Friedrich-Alexander-Universität Erlangen-Nürnberg
Studiengang Mathematik

Der kleinste quadratische Nichtrest

vorgelegt von
Harriet Fakesch

Betreuer
Professor Wolfgang Ruppert

29. April 2004

Inhaltsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einleitung

Eines der reizvollsten Kapitel der elementaren Zahlentheorie ist die Theorie der quadratischen Reste. Sie entspringt aus der Frage, für welche primen Restklassen $a \bmod m$, bei gegebenem $m \in \mathbb{N}$, $m \neq 1$ die Kongruenz

$$x^2 \equiv a \bmod m \tag{1.1}$$

eine Lösung besitzt. Existiert eine Lösung, spricht man von quadratischen Resten, andernfalls von quadratischen Nichtresten, die uns in dieser Arbeit besonders interessieren werden. Da sich, wie wir sehen werden, die Frage der Lösbarkeit der Kongruenz (1.1) auf Primzahlpotenzmoduln zurückführen läßt, beschäftigen wir uns hauptsächlich mit quadratischen Nichtresten modulo einer Primzahl p.

Während Carl Friedrich Gauss (*1777 †1855), auf den der Begriff der quadratischen Reste und Nichtreste zurückgeht, sich mit der Unterscheidung in Worten begnügte, führte Adrien-Marie Legendre (*1752 †1833) im Jahre 1785 das nach ihm benannte Legendre-Symbol $\left(\frac{a}{p}\right)$ ein, das quadratische Reste bzw. Nichtreste a modulo p danach unterscheidet, ob $\left(\frac{a}{p}\right) = 1$ bzw. $\left(\frac{a}{p}\right) = -1$ gilt.

Im zweiten Kapitel dieser Arbeit werden wir uns allgemein mit den quadratischen Resten beschäftigen und nach Einführung des Legendre-Symbols noch weitere Kriterien angeben, mit denen sich quadratische Reste bestimmen lassen. Durch diese Kriterien findet man zwar eine Antwort auf die Frage, welche Zahlen $a \neq 0$ quadratische Reste modulo einer gegebenen Primzahl p sind, jedoch ist die eigentlich interessantere Frage:

Für welche Primzahlen $p \neq 2$ ist eine gegebene ganze Zahl $a \neq 0$ quadratischer Rest?

Diese Frage führt zu dem erstmals von Gauss bewiesenen quadratischen Reziprozitätsgesetz und seinen beiden Ergänzungssätzen. Diese waren bereits Pierre de Fermat (*1601 †1665) bekannt, aber Beweise für den ersten bzw. zweiten Ergänzungssatz wurden erst von Leonhard Euler (*1707 †1783) bzw. Joseph Louis Lagrange (*1736 †1813) geliefert. Das quadratische Reziprozitätsgesetz selbst wurde etwa 1745 von Euler implizit benutzt, spätestens aber 1772 erstmals von ihm klar ausgesprochen (vgl. [Bund, S. 144]). In Artikel 151 seiner *Disquisitiones arithmeticae* schreibt Gauss, daß gewisse andere Sätze, die aus dem quadratischen Reziprozitätsgesetz folgen und zu dessen Entdeckung hätten führen können, schon

EULER um 1740 bekannt waren (vgl. [Gau], [Rem/Ull, S. 250]). Allerdings kannte EULER keine Beweise für seine Sätze.

Unabhängig davon wurde es 1785 von LEGENDRE entdeckt und teilweise bewiesen. Allerdings basierte sein Beweis auf der von ihm nicht bewiesenen Annahme, daß zu jeder Primzahl p der Form $4 \cdot k + 1$ eine Primzahl q der Form $4 \cdot l + 3$ existiert mit $\left(\frac{p}{q}\right) = -1$. Diese wesentliche Lücke hat er nie schließen können. LEGENDRES Vermutung wurde erst 1837 von GUSTAV PETER LEJEUNE DIRICHLET (*1805 †1859) bewiesen (vgl. [Rem/Ull, S. 250]).

Als Achtzehnjähriger formulierte GAUSS unabhängig von seinen Vorgängern das quadratische Reziprozitätsgesetz in Artikel 131 der *Disquisitiones arithmeticae* und lieferte 1796 nach einem Jahr harter Arbeit den ersten kompletten Beweis. Insgesamt gibt es von GAUSS acht methodisch verschiedene Beweise für das quadratische Reziprozitätsgesetz. In den Jahren zwischen 1796 und 1896 wurden von verschiedenen bekannten Mathematikern weitere 45 Beweise angegeben. Bis heute sind deutlich über 150 Beweise des quadratischen Reziprozitätsgesetzes veröffentlicht worden.

