Bachelorarbeit
Verteilung quadratischer Reste

Fabian Heinrich

30. November 2018

Contents

Chapter 1

Einleitung

Wir betrachten die ungerade Primzahl $p = 19$. Wir wissen, dass die Hälfte der Elemente von $(\mathbb{Z}/19\mathbb{Z})^\times$ quadratische Reste und die verbleibende Hälfte quadratische Nichtreste sind. Nehmen wir nun an, dass $[t]_p$ ein quadratischer Rest modulo p ist, wie wahrscheinlich ist es dann, dass $[t+1]_p$ ebenfalls ein quadratischer Rest ist? Fassen wir diesen Fall als Zufallsexperiment auf, so beträgt die Wahrscheinlichkeit dafür, dass $[t]_p$ quadratischer Rest ist gleich $\frac{1}{2}$. Wollen wir nun, dass $[t+1]_p$ ebenfalls ein quadratischer Rest ist, müssen wir die Wahrscheinlichkeiten für beide auftretenden Fälle multiplizieren. Wir können die Wahrscheinlichkeiten multiplizieren, da die Ergebnisse unseres Zufallskeitsexperiments statistisch unabhängig zu seien scheinen. Vorhergehende Aussagen über die Eigenschaft als quadratischer Rest von $[t]_p$ haben somit keinen Einfluss auf nachfolgende Aussagen. Für unseren Fall bedeutet das, dass die Wahrscheinlichkeit, dass sowohl $[t]_p$ als auch $[t+1]_p$ quadratische Reste sind, $\frac{1}{4}$ beträgt. Kommen wir auf die Auffassung als Zufallsexperiment zurück, so können wir weitere Aussagen über aufeinanderfolgende Paare von quadratischen Resten, wie in unserem Fall, treffen. Da $\mid (\mathbb{Z}/19\mathbb{Z})^\times \mid = 18$, können wir unser Zufallsexperiment 17 mal durchführen. Wir können also folgern, dass der Fall, dass sowohl $[t]_p$ als auch $[t+1]_p$ quadratische Reste sind, in unserem Beispiel mit $p = 19$ ungefähr viermal auftreten sollte. Bisher haben wir uns diese Zusammenhänge nur vorgestellt und es wird Zeit, sich unserem Beispiel von einem anschaulicheren Blickwinkel zu nähern.

x	1	2	3	4	5	6	7	8	9	10	11	12
R/N	R	N	N	R	R	R	R	N	R	N	R	N

x	13	14	15	16	17	18
R/N	N	N	N	R	R	N

In dieser Tabelle haben wir jeweils die Zuordnung von quadratischen Resten (R) beziehungsweise quadratischen Nichtresten (N) zu den Elementen von $(\mathbb{Z}/19\mathbb{Z})^\times$ dargestellt. Zur besseren Darstellung haben wir jedoch x statt $[x]_p$ geschrieben. Anhand der Tabelle können wir sehen, dass unsere Vorüberlegungen richtig er-

scheinen, da wir vier Paare quadratischer Reste erkennen. Außerdem erkennen wir ebenfalls vier Paare von aufeinanderfolgenden quadratischen Nichtresten, vier Paare von einem quadratischen Nichtrest gefolgt von einem quadratischen Rest sowie fünf Paare von einem quadratischen Rest gefolgt von einem quadratischen Nichtrest. Bei der Betrachtung der vier verschiedenen Möglichkeiten für die Anordnung von quadratischen Resten und quadratischen Nichtresten in einem Paar aufeinanderfolgenden Restklassen fällt auf, dass sich diese ebenfalls fast gleich verteilen und eine Auftrittswahrscheinlichkeit von ungefähr $\frac{1}{4}$ haben.
Mit Hilfe unseres kurzen Beispiels lassen sich viele interessante Eigenschaften von Tupeln aufeinanderfolgender quadratischer Reste erahnen. Wir fragen uns nun jedoch, ob sich diese Eigenschaften auch für wesentlich größere Primzahlen p nachweisen lassen. Aufgrund dessen wollen wir im weiteren Verlauf dieser Arbeit die gezeigten Eigenschaften für allgemeine Primzahlen p auf ihre Gültigkeit prüfen und gegebenenfalls allgemeine Aussagen über die Verteilung von quadratischen Resten formulieren. Des Weiteren wollen wir prüfen, inwiefern wir explizite Formulierungen aufstellen können oder, ob es uns nur gelingt, Abschätzungen zu treffen. Dazu werden wir entsprechende Zähl-Funktionen implementieren und nach Mustern suchen, die wir für die Formulierung der zu beweisenden Aussagen nutzen können. Diese Problemstellungen spiegeln jedoch nur einen Auszug der Fragen wider, die wir im Rahmen dieser Bachelorarbeit beantworten wollen. Die Problematik bezüglich der Verteilung von quadratischen Resten ist ein Thema, das schon seit vielen Jahrzehnten die Zahlentheorie bewegt und Potential besitzt, auch zukünftig relevant zu bleiben. Aufgrund dessen möchten wir an dieser Stelle auf die Historie der quadratischen Reste verweisen. Die älteste uns vorliegende Quelle stammt aus dem Jahr 1906. Ernst Jacobsthal war einer der ersten Mathematiker zu Beginn des 20. Jahrhunderts, der sich mit der Verteilung von quadratischen Resten beschäftigte. Er hat sich in seiner Dissertation [Jac06] mit der Verteilung von Paaren, Tripeln und 4-Tupeln von quadratischen Resten, aber auch Permutationen von quadratischen Resten und Nichtresten innerhalb von Tupeln, auseinandergesetzt. Außerdem war er der Erste, dem es gelungen ist, exakte Formeln für die Anzahl von Paaren sowie Tripeln aufzustellen. Während der 1930er Jahre entstanden die Arbeiten [Doe29], [Hop30], [Dav31] und [Bra32]. In der Arbeit [Doe29] betrachtet Dörge 4-Tupel von quadratischen Resten sowie die verschiedenen Permutationen von quadratischen Resten sowie Nichtresten innerhalb von 4-Tupeln. Die Arbeit [Hop30] baute auf [Doe29] auf und Hopf beschäftigte sich mit der entstandenen Schwierigkeit, die Summen über Produkte von Legendre-Symbolen, die bei der Betrachtungen von 4-Tupeln entstehen, abzuschätzen. Die entstehenden Summen von Legendre-Symbolen mit Polynomen über Primzahlen p spielten ebenfalls eine wichtige Rolle in Davenports Arbeit [Dav31]. Er versuchte wie Hopf Abschätzungen zu finden, um die Anzahl von 4-Tupeln quadratischer Reste zuverlässig zu bestimmen. In [Bra32] beschäftigt sich Brauer mit allgemeinen Potenzresten modulo p. Es gelang ihm, eine Abschätzung zu finden, die Ähnlichkeiten mit der Weil-Schranke aufweist. Die Weil-Schranke wird eine wichtige Rolle in dieser Arbeit spielen und wir werden in den folgenden

Kapiteln zeigen, für welche Abschätzungen wir sie nutzen können. Nichtsdestotrotz ist Davenports Arbeit besonders hervorzuheben, da es ihm gelang, eine Abschätzung des Fehlerterms für allgemeine d-Tupel zu formulieren. 1948 veröffentliche André Weil seine Arbeit [Wei48]. Diese Arbeit spielte eine wichtige Rolle für eine weitere Quelle dieser Arbeit, nämlich den Artikel [Con] von Keith Conrad. Durch die von Weil bewiesene Weil-Schranke konnte Conrad in [Con] eine weitere Abschätzung für die Anzahl von allgemeinen d-Tupeln aufstellen. Jedoch werden wir im Laufe dieser Arbeit zeigen, dass diese Abschätzung in einzelnen Punkten durchaus verbessert werden kann. Als Quelle für die Grundlagen zum Legendre-Symbol, den Jacobsthalschen Summen und der Anzahl von Paaren sowie Tripeln von quadratischen Resten haben wir das Buch [Bun08] von Peter Bundschuh aus den frühen 90er-Jahren genutzt. Diese Quelle dient als Einführung in die Zahlentheorie und war aufgrund dessen für die Grundbausteine dieser Arbeit von besonderer Bedeutung.
Wir haben bereits die Bedeutung der Verteilung quadratischer Reste in der Zukunft erwähnt. Diesem Punkt ist das letzte Kapitel dieser Arbeit gewidmet. Wir möchten versuchen, Methoden des Machine Learnings auf unsere Problemstellung anzuwenden, um neue bisher unbekannte Eigenschaften über die Verteilung der quadratischen Reste zu gewinnen. Dazu möchten wir neuronale Netze mit Hilfe der von uns erstellten Datensätze trainieren, um die Ergebnisse für zuverlässige Vorhersagen bezüglich der Verteilung von quadratischen Resten zu nutzen. Ebenfalls können wir uns vorstellen, dass wir neuronale Netze sowie weitere Methoden des Machine Learnings dazu nutzen können, um bestimmte Muster in der Verteilung von quadratischen Resten zu erkennen.

Chapter 2

Grundlagen zu quadratischen Resten

2.1 Quadratische Reste und das Legendre-Symbol

Definition 2.1.1. Ein Element $[c]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$ heißt **quadratischer Rest modulo p**, wenn die folgende Kongruenz in den ganzen Zahlen lösbar ist:

$$x^2 \equiv c \pmod{p}.$$

Es heißt **quadratischer Nichtrest modulo p**, falls die Kongruenz nicht lösbar ist. Wir bestimmen per Definition, dass das Element $[0]_p$ weder quadratischer Rest noch quadratischer Nichtrest ist, da $[0]_p \notin (\mathbb{Z}/p\mathbb{Z})^\times$.
Wir werden zur besseren Übersicht oft t statt $[t]_p$ schreiben.

Definition 2.1.2. Für $t \in \mathbb{Z}$ und eine ungerade Primzahl p definieren wir das sogenannte **Legendre-Symbol** wie folgt:

$$\left(\frac{t}{p}\right) = \begin{cases} 1 & \text{falls } [t]_p \text{ quadratischer Rest modulo } p \\ 0 & \text{falls } [t]_p = [0]_p \\ -1 & \text{falls } [t]_p \text{ quadratischer Nichtrest modulo } p. \end{cases}$$

Definition 2.1.3. Sei m eine ungerade Zahl mit $m \geq 3$ und $m = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ die Primfaktorzerlegung von m (die p_i müssen nicht alle verschieden sein). Dann definiert man für $a \in \mathbb{Z}$ das **Jacobi-Symbol** durch:

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right).$$

Falls m prim ist, stimmt das Jacobi-Symbol mit dem Legendre-Symbol überein.

Definition 2.1.4. Für die Entscheidung, ob $[t]_p$ ein quadratischer Rest beziehungsweise ein quadratischer Nichtrest modulo p ist, führen wir die charakteristische Funktion

$\mathrm{chp}_1(t)$ ein:

Sei p eine ungerade Primzahl, sei $t \in \mathbb{Z}$:

$$\mathrm{chp}_1(t) = \frac{1}{2}\left(\left(\frac{t}{p}\right)+1\right) = \begin{cases} 1 & \text{falls } [t]_p \text{ quadratischer Rest modulo } p \\ \frac{1}{2} & \text{falls } [t]_p = [0]_p \\ 0 & \text{falls } [t]_p \text{ quadratischer Nichtrest modulo } p. \end{cases}$$

Da wir in den folgenden Kapiteln d-Tupel von aufeinanderfolgenden quadratischen Resten betrachten werden, führen wir aufbauend auf $\mathrm{chp}_1(t)$ die charakteristische Funktion $\mathrm{chp}_d(t)$ für d aufeinanderfolgende quadratische Reste modulo p ein:

Sei $d < p$, sei p eine ungerade Primzahl, sei $t \in \mathbb{Z}$:

$$\mathrm{chp}_d(t) = \left(\frac{1}{2}\right)^d \cdot \prod_{i=0}^{d-1}\left(\left(\frac{t+i}{p}\right)+1\right).$$

Lemma 2.1.5. *Modulo einer ungeraden Primzahl p gibt es $\frac{1}{2}(p-1)$ quadratische Reste und ebenso viele quadratische Nichtreste.*

Beweis. Siehe Korollar 3.1.5.c in [Bun08]. □

Lemma 2.1.6. *Für $c, c' \in \mathbb{Z}$ und Primzahlen p gilt:*
(i) $c \equiv c' \pmod p \implies \left(\frac{c}{p}\right) = \left(\frac{c'}{p}\right)$.
(ii) $\left(\frac{cc'}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{c'}{p}\right)$.
(iii) $\sum_{c=1}^{p-1}\left(\frac{c}{p}\right) = 0$.

Beweis. Siehe Satz 3.2.3 in [Bun08]. □

Lemma 2.1.7 (Quadratisches Reziprozitätsgesetz)**.** *Sei m eine ungerade Zahl mit $m \geq 3$ und $k \geq 3$ eine weitere ungerade und zu m teilerfremde Zahl, so gilt:*

$$\left(\frac{k}{m}\right) = (-1)^{\frac{(k-1)(m-1)}{4}}\left(\frac{m}{k}\right).$$

Ist also k oder m kongruent zu 1 modulo 4, so gilt $\left(\frac{m}{k}\right) = \left(\frac{k}{m}\right)$; sind k und m beide kongruent zu 3 modulo 4, so hat man $\left(\frac{m}{k}\right) = -\left(\frac{k}{m}\right)$.

Beweis. Siehe Satz 11.7 in [For15]. □

Lemma 2.1.8 (1. und 2. Ergänzungssatz zum quadratischen Reziprozitätsgesetz)**.** *Für ungerade Primzahlen p ist:*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \quad \textit{beziehungsweise} \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Beweis. Siehe 1. bzw. 2. Ergänzungsatz zum quadratischen Reziprozitätsgesetz 3.2.6 in [Bun08]. □

Folgerung 2.1.9. *Nach Lemma 2.1.8 gilt:*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod 4 \\ -1 & \text{falls } p \equiv 3 \pmod 4. \end{cases}$$

Unter der Annahme, dass t ein quadratischer Rest modulo p ist, folgt:

$$1 = \left(\frac{t}{p}\right) = \left(\frac{t-p}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p-t}{p}\right).$$

Daraus schließen wir, dass $p - t$ für $p \equiv 1 \pmod 4$ ein quadratischer Rest modulo p ist, jedoch für $p \equiv 3 \pmod 4$ ein quadratischer Nichtrest ist.
Diese Folgerung reduziert den Rechenaufwand für die Bestimmung aller quadratischen Reste modulo p um die Hälfte. Davon profitieren gerade unsere Funktionen zur Erstellung der Datensätze im Rahmen des letzten Kapitels. Des Weiteren können wir daraus Rückschlüsse über Muster, die bei der Verteilung von d-Tupeln aufeinanderfolgender quadratischer Reste beziehungsweise Nichtreste auftreten, ziehen. Infolgedessen werden wir im Laufe dieser Arbeit mehrmals auf diese Folgerung verweisen.

