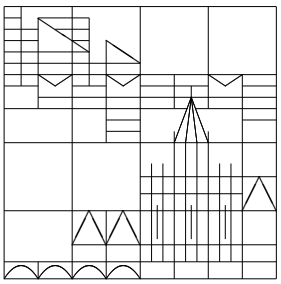
Untersuchung der oberen Schranke für Sophie-Germain-Begleitprimzahlen

Universität Konstanz
Fachbereich Mathematik und Statistik



Wissenschaftliche Arbeit
zur Erlangung des akademischen Grades
der Diplom-Mathematikerin

Untersuchung der oberen Schranke für Sophie–Germain–Begleitprimzahlen

Marina Herbst

Dezember 2007

Betreut durch Prof. Dr. Gottfried Barthel

Inhalt

Einleitung

Das Thema der vorliegenden Arbeit entstand aus der Beschäftigung mit dem Ansatz von Sophie Germain zum Beweis des großen Satzes von Fermat, auch ‚letzter Satz von Fermat' genannt. Dieser besagt, dass die Gleichung

$$x^n + y^n = z^n$$

für den ganzzahligen Exponenten $n \geq 3$ keine nicht-trivialen ganzzahligen Lösungen besitzt. Die Fermat-Gleichung mit dem Exponenten $n = 2$, die wohl jedem als der Satz von Pythagoras bekannt ist, besitzt unendlich viele ganzzahlige Lösungen. Beispielsweise genügen die Zahlen $x = 3$, $y = 4$, $z = 5$ der Gleichung $x^2 + y^2 = z^2$, das Tripel $(3, 4, 5)$ ist das kleinste pythagoreische Tripel.

Um so merkwürdiger schien die Aussage von Pierre Fermat aus dem Jahr 1637, welche sich in den Randnotizen seiner Ausgabe der *Arithmetica* des Diophantos findet. Neben der Darstellung des diophantischen Problems VIII, eine Quadratzahl in die Summe zweier Quadratzahlen zu zerlegen, notierte Fermat auf dem Rand der Buchseite, dass keine Potenz, die höher ist als zwei, in zwei Potenzen mit demselben Exponenten zerlegt werden könne. Mit anderen Worten behauptete Fermat, dass die Gleichung $x^n + y^n = z^n$ für alle Potenzen $n \geq 3$ keine nicht-trivialen ganzzahligen Lösungen besitze. Er fügte hinzu, er habe für diese Aussage einen ‚wahrhaft wunderbaren' Beweis, der jedoch nicht auf den schmalen Rand der Seite passe. Das Formulieren eines solchen Beweises hat sich als schwieriges Problem erwiesen. Die Geschichte des Fermat-Problems ist in wissenschaftlicher Darstellung in (Bachmann, 1976) ausführlich beschrieben[1].

In einer weiteren Notiz gab Fermat ein Beweisverfahren an – die Methode des unendlichen Abstiegs – mit welchem der biquadratische Fall $n = 4$ bewiesen werden konnte. In (Euler, 1770) findet sich ein Beweis für den kubischen Fall

[1] Fermats Problem ist ein beliebter Gegenstand der populären Literatur über Mathematik. Eine gute populäre Darstellung findet sich beispielsweise in (Singh, 2005).

$n = 3$ von Leonhard Euler. Ausführliche Darstellungen beider Beweise sind beispielsweise in (Ribenboim, 1979) enthalten. Ein allgemeingültiger Beweis aber stand noch aus und wurde erst zirka 350 Jahre später mit modernen Methoden erbracht. Andrew Wiles veröffentlichte den Beweis als (Wiles, 1995).

Der Satz von Fermat ist offensichtlich für einen Exponenten n bewiesen, falls er für einen Teiler d von n bewiesen ist. Daher genügt es, das Fermat-Problem für $n = 4$ und für ungeraden Primzahlexponenten $n = p$ zu untersuchen, da für alle ganzzahligen $n \geq 3$ gilt, dass n durch 4 oder eine ungerade Primzahl p teilbar ist. Da die Unmöglichkeit der Fermat-Gleichung im ersten dieser Fälle – dem biquadratischen Fall – bereits gezeigt wurde, konnte man sich seitdem auf den zweiten dieser Fälle beschränken.

Das Fermat-Problem kann also auf den folgenden Fall reduziert werden: Der Exponent ist eine ungerade Primzahl, das heißt $n = p \geq 3$. Desweiteren haben die Zahlen x, y, z keinen gemeinsamen Teiler, der ungleich ± 1 ist. Dazu genügt, dass zwei der drei Zahlen teilerfremd sind, also sind x, y, z paarweise teilerfremd. Zudem sind zwei der drei Zahlen ungerade, die dritte ist gerade. Ohne Beschränkung der Allgemeinheit seien im Folgenden x, y ungerade, z gerade.

Bei den bekannten Beweisen unterscheidet man traditionell zwei Fälle: Man beweist, dass die Fermat-Gleichung

(I. Fall) keine ganzzahligen Lösungen x, y, z besitzt, welche nicht durch p teilbar sind, also $p \nmid xyz$, bzw.

(II. Fall) keine nicht-trivialen ganzzahligen Lösungen x, y, z besitzt, von denen *genau eine* durch p teilbar ist, also $p \mid xyz$.

Seit Euler konzentrierte sich die Forschung zum Fermat-Problem auf Beweise einzelner Fälle bestimmter Exponenten p.

Der nächste bedeutende Fortschritt auf diesem Gebiet wurde um 1819 von Sophie Germain[2] erbracht. Sie arbeitete an einem *allgemeinen Lösungsansatz* für eine ‚Gruppe' von Fällen, in denen der Exponent p eine ungerade Primzahl ist, für die es eine weitere Primzahl $q \neq p$ mit folgenden Eigenschaften gibt: p ist keine p-te Potenz mod q und die Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ besitzt nur triviale Lösungen. Dann, so zeigte sie, besitzt die Fermat-Gleichung $x^p + y^p = z^p$ keine ganzzahligen Lösungen im I. Fall.

Eine Zahl q, welche die oben genannten Bedingungen erfüllt, werden wir im Folgenden eine ‚Sophie-Germain-Begleitprimzahl zu p' nennen.

[2]Sophie Germain *1. April 1776 in Paris, †27. Juni 1831 in Paris

Der Begriff der ‚Sophie-Germain-Begleitprimzahl' ist in der deutschsprachigen Literatur bis jetzt nicht gebräuchlich. In (Laubenbacher & Pengelley, 1999), (Riddle, 2001) und (MathPages, 2005) werden solche Zahlen als ‚*auxiliary primes*' bezeichnet. Hier von ‚begleitenden' Primzahlen zu sprechen schien mir nach einigen Überlegungen sinnvoller zu sein. Es gibt eine wenig verbreitete Definition von E. Dubouis aus dem Jahre 1910: Ist p prim, so bezeichnet der Autor eine Primzahl $\theta = kp + 1$ derart, dass die Kongruenz $x^p \equiv y^p + 1 \pmod{\theta}$ in ganzen durch θ nicht teilbaren Zahlen nicht lösbar ist, als ‚*sophien*' zu p (vgl. (Dickson, 1971a, Chapter XXVI)).

Aus dem Satz von Sophie Germain ergab sich die interessante Fragestellung, ob für eine Primzahl $p > 2$ unendlich viele Sophie-Germain-Begleitprimzahlen existieren. Wäre dies der Fall, so wäre damit Fermats großer Satz für jeden solchen Exponenten p in seinem gesamten Umfang bewiesen. Aber schon 1832 vermutete Guglielmo Libri, dass die Menge der Sophie-Germain-Begleitprimzahlen für jedes beliebige p beschränkt sei (siehe (Libri, 1832, Seite 75)). Diese Vermutung wurde 1909 von Leonard Eugene Dickson bewiesen. In (Dickson, 1909) wird gezeigt, dass die Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ für jede Primzahl $q \geq S(p)$ stets nicht-triviale Lösungen besitzt, wobei

$$S(p) = (p-1)^2(p-2)^2 + 6p - 2$$

ist. Damit war eine *obere Schranke* für die Sophie-Germain-Begleitprimzahlen zu einem gegebenen p formuliert und bewiesen.

Der Ansatz von Sophie Germain zur Lösung des Fermat-Problems wird in der Literatur oft betrachtet, wie beispielsweise in (Laubenbacher & Pengelley, 1999), (Ribenboim, 1979), (Riddle, 2001), (MathPages, 2005) und (Bachmann, 1976). Allerdings behandeln die meisten Arbeiten lediglich den oben genannten Satz von Sophie Germain sowie die darauf basierenden Ergebnisse von Legendre. Seltener wird Bezug zu Dicksons Schranke hergestellt (siehe (Bachmann, 1976), (Riddle, 2001)) und numerische Untersuchungen zu Dicksons Schranke existieren kaum. Auf (MathPages, 2005) sind lediglich einige Beispiele von ‚begleitenden' Primzahlen zu $p \leq 43$ angegeben. In (Riddle, 2001) geht der Autor unter anderem darauf ein, wie das Vorliegen der Bedingungen des Satzes von Sophie Germain in der Praxis überprüft werden können. Abgesehen von diesen wenigen Ansätzen hat bisher praktisch keine systematische Beschäftigung mit den von Sophie Germain untersuchten Zahlen und deren oberer Schranke eingesetzt.

Die vorliegende Arbeit betrachtet die Arbeiten von Sophie Germain (fast) unab-

hängig von der ursprünglichen Zielsetzung, welcher sie dienten. Die Tatsache, dass der von Sophie Germain formulierte Ansatz zum Beweis von Fermats großem Satz nicht zum Erfolg führte, bedeutet keineswegs, dass die weitere Untersuchung der von ihr beschriebenen Zahlen obsolet wäre. Vielmehr werden diese im Rahmen der vorliegenden Arbeit als eigenständiges Objekt der Forschung aufgefasst und behandelt.

In diesem Zusammenhang stellt die Arbeit den Bezug zu Dicksons Untersuchungen über die Fermat-Kongruenz in (Dickson, 1909) her und präsentiert weiterführende Erkenntnisse über die von uns untersuchten Zahlen. Neben der systematischen Einführung in ein neu herausgearbeitetes Gebiet der Sophie-Germain-Begleitprimzahlen stellt die vorliegende Arbeit zudem erste experimentelle Ergebnisse vor und formuliert Fragestellungen für weiterführende Untersuchungen. Eine offene Frage ist beispielsweise, ob für jede Primzahl eine Sophie-Germain-Begleitprimzahl existiert.

Den Schwerpunkt der Arbeit bilden der Beweis des Satzes von Dickson sowie die Untersuchung von Dicksons Schranke für Sophie-Germain-Begleitprimzahlen zu einem gegebenen p anhand einiger exemplarischer Berechnungen. Das praktische Verfahren zur Bestimmung von Sophie-Germain-Begleitprimzahlen wird ebenfalls ausführlich diskutiert.

Kapitel 1 enthält eine Zusammenstellung einiger zentraler zahlentheoretischer Begriffe und Sätze, welche im Laufe der Arbeit gebraucht werden.

Mit dem Ansatz von Sophie Germain zur Lösung des Fermat-Problems befassen wir uns in Kapitel 2. Der Satz von Sophie Germain wird hier ausführlich diskutiert und bewiesen. In diesem Zusammenhang führen wir den Begriff der Sophie-Germain-Begleitprimzahl zu einer gegebenen Primzahl p ein und betrachten genauer deren Eigenschaften und die sich daraus ergebende allgemeine Gestalt.

Kapitel 3 enthält eine Darstellung des Satzes von Dickson, aus dem eine obere Schranke für Sophie-Germain-Begleitprimzahlen folgt. Nach einer Fallunterscheidung wird ein vollständiger Beweis des Satzes geführt.

In Kapitel 4 werden einige experimentelle Ergebnisse dargestellt, die unter Anwendung von Maple 9.5 berechnet wurden. Daran anschließend wird das Verfahren zur Bestimmung von Sophie-Germain-Begleitprimzahlen diskutiert.

Die Ergebnisse der Arbeit werden in Kapitel 5 kurz zusammengefasst. Abschließend werden hier weiterführende Fragen zum dargestellten Thema formuliert.

An dieser Stelle möchte ich allen danken, die mich bei meiner Arbeit unter-

stützt haben. Bei meinem Betreuer Herrn Prof. Dr. G. Barthel bedanke ich mich für das interessante Thema und zahlreiche inspirierende Gespräche. Mein besonderer Dank gilt meinem Verlobten Stefan für seine fortwährende Unterstützung während meines Studiums und besonders während des Schreibens dieser Arbeit.

Kapitel 1

Grundlagen

In diesem Kapitel werden zentrale Begriffe eingeführt sowie grundlegende Erkenntnisse und Sätze formuliert, auf welche die Darstellung im weiteren Verlauf aufbauen wird. Diese stammen insbesondere aus der Zahlentheorie, aus der Kreisteilungstheorie und der Theorie der höheren Kongruenzen für einen Primzahlmodul p (siehe zu diesen drei Gebieten (Borewicz & Šafarevič, 1966), (Bachmann, 1968a), (Bachmann, 1968b)). In diesem Rahmen beweisen wir den kleinen Satz von Fermat, behandeln quadratische und m-te Potenzreste mod p sowie (primitive) n-te Einheitswurzeln und primitive Wurzeln mod p. In den letzten Abschnitten des Kapitels beschäftigen wir uns außerdem etwas ausführlicher mit den Gaußschen Perioden und den Lagrange- bzw. Jacobi-Resolventen.

1.1 Kleiner Satz von Fermat

Eine wichtige Aussage liefert der sogenannte kleine Satz von Fermat, den wir nun formulieren und beweisen werden.

Satz 1.1.1 (Kleiner Satz von Fermat)
Sei p eine Primzahl. Dann gilt für jede durch p nicht teilbare ganze Zahl a die Kongruenz

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.1}$$

Es gibt verschiedene Möglichkeiten, den kleinen Satz von Fermat zu beweisen. Der folgende Beweis basiert auf den Eigenschaften einer endlichen multiplikativen Gruppe.

Beweis: Wir setzen hier folgende Tatsache als bekannt voraus: Ist G eine endliche multiplikative Gruppe, so gilt für jedes Element $x \in G$

$$x^{\mathrm{ord}(G)} = 1, \tag{1.2}$$

wobei mit $\mathrm{ord}(G)$ die Ordnung von G bezeichnet wird.

Die Zahl a, genauer $a \pmod p$, kann als Element der multiplikativen Gruppe

$$(\mathbb{Z}/(p))^\times = \mathbb{F}_p^\times$$

aufgefasst werden. Diese Gruppe $\mathbb{F}_p^\times$ besteht aus $(p-1)$ Elementen, das heißt

$$\mathrm{ord}(\mathbb{F}_p^\times) = p - 1.$$

Mit (1.2) folgt dann die Behauptung. □

1.2 Eulersche Verallgemeinerung des kleinen Satzes von Fermat

Definition 1.2.1 (Eulersche φ-Funktion)
Sei $n \in \mathbb{N}_{\geq 1}$. Dann definiert man die Eulersche φ-Funktion *durch:*

$$\begin{aligned} \varphi(1) &:= 1 \\ \varphi(n) &:= \#\,(\mathbb{Z}/(n))^\times \quad \textit{für} \quad n > 1. \end{aligned}$$

Ist p prim, so gilt $\mathrm{ggT}(r, p) = 1$, falls $1 \leq r \leq p-1$. Deshalb ist $\varphi(p) = p - 1$.

Im Fall $n = 1$ hat der Ring $\mathbb{Z}/(n) = \{\overline{0}\}$ nur ein einziges Element, welches seine Null und Eins zugleich ist. Deshalb ist die Definition $\varphi(1) = 1$ sinnvoll.

Unter Benutzung der Eulerschen φ-Funktion kann der kleine Satz von Fermat auf folgende Weise verallgemeinert werden.

Satz 1.2.2 (Euler)
Sei $n \geq 2$ eine natürliche Zahl. Dann gilt für jede durch n nicht teilbare ganze Zahl a die Kongruenz

$$a^{\varphi(n)} \equiv 1 \pmod n. \tag{1.3}$$

Beweis: Der Beweis wird analog zum Beweis des kleinen Satzes von Fermat geführt. □

1.3 Quadratische Reste

Definition 1.3.1 (Quadratischer Rest bzw. Nichtrest mod p)
Sei p eine ungerade Primzahl. Eine zu p teilerfremde ganze Zahl a heißt quadratischer Rest mod p, *falls die Kongruenz*

$$x^2 \equiv a \pmod{p}$$

lösbar ist, das heißt falls eine ganze Zahl x existiert, deren Quadrat kongruent $a \pmod{p}$ ist. Andernfalls heißt a quadratischer Nichtrest mod p.

Definition 1.3.2 (Legendre-Symbol)
Sei p eine ungerade Primzahl. Für eine zu p teilerfremde ganze Zahl a definieren wir das Legendre-Symbol $\left(\frac{a}{p}\right)$ *(gesprochen „a* nach p*“) wie folgt:*

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{falls } a \text{ quadratischer Rest mod } p, \\ -1 & \text{sonst.} \end{cases}$$

Falls p die Zahl a teilt, so wird

$$\left(\frac{a}{p}\right) = 0$$

gesetzt. Das Legendre-Symbol ist im ersten Argument multiplikativ, das heißt für alle ganzen Zahlen a, b gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Satz 1.3.3 (Eulersches Kriterium)
Für jede ungerade Primzahl p und jede zu p teilerfremde ganze Zahl a gilt

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

Beweis: Seien p eine ungerade Primzahl und a eine zu p teilerfremde ganze Zahl. Es ist leicht zu sehen, dass $a \equiv x^2 \pmod{p}$ genau dann lösbar ist, wenn

$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ist. Es gilt ferner:

$$\begin{aligned} a^{p-1} - 1 &= \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \\ &\underset{(1.1)}{\equiv} 0 \pmod{p}. \end{aligned}$$

Das heißt $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Daraus ergibt sich die Behauptung. □

Definition 1.3.4 (Jacobi-Symbol)
Das Jacobi-Symbol $\left(\frac{a}{n}\right)$ *für* $a, n \in \mathbb{Z}$ $(n > 2)$ *ist eine Verallgemeinerung des Legendre-Symbols und ist für den Fall definiert, dass* n *eine beliebige (positive) ungerade Zahl ist.*

Ist $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ die Primfaktorzerlegung von n, so gilt für das Jacobi-Symbol:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{e_r}.$$

Für die Berechnung des Jacobi-Symbols sind das quadratische Reziprozitätsgesetz sowie dessen erster und zweiter Ergänzungssatz von Nutzen. Wir werden diese lediglich formulieren, die Beweise hierzu können in (Leutbecher, 1996) und (Borewicz & Šafarevič, 1966) nachvollzogen werden.

Satz 1.3.5 (Quadratisches Reziprozitätsgesetz)
Seien $a > 1$ *und* $n > 1$ *zueinander teilerfremde ungerade natürliche Zahlen. Dann gilt*

$$\left(\frac{a}{n}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{a}\right).$$

Der Wert des Jacobi-Symbols für den Fall $a = -1$ und $a = 2$ kann mit den Ergänzungssätzen zum quadratischen Reziprozitätsgesetz berechnet werden.

Satz 1.3.6 (Erster und zweiter Ergänzungssatz)
Sei $n > 1$ *eine ungerade natürliche Zahl. Dann gilt*

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} \qquad \text{(Erster Ergänzungssatz)}$$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} \qquad \text{(Zweiter Ergänzungssatz)}$$

Bemerke: Ist n nicht prim, so folgt aus $\left(\frac{a}{n}\right) = 1$ für das Jacobi-Symbol nicht notwendig, dass a quadratischer Rest mod n ist. Es gilt zum Beispiel mit dem

zweiten Ergänzungssatz zum quadratischen Reziprozitätsgesetz

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1)^{\frac{3^2-1}{8}} \cdot (-1)^{\frac{5^2-1}{8}} = (-1)(-1) = 1,$$

aber 2 ist weder quadratischer Rest mod 3 noch mod 5, also auch kein quadratischer Rest mod 15.

1.4 Zum Kreisteilungsproblem

Die geometrische Aufgabe der Kreisteilungstheorie, einen Kreis in eine gegebene Anzahl n gleicher Teile zu zerlegen, kann auf die algebraische Aufgabe, nämlich die Lösung der Gleichung n-ten Grades

$$x^n = 1$$

zurückgeführt werden. In Bezug auf die folgenden Definitionen und Sätze sei insbesondere auf (Bachmann, 1968a) verwiesen.

Definition 1.4.1 (n-te Einheitswurzel)
Die komplexen Wurzeln der Gleichung n-ten Grades

$$x^n = 1 \tag{1.4}$$

heißen n-te Einheitswurzeln.

Sei g eine n-te Einheitswurzel, d.h. $g^n = 1$, dann gilt für eine beliebige ganze Potenz k von g

$$(g^k)^n = (g^n)^k = 1,$$

also ist g^k ebenfalls eine Wurzel der Gleichung (1.4). Weiter gibt es unter den Wurzeln g, g^2, g^3, ... mindestens eine, die gleich Eins ist.

Der kleinste Exponent m derart, dass $g^m = 1$ gilt, wird als der Exponent bezeichnet, zu dem die Wurzel g gehört. Umgekehrt nennt man dann g die zum Exponenten m gehörige n-te Einheitswurzel. Es gilt: Jede n-te Einheitswurzel gehört zu einem Exponenten, der ein Teiler von n ist.

Definition 1.4.2 (Primitive n-te Einheitswurzel)
Eine zum Exponenten n gehörige Wurzel der Gleichung (1.4) heißt eine primitive n-te Einheitswurzel.

Für diese gilt folgender Satz: Die Gleichung $x^n = 1$ hat $\varphi(n)$ primitive Einheitswurzeln (siehe Definition 1.2.1 der Eulerschen φ-Funktion).

Sei weiter r eine primitive Wurzel der Gleichung (1.4), dann sind die Potenzen

$$r, \quad r^2, \quad r^3, \quad \ldots, \quad r^n \tag{1.5}$$

alle (verschiedene) Wurzeln der Gleichung (1.4). Damit ist die Kreisteilungsaufgabe auf die Bestimmung einer primitiven n-ten Einheitswurzel zurückgeführt.

