Element lassen sich alle anderen Elemente der Gruppe durch Punktverdopplung bzw. Punktaddition erzeugen. Der Punkt hat damit die gleiche Ordnung wie E. Ist der Erzeuger und ein weiterer Punkt gegeben, so lassen sich auch über die Punktaddition weitere Punkte finden. Weiterhin sei gesagt, dass der Punkt im Unendlichen kein Erzeuger sein kann. Die Berechnung aller Punkte auf der Kurve ist trivial, wenn der Erzeuger bekannt ist. Nehmen wir als Beispiel eine elliptische Kurve E gegeben durch

$$y^2 = x^3 + 2x + 2 \in \mathbb{F}_{17}$$

Der Erzeuger der Gruppe ist der Punkt P = (5, 1). Um zu zeigen, dass dieser Punkt ein Erzeuger oder Generator ist, muss er mit sich selbst so oft addiert werden, bis er den Punkt im Unendlichen ergibt. Bei dem gegebenen Punkt ist dies bei $19 \cdot$ P der Fall. Gegeben sei außerdem $18 \cdot$ P = (5, -1). Da $19 \cdot$ P = $18 \cdot$ P + P = (5, 1) + (5, -1) = $\mathcal{O}$. Dieses kurze Beispiel macht deutlich, dass es aufwendig sein kann zu prüfen, ob ein Punkt P ein Erzeuger ist. In der Praxis werden in Kryptosystemen Punktgeneratoren mit großer Ordnung gewählt, um die Sicherheit in den verwendeten kryptografischen System zu gewährleisten. Der Erzeuger der Gruppe ist so nicht

einfach berechenbar. In den folgenden Beispielen ist jedoch ein Erzeuger gegeben, damit die Punktaddition respektive die Punkterdopplung trivial ist.

Bevor das Beispiel durchgegangen wird, werden noch einmal die benötigten Formeln und die Vorgehensweise erläutert. Es sei ein Erzeugerpunkt P gegeben mit $P = (x_1, y_2)$. Da nur dieser gegeben ist, wird er mit sich selbst addiert. Somit gilt: $2 \cdot \mathrm{P} = \mathrm{P} + \mathrm{P}$. Durch die Punktverdopplung entsteht ein neuer Punkt. P kann jetzt mit $2 \cdot \mathrm{P}$ addiert werden. Dies wird solange fortgeführt, bis der Punkt im Unendlichen herauskommt. Anschließend hat man alle Punkte auf E berechnet. Im Folgenden wird die Vorgehensweise über Pseudocode in Python erläutert, wenn ein Erzeugerpunkt gegeben ist. Es soll gesagt sein, dass es sich hierbei um eine starke Vereinfachung handelt. Beispielsweise wird nicht darauf eingegangen, dass das p des Primkörpers für die Durchführung der Addition von Punkten benötigt wird:

```
1  function punktbestimmung(P, Q):
2      Punkte = []
3      if P = UNENDLICH:
4          return FEHLER
5      zaehler = 0
6      while 1:
7          if P = Q
8              Punkte[zaehler] = P + P
9              Q = Punkte[zaehler]
10             if Q = UNENDLICH
11             zaehler = zaehler + 1
12         if P != Q
13             Punkte[zaehler] = P + Q
14             Q = Punkte[zaehler]
15             if Q = UNENDLICH
16             zaehler = zaehler + 1
17     return Punkte
```

Listing 2.1: Punktberechnung in Python

Gegeben sei eine elliptische Kurve E
hankerson es gibt gruppen die nicht zyklisch sind zn x zn (zwei sätze) wenn zyklisch mit primzahlordnung alle punkte erzeuger
Lagrange Theorem -> wenn ordnung p prim, dann ist jeder punkt außer unendlich kleiner punkt erzeuger bzw. generator

2.1.4. Punktberechnung: Algorithmische Brute-Force-Methode

brute force mit
quadratprüfung element quadratwurzel bestimmen
kombinierung von verfahren

2.1.5. Implementierung in Python

U

2.1.6. Diskreter Logarithmusproblem über elliptischen Kurven

Wie in Kapitel XY gezeigt, kann das DLP verallgemeinert werden, sodass über jeder zyklischen Gruppe (mehr oder weniger effektiv) ein DLP definiert erden kann. Im ersten Abschnitts dieses Kapitels wurden die Gruppeneigenschaften der Punktmenge auf der elliptischen Kurve gezeigt. Gruppenelemente werden können über die Gruppenoperation + *addiert* werden. Es gilt der Folgende Satz:

Satz: Die Punkte einer elliptischen Kurve zusammen mit O haben zyklischen Untergruppen. Unter bestimmten Bedingungen bilden *alle* Punkte einer elliptischen Kurve eine zyklische Gruppe.

Um eine kryptografisch *sicheres* DLP zu konstruieren, ist es wichtig die Gruppenkardinalität zu kennen. Deren exakte Bestimmung ist bei elliptischen Kurven jedoch sehr aufwendig. Für die grobe Bestimmung der Gruppenkardinalität wurde in Kapitel XY bereits die Hasse-Weil-Schranke vorgestellt. Diese erlaubt es uns die Anzahl der Punkte einer elliptischen Kurve abzuschätzen. Vereinfacht kann man sagen das die Anzahl der Punkte in etwa p entspricht, wenn die elliptische Kurve über $\mathbb{Z}_p^*$ definiert ist.

