DHBW
Duale Hochschule
Baden-Württemberg

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

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

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 nicht als Produkt von zusammengesetzten natürlichen Zahlen gebildet werden. Man nehme als Beispiel die Primzahl 7. Sie lässt sich nicht als Produkt von natürlichen Zahlen 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 dieses Produktes heißen Primfaktoren. Die Zerlegung einer zusammengesetzten natürlichen Zahl in ihre Primfaktoren nennt man Primfaktorzerlegung. Dadurch ist die Zahl als Produkt von mehreren Primzahlen dargestellt. 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:

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

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	$\cancel{4}$	5	$\cancel{6}$	7	$\cancel{8}$	$\cancel{9}$	$\cancel{1}0$
11	$\cancel{1}2$	13	$\cancel{1}4$	$\cancel{1}5$	$\cancel{1}6$	17	$\cancel{1}8$	19	$\cancel{2}0$
$\cancel{2}1$	$\cancel{2}2$	23	$\cancel{2}4$	$\cancel{2}5$	$\cancel{2}6$	$\cancel{2}7$	$\cancel{2}8$	29	$\cancel{3}0$
31	$\cancel{3}2$	$\cancel{3}3$	$\cancel{3}4$	$\cancel{3}5$	$\cancel{3}6$	37	$\cancel{3}8$	$\cancel{3}9$	$\cancel{4}0$
41	$\cancel{4}2$	43	$\cancel{4}4$	$\cancel{4}5$	$\cancel{4}6$	47	$\cancel{4}8$	$\cancel{4}9$	$\cancel{5}0$
$\cancel{5}1$	$\cancel{5}2$	53	$\cancel{5}4$	$\cancel{5}5$	$\cancel{5}6$	$\cancel{5}7$	$\cancel{5}8$	59	$\cancel{6}0$
61	$\cancel{6}2$	$\cancel{6}3$	$\cancel{6}4$	$\cancel{6}5$	$\cancel{6}6$	67	$\cancel{6}8$	$\cancel{6}9$	$\cancel{7}0$
71	$\cancel{7}2$	73	$\cancel{7}4$	$\cancel{7}5$	$\cancel{7}6$	$\cancel{7}7$	$\cancel{7}8$	79	$\cancel{8}0$
$\cancel{8}1$	$\cancel{8}2$	83	$\cancel{8}4$	$\cancel{8}5$	$\cancel{8}6$	$\cancel{8}7$	$\cancel{8}8$	89	$\cancel{9}0$
$\cancel{9}1$	$\cancel{9}2$	$\cancel{9}3$	$\cancel{9}4$	$\cancel{9}5$	$\cancel{9}6$	97	$\cancel{9}8$	$\cancel{9}9$	$\cancel{1}00$