Behauptung 1.4.3 *Sei r eine primitive n-te Einheitswurzel. Der Exponent einer Potenz von r kann stets durch seinen kleinsten positiven Rest* mod p *ersetzt werden.*

Beweis: Für jedes $m \in \mathbb{Z}_{>0}$ gibt es Zahlen $a,\ b \in \mathbb{Z}$, wobei $0 < b < n$, sodass

$$m = an + b.$$

Daraus folgt

$$r^m = r^{an+b} = \underbrace{(r^n)^a}_{=1} \cdot r^b = r^b.$$

Somit ergibt sich die Behauptung. □

Die Behauptung 1.4.3 liefert unmittelbar eine weitere wichtige Aussage:

Folgerung 1.4.4
Es gilt genau dann $r^m = r^{m'}$, wenn $m \equiv m' \pmod{n}$ ist, wobei r eine primitive n-te Einheitswurzel bezeichnet.

Man bemerke, dass r auch mit negativem Exponenten r^{-m} aufgefasst werden kann. In diesem Fall versteht man darunter r^b, wobei b der kleinste positive Rest von $-m \pmod{n}$ ist.

Zum Spezialfall $n = p$ prim

Setzen wir nun $n = p$, ist also der Exponent eine Primzahl, so erhalten wir alle $(p-1)$ primitiven Wurzeln der Gleichung

$$x^p = 1 \tag{1.6}$$

als Wurzeln der Gleichung

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0. \tag{1.7}$$

Definition 1.4.5 (Kreisteilungsgleichung)
Die Gleichung (1.7) der primitiven p-ten Einheitswurzeln heißt Kreisteilungsgleichung.

Genügt ein r der Gleichung (1.7), so können alle Wurzeln von (1.7)

$$r, \quad r^2, \quad r^3, \quad \ldots, \quad r^{p-1} \tag{1.8}$$

bestimmt werden.

Von besonderer Bedeutung ist die Tatsache, dass die Kreisteilungsgleichung

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = \sum_{k=0}^{p-1} x^k = 0.$$

irreduzibel ist. Die entsprechenden Beweise und die Folgerungen aus der Irreduzibilität der Kreisteilungsgleichung sind in (Bachmann, 1968a, 5. Vorlesung) dargestellt.

Die Kreisteilungstheorie befasst sich fast ausschließlich mit dem Fall $n = p$ (p prim) und entwickelt Methoden zur Auflösung der Kreisteilungsgleichung. Unten werden wir das Prinzip dieser Methoden erläutern und einige Hilfsmittel betrachten.

1.5 Höhere Kongruenzen für einen Primzahlmodul

In diesem Abschnitt betrachten wir die Kongruenzen der Form

$$x^m \equiv a \pmod{p}, \tag{1.9}$$

wobei wir voraussetzen, dass p prim und a teilerfremd zu p ist.

Definition 1.5.1 (m-ter Potenzrest bzw. Nichtrest mod p)
Ist die Kongruenz (1.9) lösbar, gibt es also eine ganze Zahl x, deren m-te Potenz kongruent $a \pmod{p}$ ist, so heißt a ein m-ter Potenzrest mod p. *Andernfalls ist a ein m-ter* Nichtrest mod p.

Im Fall $m = 2$ handelt es sich also um quadratische Reste mod p bzw. quadratische Nichtreste mod p (vgl. Abschnitt 1.3).

Kriterium für einen m-ten Potenzrest bzw. Nichtrest mod p

Nach einigen Vorbereitungen möchten wir ein Kriterium ableiten, mithilfe dessen sich bestimmen lässt, ob eine Zahl a ein m-ter Potenzrest mod p ist oder nicht.

Man überlege zunächst Folgendes: Genügt eine ganze Zahl z zwei Kongruenzen, etwa

$$z^m \equiv 1 \pmod{p} \qquad \text{und} \qquad z^n \equiv 1 \pmod{p},$$

so genügt sie auch

$$z^d \equiv 1 \pmod{p},$$

wobei $d = \mathrm{ggT}(m, n)$ ist. Jede Wurzel der Kongruenz $z^m \equiv 1 \pmod{p}$ genügt nach dem kleinen Satz von Fermat der Kongruenz $z^{p-1} \equiv 1 \pmod{p}$. Also wird sie auch die Kongruenz $z^d \equiv 1 \pmod{p}$ erfüllen, wobei $d = \mathrm{ggT}(m, p-1)$ ist.

Nun kommen wir auf die Kongruenz $x^m \equiv a \pmod{p}$ zurück. Den vorangehenden Überlegungen zufolge hat diese genau dieselben Wurzeln wie auch

$$x^d \equiv a \pmod{p} \tag{1.10}$$

mit $d = \mathrm{ggT}(m, p-1)$. Durch die Erhebung der Kongruenz (1.10) zur $\left(\frac{p-1}{d}\right)$-ten Potenz ergibt sich zunächst

$$\underbrace{\left(x^d\right)^{\frac{p-1}{d}}}_{=x^{p-1}} \equiv a^{\frac{p-1}{d}} \pmod{p}.$$

Mit dem kleinen Satz von Fermat erhalten wir schließlich die Kongruenz

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}. \tag{1.11}$$

Jeder der (insgesamt $\frac{p-1}{d}$) m-ten Potenzreste mod p ist also eine Wurzel der Kongruenz (1.11). Diese hat genau $\frac{p-1}{d}$ Wurzeln, was bedeutet, dass keine weitere Zahl ihr genügen kann. Daher besteht die Kongruenz (1.11) *nicht* für m-te Nichtreste mod p.

Nun können wir das Resultat in folgendem Satz formulieren.

Satz 1.5.2 (Kriterium für einen m-ten Potenzrest mod p)
Sei p eine Primzahl und $d = \mathrm{ggT}(m, p-1)$. Eine Zahl a ist ein m-ter Potenz-

rest mod p*, das heißt die Kongruenz*

$$x^m \equiv a \pmod{p}$$

besitzt eine Lösung, genau dann, wenn gilt:

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}.$$

Über die Wurzeln der Kongruenz $x^{p-1} \equiv 1 \pmod{p}$

Die Kongruenz

$$x^{p-1} \equiv 1 \pmod{p} \tag{1.12}$$

ist von besonderer Bedeutung, weil ihre Wurzeln ähnliche Eigenschaften wie die Einheitswurzeln haben. In Analogie zur obigen Betrachtung der Wurzeln der Gleichung $x^n = 1$ betrachten wir nun die Wurzeln von (1.12).

Nach dem kleinen Satz von Fermat genügt der Kongruenz (1.12) jede durch p nicht teilbare Zahl. Da der Grad dieser Kongruenz $(p-1)$ beträgt, gibt es genau $(p-1)$ Lösungen bzw. Wurzeln. Diese sind den Zahlen

$$1, \quad 2, \quad 3, \quad \ldots, \quad p-1 \tag{1.13}$$

mod p kongruent.

Ist ω eine Wurzel der Kongruenz (1.12), so wird auch jede Potenz von ω ebenfalls eine Wurzel von (1.12) sein. Unter ihnen gibt es mindestens eine, welche kongruent Eins mod p ist. Dem kleinen Satz von Fermat zufolge ist dies nämlich ω^{p-1}.

Definition 1.5.3 (Primitive Wurzel mod p)
Eine zum Exponenten $(p-1)$ *gehörige Zahl heißt* primitive Wurzel mod p*.*

Es gilt folgender Satz: Es gibt $\varphi(p-1)$ primitive Wurzeln mod p. (Siehe Definition 1.2.1 der Eulerschen φ-Funktion.)

Sei weiter g eine primitive Wurzel mod p. Dann bilden die Potenzen

$$g, \quad g^2, \quad g^3, \quad \ldots, \quad \underbrace{g^{p-1}}_{\equiv 1 \pmod{p}} \tag{1.14}$$

alle (einander mod p inkongruente) Wurzeln der Kongruenz (1.12).

Als Ergebnis der vorangegangenen Überlegungen erhalten wir: Die Zahlen der Folge (1.13) sind (bis auf die Ordnung) den Zahlen der Folge (1.14) mod p kongruent.

Definition 1.5.4 (Index)
Ist ω eine durch p nicht teilbare Zahl, so gibt es eine Zahl μ aus der Menge

$$\{1, \quad 2, \quad 3, \quad \ldots, \quad p-1\},$$

sodass gilt

$$\omega \equiv g^{\mu} \pmod{p},$$

wobei g eine primitive Wurzel mod p *bezeichnet. Ein solches μ heißt* Index *(auch ‚diskreter Logarithmus' genannt) von ω zur* Basis *g. Die Notation ist: $\mu = \operatorname{ind}_g(\omega) = \operatorname{ind}(\omega)$.*

Im Folgenden möchten wir einige Eigenschaften der Indizes betrachten.

Seien $\omega \equiv g^{\operatorname{ind}\omega} \pmod{p}$ und $v \equiv g^{\operatorname{ind} v} \pmod{p}$. Dann gilt

$$\omega v \equiv g^{\operatorname{ind}\omega + \operatorname{ind} v} \pmod{p},$$

woraus folgt

$$\operatorname{ind}(\omega v) \equiv \operatorname{ind}\omega + \operatorname{ind} v \pmod{p-1}. \tag{1.15}$$

Ferner gilt nach dem kleinen Satz von Fermat $1 \equiv g^{p-1} \pmod{p}$ und folglich ist

$$\operatorname{ind}(1) = p - 1. \tag{1.16}$$

Außerdem ist es leicht zu sehen, dass die Gleichheit $\operatorname{ind}(\omega) = \operatorname{ind}(\omega')$ gilt, wenn $\omega \equiv \omega' \pmod{p}$ ist. Es gilt dann

$$\operatorname{ind}(p-1) = \frac{p-1}{2} \qquad \text{und} \qquad \operatorname{ind}(-1) = \frac{p-1}{2}. \tag{1.17}$$

Weiteres zu den Eigenschaften von Indizes findet sich in (Bachmann, 1968a, 4. Vorlesung).

1.6 Über die Gaußsche Methode zur Lösung der Kreisteilungsgleichung

In Abschnitt 1.4 wurde das Problem der Kreisteilung auf die Lösung der Kreisteilungsgleichung zurückgeführt. Nun wollen wir uns mit dem Prinzip der Gaußschen Methode zur Lösung der Kreisteilungsgleichung befassen. Eine ausführliche Beschreibung der Gaußschen Methode findet sich in (Bachmann, 1968a, 6. Vorlesung), einige Beispiele dazu werden in (Bachmann, 1968a, 7. Vorlesung) erläutert.

Die Idee dieser Methode ist, die Auflösung der Kreisteilungsgleichung auf die Auflösung mehrerer Gleichungen von kleinerem Grade zurückzuführen. Genauer geht man dabei folgendermaßen vor: Man bildet bestimmte ganze Funktionen von den Wurzeln der Kreisteilungsgleichung, welche durch die Auflösung einer Gleichung von kleinerem Grade bestimmt werden können. Nützlicherweise sollen diese Funktionen von der Art sein, dass sich alle Wurzeln der Kreisteilungsgleichung aus den Werten der Funktionen ergeben.

Am Ende des Abschnitts 1.4 haben wir bereits gezeigt: Ist r eine Wurzel der Kreisteilungsgleichung

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = 0, \tag{1.18}$$

so sind die Potenzen

$$r, \quad r^2, \quad r^3, \quad \ldots, \quad r^{p-1} \tag{1.19}$$

alle Wurzeln von (1.18).

In Abschnitt 1.5 wurde außerdem gezeigt, dass die Potenzen einer primitiven Wurzel $g \bmod p$

$$1, \quad g, \quad g^2, \quad g^3, \quad \ldots, \quad g^{p-2}$$

bis auf die Reihenfolge den Zahlen

$$1, \quad 2, \quad 3, \quad \ldots, \quad p-1$$

$\bmod p$ kongruent sind.

Aufgrund der Folgerung 1.4.4 können die Exponenten in der Folge (1.19) durch die zu ihnen $\bmod p$ kongruenten Zahlen ersetzt werden. Das bedeutet, dass die

Potenzen aus (1.19) bis auf die Reihenfolge mit den Potenzen

$$r, \quad r^g, \quad r^{g^2}, \quad \ldots, \quad r^{g^{p-2}} \tag{1.20}$$

übereinstimmen.

In Folge (1.20) hat jedes Glied die Eigenschaft, die g-te Potenz seines Vorgängergliedes zu sein. Das erste Glied r kann insbesondere als die g-te Potenz des letzten Gliedes $r^{g^{p-2}}$ gesehen werden, da gilt

$$r = r^1 = r^{g^{p-1}} = \left(r^{g^{p-2}}\right)^g.$$

Aus diesen Überlegungen folgt nun, dass die Wurzeln der Kreisteilungsgleichung (1.18) auch durch die Folge (1.20) gegeben werden können – also durch die Folge, in welcher die erste Wurzel eine rationale Funktion der letzten und jede andere Wurzel dieselbe rationale Funktion der vorangehenden ist.

Gaußsche Perioden

Sei weiter ℓ ein Teiler von $(p-1)$, sodass gilt

$$p - 1 = \ell f.$$

Mit r wird weiterhin eine primitive p-te Einheitwurzel und mit g eine primitive Wurzel mod p bezeichnet. Die $(p-1)$ Größen

$$r, \quad r^g, \quad r^{g^2}, \quad \ldots, \quad r^{g^{p-2}}$$

können dann in ℓ Gruppen mit jeweils f Gliedern verteilt werden:

$$\begin{array}{ccccc}
r, & r^{g^\ell}, & r^{g^{2\ell}}, & \ldots, & r^{g^{(f-1)\ell}} \\
r^g, & r^{g^{\ell+1}}, & r^{g^{2\ell+1}}, & \ldots, & r^{g^{(f-1)\ell+1}} \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
r^{g^{\ell-1}}, & r^{g^{2\ell-1}}, & r^{g^{3\ell-1}}, & \ldots, & r^{g^{f\ell-1}}
\end{array}$$

In jeder Gruppe sind die Wurzeln jeweils so geordnet, dass jede davon die g^ℓ-te Potenz der vorangehenden und die erste die g^ℓ-te Potenz der letzten ist.

Nun bilden wir für jede Gruppe die Summe aller Wurzeln dieser Gruppe.

Definition 1.6.1
Die ℓ Summen

$$\begin{aligned}
\eta_0 &= r + r^{g^\ell} + r^{g^{2\ell}} + \ldots + r^{g^{(f-1)\ell}} \\
\eta_1 &= r^g + r^{g^{\ell+1}} + r^{g^{2\ell+1}} + \ldots + r^{g^{(f-1)\ell+1}} \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\eta_{\ell-1} &= r^{g^{\ell-1}} + r^{g^{2\ell-1}} + r^{g^{3\ell-1}} + \ldots + r^{g^{f\ell-1}}
\end{aligned}$$

heißen die (f-gliedrigen) Gaußschen Perioden.

Allgemeiner kann man schreiben:

$$\eta_k = \sum_{t=0}^{f-1} r^{g^{\ell t+k}} \qquad (k = 0, 1, \ldots, \ell-1). \tag{1.21}$$

Die Summe aller Gaußschen Perioden ist gleich der Summe aller Wurzeln der Kreisteilungsgleichung, also gilt offenbar:

$$\sum_{k=0}^{\ell-1} \eta_k = -1.$$

Die Gaußschen Perioden haben eine Reihe interessanter Eigenschaften. Wir nennen hier nur einige davon.

Lemma 1.6.2

(i) Ersetzt man in einer beliebigen Periode η_k die Wurzel r durch eine andere Wurzel der Periode η_0, so bleibt η_k unverändert.

(ii) Ersetzt man in einer beliebigen Periode η_k die Wurzel r durch eine Wurzel einer anderen Periode als η_0, so vertauschen sich die Perioden zyklisch.

Beweis: (i) Wir ersetzen nun in

$$\eta_k = r^{g^k} + r^{g^{\ell+k}} + r^{g^{2\ell+k}} + \ldots + r^{g^{(f-2)\ell+k}} + r^{g^{(f-1)\ell+k}}$$

die Wurzel r durch r^{g^ℓ} und erhalten

$$\begin{aligned}
\eta_k &= \left(r^{g^\ell}\right)^{g^k} + \left(r^{g^\ell}\right)^{g^{\ell+k}} + \left(r^{g^\ell}\right)^{g^{2\ell+k}} + \ldots + \left(r^{g^\ell}\right)^{g^{(f-2)\ell+k}} + \left(r^{g^\ell}\right)^{g^{(f-1)\ell+k}} \\
&= r^{g^{\ell+k}} + r^{g^{2\ell+k}} + r^{g^{3\ell+k}} + \ldots + r^{g^{(f-1)\ell+k}} + \underbrace{r^{g^{f\ell+k}}}_{=r^{g^k}},
\end{aligned}$$

wobei für den letzten Summanden

$$r^{g^{f\ell+k}} = \left(r^{g^{f\ell}}\right)^{g^k} = \left(r^{g^{p-1}}\right)^{g^k} = r^{g^k}$$

wegen $f\ell = p-1$ und $g^{p-1} = 1$ gilt. Die Periode η_k bleibt demnach unverändert. Ebenso beim Ersetzen der Wurzel r durch $r^{g^{m\ell}}$ für die Werte $m = 0, 1, 2, \ldots, f-1$.

(ii) Wenn wir r durch r^{g^h} in η_0 ersetzen, so erhalten wir

$$\begin{aligned}&\left(r^{g^h}\right)^1 + \left(r^{g^h}\right)^{g^\ell} + \left(r^{g^h}\right)^{g^{2\ell}} + \ldots + \left(r^{g^h}\right)^{g^{(f-2)\ell}} + \left(r^{g^h}\right)^{g^{(f-1)\ell}} \\ =&r^{g^h} + r^{g^{\ell+h}} + r^{g^{2\ell+h}} + \ldots + r^{g^{(f-2)\ell+h}} + r^{g^{(f-1)\ell+h}},\end{aligned}$$

das heißt η_0 wird zu η_h. Weiter kann man sehen, dass η_1 zu η_{h+1} wird, usw. Die Perioden werden demnach um h Stellen zyklisch verschoben. □

Was die weiteren Eigenschaften der Gaußschen Perioden betrifft, erwähnen wir noch, dass die Verteilung aller Wurzeln der Kreisteilungsgleichung in Perioden von der Wahl der primitiven Einheitswurzel unabhängig ist und dass die ℓ Perioden numerisch voneinander verschieden sind. Näheres dazu findet sich ebenfalls in (Bachmann, 1968a, 6. Vorlesung).

Ferner wird ebenda gezeigt, dass die f-gliedrigen Perioden $\eta_0, \ldots, \eta_{\ell-1}$ die Wurzeln einer irreduziblen Gleichung mit ganzzahligen Koeffizienten vom Grade ℓ sind. Alle Wurzeln dieser Gleichung können aus einer beliebigen unter ihnen durch Wiederholung einer rationalen Operation bestimmt werden, wie dies auch bei der Kreisteilungsgleichung der Fall ist. Hat man zunächst eine Periode und daraus alle anderen f-gliedrigen Perioden gefunden, so können ℓ Perioden-Gleichungen vom Grade f aufgestellt werden. Ihre Auflösung ergibt dann die Auflösung der Kreisteilungsgleichung. Es ist klar, dass es dabei genügt, eine der Perioden-Gleichungen aufzulösen. Man zerlegt an dieser Stelle f in Faktoren ℓ', f', was zur Bildung von $\ell\ell'$ kleineren f'-gliedrigen Perioden führt und setzt analog wie bisher das Verfahren fort, bis man zu Perioden mit je einem Glied kommt. Darin besteht das Prinzip der Gaußschen Methode zur Auflösung der Kreisteilungsgleichung.

1.7 Lagrange- und Jacobi-Resolventen

Eine weitere Methode zur Auflösung der Kreisteilungsgleichung basiert auf Lagrangeschen und Jacobischen Resolventen, auch ‚Lagrangesche Summen' bzw. ‚Jacobische Summen' genannt. In der Literatur werden diese nicht immer unterschieden. Wir formulieren die Definitionen in Anlehnung an (Ribenboim, 1979, Lecture VII) und (Bachmann, 1968a, 8. Vorlesung).

Seien p, q ungerade Primzahlen, $q \neq p$. Weiter bezeichnet ω eine primitive $(q-1)$-te Einheitswurzel, r eine primitive q-te Einheitswurzel und g eine primitive Wurzel mod q. Die *Lagrangesche Resolvente* oder *Summe* wird dann wie folgt definiert:

$$\langle \omega, r \rangle = r + \omega r^g + \omega^2 r^{g^2} + \ldots + \omega^{q-2} r^{g^{q-2}} \tag{1.22}$$

Unter Benutzung des Summenzeichens werden die *Lagrange-Resolventen* als Summen

$$\left\langle \omega^h, r \right\rangle = \sum_{\lambda=0}^{q-2} \omega^{h\lambda} r^{g^\lambda} \qquad (h = 0, 1, \ldots, q-2) \tag{1.23}$$

dargestellt.

Sei weiter μ der (kleinste positive) λ-te Potenzrest mod q, das heißt $\mu \equiv g^\lambda \pmod q$ ist. Unter Benutzung der Definition des Index heißt dies $\lambda = \operatorname{ind}(\mu)$. Für r bzw. ω gilt dann:

$$r^{g^\lambda} = r^\mu \qquad \text{bzw.} \qquad \omega^{h\lambda} = \omega^{h \operatorname{ind}(\mu)}.$$

Da λ die Werte $0, 1, \ldots, q-2$ durchläuft, erhält μ die Werte $1, 2, \ldots, q-1$. Nun summieren wir über $\mu = 1, 2, \ldots, q-1$ und erhalten dann aus der Formel (1.23)

$$\left\langle \omega^h, r \right\rangle = \sum_{\lambda=0}^{q-2} \omega^{h\lambda} r^{g^\lambda} = \sum_{\mu=1}^{q-1} \omega^{h \operatorname{ind}(\mu)} r^\mu \qquad (h = 0, 1, \ldots, q-2). \tag{1.24}$$

Ist $h = 0$, so ergibt sich aus der letzten Formel der Wert von $\langle 1, r \rangle$, nämlich

$$\langle 1, r \rangle = \sum_{\mu=1}^{q-1} r^\mu = -1$$

wegen der Kreisteilungsgleichung für r.

Mit der Formel

$$r = \frac{1}{p-1}\left(\langle 1, r\rangle + \langle \omega, r\rangle + \left\langle \omega^2, r\right\rangle + \ldots + \left\langle \omega^{q-2}, r\right\rangle\right) \tag{1.25}$$

lassen sich ferner die Wurzeln der Kreisteilungsgleichung ermitteln, siehe dazu (Bachmann, 1968a, 8. Vorlesung).