Wie oben schon erwähnt, interessieren uns die quadratischen Nichtreste modulo einer Primzahl p, insbesondere der kleinste quadratische Nichtrest, d.h. die kleinste natürliche Zahl, die kein quadratischer Rest modulo p ist. Dabei konzentriert sich diese Arbeit auf die elementaren Methoden, die verschiedene Abschätzungen für den kleinsten quadratischen Nichtrest $n^*(p)$ bzw. für den kleinsten ungeraden quadratischen Nichtrest $n(p)$ liefern. Diese werden wir in Kapitel 3 ausführlich behandeln.

Im folgenden bezeichnen wir mit $\log n$ immer den natürlichen Logarithmus zur Basis e.

Nach den beiden Ergänzungssätzen des quadratischen Reziprozitätsgesetzes kann man in den Fällen $p \equiv 3,\ 5,\ 7 \bmod 8$ einen konkreten quadratischen Nichtrest angeben. Für Primzahlen der Form $8n \pm 3$ ist immer 2 quadratischer Nichtrest, für die Primzahlen $p \equiv 7 \bmod 8$, ist -1 ein quadratischer Nichtrest. Es bleiben also die Primzahlen der Form $p \equiv 1 \bmod 8$.

Wie in vielem ist GAUSS auch hier vorausgegangen. Im Zusammenhang mit dem ersten Beweis des quadratischen Reziprozitätsgesetzes bewies er für diese Primzahlen in den *Disquisitiones arithmeticae* in Art. 129 die Abschätzung

$$n(p) \leq 2\lfloor\sqrt{p}\rfloor + 1.$$

Erst im Jahre 1923 gelang es TRYGVE NAGELL, diese Abschätzung auch für die Primzahlen $p \equiv 3,\ 5,\ 7 \bmod 8$ nachzuweisen. Im Gegensatz zu GAUSS, der einen Widerspruchsbeweis durchführt, konstruiert NAGELL in jedem einzelnen Fall einen passenden quadratischen Nichtrest, der dann zu der gewünschten Abschätzung führt. Im Jahre 1950 veröffentlichte er für die Restklassen $1,\ 5,\ 7 \bmod 8$ verbesserte Ergebnisse. 1951 gab er die folgenden verbesserten Abschätzungen für $n(p)$ an:

1. *Ist p eine Primzahl der Form $8n+1$, dann gilt* $n(p) \leq \sqrt{\frac{1}{2} \cdot (p+1)}$.
2. *Ist p eine Primzahl der Form $8n+7$ mit $p \neq 7,\ 23$, dann gilt* $n(p) \leq \sqrt{p-6}$.
3. *Ist p eine Primzahl mit $p \equiv 5$ mod 8, dann gilt* $n(p) < \sqrt{p}$, *außer für* $p = 5,\ 13,\ 109$.

4. *Ist p eine Primzahl mit $p \equiv 3$ mod 8, dann gilt $n(p) < \sqrt{p} + 4$, außer für $p = 131$.*

In dem Buch *"An Introduction to The Theory of Numbers"* von IVAN NIVEN, HERBERT S. ZUCKERMAN und HUGH L. MONTGOMERY findet man die Abschätzung

$$n^*(p) < 1 + \sqrt{p},$$

die sich im Gegensatz zu den vorherigen Ergebnissen erstaunlich kurz und einfach beweisen läßt. Leider ist es nicht bekannt, auf wen dieser elegante Beweis zurückgeht.

In Anlehnung an NAGELLS Arbeiten bewies L. RÉDEI im Jahr 1953 für alle ungeraden Primzahlen $p \neq 3, 5, 7, 11, 13, 23, 59, 109, 131$

$$n(p) < \sqrt{p}.$$

BENGT STOLT verbesserte dieses Ergebnis und bewies 1954 für Primzahlen der Form $p = 8 \cdot n + 5$, $p \neq 5, 13, 37, 61, 109$ die Abschätzung

$$n(p) < \left(\frac{p}{2}\right)^{\frac{1}{2}}.$$

Bereits im Jahre 1931 veröffentlichte ALFRED BRAUER seine Abschätzungen für $n(p)$. Seine drei Sätze, in denen er die Fälle $p \equiv 7$ mod 8, $p \equiv 5$ mod 8 und $p \equiv \pm 3$ mod 8 betrachtet, enthalten bessere Ergebnisse als die Sätze von NAGELL. Er zeigt in teilweise sehr umfangreichen, aber kleinschrittigen Beweisen, die gut nachvollziehbar sind:

