Universität Ulm

Fakultät für Mathematik
und Wirtschaftswissenschaften

Institut für Zahlentheorie und Wahrscheinlichkeitstheorie

Ergebnisse über die Teiler der Folgen $(a^n + 1)$

Bachelorarbeit in Mathematik

vorgelegt von
Matthias Heinlein

am 17.06.2013

Betreuer:
Prof. Dr. Helmut Maier

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbständig angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.
Ich bin mir bewusst, dass eine unwahre Erklärung rechtliche Folgen haben wird.

Ulm, den 17.06.2013

(Unterschrift)

Inhaltsverzeichnis

1 Vorwort **1**

2 Einleitung und Geschichte **2**

3 Zahlentheoretische Grundlagen **4**
3.1 Elementare Teilbarkeitslehre 4
3.2 Kongruenzrechnung 5
3.3 Der Chinesische Restsatz 6
3.4 Die Eulersche Phi-Funktion 7
3.5 Die multiplikative Ordnung einer Zahl 8
3.6 Primitivwurzeln und der Index 11

4 Das Quadratische Reziprozitätsgesetz **12**
4.1 Das Kriterium von Euler und der Ergänzungssatz für 2 13
4.2 Beweis des quadratischen Reziprozitätsgesetzes mithilfe von Gauß-Summen 15
4.3 Das Lemma von Gauß und ein kombinatorischer Beweis des quadratischen Reziprozitätsgesetzes 16

5 P_a-Zahlen **18**
5.1 Teilmengenbeziehungen für verschiedene Basen 19
5.2 Kriterien zur Bestimmung von P_a-Zahlen 20
5.2.1 Notwendige Kriterien 20
5.2.2 Kriterien in Verbindung mit der Ordnung 20
5.2.3 Kriterien Potenzen betreffend 21
5.2.4 Kriterien Produkte betreffend 22
5.3 Algorithmik 24
5.3.1 Einfachste Berechnung 24
5.3.2 Siebalgorithmen 24
5.4 Vergleich mit Primzahlen 28
5.5 Lücken in den Mengen P_a 29
5.5.1 Lücken zwischen Primzahlen 29
5.5.2 Idee des Vorgehens 30
5.5.3 Unendlich viele Primzahlen mit ungerader Ordnung $\mathrm{ord}_d(a)$ 30
5.5.4 Für welche Primzahlen hat eine Zahl ungerade Ordnung? 31
5.6 Das Goldbach- und Zwillingsanalogon 33
5.6.1 Offene Vermutungen Primzahlen betreffend 33
5.6.2 Übertragung auf P_a-Zahlen 33
5.6.3 Beweis für quadratische Basen 35

6 Die Mengen Q_d und elegante Zahlen **36**
6.1 Die Mengen Q_d und ihre Größe 36
6.1.1 Charakterisierung für Primzahlen 36
6.1.2 Charakterisierung für allgemeine Zahlen 37
6.2 Elegante Zahlen 40

7 Verwandte Arbeiten und Ausblick **41**

A Funktionsweise der Woodstone-Visualisierung **42**

Literatur **43**

1 Vorwort

Die Mathematik war schon immer mein liebstes Schulfach. Eine besondere Faszination innerhalb der Mathematik bot mir bald die Zahlentheorie. Erste Berührungen damit hatte ich, als mein Lehrer uns in der fünften Klasse von der Goldbachschen Vermutung erzählte. Dass eine solch simple Aussage immer noch auf einen Beweis wartete, fand ich damals und finde es auch heute noch bemerkenswert.

Später, etwa in der achten Klasse, begann ich mit der Thematik der Teilbarkeit von Potenztermen (siehe Einleitung). Stück für Stück durfte ich das Thema weiterentwickeln und verallgemeinern. Alles passte zusammen: Meine eigenen Ideen und ersten „Forschungen“ zuhause, die Möglichkeit der Facharbeit über dieses Thema, Jugend forscht, der damit verbundene Auslandsaufenthalt mit neuen Ideen, das zweite Mal Jugend forscht, Ideen zusammen mit meinem Freund Ben Heuer und schließlich diese Bachelorarbeit.

Bei all dem kann ich nicht an Zufälle glauben. Es gibt einen, der mich durch all das hindurch geführt hat. Der mir nicht nur mein mathematisches Talent und Interesse gegeben hat, sondern auch mein Leben. Der dieses lenkt und führt, der mein Freund, Bruder, Vater und Herr zugleich ist, mein Ratgeber, Erlöser und Gott. Ich spreche von Jesus Christus, dem Sohn Gottes. Ihm gehört mein Dank und alle Ehre!

Darüber hinaus möchte ich auch einigen „irdischen Personen“ danken.
Da ist zuerst natürlich mein Betreuer Prof. Dr. Helmut Maier zu nennen, der mich während der letzten 4 Monate von der ersten Besprechung über die Anmeldung der Arbeit bis zur Abgabe sehr gut betreut hat. Ich bin auch sehr dankbar, dass ich über dieses eigens von mir gewählte Thema schreiben durfte, für all die kleinen Ideen und Anstöße, die schlussendlich doch zum einen oder anderen Beweis in dieser Arbeit geführt haben.

Weiter wären da meine Eltern, die durch die Erziehung einen Grundstein für mein heutiges Leben gelegt haben. Speziell gilt mein Dank meinem Vater, der sich immer wieder Zeit für mich genommen hat, um meine neuesten mathematischen oder informatischen Fragen zu besprechen. Vielen Dank auch an Frau Jamnitzky, Dossenberger-Gymnasium Günzburg, die durch die zweimalige Betreuung bei Jugend forscht einiges zum Entstehen dieser Arbeit beigetragen hat. Ich möchte darüber hinaus Ben Heuer von der Universität Heidelberg sehr danken. Wie in der Einleitung und dem Abschnitt über die Mengen Q_d erwähnt, konnte ich nicht nur zusammen mit ihm die Beziehung zwischen eleganten und Fermatschen Zahlen beweisen, sondern er fand auch einige schöne und tiefgreifende Sätze zur Struktur und Größe der Mengen Q_d heraus. Zuletzt möchte ich noch meiner Verlobten Jenny danken. Danke, für deine Unterstützung und Ermutigung bei dieser Arbeit, dein Interesse und vor allem all die Liebe, die du mir jeden Tag gibst. Ich liebe dich!

Günzburg/Ulm im Juni 2013

2 Einleitung und Geschichte

In diesem ersten Abschnitt soll ein wenig auf die Entstehung dieses Themas eingegangen werden. Die Thematik der Teilbarkeit von Potenztermen zieht sich durch die gesamte bisherige mathematische Arbeit des Autors. Schon in der achten Klasse entdeckte er beim „Herumspielen“ mit Zweierpotenzen den folgenden einfachen Zusammenhang: $2^n - 1$ ist genau dann durch 3 teilbar, wenn n eine gerade Zahl ist. Auch wenn dem Autor inzwischen vier konzeptionell unterschiedliche Beweise dafür bekannt sind, hat er damals selbst keinen gefunden. Der Beweis, den sein Vater daraufhin gab, soll hier kurz erklärt werden:

Sei n gerade, also etwa $n = 2k$, dann gilt $2^n - 1 = 2^{2k} - 1 = \left(2^k\right)^2 - 1 = \left(2^k + 1\right)\left(2^k - 1\right)$. Nun weiß man, dass unter drei aufeinander folgenden natürlichen Zahlen stets genau eine durch 3 teilbar ist, also auch in $\{2^k - 1, 2^k, 2^k + 1\}$. Die Potenz 2^k ist nicht durch 3 teilbar, also muss es $2^k - 1$ oder $2^k + 1$ sein. Ihr Produkt $2^n - 1$ ist dann aber auf jeden Fall durch 3 teilbar.
Wenn n nun ungerade ist, also $2k + 1$, so ist $2^n - 1 = 2^{2k+1} - 1 = 2 \cdot (2^{2k} - 1) + 2 - 1$. Dann ist $(2^{2k} - 1)$ wegen geradem Exponenten durch 3 teilbar, der Rest jedoch nicht.
Andere Beweismöglichkeiten sind vollständige Induktion über die geraden Zahlen, eine einfache Kongruenzrechnung, bei der man $2 \equiv -1 \pmod 3$ ausnutzt, oder die Betrachtung der Zahl $2^n - 1$ im Binärsystem mit dem Wissen, wann eine Binärzahl durch 3 teilbar ist.

Da sich Terme der Form $2^n - 1$ für gerades n nach der dritten binomischen Formel stets in einen weiteren Term dieser Form und einen Term der Form $2^n + 1$ zerlegen lassen, interessierte sich der Autor zunehmend für Terme der Form $2^n + 1$ mit ungeradem n.

Genauer gesagt, befasste er sich mit der Fragestellung, wann $2^n + 1$ nicht nur durch 3, sondern auch durch 9, 27, 81, also Potenzen von 3 teilbar ist. Man stellt fest: $2^3 + 1$ ist durch 9 teilbar (schreibe dafür $9 \mid 2^3 + 1$), $2^9 + 1$ ist durch 27 teilbar, $2^{27} + 1$ ist durch 81 teilbar usw. Allgemein also:

$$3^{n+1} \mid 2^{3^n} + 1$$

Dies lässt sich mit vollständiger Induktion zeigen. Genauer gilt sogar, dass 3^{n+1} die höchste Dreierpotenz ist, durch die $2^{3^n} + 1$ teilbar ist.

Untersucht man $3^{4^n} - 1$ auf Teilbarkeit durch 4^{n+1}, erhält man eine ähnliche Beziehung, genauso bei $4^{5^n} + 1$ usw. Diese Entdeckungen bildeten den Inhalt der Facharbeit des Autors, die mit dem folgenden schönen Satz ihren Höhepunkt fand.

Satz 2.1. *Seien a, n natürliche Zahlen mit $a \geq 2$. Dann gilt:*

$$(a+1)^{n+1} \mid a^{(a+1)^n} + (-1)^a \quad \textit{und} \quad (a+1)^{n+2} \nmid a^{(a+1)^n} + (-1)^a$$

Mit dieser Arbeit nahm der Autor auch an Jugend forscht teil und gewann auf dem Bundeswettbewerb neben einem dritten Platz einen sechswöchigen Forschungsaufenthalt an der Universtity of Rhode Island. Dort konnte er sich intensiv mit seinen Ideen weiterbeschäftigen. Bisher wurden nur Potenzen von a plus/minus 1 auf Teilbarkeit durch eine Potenz von $(a + 1)$ untersucht. Die neue Fragestellung war nun: Wie sieht es aus, wenn man Potenzen von a plus/minus 1 durch Potenzen einer anderen Zahl d, welche nicht zwingend mit a zusammenhängt, teilen will (d steht für Divisor)? Oder:
Was ist die höchste Potenz von d, durch die $a^c + 1$ für ein gewisses c teilbar ist ? Eine Antwort gibt folgender Satz, den der Autor während seines USA-Aufenthaltes im Sommer 2010 entdeckte:

Satz 2.2. *Sei d ungerade und $a \geq 2$. Falls d^k mit $k > 0$ die höchste Potenz von d ist, durch welche $a^c + 1$ teilbar ist, dann ist d^{k+l} die höchste d-Potenz, durch die $a^{c \cdot d^l} + 1$ teilbar ist.*

Einen ähnlichen Satz wird in Lemma 3.9 bewiesen. Der obige Satz 2.1 aus der Facharbeit war also ein Spezialfall, da bei ungeradem $d = a + 1$, also geradem a, immer $d^1 = (a + 1)^1$ die höchste Potenz ist, durch die $a^1 + 1$ teilbar ist.

Der Satz 2.2 macht allerdings keine Aussage darüber, wann die Anfangsbedingung, also dass $a^c + 1$ wenigstens durch d^1 teilbar ist, erfüllt ist. Also widmete sich der Autor der Fragestellung, ob es zu gegebenem a und d einen Exponenten c gibt, sodass $a^c + 1$ durch d teilbar ist. Denn dann sichert der Satz, dass es andere Exponenten gibt, sodass der Term auch durch d^2, d^3 etc. teilbar ist.

Dass es nicht zu jeder Kombination von a und d ein solches c gibt, wird schnell klar. Wenn a und d nicht teilerfremd sind, folgt sofort, dass es kein solches c gibt (siehe Lemma 5.2). Aber auch z.B. bei $a = 2$ und $d = 7$ hat man keinen Erfolg, da die Potenzen von 2 modulo 7 betrachtet immer nur die Werte $1, 2, 4$ durchlaufen und damit $2^c + 1$ nie kongruent zu 0 modulo 7 wird (siehe Abschnitt 5).

Es ist also naheliegend, zu gegebenem a alle Zahlen d zu betrachten, für die es ein c mit $d \mid a^c+1$ gibt. Alle diese Zahlen d bilden die Menge P_a. Die Mengen P_a haben einige schöne Eigenschaften, z.B. sind sie vermutlich ähnlich verteilt wie die Primzahlen. Der Autor fand nämlich ein Analogon zur Goldbachschen Vermutung: Statt dass man jede gerade Zahl ab 4 als Summe zweier Primzahlen darstellen kann, kann man (vermutlich) jede gerade Zahl ab einer Startzahl n_a als Summe zweier Zahlen aus P_a darstellen, sofern a gewisse Voraussetzungen erfüllt, z.B. keine Quadratzahl ist. Diese Thematik diskutieren wir in Abschnitt 5.6. Genauso scheint eine Zwillingsvermutung zu gelten: Es gibt unendlich viele Zahlen in P_a, die nur Abstand 2 voneinander haben. Desweiteren hat der Autor auch beweisen können, dass es in den Mengen P_a beliebig große Lücken zwischen aufeinander folgenden Zahlen gibt.
Der Autor hat die P_a-Zahlen auf dem hier beschriebenen Weg selbstständig definiert und alle Eigenschaften bewiesen. Später fand er heraus, dass einiges davon, insbesondere die Kriterien für P_a-Zahlen, schon von Pieter Moree (siehe [7]) in sehr ähnlicher Form hergeleitet wurden.

Wir werden in dieser Arbeit nach einer Auflistung aller benötigten zahlentheoretischen Techniken die Eigenschaften der Mengen P_a untersuchen, insbesondere, wie man herausfindet, ob $d \in P_a$ für gegebenes a und d gilt. Alle Kriterien in diesem Abschnitt, sofern nicht anders angemerkt, sind vom Autor selbst entdeckt worden, auch wenn sich ähnliche Aussagen auch bei Moree, [7], finden. Danach werden die P_a-Zahlen wie oben erwähnt mit den Primzahlen verglichen, bevor wir zuletzt zu einem weiteren interessanten Thema kommen:

Anstatt zu einem fixierten a alle passenden Zahlen d zu suchen, kann man umgekehrt auch d fixieren und alle Basen a in die Menge Q_d zusammenfassen, für welche es ein c gibt mit $d \mid a^c + 1$. Die Eigenschaften der Menge Q_d und was dies mit Fermatschen Primzahlen zu tun hat, werden in diesem Abschnitt untersuchen.

Den Abschluss bildet ein Ausblick und der Vergleich mit bisherigen Publikationen auf diesem Gebiet.

3 Zahlentheoretische Grundlagen

Die Zahlentheorie beschäftigt sich im Wesentlichen mit den natürlichen (oder ganzen) Zahlen. Der elementarste Begriff der Zahlentheorie ist der der Teilbarkeit, die spannendsten Objekte wohl die Primzahlen. Das Faszinierende ist, dass zahlentheoretische Probleme oft sehr einfach zu formulieren, ihre Beweise aber enorm schwierig sind. Man denke hier an den letzen Satz von Fermat oder die noch offenen Vermutungen von Goldbach und den Primzahlzwillingen (siehe Abschnitt 5.6).

Diese Arbeit ist der elementaren Zahlentheorie zuzurechnen (im Gegensatz zur analytischen Zahlentheorie), außer im Beweis des quadratischen Reziprozitätsgesetzes verlassen wir nie die ganzen Zahlen bzw. ihre modularen Restklassen (siehe 3.2).

Alle Zahlen, die in dieser Arbeit vorkommen, sind natürliche Zahlen (also 1, 2, 3, ...), es sei denn es wird explizit eine andere Zahlenmenge angegeben (z.B. ganze Zahlen, reelle Zahlen, ...).

Die Inhalte der ersten beiden Unterabschnitte finden sich in ähnlicher Form in nahezu jedem Buch über Zahlentheorie, es sind hier keine einzelnen Verweise angegeben. Der Autor empfiehlt zum Einstieg in die Zahlentheorie die Bücher [12] oder [9], welche sich dem Thema langsam und mit vielen Beispielen nähern. Für einen etwas schnelleren Einstieg kann man zum Beispiel [8] verwenden.

3.1 Elementare Teilbarkeitslehre

Die Aussagen dieses Unterabschnittes werden als bekannt vorausgesetzt und nicht bewiesen.

Definition 3.1. (i) a heißt teilbar durch b, falls es eine Zahl c gibt, sodass $a = b \cdot c$. Dann heißt b Teiler von a, geschrieben: $b \mid a$ (sprich: b teilt a).

(ii) Eine Zahl c heißt gemeinsamer Teiler von zwei Zahlen a, b, wenn $c \mid a$ und $c \mid b$. c heißt gemeinsames Vielfaches von a und b, falls $a \mid c$ und $b \mid c$.

(iii) Den größten gemeinsamen Teiler von a und b bezeichnen wir mit $\mathrm{ggT}(a, b)$ oder kürzer (a, b). Sofern im Kontext keine Verwechslung mit Paaren oder Vektoren möglich ist, verwenden wir immer die zweite Form. Das kleinste gemeinsame Vielfache wird durch $\mathrm{kgV}(a, b)$ ausgedrückt.

(iv) Zwei Zahlen a und b heißen teilerfremd, wenn sie außer 1 und -1 keinen gemeinsamen Teiler besitzen, das heißt, ihr ggT ist 1.

(v) Eine Zahl $p > 1$, welche nur durch 1 und sich selbst teilbar ist, heißt Primzahl.

Lemma 3.1. *Es gelten die folgenden Eigenschaften:*

(i) *Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.*

(ii) $\mathrm{ggT}(a, b) \geq 1$ *und* $\mathrm{kgV}(a, b) \leq ab$.

(iii) $\mathrm{kgV}(a, b) = \frac{ab}{\mathrm{ggT}(a,b)}$.

(iv) $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b)$

(v) *Für jede natürliche Zahl n gibt es eine (bis auf die Reihenfolge) eindeutige Primfaktorzerlegung*

$$n = \prod_{i=1}^{k} p_i^{e_i}.$$

mit paarweise verschiedenen Primzahlen $p_1, ..., p_k$ und natürlichen Zahlen $e_1, ..., e_k$.

Die Berechnung des größten gemeinsamen Teilers kann über den euklidischen Algorithmus erfolgen, den wir im folgenden Abschnitt nach Einführung des Teilens mit Rest angeben.

Definition 3.2 (h-Funktion)**.** Für jedes $k > 1$ gibt $h_k(n)$ den Exponent der größten k-Potenz an, durch die n teilbar ist.

Zum Beispiel ist $h_2(24) = 3$, weil $24 = 2^3 \cdot 3$.

3.2 Kongruenzrechnung

Eines der nützlichsten Hilfsmittel in der Teilbarkeitslehre ist das Rechnen mit Kongruenzen.

Definition 3.3. Sei $c \in \mathbb{N}$ gegeben. Zwei Zahlen a und b heißen kongruent modulo c, in Zeichen $a \equiv b \pmod{c}$, falls $c \mid a - b$.

Beispiel 3.1.

(a) $-7 \equiv -2 \equiv 3 \equiv 8 \equiv ... \equiv 1003 \equiv ... \pmod{5}$.

(b) $a \equiv 0 \pmod{b}$ bedeutet, dass b ein Teiler von a ist.

Bemerkung 3.1. Man mache sich mit der Definition klar: Falls für zwei teilerfremde Zahlen b und c jeweils $x \equiv a \pmod{b}$ und $x \equiv a \pmod{c}$ gilt, so gilt auch $x \equiv a \pmod{bc}$.

Das folgende Lemma zeigt, dass man mit Kongruenzen fast so rechnen kann wie mit Gleichungen.

Lemma 3.2 (Verträglichkeit)**.** *Sei* $a \equiv b \pmod{c}$ *und* $e \equiv f \pmod{c}$*, dann gilt auch*

(i) $a + e \equiv b + f \pmod{c}$

(ii) $ae \equiv bf \pmod{c}$

(iii) $a^n \equiv b^n \pmod{c}$.

Mit Teil (iii) dieses Lemmas kann man z.B. die erste Aussage aus der Einleitung beweisen: *Für eine gerade Zahl* n *ist* $2^n - 1$ *durch 3 teilbar.* Es ist nämlich $2 \equiv -1 \pmod{3}$ und (iii) liefert $2^n \equiv (-1)^n \pmod{3}$. Da nun n gerade ist, gilt insgesamt $2^n - 1 \equiv (-1)^n - 1 \equiv 1 - 1 = 0 \pmod{3}$, also ist $2^n - 1$ durch 3 teilbar.

Lemma 3.3 (Division mit Rest)**.** *Sei* c *gegeben.*

(i) Zu jedem a *existieren eindeutige Zahlen* q, r *mit* $0 \leq r < b$*, so dass* $a = qc + r$*. Wir definieren* $\mathrm{div}(a, c) := q$ *und* $\mathrm{rem}(a, c) := r$*.*

(ii) Die Abbildung $f : \mathbb{Z} \to \{0, 1, ..., c - 1\}$ *mit* $f : a \mapsto \mathrm{rem}(a, c)$ *ist surjektiv (Restklassenabbildung).*

(iii) Für alle a *ist* $a \equiv \mathrm{rem}(a, c) \pmod{c}$.

Definition 3.4. Sei c fest. Das Urbild einer Zahl a mit $0 \leq a \leq c - 1$ bezüglich der Restklassenabbildung $\mathrm{rem}(\cdot, c)$ heißt Restklasse von a modulo c, geschrieben $\bar{a}$. Die Zahl a heißt ein Repräsentant von $\bar{a}$. Die Menge aller Restklassen modulo c wird mit $\mathbb{Z}/c\mathbb{Z}$ bezeichnet.