2.2 Jacobsthalsche Summen

Definition 2.2.1. Sei $t \in \mathbb{Z}$, sei p eine ungerade Primzahl, dann definieren wir die sogenannten **Jacobsthalschen Summen:**

$$T_p(t) = \sum_{c=1}^{p-1} \left(\frac{c(c^2-t)}{p}\right).$$

Lemma 2.2.2. *Eigenschaften der Jacobsthalschen Summen:*
(i) *Es gilt $T_p(0) = 0$.*
(ii) *Für ganze t ist $T_p(t) = \left(1 + \left(\frac{-1}{p}\right)\right) \sum_{c=1}^{(p-1)/2} \left(\frac{c(c^2-t)}{t}\right)$.*
(iii) *Für $p \equiv 3 \pmod 4$ ist $T_p(t) = 0$ für alle ganzen t.*
(iv) *Für ganze s, t ist $T_p(s^2 t) = \left(\frac{s}{t}\right) T_p(t)$.*
(v) *$T_p(t)^2$ ist konstant für alle quadratischen Reste (bzw. Nichtreste) modulo p.*
(vi) *Ist $p \equiv 1 \pmod 4$ und t_0 irgendein quadratischer Nichtrest modulo p, so gilt*

$$T_p(1)^2 + T_p(t_0)^2 = 4.$$

Beweis. (i) $T_p(0) = \sum_{c=1}^{p-1} \left(\frac{c^3}{p}\right) = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) = 0$ nach 2.1.6(iii).

(ii)

$$\begin{aligned}
T_p(t) &= \sum_{c=1}^{p-1}\left(\frac{c(c^2-t)}{p}\right) \\
&= \sum_{c=1}^{(p-1)/2}\left(\frac{c(c^2-t)}{p}\right) + \sum_{c=(p+1)/2}^{p-1}\left(\frac{c(c^2-t)}{p}\right) \\
&= \sum_{c=1}^{(p-1)/2}\left(\frac{c(c^2-t)}{p}\right) + \sum_{c=1}^{(p-1)/2}\left(\frac{-c(c^2-t)}{p}\right) \\
&= \sum_{c=1}^{(p-1)/2}\left(\frac{c(c^2-t)}{p}\right) + \sum_{c=1}^{(p-1)/2}\left(\frac{-1}{p}\right)\left(\frac{c(c^2-t)}{p}\right) \\
&= \left(1+\left(\frac{-1}{p}\right)\right)\sum_{c=1}^{(p-1)/2}\left(\frac{c(c^2-t)}{p}\right).
\end{aligned}$$

(iii) Für $p \equiv 3 \pmod 4$ folgt aus Lemma 2.1.8, dass $\left(\frac{-1}{p}\right) = -1$ und somit folgt mit (ii) die Behauptung.
(iv) Siehe Lemma 3.3.4(iv) in [Bun08].
(v) Siehe Lemma 3.3.4(v) in [Bun08].
(vi) Siehe Lemma 3.3.4(vi) in [Bun08].

□

Chapter 3

Verteilung von quadratischen Resten

3.1 Allgemeines

Um Aussagen über die Verteilung und Anzahl von quadratischen Resten zu finden, ist es wichtig, sich Summen über gewisse Legendre-Symbole genauer anzuschauen. Betrachtet man ungerade Primzahlen p und natürliche, positive $d < p$, so möchten wir gerne die Anzahl von d-Tupeln sukzessiver natürlicher Zahlen kleiner p, die allesamt quadratische Reste modulo p sind, untersuchen. Für diesen Sachverhalt führen wir $Q_p(d)$ als Notation für die Anzahl von aufeinanderfolgenden d-Tupeln quadratischer Reste modulo p ein. Nach Lemma 2.1.5 gilt $Q_p(d) = 0$ für $\frac{1}{2}(p-1) < d$, sowie $Q_p(1) = \frac{1}{2}(p-1)$.
Im weiteren Verlauf dieses Kapitels werden zunächst Paare von quadratischen Resten, Tripel von quadratischen Resten sowie allgemeiner d-Tupel von quadratischen Resten betrachtet. Infolgedessen bestimmen wir $Q_p(2)$ sowie $Q_p(3)$ und betrachten außerdem den allgemeinen Fall $Q_p(d)$.
Ein wichtiges Lemma für die Betrachtung der Verteilung von quadratischen Resten ist folgendes:

Lemma 3.1.1.

$$S_p(a,b) = \sum_{t=0}^{p-1} \left(\frac{(t+a)(t+b)}{p} \right) = \begin{cases} p-1 & \textit{falls } a \equiv b \pmod{p} \\ -1 & \textit{sonst} \end{cases}$$

Beweis. Durch eine Verschiebung der Summationsreihenfolge um a können wir $S_p(a,b)$ schreiben als:

$$S_p(a,b) = \sum_{t=a}^{p-1+a} \left(\frac{t(t+b-a)}{p} \right).$$

Wir definieren $c = b - a$ und erhalten:

$$S_p(a,b) = \sum_{t=a}^{p-1+a} \left(\frac{t(t+c)}{p}\right). \tag{3.1}$$

Da wir in in (3.1) über ein vollständiges Restsystem modulo p summieren und nach Definition 2.1.2 gilt, dass $\left(\frac{0}{p}\right) = 0$, können wir $S_p(a,b)$ schreiben als:

$$S_p(a,b) = \sum_{t=1}^{p-1} \left(\frac{t(t+c)}{p}\right).$$

Sei jeweils $j(t)$ so, dass $j(t) \cdot t \equiv 1 \pmod{p}$ für $t \in \{1, \ldots, p-1\}$. Dann durchlaufen sowohl t als auch $j(t)$ das vollständige Restsystem modulo p. Infolgedessen können wir $S_p(a,b)$ wie folgt umformen:

$$S_p(a,b) = \sum_{t=1}^{p-1} \left(\frac{j(t)}{p}\right)^2 \left(\frac{t(t+c)}{p}\right) = \sum_{t=1}^{p-1} \left(\frac{1+j(t)c}{p}\right) = \sum_{j=1}^{p-1} \left(\frac{1+jc}{p}\right).$$

Falls $a \equiv b \pmod{p}$, so gilt $p \mid c$, daraus folgt, dass nach Lemma 2.1.6(i) alle Legendre-Symbole gleich $\left(\frac{1}{p}\right) = 1$ sind, womit der erste Teil des Lemmas gezeigt ist. Falls $a \not\equiv b \pmod{p}$ und somit $p \nmid c$, können wir folgern, dass wir für alle $j = \{1, \ldots, p-1\}$ das Restsystem modulo p ohne $[1]_p$ durchlaufen. Dadurch können wir $S_p(a,b)$ schreiben als:

$$S_p(a,b) = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) - \left(\frac{1}{p}\right) = -1.$$

Somit haben wir den zweiten Teil des Lemmas ebenfalls bewiesen. □

3.2 Paare quadratischer Reste

Für die Berechnung von $Q_p(2)$ betrachten wir zunächst die charakteristische Funktion für ein Paar von sukzessiven quadratischen Resten modulo p:

$$\mathrm{chp}_2(t) = \frac{1}{4}\left(\left(\frac{t}{p}\right)+1\right)\left(\left(\frac{t+1}{p}\right)+1\right).$$

Um die Gesamtanzahl der Paare zu ermitteln, muss man die charakteristische Funktion über alle relevanten t summieren. Dabei wird von $t = 1$ bis $t = p-2$ summiert.

$$Q_p(2) = \frac{1}{4}\sum_{t=1}^{p-2}\left(\left(\frac{t}{p}\right)+1\right)\left(\left(\frac{t+1}{p}\right)+1\right)$$

Satz 3.2.1. *Für ungerade Primzahlen p gibt es genau $\frac{1}{4}(p-4+(-1)^{(p+1)/2})$ Paare aufeinanderfolgender quadratischer Reste modulo p, die außerdem natürliche Zahlen kleiner als p sind.*

Beweis.

$$\begin{aligned} 4Q_p(2) &= \sum_{t=1}^{p-2}\left(\left(\frac{t}{p}\right)+1\right)\left(\left(\frac{t+1}{p}\right)+1\right) \\ &= \sum_{t=1}^{p-2}\left(1+\left(\frac{t}{p}\right)+\left(\frac{t+1}{p}\right)+\left(\frac{t}{p}\right)\left(\frac{t+1}{p}\right)\right) \end{aligned}$$

Für den weiteren Verlauf des Beweises trennen wir die Summe in die einzelnen Summanden und betrachten diese separat.

(i)

$$\sum_{t=1}^{p-2} 1 = p-2.$$

(ii)

$$\begin{aligned} \sum_{t=1}^{p-2}\left(\frac{t}{p}\right) &= \sum_{t=1}^{p-1}\left(\frac{t}{p}\right)-\left(\frac{p-1}{p}\right) \\ &\overset{2.1.6(iii)}{=} -\left(\frac{p-1}{p}\right) \\ &\overset{2.1.6(i)}{=} -\left(\frac{-1}{p}\right) \\ &\overset{2.1.8}{=} -(-1)^{(p-1)/2} \\ &= (-1)^{(p+1)/2}. \end{aligned}$$

(iii)

$$\begin{aligned} \sum_{t=1}^{p-2}\left(\frac{t+1}{p}\right) &= \sum_{t=2}^{p-1}\left(\frac{t}{p}\right) \\ &= \sum_{t=1}^{p-1}\left(\frac{t}{p}\right)-\left(\frac{1}{p}\right) \\ &\overset{2.1.6(iii)}{=} -1. \end{aligned}$$

(iv)

$$\begin{aligned}\sum_{t=1}^{p-2}\left(\frac{t}{p}\right)\left(\frac{t+1}{p}\right) &\overset{2.1.6(ii)}{=} \sum_{t=1}^{p-2}\left(\frac{t(t+1)}{p}\right)\\ &= \sum_{t=1}^{p-1}\left(\frac{t(t+1)}{p}\right)-\left(\frac{p(p-1)}{p}\right)\\ &= \sum_{t=0}^{p-1}\left(\frac{(t+1)(t+2)}{p}\right)\\ &= S_p(1,2)\\ &\overset{3.1.1}{=} -1.\end{aligned}$$

Daraus folgt:

$$Q_p(2)=\frac{1}{4}(p-4+(-1)^{(p+1)/2}).$$

□

Beispiel 3.2.2. Als Beispiel für die Verteilung von Paaren quadratischer Reste möchten wir im Folgenden $Q_{37}(2)$ bestimmen. Nach Satz 3.2.1 ist $Q_{37}(2)=8$. Diese Aussage kann mit Hilfe von Funktion 6.1.4 in PARI/GP beziehungsweise Funktion 6.2.4 in MATLAB überprüft werden. Dabei sind 1,3,4,7,9,10,11,12,16,21,25,26,7,28,30,33,34,36 quadratische Reste modulo 37. Wir finden dementsprechend genau die Paare (3,4), (9,10), (10,11), (11,12), (25,26), (26,27), (27,28) sowie (33,34).

x	1	2	3	4	5	6	7	8	9	10	11	12
R/N	R	N	R	R	N	N	R	N	R	R	R	R

x	13	14	15	16	17	18	19	20	21	22	23	24
R/N	N	N	N	R	N	N	N	N	R	N	N	N

x	25	26	27	28	29	30	31	32	33	34	35	36
R/N	R	R	R	R	N	R	N	N	R	R	N	R

Hier haben wir zur Abkürzung i statt $[i]_{37}$ geschrieben sowie R für "x ist quadratischer Rest modulo 37" beziehungsweise N für "x ist quadratischer Nichtrest modulo 37".

3.3 Tripel quadratischer Reste

Für die Berechnung von $Q_p(3)$ betrachten wir analog zu den Paaren quadratischer Reste zunächst die charakteristische Funktion für ein Tripel von sukzessiven

quadratischen Resten modulo p:

$$\mathrm{chp}_3(t) = \frac{1}{8}\left(\left(\frac{t-1}{p}\right)+1\right)\left(\left(\frac{t}{p}\right)+1\right)\left(\left(\frac{t+1}{p}\right)+1\right).$$

Dabei bietet es sich an, das Tripel $(t-1, t, t+1)$ statt $(t, t+1, t+2)$ zu betrachten. Um die Gesamtanzahl der Tripel zu bestimmen, muss man nun die charakteristische Funktion über alle relevanten t summieren. Durch die Wahl unseres Tripels ist eine Summation von $t = 2$ bis $t = p-2$ notwendig.

$$Q_p(3) = \frac{1}{8}\sum_{t=2}^{p-2}\left(\left(\frac{t-1}{p}\right)+1\right)\left(\left(\frac{t}{p}\right)+1\right)\left(\left(\frac{t+1}{p}\right)+1\right)$$

Satz 3.3.1. *Für ungerade Primzahlen p existieren genau*

$$Q_p(3) = \begin{cases} \frac{1}{8}(p + T_p(1) - 11 - 4(-1)^{(p-1)/4}) & \textit{falls } p \equiv 1 \pmod 4 \\ [\frac{1}{8}p] & \textit{falls } p \equiv 3 \pmod 4 \end{cases}$$

Tripel aufeinanderfolgender quadratischer Reste modulo p, die außerdem natürliche Zahlen kleiner p sind.

Hierbei handelt es sich bei $[\frac{1}{8}p]$ um die Gaußklammer, das heißt wir runden auf die nächstkleinere ganze Zahl ab.

Beweis. Für $p = 3$ können Tripel sukzessiver quadratischer Reste nicht auftreten, weshalb der behauptete Satz richtig ist. Der Beweis für $p \geq 5$ verläuft analog dem Schema des Beweises für die Anzahl von Paaren quadratischer Reste.

$$8Q_p(3) \quad = \quad \sum_{t=2}^{p-2}\left(\left(\frac{t-1}{p}\right)+1\right)\left(\left(\frac{t}{p}\right)+1\right)\left(\left(\frac{t+1}{p}\right)+1\right)$$

Nach dem Ausmultiplizieren des oberen Terms erhält man acht einzelne Summanden, die wir für den weiteren Verlauf des Beweises trennen und separat betrachten.