Jacobi definierte ähnliche Summen für den Fall, dass die Zahlen p und q der Kongruenz $q \equiv 1 \pmod{p}$ genügen, das heißt $q = pf + 1$ mit einem geraden f. Ist weiter m eine ganze durch p nicht teilbare Zahl und ist β eine primitive p-te Einheitswurzel, so sind die *Jacobi-Resolventen* oder *Summen* die folgenden Summen:

$$[\beta^m, r] = \sum_{\mu=1}^{q-1} \beta^{m\,\mathrm{ind}(\mu)} r^{\mu} = \sum_{\lambda=0}^{q-2} \beta^{m\lambda} r^{g^{\lambda}} \tag{1.26}$$

Es ist in der Tat leicht zu sehen, wie der Übergang von den Lagrange-Summen (1.24) zu den Jacobi-Summen (1.26) geschieht: Setzen wir $\beta = \omega^f$, so bedeutet β unter Beachtung, dass $\omega^{q-1} = 1$ und $q - 1 = fp$ ist, eine primitive p-te Einheitswurzel. Wenn wir außerdem $h = mf$ setzen, so erhalten wir

$$\left\langle \omega^h, r\right\rangle = \left\langle \omega^{mf}, r\right\rangle = \left\langle \left(\omega^f\right)^m, r\right\rangle = [\beta^m, r]\,. \tag{1.27}$$

Einige weitere Eigenschaften von Resolventen werden wir unter anderem in Kapitel 3 im Zusammenhang mit dem Beweis des Satzes von Dickson betrachten.

Kapitel 2

Sophie-Germain-Begleitprimzahlen

Im vorliegenden Kapitel beschäftigen wir uns mit dem Ansatz von Sophie Germain zum Beweis der Unlösbarkeit der Fermat-Gleichung für Primzahlexponenten $p \geq 3$ im I. Fall (siehe dazu unter anderem (Ribenboim, 1979)). In diesem Rahmen werden wir den Satz von Sophie Germain formulieren und beweisen. Zudem führen wir den für diese Arbeit zentralen Begriff der Sophie-Germain-Begleitprimzahl ein und untersuchen die Eigenschaften der so bezeichneten Zahlen.

2.1 Lemma von Sophie Germain

Der Ansatz von Sophie Germain zur Lösung des Fermat-Problems beruht auf einem naheliegenden Gedanken über den Zusammenhang zwischen den diophantischen Gleichungen und Kongruenzen: Falls die Gleichung

$$x^p + y^p + z^p = 0$$

eine ganzzahlige Lösung besitzt, so ist auch die Kongruenz

$$x^p + y^p + z^p \equiv 0 \pmod{m}$$

für jeden beliebigen Modul m lösbar. Um die Unmöglichkeit der Fermat-Gleichung zu zeigen, untersucht man also die Folgerungen für x, y, z aus solchen Kongruenzen für einen ‚geeigneten' Modul, bis sich ein Widerspruch ergibt.

Lemma 2.1.1 (Sophie Germain 1819, aus einem Brief an Gauß)
Falls die Fermat-Gleichung

$$x^p + y^p = z^p \tag{2.1}$$

für den Exponenten p eine nicht-triviale Lösung besitzt und falls $q \neq p$ eine weitere Primzahl ist, sodass es keine nicht-trivialen aufeinander folgenden p-ten Potenzen mod q *gibt, dann teilt q eine der Zahlen x, y, z.*

Die Bedingung des Lemmas besagt also, dass die Kongruenz

$$1 + u^p \equiv v^p \pmod{q}$$

keine Lösungen mit $uv \not\equiv 0 \pmod{q}$ besitze.

Beweis: Wir führen einen indirekten Beweis und nehmen an, dass die Fermat-Gleichung (2.1) Lösungen mit $xyz \neq 0$ und $q \nmid xyz$ besitzt. Dann existiert ein x' derart, dass

$$x'x \equiv 1 \pmod{q}.$$

Multipliziert man die Fermat-Gleichung (2.1) mit x'^p, so erhält man die Kongruenz

$$(x'x)^p + (x'y)^p \equiv (x'z)^p \pmod{q}$$

und da $(x'x)^p \equiv 1 \pmod{q}$ ist, folgt schließlich

$$1 + u^p \equiv v^p \pmod{q}.$$

Demnach sind u^p und v^p aufeinander folgende p-te Potenzen $\pmod{q}$, diese sind ungleich Null, da q keine der Zahlen x', y, z teilt. Das ergibt einen Widerspruch, daraus folgt dann die Behauptung. □

Der Ansatz von Sophie Germain beruht auf folgender Idee: Angenommen, die Fermat-Gleichung (2.1) für einen gegebenen Exponenten p besitzt eine nicht-triviale Lösung, das heißt $xyz \neq 0$. Falls es zu diesem p *unendlich viele* Primzahlen gibt, die der Bedingung des Lemmas genügen, so hätte die Zahl xyz unendlich viele Primteiler, was offensichtlich nicht sein kann. Damit wäre das Fermat-Problem für den Exponenten p gelöst. Deshalb stellt sich die Frage nach

der Existenz solcher zum Primzahlexponenten p ‚begleitender' Primzahlen q. In Kapitel 3 werden wir noch einmal darauf zurück kommen.

2.2 Satz von Sophie Germain

Die folgende Aussage enthält zusätzlich zu der Bedingung des Lemmas 2.1.1 eine weitere Voraussetzung und ist als Satz von Sophie Germain bekannt.

Satz 2.2.1 (Sophie Germain)
Es sei p eine ungerade Primzahl. Falls es zu diesem p eine weitere ungerade Primzahl $q \neq p$ gibt, sodass folgende Bedingungen erfüllt sind:

(i) p ist keine p-te Potenz mod q*, das heißt die Kongruenz $x^p \equiv p \pmod{q}$ besitzt keine Lösung, und*

(ii) aus der Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ für $x, y, z \in \mathbb{Z}$ folgt, dass q eine der Zahlen x, y oder z teilt,

dann gilt der I. Fall des letzten Satzes von Fermat (das heißt, es existiert keine ganzzahlige Lösung mit $p \nmid xyz$).

Der Beweis des Satzes von Sophie Germain wird nach einigen Vorbereitungen im letzten Abschnitt 2.5 dieses Kapitels geführt.

Wir wollen noch untersuchen, welche Gestalt ein q zum gegebenen p notwendigerweise haben muss, um den Bedingungen des Satzes von Sophie Germain zu genügen.

Jede der beiden Bedingungen (i) und (ii) des Satzes von Sophie Germain kann nur dann erfüllt sein, wenn $(q-1)$ durch p teilbar ist. Dies folgt unmittelbar aus den folgenden Lemmata 2.2.2 und 2.2.3.

Lemma 2.2.2
Sei p eine ungerade Primzahl. Weiter sei q eine ungerade Primzahl derart, dass $p \nmid (q-1)$. Dann hat die Kongruenz $x^p \equiv p \pmod{q}$ (genau) eine Lösung. Insbesondere ist dann die Bedingung (i) des Satzes von Sophie Germain verletzt.

Beweis: Seien p und q zwei ungerade Primzahlen so, dass $p \nmid (q-1)$, also ist

$$d = \mathrm{ggT}(p, q-1) = 1.$$

Zum Beweis wollen wir nun den Satz 1.5.2 benutzen, der für unsere Notation besagt: Ist $d = \mathrm{ggT}(p, q-1)$, so besitzt die Kongruenz $x^p \equiv p \pmod{q}$ genau dann eine Lösung, wenn $p^{\frac{q-1}{d}} \equiv 1 \pmod{q}$ gilt.

Da nach dem kleinen Satz von Fermat für p die Kongruenz $p^{q-1} \equiv 1 \pmod{q}$ gilt, also auch $p^{\frac{g-1}{d}} \equiv 1 \pmod{q}$ gilt, folgt dann mit dem letzten Kriterium, dass die Kongruenz

$$x^p \equiv p \pmod{q}$$

lösbar ist. Somit ist die Bedingung (i) des Satzes von Sophie Germain offensichtlich verletzt. □

Lemma 2.2.3
Sei p eine ungerade Primzahl. Weiter sei q eine ungerade Primzahl derart, dass $p \nmid (q-1)$. Dann besitzt die Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ nicht-triviale Lösungen. Insbesondere ist dann die Bedingung (ii) des Satzes von Sophie Germain verletzt.

Beweis: Seien p und q zwei ungerade Primzahlen so, dass $p \nmid (q-1)$, also ist

$$d = \mathrm{ggT}(p, q-1) = 1.$$

Dann gibt es $a,\ b \in \mathbb{Z}$ so, dass $ap + b(q-1) = 1$.
Für beliebige $u,\ v,\ w$ mit $q \nmid uvw$, welche der Kongruenz

$$u + v + w \equiv 0 \pmod{q} \tag{2.2}$$

genügen, gilt also

$$u = u^{ap+b(q-1)} = u^{ap}(u^{q-1})^b. \tag{2.3}$$

Da dem kleinen Satz von Fermat zufolge $u^{q-1} \equiv 1 \pmod{q}$ gilt, folgt aus der Gleichung (2.3)

$$u \equiv u^{ap} \equiv (u^a)^p \pmod{q}.$$

Analog gilt für v bzw. w

$$v \equiv (v^a)^p \pmod{q} \qquad \text{bzw.} \qquad w \equiv (w^a)^p \pmod{q}.$$

Betrachtet man dann die Kongruenz (2.2), so erhält man mit den letzten Kongruenzen für $u,\ v,\ w \pmod{q}$

$$(u^a)^p + (v^a)^p + (w^a)^p \equiv 0 \pmod{q}.$$

Daraus folgt, dass $x = u^a$, $y = v^a$, $z = w^a$ eine nicht-triviale Lösung der Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ darstellt. Die Bedingung (ii) des Satzes von Sophie Germain ist damit offenbar verletzt. □

Die Primzahlen p, q mit den im Satz von Sophie Germain beschriebenen Eigenschaften genügen also der Bedingung $p \mid (q-1)$ und somit der Kongruenz

$$q \equiv 1 \pmod{p}.$$

Daraus folgt, dass q folgendermaßen dargestellt werden kann:

$$q = fp + 1,$$

wobei f notwendigerweise gerade ist, da sonst q nicht prim sein könnte. Sei also $f = 2m$, dann hat q stets folgende Gestalt:

$$q = 2mp + 1.$$

2.3 Sophie-Germain-Begleitprimzahlen

2.3.1 Definition und Beispiele

Definition 2.3.1 (Sophie-Germain-Begleitprimzahl zu p)
Sei p eine ungerade Primzahl. Eine Primzahl q von der Gestalt $q = 2mp + 1$, die den Bedingungen des Satzes von Sophie Germain genügt, nennen wir Sophie-Germain-Begleitprimzahl zu p. *Ein solches m nennen wir* Multiplikator.

Beispiel 2.3.2 (Sophie-Germain-Begleitprimzahlen zu $p = 3, 5, 7$)
Zu $p = 3$ gibt es folgende zwei Sophie-Germain-Begleitprimzahlen q_i mit entsprechenden Multiplikatoren m_i, $i = 1, 2$:

$$q_1 = 2 \cdot 1 \cdot 3 + 1 = 7, \quad m_1 = 1,$$
$$q_2 = 2 \cdot 2 \cdot 3 + 1 = 13, \quad m_2 = 2.$$

Zu $p = 5$ gibt es folgende vier Sophie-Germain-Begleitprimzahlen q_i mit ent-

sprechenden Multiplikatoren m_i, $i = 1, 2, 3, 4$:

$$\begin{aligned} q_1 &= 2 \cdot 1 \cdot 5 + 1 = 11, \quad m_1 = 1, \\ q_2 &= 2 \cdot 4 \cdot 5 + 1 = 41, \quad m_2 = 4, \\ q_3 &= 2 \cdot 7 \cdot 5 + 1 = 71, \quad m_3 = 7, \\ q_4 &= 2 \cdot 10 \cdot 5 + 1 = 101, \quad m_4 = 10. \end{aligned}$$

Zu $p = 7$ *gibt es folgende vier Sophie-Germain-Begleitprimzahlen* q_i *mit entsprechenden Multiplikatoren* m_i, $i = 1, 2, 3, 4$:

$$\begin{aligned} q_1 &= 2 \cdot 2 \cdot 7 + 1 = 29, \quad m_1 = 2, \\ q_2 &= 2 \cdot 5 \cdot 7 + 1 = 71, \quad m_2 = 5, \\ q_3 &= 2 \cdot 8 \cdot 7 + 1 = 113, \quad m_3 = 8, \\ q_4 &= 2 \cdot 35 \cdot 7 + 1 = 491, \quad m_4 = 35. \end{aligned}$$

Diese und weitere Beispiele werden in Kapitel 4 genauer beschrieben und analysiert.

Es stellt sich die Frage, ob jede ganze Zahl als Multiplikator auftreten kann. Dazu zeigen wir Folgendes: Die Vielfachen von 3 können nicht als Multiplikatoren auftreten. Das folgt unmittelbar aus dem nächsten Lemma.

Lemma 2.3.3
Sei p *eine ungerade Primzahl. Weiter sei die Primzahl* q *von der Gestalt*

$$q = 2 \cdot (3k) \cdot p + 1 = 6kp + 1.$$

Dann existieren ganze Zahlen x, y, z, *alle inkongruent Null* mod q, *sodass* $x^p + y^p + z^p \equiv 0 \pmod{q}$ *gilt. Insbesondere ist dann die Bedingung (ii) des Satzes von Sophie Germain verletzt.*

Beweis: Seien also p und $q = 6kp + 1$ zwei ungerade Primzahlen. Weiter sei g eine primitive Wurzel mod q, das heißt

$$g^{q-1} \equiv 1 \pmod{q}.$$

Wegen der Gleichheit $q - 1 = 6kp$ ist dann auch

$$\left(g^{2kp}\right)^3 \equiv 1 \pmod{q}.$$

Sei $\bar{g} = g \pmod{q}$. Dann ist $\bar{g}^{2kp}$ eine primitive kubische Einheitswurzel im Körper $\mathbb{F}_q$. Daraus folgt

$$\underbrace{\left(\bar{g}^{2kp}\right)^2}_{=\bar{g}^{4kp}} + \bar{g}^{2kp} + 1 = 0 \quad \text{in} \quad \mathbb{F}_q.$$

Diese Gleichung in $\mathbb{F}_q$ kann als Kongruenz für den Primzahlmodul q dargestellt werden:

$$\left(g^{4k}\right)^p + \left(g^{2k}\right)^p + 1^p \equiv 0 \pmod{q}.$$

Somit hat die Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ eine nicht-triviale Lösung

$$x = g^{4k}, \quad y = g^{2k}, \quad z = 1.$$

Die Bedingung (ii) des Satzes von Sophie Germain für dieses q ist demnach verletzt. □

2.3.2 Sophie-Germain-Primzahlen

Definition 2.3.4 (Sophie-Germain-Primzahl)
Ist für eine Primzahl p auch die Zahl $2p + 1$ prim, so heißt p Sophie-Germain-Primzahl.

Lemma 2.3.5
Es sei p eine Sophie-Germain-Primzahl, dann gilt der I. Fall des großen Satzes von Fermat für den Exponenten p. Insbesondere ist $q := 2p + 1$ eine Sophie-Germain-Begleitprimzahl zu p mit dem kleinstmöglichen Multiplikator $m = 1$.

Beweis: Sei p eine Sophie-Germain-Primzahl, das heißt $q = 2p + 1$ ist prim. Es ist zu überprüfen, ob die Bedingungen (i) und (ii) des Satzes von Sophie Germain erfüllt sind.

Angenommen, die Kongruenz $p \equiv x^p \pmod{q}$ besitzt Lösungen. Wegen der Gleichheit $p = \frac{q-1}{2}$ und des Eulerschen Kriteriums für das Legendre-Symbol erhalten wir dann

$$p \equiv x^p = x^{\frac{q-1}{2}} \equiv \left(\frac{x}{q}\right) \pmod{q}. \tag{2.4}$$

Für das Legendre-Symbol gilt $\left(\frac{x}{q}\right) = \pm 1$. Zusammen mit (2.4) ergibt sich dann die Kongruenz $p \equiv \pm 1 \pmod{q}$. Das ist ein Widerspruch.

Weiter sei angenommen, dass die Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ gilt und dass $q \nmid xyz$. Dem kleinen Satz von Fermat zufolge gelten die Kongruenzen

$$x^{q-1} \equiv 1 \pmod{q}, \qquad y^{q-1} \equiv 1 \pmod{q}, \qquad z^{q-1} \equiv 1 \pmod{q}.$$

Daraus folgt zunächst

$$x^{\frac{q-1}{2}} \equiv \pm 1 \pmod{q}, \qquad y^{\frac{q-1}{2}} \equiv \pm 1 \pmod{q}, \qquad z^{\frac{q-1}{2}} \equiv \pm 1 \pmod{q}$$

und schließlich, da $\frac{q-1}{2} = p$ ist,

$$x^p \equiv \pm 1 \pmod{q}, \qquad y^p \equiv \pm 1 \pmod{q}, \qquad z^p \equiv \pm 1 \pmod{q}.$$

Wegen der Annahme muss somit gelten $\pm 1 \pm 1 \pm 1 \equiv 0 \pmod{q}$. Dies ergibt einen Widerspruch. □

2.3.3 Ergebnisse von Legendre und Dickson

Es gibt außerdem zwei weiterführende Resultate von Legendre und Dickson, die aus der Existenz bestimmter Primzahlen $fp + 1$ für ein p auf den I. Fall des großen Satzes von Fermat schließen lassen, siehe hierzu (Bachmann, 1976, Nr. 22 ff.) und (Dickson, 1908).

Lemma 2.3.6 (Legendre)
Es sei $p > 3$ eine Primzahl. Für den Exponenten p gilt der I. Fall des großen Satzes von Fermat, falls eine der Linearformen

$$4p + 1, \quad 8p + 1, \quad 10p + 1, \quad 14p + 1, \quad 16p + 1 \tag{2.5}$$

eine Primzahl liefert.

Auf diese Weise gelang es Legendre, die Unlösbarkeit des großen Satzes von Fermat im I. Falle für alle Primzahlexponenten $p < 197$ zu zeigen, siehe dazu Tabelle 1 in Kapitel 4.

Dabei sei noch auf die Ausnahme der Primzahl 3 hingewiesen. Denn obwohl die Zahlen

$$10p + 1 = 10 \cdot 3 + 1 = 31 \qquad \text{und} \qquad 14p + 1 = 14 \cdot 3 + 1 = 43$$

beide prim sind, gibt es in diesen Fällen aufeinander folgende dritte Potenzen mod 31 bzw. mod 43:

$$\begin{aligned} 4^3 &\equiv 1^3 + 1 \pmod{31}, \qquad \text{da} \quad 64 \equiv 2 \pmod{31} \quad \text{bzw.} \\ (-9)^3 &\equiv 1^3 + 1 \pmod{43}, \qquad \text{da} \quad -729 \equiv -41 \equiv 2 \pmod{43}. \end{aligned}$$

Dickson erweiterte die Liste (2.5) der Linearformen von Legendre und zeigte folgende Aussage:

Lemma 2.3.7 (Dickson)
Es sei p eine ungerade Primzahl. Für den Exponenten p gibt es keine ganzen durch p nicht teilbaren Lösungen der Fermat-Gleichung, falls eine der Zahlen

$$\begin{aligned} &2p+1, \quad 4p+1, \quad 8p+1, \quad 16p+1, \\ &10p+1 \quad (\textit{ausgenommen} \quad p = 3), \\ &14p+1 \quad (\textit{ausgenommen} \quad p = 3), \\ &20p+1 \quad (\textit{ausgenommen} \quad p = 3), \\ &22p+1 \quad (\textit{ausgenommen} \quad p = 3, 31), \\ &26p+1 \quad (\textit{ausgenommen} \quad p = 3, 5), \\ &28p+1 \quad (\textit{ausgenommen} \quad p = 7), \\ &32p+1 \quad (\textit{ausgenommen} \quad p = 3), \\ &40p+1 \quad (\textit{ausgenommen} \quad p = 7), \\ &56p+1 \quad (\textit{ausgenommen} \quad p = 5, 11, 17, 113, 227), \\ &64p+1 \quad (\textit{ausgenommen} \quad p = 3, 7, 229, 337, 757) \end{aligned} \tag{2.6}$$

prim ist.

Ferner stellte Dickson fest, dass es für alle ungeraden Primzahlen $p < 1700$, mit Ausnahme von

$$p = 197, 223, 257, 383, 389, 457, 569, 751, 1373, 1399, 1531, \tag{2.7}$$

mindestens eine Primzahl $fp + 1$ wie in Lemma (2.3.7) gibt. Für diese elf Primzahlen zeigt Dickson den I. Fall des großen Satzes von Fermat zum Teil mit den Kriterien von Legendre und Sophie Germain, zum Teil mit anderen Methoden. In Kapitel 4 (Tabelle 2) werden wir Sophie-Germain-Begleitprimzahlen und die entsprechenden Multiplikatoren zu allen elf Primzahlen aus (2.7) angeben.

2.4 Vorbereitungen zum Beweis des Satzes von Sophie Germain

2.4.1 Allgemeine Überlegungen

In der Bedingung (ii) des Satzes von Sophie Germain steht die Fermat-Gleichung in der symmetrischen Form. Diese erhält man, indem man eine der Zahlen x, y, z als negativ auffasst, deshalb von z zu $-z$ übergeht und z^p in der Fermat-Gleichung (2.1) $x^p + y^p = z^p$ auf die linke Seite bringt. Dann entsteht die Fermat-Gleichung in der symmetrischen Form

$$x^p + y^p + z^p = 0. \tag{2.8}$$

Daraus folgt

$$\begin{aligned}(-z)^p &= x^p + y^p \\ &= (x+y)\frac{x^p + y^p}{x+y} \\ &= (x+y)(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \ldots - xy^{p-2} + y^{p-1}) \\ &= (x+y)(x^{p-1} + x^{p-2}(-y) + \ldots + x(-y)^{p-2} + (-y)^{p-1}) \\ &= (x+y)\sum_{i=0}^{p-1} x^{p-1-i}(-y)^i. \end{aligned} \tag{2.9}$$

Man erkennt aus der Summendarstellung des zweiten Faktors, dass $\frac{x^p+y^p}{x+y}$ eine ganze Zahl ist. Später werden wir die Teilbarkeitseigenschaft dieses Ausdrucks betrachten.