Die Restklassen sind also gerade die Äquivalenzklassen bezüglich der Äquivalenzrelation $\equiv \pmod{c}$. Die Restklasse $\bar{a}$ enthält alle ganzen Zahlen n, die kongruent zu a modulo c sind.
In $\mathbb{Z}/c\mathbb{Z}$ definiert man die Addition und Multiplikation zweier Restklassen $\bar{a}$ und $\bar{b}$ über $\overline{a + b}$ bzw. $\overline{ab}$. Man zeigt schnell, dass diese Verknüpfung wohldefiniert ist, d.h. nicht von der Wahl der Repräsentanten a und b der Restklassen abhängt. Die Menge aller multiplikativ invertierbaren Elemente $\bar{a}$, d.h. jene, zu denen es eine Restklassen $\bar{b}$ mit $\bar{a}\bar{b} = \bar{1}$ gibt, wird mit $(\mathbb{Z}/c\mathbb{Z})^\times$ bezeichnet.

Satz 3.1. *Für alle $c \geq 2$ ist $(\mathbb{Z}/c\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Eins. Eine Restklasse $\bar{a}$ hat genau dann ein multiplikatives Inverses, wenn $(a, c) = 1$ gilt. $(\mathbb{Z}/c\mathbb{Z}, +, \cdot)$ ist genau dann ein Körper, wenn $(\mathbb{Z}/c\mathbb{Z})^\times = \mathbb{Z}/c\mathbb{Z} \setminus \{\bar{0}\}$, was wieder genau dann gilt, wenn c eine Primzahl ist.*

Nun kommt eine wichtige Eigenschaft der Kongruenzrechnung, welche sich aus dem vorherigen Satz schnell herleiten lässt.

Lemma 3.4 (Kürzen)**.** *Seien a und c teilerfremd. Dann gilt die Implikation*

$$ab \equiv ad \pmod{c} \;\Rightarrow\; b \equiv d \pmod{c}.$$

Beweis. Der letzte Satz besagt, dass $\bar{a}$ eine Inverse $\bar{a}^{-1}$ in $\mathbb{Z}/c\mathbb{Z}$ hat, falls $(a, c) = 1$ gilt. Für jedes Element $s \in \bar{a}^{-1}$ gilt dann $sa \equiv 1 \pmod{c}$. Die Behauptung folgt also durch Multiplikation der gegebenen Kongruenz mit s. □

Außerdem können wir jetzt den zuvor angekündigten Euklidischen Algorithmus zur Berechnung des größten gemeinsamen Teilers zweier Zahlen angeben. Der wunderschön kurze Code im Algorithmus 1 stammt aus [10], Abschnitt 7.3.

Algorithmus 1 : Euklid(a, b)

```
if b = 0 then
    return a;
end
return Euklid(b, rem(a, b));
```

3.3 Der Chinesische Restsatz

Ein System aus linearen Kongruenzgleichungen der Form

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\dots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

bezeichnet man als *simultane* Kongruenz. Zum Beispiel könnte eine natürliche Zahl gesucht sein, die beim Teilen durch 3,4 und 5 den Rest 1 hat und beim Teilen durch 7 den Rest 3.

Eine Antwort auf die Frage, ob eine gegebene simultane Kongruenz lösbar ist, gibt der sogenannte Chinesische Restsatz. Seinen Namen hat er daher, dass er wohl zuerst den Chinesen bekannt war. Er lautet:

Satz 3.2. *Eine Lösung der obigen simultanen Kongruenz existiert genau dann, wenn*

$$(m_i, m_j) \mid a_i - a_j \quad \forall\, i, j \in \{1, ..., n\}.$$

Falls die Module $m_1, ..., m_n$ paarweise teilerfremd sind, existiert also immer eine Lösung. Wenn x eine Lösung der simultanen Kongruenz ist, so sind durch $x + kM$ mit $M = \mathrm{kgV}(m_1, ..., m_n)$, $k \in \mathbb{Z}$ alle weiteren Lösungen gegeben. Insbesondere gibt es im Falle der Lösbarkeit immer eine Lösung x mit $0 \leq x < M$.

Der Beweis des Chinesischen Restsatzes wird meist konstruktiv geführt und gibt somit gleichzeitig einen Algorithmus zum Lösen einer simultanen Kongruenz. Beweise finden sich in nahezu jedem Buch über elementare Zahlentheorie und natürlich auch in der Wikipedia. Wir verweisen hier insbesondere auf [3], wo der Beweis zwar nur für teilerfremde Moduln geführt wird, aber in einem Beispiel die Aussage auf nicht teilerfremde Moduln erweitert wird.
Eine Anwendung des Chinesischen Restsatzes findet sich zum Beispiel im nächsten Unterabschnitt.

3.4 Die Eulersche Phi-Funktion

Definition 3.5. Für jede natürliche Zahl a ist $\varphi(a)$ die Anzahl aller Zahlen $b \leq a$, welche teilerfremd zu a sind.

Die Eulersche Phi-Funktion von c gibt also gerade an, wie viele invertierbare Restklassen $\bar{a}$ es in $\mathbb{Z}/c\mathbb{Z}$ gibt und damit die Größe der Einheitengruppe $(\mathbb{Z}/c\mathbb{Z})^\times$. Zum Beispiel ist $\varphi(6) = 2$, da unter 6 nur 1 und 5 teilerfremd zu 6 sind, während 2, 3 und 4 jeweils einen nichttrivialen gemeinsamen Teiler mit 6 haben. Hingegen ist $\varphi(7) = 6$, denn sämtliche Zahlen $1, 2, 3, 4, 5, 6$ sind teilerfremd zu 7, was daran liegt, dass 7 eine Primzahl ist. Diese Erkenntnis ist Inhalt des nächsten Lemmas.

Lemma 3.5. *Sei p eine Primzahl und n eine beliebige natürliche Zahl. Dann gilt*

(i) $\varphi(p) = p - 1$.

(ii) $\varphi(p^n) = (p-1)p^{n-1} = p^n \cdot \left(1 - \frac{1}{p}\right)$.

Beweis. (i) ist klar, da alle natürlichen Zahlen unter p teilerfremd zu p sind.
Die Zahlen unter p^n, welche einen gemeinsamen Teiler > 1 mit p^n haben, sind gerade die Vielfachen von p. Davon gibt es unter p^n genau p^{n-1} viele. Somit ist (ii) klar. □

Die vielleicht wichtigste Eigenschaft der Phi-Funktion ist die folgende Funktionalgleichung:

Satz 3.3 (Multiplikativität der Phi-Funktion)**.** *Seien die Zahlen a, b teilerfremd. Dann gilt:*

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

Beweis. Betrachte die beiden Mengen

$$\begin{aligned} A &= \{1 \leq t \leq ab : \mathrm{ggT}(t, ab) = 1\} \\ B &= \{(s,t) \in \mathbb{N} \times \mathbb{N} : 1 \leq s \leq a, \mathrm{ggT}(s,a) = 1, 1 \leq t \leq b, \mathrm{ggT}(t,a) = 1\} \\ &= \{s : 1 \leq s \leq a, \mathrm{ggT}(s,a) = 1, \} \times \{t : 1 \leq t \leq b, \mathrm{ggT}(t,a) = 1\}. \end{aligned}$$

Dabei ist anzumerken, dass die Elemente von B Paare (s,t) sind, die Klammern drücken hier nicht den ggT aus! Es gilt nach Definition $|A| = \varphi(ab)$ und $|B| = \varphi(a) \cdot \varphi(b)$. Man definiert nun eine Abbildung $\Phi : A \to B$ über $\Phi : t \mapsto (\mathrm{rem}(t,a), \mathrm{rem}(t,b))$.
Φ ist auch bijektiv, denn sei $(s,t) \in B$ beliebig gegeben. Dann garantiert der Chinesische Restsatz wegen der Teilerfremdheit von a und b, dass die simultane Kongruenz

$$\begin{aligned} x &\equiv s \pmod{a} \\ x &\equiv t \pmod{b} \end{aligned}$$

genau eine Lösung x mit $0 \leq x < \mathrm{kgV}(a,b) = ab$ hat. Also hat (s,t) bezüglich Φ *genau ein* Urbild. Φ ist demnach bijektiv, es gilt $|A| = |B|$ und damit die Behauptung.

□

Aus diesem Satz und dem vorherigen Lemma über Primpotenzen folgt nun induktiv ohne weiteren Beweis der

Satz 3.4. *Sei a eine natürliche Zahl und $a = \prod_{i=1}^{n} p_i^{e_i}$ die Primfaktorzerlegung von a. Dann gilt*

$$\varphi(a) = \prod_{i=1}^{n} (p_i - 1) p_i^{e_i - 1} = a \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right)$$

Die Eulersche Phi-Funktion hat eine schöne Eigenschaft, was das modulare Potenzieren angeht:

Satz 3.5 (Kleiner Satz von Euler)**.** *Es gilt für teilerfremde Zahlen a, b stets: $a^{\varphi(b)} \equiv 1 \pmod{b}$.*

Beweis. Sei $A = \{c : 0 \leq c < b \text{ mit } (c, b) = 1\}$, wobei nach Definition $|A| = \varphi(b)$. Betrachtet man nun $B = \{\text{rem}(ac, b) : 0 \leq c < b \text{ mit } (c, b) = 1\}$, stellt man leicht fest, dass $A = B$. Das liegt daran, dass wegen der Teilerfremdheit von a und b die Abbildung $c \to \text{rem}(ac, b)$ eine Bijektion ist, weil man nach Lemma 3.4 die Zahl a einfach wieder „wegkürzen“ kann. Also gilt:

$$\prod_{c \in A} c = \prod_{d \in B} d \equiv \prod_{c \in A} ac = a^{\varphi(b)} \cdot \prod_{c \in A} c \pmod{b}$$

Weil alle c aus A teilerfremd zu b sind, kann man sie wiederum nach Lemma 3.4 wegkürzen und es bleibt $1 \equiv a^{\varphi(b)} \pmod{b}$ stehen. □

Eine spezielle Version des Kleinen Satzes von Euler für Primzahlen ist das

Korollar 3.1 (Kleiner Satz von Fermat)**.** *Sei p eine Primzahl und $(a, p) = 1$. Dann gilt:*

$$a^{p-1} \equiv 1 \pmod{p}$$

3.5 Die multiplikative Ordnung einer Zahl

Definition 3.6. Seien a und b teilerfremd. Dann ist die Ordnung $\text{ord}_b(a)$ von a modulo b definiert als die kleinste Zahl $c > 0$ mit $a^c \equiv 1 \pmod{b}$.

Zum Beispiel ist die Ordnung von 4 modulo 7 gerade gleich 3, denn $4^1 = 4 \not\equiv 1 \pmod{7}$, $4^2 = 16 \equiv 2 \not\equiv 1 \pmod{7}$ und $4^3 \equiv 16 \cdot 4 \equiv 2 \cdot 4 \equiv 8 \equiv 1 \pmod{7}$.

Die Ordnung findet sich auch einer anderen Stelle in der Mathematik: Betrachte die Dezimalbruchentwicklung von Zahlen der Form $\frac{1}{n}$. Man weiß, dass für jede dieser Zahlen die Dezimalbruchentwicklung periodisch ist, wobei zwischen „abbrechenden“ Brüchen, deren Entwicklung schließlich nur noch aus der Ziffer 0 besteht und den „echt periodischen“ oder „nicht abbrechenden“ Brüchen unterschieden wird. Falls n teilerfremd zu 10 ist, stellt man fest, dass die Periodenlänge $p(n)$ gleich der Ordnung $\text{ord}_n(10)$ ist. Das kommt daher, dass man beim Divisionsalgorithmus immer abwechselnd den bisherigen Rest mit 10 malnimmt und anschließend wieder ganzzahlig durch n teilt (also modulo n reduziert). Insgesamt rechnet man also eine Potenz von 10 aus und betrachtet ihren Rest modulo n. Die Periode ist erreicht, wenn der Rest zum ersten Mal wieder 1 ist. Das ist nach genau $\text{ord}_n(10)$ Schritten der Fall.
Falls n Zweier oder Fünfer enthält, ergibt sich die Periodenlänge, indem man die Zweier und Fünfer aus der Primfaktorzerlegung entfernt und dann die Ordnung von 10 modulo der entstehenden Zahl nimmt.

Darüberhinaus ist die Ordnung ein sehr nützlicher Begriff bei der Charakterisierung der P_a-Zahlen in dieser Arbeit. Wir wollen jetzt einige Eigenschaften und Formeln herleiten.

Lemma 3.6. *Seien a und b teilerfremd. Die Kongruenzgleichung $a^c \equiv a^d \pmod{b}$ gilt genau dann, wenn $c \equiv d \pmod{\text{ord}_b(a)}$. Insbesondere folgt aus $a^c \equiv 1 \pmod{b}$ immer $\text{ord}_b(a) \mid c$.*

Beweis. Sei $o = \text{ord}_b(a)$. Nach Lemma 3.3 (Division mit Rest) existieren nichtnegative Zahlen q_1, q_2, r_1, r_2 mit $c = q_1 o + r_1$, $d = q_2 o + r_2$ und $r_1, r_2 < o$. Ohne Beschränkung der Allgemeinheit sei $r_2 \geq r_1$ (sonst vertausche c und d). Dann gelten die folgenden Äquivalenzumformungen

$$\begin{aligned} a^c \equiv a^d \pmod{b} &\Leftrightarrow a^{q_1 o + r_1} \equiv a^{q_2 o + r_2} \pmod{b} \Leftrightarrow (a^o)^{q_1} a^{r_1} \equiv (a^o)^{q_2} a^{r_2} \pmod{b} \\ &\Leftrightarrow a^{r_1} \equiv a^{r_2} \pmod{b} \Leftrightarrow 1 \equiv a^{r_2 - r_1} \pmod{b} \end{aligned}$$

Die letzte Umformung ist richtig, da $(a, b) = 1$ und somit a nach Lemma 3.4 gekürzt werden darf. Da wegen $r_1, r_2 < o$ und $r_2 \geq r_1$ auch $0 \leq r_2 - r_1 < o$ gilt und ferner nach Definition der Ordnung

$a^k \not\equiv 1 \pmod{b}$ für $0 < k < o$, ist die letzte Aussage äquivalent zu $r_2 - r_1 = 0$. Das bedeutet aber $c \equiv d \pmod{o}$, also die Behauptung.
Der Zusatz wird klar mit $d = 0$ oder $d = \mathrm{ord}_d(a)$. □

Den Zusatz „$a^c \equiv 1 \pmod{b} \Leftrightarrow \mathrm{ord}_b(a) \mid c$“ des letzten Lemmas werden wir sehr oft benutzen. Aus dem Kleinen Satz von Euler und dem vorigen Lemma folgt das

Korollar 3.2. *Für teilerfremde Zahlen a und b gilt*

$$\mathrm{ord}_b(a) \mid \varphi(b).$$

Nun gibt es ein kleines Resultat, wie die Ordnung von a^n mit der Ordnung von a zusammenhängt. Es findet sich auch in [6].

Lemma 3.7. *Seien a und b teilerfremd. Dann gilt:*

$$\mathrm{ord}_b(a^n) = \frac{\mathrm{ord}_b(a)}{(n, \mathrm{ord}_b(a))}$$

Beweis. Sei $o = \mathrm{ord}_b(a^n)$. Nach Definition gilt $a^{no} = (a^n)^o \equiv 1 \pmod{b}$. Daher muss no ein Vielfaches von $\mathrm{ord}_b(a)$ sein, sagen wir

$$no = k \cdot \mathrm{ord}_b(a) \quad \text{oder} \quad o = \frac{k \cdot \mathrm{ord}_b(a)}{n}.$$

Seien nun $g := (\mathrm{ord}_b(a), n)$ und die Zahlen s, t teilerfremd mit $\mathrm{ord}_b(a) = sg$, $n = tg$. So folgt

$$o = \frac{ksg}{tg} = \frac{ks}{t}.$$

Da s und t teilerfremd sind, kann $\frac{ks}{t}$ nur eine ganze Zahl sein, wenn $t \mid k$, also $k = lt$ für ein gewisses l. Setzt man dies wieder ein, so erhält man schließlich $o = \dfrac{lts}{t} = ls$.
Da die Ordnung minimal gewählt ist, setzt man $l = 1$ (also $t = k$) und mit der Definition von s folgt die Behauptung:

$$o = s = \frac{\mathrm{ord}_b(a)}{g} = \frac{\mathrm{ord}_b(a)}{(n, \mathrm{ord}_b(a))}.$$

□

Lemma 3.8. *Seien a, b, c paarweise teilerfremd. Dann gilt:*

$$\mathrm{ord}_{bc}(a) = \mathrm{kgV}(\mathrm{ord}_b(a), \mathrm{ord}_c(a))$$

Beweis. Sei $n = \mathrm{ord}_{bc}(a)$, dann gilt $a^n \equiv 1 \pmod{bc}$ und deswegen sowohl $a^n \equiv 1 \pmod{b}$ als auch $a^n \equiv 1 \pmod{c}$. Also muss n sowohl ein Vielfaches von $\mathrm{ord}_b(a)$ als auch $\mathrm{ord}_c(a)$ sein. Sei k also ein beliebiges gemeinsames Vielfaches von $\mathrm{ord}_b(a)$ und $\mathrm{ord}_c(a)$. Dann gilt

$$a^k \equiv 1 \pmod{b} \quad \text{und} \quad a^k \equiv 1 \pmod{d}$$

und aus der Teilerfremdheit von b und c folgt auch

$$a^k \equiv 1 \pmod{bc}.$$

Also ist jedes gemeinsame Vielfache ein Kandidat für $\mathrm{ord}_{bc}(a)$ und $\mathrm{kgV}(\mathrm{ord}_c(a), \mathrm{ord}_c(b))$ ist die kleinste Wahl für k. □

Nun ist das Ziel herzuleiten, wie die Ordnung einer Zahl a modulo einer Primzahlpotenz p^n in Abhängigkeit von $\mathrm{ord}_p(a)$ aussieht. Dazu benötigen wir zuerst ein Lemma, welches eine wichtige Aussage über die Teilbarkeit von Termen der Form a^m-1 durch Potenzen von Primzahlen p macht. Dabei wird die h-Funktion aus Definition 3.2 benutzt.

Lemma 3.9. *Sei $a \geq 2$ und p eine ungerade Primzahl. Für einen gewissen Exponenten c sei a^c-1 genau k-mal durch p teilbar, d.h. $h_p(a^c-1)=k$. Dann gilt für alle $n \in \mathbb{N}_0$:*

$$h_p\left(a^{c\cdot p^n}-1\right) = k+n.$$

Beweis. Mit vollständiger Induktion nach n.
$n=0$:

$$h_p\left(a^{c\cdot p^0}-1\right) = h_p(a^c-1) = k = k+0 \text{ nach Voraussetzung.}$$

$n \to n+1$:
Es gelte also die Aussage für n, zu zeigen ist nun, dass $a^{c\cdot p^{n+1}}-1$ genau durch p^{k+n+1} teilbar ist. Setze $u := a^{c\cdot p^n}$. Es gilt mit der geometrischen Summenformel:

$$a^{c\cdot p^{n+1}}-1 = \left(a^{c\cdot p^n}\right)^p - 1 = u^p - 1 = (u-1)\cdot\sum_{l=0}^{p-1} u^l$$

Aus der Induktionsannahme wissen wir, dass $u-1 = a^{c\cdot p^n}-1$ durch p^{k+n}, aber nicht durch p^{k+n+1} teilbar ist. Damit also $a^{c\cdot p^{n+1}}-1$ genau durch p^{k+n+1} teilbar ist, muss die Summe $\sum_{l=0}^{p-1} u^l$ gerade durch p, aber nicht p^2 teilbar sein. [Anmerkung: Da p prim ist, kann es nicht passieren, dass in beiden Faktoren noch ein Anteil von p enthalten ist, sodass das Produkt der beiden schließlich doch durch eine höhere Potenz teilbar ist.] Beachtet man, dass wegen $p^{n+k} \mid u-1$, d.h. $u \equiv 1 \pmod{p^{n+k}}$, auch $u \equiv 1 \pmod{p}$ gilt, sieht man leicht, dass die Summe durch p teilbar ist:

$$\sum_{l=0}^{p-1} u^l \equiv \sum_{l=0}^{p-1} 1^l = \sum_{l=0}^{p-1} 1 = p \equiv 0 \pmod{p}$$

Nun muss man noch zeigen, dass p^2 kein Teiler der Summe ist.
Sei dazu $u-1 = p\cdot q$, wobei q durchaus noch mehrmals durch p teilbar sein darf. Wiederum mit der geometrischen Summenformel gilt

$$\begin{aligned}\sum_{l=0}^{p-1} u^l &= p + \sum_{l=0}^{p-1}(u^l-1) = p + \sum_{l=1}^{p-1}(u^l-1) = p + \sum_{l=1}^{p-1}(u-1)\sum_{i=0}^{l-1} u^i \\ &= p + (u-1)\sum_{l=1}^{p-1}\sum_{i=0}^{l-1} u^i = p\cdot\left[1 + q\sum_{l=1}^{p-1}\sum_{i=0}^{l-1} u^i\right]\end{aligned}$$

Man muss also zeigen, dass der Term in der Klammer nicht durch p teilbar ist, d.h. $\not\equiv 0 \pmod{p}$ ist. Mit $u \equiv 1 \pmod{p}$, der Gaußschen Summenformel und der Tatsache, dass $p-1$ gerade ist, folgert man:

$$\begin{aligned}1 + q\sum_{l=1}^{p-1}\sum_{i=0}^{l-1} u^i &\equiv 1 + q\sum_{l=1}^{p-1}\sum_{i=0}^{l-1} 1 = 1 + q\sum_{l=1}^{p-1} l \\ = 1 + q\cdot\frac{(p-1)p}{2} = 1 + q\cdot\frac{p-1}{2}\cdot p &\equiv 1 \not\equiv 0 \pmod{p}.\end{aligned}$$

Somit haben wir nun ingesamt bewiesen, dass die Summe $\sum_{l=0}^{p-1} u^l$ genau durch p^1 teilbar ist. Damit ist ingesamt der Ausgangsterm durch p^{k+n+1} und keine höhere p-Potenz teilbar, was gerade behauptet wurde. □

Nun kommen wir zum eigentlich gewünschten Satz über die Ordnung.