(i)

$$\sum_{t=2}^{p-2} 1 = p - 3.$$

(ii)

$$\begin{aligned} \sum_{t=2}^{p-2}\left(\frac{t}{p}\right) \quad &= \quad \sum_{t=1}^{p-1}\left(\frac{t}{p}\right) - \left(\frac{1}{p}\right) - \left(\frac{p-1}{p}\right) \\ &\overset{2.1.6(iii)}{=} \quad -\left(\frac{1}{p}\right) - \left(\frac{p-1}{p}\right) \\ &\overset{2.1.8}{=} \quad -1 - (-1)^{(p-1)/2}. \end{aligned}$$

(iii)

$$\begin{aligned}
\sum_{t=2}^{p-2}\left(\frac{t-1}{p}\right) &= \sum_{t=1}^{p-3}\left(\frac{t}{p}\right) \\
&= \sum_{t=1}^{p-1}\left(\frac{t}{p}\right) - \left(\frac{p-2}{p}\right) - \left(\frac{p-1}{p}\right) \\
&\overset{2.1.6(iii)}{=} -\left(\frac{p-2}{p}\right) - \left(\frac{p-1}{p}\right) \\
&\overset{2.1.6(i)}{=} -\left(\frac{-2}{p}\right) - \left(\frac{-1}{p}\right) \\
&= -\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) - \left(\frac{-1}{p}\right) \\
&= -(-1)^{(p-1)/2+(p^2-1)/8} - (-1)^{(p-1)/2}.
\end{aligned}$$

(iv)

$$\begin{aligned}
\sum_{t=2}^{p-2}\left(\frac{t(t-1)}{p}\right) &\overset{3.1.1}{=} S_p(0,-1) - \left(\frac{(p-1)(p-2)}{p}\right) \\
&\overset{3.1.1}{=} -1 - \left(\frac{p-1}{p}\right)\left(\frac{p-2}{p}\right) \\
&= -1 - \left(\frac{-1}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \\
&= -1 - (-1)^{(p^2-1)/8}.
\end{aligned}$$

(v)

$$\begin{aligned}
\sum_{t=2}^{p-2}\left(\frac{t+1}{p}\right) &= \sum_{t=3}^{p-1}\left(\frac{t}{p}\right) \\
&= \sum_{t=1}^{p-1}\left(\frac{t}{p}\right) - \left(\frac{1}{p}\right) - \left(\frac{2}{p}\right) \\
&\overset{2.1.6(iii)}{=} -\left(\frac{1}{p}\right) - \left(\frac{2}{p}\right) \\
&\overset{2.1.8}{=} -1 - (-1)^{(p^2-1)/8}.
\end{aligned}$$

(vi)

$$\begin{aligned}\sum_{t=2}^{p-2}\left(\frac{t(t+1)}{p}\right) &= S_p(0,1)-\left(\frac{2}{p}\right)-\left(\frac{p(p-1)}{p}\right)\\ &= S_p(0,1)-\left(\frac{2}{p}\right)\\ &\overset{2.1.8}{=} -1-(-1)^{(p^2-1)/8}.\end{aligned}$$

(vii)

$$\begin{aligned}\sum_{t=2}^{p-2}\left(\frac{(t+1)(t-1)}{p}\right) &= S_p(1,-1)-\left(\frac{p(p-2)}{p}\right)\\ &= S_p(1,-1)-\left(\frac{-1}{p}\right)\\ &\overset{3.1.1}{=} -1-(-1)^{(p-1)/2}.\end{aligned}$$

(viii)

$$\begin{aligned}\sum_{t=2}^{p-2}\left(\frac{t(t+1)(t-1)}{p}\right) &= \sum_{t=2}^{p-2}\left(\frac{t(t^2-1)}{p}\right)\\ &\overset{2.2.1}{=} T_p(1)-\left(\frac{(p-1)((p-1)^2-1)}{p}\right)\\ &= T_p(1)-\left(\frac{p(p-1)(p-2)}{p}\right)\\ &= T_p(1).\end{aligned}$$

Daraus folgt:

$$8Q_p(3) = p-8-3(-1)^{(p-1)/2}-3(-1)^{(p^2-1)/8}-(-1)^{(p-1)/2+(p^2-1)/8}+T_p(1).$$

Für eine weitere Vereinfachung des Terms betrachten wir im Folgenden die beiden Fälle $p \equiv 1 \pmod 4$ und $p \equiv 3 \pmod 4$.

Falls $p \equiv 1 \pmod 4$ folgt daraus, dass $p \equiv 1 \pmod 8$ oder $p \equiv 5 \pmod 8$.

(i) Für $p \equiv 1 \pmod 8$ gilt $p = 1+8k, k \in \mathbb{Z}$, daraus folgt $(p^2-1)/8 = 2k+8k^2, k \in \mathbb{Z}$. Außerdem gilt $(p-1)/4 = 2k$. Da beide betrachteten Terme für beliebiges $k \in \mathbb{Z}$ gerade sind, folgt:

$$(-1)^{(p^2-1)/8} = (-1)^{(p-1)/4} \quad \text{für} \quad p \equiv 1 \pmod 8.$$

(ii) Für $p \equiv 5 \pmod 8$ gilt $p = 5 + 8k, k \in \mathbb{Z}$, daraus folgt $(p^2 - 1)/8 = 3 + 10k + 8k^2, k \in \mathbb{Z}$. Außerdem gilt $(p - 1)/4 = 1 + 2k$. Da beide betrachteten Terme für beliebiges $k \in \mathbb{Z}$ ungerade sind, folgt:

$$(-1)^{(p^2-1)/8} = (-1)^{(p-1)/4} \quad \text{für} \quad p \equiv 5 \pmod 8.$$

Aus beiden Fällen folgt, dass $(-1)^{(p^2-1)/8} = (-1)^{(p-1)/4} \quad \text{für} \quad p \equiv 1 \pmod 4$, somit folgt der erste Teil der Behauptung:

$$Q_p(3) = \frac{1}{8}(p + T_p(1) - 11 - 4(-1)^{(p-1)/4}) \quad \text{für} \quad p \equiv 1 \pmod 4.$$

Für $p \equiv 3 \pmod 4$ folgt nach Lemma 2.2.2(iii) über die Jacobsthalschen Summen

$$8Q_p(3) = p - 5 - 2(-1)^{(p^2-1)/8} = \begin{cases} p - 3 & \text{für } p \equiv 3 \pmod 8 \\ p - 7 & \text{für } p \equiv 7 \pmod 8. \end{cases}$$

Damit folgt ebenfalls der zweite Teil der Behauptung.

□

Beispiel 3.3.2. Als Beispiel für die Verteilung von Tripeln quadratischer Reste möchten wir im Folgenden $Q_{41}(3)$ sowie $Q_{43}(3)$ bestimmen.

Nach Satz 3.3.1 ist $Q_{41}(3) = \frac{1}{8}(41 + T_{41}(1) - 11 - 4(-1)^{(41-1)/4})$, da $41 \equiv 1 \pmod 4$. Durch die Berechnung der Jacobsthalschen Summe

$$T_{41}(1) = \sum_{t=1}^{40} \left(\frac{t(t^2 - 1)}{41}\right) = -10$$

folgt $Q_{41}(3) = 2$.

x	1	2	3	4	5	6	7	8	9	10	11	12
R/N	R	R	N	R	R	N	N	R	R	R	N	N

x	13	14	15	16	17	18	19	20	21	22	23	24
R/N	N	N	N	R	N	R	N	R	R	N	R	N

x	25	26	27	28	29	30	31	32	33	34	35	36
R/N	R	N	N	N	N	N	R	R	R	N	N	R

x	37	38	39	40
R/N	R	N	R	R

Nach Satz 3.3.1 ist $Q_{43}(3) = 5$, da $43 \equiv 3 \pmod 4$.

x	1	2	3	4	5	6	7	8	9	10	11	12
R/N	R	N	N	R	N	R	N	N	R	R	R	N

x	13	14	15	16	17	18	19	20	21	22	23	24
R/N	R	R	R	R	R	N	N	N	R	N	R	R

x	25	26	27	28	29	30	31	32	33	34	35	36
R/N	R	N	N	N	N	N	R	N	N	N	R	R

x	37	38	39	40	41	42
R/N	N	R	N	R	R	N

Am Ende dieses Abschnittes wollen wir noch eine abschließende Aussage bezüglich der Abschätzung für $Q_p(3)$ treffen. Für den Fall $p \equiv 3 \pmod 4$ können wir den Fehler nach 3.3.1 bis auf einen absoluten Fehler von 1 abschätzen. Da im Fall $p \equiv 1 \pmod 4$ die Jacobsthalschen Summen nicht zu Null werden, versuchen wir eine geeignete Abschätzung für $T_p(1)$ zu finden. Wendet man auf die Definition der Jacobsthalschen Summen die Dreiecksungleichung an, so erhält man $\mid T_p(1) \mid \leq p-1$. Diese Abschätzung ist jedoch weder für kleine p noch für große p zufriedenstellend. Wir nutzen deshalb Lemma 2.2.1(vi) und erhalten $\mid T_p(1) \mid \leq 2\sqrt{p}$ für $p \equiv 1 \pmod 4$. Dementsprechend folgt:

$$Q_p(3) = \frac{1}{8}p + \mathcal{O}(\sqrt{p}).$$

Wir wissen jedoch nicht, ob die aus Lemma 2.2.1(vi) folgende Abschätzung bezüglich $T_p(1)$ scharf ist.
Für die Abschätzung von $T_p(1)$ haben wir für zufällig gewählte Primzahlen p mit $p \equiv 1 \pmod 4$ aus unseren Datensätzen die Jacobsthalsche Summe $T_p(1)$ berechnet und die Abweichung zu unserer gegebenen Abschätzung $2\sqrt{p}$ ermittelt (Skript

6.2.7). Dafür haben wir die maximale relative Abweichung (1. Spalte) sowie das Mittel der relativen Abweichung (2. Spalte) bestimmt und in der unten stehenden Tabelle aufgeführt. Wir haben für alle folgenden Berechnungen Primzahlen mit Hilfe der Funktion 6.1.1 erzeugt. Die Größenordnungen unserer Datensätze können dem Skript 6.1.2 entnommen werden. Die Zeilen der Tabelle entsprechen den jeweiligen Datensätzen.

Tabelle 3.3.3.

19,03	2,4950
65,011	3,3001
17,241	1,7740
28,311	2,8231
123,48	5,0643

Anhand dieser Tabelle können wir erkennen, dass die Abschätzung $\mid T_p(1) \mid \leq 2\sqrt{p}$ für $p \equiv 1 \pmod 4$ relativ genau ist. Wir werden diese Erkenntnis im Kapitel über die Verteilung von allgemeinen d-Tupel erneut aufgreifen und versuchen auch für höherwertige Tupel quadratischer Reste zuverlässige Abschätzungen zu finden.

3.4 Verteilung von quadratischen Nichtresten

Nachdem wir uns bereits der Verteilung von aufeinanderfolgenden quadratischen Resten modulo p gewidmet haben, möchten wir analog dazu ebenfalls die Verteilung von quadratischen Nichtresten modulo p betrachten. Dazu führen wir für die Anzahl von aufeinanderfolgenden d-Tupeln quadratischer Nichtreste die Notation $\widetilde{Q}_p(d)$ ein. Bei der Bestimmung von $\widetilde{Q}_p(d)$ gehen wir in den gleichen Schritten vor und geben in diesem Abschnitt nur die zur Berechnung notwendigen Formeln sowie besondere Bemerkungen an.

Definition 3.4.1. Für ungerade Primzahlen p und $t \in \mathbb{Z}$ definieren wir

$$\widetilde{\mathrm{chp}_1}(t) = \frac{1}{2}\left(1 - \left(\frac{t}{p}\right)\right) = \begin{cases} 1 & \text{falls } [t]_p \text{ quadratischer Nichtrest modulo } p \\ \frac{1}{2} & \text{falls } [t]_p = [0]_p \\ 0 & \text{falls } [t]_p \text{ quadratischer Rest modulo } p \end{cases}$$

als charakteristische Funktion für die Bestimmung von t als quadratischen Nichtrest modulo p.

Des Weiteren definieren wir die charakteristische Funktion für d-Tupel von aufeinanderfolgenden quadratischen Nichtresten modulo p wie folgt:

Sei $d < p$, sei p eine ungerade Primzahl, sei $t \in \mathbb{Z}$:.

$$\widetilde{\mathrm{chp}_d}(t) = \left(\frac{1}{2}\right)^d \cdot \prod_{i=0}^{d-1} \left(1 - \left(\frac{t+i}{p}\right)\right).$$

3.4.1 Paare von quadratischen Nichtresten

Für die Bestimmung von $\widetilde{Q}_p(2)$ betrachten wir die folgende Summe:

$$\widetilde{Q}_p(2) = \frac{1}{4} \sum_{t=1}^{p-2} \left(1 - \left(\frac{t}{p}\right)\right)\left(1 - \left(\frac{t+1}{p}\right)\right).$$

Satz 3.4.2. *Für ungerade Primzahlen p gibt es genau $\frac{1}{4}(p-2+(-1)^{(p-1)/2})$ Paare aufeinanderfolgender quadratischer Nichtreste modulo p, die außerdem natürliche Zahlen kleiner als p sind.*

Nach Lemma 2.1.8 und Satz 3.2.1 gilt für $p \equiv 3 \pmod 4$, dass $Q_p(2) = \widetilde{Q}_p(2)$. Um über ein Muster in der Verteilung von Paaren quadratischer Reste sowie quadratischer Nichtreste Aussagen zu treffen, möchten wir die Folgerung 2.1.9 umformulieren und auf die Darstellung wie in unseren Beispielen als Tabelle anwenden.

Folgerung 3.4.3. *Betrachtet man eine Tabelle wie in unseren Beispielen, so lässt sich Folgerung 2.1.9 wie folgt umformulieren: Für $p \equiv 1 \pmod 4$ besitzt die Tabelle nach dem Wert $(p-1)/2$ eine Symmetrieachse und quadratische Reste sowie quadratische Nichtreste spiegeln sich an dieser Achse.*
Für $p \equiv 3 \pmod 4$ besitzt die Tabelle ebenfalls nach dem Wert $(p-1)/2$ eine Symmetrieachse, jedoch spiegeln sich die quadratischen Reste und quadratischen Nichtreste an dieser Achse als entgegengesetzter Wert, das heißt ein quadratischer Rest wird zum quadratischen Nichtrest und andersherum.
Um diesen Sachverhalt nachzuvollziehen, empfehlen wir dem Leser, sich das Beispiel 3.3.2 erneut anzusehen.