Zunächst definieren wir eine (homogene) ganzzahlige Funktion $Q_n(.,.)$ wie folgt: Für $n \geq 1$, a, $b \in \mathbb{Z}$, $ab \neq 0$ sei

$$Q_n(a,b) = \sum_{i=0}^{n-1} a^{n-1-i}(-b)^i. \tag{2.10}$$

Diese Summe kann auch auf folgende Weise dargestellt werden:

$$Q_n(a,b) = \sum_{i=0}^{n-1} (-b/a)^i \, a^{n-1}.$$

Ist $a+b \neq 0$, so folgt mit der geometrischen Summenformel

$$Q_n(a,b) = \frac{a^n - (-b)^n}{a-(-b)} = \frac{a^n - (-b)^n}{a+b}$$

und ist außerdem n ungerade, so gilt

$$Q_n(a,b) = \frac{a^n + b^n}{a+b}. \tag{2.11}$$

Damit wird schließlich aus (2.9)

$$(-z)^p = x^p + y^p = (x+y)\, Q_p(x,y). \tag{2.12}$$

Behauptung 2.4.1 *Falls* $p \nmid (x+y)$, *dann ist* $\mathrm{ggT}\left(Q_p(x,y), x+y\right) = 1$.

Beweis: Sei r ein Primteiler von $(x+y)$, das heißt, es gilt

$$x + y \equiv 0 \pmod{r} \tag{2.13}$$

und folglich auch

$$y \equiv -x \pmod{r}. \tag{2.14}$$

Betrachten wir die Gleichung $Q_p(x,y) = \sum_{i=0}^{p-1} x^{p-1-i}(-y)^i$ modulo r, so ergibt sich mit der Kongruenz (2.14)

$$Q_p(x,y) \equiv \sum_{i=0}^{p-1} x^{p-1-i}\, x^i \equiv p x^{p-1} \pmod{r}. \tag{2.15}$$

Wir wollen zeigen, dass $r \nmid Q_p(x,y)$. Angenommen, $r \mid Q_p(x,y)$, das heißt auch $r \mid p x^{p-1}$. Dann gibt es zwei mögliche Fälle.

Fall $r \mid p$: Da p prim ist, muss gelten $r = p$. Weiter, da $(x+y)$ durch r teilbar ist, folgt, dass $(x+y)$ auch durch p teilbar ist. Dies ergibt jedoch einen Widerspruch zur Voraussetzung, dass $p \nmid (x+y)$.

Fall $r \mid x^{p-1}$ impliziert, dass x durch r teilbar ist, was aber wegen der Kongruenz (2.14) zur Folge hätte, dass auch y durch r teilbar wäre. Dies ist ein Widerspruch zur Teilerfremdheit von x und y.

Daraus folgt die Behauptung. □

Behauptung 2.4.2 *Sei p prim. Es gilt $x^p + y^p + z^p \equiv x + y + z \equiv 0 \pmod{p}$.*

Beweis: Mit dem kleinen Satz von Fermat gelten die Kongruenzen

$$x^p \equiv x \pmod{p}, \qquad y^p \equiv y \pmod{p}, \qquad z^p \equiv z \pmod{p}.$$

Somit ergibt sich die Behauptung. □

2.4.2 Herleitung der Barlow-Abel-Relationen

Satz 2.4.3 (Barlow-Abel-Relationen)
Falls die Fermat-Gleichung (2.8) eine Lösung besitzt und $p \neq 2$ die Zahl z nicht teilt, dann existieren $u_z,\ v_z,\ u_x,\ v_x,\ u_y,\ v_y \in \mathbb{Z}$ so, dass folgende Beziehungen bestehen:

$$x + y = u_z^p, \qquad \frac{x^p + y^p}{x + y} = v_z^p, \qquad z = -u_z v_z, \tag{2.16}$$

$$y + z = u_x^p, \qquad \frac{y^p + z^p}{y + z} = v_x^p, \qquad x = -u_x v_x, \tag{2.17}$$

$$z + x = u_y^p, \qquad \frac{z^p + x^p}{z + x} = v_y^p, \qquad y = -u_y v_y. \tag{2.18}$$

Insbesondere gilt:

$$\begin{aligned} p \nmid u_z v_z, &\qquad \mathrm{ggT}(u_z, v_z) = 1, \\ p \nmid u_x v_x, &\qquad \mathrm{ggT}(u_x, v_x) = 1, \\ p \nmid u_y v_y, &\qquad \mathrm{ggT}(u_y, v_y) = 1. \end{aligned}$$

Beweis: Wegen der Behauptung 2.4.2 gilt die Kongruenz $-z \equiv x + y \pmod{p}$. Da nach Voraussetzung $p \nmid z$ gilt, folgt $p \nmid (x + y)$.

Der Einfachheit halber führen wir neue Größen s und t für $(x + y)$ bzw. $Q_p(x, y)$ ein. Nach Behauptung 2.4.1 sind s und t teilerfremd und es gilt $p \nmid st$. Mit der Gleichung (2.12) ist dann $(-z)^p = st$. Das bedeutet, dass st und folglich auch jeder der Faktoren s und t eine durch p nicht teilbare p-te Potenz einer ganzen Zahl ist. Demnach können diese dargestellt werden als

$$s = u_z^p, \qquad t = v_z^p$$

mit $u_z,\ v_z \in \mathbb{Z},\ p \nmid u_z v_z$ und $\mathrm{ggT}(u_z, v_z) = 1$.

Daraus lassen sich also folgende Beziehungen herleiten:

$$x + y = u_z^p, \qquad \frac{x^p + y^p}{x + y} = v_z^p, \qquad z = -u_z v_z.$$

Aus der Symmetrie der Fermat-Gleichung (2.8) in Bezug auf x, y, z schließt man analog weitere Relationen:

$$y + z = u_x^p, \qquad \frac{y^p + z^p}{y + z} = v_x^p, \qquad x = -u_x v_x$$

$$z + x = u_y^p, \qquad \frac{z^p + x^p}{z + x} = v_y^p, \qquad y = -u_y v_y,$$

wobei u_x, v_x bzw. u_y, v_y die analogen Eigenschaften aufweisen wie u_z, v_z. Damit ist der Satz vollständig bewiesen. □

Definition 2.4.4
Die Formeln (2.16), (2.17), (2.18) aus dem Satz 2.4.3 heißen Barlow-Abel-Relationen *oder* -Formeln.

Weiteres zu Barlow-Abel-Relationen siehe in (Ribenboim, 1979, Lecture IV).

2.4.3 Folgerungen aus den Barlow-Abel-Relationen

Aus der ersten der drei Barlow-Abel-Formeln (2.16) folgt unmittelbar:

$$x = u_z^p - y. \tag{2.19}$$

Weiter implizieren die Barlow-Abel-Relationen (2.17) die Gleichheit

$$y = u_x^p - z \tag{2.20}$$

und aus den Barlow-Abel-Formeln (2.18) folgt zudem

$$z = u_y^p - x. \tag{2.21}$$

Das Einsetzen von (2.20) bzw. (2.21) für y bzw. z in die Gleichung (2.19) liefert

$$\begin{aligned} x &\underset{(2.20)}{=} u_z^p - (u_x^p - z) \underset{(2.21)}{=} u^p - \left(u_x^p - (u_y^p - x)\right) \\ &= u_z^p - u_x^p + u_y^p - x. \end{aligned}$$

Für x ergibt sich also folgende Formel:

$$x = \frac{u_z^p - u_x^p + u_y^p}{2}. \tag{2.22}$$

Die erste der drei Barlow-Abel-Relationen (2.16) impliziert außerdem die Gleichung

$$y = u_z^p - x.$$

Setzt man hier die Formel (2.22) für x ein, so erhält man für y:

$$\begin{aligned} y &= u_z^p - \frac{u_z^p - u_x^p + u_y^p}{2} \\ &= \frac{u_z^p + u_x^p - u_y^p}{2}. \end{aligned} \tag{2.23}$$

Durch Einsetzen der Formel (2.22) für x in (2.21)

$$z = u_y^p - x$$

erhalten wir zudem für z:

$$\begin{aligned} z &= u_y^p - \frac{u_z^p - u_x^p + u_y^p}{2} \\ &= \frac{-u_z^p + u_x^p + u_y^p}{2}. \end{aligned} \tag{2.24}$$

2.5 Beweis des Satzes von Sophie Germain

Beweis: Seien p und $q = fp + 1$ zwei ungerade Primzahlen. Ferner gelten folgende Bedingungen:

(i) p ist keine p-te Potenz mod q und

(ii) $x^p + y^p + z^p \equiv 0 \pmod{q}$ impliziert $x \equiv 0$, $y \equiv 0$ oder $z \equiv 0 \pmod{q}$.

Zu zeigen ist, dass es keine ganzzahlige Lösung mit $p \nmid xyz$ gibt.

Wir führen einen indirekten Beweis und nehmen das Gegenteil an, dass es also nicht-triviale ganzzahlige Lösungen mit $p \nmid xyz$ gibt.

Seien $x, y, z \in \mathbb{Z}$ paarweise teilerfremd so, dass $x^p + y^p + z^p \equiv 0 \pmod{q}$ erfüllt ist. Nach Bedingung (ii) des Satzes von Sophie Germain teilt q eine der Zahlen x, y, z. Ohne Beschränkung der Allgemeinheit gelte $q \mid x$ und $q \nmid yz$.

Wegen der Formel (2.22) gilt die Kongruenz

$$u_z^p - u_x^p + u_y^p = 2x \equiv 0 \pmod{q}. \tag{2.25}$$

Nach der Bedingung (ii) des Satzes teilt q dann auch eine der Zahlen u_z, u_x, u_y. Es ist leicht zu sehen, dass $q \nmid u_z$ (denn sonst würde gelten $q \mid x$ und $q \mid y$) und $q \nmid u_y$ (denn sonst würde gelten $q \mid x$ und $q \mid z$). Da also $q \nmid u_z u_y$, gilt $q \mid u_x$. Somit folgt aus der ersten der drei Barlow-Abel-Relationen (2.17) die Kongruenz

$$y \equiv -z \pmod{q}. \tag{2.26}$$

Wenn man die wegen der Barlow-Abel-Relationen (2.16) bestehende Gleichung

$$(x+y)v_z^p = x^p + y^p$$

modulo q betrachtet, so erhält man mit (2.25) die Kongruenz

$$yv_z^p \equiv y^p$$

und folglich

$$v_z^p \equiv y^{p-1} \pmod{q}. \tag{2.27}$$

Für die Funktion $Q_p(y,z) = \sum_{i=0}^{p-1} y^{p-1-i}(-z)^i$ (vgl. Formel (2.10)) unter Beachtung der Kongruenz (2.26) $y \equiv -z \pmod{q}$ ergibt sich

$$\begin{aligned} Q_p(y,z) &\equiv \sum_{i=0}^{p-1} y^{p-1-i}\, y^i \pmod{q} \\ &\equiv \sum_{i=0}^{p-1} y^{p-1} \pmod{q} \\ &\equiv py^{p-1} \pmod{q}. \end{aligned} \tag{2.28}$$

Aus der zweiten der drei Barlow-Abel-Formeln (2.17) unter Anwendung der Gleichung $Q_p(y,z) = \frac{y^p+z^p}{y+z}$ (vgl. Formel (2.11)) erhält man mit der Kongruenz (2.28)

$$v_x^p = \frac{y^p + z^p}{y+z} = Q_p(y,z) \equiv py^{p-1} \pmod{q}.$$

Wegen der Kongruenz (2.27) folgt daraus schließlich

$$v_x^p \equiv p v_z^p \pmod{q}. \tag{2.29}$$

Weiter gilt $q \nmid v_z$ (denn sonst würde gelten $q \mid z$). Sei dann v_z' so, dass

$$v_z' v_z \equiv 1 \pmod{q}.$$

Durch Multiplizieren beider Seiten der letzten Kongruenz (2.29) mit ${v_z'}^p$ erhalten wir

$$v_x^p {v_z'}^p \equiv p v_z^p {v_z'}^p \pmod{q},$$

was also die Kongruenz

$$(v_x v_z')^p \equiv p \pmod{q}$$

impliziert. Demnach ist p eine p-te Potenz mod q. Dies ergibt jedoch einen Widerspruch zur Bedingung (i). Daraus folgt die Behauptung des Satzes von Sophie Germain. □

Kapitel 3

Dicksons Schranke

Dickson formulierte und bewies in (Dickson, 1909) einen Satz über die Existenz der zu q teilerfremden, also nicht-trivialen Lösungen der Fermat-Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$, sobald q eine gewisse (vom Exponenten p abhängige) Schranke übersteigt.

Mit dem Satz von Dickson ist also gezeigt, dass die Kongruenz

$$x^p + y^p + z^p \equiv 0 \pmod{q}$$

nicht zum Beweis der Unlösbarkeit der Fermat-Gleichung

$$x^p + y^p = z^p$$

für eine Primzahl $p \geq 3$ benutzt werden kann. Insbesondere liefert der Satz eine *obere Schranke* für die Sophie-Germain-Begleitprimzahlen zu einem p.

Um den großen Satz von Fermat für ein gegebenes p mit der Methode von Sophie Germain beweisen zu können, wäre jedoch der Beweis nötig, dass zu einem gegebenen p unendlich viele Sophie-Germain-Begleitprimzahlen existieren. Dieser Zusammenhang wurde bereits in Kapitel 2 ausgeführt. Der Beweis der Existenz von Dicksons Schranke zeigt daher zugleich, dass der Beweisansatz von Sophie Germain für den großen Satz von Fermat nicht erfolgreich sein kann.

Im folgenden Kapitel werden wir den Satz von Dickson formulieren und in einzelnen Schritten beweisen. Dabei werden wir die Erkenntnisse der Kreisteilungstheorie benutzen.

3.1 Satz von Dickson

Satz 3.1.1 (Dickson)
Seien p und q ungerade Primzahlen. Dann besitzt die Fermat-Kongruenz

$$x^p + y^p + z^p \equiv 0 \pmod{q} \tag{3.1}$$

nicht-triviale Lösungen x, y, z für jedes $q \geq S(p)$, wobei gilt

$$S(p) = (p-1)^2(p-2)^2 + 6p - 2. \tag{3.2}$$

In Bezug auf den Satz von Sophie Germain (siehe Satz 2.2.1) und die Sophie-Germain-Begleitprimzahlen (siehe Definition 2.3.1) bedeutet der Satz von Dickson, dass es stets nur endlich viele Primzahlen q gibt, für welche die Kongruenz (3.1) nur dann lösbar ist, wenn q mindestens eine der Zahlen x, y, z teilt. Der Satz von Dickson liefert also eine wichtige Einsicht:

Folgerung 3.1.2 (Dicksons Schranke für Sophie-Germain-Begleitprimzahlen)
Es gibt nur endlich viele Sophie-Germain-Begleitprimzahlen zu einem gegebenen p. Dicksons Schranke $S(p) = (p-1)^2(p-2)^2 + 6p - 2$ *stellt dabei eine obere Schranke für die Sophie-Germain-Begleitprimzahlen zu einem gegebenen p dar.*

Man bemerke, dass in der Voraussetzung des Satzes von Dickson nicht gefordert wird, dass $(q-1)$ durch p teilbar ist. Man beschränkt sich desweiteren nicht auf die Sophie-Germain-Begleitprimzahlen q zu p. Der Satz macht vielmehr eine allgemeine Aussage über die Lösbarkeit der Kongruenz (3.1). Der Vollständigkeit halber muss der Beweis also für zwei Fälle geführt werden:

(D1) falls $(q-1)$ und p teilerfremd sind bzw.

(D2) falls $(q-1)$ durch p teilbar ist.

3.2 Zur Struktur des Beweises

Der Beweis des Satzes von Dickson gliedert sich in zwei Teile. Der erste Teil behandelt den Fall (D1). Die Diskussion dieses Falles wird zeigen: Sind p, q zwei ungerade Primzahlen und gilt $p \nmid (q-1)$, so besitzt die Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ stets nicht-triviale Lösungen. Dies gilt offenbar auch für q, das eine gewisse Schranke übersteigt.

Der Fall (D2) für Primzahlen p und $q = 2mp + 1 = fp + 1$ wird im zweiten Teil behandelt. Zu Beginn der Diskussion wird für den Spezialfall $3 \mid m$ gezeigt, dass die Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ stets nicht-triviale Lösungen besitzt. Deshalb wird im darauf folgenden Beweis $3 \nmid f$ vorausgesetzt.

Der zweite Teil ist wiederum in mehrere Abschnitte untergliedert. Zu Beginn wird jeweils erläutert, was der Gegenstand und das Ziel der Untersuchungen in dem betreffenden Abschnitt ist.

Für den Beweis des Satzes von Dickson im Fall (D2) wird zunächst die Frage nach den nicht-trivialen Lösungen der Kongruenz

$$x^p + y^p + z^p \equiv 0 \pmod{q}$$

auf die Untersuchung der nicht-trivialen Lösungen der Kongruenz

$$1 + g^{pt} \equiv g^{p\tau} \pmod{q}$$

zurückgeführt. Daraufhin wird Bezug zur Kreisteilungstheorie hergestellt, weil diese die allgemeinere Kongruenz $1 + g^{pt+a} \equiv g^{p\tau+\alpha} \pmod{q}$ betrachtet. Die Anzahlfunktion $N(a, \alpha)$ wird eingeführt. Diese bezeichnet die Anzahl der Zahlen t, zu denen eine Zahl τ existiert, sodass die letzte Kongruenz lösbar ist ($t, \tau = 0, 1, \ldots, f-1$ und $a, \alpha = 0, 1, \ldots, p-1$). Nach diesen Überlegungen wird die Zielsetzung präzisiert: Zum gegebenen p ist eine Schranke $S(p)$ gesucht, sodass für alle $q \geq S(p)$ stets $N(0,0) > 0$ gilt.

Nachdem wir die Zielsetzung herausgearbeitet und formuliert haben, betrachten wir einige Hilfsmittel aus der Kreisteilungstheorie wie Gaußsche Perioden, Lagrange- und Jacobi-Resolventen, die Jacobi-Kreisteilungsfunktionen und deren Eigenschaften. Den Ansatz liefert schließlich die Formel $\Psi_n(\beta) \cdot \Psi_n(\beta^{-1}) = q$ ($n = 1, 2, \ldots p-2$), wobei $\Psi_n(\beta)$ die Jacobi-Kreisteilungsfunktion bezeichnet. Weiterführende Betrachtungen werden eine andere Darstellung von $\Psi_n(\beta)$ ergeben. Für die dabei neu eingeführten Größen werden in einzelnen Abschnitten Gleichungen aufgestellt oder diese werden abgeschätzt. Das Ergebnis wird folgende Ungleichung sein:

$$p^2 N(0,0) > q + 1 - 3p - (p-1)(p-2)\sqrt{q}.$$

Aus dieser Ungleichung lässt sich eine untere Schranke für q folgern, sodass für alle $q \geq S(p)$ gilt: $N(0,0) > 0$.

3.3 Beweis des Satzes von Dickson: Erster Fall

Die Frage nach der Lösbarkeit der Kongruenz (3.1) im Falle (D1) lässt sich einfach beantworten (vgl. Lemma 2.2.3 in Kapitel 2): Sind nämlich p und q ungerade Primzahlen derart, dass $p \nmid (q-1)$, so existieren ganze Zahlen a, b mit

$$ap + b(q-1) = 1.$$

Für drei durch q nicht teilbare Zahlen u, v, w gilt dann

$$\begin{aligned} u = u^{ap+b(q-1)} &\equiv (u^a)^p \pmod{q}, \\ v = v^{ap+b(q-1)} &\equiv (v^a)^p \pmod{q}, \\ w = w^{ap+b(q-1)} &\equiv (w^a)^p \pmod{q}. \end{aligned}$$

Wählt man also u, v, w mit $q \nmid uvw$, welche zudem der Kongruenz

$$u + v + w \equiv 0 \pmod{q}$$

genügen, so besteht auch die Kongruenz

$$(u^a)^p + (v^a)^p + (v^a)^p \equiv 0 \pmod{q}.$$

Demnach hat die Kongruenz

$$x^p + y^p + z^p \equiv 0 \pmod{q}$$

eine nicht-triviale Lösung $x = u^a$, $y = v^a$, $z = w^a$. Somit ist der Satz für den Fall $p \nmid (q-1)$ bewiesen. (D1) □

3.4 Beweis des Satzes von Dickson: Zweiter Fall

Nun können wir zum interessanteren Fall (3.1), nämlich $p \mid (q-1)$, übergehen. Wir erinnern uns, dass dieser Fall insbesondere bei der Betrachtung der Sophie-Germain-Begleitprimzahlen zu p zutrifft, da sonst die Bedingungen des Satzes von Sophie Germain verletzt sind. (In Kapitel 2 wurde dies durch die Lemmata 2.2.2 und 2.2.3 bereits gezeigt.) Ferner folgt daraus, dass q stets die spezielle Gestalt $q = 2mp + 1$ hat.

Weiter kann man voraussetzen, dass $3 \nmid m$. Denn für $q = 6kp + 1$ besitzt die

Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ stets die nicht-triviale Lösung $x = g^{4k}$, $y = g^{2k}$, $z = 1$, wobei g eine primitive Wurzel mod q bezeichnet, siehe dazu Lemma 2.3.3 in Kapitel 2.

Im Folgenden werden wir schreiben $q - 1 = fp$ mit einem notwendigerweise geraden $f = 2m$ so, dass $3 \nmid f$ gilt.

3.4.1 Über die Kongruenz $1 + g^{pt} \equiv g^{p\tau} \pmod{q}$

Behauptung 3.4.1 *Sei g eine primitive Wurzel* mod q. *Dann hat die Fermat-Kongruenz (3.1) $x^p + y^p + z^p \equiv 0 \pmod{q}$ genau dann zu q teilerfremde ganzzahlige Lösungen x, y, z, wenn die Kongruenz*

$$1 + g^{pt} \equiv g^{p\tau} \pmod{q} \tag{3.3}$$

ganze Lösungen t, τ hat.

Ähnliche Überlegungen zum Zusammenhang der Kongruenz (3.1) und der Kongruenz vom Typ (3.3) wurden bereits im Beweis von Lemma 2.1.1 geführt.

Beweis: „$\Longrightarrow$“: Da x, y, z teilerfremd zu q sind, gilt $q \nmid xyz$. Dann impliziert die Kongruenz (3.1), dass es ein x' derart gibt, dass $x'x \equiv 1 \pmod{q}$. Nach dem Multiplizieren von (3.1) mit x' erhalten wir

$$\underbrace{(x'x)^p}_{\equiv 1 \pmod{q}} + (x'y)^p \equiv (-x'z)^p \pmod{q}.$$

Daraus folgt, dass also die Kongruenz $1 + u^p \equiv v^p \pmod{q}$ für bestimmte u, v lösbar ist.