Satz 3.6. *Sei p eine ungerade Primzahl und $a \geq 2$ teilerfremd zu p.*
Ferner sei $k = h_2(a^{\mathrm{ord}_p(a)} - 1)$. Dann gilt:

$$\mathrm{ord}_{p^n}(a) = \begin{cases} \mathrm{ord}_p(a), & \text{falls } n \leq k, \\ \mathrm{ord}_p(a) \cdot p^{n-k}, & \text{falls } n > k. \end{cases}$$

Beweis. Zunächst sollte man sich klar machen, dass aus $m \leq n$ stets $\mathrm{ord}_{p^m}(a) \mid \mathrm{ord}_{p^n}(a)$ folgt. Insbesondere gilt immer $\mathrm{ord}_p(a) \mid \mathrm{ord}_{p^n}(a)$.
Falls $n \leq k$, dann gilt natürlich $p^n \mid p^k \mid a^{\mathrm{ord}_p(a)} - 1$, d.h. $\mathrm{ord}_{p^n}(a)$ ist Teiler von $\mathrm{ord}_p(a)$. Da die umgekehrte Teilerrelation aber wegen der Vorbemerkung auch gelten muss, gilt Gleichheit.
Sei nun $n > k$. Zur Abkürzung sei $\sigma_n = \mathrm{ord}_{p^n}(a)$. Man zeigt zuerst, dass $\mathrm{ord}_{p^n}(a)$ von der Form $\mathrm{ord}_p(a) \cdot p^l$ ist und berechnet anschließend l genauer. Wegen der Vorbemerkung ist σ_n ein Vielfaches von $\sigma_1 = \mathrm{ord}_p(a)$, sagen wir

$$\sigma_n = m\sigma_1 \tag{1}$$

Weiter gilt aber auch nach dem letzten Lemma mit $c = \sigma_1$

$$h_p(a^{\sigma_1 \cdot p^{n-k}} - 1) = k + (n-k) = n$$

Das heißt $a^{\sigma_1 \cdot p^{n-k}} \equiv 1 \pmod{p^n}$. Nach unserem vielgenutzten Lemma 3.6 ist σ_n ein Teiler von $\sigma_1 \cdot p^{n-k}$. Wegen (1) ist also m ein Teiler von p^{n-k}, d.h. $m = p^l$ für $0 \leq l \leq n-k$. Das letzte Lemma besagt aber, dass $a^{\sigma_1 \cdot p^l} - 1$ genau durch p^{k+l}, teilbar ist. Da $a^{\sigma_1 \cdot p^l} - 1$ aber durch p^n teilbar ist, muss $l = n - k$ gelten. Damit ist $\sigma_n = \sigma_1 \cdot p^{n-k}$. Das war zu zeigen. □

Mit den letzten beiden Lemmata kann man die Ordnung einer Zahl a modulo einer zu a teilerfremden Zahl b relativ effizient ausrechnen, wenn man die Primfaktorzerlegung von b kennt.

3.6 Primitivwurzeln und der Index

Wie man im letzten Unterabschnitt gesehen hat, kann die Ordnung einer Zahl a modulo b höchstens $\varphi(b)$ sein. Zahlen, die diese Ordnung haben, haben eine besondere Bedeutung:

Definition 3.7. Für teilerfremde Zahlen a und b heißt a Primitivwurzel modulo b, falls a maximale Ordnung $\mathrm{ord}_b(a) = \varphi(b)$ modulo b hat.

Wenn ξ eine Primitivwurzel modulo b ist, sind wegen Lemma 3.6 dann keine zwei Potenzen ξ^k und ξ^l mit $0 < k \neq l \leq \varphi$ gleich. Das heißt, die Potenzen von ξ modulo b durchlaufen $\varphi(b)$ verschiedene Werte, bevor sie erstmalig wieder 1 werden, das sind gerade alle modulo b multiplikativ invertierbaren Elemente. Anders gesprochen: $\bar{\xi}$ ist ein Erzeuger der Einheitengruppe $(\mathbb{Z}/b\mathbb{Z})^\times$ und $(\mathbb{Z}/b\mathbb{Z})^\times$ wird dadurch zu einer zyklischen Gruppe.

Zu jeder Zahl a mit $(a, b) = 1$ gibt es also einen eindeutig definierten Exponenten $k \leq \varphi(b)$, sodass $\xi^k \equiv a \pmod{b}$.

Definition 3.8. Diesen Exponenten k definieren wir als den Index von a modulo b bezüglich der Primitivwurzel ξ, in Formeln $\mathrm{ind}_b^\xi(a)$. Falls klar ist, von welchem Modul b und welcher Primitivwurzel ξ man spricht, schreibt man oft auch kurz nur $\mathrm{ind}(a)$.

Beispiel 3.2. Wir rechnen modulo 7. Eine Primitivwurzel ist also eine Zahl, die Ordnung 6 modulo 7 hat. Das erfüllt z.B. die 3. $3^k \bmod 7$ durchläuft für $k = 1, ..., 6$ die folgenden Werte: $3, 2, 6, 4, 5, 1$. Damit ergibt sich für die Indizes die Tabelle 1.

a	1	2	3	4	5	6
ind(a)	6	2	1	4	5	3

Tabelle 1: Indexwerte modulo 7 bzgl. der Primitivwurzel 3

Allerdings stellt sich die Frage, ob es überhaupt immer Primitivwurzeln gibt. Tatsächlich gibt es zum Beispiel keine Primitivwurzel modulo 15:
$\varphi(15) = (3-1)(5-1) = 8$. Nun haben die Elemente $2, 7, 8, 13$ jeweils Ordnung 4, die Zahlen $4, 11, 14$ haben Ordnung 2 und die 1 hat Ordnung 1. Keine Zahl, teilerfremd zu 15, hat volle Ordnung 8. Also gibt es keine Primitivwurzel modulo 15.

Der folgende Satz zeigt, wann es Primitivwurzeln gibt:

Satz 3.7. *Sei $m \geq 2$. Es gibt genau dann eine Primitivwurzel modulo m, wenn $m = 2, 4$, eine ungerade Primzahl(potenz) oder das Zweifache davon ist.*

Beweis. Einen Beweis, aufgesplittet in viele einzelne Sätze und Lemmata, kann man zum Beispiel in [9], Kapitel 9 nachlesen. □

Wir benötigen in dieser Arbeit ausschließlich einen Spezialfall des Satzes, und zwar, dass es modulo einer Primzahlpotenz stets (mindestens) eine Primitivwurzel gibt. Alle Einheitengruppen $(\mathbb{Z}/d\mathbb{Z})^\times$ mit d prim sind also zyklisch.

4 Das Quadratische Reziprozitätsgesetz

In diesem Abschnitt soll es um ein sehr hilfreiches zahlentheoretisches Resultat gehen, das nicht ganz so einfach zu beweisen ist wie die meisten Grundlagen im letzten Abschnitt. Wir orientieren uns hier am Vorgehen im Buch „Elementare und algebraische Zahlentheorie“ von Stefan Müller-Stach und Jens Piontkowski ([8]), geben aber zusätzlich zum dort geführten Beweis einen zweiten Beweis, wie er auch im Skript „Vorlesung Zahlentheorie“ von Helmut Maier ([6]) zu finden ist.

Definition 4.1. Sei p eine Primzahl. Eine Zahl $a \not\equiv 0 \pmod p$ heißt quadratischer Rest modulo p, falls es eine ganze Zahl b mit $b^2 \equiv a \pmod p$ gibt, d.h. die Gleichung $x^2 \equiv a \pmod p$ eine Lösung hat. Andernfalls heißt a quadratischer Nichtrest modulo p. 0 wird nicht als quadratischer Rest bezeichnet. Wir definieren das Legendre-Symbol wie folgt:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p \mid a, \\ +1 & \text{falls } x^2 \equiv a \pmod p \text{ lösbar ist und } p \nmid a, \\ -1 & \text{falls } x^2 \equiv a \pmod p \text{ nicht lösbar ist.} \end{cases}$$

Wenn a quadratischer Rest modulo p ist, ist natürlich $a + kp, k \in \mathbb{Z}$ auch quadratischer Rest modulo p, es reicht also die Restklassen (oder je einen Vertreter pro Restklasse) modulo p zu betrachten. Welche Zahlen/Restklassen sind zum Beispiel quadratische Reste modulo 7? Dazu kann man einfach für die Zahlen 0,1,...,6 (oder genauer die Restklassen $\bar{0}, ...\bar{6}$) das Quadrat modulo 7 berechnen und dann die Legendre-Symbole angeben, siehe Tabelle 2.

x	0	1	2	3	4	5	6
$x^2 \pmod 7$	0	1	4	2	2	4	1

a	0	1	2	3	4	5	6
$\left(\frac{a}{7}\right)$	0	1	1	-1	1	-1	-1

Tabelle 2: Quadrate modulo 7 und Werte des Legendre-Symbols

Man stellt fest, dass stets a und $p-a$ durch $x \mapsto \text{rem}(x^2, p)$ auf die selbe Zahl abgebildet wird. Damit kann es höchstens $\frac{p-1}{2}$ viele quadratische Reste geben. Die quadratischen Reste modulo 7 bilden hier sogar eine multiplikative Gruppe modulo 7, das heißt insbesondere, dass das Produkt zweier quadratischer Reste wieder quadratischer Rest ist, die 1 enthalten ist und zu jedem quadratischen Rest a auch a^{-1} quadratischer Rest ist.

Außerdem kann noch mehr entdecken: 3 ist eine Primitivwurzel modulo 7, denn $\text{ord}_7(3) = 6$. Die Potenzen $3^k \pmod p$ durchlaufen für $k = 0, ..., 6$ die Werte $1, 3, 2, 6, 4, 5, 1$. Die drei quadratischen Reste modulo 7 (also 1,2,4) haben dabei die Exponenten 0,2,4. Die quadratischen Nichtreste $3, 5, 6$ haben die Exponenten $1, 5, 3$. Es scheint so, als ob die quadratischen Reste geraden Index bzgl. der Primitivwurzel 3 haben und die Nichtreste ungeraden Index. Diese Erkenntnisse aus dem Beispiel wollen wir jetzt allgemein beweisen.

Lemma 4.1. *Sei p eine ungerade Primzahl. Es gibt genau $\frac{p-1}{2}$ viele quadratische Reste und genauso viele quadratische Nichtreste.*

Beweis. Da $a^2 \equiv (p-a)^2 \pmod p$, gibt es höchstens $\frac{p-1}{2}$ viele quadratische Reste, nämlich die Quadrate von $1, 2, ...\frac{p-1}{2}$. Es bleibt zu zeigen, dass die Reste der Quadrate dieser Zahlen alle verschieden voneinander sind. Seien also $1 \leq a, b \leq \frac{p-1}{2}$ mit $a^2 \equiv b^2 \pmod p$. Das ist äquivalent zu $p \mid (a+b)(a-b)$ und, da p prim ist, zu $p \mid a+b$ oder $p \mid a-b$. Da $1 \leq a, b \leq \frac{p-1}{2}$, ist $2 \leq a+b \leq p-1$ und $p \mid a+b$ kann damit nicht gelten. Also muss $p \mid a-b$ erfüllt sein. Wiederum wegen der Wahl von a und b kann dies nur gelten, wenn $a-b=0$ ist, also $a=b$. Damit gibt es mindestens und höchstens $\frac{p-1}{2}$ quadratische Reste. Die übrigen $\frac{p-1}{2}$ Zahlen müssen die Nichtreste sein. □

Lemma 4.2. *Sei p eine ungerade Primzahl, ξ eine Primitivwurzel gemäß dem Satz aus dem letzten Abschnitt und* $\text{ind} = \text{ind}_p^\xi$ *die Indexfunktion modulo p bzgl. ξ. Dann gilt:*

$$\left(\frac{a}{p}\right) = (-1)^{\text{ind}(a)}$$

Beweis. Sei $\text{ind}(a)$ gerade, also $\text{ind}(a) = 2k$ für ein $k \in \mathbb{N}$. Dann gilt: $a \equiv \xi^{\text{ind}(a)} \equiv \xi^{2k} \equiv (\xi^k)^2 \pmod p$, d.h. a ist quadratischer Rest modulo p, also $\left(\frac{a}{p}\right) = 1$ und $(-1)^{\text{ind}(a)} = 1$, weil der Index gerade ist.
Da es nach dem letzten Lemma gleich viele quadratische Reste wie Nichtreste gibt, und es ebenfalls genau so viele Zahlen mit geradem wie ungeradem Index gibt, müssen die quadratischen Nichtreste die Zahlen mit ungeraden Index sein. □

Wir wollen nun im nächsten Unterabschnitt die ersten Kriterien für quadratische Reste herleiten.

4.1 Das Kriterium von Euler und der Ergänzungssatz für 2

Lemma 4.3. *Die Kongruenzgleichung $x^2 \equiv 1 \pmod p$ hat für eine Primzahl p nur die Lösungen 1 und -1.*

Beweis. $x^2 \equiv 1 \pmod p \;\Leftrightarrow\; p \mid x^2 - 1 = (x+1)(x-1)$. Da p prim ist, teilt p schon einen der Faktoren, also gilt $x \equiv 1 \pmod p$ oder $x \equiv -1 \pmod p$. □

Lemma 4.4 (Eulersches Kriterium mit Folgerungen)**.** *Sei p eine ungerade Primzahl.*

(i) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, *und falls* $p \nmid b$ *auch* $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

(iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Beweis. Zu (i): Falls $a \equiv 0 \pmod{p}$, so gilt (i) trivialerweise. Falls $a \not\equiv 0 \pmod{p}$, gilt nach dem Satz von Fermat

$$1 \equiv a^{p-1} = \left(a^{\frac{p-1}{2}}\right)^2 \pmod{p}$$

Nach Lemma 4.3 kann damit $a^{\frac{p-1}{2}}$ nur 1 oder -1 modulo p sein. Falls a quadratischer Rest modulo p ist, also $a \equiv b^2 \pmod{p}$ für ein b gilt, so gilt:

$$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \overset{\text{Fermat}}{\equiv} 1 \pmod{p}$$

Also sind $\left(\frac{a}{p}\right)$ und $a^{\frac{p-1}{2}}$ kongruent, falls a quadratischer Rest ist.
Sei nun a quadratischer Nichtrest modulo p und ξ eine Primitivwurzel modulo p, d.h. $\operatorname{ind}(a) = \operatorname{ind}_p^{\xi}(a)$ ist von der Form $2k+1$, $k \in \mathbb{N}_0$. Dann folgt:

$$a^{\frac{p-1}{2}} = (\xi^{2k+1})^{\frac{p-1}{2}} \equiv (\xi^{2k})^{\frac{p-1}{2}} \cdot \xi^{\frac{p-1}{2}} \equiv \xi^{p-1}\xi^{\frac{p-1}{2}} \equiv \xi^{\frac{p-1}{2}} \pmod{p}$$

Wegen obiger Überlegung muss das Ergebnis kongruent zu 1 oder -1 sein. Da aber ξ eine Primitivwurzel modulo p ist, kann nicht $\xi^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ gelten. Also gilt auch für quadratische Nichtreste a das Eulersche Kriterium.

Zu (ii): Durch mehrmaliges Anwenden von (i) erhält man:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$$

Da nur die Werte 1 und -1 angenommen werden, gilt hier nicht nur Kongruenz, sondern sogar Gleichheit.

(iii) ist nur die Anwendung des Eulerschen Kriteriums auf $a = -1$. □

Für den Beweis des Reziprozitätsgesetzes ist das folgende Lemma zwar nicht wichtig, jedoch benötigen wir es an späterer Stelle.

Lemma 4.5. -1 *ist genau dann ein quadratischer Rest modulo* 2^k*, wenn* $k = 1$.

Beweis. Falls $k = 1$ ist, so gilt $-1 \equiv 1 \equiv 1^2 \pmod{2}$ und deswegen ist -1 ein quadratischer Rest. Sei nun $k \geq 2$ und -1 ein quadratischer Rest modulo 2^k. Dann ist wegen $k \equiv 2$ die 4 ein Teiler von 2^k und -1 ist somit auch modulo 4 ein quadratischer Rest. Dies ist aber nicht möglich, wie man durch Berechnung der Quadrate von $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ modulo 4 einsieht. □

Bevor nun das Quadratische Reziprozitätsgesetz für ungerade Primzahlen beweisen, wollen wir den Ergänzungssatz für die 2 erklären.

Satz 4.1 (siehe [8], Lemma 8.6)**.** *Für eine ungerade Primzahl p gilt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$$

Beweis. Wir benutzen das Eulersche Kriterium $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}}$. Wir gehen nun kurzzeitig in den Ring $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$. Das hat den Grund, dass die 2 dort keine Primzahl ist, sondern sich als Produkt $2 = (-i)(1+i)^2$ darstellen lässt. Damit gilt mithilfe der Identität $(1+i)^p \equiv 1 + i^p \pmod p$ (siehe [8], Lemma 4.6):

$$\begin{aligned}\left(\frac{2}{p}\right) &\equiv 2^{\frac{p-1}{2}} = \left((-i)(1+i)^2\right)^{\frac{p-1}{2}} = (-i)^{\frac{p-1}{2}}(1+i)^{p-1} = \frac{(-i)^{\frac{p-1}{2}}}{1+i}(1+i)^p \\ &\equiv \frac{(-i)^{\frac{p-1}{2}}}{1+i}(1+i^p) = \frac{(-i)^{\frac{p-1}{2}}(1-i)}{(1+i)(1-i)}(1+i^p) = \frac{(-i)^{\frac{p-1}{2}} + (-i)^{\frac{p+1}{2}}}{2}(1+i^p) \pmod p.\end{aligned}$$

Es gilt $i^4 = 1$, das heißt im Zähler des Bruches treten nur die Werte $1, i, -1, -i$ auf, und zwar in Abhängigkeit davon, ob $\frac{p-1}{2}$ bzw. $\frac{p+1}{2}$ den Rest $0, 1, 2$ oder 3 modulo 4 hat, was gleichbedeutend damit ist, dass $p-1$ bzw. $p+1$ den Rest $0, 2, 4, 6$ modulo 8 hat. Wenn nun $p \equiv \pm 1 \pmod 8$ ist, ergibt sich als Ergebnis +1, bei $p \equiv \pm 3 \pmod 8$ gerade -1. Da auf linker und rechter Seite nur 1 oder -1 steht und $1 \not\equiv -1 \pmod p$ ist, wird aus der Kongruenz eine Gleichheit und man hat die Gleichheit von linkem und rechtem Term der Behauptung gezeigt.

Es bleibt also zu zeigen, dass der Term $(-1)^{\frac{p^2-1}{8}}$ genau die gleichen Werte erzeugt. Das rechnet man aber einfach nach, in dem man für p wiederum die Reste $1, 3, 5, 7 \pmod 8$ einsetzt. □

4.2 Beweis des quadratischen Reziprozitätsgesetzes mithilfe von Gauß-Summen

Satz 4.2 (Quadratisches Reziprozitätsgesetz)**.** *Seien p und q verschiedene ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Für den Beweis benutzen wir die sogenannten Gaußsummen, die in der folgenden Definition eingeführt und im darauffolgenden Lemma charakterisiert werden. Das Lemma werden wir hier aus Platzgründen nicht beweisen, sondern nur den Beweis des Reziprozitätsgesetzes geben.

Definition 4.2 (siehe [8])**.** Sei p eine ungerade Primzahl und $\xi \in \mathbb{C}$ eine primitive p-te Einheitswurzel, d.h. $\xi = \exp(\frac{2\pi i}{p})$. Dann ist für $a \in \mathbb{Z}$ mit $p \nmid a$ die Gaußsumme g_a durch

$$g_a = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \xi^{ak}$$

gegeben.

Wir rechnen nun im Ring

$$\begin{aligned}\mathbb{Z}[\xi] &= \mathbb{Z}[\xi, \xi^2, ..., \xi^{p-1}] \\ &= \{a_0 + a_1\xi + ... + a_{p-1}\xi^{p-1} \mid a_i \in \mathbb{Z}\ \forall\, i = 0, ..., p-1\} = \bigoplus_{k=0}^{p-1} \xi^k\mathbb{Z}\end{aligned}$$

Man kann auf diesem Ring ebenfalls Kongruenz modulo q definieren, indem man alle Koeffizienten a_i modulo q betrachtet. Schnell kann man überprüfen, dass man mit diesem Kongruenzbegriff genauso umgehen kann wie mit dem üblichen in $\mathbb{Z}$, also dass aus $a \equiv b \pmod q$ (in $\mathbb{Z}[\xi]$) und $d \equiv e \pmod q$, $n \in \mathbb{N}$ stets $a + d \equiv b + e, ad \equiv be$ und $a^n \equiv b^n \pmod q$ folgt.

Lemma 4.6. *Seien $p \neq q$ ungerade Primzahlen und $a \not\equiv 0 \pmod{p}$. Dann gilt:*

1. $g_a = \left(\frac{a}{p}\right) g_1$,
2. $g_1^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p =: p^*$,
3. $g_1^q \equiv g_q \pmod{q}$.

Beweis. Kann in [8], Lemma 8.9, nachgelesen werden. □

Beweis des Quadratischen Reziprozitätsgesetzes. Wir beginnen mit $\left(\frac{q}{p}\right) g_1$ und formen dies modulo q in $\mathbb{Z}[\xi]$ um (die Hinweise (i), (ii) und (iii) beziehen sich auf Lemma 4.6):

$$\left(\frac{q}{p}\right) g_1 \overset{(i)}{=} g_q \overset{(iii)}{\equiv} g_1^q = g_1 \left(g_1^2\right)^{\frac{q-1}{2}} \overset{(ii)}{=} g_1 {p^*}^{\frac{q-1}{2}} \overset{Euler}{\equiv} g_1 \left(\frac{p^*}{q}\right) \pmod{q}$$

Nun multiplizieren wir beide Seiten mit g_1 und erhalten wegen $g_1^2 = p^*$ schließlich

$$p^* \left(\frac{q}{p}\right) \equiv p^* \left(\frac{p^*}{q}\right) \pmod{q}.$$

Rechts und links befinden sich nur ganze Zahlen, das heißt, wir können vom Ring $\mathbb{Z}[\xi]$ wieder zu $\mathbb{Z}$ zurückkehren. Da $p^* = p \cdot (-1)^{\frac{p-1}{2}}$ und $p \neq q$, ist $p^* \not\equiv 0 \pmod{q}$, also kann man p^* kürzen und mit den Regeln (ii) und (iii) von Lemma 4.4 weiterrechnen:

$$\begin{aligned}\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) &\overset{\text{Def. } p^*}{=} \left(\frac{p(-1)^{\frac{p-1}{2}}}{q}\right) \overset{(ii)}{=} \left(\frac{p}{q}\right)\left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \\ &\overset{(iii)}{=} \left(\frac{p}{q}\right)\left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod{q}\end{aligned}$$

Rechte und linke Seite sind also kongruent modulo q. Da die auftretenden Werte aber nur 1 oder -1 sind, muss sogar Gleichheit gelten, da $1 \not\equiv -1 \pmod{q}$ mit $q > 2$. Daraus folgt durch Multiplizieren mit $\left(\frac{p}{q}\right)$ die Behauptung. □

4.3 Das Lemma von Gauß und ein kombinatorischer Beweis des quadratischen Reziprozitätsgesetzes

Hier orientieren wir uns an [6].