In [Jac06] betrachtet Jacobsthal auch die verschiedenen Permutationen von quadratischen Resten sowie Nichtresten innerhalb von Paaren. Für die Vollständigkeit dieses Abschnittes wollen wir diese Formeln ohne Beweis aufführen.

Satz 3.4.4. *Für ungerade Primzahlen p gibt es genau $\frac{1}{4}(p-2+(-1)^{(p-1)/2})$ Paare, bestehend aus einem quadratischen Nichtrest modulo p gefolgt von einem quadratischen Rest modulo p.*

Satz 3.4.5. *Für ungerade Primzahlen p gibt es genau $\frac{1}{4}(p-(-1)^{(p-1)/2})$ Paare, bestehend aus einem quadratischen Rest modulo p gefolgt von einem quadratischen Nichtrest modulo p.*

Für eine anschauliche Anwendung dieser beiden Sätze empfehlen wir dem Leser, sich das Beispiel 3.3.2 erneut anzusehen.

3.4.2 Tripel von quadratischen Nichtresten

Für die Bestimmung von $\widetilde{Q}_p(3)$ betrachten wir die folgende Summe:

$$\widetilde{Q}_p(3) = \frac{1}{8}\sum_{t=2}^{p-2}\left(1-\left(\frac{t-1}{p}\right)\right)\left(1-\left(\frac{t}{p}\right)\right)\left(1-\left(\frac{t+1}{p}\right)\right).$$

Satz 3.4.6. *Für ungerade Primzahlen p existieren genau*

$$\widetilde{Q}_p(3) = \begin{cases} \frac{1}{8}\left(p-3-2T_p(1)\right) & \text{falls } p \equiv 1 \pmod 4 \\ \frac{1}{8}\left(p-5-2(-1)^{(p^2-1)/8}\right) & \text{falls } p \equiv 3 \pmod 4 \end{cases}$$

Tripel aufeinanderfolgender quadratischer Nichtreste modulo p, die außerdem natürliche Zahlen kleiner als p sind.

Wie auch bei den Paaren quadratischer Nichtreste können wir die Folgerung 2.1.9 nutzen, um Rückschlüsse auf die Verteilung von quadratischen Nichtresten modulo p anhand von Symmetrien in den Beispieltabellen zu finden.
In [Jac06] betrachtet Jacobsthal auch die verschiedenen Permutationen von quadratischen Resten sowie Nichtresten innerhalb von Tripeln. Aufgrund der Vielzahl der möglichen Permutationen möchten wir diese Formeln nicht explizit angeben und verweisen den interessierten Leser an dieser Stelle auf [Jac06].

3.5 n-Tupel quadratischer Reste

Die Berechnung der Anzahl von beliebigen d-Tupeln von aufeinanderfolgenden quadratischen Resten modulo p wird in der uns vorliegenden Hauptquelle [Bun08] von Bundschuh nicht weiter behandelt. Dennoch möchten wir im Rahmen dieser Arbeit die Anzahl $Q_p(d)$ für allgemeine d-Tupel bestimmen beziehungsweise versuchen, diese möglichst zuverlässig abzuschätzen. Dazu haben wir die weitere Literatur [Bra32],[Dav31],[Hop30] und [Doe29] von Autoren hinzugezogen, die sich bereits zu Beginn des 20. Jahrhunderts mit dieser Frage beschäftigt haben. Die wichtigen Punkte der ersten Arbeiten wurden im Laufe des 20. Jahrhunderts immer wieder aufgegriffen und die bereits gewonnene Abschätzung weiter verbessert.

Zu Beginn wollen wir den Fall d=4 betrachten. Dazu haben wir mit Hilfe der von uns implementierten Funktion 6.2.4 eine numerische Bestimmung von $Q_p(4)$ für unsere verschiedenen Datensätze durchgeführt. Bereits bei den Paaren und Tripeln von quadratischen Resten konnten wir erkennen, dass der größte Einfluss auf $Q_p(d)$

von den Konstanten der charakteristischen Funktionen stammt. Für unseren Fall d=4 gilt somit der Term $\frac{1}{16}p$ als erste Näherung für $Q_p(4)$. Aufgrund dessen haben wir unsere mit Skript 6.2.8 gewonnenen Daten mit dem Term $\frac{1}{16}p$ verglichen. Um mögliche Muster für verschiedene Arten von Primzahlen zu finden, haben wir die Primzahlen p in unseren Datensätzen (Skript 6.1.2) in die beiden Kongruenzklassen $p \equiv 1 \pmod 4$ und $p \equiv 3 \pmod 4$ unterteilt. Die Abweichung zum Hauptterm $\frac{1}{16}p$ haben wir in der ersten Tabelle als relativen Fehler und in der zweiten Tabelle als absoluten Fehler aufgeführt. Dabei kann der ersten Spalte die Kongruenzklasse, der zweiten Spalte der maximale betrachtete Fehler sowie der dritten Spalte das Mittel des jeweiligen betrachteten Fehlers entnommen werden:

Tabelle 3.5.1.

$p \equiv 1 \pmod 4$	0,6	0,0378
$p \equiv 3 \pmod 4$	0,25	0,0109

$p \equiv 1 \pmod 4$	418	68,1290
$p \equiv 3 \pmod 4$	100	21,903

Wir können den Tabellen entnehmen, dass sich sowohl relative sowie absolute Fehler und Mittel der Fehler für die beiden Kongruenzklassen stark unterscheiden. Auffällig ist vor allem der absolute Fehler für die Kongruenzklasse $p \equiv 3 \pmod 4$, der deutlich geringer als für die Kongruenzklasse $p \equiv 1 \pmod 4$, ausfällt. Diese Auffälligkeit weist darauf hin, dass wir analog zur Bestimmung der Anzahl von Tripel quadratischer Reste modulo p für den Fall $p \equiv 3 \pmod 4$ eine zuverlässigere Abschätzung finden können. Um sicher zu gehen, dass wir kein Muster übersehen, haben wir zusätzlich das gleiche Verfahren mit $p \equiv k \pmod 8, k \in 1, 3, 5, 7$ angewendet. Wir haben erneut die relative Abweichung vom Hauptterm $\frac{1}{16}p$ in der ersten Tabelle und die absolute Abweichung der zweiten Tabelle dargestellt (die Zuordnung der Spalten entspricht der oberen Tabelle):

Tabelle 3.5.2.

$p \equiv 1 \pmod 8$	0,6	0,0387
$p \equiv 3 \pmod 8$	0,1177	0,0081
$p \equiv 5 \pmod 8$	0,5556	0,0370
$p \equiv 7 \pmod 8$	0,25	0,0146

$p \equiv 1 \pmod 8$	404	62,162
$p \equiv 3 \pmod 8$	100	22,685
$p \equiv 5 \pmod 8$	418	73,023
$p \equiv 7 \pmod 8$	98	20,848

Die Ergebnisse der Betrachtung der Kongruenz modulo 8 bringen uns die Bestätigung, dass wir kein Muster übersehen haben, da $[1]_4 = [1]_8 \cup [5]_8$. Analog dazu gilt $[3]_4 = [3]_8 \cup [7]_8$. Dies gibt uns den Anlass, im weiteren Verlauf dieses Kapitels den Fall d=4 weiter zu betrachten und gegebenenfalls eine mathematische Begründung für unsere Resultate zu finden. Da wir bisher die 4-Tupel von aufeinanderfolgenden quadratischen Resten nur numerisch untersucht haben, wenden wir uns nun explizit

der Anzahl $Q_p(4)$ zu:

$$Q_p(4) = \frac{1}{16}\sum_{t=2}^{p-3}\left(\left(\frac{t-1}{p}\right)+1\right)\left(\left(\frac{t}{p}\right)+1\right)\left(\left(\frac{t+1}{p}\right)+1\right)\left(\left(\frac{t+2}{p}\right)+1\right).$$

Im bisherigen Verlauf dieser Arbeit haben wir bereits einen Großteil der durch das Ausmultiplizieren entstehenden Terme genauer untersucht und vereinfacht. Deshalb führen wir im Folgenden nur die durch das Ausmultiplizieren entstehenden Terme auf, die ein Produkt von drei oder vier Legendre-Symbolen enthalten. Diese Arten von Termen lassen sich nicht auf die übliche Weise abschätzen und spielen für eine Abschätzung von $Q_p(4)$ somit eine gesonderte Rolle.

(i)

$$\begin{aligned}
\sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t}{p}\right)\left(\frac{t+1}{p}\right) &= T_p(1) - \left(\frac{(p-1)(p-2)(p-3)}{p}\right) \\
&= T_p(1) - \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right). \\
\sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t}{p}\right)\left(\frac{t+2}{p}\right) &= \sum_{t=3}^{p-2}\left(\frac{t-1}{p}\right)\left(\frac{t}{p}\right)\left(\frac{t+1}{p}\right) \\
&= T_p(1) - \left(\frac{1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) \\
&= T_p(1) + \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right).
\end{aligned}$$

Addieren wir beide Summen, so fällt auf, dass sich die beiden Produkte aus den Legendre-Symbolen gegenseitig aufheben und wir können schreiben:

$$\sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t}{p}\right)\left(\frac{t+1}{p}\right) + \sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t}{p}\right)\left(\frac{t+2}{p}\right) = 2T_p(1).$$

Nach Lemma 2.2.2(iii) gilt $T_p(t=1) = 0$ für $p \equiv 3 \pmod 4$, sodass wir einen Hinweis für unsere Beobachtung aus der Tabelle 3.5.1 erhalten.

(ii) Die beiden verbleibenden Summen über ein Produkt von drei Legendre-Symbolen lassen sich durch eine genaue Betrachtung der zu multiplizierenden Legendre-Symbole vereinfachen.

$$\lambda = \sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t}{p}\right)\left(\frac{t+2}{p}\right)$$

$$\mu = \sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t+1}{p}\right)\left(\frac{t+2}{p}\right)$$

Im ersten Term summieren wir über die folgenden Tupel für t:

$$(1,2,4),(2,3,5),(3,4,6), \quad ... \quad ,(p-5,p-4,p-2),(p-4,p-3,p-1).$$

Im Vergleich dazu findet die Summation in μ über folgende Tupel für t statt:

$$(1,3,4),(2,4,5),(3,5,6), \quad ... \quad ,(p-5,p-3,p-2),(p-4,p-2,p-1).$$

Durch diese Darstellung erkennen wir, dass es sich bei den Werten für t in μ um die Werte von t in λ modulo p mit negativen Vorzeichen handelt. Aufgrund dessen können wir den zweiten Term mit $\left(\frac{-1}{p}\right)$ multiplizieren und erhalten durch Anwendung von Lemma 2.1.6(i):

$$\sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t}{p}\right)\left(\frac{t+2}{p}\right) = \left(\frac{-1}{p}\right)\sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t+1}{p}\right)\left(\frac{t+2}{p}\right). \tag{3.2}$$

Für unseren Sonderfall $p \equiv 3 \pmod 4$ heben sich beide Summen gegenseitig auf, da nach Satz 2.1.8 $\left(\frac{-1}{p}\right) = -1$ für $p \equiv 3 \pmod 4$ gilt. Dies liefert uns einen weiteren Hinweis für unsere Beobachtungen aus Tabelle 3.5.1. Im Fall $p \equiv 1 \pmod 4$ können wir vorerst keine Aussagen treffen. Wir werden jedoch im weiteren Verlauf dieses Kapitels eine Möglichkeit zur Abschätzung dieser Summen finden.

(iii) Der letzte zu betrachtende Term ist die Summe über vier Legendre-Symbole. Für diesen Fall lassen sich keine Vereinfachungen, die mit den bereits aufgeführten vergleichbar sind, finden. Bereits in den 1930ern beschäftigten sich Davenport und Brauer mit einer Abschätzung dieser Art von Termen:

$$\sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t}{p}\right)\left(\frac{t+1}{p}\right)\left(\frac{t+2}{p}\right).$$

Wie wir diese Summe dennoch abschätzen können, möchten wir an dieser Stelle noch nicht weiter ausführen. Wir werden diese Problematik jedoch nur kurz ruhen lassen und später erneut aufgreifen.

Durch das Umformen aller 16 Terme, die wir durch das Ausmultiplizieren erhalten,

ergibt sich die folgende Formel zur Berechnung von $Q_p(4)$:

$$\begin{aligned} 16Q_p(4) = p &- 13 \\ &+ \left(1+\left(\frac{-1}{p}\right)\right)\lambda + 2T_p(1) \\ &- \left(\frac{-1}{p}\right)\left(5+4\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)+\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)\right) \\ &- \left(\frac{2}{p}\right)\left(6+3\left(\frac{3}{p}\right)\right) \\ &- 3\left(\frac{3}{p}\right) \\ &+ \sum_{t=2}^{p-3}\left(\frac{t-1}{p}\right)\left(\frac{t}{p}\right)\left(\frac{t+1}{p}\right)\left(\frac{t+2}{p}\right). \end{aligned}$$

Wie bereits in diesem Kapitel erwähnt, wirkt sich der Term $\left(\frac{1}{2}\right)^d \cdot p$ am stärksten auf die Anzahl $Q_p(d)$ aus. Des Weiteren können wir den Großteil der restlichen Terme ohne großen rechnerischen Aufwand bestimmen. Dennoch ist uns dies nicht mit allen auftretenden Termen möglich. Nichtsdestotrotz wollen wir im weiteren Verlauf dieses Kapitels eine möglichst genaue Abschätzung finden. In [Con] hat Conrad bereits mit Hilfe der Weil-Schranke eine Abschätzung, die sogar für allgemeine d-Tupel quadratischer Reste genutzt werden kann, gefunden.

Satz 3.5.3 (Weil-Schranke für das Legendre-Symbol)**.** *Für ungerade Primzahlen p und nicht-konstante Polynome $f(x) \in \mathbb{F}_p[x]$ ohne mehrfache Nullstellen, gilt:*

$$\left|\sum_{a\in\mathbb{F}_p}\left(\frac{f(a)}{p}\right)\right| \leq (\mathrm{grad}(f)-1)\sqrt{p}.$$

Beweis. Siehe [Con] und [Wei48]. □

Lemma 3.5.4. *In [Con] gibt Conrad die folgende Abschätzung für die Anzahl von allgemeinen d-Tupeln quadratischer Reste modulo p an:*

$$\mid Q_p(d) - \left(\frac{p}{2^d}\right) \mid < (d-1)\sqrt{p} + \frac{d}{2}.$$

Bei dieser Abschätzung geht Conrad sehr grob vor, da er alle Terme, die durch das Ausmultiplizieren der charakteristischen Funktionen entstehen, bis auf den konstanten Term mit Hilfe der Weil-Schranke abschätzt. Schon unser Beispiel für die Anzahl von Tripeln quadratischer Reste modulo p hat gezeigt, dass durchaus eine bessere Abschätzung möglich ist, indem wir nur die Terme mit Polynomen von Grad 3 oder höher in den Legendre-Symbolen mit Hilfe der Weil-Schranke abschätzen. Aufgrund

dessen werden wir im weiteren Verlauf dieses Kapitels versuchen, die von Conrad verwendete Konstante $(d-1)$ vor $\sqrt{p}$ zu verkleinern und somit eine genauere Abschätzung zu erhalten.