Ist g eine primitive Wurzel mod q, so existieren Zahlen t, $\tau \in \mathbb{Z}$, welche den Kongruenzen $u \equiv g^t \pmod{q}$ und $v \equiv g^\tau \pmod{q}$ genügen. Somit ist auch die Kongruenz

$$1 + g^{pt} \equiv g^{p\tau} \pmod{q}$$

lösbar.

„$\Longleftarrow$“: Gehen wir von der Lösbarkeit der Kongruenz $1 + g^{pt} \equiv g^{p\tau} \pmod{q}$ aus, wobei t, $\tau \in \mathbb{Z}$ und g eine primitive Wurzel mod q bezeichnet, so ist auch die Kongruenz

$$g^{pf} + g^{pt} \equiv g^{p\tau} \pmod{q}$$

lösbar, da $1 \equiv g^{q-1} \pmod{q}$ und $q - 1 = pf$ ist. Die letzte ist gleichbedeutend mit

$$(g^f)^p + (g^t)^p \equiv (g^\tau)^p \pmod{q}.$$

Folglich besitzt die Kongruenz

$$x^p + u^p + z^p \equiv 0 \pmod{q}$$

zu q teilerfremde Lösungen $x = g^f$, $y = g^t$, $z = -g^\tau$.

Somit ist die Behauptung 3.4.1 bewiesen. □

3.4.2 Die Anzahlfunktion N und die Formulierung des Ziels

Mit g sei weiterhin die primitive Wurzel mod q bezeichnet. Die Kongruenz (3.3) ist ein Spezialfall der allgemeineren Kongruenz

$$1 + g^{pt+a} \equiv g^{p\tau+\alpha} \pmod{q}. \tag{3.4}$$

Diese Kongruenz bedeutet, dass von zwei aufeinander folgenden Zahlen die erste den Restcharakter a und die zweite den Restcharakter α hat. Die Größen a, α durchlaufen dabei die Werte $0, 1, \ldots, p-1$. Die Kongruenz vom Typ (3.4) spielt eine Rolle in der Kreisteilungstheorie bei Aufstellung der Gleichungen, denen die Gaußschen Perioden (siehe Abschnitt 1.6) genügen, ausführlicher siehe dazu (Bachmann, 1968a, 15. Vorlesung).

Für gegebene $a, \alpha \in \{0, 1, \ldots, p-1\}$ sei $N_{p,q}(a, \alpha)$ die Anzahlfunktion. Im Folgenden schreiben wir dafür $N(a, \alpha)$. Diese steht für die Anzahl der ganzen Zahlen $t \in \{0, 1, \ldots, f-1\}$, für welche die Kongruenz (3.4) durch ein geeignetes $\tau \in \{0, 1, \ldots, f-1\}$ gelöst werden kann. Setzt man weiter $a = 0$ und $\alpha = 0$, so bedeutet $N(0,0)$ die Anzahl der Zahlen t, zu denen es ein τ gibt, sodass die Kongruenz (3.3) Lösungen besitzt, wobei $t, \tau \in \{0, 1, \ldots, f-1\}$.

Mit Behauptung 3.4.1 wurde die Frage nach den nicht-trivialen Lösungen der Fermat-Kongruenz (3.1) zunächst auf die Untersuchung der Lösungen der Kongruenz (3.3) zurückgeführt. Nachdem wir nun die Anzahlfunktion eingeführt haben, können wir die Fragestellung noch spezieller formulieren, nämlich: Unter welchen Bedingungen gilt $N(0,0) > 0$?

Unser *Ziel* ist also, zum gegebenen p eine Schranke $S(p)$ zu finden, sodass für alle $q \geq S(p)$ stets $N(0,0) > 0$ gilt.

3.4.3 Gaußsche Perioden, Lagrange- und Jacobi-Summen

Wir erinnern uns, dass $q-1=pf$ gilt. Im Folgenden seien r eine primitive q-te Einheitswurzel und g eine primitive Wurzel mod q. Die p (f-gliedrigen) Gaußschen Perioden sind folgende Summen (vgl. Abschnitt 1.6 und Definition 1.6.1 bzw. Formel (1.21)):

$$\eta_k = \sum_{t=0}^{f-1} r^{g^{pt+k}} \qquad (k=0,\,1,\,\ldots,\,p-1). \tag{3.5}$$

Sei weiter ω eine primitive $(q-1)$-te Einheitswurzel. Die Lagrangeschen Resolventen können dann auf folgende Weise bestimmt werden (vgl. Abschnitt 1.7, Formel (1.24)):

$$\begin{aligned} \left\langle \omega^h, r \right\rangle &= \sum_{\lambda=0}^{q-2} \omega^{h\lambda} r^{g^\lambda} && (h=1,\,\ldots,\,p-1), \\ \langle 1, r\rangle &= -1 && (h=0). \end{aligned} \tag{3.6}$$

Wenn wir $\beta=\omega^f$ setzen, so ist β eine primitive p-te Einheitswurzel (wegen $\omega^{q-1}=1$ und $q-1=fp$). Wird noch $h=mf$ gesetzt, so ist $\omega^h=\omega^{mf}=\beta^m$. Aus (3.6) erhält man dann die Jacobi-Summen (vgl. Abschnitt 1.7, Formel (1.26)):

$$\begin{aligned} [\beta^m, r] &= \sum_{\lambda=0}^{q-2} \beta^{m\lambda} r^{g^\lambda} && (m=1,\,\ldots,\,p-1), \\ [1, r] &= -1 && (m=0). \end{aligned} \tag{3.7}$$

Schreiben wir in (3.7) weiter $\lambda=pt+k$, so ergeben sich *spezielle* Jacobi-Summen, welche lineare Kombinationen der Gaußschen Perioden darstellen:

$$\begin{aligned} [\beta^m, r] &= \sum_{\lambda=0}^{q-2} \beta^{m\lambda} r^{g^\lambda} \underset{(\lambda=pt+k)}{=} \sum_{k=0}^{p-1}\sum_{t=0}^{f-1} \beta^{m(pt+k)} r^{g^{pt+k}} \\ &\underset{(\beta^{mpt}=1)}{=} \sum_{k=0}^{p-1}\sum_{t=0}^{f-1} \beta^{km} r^{g^{pt+k}} = \sum_{k=0}^{p-1} \beta^{km} \underbrace{\sum_{t=0}^{f-1} r^{g^{pt+k}}}_{\underset{(3.5)}{=}\eta_k} \\ &= \sum_{k=0}^{p-1} \beta^{km}\eta_k \qquad (m=0,\,1,\,\ldots,\,p-1). \end{aligned} \tag{3.8}$$

3.4.4 Über die Eigenschaften der Resolventen und die Jacobi-Kreisteilungsfunktion $\Psi_n(\beta)$

In diesem Abschnitt wollen wir zunächst einige Eigenschaften der Lagrangeschen bzw. Jacobischen Resolventen betrachten, welche in der Kreisteilungstheorie gezeigt werden. Ferner werden wir die Jacobi-Kreisteilungsfunktionen $\Psi_n(\beta)$ für $n = 1, \ldots, p-2$ definieren und zeigen:

$$\Psi_n(\beta) \cdot \Psi_n(\beta^{-1}) = q \qquad (n = 1, 2, \ldots p-2).$$

An dieses Ergebnis werden wir in Abschnitt 3.4.7 anschließen.

Im Folgenden wird unter $\operatorname{ind}(.)$ der Index zur Basis g für den Primzahlmodul q verstanden, wobei g eine fest gewählte primitive Wurzel mod q ist. Falls gilt $(q-1) \nmid (h+k)$, so lässt sich für die Lagrangeschen Summen folgende Formel herleiten:

$$\frac{\langle \omega^h, r\rangle \langle \omega^k, r\rangle}{\langle \omega^{h+k}, r\rangle} = \sum_{\mu=1}^{q-2} \omega^{h \operatorname{ind}(\mu) - (h+k)\operatorname{ind}(1+\mu)}. \qquad (*)$$

Dabei bezeichnet ω eine primitive $(q-1)$-te Einheitswurzel (siehe (Bachmann, 1968a, Seite 86, Formel (28))). Der Ausdruck auf der linken Seite ist demnach eine ganze und ganzzahlige Funktion der Wurzel ω.

Für die Jacobi-Summen ergibt sich aus $(*)$ eine analoge Formel für den Fall, dass $p \nmid (m+n)$, für $h = mf$ und $k = nf$:

$$\frac{[\beta^m, r][\beta^n, r]}{[\beta^{m+n}, r]} = \sum_{\mu=1}^{q-2} \beta^{m \operatorname{ind}(\mu) - (m+n)\operatorname{ind}(1+\mu)}, \qquad (3.9)$$

dabei bezeichnet β eine primitive p-te Einheitswurzel.

Setzt man in der Formel (3.9) entsprechend $m = 1$, so erhält man für $p \nmid (1+n)$

$$\frac{[\beta, r][\beta^n, r]}{[\beta^{1+n}, r]} = \sum_{\mu=1}^{q-2} \beta^{\operatorname{ind}(\mu) - (1+n)\operatorname{ind}(1+\mu)}. \qquad (3.10)$$

Die Funktionen aus (3.10)

$$\Psi_n(\beta) := \sum_{\mu=1}^{q-2} \beta^{\operatorname{ind}(\mu) - (1+n)\operatorname{ind}(1+\mu)} \qquad (n = 1, 2, \ldots, p-2) \qquad (3.11)$$

heißen *Jacobi-(Kreisteilungs-)Funktionen* (siehe (Ribenboim, 1979, Lecture VII)).

Falls gilt $(q-1) \nmid h$, so bildet man in der Kreisteilungstheorie das Produkt der Lagrange-Summen $\langle \omega^h, r \rangle \langle \omega^{-h}, r \rangle$. Nach einigen Zwischenschritten erhält man dann folgende Formel (siehe (Bachmann, 1968a, Seite 87, Formel (29))):

$$\left\langle \omega^h, r \right\rangle \left\langle \omega^{-h}, r \right\rangle = (-1)^h q, \qquad (h = 1, \ldots, p-1). \tag{$**$}$$

Ähnlich wie oben wollen wir jedoch zum Produkt der Jacobi-Summen im Fall $p \nmid m$ übergehen. Wegen der Gleichheit $h = mf$ und $\omega^f = \beta$ können wir $[\beta^m, r]$ statt $\langle \omega^h, r \rangle$ und $[\beta^{-m}, r]$ statt $\langle \omega^{-h}, r \rangle$ schreiben (vgl. Abschnitt 3.4.3 sowie Abschnitt 1.7, Formel (1.27)). Da zudem f in $h = mf$ gerade und daher auch h gerade ist, gilt $(-1)^h = 1$. Also erhalten wir aus der Formel $(**)$

$$[\beta^m, r][\beta^{-m}, r] = q \qquad (m = 1, \ldots, p-1). \tag{3.12}$$

Mit Hilfe der Gleichung (3.12) können wir nun das Produkt $\Psi_n(\beta) \cdot \Psi_n(\beta^{-1})$ berechnen und erhalten

$$\begin{aligned} \Psi_n(\beta) \cdot \Psi_n(\beta^{-1}) &= \frac{[\beta, r][\beta^n, r]}{[\beta^{1+n}, r]} \cdot \frac{[\beta^{-1}, r][\beta^{-n}, r]}{[\beta^{-(1+n)}, r]} = \frac{q \cdot q}{q} \\ &= q \qquad (n = 1, 2, \ldots p-2). \end{aligned} \tag{3.13}$$

3.4.5 Andere Darstellung der Jacobi-Funktion $\Psi_n(\beta)$

Im folgenden Schritt wollen wir genauer die Terme der Jacobi-Funktion (3.11)

$$\Psi_n(\beta) = \sum_{\mu=1}^{q-2} \beta^{\operatorname{ind}(\mu) - (1+n)\operatorname{ind}(1+\mu)}$$

für ein n betrachten und werden dann $\Psi_n(\beta)$ in einer anderen Weise darstellen.

Jeder Summand in $\Psi_n(\beta)$ hat die Gestalt

$$\beta^{\operatorname{ind}(\mu) - (1+n)\operatorname{ind}(1+\mu)} \qquad (\mu = 1, 2, \ldots, q-2),$$

wobei β eine primitive p-te Einheitswurzel bezeichnet. Nun können die Exponenten aller Terme durch ihre Reste mod p ersetzt werden. Dann fassen wir die gleichen Potenzen von β zusammen, indem wir abzählen, wie oft unter diesen Resten mod p die Zahlen $0, 1, \ldots, p-1$ vorkommen, und bezeichnen diese Anzahlen mit $A_{n,0}, A_{n,1}, \ldots, A_{n,p-1}$. So kann die Jacobi-Funktion $\Psi_n(\beta)$ auf folgen-

de Weise aufgefasst werden:

$$\Psi_n(\beta) = \sum_{k=0}^{p-1} A_{n,k}\beta^k = A_{n,0} + \sum_{k=1}^{p-1} A_{n,k}\beta^k. \tag{3.14}$$

3.4.6 Die Anzahlen $A_{n,k}$

Wir bemerken, dass nach der obigen Bezeichnung $A_{n,0}$ die Anzahl derjenigen Terme in $\Psi_n(\beta)$ bedeutet, deren Exponent ein Vielfaches von p ist.

Es gilt offensichtlich

$$\Psi_n(1) = A_{n,0} + \sum_{k=1}^{p-1} A_{n,k} = q - 2, \tag{3.15}$$

da $\Psi_n(\beta)$ nach (3.10) insgesamt $(q-2)$ Summanden enthält. Aus (3.15) folgt unmittelbar die Gleichung

$$\sum_{k=1}^{p-1} A_{n,k} = q - 2 - A_{n,0}. \tag{3.15'}$$

Ferner folgt aus der Kreisteilungsgleichung $\sum_{k=0}^{p-1}\beta^k = 0$, dass $\sum_{k=1}^{p-1}\beta^k = -1$ für eine primitive p-te Einheitswurzel β ist. Demnach erhalten wir weiter

$$\begin{aligned} A_{n,0} &= (-A_{n,0})\,(-1) = -A_{n,0}\sum_{k=1}^{p-1}\beta^k \\ &= -\sum_{k=1}^{p-1} A_{n,0}\beta^k. \end{aligned} \tag{3.16}$$

Das Einsetzen des letzten Ausdrucks (3.16) für $A_{n,0}$ in die Gleichung (3.14) liefert

$$\begin{aligned} \Psi_n(\beta) &= -\sum_{k=1}^{p-1} A_{n,0}\beta^k + \sum_{k=1}^{p-1} A_{n,k}\beta^k \\ &= \sum_{k=1}^{p-1} \underbrace{(A_{n,k} - A_{n,0})}_{=:\,c_{n,k}}\beta^k \\ &= \sum_{k=1}^{p-1} c_{n,k}\beta^k, \end{aligned} \tag{3.17}$$

wobei gilt

$$\sum_{k=1}^{p-1} c_{n,k} = \sum_{k=1}^{p-1} (A_{n,k} - A_{n,0}) = \overbrace{\sum_{k=1}^{p-1} A_{n,k}}^{=q-2-A_{n,0}} - \overbrace{\sum_{k=1}^{p-1} A_{n,0}}^{=(p-1)A_{n,0}}$$
$$= q - 2 - pA_{n,0}. \tag{3.18}$$

3.4.7 Zur Ungleichung $(p-1)\sqrt{q} > q - 2 - pA_{n,0}$

In diesem Abschnitt werden wir ein wichtiges Zwischenresultat erhalten, nämlich die Ungleichung $(p-1)\sqrt{q} > q - 2 - pA_{n,0}$ $(n = 1, \ldots, p-2)$. *Weiter unten in Abschnitt 3.4.8 werden wir zudem zeigen, dass* $A_{n,0} = pN(0,0) + f(p-3) + 2$ *ist. Zu diesen Ergebnissen werden wir in Abschnitt 3.4.9 zurückkehren.*

Für die Jacobi-Funktion wurde in Abschnitt 3.4.4 in (3.13) gezeigt, dass

$$q = \Psi_n(\beta) \cdot \Psi_n(\beta^{-1})$$

ist. Unter Anwendung der anderen Darstellung von $\Psi_n(\beta)$ aus (3.17) erhält man dann weiter

$$\begin{aligned} q &= \left(\sum_{k=1}^{p-1} c_{n,k}\beta^k\right)\left(\sum_{\ell=1}^{p-1} c_{n,\ell}\beta^{-\ell}\right) \\ &= \sum_{k=1}^{p-1} c_{n,k}^2 + \sum_{\substack{k,\ell=1 \\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}\left(\beta^{k-\ell} + \beta^{-(k-\ell)}\right) \\ &= \sum_{k=1}^{p-1} c_{n,k}^2 + \sum_{s=1}^{\frac{1}{2}(p-1)} C_{n,s}\left(\beta^s + \beta^{-s}\right), \end{aligned} \tag{3.19}$$

wobei gilt

$$\sum_{s=1}^{\frac{1}{2}(p-1)} C_{n,s} = \sum_{\substack{k,\ell=1 \\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}. \tag{3.20}$$

Man beachte dabei, dass die Bezeichnung $\sum_{\substack{k,\ell=1 \\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}$ eine Doppelsumme bedeutet.

Aufgrund der Irreduzibilität der Kreisteilungsgleichung der primitiven p-ten Einheitswurzeln β muss $C_{n,s}$ zudem konstant sein. Da außerdem offensichtlich

$\sum_{s=1}^{\frac{1}{2}(p-1)}(\beta^s + \beta^{-s}) = -1$ gilt, ist also

$$C_{n,s} = \sum_{k=1}^{p-1} c_{n,k}^2 - q \qquad \left(s = 1, \ldots, \frac{1}{2}(p-1)\right). \tag{3.21}$$

Aus der Gleichung (3.21) ergibt sich unmittelbar

$$q = \sum_{k=1}^{p-1} c_{n,k}^2 - C_{n,s}. \tag{3.21'}$$

Da nun $C_{n,s}$ unabhängig vom Index s ist, folgt weiter aus (3.20), dass

$$\frac{1}{2}(p-1)C_{n,s} = \sum_{\substack{k,\ell=1 \\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}$$

und schließlich

$$C_{n,s} = \frac{2\sum_{\substack{k,\ell=1 \\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}}{p-1}. \tag{3.22}$$

Setzt man diesen Ausdruck für $C_{n,s}$ in die Gleichung (3.21') ein, so erhält man weiter

$$q = \sum_{k=1}^{p-1} c_{n,k}^2 - \frac{2\sum_{\substack{k,\ell=1 \\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}}{p-1}. \tag{3.23}$$

Unter Benutzung der Gleichung $\left(\sum_{k=1}^{p-1} c_{n,k}\right)^2 = \sum_{k=1}^{p-1} c_{n,k}^2 + 2\sum_{k\neq\ell} c_{n,k}c_{n,\ell}$ ergibt sich aus (3.23)

$$\begin{aligned}
(p-1)q &= (p-1)\left(\sum_{k=1}^{p-1} c_{n,k}^2 - \frac{2\sum_{\substack{k,\ell=1 \\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}}{p-1}\right) \\
&= p\sum_{k=1}^{p-1} c_{n,k}^2 - \underbrace{\left(\sum_{k=1}^{p-1} c_{n,k}^2 + 2\sum_{\substack{k,\ell=1 \\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}\right)}_{=\left(\sum_{k=1}^{p-1} c_{n,k}\right)^2} \\
&= p\sum_{k=1}^{p-1} c_{n,k}^2 - \left(\sum_{k=1}^{p-1} c_{n,k}\right)^2.
\end{aligned}$$

Multipliziert man beide Seiten der letzen Gleichung mit $(p-1)$, so erhält man

$$\begin{aligned}(p-1)^2 q &= (p-1)\left(p\sum_{k=1}^{p-1} c_{n,k}^2 - \left(\sum_{k=1}^{p-1} c_{n,k}\right)^2\right)\\ &= p(p-1)\sum_{k=1}^{p-1} c_{n,k}^2 - (p-1)\left(\sum_{k=1}^{p-1} c_{n,k}\right)^2\\ &= p(p-1)\sum_{k=1}^{p-1} c_{n,k}^2 - p\left(\sum_{k=1}^{p-1} c_{n,k}\right)^2 + \left(\sum_{k=1}^{p-1} c_{n,k}\right)^2,\end{aligned}$$

woraus schließlich folgt:

$$\begin{aligned}&(p-1)^2 q - \left(\sum_{k=1}^{p-1} c_{n,k}\right)^2\\ &= p(p-1)\sum_{k=1}^{p-1} c_{n,k}^2 - p\left(\sum_{k=1}^{p-1} c_{n,k}\right)^2\\ &= p^2\sum_{k=1}^{p-1} c_{n,k}^2 - p\sum_{k=1}^{p-1} c_{n,k}^2 - p\sum_{k=1}^{p-1} c_{n,k}^2 - 2p\sum_{\substack{k,\ell=1\\ k<\ell}}^{p-1} c_{n,k}c_{n,l}\\ &= \underbrace{p\left((p-2)\sum_{k=1}^{p-1} c_{n,k}^2 - 2\sum_{\substack{k,\ell=1\\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}\right)}_{=:M_n}\\ &= pM_n. \qquad (3.24)\end{aligned}$$

Die Größe M_n

Wir betrachten die Größe

$$M_n = (p-2)\sum_{k=1}^{p-1} c_{n,k}^2 - 2\sum_{\substack{k,\ell=1\\ k<\ell}}^{p-1} c_{n,k}c_{n,\ell}$$

und zeigen, dass $M_n > 0$ ist.

Es ist zunächst leicht zu sehen, dass M_n auch in der Form

$$M_n = \sum_{\substack{k,\ell=1\\ k<\ell}}^{p-1} (c_{n,k} - c_{n,\ell})^2 \qquad (3.25)$$

dargestellt werden kann.