Lemma 4.7 (Lemma von Gauß)**.** *Sei p eine ungerade Primzahl und a mit $(a,p) = 1$. Betrachte die Zahlen $a, 2a, ..., \frac{p-1}{2}a$ und ihre (kleinsten) Reste* mod$p$. *Sei s die Anzahl der Zahlen, die Rest $> \frac{p}{2}$ haben. Dann gilt:*

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Beweis. Sei für den Beweis $b = \frac{p-1}{2}$.
Zunächst gilt $ak \not\equiv aj \pmod{p}$ für $k \neq j$, $1 \leq k, j \leq b$, denn wegen der Teilerfremdheit von a und p würde aus $ak \equiv aj \pmod{p}$ dann $k \equiv j \pmod{p}$ und wegen $1 \leq k, j \leq b < p$ sogar $k = j$ folgen. Alle Reste sind also verschieden.
Nun seien $u_1, ..., u_s$ die Reste, welche größer als $\frac{p}{2}$ sind, und $v_1, ...v_t$ die anderen. Es ist also $s+t = b$. Dann gilt $v_i \neq p - u_j$ für alle $1 \leq i, j \leq b$, denn sei $v_i \equiv la \pmod{p}$ und $u_i \equiv ka \pmod{p}$, dann

würde $la \equiv p-ka \pmod p$ gelten. Das bedeutet aber $p \mid a(l+k)$ und wegen $(a,p)=1$ auch $p \mid l+k$. Wegen $1 \leq l,k \leq b$ ist dies aber nicht möglich. Also handelt es sich auch bei $p-u_1,...,p-u_s,v_1,...,v_t$ um b verschiedene Reste.
Die v_i sind per Definition kleiner als $\frac{p}{2}$ und wegen $u_i > \frac{p}{2}$ ist $p-u_i < \frac{p}{2}$. Da somit die $s+t=b$ vielen Zahlen $p-u_1,...,p-u_s,v_1,...,v_t$ alle verschieden und $< \frac{p}{2}$, also $\leq b$ sind, stellen sie die Zahlen $1,2...,b$ in irgendeiner Reihenfolge dar. Damit folgt modulo p gerechnet:

$$\begin{aligned} b! &= \prod_{i=1}^{s}(p-u_i)\prod_{i=1}^{t}v_i \equiv \prod_{i=1}^{s}(-u_i)\prod_{i=1}^{t}v_i \equiv (-1)^s\prod_{i=1}^{s}u_i\prod_{i=1}^{t}v_i \\ &\equiv (-1)^s\prod_{j=1}^{b}ja \equiv (-1)^s a^b\prod_{j=1}^{b}j = (-s)^s a^b b! \pmod p \end{aligned}$$

Weil p prim ist, sind alle $j<p$ teilerfremd zu p und damit auch $b!$. Also kann man $b!$ nach Lemma 3.4 kürzen und erhält $1 \equiv (-1)^s a^b$, was wegen dem Eulerschen Kriterium äquivalent ist zu

$$(-1)^s \equiv a^b = a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Weil linke und rechte Seite nur 1 oder -1 sein können und wegen $p>2$ auch $1 \not\equiv -1 \pmod p$ gilt, gilt hier sogar Gleichheit. □

Lemma 4.8. *Sei p eine ungerade Primzahl und a mit $(a,2p)=1$. Dann gilt*

$$\left(\frac{a}{p}\right) = (-1)^w \quad \textit{mit } w = \sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{ja}{p}\right\rfloor$$

Beweis. Aus $(a,2p)=1$ folgt, dass a ungerade ist.
Wir benutzen dieselben Bezeichnungen b, $u_1,...,u_s,v_1,...,v_t$ wie im Lemma von Gauß. Nach der Division mit Rest (Lemma 3.3) gilt $ja = p\left\lfloor\frac{ja}{p}\right\rfloor + r_j$, wobei $r_j \in \{u_1,...,u_s,v_1,...,v_t\}$ nach Definition der u_i und v_i. Also gilt

$$\sum_{j=1}^{b}ja = \sum_{j=1}^{b}p\left\lfloor\frac{ja}{p}\right\rfloor + \sum_{j=1}^{b}r_j = p\sum_{j=1}^{b}\left\lfloor\frac{ja}{p}\right\rfloor + \sum_{i=1}^{s}u_i + \sum_{i=1}^{t}v_j = pw + \sum_{i=1}^{s}u_i + \sum_{i=1}^{t}v_j \tag{2}$$

und da, wie im Beweis des letzten Lemmas gezeigt, $p-u_1,...,p-u_s,v_1,...,v_t$ die Zahlen $1,...,b$ darstellen, gilt ebenso

$$\sum_{j=1}^{b}j = \sum_{j=1}^{s}(p-u_j) + \sum_{j=1}^{t}v_j = sp - \sum_{j=1}^{s}u_j + \sum_{j=1}^{t}v_j \tag{3}$$

Durch Subtraktion von (3) von (2) folgt

$$(a-1)\sum_{j=1}^{b}j = p(w-s) + 2\sum_{j=1}^{s}u_j.$$

Da $(a-1)$ gerade ist, $2\sum_{j=1}^{s}u_j$ ebenso, muss auch $p(w-s)$ gerade sein. Weil p ungerade ist, heißt das, dass w und s entweder beide gerade oder beide ungerade sind, also folgt mit dem Lemma von Gauß

$$(-1)^w = (-1)^s = \left(\frac{a}{p}\right).$$

□

Satz 4.3 (Quadratisches Reziprozitätsgesetz)**.** *Seien p und q verschiedene ungerade Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Beweis. Definiere die Menge von Paaren $\sigma = \{(x,y) : 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}\}$ und die beiden Teilmengen $\sigma_1 = \{(x,y) \in \sigma : qx > py\}$ und $\sigma_2 = \{(x,y) \in \sigma : qx < py\}$. Für *kein* Paar $(x,y) \in \sigma$ kann $qx = py$ gelten, weil sonst wegen der Teilerfremdheit von p und q dann $p \mid x$ und $q \mid y$ gelten müsste, was für $(x,y) \in \sigma$ nicht möglich ist. Also sind σ_1 und σ_2 nach Definition disjunkt und ergeben vereinigt ganz σ:

$$\sigma = \sigma_1 \dot\cup \sigma_2 \quad \text{und} \quad |\sigma| = |\sigma_1| + |\sigma_2| \tag{4}$$

Ferner berechnet sich $|\sigma|$ durch $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Wir bestimmen nun die beiden Größen $|\sigma_1|$ und $|\sigma_2|$. Für festes x liegen in σ_1 alle (x,y) mit $y < \frac{qx}{p}$, das sind $\left\lfloor \frac{qx}{p} \right\rfloor$ viele verschiedene. Also ist

$$|\sigma_1| = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor =: w_1$$

wofür nach dem letzten Lemma $\left(\frac{q}{p}\right) = (-1)^{w_1}$ gilt. Analog gilt

$$|\sigma_1| = \sum_{y=1}^{\frac{p-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor =: w_2$$

mit $\left(\frac{p}{q}\right) = (-1)^{w_2}$. Wegen (4) gilt also

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{w_1}(-1)^{w_2} = (-1)^{|\sigma_1|+|\sigma_2|} = (-1)^{|\sigma|} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

□

Auf den entsprechenden Beweis des Ergänzungssatzes verzichten wir hier aus Platzgründen, da wir ihn im letzten Unterabschnitt schon bewiesen haben. Eine Version, die das Lemma von Gauß benutzt, ist in [6] nachzulesen.

5 P_a-Zahlen

Definition 5.1. Für jedes $a \ge 2$ besteht die Menge $P_a \subset \mathbb{N}$ aus allen Teilern von Zahlen der Form $a^n + 1$, d.h.

$$P_a := \{d : \ \exists\, n \text{ mit } d \mid a^n + 1\} = \{d : \ \exists\, n \text{ mit } a^n \equiv -1 \pmod d\}.$$

Wir nennen die Elemente von P_a „gut für a“ (siehe Pieter Moree, [7]). Moree betrachtet dort die Teiler von $a^k + b^k$ und nennt diese „good numbers“. Unsere P_a-Zahlen sind also der Spezialfall für $b = 1$.

Nehmen wir beispielsweise als Basis $a = 2$, so berechnet man die Zahlen $2^1 + 1 = 3$, $2^2 + 1 = 5$, $2^3 + 1 = 9$, $2^4 + 1 = 17$, $2^5 + 1 = 33$ usw. und schreibt alle ihre Teiler $1, 3, 5, 9, 17, 11, 33, \ldots$ (diese

heißen dann gut für 2) in die Menge P_2. Sortiert man die auftretenden Teiler, so sind die ersten 20 Elemente von P_2 die folgenden:

$$1, 3, 5, 9, 11, 13, 17, 19, 25, 27, 29, 33, 37, 41, 43, 53, 57, 59, 61, 65.$$

P_2 enthält natürlich nur ungerade Zahlen, da $2^n + 1$ für $n > 0$ nur ungerade Werte annimmt und die Teiler damit auch ungerade sein müssen. Die Elemente der Menge P_3 hingegen können auch gerade sein.

Betrachtet man die Auflistung der Elemente von P_2, könnte einem auffallen, dass die 7 und die 15 nicht enthalten sind, alle anderen ungeraden Zahlen in diesem Bereich jedoch schon. Warum ist die 7 nicht gut für 2? Nun, damit 7 gut für 2 ist, muss es ein n geben mit $7 \mid 2^n + 1$. Ausgedrückt mit den Mitteln der Kongruenzrechnung heißt das $2^n + 1 \equiv 0 \pmod 7$ oder $2^n \equiv -1 \equiv 6 \pmod 7$. Betrachtet man nun aber die Zweierpotenzen modulo 7

$$\begin{aligned}
n = 1 &: \quad 2^1 = 2 \equiv 2 \pmod 7 \\
n = 2 &: \quad 2^2 = 4 \equiv 4 \pmod 7 \\
n = 3 &: \quad 2^3 = 8 \equiv 1 \pmod 7 \\
n = 4 &: \quad 2^4 = 16 \equiv 2 \pmod 7 \\
n = 5 &: \quad 2^5 = 32 \equiv 4 \pmod 7 \\
n = 6 &: \quad 2^6 = 64 \equiv 1 \pmod 7
\end{aligned}$$

so fällt auf, dass nur die Werte 2,4,1 angenommen werden, nicht jedoch der benötigte Rest -1. Die Reste von 2^n modulo 7 wiederholen sich in einem Dreierzyklus (2,4,1) und nehmen deshalb nie den Wert -1 an (die Ordnung von 2 modulo 7 ist 3). Auch die 15 ist nicht gut für 2, obwohl immerhin alle ihre Teiler 1,3 und 5 enthalten sind. Woran das liegt, wird in Abschnitt 5.2.4 erklärt.
Bevor wir uns der Frage widmen, wie man herausfinden kann, ob eine Zahl gut für a ist, wollen wir zunächst eine interessante Teilmengeneigenschaft zwischen den Mengen P_a zeigen.

5.1 Teilmengenbeziehungen für verschiedene Basen

Betrachten wir die Mengen P_2, P_4, P_8, P_{16}:

$$\begin{aligned}
P_2 &= \{3, 5, 9, 11, 13, 17, 19, 25, 27, 29, 33, 37, 41, 43, 53, 57, 59, 61, 65, 67, 81, ...\} \\
P_4 &= \{5, 13, 17, 25, 29, 37, 41, 53, 61, 65, 97, 101, 109, 113, 125, 137, 145, 149, ...\} \\
P_8 &= \{3, 5, 9, 11, 13, 17, 19, 25, 27, 29, 33, 37, 41, 43, 53, 57, 59, 61, 65, 67, 81, ...\} \\
P_{16} &= \{17, 97, 193, 241, 257, 289, 353, 401, 433, 449, 577, 641, 673, 769, 929, ...\}
\end{aligned}$$

Es fällt auf, dass in P_2 und P_8 exakt die gleichen Zahlen zu sein scheinen. P_4 hingegen ist eine echte Teilmenge von P_2 und P_{16} wiederum eine von P_4. Anders gesprochen, kann eine Zahl für 4 nur gut sein, wenn sie auch für 2 gut ist. Die Entdeckungen wollen wir nun etwas allgemeiner im nächsten Satz festhalten.

Satz 5.1. *Sei $a \geq 2$. Dann gilt für alle e stets $P_{a^e} \subseteq P_a$. Mengengleichheit gilt genau dann, wenn e ungerade ist.*

Beweis. Sei also $d \in P_{a^e}$. Nach Definition gibt es ein n mit $d \mid (a^e)^n + 1$ bzw. $(a^e)^n \equiv -1 \pmod d$. Das heißt aber $a^{en} \equiv -1 \pmod d$, also $d \mid a^{e \cdot n} + 1$. Also liegt d nach Definition in P_a. Also gilt $P_{a^e} \subseteq P_a$.
Falls nun e ungerade ist, gilt auch die umgekehrte Richtung: Sei $d \in P_a$, das heißt für ein n ist

$a^n \equiv -1 \pmod{d}$. Wegen der Ungeradheit von e ist dann auch $(a^e)^n = (a^n)^e \equiv (-1)^e = -1 \pmod{d}$ und d liegt in P_{a^e} nach Definition.
Es bleibt zu zeigen, dass die Gleichheit tatsächlich nur gilt, wenn e ungerade ist. Sei dazu $e = 2k$ gerade und man betrachtet $d = a+1$. Da $d = a+1 \mid a^1+1$, liegt d in P_a. Aber für alle n ist $a+1$ kein Teiler von $(a^e)^n + 1$, denn wegen $a \equiv -1 \pmod{d}$ folgt

$$(a^e)^n + 1 = a^{2kn} + 1 \equiv (-1)^{2kn} + 1 \equiv 2 \not\equiv 0 \pmod{d}$$

falls $d > 2$ ist, also $a > 1$, was ja erfüllt ist. Das heißt, es gibt stets mindestens ein Element in P_a, welches nicht in P_{a^e} für gerades e liegt. □

5.2 Kriterien zur Bestimmung von P_a-Zahlen

Die Herleitung von Kriterien zur Bestimmung von P_a-Zahlen ist eines der wichtigsten Aufgaben in dieser Arbeit. Sie liefern die Grundlage für die Algorithmik der P_a-Zahlen und auch für den Vergleich mit Primzahlen im Abschnitt 5.6.

5.2.1 Notwendige Kriterien

Lemma 5.1. *Falls $d \in P_a$ und $t \mid d$, dann ist auch $t \in P_a$.*

Beweis. Für ein gewisses n ist d Teiler von $a^n + 1$. Da $t \mid d$ gilt, folgt auch $t \mid a^n + 1$, also $t \in P_a$ nach Definition. □

Lemma 5.2. *Falls $d \in P_a$, dann ist $(a, d) = 1$.*

Beweis. Sei t ein gemeinsamer Teiler von a und d. Da $d \mid a^n + 1$ für ein n und $t \mid d$, folgt $t \mid a^n + 1$ (1). Wegen $t \mid a$ folgt auch $t \mid a^n$ (2). Wegen (1) und (2) muss t also auch die Differenz teilen: $t \mid 1$. Also ist jeder gemeinsame Teiler 1 oder -1 und $(a, d) = 1$. □

Diese beiden Lemmata werden meistens in umgekehrter Richtung als Ausschlusskriterium genutzt: Wenn der ggT nicht 1 ist, kann d nicht gut für a sein. Entsprechend müssen alle Teiler von d gut sein, sonst kann d selbst auch nicht gut für a sein.

5.2.2 Kriterien in Verbindung mit der Ordnung

Die Kriterien in diesem Abschnitt werden uns durch die gesamte weitere Arbeit begleiten. Wir beginnen mit einem einfachen Lemma, welches die Periodizität der Potenzen a^n modulo d benutzt.

Lemma 5.3. *Falls $d \in P_a$, so gibt es ein $n \leq \mathrm{ord}_d(a)$ mit $d \mid a^n + 1$. Falls zusätzlich $d > 2$ ist, gilt sogar $n < \mathrm{ord}_d(a)$.*

Beweis. Da $d \in P_a$, existiert nach Definition ein c mit $d \mid a^c + 1$, also $a^c \equiv -1 \pmod{d}$. Das Lemma 3.6 besagt, dass $a^n \equiv -1 \pmod{d}$ genau dann gilt, wenn $n \equiv c \pmod{\mathrm{ord}_d(a)}$. Insbesondere gibt es ein n mit $0 < n \leq \mathrm{ord}_d(a)$, welches kongruent zu c ist [explizit angegeben ist dies $n = c - \left\lfloor \frac{c}{\mathrm{ord}_d(a)} \right\rfloor \mathrm{ord}_d(a)$], das ist das gesuchte n.
Zusatz: Angenommen, $d \in P_a$ und $n = \mathrm{ord}_d(a)$. Dann gilt also $a^n \equiv 1 \pmod{d}$, was äquivalent mit $d \mid a^n - 1$ ist. Nach der Voraussetzung gilt auch $d \mid a^n + 1$, also teilt d die Differenz der beiden: $d \mid 2$, also $d \leq 2$. □

Dieses unscheinbare Lemma beantwortet eine elementare Frage in der Algorithmik der P_a-Zahlen: Kann man in endlicher Zeit entscheiden, ob eine Zahl d gut für a ist? Denn ohne dieses Lemma konnte man prinzipiell so viele Terme der Form $a^n + 1$ ohne Erfolg auf Teilbarkeit durch d überprüfen wie man wollte, ohne dass man sich sicher sein konnte, ob vielleicht doch irgendwann

noch der passende Exponent kommt. Nun weiß man, dass man n nur bis $\mathrm{ord}_d(a)$ durchlaufen muss, was nach Korollar 3.2 höchstens $\varphi(d)$ ist und dieses höchstens $d-1$. Die Aussage des letzten Lemmas wollen wir nun noch verbessern.

Satz 5.2. *Sei $a \geq 2$, $d > 2$. Dann ist $d \in P_a$ genau dann, wenn $\mathrm{ord}_d(a)$ gerade ist und $d \mid a^c + 1$ für $c = \frac{\mathrm{ord}_d(a)}{2}$.*

Beweis. Sei $d \in P_a$ und $d > 2$. Dann existiert nach dem letzten Lemma (mit Zusatz) ein $n < \mathrm{ord}_d(a)$ mit $d \mid a^n + 1$, also $a^n \equiv -1 \pmod{d}$. Es gilt $a^{2n} = (a^n)^2 \equiv (-1)^2 = 1 \pmod{d}$, also muss $2n$ ein Vielfaches der Ordnung $\mathrm{ord}_d(a)$ sein. Aus $n < \mathrm{ord}_d(a)$ folgt $0 < 2n < 2\mathrm{ord}_d(a)$. Also muss $2n = \mathrm{ord}_d(a)$ gelten, weswegen die Ordnung gerade ist und $d \mid a^n + 1$ für $n = \frac{\mathrm{ord}_d(a)}{2}$.
Wenn umgekehrt die Ordnung gerade ist und $d \mid a^c + 1$ für $c = \frac{\mathrm{ord}_d(a)}{2}$ gilt, hat man natürlich das in der Definition geforderte n gefunden und $d \in P_a$ ist nach Definition erfüllt. □

Dieser Satz konkretisiert also die Aussage aus dem letzten Lemma: Statt aller Exponenten $n < \mathrm{ord}_d(a)$ ist im Grunde nur einziger zu überprüfen. Funktioniert es mit diesem nicht, so weiß man, dass auch kein anderer Exponent das gewünschte Ergebnis liefert.
Lässt man für d nur Primzahlen zu, wird die Aussage noch schöner, was der Autor allerdings erst nach einem Kommentar von Betreuer Prof. Maier bemerkt hat:

Satz 5.3. *Sei $a \geq 2$ und $d > 2$ eine Primzahl. Dann ist $d \in P_a$ genau dann, wenn $\mathrm{ord}_d(a)$ gerade ist.*

Beweis. Sei $\mathrm{ord}_d(a)$ gerade, sagen wir $\mathrm{ord}_d(a) = 2k$. Dann gilt $(a^k)^2 = a^{2k} \equiv 1 \pmod{d}$. Nach Lemma 4.3 kann a^k nur die Werte 1 oder -1 annehmen. Falls $a^k \equiv 1 \pmod{d}$ gelten würde, wäre das wegen $k < \mathrm{ord}_d(a)$ ein Widerspruch zur Definition der Ordnung. Also muss $a^k \equiv -1 \pmod{d}$ gelten, demnach ist $d \in P_a$.
Falls $\mathrm{ord}_d(a)$ nicht gerade ist, sagt schon der letzte Satz, dass $d \notin P_a$. □

5.2.3 Kriterien Potenzen betreffend

Lemma 5.4. *Sei $a \geq 2$ und $d > 2$ ungerade und $d \in P_a$. Dann gilt $d^n \in P_a$ für alle $n \in \mathbb{N}$.*

Beweis. Wir führen einen ähnlichen Beweis durch vollständige Induktion nach n wie im Lemma 3.9, nur unter schwächeren Voraussetzungen und Ergebnissen.
$n = 1$: Klar nach Voraussetzung.
$n \to n+1$: Es sei also $d^n \in P_a$ für ein gewisses n. Nach Definition existiert also ein c mit $d^n \mid a^c + 1$. Wir zeigen, dass

$$d^{n+1} \mid a^{cd} + 1.$$

Weil d ungerade ist, folgt mit der geometrischen Summenformel:

$$a^{cd} + 1 = (a^c)^d + 1 = -(-a^c)^d + 1 = -((-a^c)^d - 1) = -(-a^c - 1) \cdot \sum_{k=0}^{d-1} (-a^c)^k = (a^c + 1) \sum_{k=0}^{d-1} (-a^c)^k$$

Nun wissen wir, dass $(a^c + 1)$ schon durch d^n teilbar ist. Aus $d^n \mid a^c + 1$ folgt insbesondere $a^c \equiv -1 \pmod{d}$ und wegen

$$\sum_{k=0}^{d-1} (-a^c)^k \equiv \sum_{k=0}^{d-1} (-(-1))^k = \sum_{k=0}^{d-1} 1 = d \equiv 0 \pmod{d}$$

ist die Summe auch durch d teilbar. Insgesamt ist $a^{cd} + 1$ also durch d^{n+1} teilbar und damit $d^{n+1} \in P_a$. □

Die Aussage des letzten Lemmas ist nicht richtig für gerade Zahlen d. Auf den Fall $d = 2$ wird im nächsten Lemma eingegangen.