Durch Umformung unserer Gleichung für die Anzahl $Q_p(4)$ und Anwendung der Weil-Schranke erhalten wir die folgende Abschätzung:

Satz 3.5.5.

$$\mid Q_p(4) - \frac{1}{16}p \mid < \begin{cases} \frac{11}{16}\sqrt{p} + \frac{36}{16} & \textit{für } p \equiv 1 \pmod 4 \\ \frac{3}{16}\sqrt{p} + \frac{36}{16} & \textit{für } p \equiv 3 \pmod 4. \end{cases}$$

Wir sehen bereits, dass diese Abschätzung deutlich stärker ist als die von Conrad angegebene. Um die Verbesserung der Abschätzung zu verdeutlichen, bestimmen wir die größte Primzahl p, für die $Q_p(4)$ nach der von Conrad gegebenen Schranke gleich Null sein kann.

Wir setzen $Q_p(4) = 0$, daraus folgt $p < 48\sqrt{p}+32$. Diese Ungleichung wird von allen $0 < p < 2367,56$ erfüllt. Die nächstkleinere Primzahl ist $p = 2357$. Wir schließen daraus, dass für alle Primzahlen $p > 2357$ gelten muss: $Q_p(4) > 0$.

Es lässt sich erkennen, dass es sich bei dem nach Condrad bestimmten p um eine sehr hohe Primzahl handelt, und bereits unsere ersten numerischen Beispiele lassen darauf schließen, dass Conrads Schranke nicht scharf erscheint, da wir bereits in unserem Beispiel in der Einleitung sehen können, das wir für $p = 19$ ein 4-Tupel erhalten. Wir möchten dennoch Conrads Abschätzung nicht schmälern und mit der von uns bestimmten Abschätzung fortfahren und die gleiche Rechnung durchführen:

(i) für $p \equiv 1 \pmod 4$ folgt: $p < 186,03$.
(ii) für $p \equiv 3 \pmod 4$ folgt: $p < 59,05$.

Dementsprechend gelten für unsere Abschätzung, dass die Anzahl $Q_p(4) > 0$ sein muss für alle Primzahlen p mit $p \equiv 1 \pmod 4$ und $p > 181$ sowie, dass die Anzahl $Q_p(4) > 0$ sein muss für alle Primzahlen p mit $p \equiv 3 \pmod 4$ und $p > 59$. Wir sehen nun deutlich, dass unsere Abschätzung das minimale p genauer bestimmt. Auch unsere Abschätzung kann aufgrund des Beispiels der Einleitung noch verbessert werden. Des Weiteren liefert Jacobsthal in [Jac06] einen Beweis, dass $p = 19$ die kleinste Primzahl mit $Q_p(4) > 0$ ist.

Nachdem wir d-Tupel für $d = 4$ betrachtet haben, möchten wir zum Abschluss d-Tupel für $d = 5$ betrachten. Dazu betrachten wir die Zähl-Funktion für $Q_p(5)$:

$$Q_p(4) = \frac{1}{32}\sum_{t=3}^{p-3}\prod_{i=1}^{5}\left(\left(\frac{t-3+i}{p}\right)+1\right).$$

Wie bereits bei der Vereinfachung von $Q_p(4)$ haben wir im Rahmen dieser Arbeit den Großteil der 32 nach dem Ausmultiplizieren auftretenden Terme bereits vereinfacht. Aufgrund dessen gehen wir für $Q_p(5)$ nur auf Summen über Legendre-Symbole ein, die sich in bestimmten Fällen besonders leicht darstellen lassen.
Betrachten wir die zehn entstehenden Summen über drei Legendre-Symbole so erkennen wir, dass wir aus zwei dieser Terme die Jacobsthalschen Summen $T_p(1)$ und $T_p(4)$ erhalten. Beide Jacobsthalschen Summen sind nach Lemma 2.2.1(iii) gleich Null, falls $p \equiv 3 \pmod 4$. Außerdem können wir durch den gleichen Trick wie in (3.2) zeigen, dass sich die verbleibenden acht Terme jeweils paarweise wie in (3.2) für den Fall $p \equiv 3 \pmod 4$ aufheben. Durch den gleichen Trick, nur auf die Summation über fünf Legendre-Symbole, fällt auch dieser Term für $p \equiv 3 \pmod 4$ weg. Wir können also zusammenfassend sagen, dass im Fall $p \equiv 3 \pmod 4$ alle Summen über drei sowie fünf Legendre-Symbole wegfallen oder sich gegenseitig aufheben. Für den Fall $p \equiv 1 \pmod 4$ sowie Summen über vier Legendre-Symbole können wir keine Aussagen über eine Vereinfachung treffen. Aufgrund dessen schätzen wir diese mit Hilfe der Weil-Schranke ab. Somit können wir für $Q_p(5)$ die folgende Abschätzung beweisen:

Satz 3.5.6.

$$| Q_p(5) - \frac{1}{32}p | < \begin{cases} \frac{39}{32}\sqrt{p} + \frac{139}{32} & \textit{für } p \equiv 1 \pmod 4 \\ \frac{15}{32}\sqrt{p} + \frac{139}{32} & \textit{für } p \equiv 3 \pmod 4. \end{cases}$$

Auch für $Q_p(5)$ wollen wir unsere Abschätzung mit der von Conrad vergleichen, indem wir die größte Primzahl p berechnen, für die gilt $Q_p(5) = 0$. Nach Conrads Abschätzung erhalten wir: $p = 16.543,61$, so dass für alle $p > 16.529$ gilt $Q_p(5) \geq 1$. Für unsere Abschätzungen ergeben sich jedoch in beiden Fällen deutlich bessere Ergebnisse:

(i) für $p \equiv 1 \pmod 4$ folgt: $p < 1.788,20$.
(ii) für $p \equiv 3 \pmod 4$ folgt: $p < 461,01$.

Daraus folgern wir, dass für Primzahlen $p \equiv 1 \pmod 4$ gilt, dass $Q_p(5) \geq 1$ für $p > 1787$. Für $p \equiv 3 \pmod 4$ erhalten wir mit unserer Abschätzung, dass für Primzahlen $p > 461$ gilt $Q_p(5) \geq 1$. Ein gewisses Potential zur Verbesserung lässt sich auch hier erkennen, da bereits in unserem Beispiel 3.3.2 für $p = 43$ ein 5-Tupel zu erkennen ist.

3.6 Verteilung von isolierten Tupeln

Betrachtet man das Beispiel 3.3.2 für $p = 43$ erneut, fällt auf, dass drei der Tripel aufeinanderfolgender quadratischer Reste aus einem 5-Tupel aufeinanderfolgender

quadratischer Reste resultieren. Infolgedessen wollen wir im folgenden Abschnitt die Anzahl von "echten" d-Tupeln untersuchen. Diese Idee hat bereits Jacobsthal in [Jac06] näher betrachtet. Wir nennen diese Art von Tupeln **isolierte Tupel** und werden in diesem Abschnitt Jacobsthals Gedanken aufgreifen und numerische Berechnungen für isolierte Tupel anstellen.

Definition 3.6.1. Wir wählen die Notation $\bar{Q}_p(d)$ für die Anzahl von isolierten d-Tupeln aufeinanderfolgender quadratischer Reste modulo p. Für die aufeinanderfolgenden Elemente $e_1, \ldots, e_d$ in einem isolierten d-Tupel quadratischer Reste modulo p gilt somit:

$$\left(\frac{e_1}{p}\right) = \left(\frac{e_2}{p}\right) = \cdots = \left(\frac{e_d}{p}\right) = 1.$$

Für die angrenzenden Elemente $e_1 - 1$ sowie $e_d + 1$ gilt:

$$\left(\frac{e_1 - 1}{p}\right) = \left(\frac{e_d + 1}{p}\right) = -1.$$

Um Aussagen über die Anzahl von isolierten d-Tupeln quadratischer Reste zu treffen, müssen wir zunächst zu den allgemeinen d-Tupeln zurückkehren. Dafür betrachten wir die Anzahl $Q_p(d)$, die wir im Folgenden über die nachstehende Summe darstellen:

$$Q_p(d) = \sum_{k=d}^{\infty} (k + 1 - d)\bar{Q}_p(k).$$

Dass diese Summation wirklich $Q_p(d)$ ergibt, scheint auf den ersten Blick nicht direkt ersichtlich. Dennoch können wir erläutern, warum $Q_p(d)$ genau das Ergebnis dieser Summation ist. Betrachten wir den ersten Term $k = d$ folgt daraus, dass wir die Anzahl von isolierten d-Tupeln mit dem Faktor 1 addieren, für $k = d+1$ addieren wir die Anzahl von isolierten $(d+1)$-Tupeln mit dem Faktor 2, für $k = d+2$ addieren wir die Anzahl von isolierten $(d + 1)$-Tupeln mit dem Faktor 3. Diese Summation führen wir immer weiter fort. Warum die beschriebene Summation $Q_p(d)$ ergibt, folgt daraus, dass in jedem isolierten d-Tupel genau ein allgemeines d-Tupel enthalten ist. Des Weiteren enthält jedes isolierte $(d + 1)$-Tupel zwei allgemeine d-Tupel und jedes $(d + 2)$-Tupel enthält drei allgemeine d-Tupel. Diese Schema führen wir immer weiter fort und erhalten schließlich $Q_p(d)$. Für eine anschauliche Darstellung dieses Schemas verweisen wir an dieser Stelle erneut auf das Beispiel 3.3.2 für $p = 43$ und $d = 3$.

Wir können $Q_p(d+1)$ als $Q_p(d+1) = \sum_{k=1}^{\infty} k \cdot \bar{Q}_p(d+k)$ schreiben. Danach subtrahieren wir diesen Ausdruck auf der linken und rechten Seite unserer oberen Summation und erhalten:

$$Q_p(d) - Q_p(d + 1) = \sum_{k=d}^{\infty} \bar{Q}_p(k). \tag{3.3}$$

Die rechte Seite enthält nun also nur noch die Summation über alle $\bar{Q}_p(k)$ mit $k \geq d$. Des Weiteren können wir $Q_p(d+2)$ schreiben als:

$$Q_p(d+2) = \sum_{k=1}^{\infty} k \cdot \bar{Q}_p(d+1+k).$$

Subtrahieren wir nun $Q_p(d+1)$ ein weiteres Mal auf beiden Seiten der Gleichung (3.3) und addieren $Q_p(d+2)$ auf beiden Seiten heben sich auf der rechten Seite alle $\bar{Q}_p(k+i)$ für $i \geq 1$ auf und wir erhalten:

$$\bar{Q}_p(k) = Q_p(k) - 2Q_p(k+1) + Q_p(k+2).$$

Möchten wir nun eine Abschätzung für die Anzahl von isolierten d-Tupeln quadratischer Reste modulo p finden, so können wir die bereits gezeigten Abschätzungen der drei Terme auf der rechten Seite nutzen, so dass daraus folgt:

$$\begin{aligned} \bar{Q}_p(k) &= \frac{1}{2^k}p - \frac{2}{2^{k+1}}p + \frac{1}{2^{k+2}}p + \mathcal{O}(\sqrt{p}) \\ &= \frac{1}{4} \cdot \frac{1}{2^k}p + \mathcal{O}(\sqrt{p}) \\ &= \frac{1}{4}Q_p(k) + \mathcal{O}(\sqrt{p}). \end{aligned}$$

Wir können also erkennen, dass es sich bei ungefähr einem Viertel aller d-Tupel quadratischer Reste um isolierte d-Tupel handelt.

Chapter 4

Quadratische Reste und Methoden des Machine Learnings

Im letzten Kapitel dieser Bachelorarbeit möchten wir Methoden des Machine Learnings anwenden, um Aussagen über die Verteilung von quadratischen Resten zu bestimmen. Es gibt unendlich viele Primzahlen, sodass uns unendlich viele Datensätze zum Trainieren von neuronalen Netzen oder anderen Methoden des Machine Learnings zur Verfügung stehen. Bisher konnten wir keine Quellen finden, in denen ähnliche Ansätze verfolgt wurden. Aufgrund dessen haben wir uns eigenständig für mögliche Anwendungsgebiete entschieden, ohne zu wissen, ob unsere Arbeit zu einem Erfolg führen kann. Wir möchten mit Hilfe von verschiedenen Methoden des Machine Learnings neue und bisher unbekannte Eigenschaften bezüglich der Verteilung von quadratischen Resten finden. Dazu gehören beispielsweise bestimmte Muster, die wir durch das Trainieren von neuronalen Netzen erkennen können, wie etwa Zusammenhänge zwischen quadratischen Resten modulo p und der Kongruenzklasse von p.
Während unserer Literaturrecherche fanden wir die Arbeit [Hil], die sich mit dem "Quadratic Residue Random Walk" auseinandergesetzt hat.

Definition 4.0.1 (Gauß'sche Summe modulo p)**.** $G(p)$ kann über die folgenden zwei Formulierungen dargestellt werden:

(i) $G(p) = \sum_{t=1}^{p} e^{2\pi i t^2/p}$.

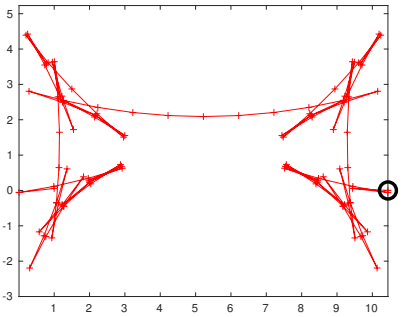
(ii) $G(p) = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) e^{2\pi i t/p}$.

(Man kann zeigen, dass diese beiden Ausdrücke gleich sind.)