Dazu führen wir folgende Rechnung:

$$
\begin{aligned}
&\sum_{\substack{k,\ell=1\\k<\ell}}^{p-1} (c_{n,k} - c_{n,\ell})^2 \\
&= (c_{n,1} - c_{n,2})^2 + (c_{n,1} - c_{n,3})^2 + (c_{n,1} - c_{n,4})^2 + \ldots + (c_{n,1} - c_{n,p-1})^2 \\
&\quad + (c_{n,2} - c_{n,3})^2 + (c_{n,2} - c_{n,4})^2 + \ldots + (c_{n,2} - c_{n,p-1})^2 \\
&\quad + \ldots + (c_{n,p-2} - c_{n,p-1})^2 \\
&= c_{n,1}^2 - 2c_{n,1}c_{n,2} + c_{n,2}^2 + \ldots + c_{n,1}^2 - 2c_{n,1}c_{n,p-1} + c_{n,p-1}^2 \\
&\quad + c_{n,2}^2 - 2c_{n,2}c_{n,3} + c_{n,3}^2 + \ldots + c_{n,2}^2 - 2c_{n,2}c_{n,p-1} + c_{n,p-1}^2 \\
&\quad + \ldots + c_{n,p-2}^2 - 2c_{n,p-2}c_{n,p-1} + c_{n,p-1}^2 \\
&= (p-2)\sum_{k=1}^{p-1} c_{n,k}^2 - 2\sum_{\substack{k,\ell=1\\k<\ell}}^{p-1} c_{n,k}c_{n,\ell} \\
&= M_n.
\end{aligned}
$$

Als Summe der Quadrate (siehe (3.25)) ist $M_n \geq 0$. Ferner gilt sogar strikt $M_n > 0$. Um zu zeigen, dass $M_n \neq 0$ gilt, nehmen wir an, dass $M_n = 0$ ist. Dann kann in der Gleichung (3.24) entsprechend $pM_n = 0$ gesetzt werden. Auf diese Weise erhält man

$$(p-1)^2 q - \left(\sum_{k=1}^{p-1} c_{n,k}\right)^2 = 0. \tag{3.26}$$

Ist $M_n = 0$, so müssen der Formel (3.25) zufolge alle Größen $c_{n,k}$ und $c_{n,\ell}$ für $k, \ell = 1, \ldots, p-1$ gleich sein. O.B.d.A. bezeichnen wir diese Größe mit $c_{n,1}$. Da

$$\sum_{k=1}^{p-1} c_{n,1} = (p-1)c_{n,1},$$

folgt dann aus der Gleichung (3.26)

$$(p-1)^2 q = (p-1)^2 c_{n,1}^2.$$

Die Zahl q ist demnach nicht prim. Dies ist jedoch ein Widerspruch.

Da nun $M_n > 0$ und folglich auch $pM_n > 0$ für $p \geq 3$ gilt, erhalten wir aus

der Gleichung (3.24) folgende Ungleichung:

$$(p-1)^2 q - \left(\sum_{k=1}^{p-1} c_{n,k} \right)^2 > 0,$$

woraus sich

$$(p-1)\sqrt{q} > \sum_{k=1}^{p-1} c_{n,k} \tag{3.27}$$

durch Quadratwurzelziehen ergibt.

In Abschnitt 3.4.6 in (3.18) haben wir bereits gezeigt, dass

$$\sum_{k=1}^{p-1} c_{n,k} = q - 2 - pA_{n,0}$$

ist. Somit folgt aus der Ungleichung (3.27)

$$(p-1)\sqrt{q} > q - 2 - pA_{n,0}, \tag{3.28}$$

dabei ist $n = 1, \ldots p-2$.

3.4.8 Die Anzahl $A_{n,0}$

Wir erinnern uns, dass $A_{n,0}$ per Definition die Anzahl derjenigen Summanden in $\Psi_n(\beta)$ bedeutet, deren Exponent ein Vielfaches von p ist, für welche also gilt

$$\operatorname{ind}(\mu) - (1+n)\operatorname{ind}(1+\mu) \equiv 0 \pmod{p} \qquad (\mu = 1, \ldots, q-2).$$

Die letzte Kongruenz ist offenbar gleichbedeutend mit

$$\operatorname{ind}(\mu) \equiv (1+n)\operatorname{ind}(1+\mu) \pmod{p} \qquad (\mu = 1, \ldots, q-2). \tag{3.29}$$

Seien weiter

$$\mu \equiv g^{d+kp} \pmod{p}, \qquad 1+\mu \equiv g^{\ell+hp} \pmod{p}, \tag{3.30}$$

$$1+n \equiv \frac{1}{\varrho} \pmod{p}, \tag{3.31}$$

wobei $0 \le d, \ell < p$ und $0 \le k, h \le f-1$ ist.

Mit diesen Bezeichnungen gilt aufgrund der Kongruenz (3.29) auch die Kongruenz

$$d + kp \equiv \frac{1}{\varrho} \cdot (\ell + hp) \pmod{p}. \tag{3.32}$$

Und da $kp \equiv 0$ und $hp \equiv 0 \pmod{p}$ gilt, so ist

$$d\varrho \equiv \ell \pmod{p}. \tag{3.33}$$

Unter Benutzung der Bezeichnungen (3.30) können wir ferner schreiben:

$$1 + g^{d+kp} \equiv g^{\ell+hp} \pmod{q} \tag{3.34}$$

Wegen der Kongruenz (3.33) ist die letztere gleichbedeutend mit

$$1 + g^{d+kp} \equiv g^{d\varrho+hp} \pmod{q}. \tag{3.35}$$

Ein Zwischenergebnis hieraus ist, dass es genau so viele Exponenten gibt, welche ein Vielfaches von p sind, wie es Paare von d, $d\varrho$ gibt, sodass die Kongruenz (3.35) gilt.

Unter Berücksichtigung der Definition der Anzahlfunktion $N(.,.)$ können wir die Anzahl $A_{n,0}$ der Summanden in $\Psi_n(\beta)$, deren Exponent ein Vielfaches von p ist, auf folgende Weise auffassen:

$$A_{n,0} = \sum_{d=0}^{p-1} N(d, d\varrho) \qquad (0 \leq d < p). \tag{3.36}$$

Man beachte dabei, dass Resultat (3.36) für alle Werte

$$n = 1, 2, \ldots, p-2$$

gilt. (Zur Erinnerung: Die Formel (3.11) für die Jacobi-Funktionen $\Psi_n(\beta)$ ist für $n = 1, 2, \ldots, p-2$ definiert.) Da aufgrund der Bezeichnung (3.31) $1 + n \equiv \frac{1}{\varrho} \pmod{p}$ und folglich $\varrho \equiv (1+n)^{-1} \pmod{p}$ gilt, nimmt $\varrho \pmod{p}$ bis auf die Reihenfolge folgende Werte an:

$$\varrho = 2, 3, \ldots, p-1.$$

Das Aufsummieren von $A_{n,0}$ über alle Werte von n liefert dann

$$\begin{aligned}
\sum_{n=1}^{p-2} A_{n,0} &= \sum_{n=1}^{p-2} \sum_{d=0}^{p-1} N(d, d\varrho) \\
&= \sum_{d=0}^{p-1} \sum_{\varrho=2}^{p-1} N(d, d\varrho) \\
&= \sum_{\varrho=2}^{p-1} N(0,0) + \sum_{d=1}^{p-1} \sum_{\varrho=2}^{p-1} N(d, d\varrho) \\
&= (p-2)N(0,0) + \sum_{d=1}^{p-1} \sum_{\varrho=2}^{p-1} N(d, d\varrho) \\
&= (p-2)N(0,0) + \sum_{d=1}^{p-1} \underbrace{\sum_{\substack{j=1 \\ j\neq d}}^{p-1} N(d,j)}_{=: L_d} \\
&= (p-2)N(0,0) + \sum_{d=1}^{p-1} L_d. \qquad (3.37)
\end{aligned}$$

Der Übergang von $\sum_{\varrho=2}^{p-1} N(d, d\varrho)$ zu $\sum_{\substack{j=1 \\ j\neq d}}^{p-1} N(d,j)$ in der vorletzten Zeile erfolgte aufgrund folgender Überlegungen: Ist $d \not\equiv 0 \pmod p$, so gilt für kein $\varrho \in \{2, 3, \ldots, p-1\}$ die Kongruenz $d\varrho \equiv d \pmod p$, da sonst $p \mid d$ oder $p \mid (\varrho - 1)$ gelten muss, was nicht sein kann. Für ein $d \not\equiv 0 \pmod p$ sind also die Werte $d\varrho$, genauer $2d, 3d, \ldots, (p-1)d$ bis auf die Reihenfolge den Zahlen $1, 2, \ldots, d-1, d+1, \ldots, p-1 \pmod p$ kongruent.

Die Größe L_d

In der Kreisteilungstheorie werden folgende Eigenschaften der Anzahlfunktion für den Fall, dass p prim und f gerade ist, gezeigt (siehe hierzu (Bachmann, 1968a, 15. Vorlesung)):

$$\sum_{j=0}^{p-1} N(0,j) = f - 1 \qquad (d = 1, \ldots, p-1), \qquad (3.38)$$

$$\sum_{j=0}^{p-1} N(d,j) = f \qquad (d = 1, \ldots, p-1), \qquad (3.39)$$

$$N(d,\delta) = N(\delta,d) \qquad (d, \delta = 1, \ldots, p-1), \qquad (3.40)$$

$$N(d,\delta) = N(\delta - d, p - d) \qquad (d, \delta = 1, \ldots, p-1), \qquad (3.41)$$

Die Eigenschaft (3.41) impliziert weiter:

$$N(d,d) = N(0,p-d) \qquad (d = 1, \ldots, p-1). \tag{3.42}$$

Mithilfe dieser Eigenschaften wollen wir nun die in (3.37) neu definierte Größe

$$L_d = \sum_{\substack{j=1 \\ j\neq d}}^{p-1} N(d,j)$$

genauer bestimmen. Mit der Indexverschiebung von $j = 1$ zu $j = 0$ ergibt sich

$$L_d = \left(\sum_{j=0}^{p-1} N(d,j) \right) - N(d,0) - N(d,d).$$

Das Aufsummieren von L_d über alle Werte $d = 1, \ldots, p-1$ liefert:

$$\begin{aligned}
\sum_{d=1}^{p-1} L_d &= \sum_{d=1}^{p-1} \left(\underbrace{\sum_{j=0}^{p-1} N(d,j)}_{\underset{(3.39)}{=} f} - N(d,0) - \underbrace{N(d,d)}_{\underset{(3.42)}{=} N(0,p-d)} \right) \\
&= \sum_{d=1}^{p-1} \left(f - N(d,0) - N(0,p-d) \right) \\
&= \sum_{d=1}^{p-1} f - \underbrace{\sum_{d=1}^{p-1} N(d,0)}_{=\sum_{j=1}^{p-1} N(0,j)} - \underbrace{\sum_{d=1}^{p-1} N(0,p-d)}_{=\sum_{j=1}^{p-1} N(0,j)} \\
&= f(p-1) - 2 \sum_{j=1}^{p-1} N(0,j) = f(p-1) - 2 \left(\sum_{j=0}^{p-1} N(0,j) - N(0,0) \right) \\
&= f(p-1) - 2 \underbrace{\sum_{j=0}^{p-1} N(0,j)}_{\underset{(3.38)}{=} f-1} + 2N(0,0) = f(p-1) - 2(f-1) + 2N(0,0) \\
&= f(p-1) - 2f + 2 + 2N(0,0) \\
&= f(p-3) + 2 + 2N(0,0).
\end{aligned}$$

Durch das Einsetzen dieses Resultates für $\sum_{d=1}^{p-1} L_d$ in (3.37)

$$\sum_{n=1}^{p-2} A_{n,0} = (p-2)N(0,0) + \sum_{d=1}^{p-1} L_d$$

erhalten wir

$$\begin{aligned}\sum_{n=1}^{p-2} A_{n,0} &= (p-2)N(0,0) + f(p-3) + 2 + 2N(0,0) \\ &= pN(0,0) + f(p-3) + 2. \end{aligned} \tag{3.43}$$

3.4.9 Zur Ungleichung $p^2N(0,0) > q + 1 - 3p - (p-1)(p-2)\sqrt{q}$

In diesem Abschnitt erhalten wir schließlich das entscheidende Resultat: Es gilt die Ungleichung

$$p^2N(0,0) > q + 1 - 3p - (p-1)(p-2)\sqrt{q}.$$

Daraus werden wir dann in Abschnitt 3.4.10 die gesuchte obere Schranke $S(p)$ für q folgern, für welche $N(0,0) > 0$ gilt.

Das Zwischenergebnis in Abschnitt 3.4.7 war die Ungleichung (3.28)

$$(p-1)\sqrt{q} > q - 2 - pA_{n,0} \qquad (n = 1, \ldots p-2).$$

Das Aufsummieren über n liefert

$$\sum_{n=1}^{p-2} (p-1)\sqrt{q} > \sum_{n=1}^{p-2} ((q-2) - pA_{n,0})$$

und schließlich auch

$$(p-2)(p-1)\sqrt{q} > (p-2)(q-2) - p\sum_{n=1}^{p-2} A_{n,0}. \tag{3.44}$$

Setzt man in (3.44) den Ausdruck für $\sum_{n=1}^{p-2} A_{n,0}$ aus (3.43) ein, so folgt

$$(p-1)(p-2)\sqrt{q} > (p-2)(q-2) - p\left(pN(0,0) + (p-3)f + 2\right),$$

also

$$(p-1)(p-2)\sqrt{q} > (p-2)(q-2) - p^2N(0,0) - pf(p-3) - 2p.$$

Wegen der Gleichheit $pf = q-1$ erhalten wir weiter

$$(p-1)(p-2)\sqrt{q} > \underbrace{(p-2)(q-2)}_{=pq-2q-2p+4} - p^2N(0,0) - \underbrace{(q-1)(p-3)}_{=pq-p-3q+3} - 2p,$$

woraus schließlich die Ungleichung

$$p^2N(0,0) > q+1-3p-(p-1)(p-2)\sqrt{q} \tag{3.45}$$

folgt.

3.4.10 Hinreichende Bedingung und Schranke

Nach der Fragestellung des Satzes wollen wir bestimmen, unter welcher Bedingung es nicht-triviale Lösungen der Kongruenz (3.1)

$$x^p + y^p + z^p \equiv 0 \pmod{q}$$

gibt, was gleichbedeutend mit der Frage nach Lösungen der Kongruenz (3.3)

$$1 + g^{pt} \equiv g^{p\tau} \pmod{q}$$

ist. Unter Benutzung der Anzahlfunktion lautet die Fragestellung: Oberhalb welcher Schranke $S(p)$ liegt q, sodass $N(0,0) > 0$ gilt?

Eine hinreichende Bedingung für $N(0,0) > 0$ kann aus der Abschätzung (3.45) hergeleitet werden, denn man sieht leicht, dass aus der Ungleichung

$$q+1-3p \geq (p-1)(p-2)\sqrt{q}$$

folgt: $N(0,0) > 0$.

Nun werden wir diese Ungleichung so umformen, dass wir schließlich eine untere Schranke von q bekommen, welche nur von p abhängt.

Die rechte Seite der Ungleichung ist positiv. Aufgrund der Ungleichungsbeziehung ist folglich auch die linke Seite positiv, also dürfen beide Seiten quadriert

werden. Es folgt dann

$$(q+1-3p)^2 \geq (p-1)^2(p-2)^2 q.$$

Weiter ergibt sich:

$$\begin{aligned} 0 &\leq q^2 + \underbrace{2q-6pq}_{=q(2-6p)} + \underbrace{9p^2-6p+1}_{=(3p-1)^2} - (p-1)^2(p-2)^2 q \\ &= q^2 - q\underbrace{\left((p-1)^2(p-2)^2+6p-2\right)}_{=:S} + (3p-1)^2 \\ &= q^2 - qS + (3p-1)^2. \end{aligned} \tag{3.46}$$

Die Bedingung (3.46) ist erfüllt, falls gilt

$$q \geq S, \qquad \text{wobei} \qquad S = (p-1)^2(p-2)^2 + 6p - 2.$$

Die Ungleichung $q \geq S$ ist offenbar gleichbedeutend mit $pf+1 > S-1$ (wegen $q = pf+1$) und schließlich auch mit

$$pf > S-2.$$

Setzt man in die letzte Ungleichung den Ausdruck für S ein und kürzt man beide Seiten durch p, so erhält man

$$\begin{aligned} f &> \frac{1}{p}\left((p-1)^2(p-2)^2+6p-2-2\right) \\ &= \frac{1}{p}\left(p^4-2p^3+p^2-4p^3+8p^2-4p+4p^2-8p+4+6p-4\right) \\ &= \frac{1}{p}\left(p^4-6p^3+13p^2-6p\right) \\ &= p^3-6p^2+13p-6. \end{aligned} \tag{3.47}$$

3.4.11 Ergebnisse

Wir haben Folgendes bewiesen:

(i) Seien p, $q = pf+1$ zwei ungerade Primzahlen und f mit $\mathrm{ggT}(f,3) = 1$. Für alle

$$q \geq (p-1)^2(p-2)^2 + 6p - 2 = S(p)$$

besitzt die Kongruenz

$$x^p + y^p + z^p \equiv 0 \pmod{q}$$

nicht-triviale Lösungen.

(ii) Sind p, $q = pf + 1$ zwei ungerade Primzahlen und ist f mit $\mathrm{ggT}(f, 3) = 1$ derart, dass

$$f > p^3 - 6p^2 + 13p - 6,$$

so besitzt die Kongruenz

$$x^p + y^p + z^p \equiv 0 \pmod{q}$$

nicht-triviale Lösungen.

Der Satz von Dickson ist somit vollständig bewiesen. □

Kapitel 4

Experimentelle Ergebnisse

Nachdem wir in den vorherigen Kapiteln den Begriff der Sophie-Germain-Begleitprimzahl eingeführt und eine obere Schranke für die Sophie-Germain-Begleitprimzahlen hergeleitet haben, möchten wir einige experimentelle Ergebnisse vorstellen und erläutern. Darüberhinaus werden wir das numerische Verfahren zur Bestimmung der Sophie-Germain-Begleitprimzahlen und dessen Implementierung in Maple 9.5 diskutieren.

4.1 Einige Beispiele

Die folgende Tabelle 1 enthält zu allen ungeraden Primzahlen $p < 200$ eine, nämlich die kleinste, Sophie-Germain-Begleitprimzahl $q = 2mp + 1$ und den entsprechenden Multiplikator m, dabei wurden die Sophie-Germain-Primzahlen hervorgehoben dargestellt. Aus dieser Tabelle wird unter anderem ersichtlich, warum die Untersuchungen von Legendre zunächst nur die Primzahlen bis 197 berücksichtigten: Die Zahl 197 ist die erste, zu der es keine Sophie-Germain-Begleitprimzahl mit einem der von Legendre untersuchten Multiplikatoren

$$1, \quad 2, \quad 4, \quad 5, \quad 7, \quad 8 \tag{4.1}$$

gibt (vgl. Lemmata 2.3.6 und 2.3.5).

Sophie-Germain-Begleitprimzahlen zu p**,** $3 \leq p < 200$								
p	m	$q = 2mp + 1$	p	m	$q = 2mp + 1$	p	m	$q = 2mp + 1$
3	1	7	**5**	1	11	7	2	29
11	1	23	13	2	53	17	4	137
19	5	191	**23**	1	47	**29**	1	59
31	5	311	37	2	149	**41**	1	83
43	2	173	47	7	659	**53**	1	107
59	7	827	61	8	977	67	2	269
71	4	569	73	2	293	79	2	317
83	1	167	**89**	1	179	97	2	389
101	4	809	103	5	1031	107	4	857
109	5	1091	**113**	1	227	127	2	509
131	1	263	137	4	1097	139	2	557
149	4	1193	151	5	1511	157	5	1571
163	2	653	167	7	2339	**173**	1	347
179	1	359	181	5	1811	**191**	1	383
193	2	773	197	19	7487	199	2	797

Tabelle 1

Die Untersuchung weiterer Primzahlen erforderte also die Erweiterung der Liste möglicher Multiplikatoren. So gelang es Dickson (mindestens) eine Sophie-Germain-Begleitprimzahl zu jeder Primzahl $p < 1700$ zu finden mit Ausnahme von elf bestimmten (siehe Folge (2.7) sowie folgenden Abschnitt zu Dicksons elf Ausnahmefällen). Dabei enthält die Liste der vorkommenden Multiplikatoren neben den von Legendre erwähnten (siehe (4.1)) noch acht weitere (vgl. Lemma 2.3.7):

$$\begin{aligned} &1, \quad 2, \quad 4, \quad 5, \quad 7, \quad 8, \\ 10, \quad 11, \quad 13, \quad 14, \quad &16, \quad 20, \quad 28, \quad 32. \end{aligned} \tag{4.2}$$

Dicksons elf Ausnahmefälle

Da es zu $p = 197, 223, 257, 383, 389, 457, 569, 751, 1373, 1399, 1531$ keine Sophie-Germain-Begleitprimzahlen mit einem der Multiplikatoren aus der Menge (4.2) gibt, bewies Dickson für diese Primzahlexponenten den I. Fall des großen

Satzes von Fermat zum Teil mit anderen Methoden, zum Teil mit den Kriterien von Sophie Germain. Auch für diese elf Primzahlen lässt sich (mindestens) eine Sophie-Germain-Begleitprimzahl finden, wenn auch mit anderen Multiplikatoren als in (4.2). Bei den in Tabelle 2 angegebenen Beispielen beschränkten wir uns auf die Multiplikatoren $m \leq 35$.

Sophie-Germain-Begleitprimzahlen zu Dicksons elf Ausnahmen						
p	m_1	$q_1 = 2m_1p + 1$	m_2	$q_2 = 2m_2p + 1$	m_3	$q_3 = 2m_3p + 1$
197	19	7487	22	8669	25	9851
223	17	7583	23	10259	26	11597
257	19	9767	34	17477		
383	31	23747				
389	19	14783	22	17117		
457	23	21023	35	31991		
569	22	25037	31	35279	34	38693
751	35	52571				
1373	22	60413				
1399	35	97931				
1531	26	79613	29	88799	35	107171

Tabelle 2

Auch zu den weiteren Primzahlen p, $1700 < p < 2007$ gibt es (mindestens) eine Sophie-Germain-Begleitprimzahl. Dabei gibt es zu allen davon mit Ausnahme von 1787, 1933, 1949, 1993 eine Sophie-Germain-Begleitprimzahl mit einem der Multiplikatoren wie in (4.2). Die Sophie-Germain-Begleitprimzahlen zu den letztgenannten vier Primzahlen sind in der folgenden Tabelle 3 angegeben.