Lemma 5.5. *Es ist 2^k genau dann gut für a, wenn 2^k die Zahl $a + 1$ teilt.*

Beweis. Die Rückrichtung ist klar.
Sei also $2^k \in P_a$. Dann ist $(2^k, a) = 1$, a also ungerade. Im Falle $k = 1$, teilt 2^1 trivialerweise die gerade Zahl $a + 1$.
Sei nun $k > 1$. Wegen $\varphi(2^k) = 2^{k-1}$ und Korollar 3.2 gilt $\mathrm{ord}_{2^k}(a) = 2^l$ für ein l mit $0 \leq l \leq k-1$. Der Fall $l = 0$, also $\mathrm{ord}_{2^k}(a) = 1$ tritt nur ein, wenn $a \equiv 1 \pmod{2^k}$ erfüllt ist. Dann ist aber $a^n + 1 \equiv 1^n + 1 \equiv 2 \not\equiv 0 \pmod{2^k}$ für alle n und 2^k ist nicht gut für a.
Wenn nun $l > 0$ ist, muss nach Satz 5.2 gerade $2^k \mid a^{2^{l-1}} + 1$ gelten. Falls $l > 1$, ist $2^k \mid a^{2^{l-1}} + 1$ äquvialent zu

$$\left(a^{2^{l-2}}\right)^2 \equiv -1 \pmod{2^k}.$$

Also ist -1 ein quadratischer Rest modulo 2^k. Das ist aber nach Lemma 4.5 nur für $k = 1$ möglich. Widerspruch.
Es bleibt nur der Fall $l = 1$ übrig, in welchem $2^k \mid a^1 + 1$ gilt. Das wurde behauptet.

□

Lemma 5.6. *Seien $a, d \geq 2$ und $d \in P_a$. Dann ist $d \in P_{a^2}$, genau dann, wenn $\mathrm{ord}_d(a)$ durch 4 teilbar ist.*

Beweis. Sei $d \in P_a$. Dann ist (nach Satz 5.2) $\mathrm{ord}_d(a)$ gerade und wegen Lemma 3.7 folgt $\mathrm{ord}_d(a^2) = \frac{\mathrm{ord}_d(a)}{2}$. Unter diesen Voraussetzungen gelten mit Satz 5.2 die folgenden Äquivalenzen:

$$\begin{aligned} d \in P_{a^2} &\Leftrightarrow 2 \mid \mathrm{ord}_d(a^2) \text{ und } d \mid (a^2)^{\frac{\mathrm{ord}_d(a^2)}{2}} + 1 \\ &\Leftrightarrow 2 \mid \frac{\mathrm{ord}_d(a)}{2} \text{ und } d \mid a^{\mathrm{ord}_d(a^2)} + 1 = a^{\frac{\mathrm{ord}_d(a)}{2}} + 1 \Leftrightarrow 4 \mid \mathrm{ord}_d(a) \text{ und } d \in P_a \end{aligned}$$

□

5.2.4 Kriterien Produkte betreffend

Man weiß, dass alle Teiler einer P_a-Zahl wieder in P_a enthalten sind. Aber gilt es auch umgekehrt? Wenn d und e in P_a liegen, tut es dann auch ihr Produkt? Schon ein einfaches Beispiel zeigt, dass dies nicht immer der Fall ist: $3 \in P_2$, $5 \in P_2$, aber $15 \notin P_2$. Wann geht es aber? Die Antwort liefert der folgende schöne Satz. Er entstand aus einer Bemerkung von Prof. Maier, dass aus $d_1, d_2 \in P_a$ für zwei Primzahlen d_1, d_2 mit $d_1, d_2 \equiv 3 \pmod 8$ stets $d_1 d_2 \in P_a$ folgt.

Satz 5.4. *Das Produkt $d \cdot e$ zweier teilerfremder Zahlen d und e liegt genau dann in P_a, wenn d und e in P_a liegen und*

$$h_2(\mathrm{ord}_d(a)) = h_2(\mathrm{ord}_e(a))$$

gilt.

Beweis. Wir beweisen den Satz über mehrere Äquivalenzumformungen.
Sei $d \cdot e \in P_a$. Das ist per Definition äquivalent zu

$$\exists\, c: \quad de \mid a^c + 1, \text{ d.h. } a^c \equiv -1 \pmod{de}$$

Wegen der Teilerfremdheit von d und e ist dies gleichbedeutend mit

$$\exists\, c: \quad a^c \equiv -1 \pmod{d} \quad \text{und} \quad a^c \equiv -1 \pmod{e}$$

Mit der Definition von P_a und der Tatsache, dass $a^x \equiv -1 \pmod{d}$ nur dann gelten kann, wenn $x \equiv \frac{\mathrm{ord}_d(a)}{2} \pmod{\mathrm{ord}_d(a)}$, ist dies wiederum äquivalent zu:
$d, e \in P_a$ und das lineare Kongruenzsystem

$$x \equiv c_1 := \frac{\mathrm{ord}_d(a)}{2} \pmod{\mathrm{ord}_d(a)}$$
$$x \equiv c_2 := \frac{\mathrm{ord}_e(a)}{2} \pmod{\mathrm{ord}_e(a)}$$

hat eine Lösung. Nach dem Chinesischen Restsatz ist das äquivalent zu:
$d, e \in P_a$ und $g = (\mathrm{ord}_d(a), \mathrm{ord}_e(a))$ teilt die Differenz $c_1 - c_2$. Setzt man $\mathrm{ord}_d(a) = g \cdot s$ und $\mathrm{ord}_e(a) = g \cdot t$ mit teilerfremden Zahlen s und t, ist die letzte Aussage wieder gleichbedeutend mit

$$g \mid c_1 - c_2 = \frac{1}{2} \cdot (gs - gt) = g \cdot \frac{s-t}{2}$$

was genau dann gilt, wenn $2 \mid s - t$. Das ist genau dann wahr, wenn s und t beide ungerade sind (wären beide gerade, wären sie nicht teilerfremd). Dazu äquivalent ist, dass die jeweils höchste Zweierpotenz von $\mathrm{ord}_d(a)$ und $\mathrm{ord}_e(a)$ schon in g steckt, d.h.

$$h_2(\mathrm{ord}_d(a)) = h_2(\mathrm{ord}_e(a)).$$

□

Bemerkung 5.1. Man kann auch zeigen, dass aus $h_2(\mathrm{ord}_d(a)) = h_2(\mathrm{ord}_e(a))$ für die Ordnung modulo des Produkts folgt:

$$h_2(\mathrm{ord}_{de}(a)) = h_2(\mathrm{ord}_d(a)) = h_2(\mathrm{ord}_e(a)).$$

Das liegt daran, dass wegen Lemma 3.8 $\mathrm{ord}_{de}(a)) = \mathrm{kgV}(\mathrm{ord}_d(a), \mathrm{ord}_e(a))$ gilt, und sich deswegen nichts an der höchsten enthaltenen Zweierpotenz ändert.

Satz 5.5. *Sei d eine natürliche Zahl mit Primfaktorzerlegung $d = 2^k \cdot \prod_{i=1}^m p_i^{k_i}$. Dann ist $d \in P_a$ genau dann, wenn gilt einer der folgenden Fälle gilt:*

- *$k = 0$ und es gibt ein $o > 0$ mit $h_2(\mathrm{ord}_{p_i}(a)) = o$ für alle $i = 1, ...m$.*
- *$k = 1$, a ist ungerade und es gibt ein $o > 0$ mit $h_2(\mathrm{ord}_{p_i}(a)) = o$ für alle $i = 1, ...m$.*
- *$k = 2$, $2^k \mid a + 1$ und $h_2(\mathrm{ord}_{p_i}(a)) = 1$ für alle $i = 1, ...m$.*

Beweis. Betrachten wir den Fall $k = 0$, d.h. d ist ungerade. Gäbe es dann zwei Primteiler p_i und p_j von d, für die $\mathrm{ord}_{p_i}(a)$ und $\mathrm{ord}_{p_j}(a)$ nicht die gleiche Zweierpotenz enthalten, so besagt der letzte Satz, dass $p_i p_j$ nicht gut für a ist und damit liegt auch d, was ein Vielfaches von $p_i p_j$ ist, nicht in P_a.
Falls nun andersrum alle Ordnungen die gleiche Zweierpotenz 2^o mit $o > 0$ enthalten, gilt: Nach Satz 5.3 sind alle p_i gut für a, nach Lemma 5.4 damit auch alle Potenzen $p_i^{k_i}$ und nach Satz 3.6 erfüllen die Ordnungen $\mathrm{ord}_{p_i^{k_i}}(a)$ ebenfalls $h_2(\mathrm{ord}_{p_i^{k_i}}(a)) = o$. Definiere $d_j = \prod_{i=1}^j p_i^{k_i}$ für $j = 1, ...m$, das heißt $d_1 = p_1^{k_1}$, $d_{j+1} = d_j \cdot p_{j+1}^{k_{j+1}}$ und $d_m = d$. Dann gilt:

$$d_j \in P_a \quad \text{und} \quad h_2(\mathrm{ord}_{d_j}(a)) = o \; \forall \, j = 1, ..., m$$

Das folgt induktiv aus dem letzten Satz und Lemma 3.8: Wenn die Aussage für ein j richtig ist, so gilt $h_2(\mathrm{ord}_{d_j}(a)) = o$ und $h_2(\mathrm{ord}_{p_{j+1}^{k_{j+1}}}(a)) = o$ und somit nach dem letzten Satz $d_{j+1} = d_j \cdot p_{j+1}^{k_{j+1}} \in P_a$. Nach der Bemerkung 5.1 gilt auch $h_2(\mathrm{ord}_{d_{j+1}}(a)) = o$. Das war genau die Behauptung, die im

Induktionsschritt zu zeigen war.
Schließlich gilt die Aussage auch für $j = m$ und somit liegt d in P_a.

Sei nun $k = 1$. Dann ist d gerade und kann nur dann gut für a sein, wenn a ungerade ist. Da $k = 1$ gilt, ist $\frac{d}{2} = \prod_{i=1}^{m} p_i^{k_i}$ ungerade und nach dem eben behandelten Fall genau dann in P_a, wenn die zweite Bedingung im Fall 2 erfüllt ist. Das heißt, es gibt ein n mit $\frac{d}{2} \mid a^n + 1$. Da a ungerade ist, ist $a^n + 1$ gerade und somit gilt nicht nur $\frac{d}{2} \mid a^n + 1$, sondern auch $d \mid a^n + 1$, also $d \in P_a$.

Zuletzt sei $k > 1$. Nach Lemma 5.5 ist $2^k \in P_a$ genau dann, wenn $a \equiv -1 \pmod{2^k}$, d.h. $2^k \mid a + 1$. Das ist nötig für $d \in P_a$, weil sonst nicht alle Teiler von d gut für a wären. Aus $2^k \mid a + 1 = a^1 + 1$ und Satz 5.2 folgt $\mathrm{ord}_{2^k}(a) = 2$.
Die Zahl $\frac{d}{2^k}$ ist ungerade und nach den Überlegungen im ersten Fall ($k = 0$) genau dann gut für a, wenn es ein $o > 0$ mit den aufgeführten Eigenschaften gibt. Insbesondere ist in diesem Fall dann $h_2(\mathrm{ord}_{d/2^k}(a)) = o$. Die Zahl $d = 2^k \cdot \frac{d}{2^k}$ ist nach Satz 5.4 genau dann gut für a, wenn für das oben gefundene o gerade $o = h_2(\mathrm{ord}_{d/2^k}(a)) = h_2(\mathrm{ord}_{2^k}(a)) = h_2(2) = 1$ gilt. Das ist die Behauptung. □

Dieser Satz liefert die theoretische Grundlage für den Algorithmus `4 BestSieve` (siehe Abschnitt 5.3.2) und damit für eine relativ effiziente Berechnung der P_a-Zahlen bis zu einer gewissen Zahl n. Darüber hinaus wird ein ähnliches Arguement auch bei der Charakterisierung der Menge Q_d für zusammengesetzte Zahlen d in Abschnitt 6.1.2 angewandt.

5.3 Algorithmik

In diesem Abschnitt soll der Frage nachgegangen werden, wie man P_a-Zahlen möglichst effizient berechnen kann. Effiziente Verfahren und Implementierungen derselben sind wichtig, um neue Vermutungen über P_a-Zahlen schnell überprüfen zu können. Außerdem stellen die Algorithmen eine schöne Anwendung der theoretischen Kriterien aus dem letzten Unterabschnitt dar.

Die Algorithmen sind in einem Pseudocode angegeben, können aber leicht selbst programmiert werden. Der Autor empfiehlt dafür Python, da es sich dabei um eine sehr einfache Sprache handelt, die trotzdem große Möglichkeiten bietet. Es lässt sich weitaus angenehmer programmieren als z.B. mit Maple und trotzdem kann Pyton ohne Weiteres mit beliebig großen Ganzzahlen rechnen. Mehr dazu unter http://www.python.org

5.3.1 Einfachste Berechnung

Der erste Algorithmus `2` (`isPaSimple`) testet auf Brute-Force-Weise, ob d in P_a liegt. Man erhöht Stück für Stück die Potenz a^n, bis n die Ordnung erreicht hat. Falls dabei irgendwann $d \mid a^n + 1$ erfüllt ist, terminiert der Algorithmus.

Eine Verbesserung kann man erreichen, indem man nicht alle Potenzen a^n bis $n = \frac{\mathrm{ord}_d(a)}{2}$ ausprobieren muss, sondern nur die Potenzen a^t mit $t \mid \varphi(d)$ (nach dem Kleinen Satz von Euler teilt $\mathrm{ord}_d(a)$ ja $\varphi(d)$). Den Wert einer Potenz a^t modulo d kann man am Besten mit dem sogenannten schnellen modularen Potenzieren errechnen. Dies kann zum Beispiel in [10], Abschnitt 7.5, nachgelesen werden.

5.3.2 Siebalgorithmen

Bevor wir uns wieder den P_a-Zahlen zuwenden, betrachten wir kurz die Aufgabe, herauszufinden, ob eine Zahl eine Primzahl ist: Das intuitivste Verfahren besteht darin, alle Zahlen unterhalb dieser Zahl zu testen, ob sie ein Teiler der betrachteten Zahl sind. Falls dies keiner ist, handelt es sich um eine Primzahl.

Algorithmus 2 : isPaSimple(a,d)

```
if ggT(a, d) ≠ 1 then
    return false;
end
if d = 2 then
    return isOdd(a);
end
power := a;
while rem(power, d) ≠ 1 do
    power := rem(power · a, d);
    if power = d − 1 then
        return true;
    end
end
return false;
```

Will man nun aber alle Primzahlen bis z.B. 1000 bestimmen, ist es ineffizient, das gerade beschriebene Verfahren für jede einzelne Zahl anzuwenden. Es ist jetzt besser, ein sogenanntes Sieb zu verwenden, das Eratosthenes zugeschrieben wird:

1. Man stelle sich eine Liste aller Zahlen von 1 bis N vor. 1 ist nicht prim, also streiche man sie durch.
   2 ist prim. Alle ihre echten Vielfachen können keine Primzahlen seien, weil sie durch 2 teilbar sind, also streiche alle Zweiervielfachen unter N durch.

2. Gehe zur nächsten nicht durchgestrichenen Zahl. Das ist eine Primzahl. Streiche wiederum alle ihre echten Vielfachen unter N heraus.

3. Wiederhole Schritt 2, bis man bei N angekommen ist. Alle nicht durchgestrichenen Zahlen sind Primzahlen.

Schöne Beschreibungen dazu finden sich in der Wikipedia.

Nun wollen wir untersuchen, in wie weit sich das ganze für P_a-Zahlen auch anwenden lässt. Wir wissen hier zunächst allerdings nur, dass die Vielfachen von Nicht-P_a-Zahlen auch keine P_a-Zahlen sein können. Das heißt, jedes Mal, wenn eine Zahl als nicht gut erkannt wurde, werden ihre Vielfachen ebenfalls gestrichen. Diese Idee ist im Algorithmus 3 (`badSieve`) umgesetzt. Der Name kommt daher, dass nur bei für a nicht-guten (also bösen) Zahlen die Vielfachen herausgeworfen werden.

Der Nachteil ist nun, dass man zwar bei Nicht-P_a-Zahlen alle Vielfachen herauswerfen kann, aber dafür bei guten Zahlen zunächst einmal nichts machen kann. Man benötigt den Satz 5.4, um zu entscheiden, wann das Produkt zweier guter Zahlen wieder gut ist. Im folgenden verbesserten Sieb wird das angewandt. Hier zunächst eine grobe Beschreibung:

- Man arbeitet mit drei Zuständen: P_a-Zahl (2), keine P_a-Zahl (1), unentschieden (0).
- Wie bisher: Sobald eine Zahl als nicht gut identifiziert wurde, werden alle ihre Vielfachen auf nicht gut (1) gesetzt.
- Wenn eine Zahl d gut ist, wird der Zweieranteil der Ordnung $\mathrm{ord}_d(a)$ abgespeichert. Außerdem bildet man das Produkt mit allen schon entschiedenen guten Zahlen, zu denen der gleiche Zweieranteil gehört und markiert dieses Produkt als gut (2). Das Produkt mit allen guten Zahlen, zu denen ein anderer Zweieranteil gehört, werden negativ (1) gekennzeichnet.

Algorithmus 3 : badSieve(N)

```
s:=array[1..N];
Initialisiere s mit 1ern;
p:=list();
i:=2;
while i ≤ N do
    if s[i] = 1 then
        if isPaSimple(a,i) then
            p.add(i);
        else
            for j := i to N by i do
                s[j] := 0; //i und alle Vielfachen streichen
            end
        end
    end
end
return p;
```

Diese Ideen sind in Algorithmus 4 (`BestSieve`) umgesetzt (etwas weniger explizit als die letzten beiden Algorithmen).

Ein Vergleich der Laufzeiten der Programme ist in Tabelle 3 zu finden. `simple` ist dabei einfach die iterative Anwendung von Algorithmus 2, `badSieve` das erste Sieb und die beiden weiteren kommen vom Algorithmus `BestSieve`. Der erste der beiden arbeitet allerdings mit einer Standard-Implementierung der Ordnung, während zweiterer ausnutzt, dass man nur die Ordnung modulo Primzahlen berechnen muss und tut dies sehr viel effizienter (Erklärung weiter unten). Der Zeitunterschied ist gewaltig und zeigt, dass ein sehr großer Teil der Arbeit darin besteht, die Ordnung von a modulo den Primzahlen zwischen 1 und n zu bestimmen.
Das zugehörige Python-Programm wurde dabei auf einem modernen Rechner mit vier Kernen laufen gelassen, wobei vermutlich nur ein Kern verwendet wurde. Interessant ist auch, dass sich `BestSieve` beinahe linear verhält. Für die Werte $n = 10^3, 10^4, 10^5, 10^6, 10^7, 10^8$ berechnete er die P_2-Zahlen bis n in den folgenden Sekundenzeiten $0.09, 0.107, 1.260, 15.363, 182.913, 2074.410$. Die anderen Verfahren weißen eher eine quadratische Zeitzunahme auf.

Was nun macht den `BestSieve`-Algorithmus so gut gegenüber den anderen Verfahren? Dadurch, dass in jedem Fall für die meisten Vielfachen der momentanen Zahl bereits sofort entschieden werden kann, ob diese gut sind, bleiben nur noch die Primzahlen übrig, die man darauf prüfen muss, ob sie in P_a liegen. Man weiß, dass die Ordnung den Wert $\varphi(p) = p - 1$ teilen muss und da der entscheidende Exponent $c = \frac{\mathrm{ord}_p(a)}{2}$ damit auch ein Teiler von $\varphi(p) = p - 1$ ist, muss man nur diese Teiler überprüfen. Das geht am Besten mit dem schnellen modularen Potenzieren. Speichert man dabei schon berechnete Potenzen ab und verwendet sie bei erneutem Auftreten wieder, so holt man das Optimum an Geschwindigkeit heraus. Nachteil des Verfahrens ist, dass man für alle Primzahlen p die Teiler von $\varphi(p) = p - 1$ bestimmen muss. Dies kann zu Beginn erledigt werden und ist – wenn richtig implementiert – vergleichsweise schnell im Vergleich zum restlichen Programm. Eine ausführliche Beschreibung der konkreten Implementierung würde hier zu viel Platz in Anspruch nehmen. Interessierte Leser können sich gerne über `matthias.heinlein@uni-ulm.de` an den Autor wenden, er wird die Python-Codes gerne zusenden oder Fragen beantworten.

Nachdem wir nun alle wichtigen Kriterien für P_a-Zahlen erklärt haben und wie man diese algorithmisch umsetzt, wollen wir uns nun dem spannendsten Teil widmen: Dem Vergleich mit Primzahlen.