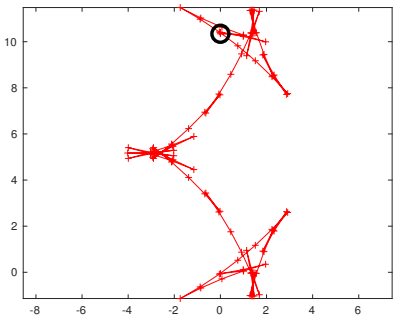
Tragen wir von jeder Teilsumme der Darstellung von Definition 4.0.1(ii) den Ima-

ginärteil gegenüber dem Realteil auf, erhalten wir folgende beispielhafte Grafiken für verschiedene ungerade Primzahlen p:

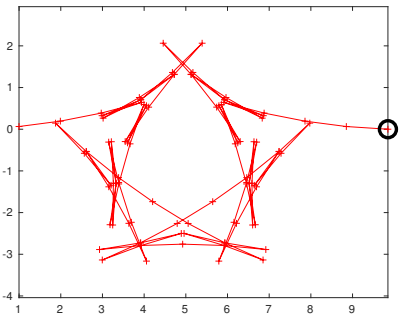
Grafik 4.0.2.



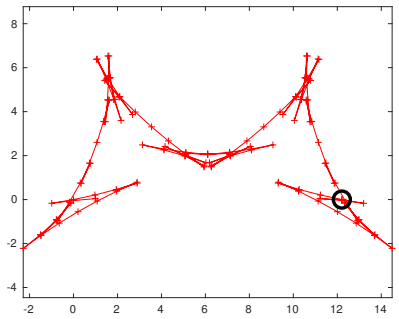
(i) $p = 109$



(ii) $p = 107$



(iii) $p = 97$



(iv) $p = 149$

Betrachten wir diese Grafiken in Bezug auf die Kongruenzklassen der Primzahlen, so fällt auf, dass die Entwicklung der einzelnen Teilsummen für $p \equiv 1 \pmod 4$ entlang der reellen Achse verläuft sowie für $p \equiv 3 \pmod 4$ entlang der Achse des Imaginärteils. Für diese Eigenschaft unseres "Quadratic Residue Random Walk" können wir eine mathematische Begründung herleiten. Dazu betrachten wir die Definition 4.0.1(ii):

$$G(p) = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) e^{2\pi i t/p}.$$

Wie in 3.5(ii) können wir die Summe in 4.0.1(ii) in zwei Summen unterteilen:

$$G(p) = \sum_{t=1}^{(p-1)/2} \left(\frac{t}{p}\right) e^{2\pi i t/p} + \left(\frac{-1}{p}\right) \sum_{t=1}^{(p-1)/2} \left(\frac{t}{p}\right) e^{-2\pi i t/p}. \tag{4.1}$$

In dieser Aufteilung entspricht die erste Summe den Indizes t für $t = 1, \ldots, \frac{p-1}{2}$ der ursprünglichen Summe. Die zweite Summe entspricht den Indizes t für $t =$

$\frac{p-1}{2}+1,\ldots,p-1$ der ursprünglichen Summe. Des Weiteren fällt auf, dass es sich bei beiden Summen um den jeweiligen konjugiert komplexen Ausdruck handelt. Für $p \equiv 1 \pmod 4$ gilt nach Lemma 2.1.8: $\left(\frac{-1}{p}\right) = 1$, sodass die beiden Summen in (4.1) addiert werden. Betrachten wir an dieser Stelle die Darstellung der komplexen Zahlen als Summe von Real- und Imaginärteil $a+ib$, so besitzt die dazu komplex konjugierte Zahl die Darstellung $a-ib$. Dadurch heben sich die Imaginärteile der beiden Summen in (4.1) gegenseitig auf. Infolgedessen entwickelt sich der "Quadratic Residue Random Walk" für den Fall $p \equiv 1 \pmod 4$ in der ersten Hälfte für $t = 1,\ldots,\frac{p-1}{2}$ sowohl in Richtung der Realteilachse als auch in Richtung der Achse des Imaginärteils, jedoch werden für jedes t der zweiten Hälfte ($t = \frac{p-1}{2}+1,\ldots,p-1$) die Imaginärteile der ersten Hälfte wieder subtrahiert und die Realteile addiert, sodass sich der Random Walk entlang der Achse des Realteils entwickelt.
Analog dazu gilt für $p \equiv 3 \pmod 4$ nach 2.1.8: $\left(\frac{-1}{p}\right) = -1$, sodass sich in diesem Fall die Realteile der beiden Summen in (4.1) aufheben und sich der Random Walk entlang imaginären Achse bewegt.
Wir können außerdem auf einen Zusammenhang zwischen der Kongruenzklasse der Primzahlen modulo 4 und dem jeweiligen Endpunkt des "Quadratic Residue Random Walk" schließen. Der Endpunkt unseres Random Walks stellt nach 4.0.1(ii) den Wert von $G(p)$ dar. Durch unsere Betrachtung der Ausbreitung des Random Walks haben wir gezeigt: der Wert von $G(p)$ ist für $p \equiv 1 \pmod 4$ rein reell, da sich alle Imaginärteile der Summanden gegenseitig aufheben. Dementsprechend ist $G(p)$ für $p \equiv 3 \pmod 4$ rein imaginär. Aufgrund dieser Feststellung reicht es im Folgenden nur den Betrag von $G(p)$ zu betrachten, um den Endpunkt des Random Walks (bis auf sein Vorzeichen) zu bestimmen.

$$\begin{aligned} \mid G(p) \mid = G(p)\overline{G(p)} &= \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)e^{2\pi ia/p}\cdot\sum_{b=1}^{p-1}\left(\frac{b}{p}\right)e^{-2\pi ib/p} \\ &= \sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\left(\frac{ab}{p}\right)e^{2\pi ia/p}e^{-2\pi ib/p}. \end{aligned}$$

Da $a \not\equiv 0 \pmod p$, können wir c mit $c \equiv -a^{-1}b \pmod p$ ($b \equiv -ac \pmod p$) finden, sodass $-ac$ genau wie a das vollständige Restsystem modulo p durchläuft. Auf die dadurch veränderte Reihenfolge der Summanden muss aufgrund der Kommutativität keine Rücksicht genommen werden. Aufgrund dessen können wir das b in $G(p)$ durch das von uns definierte $-ac$ ersetzen und erhalten:

$$\mid G(p) \mid = \sum_{c=1}^{p-1}\sum_{a=1}^{p-1}\left(\frac{-aac}{p}\right)e^{2\pi ia/p}e^{2\pi iac/p}.$$

Da $\left(\frac{-aac}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right)\left(\frac{-c}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{c}{p}\right)$ gilt, können wir durch die Eigenschaften der

Exponential-Funktion $\mid G(p) \mid$ schreiben als:

$$\mid G(p) \mid = \left(\frac{-1}{p}\right) \sum_{c=1}^{p-1} \sum_{a=1}^{p-1} \left(\frac{c}{p}\right) e^{2\pi i a(1+c)/p}.$$

Im Folgenden vertauschen wir die Reihenfolge der Summation von c und a und trennen unsere Summen, sodass wir den Summanden für $c = p-1$ separat betrachten können:

$$\begin{aligned} \mid G(p) \mid &= \left(\frac{-1}{p}\right) \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \sum_{a=1}^{p-1} e^{2\pi i a(1+c)/p} \\ &= \left(\frac{-1}{p}\right) \left(\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) \sum_{a=1}^{p-1} e^{2\pi i (a+ac)/p} + \left(\frac{p-1}{p}\right) \sum_{a=1}^{p-1} e^{2\pi i a(1+(p-1))/p} \right) \\ &= \left(\frac{-1}{p}\right) \left(\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) \sum_{a=1}^{p-1} e^{2\pi i (a+ac)/p} + \left(\frac{p-1}{p}\right) \sum_{a=1}^{p-1} e^{2\pi i a} \right) \end{aligned}$$

Man kann zeigen, dass $\sum_{a=1}^{p-1} e^{2\pi i(a+ac)/p} = -1$ für alle $c \in 1, \ldots, p-2$, sodass wir -1 als Konstante vor $\sum_{c=1}^{p-2} \left(\frac{c}{p}\right)$ ziehen können. Außerdem gilt $\sum_{a=1}^{p-1} e^{2\pi i a} = p-1$, da $e^{2\pi i k} = 1$ für alle $k \in \mathbb{Z}$. Diese beiden Schritte zur Vereinfachung besitzen eine gewisse Analogie zur Aussage von Lemma 3.1.1. Wir können $\mid G(p) \mid$ nun wie folgt schreiben:

$$\mid G(p) \mid = \left(\frac{-1}{p}\right) \left(-\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right)(p-1) \right).$$

Durch Ausmultiplizieren und mit Lemma 2.1.6(iii) folgt:

$$\begin{aligned} \mid G(p) \mid &= (1 + p - 1) \\ &= p. \end{aligned}$$

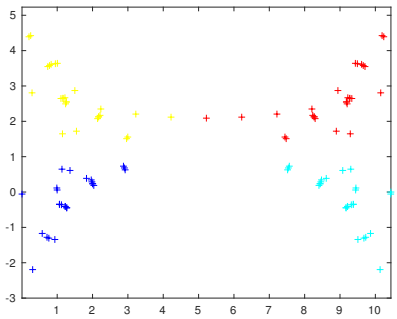
Zusammen mit unserer Betrachtung bezüglich der Entwicklung unseres Random Walks entlang der imaginären beziehungsweise reellen Achse können wir folgern:

$$G(p) = \begin{cases} \pm\sqrt{p} & \text{für } p \equiv 1 \pmod 4 \\ \pm i\sqrt{p} & \text{für } p \equiv 3 \pmod 4. \end{cases}$$

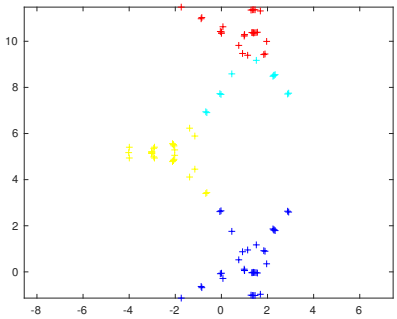
Die Entscheidung über das Vorzeichen beider Ausdrücke lässt sich nur mit großem Aufwand zeigen und soll nicht Teil dieser Arbeit sein. In seinem Tagebuch schrieb Gauss 1805, dass es über vier Jahre dauerte die Vorzeichen der beiden Fälle zu bestimmen. Es handelt sich bei beiden Vorzeichen um +. Zur Verdeutlichung haben wir den Endpunkt unseres Random Walks in den Plots von Grafik 4.0.2 mit einem

Kreis markiert.
Anhand der grafischen Darstellungen von 4.0.1(ii) in Grafik 4.0.2 wir versucht, mit Hilfe einer Methode des Machine Learnings (k-Means) eine Cluster-Analyse durchzuführen, um durch die Zuordnung der Werte zu den verschiedenen Klassen auf einen Zusammenhang zwischen zugeordneten Klassen und den verschiedenen Werten der Legendre-Symbole zu schließen. In Skript 6.2.9 haben wir MATLAB-Skripte implementiert, die eine solche Cluster-Analyse durchführen. Die Ergebnisse haben wir an dieser Stelle aufgeführt:

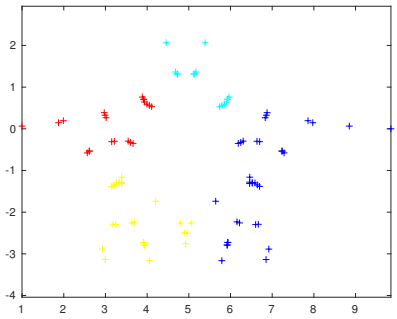
Grafik 4.0.3.



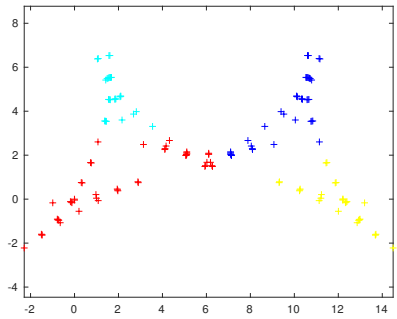
(i) $p = 109$



(ii) $p = 107$



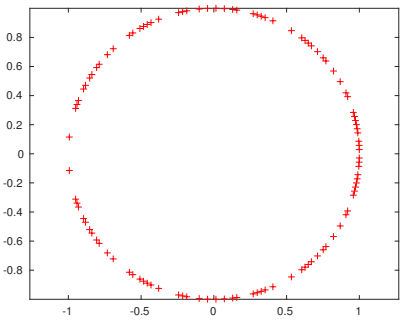
(iii) $p = 97$



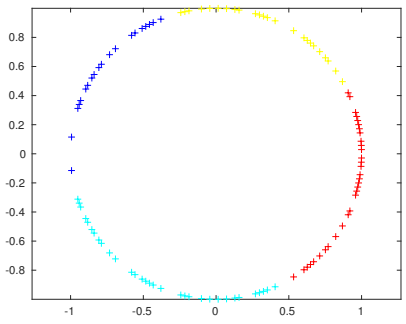
(iv) $p = 149$

Wir können am Beispiel dieser beiden Cluster-Analysen erkennen, dass die Zuordnungen zu den verschiedenen Klassen auf triviale Weise entstehen und anhand von den Abständen der Werte bestimmt werden. Wir können somit keine Rückschlüsse auf Abhängigkeiten zwischen Kongruenzklassen der Primzahlen und zugeordneten Klassen der Werte ziehen. Des Weiteren lassen sich auch keine weiteren Muster in der Zuordnung erkennen. Dieses Ergebnis können wir damit begründen, dass die mit Hilfe von 4.0.1(ii) bestimmten Werte über eine Summe definiert werden. Aufgrund dessen besteht zwischen jedem Wert sowie allen seinen Vorgängern eine Korrelation. Diese Abhängigkeit erkennen wir auch in unseren Grafiken wieder. Dementsprechend werden aufeinanderfolgende Werte, die einen ausreichend kleinen Abstand besitzen, der gleichen Klasse zugeordnet. Um diese Abhängigkeit der Werte zu vermeiden, haben wir die Summe in der Definition 4.0.1(ii) entfernt und alle Werte mit Hilfe von Skript 6.2.10 vom Nullpunkt aus dargestellt sowie die entsprechende Cluster-Analyse durchgeführt:

Grafik 4.0.4.