Im folgenden wollen wir das DLP über elliptischen Kurven definieren:

Definition: Das DLP über elliptischen Kurven (ECDLP) Gegeben sei eine elliptische Kurve E. Wir betrachten ein primitives Element P und ein beliebiges weiteres Element T. Das DLP ist die Bestimmung der natürlichen Zahl d zwischen $1 \leq d \leq \#E$, sodass gilt:

$$\underbrace{P + P + \cdots + P}_{d-mal} = dP = T$$

Die Bestimmung der natürlichen Zahl d ist wie auch schon beim DLP über $\mathbb{Z}_p^*$ nicht trivial. In einem Kryptosystem wäre dementsprechend die natürliche Zahl d der private Schlüssel und das Element T der öffentliche Schlüssel. Anders als beim DLP über Primkörpern, wo beide Schlüssel natürliche Zahlen waren, ist der private Schlüssel T hier ein Punkt der elliptischen Kurve. Der in der obigen Definition verwendete Ausdruck dP wird *Punktmultiplikation* genannt, da man schreiben kann $T = dP$. Es ist jedoch zu beachten das es dafür keine Rechenvorschrift gibt, die Zahl d mit P zu multiplizieren. Der Ausdruck bedeutet lediglich, dass die Gruppenoperation d mal auf P angewendet wird.

Der Erzeuger eines Schlüsselpaars muss allerdings nicht einzeln d mal P auf sich selbst addieren, sonder kann sich eines *Tricks* bedienen. Wie beim DLP über dem Primkörper $\mathbb{Z}_p^*$, wo der Square-And-Multiply-Algorithmus zu effizienten Berechnung des öffentlichen Schlüssels verwendet wurde, kann hier der sog. *Double-And-Add-Algorithmus* verwendet werden. Dieser ist von der Idee her zum Square-And-Multiply-Algorithmus identisch, und unterscheidet sich nur durch die angewandten Operationen. Der folgende Code zeigt eine Beispielhafte Implementierung:

```
1  def doubble_and_add(kPriv, start_point):
2      binary = bin(kPriv)
3      binary = binary[3:]
4      cur_point = start_point
5      for digit in binary:
6          # Doubble
7          cur_point = curve.add(cur_point, cur_point)
8          if digit == "1":
9              # Add
10             cur_point = curve.add(cur_point, start_point)
11     return cur_point
```

Listing 2.2: Double-And-Add-Algorithmus in Python

Zuerst wird die Binärdarstellung des private Schlüssels d in *binary* gespeichert. Nun wird diese Binärdarstellung von links nach rechts durchlaufen, wobei die vorderste 1 ignoriert wird, da diese quasi schon in 1· Startpunkt P steckt. Für jede Ziffer wird zunächst der aktuelle Punkt verdoppelt und im Falle einer 1 wird zudem

noch der Startpunkt addiert. Dieses Vorgehen wird angewandt bis die komplette Binärdarstellung von d abgearbeitet ist. Der Output entspricht dP.
Nachfolgend wollen wir verstehen, warum dieser Algorithmus funktioniert. Dazu betrachten wir das folgende Beispiel:
Das Ziel ist es den Punkt $19P$ zu berechnen:

$$21P = (10101_2)P = (d_4 d_3 d_2 d_1 d_0)_2 P$$

Die Bits d_4 bis d_0 werden in absteigender Reihenfolge verarbeitet:

$d_4 = 1:$	$P = \mathbf{1}_2\ P$	Startwert 1
$d_3 = 0:$	$P + P = 2\ P = \mathbf{10}_2\ P$	double
$d_2 = 1:$	$2\ P + 2\ P = 4P = \mathbf{100}_2\ P$	double
	$4\ P + P = 5\ P = \mathbf{101}_2\ P$	add, da $d_2 = 1$
$d_1 = 1:$	$5\ P + 5\ P = 10\ P = \mathbf{1010}_2\ P$	double
$d_0 = 1$	$10\ P + 10\ P = 20\ P = \mathbf{10100}_2\ P$	double
	$20\ P + P = 21\ P = \mathbf{10101}_2\ P$	add, da $d_0 = 1$

Das darstellen von d als binäre Zahl ermöglicht es, diese ausgehend von der ersten 1 ausgehend *zusammenzubauen*. Jede Stelle im Binärsystem ist doppelt so wertig wie die vorherige, weshalb durch Verdoppeln die ganze Zahl um eine Stelle nach links geschoben wird. Durch diese Operation wird dann sozusagen eine 0 *erzeugt*. Wenn nun eine 1 benötigt wird kann diese durch die Addition von 1 bzw. dem Startpunkt *erzeugt* werden.

Mittels dieses Algorithmus von die Komplexität der Berechnung des Punktes $T = dP$ von $O(d)$ auf $O(1,5 \cdot \log_{10} d)$ reduziert werden. Wodurch die Berechnung von T auch für große d verhältnismäßig schnell durchzuführen ist. Der Angreifer hat keine Möglichkeit die Berechnung von d derart zu beschleunigen, was das DLP auch hier zu einer Einwegfunktion macht.