Algorithmus 4 : BestSieve(a,N)

```
s :=array(1..N); //mit 0 initialisiert
orders:=array(1..N);
if a ungerade then
    k := h_2(a + 1); //k ist somit Exponent der höchsten Zweierpotenz, die in P_a liegt
    for l = 1..k mit 2^l ≤ N do
        s[2^l] := 2;
        orders[2^l] = h_2(ord_{2^l}(a));
    end
    for l ≥ k + 1 mit 2^l ≤ N do
        Streiche alle Vielfachen von 2^l (d.h. auf 1 setzen);
    end
else
    Streiche alle geraden Zahlen;
end
for d=3..N do
    if s[d] ≠ 0 then
        d wurde schon bearbeitet, weiter zum nächsten d;
    end
    if ggT(a, d) ≠ 1 then
        Streiche d und alle Vielfachen von d;
    end
    //d ist jetzt prim;
    o :=primeOrder(a, d);
    k := h_2(o);
    if k = 0 then
        //d.h. ord ist ungerade
        Streiche alle Vielfachen von d und weiter zum nächsten d;
    end
    l_1 := {e mit s[e] = 2 und orders[a] = k};
    l_2 := {e mit s[e] = 2 und orders[a] ≠ k};
    for (e, t) ∈ l_1 × ℕ mit e · d^t < N do
        s[e · d^t] := 2 ;
        orders[e · d^t] := k;
    end
    for e ∈ l_2 mit e · d ≤ N do
        Streiche d · e und alle Vielfachen davon;
    end
end
```

n	simple	badSieve	BestSieveBad	BestSieve
1000	0.037	0.016	0.012	0.009
10000	1.388	0.887	0.776	0.107
100000	118.341	71.340	58.865	1.270

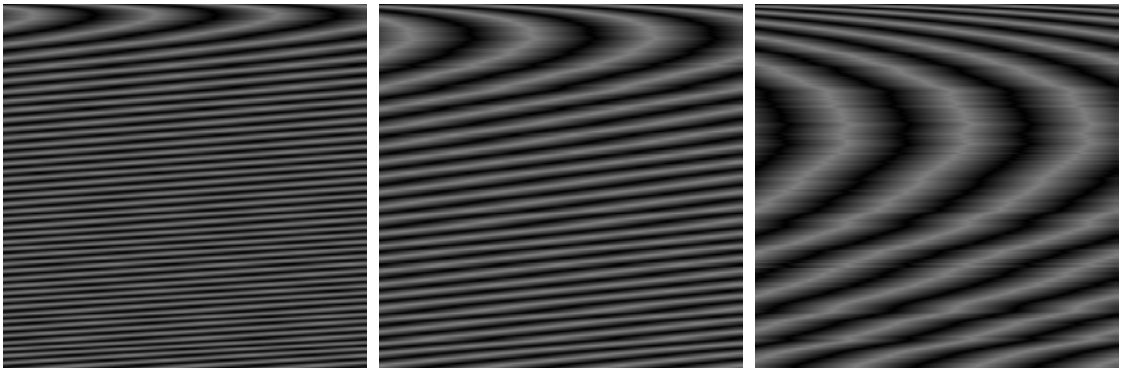
Tabelle 3: Laufzeiten in Sekunden der verschiedenen Algorithmen für $P_2 \cap \{1, ..., n\}$

5.4 Vergleich mit Primzahlen

Wie in der Einleitung erwähnt, entwickelte sich die Idee der P_a-Zahlen aus der Untersuchung von Termen der Form $a^n + 1$ auf Teilbarkeit durch Potenzen d^k.

Schon zuvor hatte der Autor eine Visualisierung für Primzahlen und andere Zahlenmengen entwickelt, die sogenannte Woodstone-Visualisierung. Mit dieser Visualisierung kann man die Primzahlen in einem bestimmten Bereich der natürlichen Zahlen grafisch darstellen, wobei die „Schönheit“ der entstehenden Bildern noch von einem Parameter k abhängt. Wie die Visualisierung im Detail funktioniert, ist in aller Kürze im Anhang zu finden. Hier wollen wir lediglich einige Bilder dieser Visualisierung zeigen und die Verbindung mit P_a-Zahlen herstellen.

Die Primzahlen bis 250000 sehen in der Woodstone-Visualisierung wie in Abbildung 1 dargestellt aus.

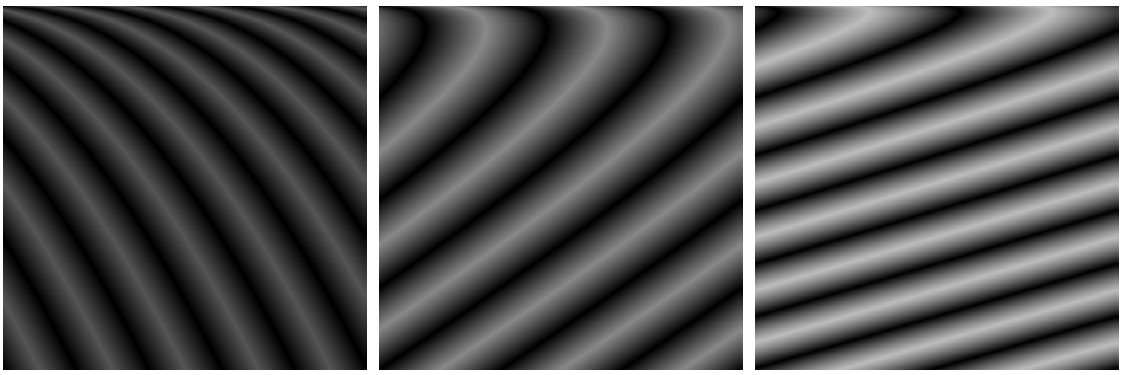


(a) $k = 74$ (b) $k = 75$ (c) $k = 76$

Abbildung 1: Primzahlen in Woodstone für verschiedene Parameter k

Man erkennt (für passenden Parameter k) ineinander geschobene Kurven, die an ihren Rändern sehr unscharf sind. Interessant ist aber, dass sich überhaupt Muster ergeben, wenn man bedenkt, dass die Primzahlen unregelmäßig angeordnet sind. Doch ähnlich wie auch der Primzahlsatz, suggeriert diese Visualisierung, dass die Primzahlen – betrachtet man sie „aus einiger Entfernung“ doch eine gewisse Regelmäßigkeit besitzen.

Genauso wie Primzahlen kann man auch andere Teilmengen der natürlichen Zahlen mit Woodstone visualisieren, so zum Beispiel in Abbildung 2 die Menge der Quadratzahlen bis 250000.



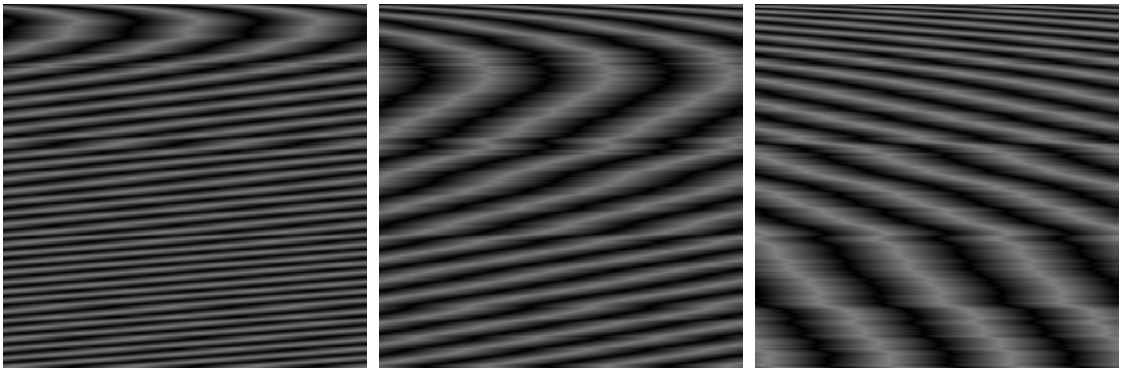
(a) $k = 50$ (b) $k = 83$ (c) $k = 124$

Abbildung 2: Quadratzahlen in Woodstone

Vergleicht man die Muster der Quadratzahlen mit denen der Primzahlen, so fällt auf, dass sie eine andere Form besitzen und sehr viel gleichmäßiger und vor allem schärfer aussehen. Das liegt natürlich daran, dass die Quadratzahlen im Vergleich zu den Primzahlen regelmäßig angeordnet sind. Man kann auf jeden Fall festhalten, dass sich nicht für alle denkbaren Zahlenmengen die gleichen Muster ergeben.

Weitere Zahlenmengen wie die Fibonaccizahlen wären denkbar, allerdings sieht man dabei im Bild keine auffälligen Linien, da es zu wenig Fibonaccizahlen unter den natürlichen Zahlen gibt.

Nachdem nun die P_a-Zahlen definiert waren, lag die Idee relativ nahe, auch diese mit Woodstone zu visualisieren. Einige Ergebnisse der Menge P_2 sind in der Abbildung 3 zu finden.



(a) $k = 72$ (b) $k = 73$ (c) $k = 74$

Abbildung 3: P_2-Zahlen in Woodstone

Interessanterweise ergeben sich ähnliche Muster wie beim Visualisieren der Primzahlen. Die Linien sind zwar noch unschärfer und unregelmäßiger, aber man kann eine Ähnlichkeit entdecken. Das ist sehr faszinierend und führte den Autor zu der zunächst sehr kühnen Vermutung, dass die P_a-Zahlen ähnlich verteilt sind wie Primzahlen (dazu ist es sinnvoll zu verstehen, wie die Visualierung erstellt wird, siehe Anhang). Es inspirierte ihn auch dazu, nach anderen Ähnlichkeiten zwischen P_a-Zahlen und Primzahlen zu suchen. Wir wollen im Folgenden drei wichtige Eigenschaften der Primzahlen auf P_a-Zahlen übertragen: Die Lücken zwischen aufeinanderfolgenden Zahlen, die Goldbachsche Vermutung und die Zwillingsvermutung.

5.5 Lücken in den Mengen $\mathbf{P_a}$

5.5.1 Lücken zwischen Primzahlen

Untersucht man die Verteilung der Primzahlen in den natürlichen Zahlen, so stellt man sich früher oder später die folgende Frage: Wie „nah“ können zwei aufeinanderfolgende Primzahlen zusammenliegen und wie „weit“ können sie höchstens von einander entfernt sein. Also: Was sind die größten und die kleinsten Lücken in der Folge der Primzahlen.

Die kleinsten Entfernungen (von der zwischen 2 und 3 abgesehen) sind sicherlich 2, sie treten bei sogenannten Primzahlzwillingen auf, z.B. 3 und 5, 5 und 7, 11 und 13, 17 und 19, ... Ungeklärt ist hier allerdings, ob es unendlich viele dieser Zwillinge gibt. Mit dieser Fragestellung, übertragen auf P_a-Zahlen, beschäftige ich mich in dieser Arbeit auch noch.

Die Frage nach den größten Lücken dagegen ist relativ leicht beantwortet: Es gibt keine größten Lücken. Oder anders:

Für jede natürliche Zahl n gibt es eine Zahl a sodass keine der Zahlen $a+1, a+2, ...a+n$ eine Primzahl ist. Der Beweis geht recht leicht: Definiere $a := (n+1)! + 1 = 2 \cdot 3 \cdot 4 \cdot ... \cdot n \cdot (n+1) + 1$.

Es ist $a+1 = (n+1)!+2$ durch 2 teilbar, $a+2 = (n+1)!+3$ durch 3 teilbar, schließlich $a+n = (n+1)!+(n+1)$ durch $n+1$ teilbar, also sind sie allesamt keine Primzahlen.

Die Frage nach beliebig großen Abständen wird nun auf P_a-Zahlen übertragen.

5.5.2 Idee des Vorgehens

In diesem Abschnitt soll zunächst anhand eines Beispiels gezeigt werden, wie man beweisen kann, dass es in den Mengen P_a beliebig große Lücken gibt.

Betrachten wir die Menge P_2. Beispielsweise wollen wir eine Lücke der Größe 5 finden, d.h. 5 aufeinanderfolgende Zahlen sollen nicht in P_2 liegen. Wie kann man – ähnlich wie bei den Primzahlen – bei einer Zahl sofort feststellen, dass sie keine P_a-Zahl ist? Dann, wenn sie das Vielfache einer Nicht-P_a-Zahl ist. Wir suchen eine Zahl x, sodass $x+1$ Vielfaches einer Nicht-P_a-Zahl p_1 ist, gleichzeitig $x+2$ das Vielfache einer Nicht-P_a-Zahl p_2 und schließlich $x+5$ Vielfaches einer Nicht-P_a-Zahl p_5, also:

$$\begin{array}{lll} x+1 \equiv 0 \pmod{p_1} & & x \equiv -1 \pmod{p_1} \\ x+2 \equiv 0 \pmod{p_2} & \text{oder} & x \equiv -2 \pmod{p_2} \\ \quad\ldots & & \quad\ldots \\ x+5 \equiv 0 \pmod{p_5} & & x \equiv -5 \pmod{p_5} \end{array}$$

Das sieht doch sehr nach dem Chinesischen Restsatz aus! Dieser garantiert uns eine Lösung x, wenn die Module $p_1, ..., p_5$ teilerfremd sind. Wir brauchen also fünf teilerfremde Zahlen, die nicht in P_2 liegen. Natürlich eignen sich dafür fünf Primzahlen, die nicht in P_a liegen, z.B. $7, 23, 31, 47, 89$. Der Chinesische Restsatz liefert dann in unserem Beispiel für x den Wert 4691630. Relativ sicher tritt in P_2 schon weitaus früher eine Lücke der Länge 5 auf. Wir sind aber mit dem obigen Resultat zufrieden, weil es uns sicherstellt, dass wenigstens irgendwann eine solche Lücke auftritt.

Wenn man also beweisen will, dass es in P_a Lücken der Länge n gibt, muss man n verschiedene Primzahlen finden, die nicht in P_a liegen, d.h. die Ordnung von a modulo p muss ungerade sein. Im Folgenden wollen wir beweisen, dass es zu jedem $a \geq 2$ stets unendlich viele Primzahlen p gibt, sodass die Ordnung $\mathrm{ord}_p(a)$ ungerade ist. Das vervollständigt dann die Überlegungen zu beliebig große Lücken in den P_a-Zahlen ab.

5.5.3 Unendlich viele Primzahlen mit ungerader Ordnung $\mathrm{ord}_\mathbf{d}(\mathbf{a})$

Hier orientieren wir uns am Vorgehen von W. Sierpinski in seinem kurzen Paper „Sur une decomposition des nombres premiers en deux classes“. Dort hat er gezeigt, dass es unendlich viele Primzahlen p gibt, für die $\mathrm{ord}_p(2)$ ungerade ist. Das wollen wir nun verallgemeinern.
Für $a \geq 2$ sei B_a die Menge aller Primteiler von $a^n - 1$ für ungerades n. Wir werden zeigen, dass B_a unendlich viele Element enthält und a bzgl. all dieser ungerade Ordnung hat.

Lemma 5.7. *Sei $a \geq 2$.*

(i) $a-1 \mid a^m - 1$ für alle $m \in \mathbb{N}$.

(ii) Wenn $d > 1$ ein Teiler von $a-1$ ist, dann gilt $(a-1)d \mid a^m - 1$ genau dann, wenn $d \mid m$.

Beweis. Teil (i) ist klar mit der geometrischen Summenformel:

$$a^m - 1 = (a-1)\sum_{k=0}^{m-1} a^k$$

Falls $a^m - 1$ nicht nur durch $a-1$, sondern sogar durch $d(a-1)$ mit $d \mid a-1$ teilbar wäre, dann teilt d also die Summe $\sum_{k=0}^{m-1} a^k$. Aus $d \mid a-1$ folgt $a \equiv 1 \pmod{d}$ und damit also:

$$\sum_{k=0}^{m-1} a^k \equiv \sum_{k=0}^{m-1} 1^k \equiv m \begin{cases} \equiv 0 \pmod{d} & \text{falls } d \mid m \\ \not\equiv 0 \pmod{d} & \text{sonst} \end{cases}$$

Damit gilt also $(a-1)d \mid a^m - 1$ genau dann, wenn $d \mid m$ gilt. □

Lemma 5.8. *Seien n und m teilerfremde natürliche Zahlen. Dann ist $a-1$ der größte gemeinsame Teiler von $a^n - 1$ und $a^m - 1$.*

Beweis. $a-1$ ist ein gemeinsamer Teiler, wie im letzten Lemma mit der geometrischen Summe begründet. Zu zeigen ist also, dass es kein $d > 1$ gibt, sodass $(a-1)d$ ein gemeinsamer Teiler von $a^n - 1$ und $a^m - 1$ ist.
Sei d ein solcher Teiler.
Fall 1: $d \mid a-1$. Dann besagt das letzte Lemma, Teil (ii), dass $d \mid n$ und $d \mid m$ gilt. Da $d > 1$, wären dann aber n und m nicht teilerfremd.
Fall 2: $d \nmid a-1$. Dann ist $a^1 = a \not\equiv 1 \pmod{d}$, also ist $\mathrm{ord}_d(a) > 1$. Da d gemeinsamer Teiler von $a^n - 1$ und $a^m - 1$ ist, folgt: $a^n \equiv 1 \pmod{d}$ und $a^m \equiv 1 \pmod{d}$, also muss sowohl n als auch m ein Vielfaches von $\mathrm{ord}_d(a)$ sein. Da $\mathrm{ord}_d(a) > 1$ also ein gemeinsamer Teiler von m und n ist, sind sie nicht teilerfremd. Widerspruch.
Also ist $a-1$ der größte gemeinsame Teiler von $a^n - 1$ und $a^m - 1$. □

Satz 5.6. *Zu jedem $a > 1$ gibt es unendlich viele Primzahlen p, für die $\mathrm{ord}_p(a)$ ungerade ist.*

Beweis. Der Beweis geht in zwei Schritten:

a) Für alle Elemente $p \in B_a$ ist $\mathrm{ord}_p(a)$ ungerade. Das gilt, weil zu $p \in B_a$ nach Definition eine ungerade Zahl n existiert, sodass $a^n \equiv 1 \pmod{d}$. Aus dieser Kongruenz folgt, dass die Ordnung $\mathrm{ord}_p(a)$ die ungerade Zahl n teilt, insbesondere muss $\mathrm{ord}_p(a)$ selbst ungerade sein.

b) B_a enthält unendlich viele Elemente. Beweis:
Wenn p eine ungerade Primzahl ist, dann sind alle Primteiler von $a^p - 1$ definitionsgemäß in B_a. Nach dem letzten Lemma ist der größte gemeinsame Teiler von $a^p - 1$ und $a^q - 1$ für zwei verschiedene ungerade Primzahlen p und q gerade $a-1$. Das heißt, alle Primteiler (außer denen von $a-1$) von $a^p - 1$ sind verschieden von den Primteilern von $a^q - 1$. Da es unendlich viele Primzahlen p gibt, gibt es also unendlich viele verschiedene Primteiler von $a^p - 1$. Somit ist B_a unendlich groß.

□

Zusammen mit den Überlegungen mit dem Chinesischen Restsatz im letzten Teilabschnitt ist nun vollständig bewiesen, dass es in jeder Menge P_a beliebig große Lücken zwischen aufeinanderfolgenden Elementen gibt.

5.5.4 Für welche Primzahlen hat eine Zahl ungerade Ordnung?

Im letzten Teilabschnitt haben wir bewiesen, dass es zu jedem $a \geq 2$ unendlich viele Primzahlen p gibt, für die $\mathrm{ord}_p(a)$ ungerade ist. Es ist ganz interessant, zu untersuchen, welche Primzahlen diese Eigenschaft haben. Zwar ist dies nicht von Bedeutung für den Rest der Arbeit, bietet aber eine schöne Möglichkeit für die Anwendung des Quadratischen Reziprozitätsgesetzes. Der Autor ist Herrn Maier sehr dankbar für dessen Idee zum Spezialfall $a = 2$, welche sich auf schöne Art und Weise verallgemeinern ließ.

Schaut man sich die fünf Primzahlen an, die wir bei den Lücken benutzt hatten, fällt einem eventuell auf, dass die Abstände zwischen ihnen 8 oder 16 sind. Man kann also vermuten, dass stets $p \equiv 7 \pmod 8$ für sie gilt.
Indem man für jedes a die Menge P_a bis zu einer bestimmten Grenze berechnet und dann die enthaltenen Zahlen modulo verschiedener Module betrachtet, kann man die folgende allgemeinere Regel entdecken:

Satz 5.7. *Sei $a \geq 2$. Dann liegen alle Primzahlen p, für die $p \equiv -1 \pmod{4a}$ gilt, nicht in P_a.*

Beweis. Sei a zunächst eine ungerade Zahl mit Primfaktorzerlegung $a = \prod_{i=1}^{n} q_i$ (mit nicht notwendig verschiedenen Primzahlen q_i) und p eine Primzahl, welche $p \equiv -1 \pmod{4a}$ erfüllt. Wir wollen nun auf zwei verschiedene Arten berechnen, ob a ein quadratischer Rest modulo p ist, einmal mit den Regeln (ii) und (iii) von Lemma 4.4 und dem quadratische Reziprozitätsgesetz und einmal über das Euler Kriterium (Lemma 4.4 (i)) direkt.
Zunächst gilt für jeden Primfaktor $q \in \{q_1, ..., q_n\}$:

$$p \equiv -1 \pmod{4a} \quad \text{und} \quad q \mid 4a \;\Rightarrow\; p \equiv -1 \pmod{q}$$

also

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}. \tag{5}$$

Nun berechnet man $\left(\frac{a}{p}\right)$ mithilfe von Lemma 4.4 und dem Quadratischen Reziprozitätsgesetz:

$$\begin{aligned}\left(\frac{a}{p}\right) = \left(\frac{q_1 \cdot \ldots \cdot q_n}{p}\right) = \prod_{i=1}^{n}\left(\frac{q_i}{p}\right) = \prod_{i=1}^{n}\left(\frac{p}{q_i}\right)\cdot(-1)^{\frac{p-1}{2}\frac{q_i-1}{2}} = \\ \overset{(5)}{=} \prod_{i=1}^{n}(-1)^{\frac{q_i-1}{2}}\cdot(-1)^{\frac{p-1}{2}\frac{q_i-1}{2}} = \prod_{i=1}^{n}(-1)^{\frac{q_i-1}{2}\cdot\left(1+\frac{p-1}{2}\right)} = \\ = \prod_{i=1}^{n} 1 = 1\end{aligned}$$

Von der zweiten zur dritten Zeile wird ausgenutzt, dass $1 + \frac{p-1}{2}$ gerade ist. Das gilt, weil: $p \equiv -1 \pmod{4a}$, d.h. $p = 4ak - 1$ für ein $k \in \mathbb{N}$. Also ist $\frac{p-1}{2} = \frac{4ak-2}{2} = 2ak - 1$ ungerade und damit $1 + \frac{p-1}{2}$ gerade.

Also gilt $\left(\frac{a}{p}\right) = 1$. Mit dem Eulerschen Kriterium gilt dann:

$$1 = \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Also teilt die Ordnung $\mathrm{ord}_p(a)$ den Exponenten $\frac{p-1}{2}$. Da dieser aber ungerade ist, muss auch $\mathrm{ord}_p(a)$ ungerade sein. Damit ist $p \notin P_a$.