Sophie-Germain-Begleitprimzahlen		
p	m	$q = 2mp + 1$
1787	52	185849
1933	23	88919
1949	34	132533
1993	17	67763

Tabelle 3

4.2 Gibt es zu jeder Primzahl eine Sophie-Germain-Begleitprimzahl?

Der Satz von Dirichlet über Primzahlen in arithmetischen Progressionen besagt, dass jede unbegrenzte arithmetische Progression $ax + b$ mit $\mathrm{ggT}(a, b) = 1$ unendlich viele Primzahlen enthält (siehe (Bachmann, 1968b, 2. Kapitel)). In (Wendt, 1895) ist insbesondere der Spezialfall für $b = 1$ (mit arithmetischen Mitteln) bewiesen. Daraus folgt, dass es für eine gegebene ungerade Primzahl p unendlich viele Primzahlen der Gestalt $q = 2mp + 1$ mit $\mathrm{ggT}(m, 3) = 1$ gibt. Es stellt sich die Frage: Ist mindestens eine dieser Primzahlen $q = 2mp + 1$ auch eine Sophie-Germain-Begleitprimzahl zu p?

Unter Benutzung von Maple 9.5 verifizierte ich zuerst $n = 5000$ ungerade Primzahlen und stellte fest, dass zu allen Primzahlen p, $3 \leq p \leq 48619$, mindestens eine Sophie-Germain-Begleitprimzahl existiert. Die Suche beschränkte sich dabei auf die jeweils kleinste Sophie-Germain-Begleitprimzahl q. Der dabei größte vorkommende Multiplikator ist $m = 83$.

n	p	m	$q = 2mp + 1$	n	p	m	$q = 2mp + 1$
1	3	1	7	2	5	1	11
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
4971	48313	83	8019959	4972	48337	8	773393
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
4999	48611	10	972221	5000	48619	29	2819903

Tabelle 4

Für die ersten 5000 ungeraden Primzahlen kommen 48 verschiedene Multiplikatoren vor (aus insgesamt 56 Zahlen $k \leq 83$ mit $\mathrm{ggT}(k, 3) = 1$):

Multiplikatoren für erste 5000 ungeraden Primzahlen											
1	2	4	5	7	8	10	11	13	14	16	17
19	20	22	23	25	26	28	29	31	32	34	35
37	38	40	41	43	44	46	47	49	50	52	53
55	56	59	61	65	68	70	71	73	76	82	83

Tabelle 5

Unten sind einige Ausschnitte aus der Ausgabe-Datei eingefügt. Diese besteht aus einer Liste von Tripeln $[p, m, q]$, wobei q die kleinste Sophie-Germain-Be-

gleitprimzahl zu p mit dem Multiplikator m ist.

'[p,m,q]:', [[3, 1, 7], [5, 1, 11], [7, 2, 29], [11, 1, 23], [13, 2, 53], [17, 4, 137], [19, 5, 191], [23, 1, 47], [29, 1, 59], [31, 5, 311], [3 7, 2, 149], [41, 1, 83], [43, 2, 173], [47, 7, 659], [53, 1, 107], [59, 7, 827], [61, 8, 977], [67, 2, 269], [71, 4, 569], [73, 2, 293], [79, 2, 317], [83, 1, 167], [89, 1, 179], [97, 2, 389], [101, 4, 809], [103, 5, 1031], [107, 4, 857], [109, 5, 1091], [113, 1, 227], [127, 2, 509], [13 1, 1, 263], [137, 4, 1097], [139, 2, 557], [149, 4, 1193], [151, 5, 1511], [157, 5, 1571], [163, 2, 653], [167, 7, 2339], [173, 1, 347], [179, 1 , 359], [181, 5, 1811], [191, 1, 383], [193, 2, 773], [197, 19, 7487], [199, 2, 797], [211, 5, 2111], [223, 17, 7583], [227, 13, 5903], . . . , [23813, 7, 333383], [23819, 1, 47639], [23827, 8, 381233], [23831, 4, 190649], [23833, 5, 238331], [23857, 2, 95429], [23869, 5, 238691], [23873, 10, 477461], [23879, 4, 191033], [23887, 2, 95549], [23893, 17, 8 12363], [23899, 2, 95597], [23909, 1, 47819], [23911, 26, 1243373], [239 17, 5, 239171], [23929, 2, 95717], [23957, 4, 191657], [23971, 5, 239711], [23977, 8, 383633], [23981, 1, 47963], [23993, 10, 479861], [24001, 5 , 240011], [24007, 8, 384113], [24019, 11, 528419], [24023, 10, 480461], [24029, 4, 192233], [24043, 11, 528947], [24049, 5, 240491], [24061, 11 , 529343], [24071, 40, 1925681], [24077, 4, 192617], [24083, 13, 626159] , [24091, 44, 2120009], [24097, 14, 674717], [24103, 11, 530267], . . . ,
[48311, 4, 386489], [48313, 83, 8019959], [48337, 8, 773393], [48341, 13, 1256867], [48353, 7, 676943], [48371, 13, 1257647], [48383, 13, 1257959], [48397, 5, 483971], [48407, 10, 968 141], [48409, 5, 484091], [48413, 1, 96827], [48437, 43, 4165583], [4844 9, 25, 2422451], [48463, 23, 2229299], [48473, 10, 969461], [48479, 1, 9 6959], [48481, 35, 3393671], [48487, 20, 1939481], [48491, 10, 969821], [48497, 4, 387977], [48523, 2, 194093], [48527, 19, 1844027], [48533, 7, 679463], [48539, 4, 388313], [48541, 5, 485411], [48563, 1, 97127], [48571, 8, 777137], [48589, 20, 1943561], [48593, 1, 97187], [48611, 10, 972221], [48619, 29, 2819903]]

Interessant ist, dass (bis auf *eine* Ausnahme) zu jedem untersuchten p die *erste* Primzahl $q = 2mp + 1$ mit $\mathrm{ggT}(m, 3) = 1$ in der Tat eine Sophie-Germain-Begleitprimzahl ist. Ausgenommen ist die 465-te ungerade Primzahl:

Ausnahme				
$n = 465$	$p = 3313$	$\overline{m} = 17$	$\overline{q} = 2\overline{m}p + 1 = 112643$	*keine* SGB
		$m = 38$	$q = 2mp + 1 = 251789$	kleinste SGB

Tabelle 6

Im Fall $\overline{m} = 17$ gilt zwar $3 \nmid \overline{m}$ und $\overline{q} = 2\overline{m}p + 1$ ist eine Primzahl, aber p ist eine p-te Potenz mod $\overline{q}$, das heißt die erste Bedingung der Sophie-Germain-Begleitprimzahl zu p ist verletzt. Die zweite Primzahl der Form $q = 2mp + 1$ mit einem durch 3 nicht teilbaren m, nämlich $m = 38$, ist dann eine Sophie-Germain-Begleitprimzahl zu p.

Weiter ließ sich feststellen, dass auch für die ersten $n = 100000$ ungeraden Primzahlen, also für p, $3 \leq p \leq 1299721$ (mindestens) eine Sophie-Germain-Begleitprimzahl existiert. Auch hier beschränkten wir uns auf die jeweils kleinste Sophie-Germain-Begleitprimzahl. Bis auf die bereits erwähnte einzige Ausnahme (siehe Tabelle 6) ist zu jedem untersuchten p die *erste* Primzahl $q = 2mp + 1$ mit $\text{ggT}(m, 3) = 1$ eine Sophie-Germain-Begleitprimzahl. Für die vorkommenden Multiplikatoren m gilt: $m \leq 158$.

n	p	m	$q = 2mp + 1$
⋮	⋮	⋮	⋮
36724	437077	158	138116333
⋮	⋮	⋮	⋮
100000	1299721	26	67585493

Tabelle 7

Es gibt 106 Zahlen $k \leq 158$, sodass $\text{ggT}(k, 3) = 1$. Bis einschließlich $k = 119$ kommen diese als Multiplikatoren für die ersten 100000 ungeraden Primzahlen vor:

Multiplikatoren für erste 100000 ungeraden Primzahlen												
1	2	4	5	7	8	10	11	13	14	16	17	19
20	22	23	25	26	28	29	31	32	34	35	37	38
40	41	43	44	46	47	49	50	52	53	55	56	58
59	61	62	64	65	67	68	70	71	73	74	76	77
79	80	82	83	85	86	88	89	91	92	94	95	97
98	100	101	103	104	106	107	109	110	112	113	115	116
118	119	122	124	125	127	128	143	145	146	148	155	158

Tabelle 8

Folgende Zahlen k mit $\text{ggT}(k, 3) = 1$ treten *nicht* als Multiplikatoren für die ersten 100000 ungeraden Primzahlen auf: $k = 121$, 130, 131, 133, 134, 136, 137, 139, 140, 142, 149, 151, 152, 154, 157.

Unten ist ein Ausschnitt aus der Ausgabe-Datei eingefügt. Diese enhält Tripel $[p, m, q]$, wobei q die kleinste Sophie-Germain-Begleitprimzahl zu p mit dem Multiplikator m ist.

..., [1299317, 4, 10394537], [1299323, 22, 57170213], [1299341, 49, 127335419], [1299343, 23, 59769779], [1299349, 2, 5197397], [1299359, 19, 49375643], [1299367, 17, 44178479],

[1299377, 34, 88357637], [1299379, 11, 28586339], [1299437, 10, 25988741], [1299439, 5, 12994391], [1299449, 1, 2598899], [1299451, 35, 90961571], [1299457, 17, 44181539], [1299491, 1, 2598983], [1299499, 11, 28588979], [1299533, 10, 25990661], [1299541, 8, 20792657], [1299553, 2, 5198213], [1299583, 35, 90970811], [1299601, 20, 51984041], [1299631, 14, 36389669], [1299637, 23, 59783303], [1299647, 19, 49386587], [1299653, 7, 18195143], [1299673, 2, 5198693], [1299689, 31, 80580719], [1299709, 14, 36391853], [1299721, 26, 67585493].

4.3 Zu Dicksons Schranke

Betrachtet man genauer die Linearformen $fp+1$ und insbesondere die jeweiligen p-Ausnahmen dazu in Lemma 2.3.7 von Dickson, so fällt auf, dass beispielsweise für $p = 3$ zwar größere Primzahlen der Linearform $q = 2mp+1$ mit $m = 5, 7, 10, 11, 13, 16, 32$ existieren, sie erfüllen aber die beiden Kriterien der Sophie-Germain-Begleitprimzahlen zu 3 nicht. Zu $p = 3$ gibt es nur zwei Sophie-Germain-Begleitprimzahlen:

$$7 = 2 \cdot 1 \cdot 3 + 1 \quad \text{und} \quad 13 = 2 \cdot 2 \cdot 3 + 1.$$

In Kapitel 3 haben wir eine obere Schranke für die Sophie-Germain-Begleitprimzahlen zu einem p hergeleitet (siehe Satz 3.1.1 von Dickson und Folgerung 3.1.2 daraus):

$$S(p) = (p-1)^2(p-2)^2 + 6p - 2.$$

Für den Fall $p = 3$ ist leicht zu sehen, dass die Sophie-Germain-Begleitprimzahlen Dicksons Schranke $S(3) = 20$ nicht übersteigen. Aus sechs Primzahlen, die größer 3, kleiner 20 sind ($5, 7, 11, 13, 17, 19$) können nur zwei in der Form $2m \cdot 3 + 1$ mit einem durch 3 nicht teilbaren Multiplikator m dargestellt werden, nämlich 7 und 13. Diese beiden erfüllen die Bedingungen des Satzes von Sophie Germain und sind daher Sophie-Germain-Begleitprimzahlen zu 3.

Aus der oberen Schranke $S(p)$ von Dickson kann man also ein Abbruchkriterium für die Suche nach Sophie-Germain-Begleitprimzahlen zu p ableiten. Für den Fall $p = 3$ bedeutet dies konkret, dass alle $q = 2mp + 1 > 20$ nicht mehr betrachtet werden müssen, da es für diese stets nicht-triviale Lösungen der Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{q}$ gibt und somit die zweite Bedingung des Satzes von Sophie Germain stets verletzt ist.

Allerdings werden wir später sehen, dass nur die Folge der Sophie-Germain-

Begleitprimzahlen zu $p = 3$ Dicksons Schranke nahe kommt. Für größere p wächst der Wert $S(p)$ sehr schnell und je größer p ist, desto stärker ‚überschätzt' $S(p)$ die größte Sophie-Germain-Begleitprimzahl zu p. Für die Praxis bedeutet dies, dass man die Suche nach Sophie-Germain-Begleitprimzahlen zu einem gegebenen p in der Regel schon (viel) früher abbrechen kann. In der nachfolgenden Tabelle 9 sind für einige Primzahlen p unter anderem der Wert $S(p)$ und die größte Sophie-Germain-Begleitprimzahl angegeben.

Für die kleineren Primzahlen p kann man einfach alle in Frage kommenden Primzahlen $2mp + 1$ mit einem durch 3 nicht teilbaren Faktor m, welche unterhalb der Schranke $S(p)$ liegen (deren Anzahl wird weiter mit K bezeichnet), daraufhin überprüfen, ob sie den beiden Bedingungen von Sophie-Germain-Begleitprimzahlen genügen (die Anzahl der Sophie-Germain-Begleitprimzahlen zu einem p wird weiter mit B bezeichnet). So stellt man folgende Ergebnisse fest:

Alle Sophie-Germain-Begleitprimzahlen zu p, $3 \leq p \leq 37$										
p	$S(p)$	K	B	q						
3	20	2	2	7	13					
5	172	5	4	11	41	71	101			
7	940	14	4	29	71	113	491			
11	8164	51	4	23	89	947	1409			
13	17500	86	3	53	131	521				
17	57700	190	5	137	239	443	1667	4013		
19	93748	243	7	191	419	647	761	1217	1901	2129
23	213580	429	12	47	461	599	1289	1427	1979	3083
				3221	3911	4049	4877	6947		
29	571708	850	13	59	233	929	1103	1277	1451	2843
				3539	4409	6323	7193	7541	10847	
31	757084	996	9	311	1427	2357	2543	3659	5147	6263
				15377	33791					
37	1587820	1670	11	149	593	1259	1481	2591	3923	5477
				7253	10139	11027	13469			
41	2433844	2211	13	83	821	1559	2297	2543	2789	3527
				4019	8447	9923	13367	22469	34031	

Tabelle 9

Bereits aus diesen Beispielen wird die mit p wachsende Differenz zwischen der Schranke $S(p)$ und der größten Sophie-Germain-Begleitprimzahl zu p ersichtlich.

Für $p = 31$ liegen alle 9 Sophie-Germain-Begleitprimzahlen unter den ersten 60 aus insgesamt 996 überprüften Primzahlen $2m \cdot 31 + 1$ mit einem durch 3 nicht teilbaren m. Die Zahl $q = 33791$ mit $m = 545$ ist die größte Sophie-Germain-Begleitprimzahl, für die sonstigen m mit $545 < m \leq 12206$ bzw. die sonstigen q mit $33791 < q \leq 756773$ lieferte die Suche keine weiteren Sophie-Germain-Begleitprimzahlen. Dabei ist Dicksons Schranke $S(31) = 757084$, also um Faktor $22,4$ größer als das größte q.

Zu $p = 37$ wurden 11 Sophie-Germain-Begleitprimzahlen bestimmt. Diese liegen unter den ersten 20 aus insgesamt 1670 überprüften Primzahlen der Form $2m \cdot 37 + 1$ mit einem durch 3 nicht teilbaren m. Dicksons Schranke $S(37) = 1587820$ ist etwa um Faktor 118 größer als die größte Sophie-Germain-Begleitprimzahl $q = 13469$ (mit $m = 182$).

Zu $p = 41$ wurden 13 Sophie-Germain-Begleitprimzahlen bestimmt. Alle liegen unter den ersten 47 aus insgesamt 2211 überprüften Primzahlen der Form $2m \cdot 41 + 1$ mit einem durch 3 nicht teilbaren m. Dabei ist $S(41) = 2433844$ etwa um Faktor $71,5$ größer als die größte Sophie-Germain-Begleitprimzahl $q = 34031$ (mit $m = 415$).

4.4 Verfahren zur Bestimmung der Sophie-Germain-Begleitprimzahlen

Einem Verfahren zur Bestimmung der Sophie-Germain-Begleitprimzahlen zu einem gegebenen p werden die Definition und die uns bekannten Eigenschaften von Sophie-Germain-Begleitprimzahlen und Multiplikatoren zugrunde gelegt (siehe Kapitel 2). Zum einen wissen wir, dass für den Multiplikator m kein Vielfaches von 3 gewählt werden darf und dass eine Sophie-Germain-Begleitprimzahl zu p von der Form $q = 2mp + 1$ ist. Weiter müssen die beiden Bedingungen des Satzes von Sophie Germain verifiziert werden: erstens, ob p eine p-te Potenz mod q ist und zweitens, ob es zwei aufeinander folgende Potenzen mod q gibt.

Problem: *Sei eine ungerade Primzahl p gegeben. Gesucht ist die Menge der Sophie-Germain-Begleitprimzahlen zu p.*

Eine naive Möglichkeit besteht darin, zunächst die Menge der zu überprüfenden Faktoren m zu bestimmen (ausgenommen die Vielfachen von 3), die alle Primzahlen der Form $2mp + 1$ unterhalb Dicksons Schranke $S(p)$ ergeben. Ein solches m nennen wir zu Beginn der Suche auch ‚Kandidat' (für den Multiplikator). Ausgehend von $S(p)$ kann zudem eine obere Schranke $m_{max}(p)$ für Multiplikatoren bestimmt werden.

```
S:=n->(n-1)^2*(n-2)^2+6*n-2:  ### Dicksons Schranke
m_max:=floor((S(p)-1)/(2*p)): ### obere Schranke für m
```

Danach wird jeder Kandidat für den Multiplikator darauf getestet, ob die weiteren zwei Bedingungen erfüllt sind. Es wird jedoch schnell klar, dass diese Methode nicht effizient ist:

Für $p = 37$ wird eine Liste aus 1670 Kandidaten bestimmt, dabei ist die obere Schranke für Multiplikatoren $m_{max}(37) = 21457$ und Dicksons Schranke $S(37) = 1587820$.

Für $p = 67$ sind 8898 Kandidaten unterhalb von $m_{max}(67) = 137347$ zu testen, dabei ist $S(67) = 18404500$.

Für $p = 199$ sind insgesamt 191699 Kandidaten zu überprüfen, die unterhalb von $m_{max}(p) = 3822787$ liegen, wobei $S(199) = 1521469228$ ist.

In der Praxis kann aber die Suche bereits deutlich früher abgebrochen werden als es der Wert $S(p)$ bzw. $m_{max}(p)$ angibt, wie dies im letzten Abschnitt bereits erwähnt wurde.

Eine effizientere Methode ist, mit dem Überprüfen der Bedingungen zu beginnen, sobald ein Kandidat für den Multiplikator m gefunden wurde, d.h. m ist nicht durch drei teilbar und die Zahl $2mp + 1$ ist prim. Die Schranke $m_{max}(p)$, deren Erreichnen zum Abbruch der Schleife führt, kann in diesem Fall kleiner gewählt werden.

```
for k from 1 to m_max
do
    bed1_||k:=true:
    bed2_||k:=true:

    ### Schließe die Vielfachen von 3 als Multiplikatoren aus
```

```
    if irem(k,3)<>0 then

            q:= 2*k*p+1:

            ### Falls q prim ist,
            ### überprüfe erste und zweite Bedingung
            if isprime(q) then

                ### Überprüfe erste Bedingung
                test_bed_1(q);

                ### Überprüfe zweite Bedingung
                test_bed_2(q);

            end if; ###isprime()
    end if: ###irem()
od; ###for k
```

4.4.1 Überprüfung der ersten Bedingung

Die erste Bedingung für eine Sophie-Germain-Begleitprimzahl q zu p, ob p eine p-te Potenz mod q ist, kann einfach unter Anwendung des Satzes 1.5.2 überprüft werden. Dem darin formulierten Kriterium zufolge gilt:

$$p \equiv x^p \pmod{q} \text{ ist lösbar} \quad \Longleftrightarrow \quad p^{\frac{q-1}{p}} \equiv 1 \pmod{q}.$$

Der entsprechende Maple-Code dazu:

```
f:=(q-1)/p:
p &^f mod q;
if %=1 then
    bed1_||k:=false; ### erste Bedingung ist verletzt
else
    ### Überprüfe zweite Bedingung
    test_bed_2(q);

end if;
```

4.4.2 Überprüfung der zweiten Bedingung

Eine Möglichkeit zur Überprüfung der zweiten Bedingung ist, für alle ganzen a, $1 \leq a \leq q-1$ die Potenzen $a^p \pmod{q}$ zu berechnen, die Werte zu sortieren und

zu überprüfen, ob es in der sortierten Folge zwei aufeinander folgende Zahlen mit der Differenz 1 gibt.

Seien $p = 31$ und $q = 683 = 2 \cdot 11 \cdot 31 + 1$. Die (bereits sortierten) Potenzen $a^{31} \pmod{683}$ für alle $a = 1, \ldots, 682$ sind:

1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 64, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 128, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 171, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 256, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 341, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 342, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 427, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 512, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 555, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 619, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 651, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 667, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 675, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 679, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 681, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, 682, Anzahl = 682

Zum einen fällt hier auf, dass unter diesen $q-1 = 682$ Werten viele sich (mehrfach) wiederholen. Es treten dabei $(q-1)/p = 2m = 22$ unterschiedliche Werte auf, nämlich

$$1, 2, 4, 8, 16, 32, 64, 128, 171, 256, 341,$$
$$342, 427, 512, 555, 619, 651, 667, 675, 679, 681, 682.$$

Diese Liste ist offenbar gleichbedeutend mit der folgenden:

$$\pm1, \pm2, \pm4, \pm8, \pm16, \pm32, \pm64, \pm128, \pm171, \pm256, \pm341,$$

da $682 \equiv -1 \pmod{683}$, $681 \equiv -2 \pmod{683}$, $679 \equiv -4 \pmod{683}$, ..., $342 \equiv -341 \pmod{683}$ ist.

Da p ungerade ist, gilt allgemein: Ist w eine p-te Potenz mod q, so ist auch $(q-w)$ eine p-te Potenz mod q. Es genügt daher, die Potenzrechnungen $a^p \pmod{q}$ für $a = 1, \ldots, \frac{q-1}{2}$ auszuführen, dabei die symmetrische Darstellung der Restklassen mod q zu wählen und schließlich nur die Absolutbeträge zu betrachten.

Zu beachten ist jedoch ein Spezialfall: Ist $\frac{q-1}{2}$ eine p-te Potenz mod q, so gilt dies auch für $q - \frac{q-1}{2} = \frac{q+1}{2}$. Diese haben die Differenz Eins und die zweite Bedingung ist somit verletzt. Ist dieser Spezialfall eingetroffen, so werden die Berechnungen aller anderen p-ten Potenzen mod q nicht benötigt. Ebenso kann man vorgehen, falls 2 p-te Potenz mod q ist, da es stets gilt, dass 1 p-te Potenz mod q ist.