Hier kommt noch Text

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

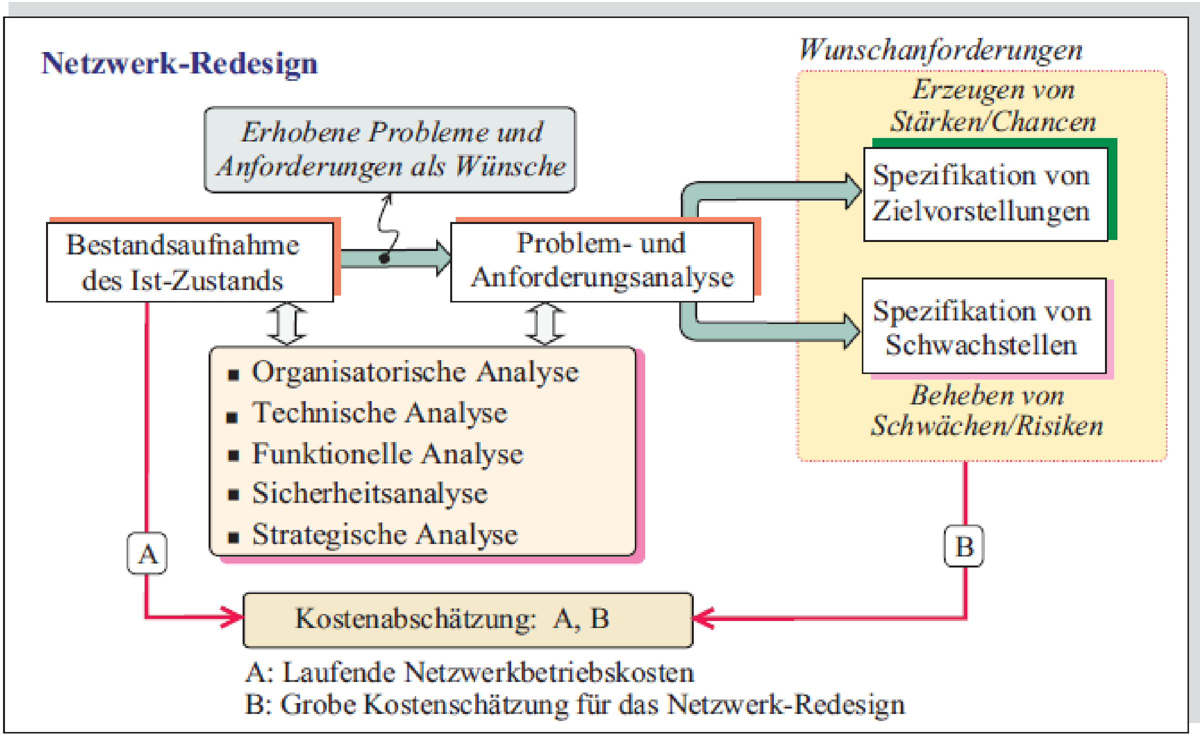

Abbildung 1.1.: Hauptaufgaben der Ist-Analyse beim Redesign einer Netzwerkinfrastruktur
Quelle: [**Berghammer.2021**]

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:

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

1.2.3. 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.

1.2.4. 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

2. Elliptsiche Kurven

Als Basis für Asymentrische Kryptosysteme können elliptische Kurven dazu genutzt werden, die verschlüsselungstechnische Effektivität mathematischer Probleme, wie das des diskreten Logarithmus, zu erhöhen. Bei der Kryptographie unter Verwendung elliptsicher 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 uns 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

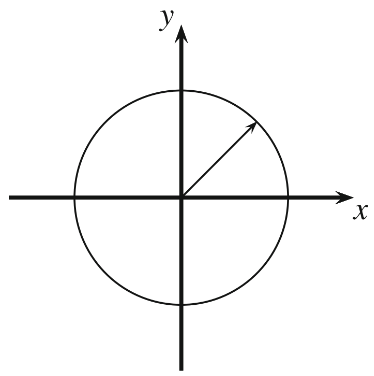

Abbildung 2.1.: r

Kreisgleichung kann verallgemeinert werden, indem 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.

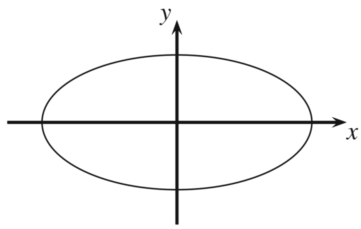

Abbildung 2.2.: r

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 können,

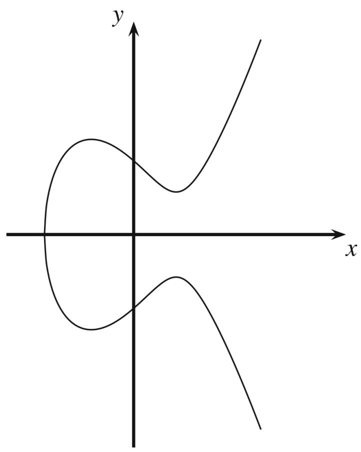

Abbildung 2.3.: r

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 $\mathbb{F}_p$, ist die Menge aller Punkte (x, y) mit $x, y \in \mathbb{F}_p$, welche die folgende Gleichung erfüllen:

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

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 nun 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.

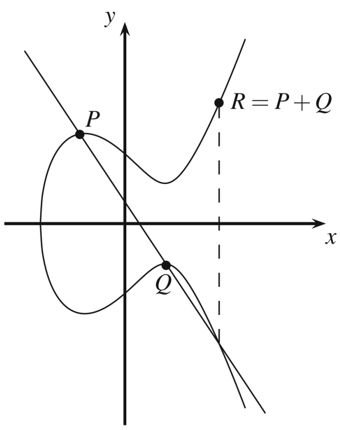

Abbildung 2.4.: r

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.

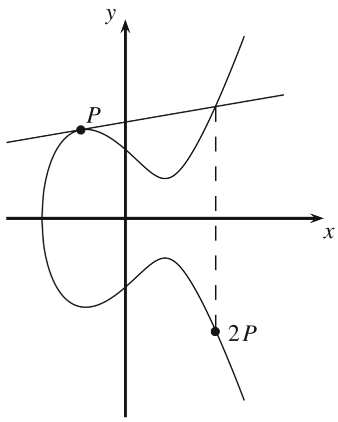

Abbildung 2.5.: r

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 $\mathbb{F}_{|}$ durchgeführt werden kann.

Formel: Punktaddition und -verdopplung auf elliptischen Kurven:

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

$$y_3 = s(x_1 - x_2) - y_1$$

, wobei

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