(i) $p = 109$



(ii) $p = 109$

Da alle Werte die Länge 1 besitzen, liegen sie alle auf dem Einheitskreis. Wir können erkennen, dass der Einheitskreis ohne sichtliche Häufungspunkte dargestellt wird. Dementsprechend können wir anhand dieser Darstellung ebenfalls darauf schließen, dass die quadratischen Reste gleichmäßig verteilt erscheinen.
Nachdem unsere erste Idee von einer möglichen Cluster-Analyse nicht die von uns erhofften Ergebnisse lieferte, wollen wir versuchen, ähnlich zu den Fallunterscheidungen in den Ergänzungssätzen des Quadratischen Reziprozitätsgesetzes 2.1.8, eigene Fallunterscheidungen für $\left(\frac{3}{p}\right)$ zu finden. Wir erhoffen uns, dass ein neuronales Netz mit einer ausreichenden Anzahl von Trainingsdatensätzen die Zusammenhänge zwischen den Primzahlen p und den entsprechenden Werten von $\left(\frac{3}{p}\right)$ erkennt und wir anhand der erlernten Muster eine ähnliche Fallunterscheidung aufstellen können. Die Implementierung eines solchen trainierten neuronalen Netzes in MATLAB findet der Leser in Skript 6.2.11. Unsere Trainingsdaten bestehen aus ungefähr 45.000 Primzahlen p und den Werten $\left(\frac{3}{p}\right)$. Zudem kann die Anzahl unserer Trainingssamples (unter der Gefahr des Übertrainierens) beliebig erhöht werden. Nach der Generierung unseres Datensatzes fiel uns erneut die Gleichverteilung der quadratischen Reste ins Auge, da die Zuordnung von $[3]_p$ zu den quadratischen Resten beziehungsweise den quadratischen Nichtresten bei jeweils 50% lag. Dadurch unterteilt sich unser Datensatz in zwei Hälften mit $[3]_p$ als quadratischen Rest und $[3]_p$ als quadratischen Nichtrest sowie den entsprechenden Primzahlen p. Nach den ersten Trainingsdurchläufen erhielten wir stets Fehlerwahrscheinlichkeiten von ungefähr 50%, auch mehrfaches Anpassen der Eigenschaften des neuronalen Netzes brachte uns keine Verbesserung der Fehlerwahrscheinlichkeit. Dieses Resultat ist überaus unbefriedigend, da wir aufgrund der gleichmäßigen Verteilung von $[3]_p$ als quadratischen Rest beziehungsweise quadratischen Nichtrest die gleiche Fehlerwahrscheinlichkeit erhalten, wenn wir eine Münze werfen würden. Gründe für die schlechten Resultate und die daraus fehlende Eigenschaft des neuronalen

Netzes, Kongruenzen zu erlernen, können darin liegen, dass die Daten aufgrund der erwähnten Gleichverteilung zu wenig Informationen enthalten. Ebenfalls wird dieser geringe Informationsgehalt durch die Eindimensionalität der Eingabedaten unterstützt. Das neuronale Netz erlernt dementsprechend, dass es sich um eine 50/50-Entscheidung handelt und sagt bei jeder Entscheidung konstant den gleichen Wert voraus. Um weitere Gründe für das Versagen des neuronalen Netz zu finden, haben wir versucht, einem weiteren neuronalen Netz mit Hilfe von Skript 6.2.12 die Kongruenz modulo 2 beizubringen. Diese einfache Unterscheidung zwischen geraden und ungeraden Zahlen beziehungsweise das zugrunde liegende Rechnen mit Kongruenzen bilden die Grundlage für unsere vorherigen Ziele für das Trainieren von neuronalen Netzen. Jedoch zeigt auch dieser Versuch ganz deutlich eine Schwäche der neuronalen Netze auf. Die Muster sind zu sehr gleich verteilt, als dass das neuronale Netz eine eindeutige Entscheidung treffen könnte, und deshalb sagt es stets den gleichen Wert voraus.
Um dennoch unser Ziel bezüglich der Bestimmung von $\left(\frac{3}{p}\right)$ anhand der Kongruenzklasse von p herzuleiten, möchten wir den Trainingsvorgang, den das neuronale Netz nicht im Stande war zu erlernen, per Hand implementieren. Für diesen Ansatz nutzen wir das Quadratische Reziprozitätsgesetz 2.1.7 sowie den Chinesischen Restsatz.

Satz 4.0.5 (Chinesischer Restsatz)**.**

$$X \equiv c_1 \pmod{m_1}, \ldots, X \equiv c_k \pmod{m_k}$$

Seien $m_1, \ldots, m_k \geq 2$ paarweise teilerfremd, sei m ihr kleinstes gemeinsames Vielfaches, sind $c_1, \ldots, c_k \in \mathbb{Z}$ beliebig, dann hat das oben stehende System modulo m genau eine Lösung.

Beweis. Siehe Satz 2.2.2 in [Bun08]. □

Da es bereits entsprechende Fallunterscheidungen für $\left(\frac{3}{p}\right)$ sowie $\left(\frac{5}{p}\right)$ gibt, haben wir unser Ziel auf Fallunterscheidungen für $\left(\frac{7}{p}\right)$,$\left(\frac{11}{p}\right)$, $\left(\frac{13}{p}\right)$ sowie $\left(\frac{17}{p}\right)$ für ungerade Primzahlen p erweitert. Mit Hilfe des quadratischen Reziprozitätsgesetzes 2.1.7 können wir $\left(\frac{q}{p}\right)$ schreiben als:
(i) Falls $p \equiv 1 \pmod 4$ oder $q \equiv 1 \pmod 4$, gilt:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{p \pmod q}{p}\right).$$

(ii) Falls $p \equiv 3 \pmod 4$ und $q \equiv 3 \pmod 4$, gilt:

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = \left(\frac{-p \pmod q}{p}\right).$$

Aufgrund dessen erhalten wir für $q = 7$, da $7 \equiv 3 \pmod 4$:

$$\left(\frac{7}{p}\right) = \begin{cases} \left(\frac{p \pmod 7}{7}\right) & \text{falls } p \equiv 1 \pmod 4 \\ \left(\frac{-p \pmod 7}{7}\right) & \text{falls } p \equiv 3 \pmod 4. \end{cases}$$

Die quadratischen Reste modulo 7 lauten: $[1]_7, [2]_7, [4]_7$. Somit müssen wir die beiden folgenden Kongruenzen modulo 4 und modulo 7 lösen:

$$\begin{cases} p \equiv 1, 2, 4 \pmod 7 \\ p \equiv 1 \pmod 4 \end{cases}$$

oder

$$\begin{cases} p \equiv 3, 5, 6 \pmod 7 \\ p \equiv 3 \pmod 4. \end{cases}$$

Da die beiden Moduln 4 und 7 teilerfremd sind, können wir den Chinesischen Restsatz 4.0.5 anwenden und erhalten eine Lösung, die eindeutig modulo 28 ist. Nach dem Lösen des Kongruenzsystems erhalten wir die folgende Fallunterscheidung zur Bestimmung von $\left(\frac{7}{p}\right)$:

Satz 4.0.6.

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \textit{falls } p \equiv 1, 3, 9, 19, 25, 27 \pmod{28} \\ 0 & \textit{falls } p = 7 \\ -1 & \textit{sonst} \end{cases}$$

Für $p = 11$ erhalten wir dementsprechend eine Fallunterscheidung bezüglich der Kongruenz modulo 44. Im Fall $q = 13$ sowie $q = 17$ können wir $\left(\frac{q}{p}\right)$ mit Hilfe einer Fallunterscheidung modulo 13 beziehungsweise modulo 17 bestimmen, da $13, 17 \equiv 1 \pmod 4$. Allgemein können wir folgern, dass wir eine Fallunterscheidung modulo $4q$ für $q \equiv 3 \pmod 4$ sowie eine Fallunterscheidung modulo q für $q \equiv 1 \pmod 4$ erhalten.

Satz 4.0.7.

$$\left(\frac{11}{p}\right) = \begin{cases} 1 & \textit{falls } p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44} \\ 0 & \textit{falls } p = 11 \\ -1 & \textit{sonst} \end{cases}$$

$$\left(\frac{13}{p}\right) = \begin{cases} 1 & \textit{falls } p \equiv 1, 3, 4, 9, 10, 12 \pmod{13} \\ 0 & \textit{falls } p = 13 \\ -1 & \textit{sonst} \end{cases}$$

$$\left(\frac{17}{p}\right) = \begin{cases} 1 & \textit{falls } p \equiv 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17} \\ 0 & \textit{falls } p = 17 \\ -1 & \textit{sonst} \end{cases}$$

Chapter 5

Zusammenfassung

In dieser Bachelorarbeit haben wir explizite Formeln zur Berechnung der Anzahl von Paaren sowie Tripeln aufeinanderfolgender quadratischer Reste beziehungsweise Nichtreste formuliert. Für 4-Tupel sowie 5-Tupel konnten wir Abschätzungen aufstellen und ihren Fehlerterm im Vergleich zu den bisher in der Literatur verfügbaren Abschätzungen deutlich reduzieren. Des Weiteren haben wir numerische Berechnungen durchgeführt, um die Zuverlässigkeit von Abschätzungen zu verifizieren. Infolgedessen haben wir uns ebenfalls mit einer effizienten Programmierung von Zähl-Funktionen zur Bestimmung von allgemeinen d-Tupeln quadratischer Reste und quadratischer Nichtreste beschäftigt. Die Implementierung dieser Funktionen haben wir in PARI/GP sowie in MATLAB umgesetzt. Die Umsetzung in MATLAB geschah mit dem Hintergedanken, mit Hilfe dieser Funktionen Datensätze zu generieren, die wir benutzen können, um neuronale Netze sowie weitere Methoden des Machine Learnings zu trainieren. Wir haben uns erhofft, dass wir durch das Trainieren von neuronalen Netzen mit einer ausreichenden Anzahl an Trainingsdatensätzen Muster in den Datensätzen finden können und mit diesen Erkenntnissen allgemeine Aussagen über die Verteilung von quadratischen Resten treffen können. Allerdings gestaltete sich die Anwendung von Methoden des Machine Learnings als schwierig und die Ergebnisse lieferten keine neuen Erkenntnisse. Wir konnten dennoch unsere anvisierten Ziele erreichen, indem wir das Training, das eigentlich dem neuronalen Netz dienen sollte, um Kongruenzen zu erkennen, per Hand implementiert haben.
Der erwähnte Punkt bezüglich des Scheiterns der Methoden des Machine Learnings liefert allerdings auch einige offene Fragestellung zu den quadratischen Resten und ihrer Verteilung. In diesem Bereich gibt es noch viele Themen, die bei näherer Betrachtung interessante Folgerungen zulassen. Vorstellbare Ausweitungen des Themengebiets könnten eine Betrachtung der quadratischen Reste von einem stochastischen Standpunkt sein. Dazu könnte man die Eigenschaft der quadratischen Reste, inwiefern quadratische Reste wirklich zufällig verteilt sind, weiter ausführen. Gerade in diesem Punkt der zufälligen Verteilung könnte auch ein weiterer Durchbruch im Machine Learning einige neue Erkenntnisse bringen. Allerdings ist es momen-

tan nicht zu empfehlen Methoden des Machine Learnings auf die Verteilung von quadratischen Resten anzuwenden, da es mit den heutigen Methoden nicht möglich ist, neuronalen Netzen den Kongruenz-Begriff anzutrainieren. Sobald künstlichen Intelligenzen diese Fähigkeit antrainiert werden kann, sollte einer Anwendung von Methoden des Machine Learnings zu den in dieser Arbeit behandelten Themen nichts mehr im Weg stehen.

Chapter 6

Anhang

6.1 Code in PARI/GP

Funktion 6.1.1. Funktion zur Erstellung eines Datensatzes von Primzahlen

```
generate_primes(p1,p2,name)={
    p=vector(p2-p1);
    counter=1;
    for(i=p1,p2-1,
        p[counter]=prime(i);
        counter+=1;
    );
    write(name,p);
}
```

Skript 6.1.2. Skript zur Erstellung unseres Datensatzes

```
generate_primes(2,100,"primes1.txt");
generate_primes(500,1000,"primes2.txt");
generate_primes(10000,15000,"primes3.txt");
generate_primes(20000,25000,"primes4.txt");
generate_primes(50000,55000,"primes5.txt");
```

Funktion 6.1.3. Funktion zur Berechnung der Legendre-Symbole von $\left(\frac{1}{p}\right)$ bis $\left(\frac{p-1}{p}\right)$ unter Verwendung von Folgerung 2.1.9

```
legendre_fast(p)={
    y=vector(p-1);

    if(p%4==1,
        for(i=1,(p-1)/2,
            y[i]=kronecker(i,p);
            y[p-i]=y[i];
```

```
        );,
        for(i=1,(p-1)/2,
            y[i]=kronecker(i,p);
            y[p-i]=-y[i];
        );
    );
    return(y);
};
```

Funktion 6.1.4. Funktion zur Berechnung von $Q_p(d)$

```
d_tupel_r(p,d)={
  x=legendre_fast(p);

  y1=matrix(p-1,d);
  bool=1;
  counter=0;

  for(j=1,p-d,
    for(k=1,d,
      if(x[j+k-1]==-1,bool=0)
     );
     if(bool==1,
        for(l=1,d,y1[j,l]=j+l-1);counter=counter+1);
     bool=1;
  );

  /* ausgabe generieren */
  c=0;
  y2=matrix(counter,d);
  for(i=1,p-1,if(y1[i,1]!=0,
    c=c+1;
    for(j=1,d,y2[c,j]=y1[i,j]);
    )
  );
  return(counter);
}
```

Funktion 6.1.5. Funktion zur Berechnung von $\bar{Q}_p(d)$

```
iso_d_tupel_r(p,d)={
  x=legendre_fast(p);
  x=concat(-1,x);

  y1=matrix(p-1,d);
```

```
  bool=1;
  counter=0;

  for(j=1,p-d,
    for(k=1,d,
      if(x[j+k]==-1,bool=0)
    );
    if(bool==1
       && x[j]==-1
       && if(j+d+1<p-1,x[j+d+1]==-1,0),
        for(l=1,d,y1[j,l]=j+l-1);counter=counter+1
    );
    bool=1;
  );
  return(counter);
}
```

Funktion 6.1.6. Funktion zur Berechnung der Jacobsthalschen Summe $T_p(t)$

```
jacobsthal(p,t)={
    if(p%4==3,
        return(0),
        return(sum(c=1,p-1,kronecker(c*(c^2-t),p))));
}
```

6.2 Code in MATLAB

Funktion 6.2.1. Funktion zur Bestimmung des Jacobi-Symbols $\left(\frac{c}{d}\right)$

```
function j=jacobi(c,d)

    if mod(d,2)==0
        error('d soll ungerade sein');
    end
    s=1;

    if(c<0)
        c=abs(c);
        s=(-1)^((d-1)/2);
    end

    while(~(c==1 || c==0))
        r=mod(c,d);
        c=r;
```

```
        if(mod(c,2)==0 && c>1)
            [u,t]=hilfsfunktion(c);
            c=u;
            s=(((-1)^((d^2-1)/8))^t)*s;
        end

        if(c>1)
            s=(-1)^((c-1)*(d-1)/4)*s;
            dummy=c;
            c=d;
            d=dummy;
        end
    end

    if(c==0)
        s=0;
    end

    j=s;

    function [u,t]=hilfsfunktion(c)
        t=0;
        u=c;
        while(mod(c,2)==0)
            c=c/2;
            t=t+1;
            u=u/2;
        end
    end
end
```