Dieser Spezialfall tritt in dem obigen Beispiel $p = 31$, $q = 683$ auf, denn 341, 342 beide p-te Potenzen mod q sind. Für $p = 31$, $q = 683$ ist die zweite Bedingung sogar mehrfach verletzt, denn 1, 2 ebenfalls zwei aufeinander folgende p-te Potenzen mod q sind.

Die zweite Methode basiert auf folgenden Überlegungen: Die Untergruppe der p-ten Potenzen mod q in der multiplikativen Gruppe $\mathbb{F}_q^\times$ ist zyklisch von der Ordnung $(q-1)/p = 2m$. Diese wird von $v = u^p$ erzeugt, wobei u eine primitive Wurzel mod q ist. Zu betrachten sind daher die Potenzen $v^h \pmod{q}$ für $h = 0, 1, \ldots, 2m-1$. Nutzt man weiter die symmetrische Darstellung der Repräsentanten, so genügt es, die Rechnungen für $h = 0, 1, \ldots, m-1$ auszuführen.

Aufgrund von solchen Beobachtungen lässt sich die Überprüfung der zweiten Bedingung effizienter implementieren. Folgender Maple-Code überprüft die

zweite Bedingung:

```
### Benutze Maple-Funktion mods
### für symmetrische Darstellung der Restklassen mod q
`mod` := mods:

### Bestimme eine Primitivwurzel mod q
u := numtheory[primroot](q):
w := u &^ p mod q:

### Liste der Potenzen von w (mod q)
pot_liste_||q:=[];

spezfall:=false:

for a from 0 to k-1 do

    wpot:=w &^a mod q; ###  berechne Potenzen von w
    wpos:=abs(wpot): ### Absolutbetrag

    ### Spezialfall-Abfrage
    if wpos=2 or wpos=(q-1)/2 then
        bed2_||k:=false; ### zweite Bedingung ist verletzt
        spezfall:=true:  ### Spezialfall ist eingetroffen
        break;           ### verlasse die for-Schleife

    ### Falls wpos nicht in der Liste,
    ### schreibe wpos in die Liste
    elif member(wpos,pot_liste_||q)=false then
        pot_liste_||q:=[op(pot_liste_||q),wpos];
    end if;
od;

### Wenn Spezialfall nicht eingetroffen ist,
### sortiere die Liste
if spezfall=false then
    L:=sort(pot_liste_||q);

    ### Teste Differenz der jeweils aufeinander folgenden Zahlen
    for j from 1 to nops(L)-1 do
        if L[j+1]-L[j]=1 then
            bed2_||k:=false; ### zweite Bedingung ist verletzt
```

```
            break;
        end if;
    od; ### for j
end if: ## if spezfall
```

4.5 Weitere Aspekte

Nach unseren Beobachtungen sind es nur wenige Kandidaten, die bereits nach dem Überprüfen der ersten Bedingung aussortiert werden. Bis auf diese wenigen muss für alle Kandidaten die zweite Bedingung überprüft werden, wie man dies aus den Beispielen weiter unten sehen kann.

Für $p = 37$ wurden alle 1670 Kandidaten getestet. Es wurden 11 Sophie-Germain-Begleitprimzahlen gefunden. Die auf Position 20 gefundene Primzahl $q = 13469$ mit $m = 182$ ist die größte Sophie-Germain-Begleitprimzahl. Für 51 Kandidaten war bereits die erste Bedingung verletzt. Für die restlichen 1608 davon ist die zweite Bedingung verletzt.

Für $p = 251$ wurden 501 Kandidat getestet, der letzte war $m = 6973$ zu $q = 3500447$. Es wurden 57 Sophie-Germain-Begleitprimzahlen gefunden. Die größte davon ist die auf Position 199 gefundene Primzahl $q = 1300181$ mit $m = 2590$. Nur für vier Kandidaten war bereits die erste Bedingung verletzt: Die anderen 440 Kandidaten fielen wegen der Verletzung der zweiten Bedingung durch.

Für $p = 503$ wurden 653 Kandidaten getestet, der letzte war $m = 9556$ zu $q = 9613337$. Es wurden dabei 115 Sophie-Germain-Begleitprimzahlen gefunden. Die zuletzt (auf Position 525) gefundene Sophie-Germain-Begleitprimzahl ist die Primzahl $q = 7727087$ mit $m = 7681$. Für keinen Kandidaten ist die erste Bedingung verletzt. Allerdings ist in 538 Fällen die zweite Bedingung verletzt.

Die Überprüfung der zweiten Bedingung für große p und große m kann viel Zeit in Anspruch nehmen, daher ist es von entscheidender Bedeutung, die Überprüfung dieser Bedingung performanter zu machen.

Ein weiterer Aspekt unserer Beobachtungen war die Dichte der Sophie-Germain-Begleitprimzahlen. Weiter unten geben wir als Beispiel die Ausgabe-Daten für $p = 5$ und $p = 41$ an, dabei steht SGB für eine Sophie-Germain-Begleitprimzahl zu p mit dem Multiplikator $mult$.

Für $p = 5$ ist $S(5) = 172$ und $m_{max} = 17$. Die Sophie-Germain-Begleitprimzahlen sind auf den ersten vier Positionen, das heißt die ersten vier Kandidaten für den Multiplikator liefern tatsächlich alle Sophie-Germain-Begleitprimzahlen.

```
'Gefunden auf', pos = 1, mult(5) = 1, SGB(5) = 11
'Gefunden auf', pos = 2, mult(5) = 4, SGB(5) = 41
'Gefunden auf', pos = 3, mult(5) = 7, SGB(5) = 71
'Gefunden auf', pos = 4, mult(5) = 10, SGB(5) = 101
pos = 5, k = 13, q = 131, 'Bed.2 verletzt'
```

Für $p = 41$ ist $S(41) = 2433844$ und $m_{max} = 29681$. Die ersten acht Kandidaten für den Multiplikator liefern Sophie-Germain-Begleitprimzahlen. Die Sophie-Germain-Begleitprimzahlen treten folgendermaßen auf:

```
'Gefunden auf', pos = 1, mult(41) = 1, SGB(41) = 83
'Gefunden auf', pos = 2, mult(41) = 10, SGB(41) = 821
'Gefunden auf', pos = 3, mult(41) = 19, SGB(41) = 1559
'Gefunden auf', pos = 4, mult(41) = 28, SGB(41) = 2297
'Gefunden auf', pos = 5, mult(41) = 31, SGB(41) = 2543
'Gefunden auf', pos = 6, mult(41) = 34, SGB(41) = 2789
'Gefunden auf', pos = 7, mult(41) = 43, SGB(41) = 3527
'Gefunden auf', pos = 8, mult(41) = 49, SGB(41) = 4019
pos = 9, k = 61, q = 5003, 'Bed.2 verletzt'
pos = 10, k = 70, q = 5741, 'Bed.2 verletzt'
pos = 11, k = 73, q = 5987, 'Bed.2 verletzt'
pos = 12, k = 85, q = 6971, 'Bed.2 verletzt'
'Gefunden auf', pos = 13, mult(41) = 103, SGB(41) = 8447
pos = 14, k = 106, q = 8693, 'Bed.2 verletzt'
pos = 15, k = 115, q = 9431, 'Bed.2 verletzt'
pos = 16, k = 118, q = 9677, 'Bed.2 verletzt'
'Gefunden auf', pos = 17, mult(41) = 121, SGB(41) = 9923
pos = 18, k = 124, q = 10169, 'Bed.2 verletzt'
pos = 19, k = 139, q = 11399, 'Bed.2 verletzt'
pos = 20, k = 160, q = 13121, 'Bed.2 verletzt'
'Gefunden auf', pos = 21, mult(41) = 163, SGB(41) = 13367
pos = 22, k = 166, q = 13613, 'Bed.2 verletzt'
pos = 23, k = 169, q = 13859, 'Bed.2 verletzt'
pos = 24, k = 181, q = 14843, 'Bed.2 verletzt'
pos = 25, k = 190, q = 15581, 'Bed.2 verletzt'
pos = 26, k = 196, q = 16073, 'Bed.2 verletzt'
```

```
pos = 27, k = 199, q = 16319, 'Bed.2 verletzt'
pos = 28, k = 205, q = 16811, 'Bed.2 verletzt'
pos = 29, k = 220, q = 18041, 'Bed.2 verletzt'
pos = 30, k = 223, q = 18287, 'Bed.2 verletzt'
pos = 31, k = 241, q = 19763, 'Bed.2 verletzt'
pos = 32, k = 253, q = 20747, 'Bed.2 verletzt'
pos = 33, k = 268, q = 21977, 'Bed.1 verletzt'
'Gefunden auf', pos = 34, mult(41) = 274, SGB(41) = 22469
pos = 35, k = 280, q = 22961, 'Bed.2 verletzt'
pos = 36, k = 301, q = 24683, 'Bed.2 verletzt'
pos = 37, k = 313, q = 25667, 'Bed.2 verletzt'
pos = 38, k = 316, q = 25913, 'Bed.2 verletzt'
pos = 39, k = 331, q = 27143, 'Bed.2 verletzt'
pos = 40, k = 349, q = 28619, 'Bed.2 verletzt'
pos = 41, k = 370, q = 30341, 'Bed.2 verletzt'
pos = 42, k = 379, q = 31079, 'Bed.2 verletzt'
pos = 43, k = 388, q = 31817, 'Bed.2 verletzt'
pos = 44, k = 391, q = 32063, 'Bed.2 verletzt'
pos = 45, k = 394, q = 32309, 'Bed.2 verletzt'
pos = 46, k = 400, q = 32801, 'Bed.2 verletzt'
'Gefunden auf', pos = 47, mult(41) = 415, SGB(41) = 34031
pos = 48, k = 433, q = 35507, 'Bed.2 verletzt'
.
.
.
pos = 2211, k = 29650, q = 2431301, 'Bed.2 verletzt'
```

Bereits aus diesen Beispielen wird ersichtlich, dass die Sophie-Germain-Begleitprimzahlen zu einem p sehr dicht am Beginn des Suchraumes liegen und dann immer seltener werden. Dabei kann es größere Lücken zwischen zwei aufeinander folgenden Vorkommen von Sophie-Germain-Begleitprimzahlen geben. Die Verteilung der Sophie-Germain-Begleitprimzahlen genauer zu beobachten und zu beschreiben ist eine weitere interessante Aufgabe.

Kapitel 5

Zusammenfassung und Ausblick

In der vorliegenden Arbeit wurde der Begriff der Sophie-Germain-Begleitprimzahl zu einer beliebigen ungeraden Primzahl p eingeführt und Dicksons obere Schranke für die Sophie-Germain-Begleitprimzahlen bewiesen. Zudem wurde Dicksons Schranke anhand von experimentellen Ergebnissen diskutiert. Dickson bewies eine bereits früher ausgesprochene Vermutung von Libri, wonach die Anzahl der Sophie-Germain-Begleitprimzahlen zu jedem p endlich ist. Nicht zuletzt war es interessant, mithilfe von modernen Möglichkeiten die Sophie-Germain-Begleitprimzahlen sowie Dicksons Schranke für einige Zahlen p zu bestimmen und die Ergebnisse zu analysieren.

Bei der Diskussion der Ergebnisse ging es insbesondere um die Bestimmung der Sophie-Germain-Begleitprimzahlen zu verschiedenen ungeraden Primzahlen p und um den Vergleich zwischen der jeweils größten Sophie-Germain-Begleitprimzahl zu p und Dicksons Schranke $S(p)$. Aus der Analyse der Ergebnisse wurde ersichtlich, dass Dicksons Schranke nicht die bestmögliche ist[1]: Für große p überschätzt Dicksons Schranke die größte Sophie-Germain-Begleitprimzahl q stark. Eine andere Schranke wird in (Schur, 1917) bewiesen. Dicksons Schranke ist jedoch schärfer als die von Schur.

Ein weiterer Aspekt unserer Betrachtungen waren die jeweils kleinsten Sophie-Germain-Begleitprimzahlen mit den entsprechenden Multiplikatoren für die ersten 100000 ungeraden Primzahlen. Nicht zuletzt haben wir das Verfahren zur Bestimmung der Sophie-Germain-Begleitprimzahlen und seine Implementation in Maple 9.5 diskutiert.

Aufbauend auf diese Ergebnisse lassen sich einige weiterführende Fragen for-

[1] Siehe (Ribenboim, 1979, Lecture XII, p.250)

mulieren, die im Rahmen dieser Arbeit nicht ausgearbeitet werden können.

Eine wesentliche Frage ist, ob für große p eine möglichst kleine obere Schranke für $q = 2kp + 1$ bestimmt werden kann. Das entscheidende Problem in der Praxis ist, eine Heuristik zu finden, die zu einer sinnvollen Abbruchbedingung der Suche nach Sophie-Germain-Begleitprimzahlen führt, um den Rechenaufwand geringer zu halten.

Für große Zahlen p und k ist es insbesondere schwierig, die zweite Bedingung der Sophie-Germain-Begleitprimzahl zu überprüfen, nämlich ob es zwei aufeinander folgende p-te Potenzen mod q gibt. Daher ist es sinnvoll, nach weiteren Optimierungsmöglichkeiten der Überprüfung dieser Bedingung zu forschen.

Eine mögliche Strategie zur Optimierung basiert auf folgenden Überlegungen. Für die Überprüfung der zweiten Bedingung der Sophie-Germain-Begleitprimzahlen könnte die Berechnung der Wahrscheinlichkeit nützlich sein, dass in der entsprechenden Menge der p-ten Potenzen mod q keine zwei Zahlen die Differenz Eins haben. Eine Formulierung des *verallgemeinerten Geburtstagsproblems* nach (Abramson & Moser, 1970) lautet: Sei $s \geq 1$ gegeben und sei t die Anzahl der *zufällig* ausgewählten Personen. Wie hoch ist die Wahrscheinlichkeit, dass Geburtstage eines jeden Paares einen Abstand von mindestens s Tagen haben? Um jedoch zu überprüfen, ob die uns interessierende Frage auf das verallgemeinerte Geburtstagsproblem zurückgeführt werden kann, muss zunächst untersucht werden, ob die p-ten Potenzen mod q als zufällig aufgefasst werden können. Daher wäre es interessant zu einem festen p und für verschiedene Primzahlen $q = 2kp + 1$ die tatsächliche Verteilung der p-ten Potenzen mod q mit statistischen Methoden zu untersuchen.

Es könnte ferner nützlich sein, das Verfahren zur Bestimmung der Sophie-Germain-Begleitprimzahlen in einer effizienter ausführbaren Programmiersprache als Maple zu implementieren und die Berechnungszeiten zu vergleichen. PARI/GP ist ein für schnelle zahlentheoretische Berechnungen ausgelegtes Computeralgebrasystem, auf dem eine performantere Implementation als in Maple möglich wäre. PARI/GP unterliegt der GPL und ist frei erhältlich [2].

Eine weitere wichtige Frage ist, ob zu jeder ungeraden Primzahl mindestens eine Sophie-Germain-Begleitprimzahl existiert. Experimentell wurde im Rahmen der Arbeit für die ersten 100000 ungeraden Primzahlen p, $3 \leq p \leq 1299721$ mindestens eine Sophie-Germain-Begleitprimzahl bestimmt. Doch auch wenn für größere p Sophie-Germain-Begleitprimzahlen bestimmt werden, steht ein allgemeingültiger Beweis aus.

[2] `http://pari.math.u-bordeaux.fr/` (Stand: 15.12.2007)

Bis auf eine einzige Ausnahme gilt für die Primzahlen p in diesem Suchraum, dass die erste Primzahl $q = 2kp + 1$ mit k derart, dass $\mathrm{ggT}(k, 3) = 1$ ist, tatsächlich eine Sophie-Germain-Begleitprimzahl ist. Ob es weitere solche Ausnahmen gibt, muss untersucht werden.

In (Ribenboim, 1979, Lecture IV) ist ferner folgende Frage formuliert: Sei $k \geq 1$ gegeben. Was lässt sich über die Menge der Primzahlen p aussagen, für welche ein h, $1 \leq h \leq k$ existiert, sodass auch $2hp + 1$ prim ist? Speziell für $k = h = 1$ ist dies die Menge der Sophie-Germain-Primzahlen. Ein Beweis der Vermutung, dass es unendlich viele Sophie-Germain-Primzahlen gibt, wurde noch nicht erbracht.

Literatur

ABRAMSON, MORTON, & MOSER, W. O. J. 1970. More Birthday Surprises. *The American Mathematical Monthly*, **77**(8), 856–858.

BACHMANN, PAUL. 1968a. *Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie*. Leipzig: Druck und Verlag von B. G. Teubner. Nachdruck der 1. Auflage von 1872.

BACHMANN, PAUL. 1968b. *Niedere Zahlentheorie*. Chelsea Publishing Company. Nachdruck der Auflage von 1902.

BACHMANN, PAUL. 1976. *Das Fermatproblem in seiner bisherigen Entwicklung*. Springer Verlag. Nachdruck der Auflage von 1919.

BOREWICZ, SENON I., & ŠAFAREVIČ, IGOR R. 1966. *Zahlentheorie*. Birkhäuser Verlag.

DICKSON, LEONHARD E. 1908. On the Last Theorem of Fermat. *Messenger of Mathematics*, **38**, 14–32.

DICKSON, LEONHARD E. 1909. Lower Limit for the Number of Sets of Solutions of $x^e + y^e + z^e \equiv 0 \pmod{p}$. *Journal für die reine und angewandte Mathematik*, **135**, 181–188.

DICKSON, LEONHARD E. 1917. Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers. *The Annals of Mathematics*, **18**(4), 161–187.

DICKSON, LEONHARD E. 1971a. *History of the Theory of Numbers: Diophantine Analysis*. Vol. 2. Carnegie Institution. Nachdruck der Auflage von 1920.

DICKSON, LEONHARD E. 1971b. *History of the Theory of Numbers: Divisibility and Primality*. Vol. 1. Carnegie Institution. Nachdruck der Auflage von 1919.

DICKSON, LEONHARD E. 1971c. *History of the Theory of Numbers: Quadratic and Higher Forms*. Vol. 3. Carnegie Institution. Nachdruck der Auflage von 1923.

EDWARDS, HAROLD M. 1977. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*. Springer Verlag.

EULER, LEONHARD. 1770. *Vollständige Anleitung zur Algebra*. St. Petersburg: Royal Acad. of Sciences. Übersetzung ins Deutsche 1802, Übersetzung ins Englische 1822.

HURWITZ, A. 1909. Über die Kongruenz $ax^e + by^e + cz^e \equiv 0 \pmod{p}$. *Journal für die reine und angewandte Mathematik*, **136**, 273–292.

JANTZEN, JENS CARSTEN, & SCHWERMER, JOACHIM. 2006. *Algebra*. Springer Verlag.

JÄNICHEN, W. 1923. Über einen zahlentheoretischen Satz von Hurwitz. *Mathematische Zeitschrift*, **17**(1), 277–292.

KLÖSGEN, WILLI. 1970. *Untersuchungen über Fermatsche Kongruenzen*. Berichte der Gesellschaft für Mathematik und Datenverarbeitung. Gesellschaft für Mathematik und Datenverarbeitung.

KOCH, HELMUT. 1997. *Zahlentheorie: Algebraische Zahlen und Funktionen*. Vieweg Studium.

LAUBENBACHER, REINHARD, & PENGELLEY, DAVID. 1999. *Mathematical Expeditions: Chronicles by the Explorers*. Springer Verlag.

LEMMERMEYER, FRANZ. 2000. *Reciprocity Laws: From Euler to Eisenstein*. Springer Verlag.

LEUTBECHER, ARMIN. 1996. *Zahlentheorie: Eine Einführung in die Algebra*. Springer Verlag.

LEVEQUE, WILLIAM J. 1956a. *Topics in Number Theory*. Vol. 1. Addison-Wesley Publishing Company.

LEVEQUE, WILLIAM J. 1956b. *Topics in Number Theory*. Vol. 2. Addison-Wesley Publishing Company.

LEVEQUE, WILLIAM J. 1977. *Fundamentals of Number Theory*. Addison-Wesley Publishing Company.

LIBRI, GUGLIELMO. 1832. Mémoire sur la théorie des nombres. *Journal für die reine und angewandte Mathematik*, **9**, 261–276.

MATHPAGES. 2005. *On Case 1 of Fermat's Last Theorem*. Online. URL: <http://www.mathpages.com/home/kmath367.htm> (Stand: 02.12.2007).

RIBENBOIM, PAULO. 1979. *13 Lectures on Fermat's Last Theorem*. Springer Verlag.

RIBENBOIM, PAULO. 2004. *The Little Book of Bigger Primes*. 2 edn. Springer Verlag.

RIDDLE, LAWRENCE H. 2001. *Sophie Germain and Fermat's Last Theorem*. Online. URL: <http://www.agnesscott.edu/lriddle/women/germain-FLT/SGandFLT.htm> (Stand: 02.12.2007).

SCHUR, I. 1917. Über die Kongruenz $x^m + y^m \equiv z^m \pmod{p}$. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, **25**, 114–117.

SINGH, SIMON. 2005. *Fermats letzter Satz*. dtv.

WENDT, E. 1895. Elementarer Beweis des Satzes, dass in jeder unbegrenzter arithmetischen Progression $my + 1$ unendlich viele Primzahlen vorkommen. *Journal für die reine und angewandte Mathematik*, **115**, 85–88.

WILES, ANDREW. 1995. Modular Elliptic Curves and Fermat's Last Theorem. *The Annals of Mathematics*, **141**(3), 443–551.

Erklärung

1. Ich versichere hiermit, dass ich die vorliegende Arbeit mit dem Thema

   „Untersuchung der oberen Schranke
   für Sophie–Germain–Begleitprimzahlen“

   selbstständig verfasst und keine anderen Hilfsmittel als die angegebenen benutzt habe. Die Stellen, die anderen Werken dem Wortlaut oder dem Sinne nach entnommen sind, habe ich in jedem einzelnen Falle durch Angabe der Quelle, auch der benutzten Sekundärliteratur, als Entlehnung kenntlich gemacht.

   Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

2. Diese Arbeit wird nach Abschluss des Prüfverfahrens der Universitätsbibliothek Konstanz übergeben und ist durch Einsicht und Ausleihe somit der Öffentlichkeit zugänglich. Als Urheber der anliegenden Arbeit stimme ich diesem Verfahren *zu / nicht zu*. [3]

Konstanz, den _____ _____

(Marina Herbst)

[3] Nichtzutreffendes bitte streichen