Sei nun $a = 2^r \cdot b$ mit $r > 0$ und b ungerade (auch $=1$ möglich). Das Vorgehen ist das gleiche wie oben. Wir berechnen zunächst $\left(\frac{2}{p}\right)$: Da $p \equiv -1 \pmod{4a}$ gilt und a gerade ist, folgt $p \equiv -1 \pmod 8$, also $8 \mid p + 1$. Da $p - 1$ auch gerade ist, also $2 \mid p - 1$, folgt: $16 \mid (p + 1)(p - 1) = p^2 - 1$. Dann ist aber $\frac{p^2-1}{8}$ gerade und nach dem Ergänzungssatz gilt:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$$

Für $\left(\frac{b}{p}\right)$ folgert man wie im ersten Teil, dass $\left(\frac{b}{p}\right) = 1$. Falls $b = 1$, gilt dies ebenso, da 1 immer ein quadratischer Rest ist. Dann gilt insgesamt:

$$\left(\frac{a}{p}\right) = \left(\frac{2^r \cdot b}{p}\right) = \left(\frac{2}{p}\right)^r \cdot \left(\frac{b}{p}\right) = 1^r \cdot 1 = 1$$

Wiederum folgt mit dem Eulerschen Kriterium

$$1 = \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

und somit, dass $\mathrm{ord}_p(a)$ ungerade ist, weil $\frac{p-1}{2}$ ungerade ist.

Damit ist ingesamt gezeigt, dass alle Primzahlen $p \equiv -1 \pmod{4a}$ nicht in P_a liegen. □

Man könnte hiermit auch einen zweiten Beweis dafür führen, dass es unendlich viele Primzahlen außerhalb von P_a gibt, Der Satz von Dirichlet über Primzahlen in arithmetischen Progressionen stellt nämlich sicher, dass es unendlich viele Primzahlen p mit $p \equiv -1 \pmod{4a}$ gibt. Da der Beweis dieses Satzes sehr fortgeschrittene Techniken voraussetzt, werden wir hier nicht weiter darauf eingehen und uns mit dem an Sierpinski angelehnten Beweis im letzten Abschnitt begnügen.

5.6 Das Goldbach- und Zwillingsanalogon

5.6.1 Offene Vermutungen Primzahlen betreffend

Einem Briefwechsel von 1742 zwischen Euler und Goldbach entstammt die

Vermutung 5.1 (Goldbach)**.** *Jede gerade Zahl ab 4 lässt sich also Summe zweier Primzahlen darstellen.*

Seit über 250 Jahren ist diese Vermutung nun schon ungelöst und vermutlich verwandt mit der Vermutung über Primzahlzwillinge.
Dabei ist Primzahlzwilling ein Paar (p, q) zweier Primzahlen, die nur den Abstand 2 voneinander haben, also $|p - q| = 2$. Zum Beispiel sind $(3, 5), (5, 7), (11, 13), (17, 19), (41, 43)$ die ersten fünf Primzahlzwillinge. Die Frage, ob es unendlich viele davon gibt, ist offen:

Vermutung 5.2 (Zwillinge)**.** *Es gibt unendlich viele Primzahlzwillinge.*

Wolfgang Blum stellt die Primzahlen, insbesondere das Problem der Zwillinge und der Goldbachschen Vermutung sehr schön und auch für Laien lesbar in [1] dar.

5.6.2 Übertragung auf P_a-Zahlen

Nachdem der Autor mittels einer Visualisierung die grobe Vermutung aufstellte, dass P_a-Zahlen und Primzahlen ähnlich verteilt sind, untersuchte er, ob sich die eben erwähnten Primzahlvermutungen auch auf P_a-Zahlen übertragen lassen.

Statt also jede gerade Zahl als Summe zweier Primzahlen darzustellen, könnte man sie ja als Summe zweier P_a-Zahlen darstellen. Wählen wir zum Beispiel $a = 2$, dann enthält P_2 die Zahlen

$$1, 3, 5, 9, 11, 13, 17, 19, 25, 27, 29, ...$$

und es gibt folgende Darstellungen für die geraden Zahlen:

$$2 = 1 + 1, \quad 4 = 3 + 1, \quad 6 = 3 + 3, \quad 8 = 5 + 3, \quad 10 = 9 + 1 = 5 + 5, ...$$

Das Ganze kann man mit dem Computer wunderbar testen und es scheint so, als würde es für alle geraden Zahlen funktionieren. Auch mit P_3-Zahlen anstelle der Primzahlen scheint es zu gehen.

a	2	3	5	6	7	8	10	11	13	14	15	17	18	19	20
n_a	0	0	0	16	0	0	44	0	0	0	22	0	52	0	0

Tabelle 4: Startzahlen für das Goldbach-Analogon

a, n	10	100	1000	10000	100000	1000000	10000000
2	2	13	55	347	2439	17903	140888
3	2	6	35	216	1438	10737	84069
4	0	0	0	0	0	0	0
5	1	7	33	228	1771	13522	109057
6	0	4	24	142	978	7223	56651
7	2	9	39	202	1397	10115	78652
8	2	13	55	347	2439	17903	140888
9	0	0	0	0	0	0	0
10	0	5	27	178	1284	9346	74137
11	1	8	60	317	2279	17229	136758
12	1	5	27	156	1014	7256	55479
13	1	6	30	179	1196	9030	71006
14	2	15	65	404	2757	20449	159570
15	1	5	28	189	1300	9998	79184
16	0	0	0	0	0	0	0
17	2	14	68	420	2984	22590	178247
18	0	3	25	172	1213	8906	69981
19	2	13	48	316	2221	16264	126984
20	2	7	42	250	1878	14369	114494

Tabelle 5: Anzahl der Zwillinge in $P_a \cap \{1, ..., N\}$

Nimmt man nun $a = 4$, hat man die P_4-Zahlen

$$1, 5, 13, 17, 25, 29, 37, 41, 53, 61, 65, 97, ...$$

und kann eine Reihe von geraden Zahlen nicht als Summe zweier solcher P_4-Zahlen darstellen, so zum Beispiel

$$4, 8, 12, 16, 20, 24, ...$$

welche interessanterweise alle durch 4 teilbar sind (mehr dazu in 5.6.3). Hier kann man wohl keine analoge Regel wie für Primzahlen formulieren. Testet man mit dem Computer, für welche Basen a man ein Analogon zur Goldbachschen Vermutung findet, gelangt man zu folgender

Vermutung 5.3. *Es existiert genau dann eine Startzahl n_a, sodass sich alle geraden Zahlen ab n_a als Summe zweier Zahlen aus P_a darstellen lässt, wenn a keine Quadratzahl oder das Zwölffache einer Quadratzahl ist.*

Die empirisch ermittelten Startzahlen n_a sind in Tabelle 4 festgehalten.

Ferner findet man auch heraus, dass es für nichtquadratisches a vermutlich unendlich viele P_a-Zahl-Zwillinge gibt, d.h. Zahlen $p, q \in P_a$ mit Abstand $|p - q| = 2$. Falls a quadratisch ist, gibt es keine Zwillinge (die Vielfachen von 12 treten hier nicht als Ausnahmen auf). Eine Übersicht über die Anzahl der Zwillinge in P_a im Bereich $0..n$ findet sich in Tabelle 5.

Es soll jetzt erklärt werden, warum es für quadratische Basen a keine Zwillinge gibt und das Goldbach-Analogon nicht gilt. Dazu verwenden wir das quadratische Reziprozitätsgesetz aus Abschnitt 4, genauergesagt den Ergänzungssatz für -1:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{für Primzahlen } p$$

5.6.3 Beweis für quadratische Basen

Die Idee zum Beweis des nächsten Lemmas gab Prof. Maier. Die Idee für den Beweis des folgenden Lemmas hatte Prof. Maier während einer Besprechung über diese Arbeit.

Lemma 5.9. *Sei $d \in P_{a^2}$. Dann gilt:*

(i) $d \equiv 1 \pmod 4$, *falls d ungerade ist und*

(ii) $d \equiv 2 \pmod 8$, *falls d gerade ist.*

Beweis. Zu (i): Sei d ungerade und $p|d$ ein (ungerader) Primteiler von d. Wenn nun $d \in P_{a^2}$ gilt, so auch $p \in P_{a^2}$. Also gibt es nach Definition ein c mit $p \mid (a^2)^c + 1$, also

$$-1 \equiv (a^2)^c = (a^c)^2 \pmod p$$

Das bedeutet, dass -1 quadratischer Rest modulo p ist und der Ergänzungssatz besagt dann $p \equiv 1 \pmod 4$. Alle Primteiler p von d erfüllen also $p \equiv 1 \pmod 4$, dann muss es d selbst auch tun.
Zu (ii): Sei d gerade. Dann muss a ungerade sein (sonst sind a und d nicht teilerfremd).
Zunächst weißen wir nach, dass d nicht durch 4 teilbar ist. Da a ungerade ist, ist es von der Form $a \equiv \pm 1 \pmod 4$ und $a^2 \equiv 1 \pmod 4$. Also ist auch $(a^2)^c \equiv 1 \pmod 4$ und damit $(a^2)^c + 1 \equiv 2 \not\equiv 0 \pmod 4$ für alle c. Demnach ist $(a^2)^c + 1$ nicht durch 4 teilbar.
Also ist $\frac{d}{2}$ ungerade und als Teiler von d wieder in P_2 enthalten. Dann besagt aber Teil (i), dass $\frac{d}{2} \equiv 1 \pmod 4$ und damit auch

$$4 \mid \frac{d}{2} - 1 \;\Rightarrow\; 4 \mid \frac{d-2}{2} \;\Rightarrow\; 8 \mid d-2 \;\Rightarrow\; d \equiv 2 \pmod 8$$

□

Korollar 5.1. *P_{a^2} enthält keine Zwillinge und das Goldbach-Analogon stimmt für P_{a^2} nicht.*

Beweis. Damit zwei Zahlen d_1 und d_2 ein Zwillingspaar bilden können, müssen beide entweder gerade oder ungerade sein. Das letzte Lemma zeigt aber, dass im geraden Fall alle Elemente von P_{a^2} mindestens Abstand 8 voneinander haben, im ungeraden Fall immer mindestens Abstand 4. Somit kann es keine Zwillinge geben.
Ähnlich beim Goldbach-Analogon: Damit $n = d_1 + d_2$ gerade sein kann, müssen beide gerade oder ungerade sein. Falls beide gerade sind, sagt das Lemma, dass $n = d_1 + d_2 \equiv 2 + 2 = 4 \pmod 8$ und falls beide ungerade sind, entsprechend $n = d_1 + d_2 \equiv 1 + 1 = 2 \pmod 4$. Insgesamt werden dann aber gerade Zahlen n der Form $n \equiv 0 \pmod 8$ gar nie erreicht. Also gilt das Goldbach-Analogon für P_{a^2} nicht. □

Leider konnte der Autor bisher keinen Beweis finden, warum es bei nichtquadratischen Basen stets Zwillinge gibt und (abgesehen von den Zwölffachen der Quadratzahlen) immer das Goldbach-Analogon funktioniert.

6 Die Mengen Q_d und elegante Zahlen

6.1 Die Mengen Q_d und ihre Größe

Im letzten großen Abschnitt wurden für festes a alle Teiler d betrachtet, für die es ein c mit $d \mid a^c+1$ gibt. Nun halten wir d fest und suchen nach Basen a, sodass $d \mid a^c+1$ für ein c erfüllt ist. Für jede Zahl $d \in \mathbb{N}$, $d > 1$ ist $\tilde{Q_d}$ definiert als

$$\tilde{Q_d} = \{a : \exists\, c : d \mid a^c + 1\} = \{a : \exists\, c : a^c \equiv -1 \pmod{d}\}$$

Man sieht schnell, dass aus $a \in \tilde{Q_d}$ auch $a + kd \in \tilde{Q_d}$ für beliebiges $k \in \mathbb{Z}$ folgt, da $a^c \equiv -1 \pmod{d}$ sofort $(a+kd)^c \equiv a^c \equiv -1 \pmod{d}$ impliziert. Wenn also eine Zahl enthalten ist, ist auch ihre ganze Restklasse $\bar{a}$ modulo d enthalten. Deswegen definiert man sich die Menge Q_d nun wie folgt.

Definition 6.1. Sei $d \geq 2$. Dann definiere

$$Q_d = \{\bar{a} \in \mathbb{Z}/d\mathbb{Z} : \exists\, n : \bar{a}^n = \overline{-1}\}$$

und

$$G_d = (\mathbb{Z}/d\mathbb{Z})^\times \setminus Q_d$$

Nach Lemma 5.2 gilt $Q_d \subset (\mathbb{Z}/d\mathbb{Z})^\times$.

Alle Ideen in den nächsten zwei Unterabschnitten stammen von Ben Heuer, der die Gruppenstruktur von G_d erkannt hat und umfassende Formeln zur Berechnung der Größe von Q_d entdeckt und bewiesen hat.

6.1.1 Charakterisierung für Primzahlen

Im Folgenden sei d stets eine Primzahl. In Q_d sind also gerade die Restklassen aus $(\mathbb{Z}/d\mathbb{Z})^\times$, die gerade Ordnung haben und G_d die mit ungerader Ordnung. Die Beweise der folgenden Resultate wurden von Heuer zuerst algebraisch geführt und dann vom Autor in der folgenden, eher zahlentheoretischen Weise, neu formuliert.

Satz 6.1. *G_d ist eine multiplikative Gruppe.*

Beweis. Man rechnet die Gruppenaxiome nach.

- Abgeschlossenheit von G_d: Seien $\bar{a}, \bar{b} \in G_d$, d.h. ihre Ordnungen sind ungerade. Wegen
$$(\bar{a}\bar{b})^{\mathrm{ord}(\bar{a})\cdot\mathrm{ord}(\bar{b})} = 1$$
gilt, dass $\mathrm{ord}(\bar{a}\bar{b}) \mid \mathrm{ord}(\bar{a}) \cdot \mathrm{ord}(\bar{b})$. Da $\mathrm{ord}(\bar{a})$ und $\mathrm{ord}(\bar{b})$ beide ungerade sind, ist es auch ihr Produkt und auch $\mathrm{ord}(\bar{a}\bar{b})$ als Teiler desselben. Also: $\bar{a}\bar{b} \in G_d$.
- Die Assoziativität wird von $(\mathbb{Z}/d\mathbb{Z})^\times$ vererbt.
- $1 \in G_d$, da $\mathrm{ord}(1) = 1$, also ungerade.
- Existenz des inversen Elements: Dazu zeigt man, dass $\mathrm{ord}(\bar{a}) = \mathrm{ord}(\bar{a}^{-1})$. Klar ist $\bar{a}^{-1} = \bar{a}^{\mathrm{ord}(\bar{a})-1}$. Es gilt
$$\left(\bar{a}^{-1}\right)^{\mathrm{ord}\bar{a}} = \left(\bar{a}^{\mathrm{ord}(\bar{a})-1}\right)^{\mathrm{ord}(\bar{a})} \left(\bar{a}^{\mathrm{ord}(\bar{a})}\right)^{\mathrm{ord}(\bar{a})-1} = 1$$
Also gilt: $\mathrm{ord}(\bar{a}^{-1}) \mid \mathrm{ord}(\bar{a})$.

  Genauso leitet man aber über $\bar{a} = (\bar{a}^{-1})^{\mathrm{ord}(\bar{a}^{-1})-1}$ her, dass $\mathrm{ord}(\bar{a}) \mid \mathrm{ord}(\bar{a}^{-1})$. Insgesamt ist also $\mathrm{ord}(\bar{a}^{-1}) = \mathrm{ord}(\bar{a})$. Da $\bar{a} \in G_d$ ungerade Ordnung modulo d hat, hat es also auch $\bar{a}^{-1}$ und liegt damit in G_d.

□

Korollar 6.1. *G_d ist eine zyklische Gruppe.*

Beweis. $(\mathbb{Z}/d\mathbb{Z})^\times$ ist zyklisch, da es nach dem Satz über Primitivwurzeln (Satz 3.7) eine Primitivwurzel $\bar{a}$ gibt, weil d prim ist. Diese Primitivwurzel hat Ordnung $d-1$, erzeugt also $(\mathbb{Z}/d\mathbb{Z})^\times$.

Da nach einem Satz aus der Algebra (siehe [2], Satz 5 in Abschnitt 1.3 (Zyklische Gruppen)) jede Untergruppe einer zyklischen Gruppe auch zyklisch ist, ist G_d als Untergruppe von $(\mathbb{Z}/d\mathbb{Z})^\times$ zyklisch. □

Lemma 6.1. *Für jeden Teiler t von $d-1$ gibt es ein Element $\bar{a} \in (\mathbb{Z}/d\mathbb{Z})^\times$ mit Ordnung t.*

Beweis. Da d prim ist, existiert eine Primitivwurzel $\bar{\xi}$ modulo d. Sei t Teiler von $\mid (\mathbb{Z}/d\mathbb{Z})^\times \mid = \mathrm{ord}(\bar{\xi}) = d-1$, etwa $d-1 = k \cdot t$. Setze $\bar{a} = \bar{\xi}^k$. Dann hat $\bar{a}$ die Ordnung t, denn $a^t = \bar{\xi}^{kt} = 1$ und für $l < t$ ist $\bar{a}^l = \bar{\xi}^{kl} \neq 1$, da $k \cdot l < d-1 = \mathrm{ord}(\bar{\xi})$. □

Im Folgenden sei für jedes k mit $h(k,n)$ die höchste $k-Potenz$ bezeichnet, die n teilt.

Satz 6.2. $|G_d| = \frac{d-1}{h(2,d-1)}$ *und* $|Q_d| = d-1-|G_d|$.

Beweis. Wir zeigen: G_d hat höchstens Ordnung $\frac{d-1}{h(2,d-1)}$ und es hat mindestens Ordnung $\frac{d-1}{h(2,d-1)}$. Da G_d Untergruppe von $(\mathbb{Z}/d\mathbb{Z})^\times$ ist, teilt $|G_d|$ die Zahl $d-1$. Außerdem muss G_d ungerade Ordnung haben, denn wenn sie gerade Ordnung hätte, so hätte einer ihrer Erzeuger $\bar{a} \in G_d$ eben diese gerade Ordnung. Dann wäre $\bar{a}$ aber in Q_d und nicht in G_d. Also ist $|G_d|$ ein ungerader Teiler von $d-1$, $\frac{d-1}{h(2,d-1)}$ ist der größte davon, also $|G_d| \leq \frac{d-1}{h(2,d-1)}$.
Andererseits ist $|G_d|$ auch mindestens gleich $\frac{d-1}{h(2,d-1)}$. Denn nach dem vorherigen Satz gibt es in $(\mathbb{Z}/d\mathbb{Z})^\times$ ein Element $\bar{a}$ mit Ordnung $\mathrm{ord}(\bar{a}) = \frac{d-1}{h(2,d-1)}$. Diese Ordnung ist ungerade, also ist $\bar{a} \in G_d$. Dann liegen aber auch alle Potenzen von $\bar{a}$ in G_d und $|G_d| \geq | < \bar{a} > | = \mathrm{ord}(\bar{a})$.
Insgesamt gilt also $|G_d| = \frac{d-1}{h(2,d-1)}$. □

6.1.2 Charakterisierung für allgemeine Zahlen

Hier ist mit $h_k(n)$ wieder der Exponent der höchsten k-Potenz bezeichnet, die n teilt.

Lemma 6.2. *Sei G eine endliche, zyklische Gruppe mit Ordnung d. Ferner sei $h = h_2(d)$. Für $0 \leq k \leq h$ gibt es dann genau*

$$l_k = \begin{cases} \frac{d}{2^h} 2^{k-1}, & k > 0 \\ \frac{d}{2^h}, & k = 0 \end{cases}$$

viele Elemente a in G, für die $h_2(\mathrm{ord}(a)) = k$ gilt.