Funktion 6.2.2. Funktion zur Berechnung der Legendre-Symbole von $\left(\frac{1}{p}\right)$ bis $\left(\frac{p-1}{p}\right)$ unter Verwendung von Folgerung 2.1.9

```
function y=legendre_fast(p)

    y=zeros(p-1,1);

    if mod(p,4)==1
       for i=1:(p-1)/2
          y(i)=jacobi(i,p);
          y(p-i)=y(i);
       end
```

```
    else
        for i=1:(p-1)/2
            y(i)=jacobi(i,p);
            y(p-i)=-y(i);
        end
    end
end
```

Skript 6.2.3. Skript zur Erstellung unseres Datensatzes

```
clc; clear all; close all;
p1=load('primes1.txt');
p2=load('primes2.txt');
p3=load('primes3.txt');
p4=load('primes4.txt');
p5=load('primes5.txt');
% zur verringerung der daten
p3=p3(1:1000);
p4=p4(1:500);
p5=p5(1:250);

data1=cell(numel(p1),2);
data2=cell(numel(p2),2);
data3=cell(numel(p3),2);
data4=cell(numel(p4),2);
data5=cell(numel(p5),2);

for i=1:numel(data1(:,1))
    data1{i,1}=p1(i);
    data1{i,2}=legendre_fast(p1(i));
end
save('data1.mat','data1');

for i=1:numel(data2(:,1))
    data2{i,1}=p2(i);
    data2{i,2}=legendre_fast(p2(i));
end
save('data2.mat','data2');

for i=1:numel(data3(:,1))
    data3{i,1}=p3(i);
    data3{i,2}=legendre_fast(p3(i));
end
save('data3.mat','data3');
```

```
for i=1:numel(data4(:,1))
    data4{i,1}=p4(i);
    data4{i,2}=legendre_fast(p4(i));
end
save('data4.mat','data4');

for i=1:numel(data5(:,1))
    data5{i,1}=p5(i);
    data5{i,2}=legendre_fast(p5(i));
end
save('data5.mat','data5');
```

Funktion 6.2.4. Funktion zur Berechnung von $Q_p(d)$

```
function q=d_tupel_r(p,d)

    pattern=ones(d,1);
    y=legendre_fast(p);

    q=numel(strfind(y',pattern'));
end
```

Funktion 6.2.5. Funktion zur Berechnung von $\bar{Q}_p(d)$

```
function [q,q_iso]=iso_d_tupel_r(p,d)

    pattern=[-1;ones(d,1);-1];
    y=legendre_fast(p);

    q=numel(strfind(y',ones(d,1)'));
    q_iso=numel(strfind(y',pattern'));

    bool1=isequal(y(1:d),ones(d,1)) && y(d+1)==-1;
    if bool1
        q_iso=q_iso+1;
    end
    bool2=isequal(y(end-d+1:end),ones(d,1)) && y(end-d)==-1;
    if bool2
        q_iso=q_iso+1;
    end
end
```

Funktion 6.2.6. Funktion zur Berechnung der Jacobsthalschen Summe $T_p(t)$

```
function y=jacobsthal(p,t)

    if mod(p,4)==3
        y=0;
    else
        y=1:p-1;
        y=y.*(y.^2-t);

        for i=1:numel(y)
            y(i)=jacobi(y(i),p);
        end
        y=sum(y);
    end
end
```

Skript 6.2.7. Skript zur Berechnung des Fehlers der Abschätzung der Jacobsthalschen Summen $T_p(t)$

```
clear all; clc; close all;

data1=load('primes1.txt');
data1=data1(randperm(numel(data1),50));
data2=load('primes2.txt');
data2=data2(randperm(numel(data2),100));
data3=load('primes3.txt');
data3=data3(randperm(numel(data3),100));
data4=load('primes4.txt');
data4=data4(randperm(numel(data4),100));
data5=load('primes5.txt');
data5=data5(randperm(numel(data5),100));

t=1;

data1=data1(mod(data1,4)==1);
res1=zeros(numel(data1),3);
res1(:,1)=data1;
res1(:,2)=2*sqrt(data1);
for i=1:numel(data1)
    res1(i,3)=jacobsthal(res1(i,1),t);
end
eval1_rel=abs(1-abs(res1(:,2)./res1(:,3)));
eval1=[max(eval1_rel),mean(eval1_rel)];

data2=data2(mod(data2,4)==1);
```

```
res2=zeros(numel(data2),3);
res2(:,1)=data2;
res2(:,2)=2*sqrt(data2);
for i=1:numel(data2)
    res2(i,3)=jacobsthal(res2(i,1),t);
end
eval2_rel=abs(1-abs(res2(:,2)./res2(:,3)));
eval2=[max(eval2_rel),mean(eval2_rel)];

data3=data3(mod(data3,4)==1);
res3=zeros(numel(data3),3);
res3(:,1)=data3;
res3(:,2)=2*sqrt(data3);
for i=1:numel(data3)
    res3(i,3)=jacobsthal(res3(i,1),t);
end
eval3_rel=abs(1-abs(res3(:,2)./res3(:,3)));
eval3=[max(eval3_rel),mean(eval3_rel)];

data4=data4(mod(data4,4)==1);
res4=zeros(numel(data4),3);
res4(:,1)=data4;
res4(:,2)=2*sqrt(data4);
for i=1:numel(data4)
    res4(i,3)=jacobsthal(res4(i,1),t);
end
eval4_rel=abs(1-abs(res4(:,2)./res4(:,3)));
eval4=[max(eval4_rel),mean(eval4_rel)];

data5=data5(mod(data5,4)==1);
res5=zeros(numel(data5),3);
res5(:,1)=data5;
res5(:,2)=2*sqrt(data5);
for i=1:numel(data5)
    res5(i,3)=jacobsthal(res5(i,1),t);
end
eval5_rel=abs(1-abs(res5(:,2)./res5(:,3)));
eval5=[max(eval5_rel),mean(eval5_rel)];

eval=[eval1;eval2;eval3;eval4;eval5];
dlmwrite('eval_jacobsthal1000.txt',eval);
```

Skript 6.2.8. Skript zur Betrachtung des Fehlers für 4-Tupel

```
clear all; clc; close all;
data1=load('primes1.txt');
data2=load('primes2.txt');
data3=load('primes3.txt');
data4=load('primes4.txt');
data5=load('primes5.txt');

rng(712);
index1=randperm(numel(data1),50);
index2=randperm(numel(data2),100);
index3=randperm(numel(data3),100);
index4=randperm(numel(data4),100);
index5=randperm(numel(data5),100);

data1_rand=data1(index1);
data2_rand=data2(index2);
data3_rand=data3(index3);
data4_rand=data4(index4);
data5_rand=data5(index5);

data=[data1_rand,data2_rand,data3_rand,data4_rand,data5_rand]';
data=data(floor(1/16*data)>=1);
res=zeros(numel(data),3);
res(:,1)=data;
res(:,2)=floor(1/16*data);

d=4;

for i=1:numel(data)
    i
    res(i,3)=d_tupel_r(data(i),d);
end
eval_abs=abs(res(:,2)-res(:,3));
eval_rel=abs(1-res(:,3)./res(:,2));

%kongruenz 1 modulo 4
eval_4_1(:,1)=eval_abs(mod(data,4)==1);
eval_4_1(:,2)=eval_rel(mod(data,4)==1);
%kongruenz 3 modulo 4
eval_4_3(:,1)=eval_abs(mod(data,4)==3);
eval_4_3(:,2)=eval_rel(mod(data,4)==3);

eval_4=[max(eval_4_1(:,1)),mean(eval_4_1(:,1)),
```

```
        max(eval_4_1(:,2)),mean(eval_4_1(:,2));
        max(eval_4_3(:,1)),mean(eval_4_3(:,1)),
        max(eval_4_3(:,2)),mean(eval_4_3(:,2))];

%kongruenz 1 modulo 8
eval_8_1(:,1)=eval_abs(mod(data,8)==1);
eval_8_1(:,2)=eval_rel(mod(data,8)==1);
%kongruenz 3 modulo 8
eval_8_3(:,1)=eval_abs(mod(data,8)==3);
eval_8_3(:,2)=eval_rel(mod(data,8)==3);
%kongruenz 5 modulo 8
eval_8_5(:,1)=eval_abs(mod(data,8)==5);
eval_8_5(:,2)=eval_rel(mod(data,8)==5);
%kongruenz 7 modulo 8
eval_8_7(:,1)=eval_abs(mod(data,8)==7);
eval_8_7(:,2)=eval_rel(mod(data,8)==7);

eval_8=[max(eval_8_1(:,1)),mean(eval_8_1(:,1)),
        max(eval_8_1(:,2)),mean(eval_8_1(:,2));
        max(eval_8_3(:,1)),mean(eval_8_3(:,1)),
        max(eval_8_3(:,2)),mean(eval_8_3(:,2));
        max(eval_8_5(:,1)),mean(eval_8_5(:,1)),
        max(eval_8_5(:,2)),mean(eval_8_5(:,2));
        max(eval_8_7(:,1)),mean(eval_8_7(:,1)),
        max(eval_8_7(:,2)),mean(eval_8_7(:,2))
       ];


format longG;
% disp(eval);
dlmwrite('eval_4_tupel_r4.txt',eval_4);
dlmwrite('eval_4_tupel_r8.txt',eval_8);
```

Skript 6.2.9. Skript zur Cluster-Analyse des Quadratic Residue Random Walk

```
close all; clear all; clc;

p=109;
x=1:p-1;
y=x;
a=0;
for k=x
    a=jacobi(k,p)*exp(2*pi*1i*k/p)+a;
    y(k)=a;
```

```
end
x1=real(y);
x2=imag(y);

figure(1);
plot(x1,x2,'r+-');
hold on
plot(x1(end),x2(end),'o','markeredgecolor','k',
     'markersize',15,'linewidth',3);
hold off
axis equal

%unsupervised learning
label=kmeans([x1',x2'],4);
k1=strfind(label',1);
k2=strfind(label',2);
k3=strfind(label',3);
k4=strfind(label',4);

figure(2);
plot(x1(k1),x2(k1),'r+'); hold on;
plot(x1(k2),x2(k2),'b+'); hold on;
plot(x1(k3),x2(k3),'y+'); hold on;
plot(x1(k4),x2(k4),'c+'); hold on;
axis equal;
```

Skript 6.2.10. Skript zur Cluster-Analyse des veränderten Quadratic Residue Random Walk

```
close all; clear all; clc;

p=109;
x=1:p-1;
y=x;
for k=x
    y(k)=jacobi(k,p)*exp(2*pi*1i*k/p);
end
x1=real(y);
x2=imag(y);

figure(1);
plot(x1,x2,'r+--');
axis equal;
```

```
%unsupervised learning
label=kmeans([x1',x2'],4);
k1=strfind(label',1);
k2=strfind(label',2);
k3=strfind(label',3);
k4=strfind(label',4);

figure(2);
plot(x1(k1),x2(k1),'r+'); hold on;
plot(x1(k2),x2(k2),'b+'); hold on;
plot(x1(k3),x2(k3),'y+'); hold on;
plot(x1(k4),x2(k4),'c+'); hold on;
axis equal;
```

Skript 6.2.11. Skript zur Implementierung und Training eines neuronalen Netzes für $\left(\frac{3}{p}\right)$

```
clear all; clc;
% generate data for binary classifaction
% legendre symbol (3/x)
p=primes(500000);
p=p(3:end);
t=arrayfun(@(x) 1/2*(1+jacobi(3,x)),p);

net=patternnet(10);
net=train(net,p,t);
view(net)
y=net(p);

% refer to binary classification
y(y>0.5)=1;
y(y<=0.5)=0;

% #errors
num_error=sum(abs(y-t));
error_ratio=num_error/numel(p);
disp(error_ratio);
```

Skript 6.2.12. Skript zur Implementierung und Training eines neuronalen Netzes zum Erlernen des Kongruenzbegriffes modulo 2

```
clear all; clc;
% generate data for binary classifaction
% modulo 2
```

```
x=1:10e5;
t=mod(x,2);

net=patternnet(10);
net=train(net,x,t);
view(net)
y=net(x);

% refer to binary classification
y(y>0.5)=1;
y(y<=0.5)=0;

% #errors
num_error=sum(abs(y-t));
error_ratio=num_error/numel(x);
disp(error_ratio);
```

Bibliography

[Bra32] Alfred Brauer. Über die Verteilung der Potenzreste. *Math. Z.*, 35:39–50, 1932.

[Bun08] Peter Bundschuh. *Einführung in die Zahlentheorie.* Berlin: Springer, 6th, revised and updated edition, 2008.

[Con] Keith Conrad. Quadratic residue patterns modulo a prime. `http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/QuadraticResiduePatterns.pdf`.

[Dav31] H. Davenport. On the distribution of quadratic residues (mod p). *J. Lond. Math. Soc.*, 6:49–54, 1931.

[Doe29] K. Doerge. Zur Verteilung der qaudratischen Reste. *Jahresber. Dtsch. Math.-Ver.*, 38:41–49, 1929.

[For15] Otto Forster. *Algorithmic number theory. (Algorithmische Zahlentheorie.).* Heidelberg: Springer Spektrum, 2nd revised and extended edition, 2015.

[Hil] M. Hildebrand, A.J. und Tip Phaovibul. The quadratic residue random walk. `https://faculty.math.illinois.edu/~hildebr/ugresearch/qrrw-fall2012report.pdf`.

[Hop30] H. Hopf. Über die Verteilung quadratischer Reste. *Math. Z.*, 32:222–231, 1930.

[Jac06] E. Jacobsthal. Anwendungen einer Formel aus der Theorie der quadratischen Reste. Berlin, 1906.

[Wei48] André Weil. On some exponential sums. *Proc. Natl. Acad. Sci. USA*, 34:204–207, 1948.

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, die Zitate ordnungsgemäß gekennzeichnet habe und keine anderen als die im Literaturverzeichnis angegebenen Quellen und Hilfsmittel benutzt wurden. Ferner habe ich vom Merkblatt über die Verwendung von Bachelor- und Abschlussarbeiten Kenntnis genommen und räume das einfache Nutzungsrecht an meiner Bachelor-Arbeit der Universität der Bundeswehr München ein.

.....

(Unterschrift)