Beweis. Da G ist zyklisch, gibt es einen Erzeuger ξ und zu jedem $a \in G$ eine Zahl $i = \mathrm{ind}_\xi(a)$ mit $a = \xi^i$. Nun haben genau $d/2$ alle Elemente einen ungeraden Index und $d/2$ geraden Index. Von den $d/2$ vielen mit geradem Index haben genau $d/4$ einen durch 4 teilbaren Index und die anderen $d/4$ vielen einen Index i mit $h_2(i) = 1$. Von den $d/4$ vielen, deren Index durch 4 teilbar ist, haben wiederum $d/8$ viele einen durch 8 teilbaren Index usw. Das geht soweit, bis $d/2^h$ viele Elemente einen Index haben, der durch 2^h teilbar ist. Wie viele davon jetzt einen Index haben, der genau durch 2^h teilbar ist und wie viele es gibt, der Index durch eine höhere Zweierpotenz teilbar ist, ist nicht mehr so leicht anzugeben und auch nicht von Interesse. Daraus ergibt sich:
Für $0 \leq k < h$ gibt genau $d/2^{k-1}$ viele Elemente a, für die $h_2(\mathrm{ind}(a)) = k$ ist und es gibt $d/2^h$ viele Elemente a mit $h_2(\mathrm{ind}(a)) \geq h$.
Nun gilt ja

$$1 = a^{\mathrm{ord}(a)} = \xi^{i \cdot \mathrm{ord}(a)},$$

also teilt d die Zahl $i \cdot \mathrm{ord}_(a)$. Die Ordnung $\mathrm{ord}(a)$ ist also die kleinste Zahl m, sodass $d \mid im$. Somit enthält $\mathrm{ord}(a)$ genau jene Zweierpotenz, die zusammen mit der Zweierpotenz von i die Zweierpotenz von n ergibt. Gemäß den Überlegungen mit den Indizes gibt es also für $0 < k < h$ genau $d/2^{k-1}$ viele Elemente a, für die $h_2(\mathrm{ord}(a)) = h - k$ ist und $d/2^h$ viele Elemente a mit $h_2(\mathrm{ord}(a)) = 0$. Der erste Fall ist gleichbedeutend mit der in der Behauptung geforderten Formel (man ersetze einfach k durch $h - k$). □

Lemma 6.3. *Für $d = 2^k$ ist $Q_d = \{-\bar{1}\}$.*

Beweis. Das ist einfach nur eine Umformulierung von Lemma 5.5: $\bar{a} \in Q_{2^k}$ gilt genau dann, wenn $2^k \mid a + 1$, also $a \equiv -1 \pmod{2^k}$. □

Satz 6.3. *Sei $d = 2^k \cdot \prod_{i=1}^{m} p_i^{k_i}$ die Primfaktorzerlegung von d. Sei $h_i = h_2(p_i - 1)$. Falls $k \leq 1$, gilt*

$$|Q_d| = \sum_{l=1}^{\min_i h_i} \prod_{i=1}^{m} \frac{p_i - 1}{2^{h_i}} \cdot 2^{l-1} \cdot p_i^{k_i - 1} = \frac{\varphi(d)}{h(2, \varphi(d))} \cdot \frac{2^{m \cdot \min_i h_i} - 1}{2^m - 1}$$

und für $k > 1$

$$|Q_d| = \prod_{i=1}^{m} \frac{p_i - 1}{2^{h_i}} \cdot p_i^{k_i - 1} = \frac{\varphi(d)}{h(2, \varphi(d))}.$$

Beweis. Nach dem Vorgehen von Heuer:
Zunächst macht man sich klar, dass die beiden Mengen

$$A = \mathbb{Z}/d\mathbb{Z} \quad \text{und} \quad B = (\mathbb{Z}/2^k\mathbb{Z}) \times (\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times ... \times (\mathbb{Z}/p_m^{k_m}\mathbb{Z})$$

isomorph zueinander sind. Das geht in folgenden Schritten:

1. Die Funktion

   $$\Phi : A \to B, \quad \Phi(\bar{a}) = (a_0, a_1, ..., a_m) := (\mathrm{rem}(a, 2^k), \mathrm{rem}(a, p_1^{k_1}), ..., \mathrm{rem}(a, p_m^{k_m}))$$

   ist eine Bijektion. Dies folgt aus dem Chinesischen Restsatz: Da die Module $2^k, p_1^{k_1}, ..., p_m^{k_m}$ teilerfremd sind, existiert genau eine Lösung der simultanen Kongruenz

   $$\begin{aligned} x &\equiv a_0 \pmod{2^k} \\ x &\equiv a_1 \pmod{p_1^{k_1}} \\ &\dots \\ x &\equiv a_n \pmod{p_m^{k_m}}. \end{aligned}$$

   zwischen 0 und $M = \mathrm{kgV}(2^k, p_1^{k_1}, ..., p_m^{k_m}) = \prod_{i=0}^{m} p_i^{k_i} = d$ (wobei $p_0 = 2$ und $k_0 = k$ gesetzt ist). Anders ausgedrückt: Für jedes $(a_0, ...a_m) \in B$ gibt es genau ein Urbild in A. Daraus folgt die Bijektivität.

2. Wenn man in B die Addition und Multiplikation komponentenweise definiert, wird B zu einem Ring und die Verträglichkeit von Φ mit den Ringstrukturen in A und B, dass also $\Phi(a + b) = \Phi(a) + \Phi(b)$ und $\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b)$ gilt, ergibt sich aus den Regeln der modularen Arithmetik (siehe Lemma 3.2).

Genauso ist auch die Einschränkung von Φ auf die Einheitengruppen ein Isomorphismus, also

$$A^\times = (\mathbb{Z}/d\mathbb{Z})^\times \;\cong\; B^\times = (\mathbb{Z}/2^k\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times ... \times (\mathbb{Z}/p_m^{k_m}\mathbb{Z})^\times.$$

Es gilt $\Phi(-1) = (-1, ..., -1)$. Wenn nun $\bar{a} \in Q_d$ ist, so gibt es nach Definition ein n mit $\bar{a}^n = -1$ (in A). Dann muss aber für dieses n auch gelten, dass $(a_0, ..., a_m)^n = (a_0^n, ...a_m^n) = (-1, ..., -1)$ in B erfüllt ist.
Das bedeutet einerseits, dass $a_i \in Q_{p_i^{k_i}}$ und andererseits gemäß Satz 5.2 und Lemma 3.6

$$\begin{aligned} n &\equiv \frac{1}{2}\mathrm{ord}_{2^k}(a_0) \pmod{\mathrm{ord}_{2^k}(a_0)} \\ n &\equiv \frac{1}{2}\mathrm{ord}_{p_1^{k_1}}(a_1) \pmod{\mathrm{ord}_{p_1^{k_1}}(a_1)} \\ &... \\ n &\equiv \frac{1}{2}\mathrm{ord}_{p_m^{k_m}}(a_m) \pmod{\mathrm{ord}_{p_m^{k_m}}(a_m)}, \end{aligned}$$

falls $k \geq 2$ (nur dann ist $2^k > 2$, was in Satz 5.2 gefordert ist) und

$$\begin{aligned} n &\equiv \frac{1}{2}\mathrm{ord}_{p_1^{k_1}}(a_1) \pmod{\mathrm{ord}_{p_1^{k_1}}(a_1)} \\ &... \\ n &\equiv \frac{1}{2}\mathrm{ord}_{p_m^{k_m}}(a_m) \pmod{\mathrm{ord}_{p_m^{k_m}}(a_m)}, \end{aligned}$$

falls $k \leq 1$ (da in $(\mathbb{Z}/2^1\mathbb{Z})^\times = \{\bar{1}\}$ ja $\bar{-1} = \bar{1}$ gilt und somit bei ungeradem a für alle n stets $a_0^n = \bar{1}^n = \bar{1} = -\bar{1}$ gilt, d.h. es gibt keine Einschränkung an n). Die beiden obigen Kongruenzsysteme sind wie in Satz 5.4 oder 5.5 nur dann erfüllbar, wenn alle Ordnungen die gleiche Zweierpotenz enthalten. Sei l nun eine bestimmte natürliche Zahl. Wenn es nun b_i viele Elemente in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$ gibt mit $h_2(\mathrm{ord}_{p_i^{k_i}}(a_i)) = l$, so gibt es in A genau $b_0 \cdot b_1 \cdot ... \cdot b_m$ viele Elemente, welche in Q_d liegen und deren Ordnung genau die Zweierpotenz 2^l enthält.
Da die Gruppen $\mathbb{Z}/p_i^{k_i}\mathbb{Z}$ zyklisch sind, zeigt Lemma 6.2 uns, dass es genau

$$b_i = \frac{\varphi(p_i^{k_i})}{2^h} \cdot 2^{l-1} = \frac{(p_i - 1)p_i^{k_i - 1}}{2^h} \cdot 2^{l-1}$$

viele Elemente in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$ mit dieser Eigenschaft gibt. Somit muss es in B genau

$$\prod_{i=0}^{m} \frac{(p_i - 1)p_i^{k_i - 1}}{2^h} \cdot 2^{l-1} \tag{6}$$

Elemente mit höchster Zweierpotenz 2^l in der $\mathrm{ord}(a_i)$ geben. Was sind die möglichen Werte für l? Falls $k \geq 2$, so sagt uns das Lemma 6.3, dass nur die -1 in Q_{2^k} liegt. Diese hat Ordnung 2, enthält also die Zweierpotenz 1. Alle anderen Ordnungen müssen also auch diese Zweierpotenz enthalten, der einzige Wert für l ist somit $l = 1$. Damit ergibt sich die Formel

$$|Q_d| = \prod_{i=1}^{m} \frac{p_i - 1}{2^{h_i}} \cdot p_i^{k_i - 1} = \frac{\varphi(d)}{\prod_{i=1}^{m} 2^{h_i}} = \frac{\varphi(d)}{h(2, \varphi(d))}.$$

Falls $k \leq 1$ ist die einzige Einschränkung für l, dass es höchstens so groß werden kann wie der kleinste aller Werte

$$h_i := h_2(\varphi(p_i^{k_i})) = h_2((p_i - 1)p_i^{k_i - 1})) = h_2(p_i - 1), \qquad i = 1, ..., m$$

wobei die letzte Umformung gilt, weil die p_i für i=1,...,m ungerade sind. Summiert man also die Werte aus (6) für die möglichen l-Werte $1, 2, ..., \min_i h_i$ auf und wendet am Schluss noch die geometrische Summenformel an, erhält man die behauptete Formel

$$\begin{aligned}|Q_d| &= \sum_{l=1}^{\min_i h_i} \prod_{i=1}^{m} \frac{p_i - 1}{2^{h_i}} \cdot 2^{l-1} \cdot p_i^{k_i - 1} = \sum_{l=1}^{\min_i h_i} \left(2^{l-1}\right)^m \prod_{i=1}^{m} \frac{p_i - 1}{2^{h_i}} \cdot p_i^{k_i - 1} \\ &= \left(\prod_{i=1}^{m} \frac{p_i - 1}{2^{h_i}} \cdot p_i^{k_i - 1} \right) \cdot \sum_{l=1}^{\min_i h_i} (2^m)^{l-1} = \frac{\varphi(d)}{h(2, \varphi(d))} \cdot \sum_{l=0}^{\min_i h_i - 1} (2^m)^l \\ &= \frac{\varphi(d)}{h(2, \varphi(d))} \cdot \frac{2^{m \cdot \min_i h_i} - 1}{2^m - 1}\end{aligned}$$

□

6.2 Elegante Zahlen

Definition 6.2. Eine Zahl $d > 2$ heißt elegant, falls $\bar{a} \in Q_d$ für alle $\bar{a} \in (\mathbb{Z}/d\mathbb{Z})^\times \setminus \{\bar{1}\}$ gilt, d.h. $G_d = \{1\}$.

Die Idee der eleganten Zahlen sowie die vermutete Beziehung zu den Fermatschen Primzahlen stammt vom Autor der Arbeit. Einen Beweis dafür fand er im März 2012 zusammen mit Heuer.

Bemerkungen zur Definition Eine elegante Zahl ist also eine Zahl d, die für maximal viele a ein Teiler von $a^c + 1$ ist. Der Autor berechnete die eleganten Zahlen $3, 5, 17, 257, 65537$, konnte damals aber aufgrund des ineffizienten Algorithmus nicht nachprüfen, ob es zwischen 257 und 65537 noch weitere elegante Zahlen gibt. Das hat Heuer mit einem weitaus besseren Algorithmus im März 2012 geschafft, welcher dem Autor auch Motivation gab, sich mit Python zu beschäftigen.

Dem Leser werden die oben aufgelisteten eleganten Zahlen eventuell bekannt vorkommen. Es sind genau die sogenannten Fermatschen Primzahlen $2^{2^n} + 1$. Die Fermatschen Primzahlen gehen auf Pierre Fermat zurück, der vermutete, dass alle Zahlen der Form $2^{2^n} + 1$ Primzahlen sind. Er verifizierte dies für $n = 0$ bis $n = 4$. Euler fand jedoch heraus, dass $2^{2^5} + 1$ nicht prim ist. Mit Computern wurde die Vermutung weiter getestet und inzwischen umgekehrt: Man vermutet, dass es außer den ersten fünf Fermatzahlen gar keine anderen Fermatschen Primzahlen gibt. Die einzigen fünf bekannten Fermatschen Primzahlen sind $3, 5, 17, 257, 65537$. In diesem Abschnitt werden wir die Beziehung zwischen eleganten Zahlen und Fermatschen Primzahlen untersuchen.

Lemma 6.4. *Jede elegante Zahl ist eine Primzahl.*

Beweis. Wenn d keine Primzahl ist, gibt es zwischen 2 und $d - 1$ mindestens eine Zahl a, die d teilt, also insbesondere $\mathrm{ggT}(a, d) \neq 1$. Dann ist $\bar{a} \notin Q_d$ und d ist nach Definition nicht elegant. □

Lemma 6.5. *Falls $2^k + 1$ prim ist, so ist k von der Form $k = 2^n$, $n \in \mathbb{N}_0$.*

Beweis. Angenommen, k habe einen ungeraden Teiler, also $k = a \cdot b$ mit b ungerade (wobei a auch 1 sein kann). Dann gilt wegen der Ungeradheit von b und der geometrischen Summenformel:

$$2^k + 1 = 2^{ab} + 1 = (2^a)^b + 1 = -((-2^a)^b - 1) = -(-2^a - 1) \cdot \sum_{i=0}^{c-1} (-2^a)^i = (2^a + 1) \cdot \sum_{i=0}^{c-1} (-2^a)^i$$

Damit hat $2^k + 1$ den Teiler $2^a + 1 \neq 1$ und ist damit nicht prim. Falls $2^k + 1$ also prim ist, dann kann k keinen ungeraden Teiler haben, d.h. es muss von der Form $k = 2^n$ sein. □

Nun können wir die Verbindung zwischen eleganten Zahlen und Fermatschen Primzahlen beweisen:

Satz 6.4. *Die eleganten Zahlen sind genau die Fermatschen Primzahlen.*

Beweis. Sei d elegant, d.h. $|G_d| = 1$. Dann ist nach dem vorletzten Lemma d prim und es gilt $|G_d| = \frac{d-1}{h(2,d-1)}$. Also ist $\frac{d-1}{h(2,d-1)} = 1$, was bedeutet, dass $d-1$ von der Form 2^k ist. d selbst ist also eine Primzahl der Form 2^k+1 und nach dem letzten Lemma sogar von der Form $2^{2^n}+1$, also eine Fermatsche Primzahl.
Wenn d andersrum eine Fermatsche Primzahl ist, dann gilt $d-1 = 2^{2^n}$ und d prim. Das heißt

$$|G_d| = \frac{2^{2^n}}{h(2, 2^{2^n})} = 1.$$

Also ist d elegant. □

7 Verwandte Arbeiten und Ausblick

Hier sollen noch zwei Fragen beantwortet werden: Ist das Konzept der P_a-Zahlen völlig neu oder wurde es schon von anderen Autoren eingeführt? Und: Ist die Betrachtung der Mengen P_a und Q_d an dieser Stelle vorbei oder kann man noch mehr machen?

Zur ersten Frage: Schon einige andere Autoren haben sich mit Teilern (oder spezieller: Primteilern) von Termen der Form a^n+1 beschäftigt. Sierpinski tut dies in [11] für den Spezialfall $a = 2$ und zeigt, dass es unendlich viele Primzahlen gibt, die nicht in P_a liegen. Brauer ([4]) und Hasse ([5]) verallgemeinern das ganze in verschiedene Richtungen, doch erst Moree ([7]) interessierte sich für Zahlen, die fast den P_a-Zahlen in dieser Arbeit entsprechen. Er betrachtet die Teiler von a^k+b^k und nennt diese „good numbers“. Die P_a-Zahlen dieser Arbeit ergeben sich also im Spezialfall $b = 1$. Moree beweist auf den ersten drei Seiten Aussagen, die im Wesentlichen den folgenden Sätzen dieser Arbeit entsprechen: Lemmata 5.1, 5.2, 5.4, Sätze 5.2, 5.3, 3.6. Sein Theorem 1 geht in die Richtung von Satz 5.5. Anschließend widmet er sich der Frage, wie viele „gute Zahlen“ es unterhalb einer Zahl n gibt. Moree's Arbeit war für den Autor lediglich eine Bestätigung, nicht aber eine Inspiration. Sie zeigt, dass das Thema in der Fachwelt durchaus von Interesse ist (wenn auch vor einigen Jahren).

Zur zweiten Frage: Natürlich ist die Untersuchung noch lange nicht beendet. Wie Moree kann man sich der Frage nach der Dichte der P_a-Zahlen in den natürlichen Zahlen widmen. Dann sind natürlich die beiden Vermutungen über das Goldbach-Analogon und die Zwillinge noch offen. Die Gegenbeweise für quadratische Basen waren relativ einfach, doch für einen Beweis der beiden Vermutungen ist vermutlich eine deutlich tiefere Kenntnis der P_a-Zahlen nötig. Schließlich können die P_a-Zahlen verallgemeinert werden, aber nicht in die Richtung wie Moree es tut, sondern auf allgemeinere Ringe, in denen man Teilbarkeitstheorie betreiben kann. Der Autor vermutet, dass sich dafür Polynomringe, insbesondere die über endlichen Körpern gut eignen würden. Auch Matrizen fester Größe wären denkbar. Der Ring sollte natürlich nicht selber ein Körper sein, da sonst der Begriff der Teilbarkeit keine Bedeutung mehr hat. Es übertragen sich die Kriterien aus den Unterabschnitten 5.2.1 und 5.2.2 direkt auf Ringe.

Ebenfalls interessant ist die weitere Untersuchung der Woodstone-Visualisierung. Wie hängt die Form der Muster mit der Verteilung und Dichte der verwendeten Zahlenmenge zusammen?

Ein anderes Gebiet wären die eleganten Zahlen. Eventuell kann man so mehr über Fermatsche Zahlen lernen, womit man vielleicht eines Tages beweisen kann, dass es außer den ersten fünf keine weiteren gibt.

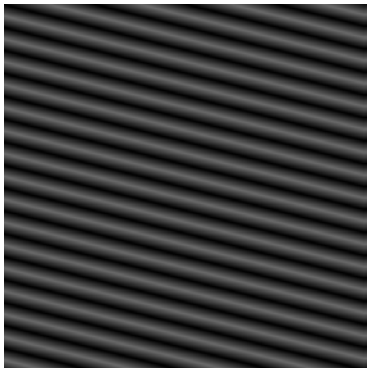
Der Autor freut sich sehr über jegliche Rückmeldungen, Verbesserungen, Fragen, Kritik und Ideen zu dieser Arbeit. Dafür wende man sich an `matthias.heinlein@uni-ulm.de`.

A Funktionsweise der Woodstone-Visualisierung

Man betrachtet eine Grafik mit 500 x 500 Pixeln, die nach den folgenden Regeln eingefärbt wird:

- Es werden nur Graustufenfarben verwendet, der Wert 0 kennzeichnet die Farbe Schwarz, der Wert 255 die Farbe Weiß.
- Man beginnt links oben beim ersten Pixel mit der Farbe 0, also ganz schwarz, und wird nun mit jedem Pixel nach rechts um eine Farbstufe heller. Für jedes Bild wird ein fester Maximalwert k festgelegt. Die Pixel werden immer heller, bis am $(k+1)$-ten Pixel die Farbe k erreicht ist. Dann wird mit jedem Pixel der Farbwert um eins dunkler, bis man wieder bei 0 angekommen ist. Ab da geht alles wieder von vorne los. Die Farbwerte haben also eine Periode von $2 \cdot k$ Pixeln.
- Wenn man am Ende einer Zeile angekommen ist, geht es links in der nächsten Zeile mit dem nächsten Farbwert weiter, d.h. nicht jede Zeile fängt mit 0 an.

(a) $k = 50$



(b) $k = 63$

0	1	2	...		499
500	501				
...					
					249 999

(c) Zahlenbelegung

Abbildung 4: Streifenmuster und Zahlenbelegung

Es gibt zwei grundsätzliche Situationen, wie das Ergebnis aussieht. Wenn $2 \cdot k$ ein Teiler von 500 ist, passt eine ganze Zahl von Streifen in eine Zeile und die nächste Zeile geht wieder mit dem Farbwert 0 los. Da dann jede Zeile mit dem gleichen Farbwert beginnt, liegen die hellsten Stellen in jeder Zeile genau untereinander und es ergibt sich ein Streifenmuster mit parallelen, senkrechten Streifen (Abb. 1a). Wenn $2k$ allerdings kein Teiler von 500 ist, beginnen nicht alle Zeilen mit dem gleichen Farbwert, d.h. die hellsten Stellen in jeder Zeile befinden sich nicht an der gleichen Stelle. Es ergibt sich ein Muster mit parallelen, aber schrägen Streifen (z.B. Abb. 1b). Wenn die Streifen sehr flach sind, sieht man manchmal auch fast nichts. Die Werte unter den Abbildungen geben jeweils den maximalen Farbwert (und damit die halbe Streifenbreite) k an.

Nun kommen die Zahlen, die man visualisieren will, ins Spiel. Das können zum Beispiel Prim-, Quadrat- oder Kubikzahlen, Fastprimzahlen, unsere Pa -Zahlen oder andere Pseudoprimzahlen sein. Sei allgemein $M \subset \mathbb{N}$ eine Menge, die wir visualisieren wollen. Der oben beschriebene Ablauf wird nun folgendermaßen abgeändert: Man nummeriert die Pixel des Bildes in Gedanken so durch wie in Abbildung 1c angedeutet ist. An jedem Pixel, der eine Zahl $m \in M$ trägt, wird nicht der nächsthellere oder nächstdunklere Farbwert angenommen, sondern man ubernimmt einmal den Farbwert des vorherigen Pixels. Erst beim nächsten Pixel, wo keine Zahl aus M steht, wird der Farbwert verändert. Dadurch verschieben sich an Stellen mit Elementen aus M das ganze Muster.

Mehr steckt nicht hinter der Visualisierung und man erhält Bilder wie in Abschnitt 5.4.

Literatur

[1] Wolfgang Blum: *Goldbach und die Zwillinge*, Mitteilungen der DMV, Deutsche Mathematiker Vereinigung, Ausgabe 18 (2010), Seiten 222-226

[2] Siegfried Bosch: *Algebra*, Springer, Berlin, 1993

[3] Irene I. Bouw: *Elementare Zahlentheorie*, Vorlesungsskript der Universität Ulm, Sommersemester 2008

[4] Alfred Brauer: *A note on a number theoretical paper of Sierpinski* Proc. Am. Math. Soc. ll, 406 409 (1960)

[5] Helmut Hasse: *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod. p ist*, Math. Annalen 166, 19–23 (1966)

[6] Helmut Maier: *Vorlesung Zahlentheorie*, Vorlesungskript der Universität Ulm, Wintersemester 1996/97

[7] Pieter Moree: *On the divisors of $a^k + b^k$*, Acta Arithmetica, Vol. 80 (1997), Artikel 3, Seiten 197-212

[8] Stefan Müller-Stach, Jens Piontowski: *Elementare und algebraische Zahlentheorie*, Vieweg, Wiesbaden, 2006

[9] Kenneth. H. Rosen: *Elementary Number Theory*, Sechste Auflage, Pearson, Boston, Mass., 2011

[10] Uwe Schöning: *Skript zu Algorithmen und Datenstrukturen*, Vorlesungsskript der Universität Ulm, Wintersemester 2012/13

[11] Wacław Sierpiński: *Sur une décomposition des nombres premiers en deux classes*, Collect. Math. Vol. 10 (1958), Seiten 81-84

[12] Joseph H. Silverman: *A Friendly Introduction to Number Theory*, Dritte Auflage, Pearson Prentice Hall, Upper Saddle River, NJ, 2006