1. *Ist p eine Primzahl der Form $8n + 7$, so gilt $n^*(p) < (2p)^{\frac{2}{5}} + 3(2p)^{\frac{1}{5}} + 1$.*
2. *Ist p eine Primzahl der Form $8n + 5$, so gilt $n(p) < \sqrt{p+4} + 2$.*
3. *Ist $p > 3$ eine Primzahl der Form $8n \pm 3$, so gilt $n(p) < 2\left[(4p)^{\frac{2}{5}} + (4p)^{\frac{1}{5}}\right] + 1$.*

In Anlehnung an BRAUERS Arbeiten veröffentlichten RICHARD H. HUDSON und KENNETH S. WILLIAMS im Jahre 1980 die leicht verbesserte Abschätzung

$$n(p) < p^{\frac{2}{5}} + 12 \cdot p^{\frac{1}{5}} + 33$$

für ungerade Primzahlen der Form $p \not\equiv 1$ mod 8.

LARS FJELLSTEDT publizierte im Jahre 1956 in der Zeitschrift *Arkiv för Matematik* die Abschätzung

$$n(p) < 6 \cdot \log p$$

für alle Primzahlen p ab einer gewissen Schranke $p_0 > 0$. Sein Beweis enthält jedoch einen Fehler.

Neben den elementaren Abschätzungen für den kleinsten quadratischen Nichtrest gibt es auch verschiedene analytische Ergebnisse, die im vierten Kapitel dieser Arbeit aufgeführt werden. Einige stützen sich jedoch auf die erweiterte Riemannsche Vermutung (ERH), die bisher immer noch unbewiesen ist. Ohne ERH kommen die Abschätzungen von IVAN MATVEEVICH VINOGRADOV (*1891 †1983) und D. A. BURGESS aus.

Schon sehr früh, im Jahre 1919, zeigte VINOGRADOV, daß ab einer gewissen Schranke

$$n^*(p) < p^{\frac{1}{2\sqrt{e}}} \cdot (\log p)^2$$

gilt. Sieben Jahre später gab er eine verallgemeinerte Abschätzung für Nichtreste n-ten Grades modulo p an.

Mit ähnlichen Mitteln wie VINOGRADOV bewies BURGESS im Jahre 1957, daß für hinreichend große Primzahlen p und für alle $\alpha > \frac{1}{4\sqrt{e}} \approx 0,1516$ gilt

$$n^*(p) = O(p^\alpha).$$

Dies ist die beste heute bekannte Abschätzung, die ohne die erweiterte Riemannsche Vermutung auskommt.

Die weiteren Abschätzungen des kleinsten quadratischen Nichtrestes lassen sich nur unter Annahme der ERH beweisen.

Im Jahre 1952 bewies NESMITH C. ANKENY, daß unter Voraussetzung der ERH gilt

$$n^*(p) = O\left((\log p)^2\right).$$

Sein Beweis zu der Abschätzung

$$n^*(p) < p^\epsilon$$

für $p \equiv 3 \bmod 4$ und für alle $\epsilon > 0$ und $p > p_0(\epsilon)$, den er 1954 veröffentlicht, wird zunächst als richtig angesehen. Erst 1956 bemerkte RODOSSKIĬ in einem Artikel in den *Mathematical Reviews*, daß ANKENYS Beweis einen Fehler enthält.

In seiner Dissertation konnte ERIC BACH 1984 für die Abschätzung $n^*(p) = O\left((\log p)^2\right)$ von ANKENY konkrete Konstanten bestimmen. Er zeigte, daß

$$n^*(p) \leq 2 \cdot (\log p)^2$$

gilt, falls die erweiterte Riemannsche Vermutung stimmt.

In seiner Dissertation bewies SEBASTIAN WEDENIWSKI im Jahre 2001 unter Voraussetzung der erweiterten Riemannschen Vermutung für $x = \min\left\{k \in \mathbb{N} \mid \left(\frac{k}{m}\right) \neq 1\right\}$ die Abschätzung

$$x < \frac{3}{2} \cdot \log(m)^2 - \frac{44}{5} \cdot \log m + 13,$$

wobei $m > 1$ eine ungerade positive ganze Zahl ist mit $m \neq n^2$ für $n \in \mathbb{N}$. Das Ergebnis scheint besser zu sein als die Abschätzung von BACH, allerdings ist der Satz in der angegebenen Form nicht richtig.

Als Folgerung eines Primzahlsatzes von ERIC BACH und JEFFREY SHALLIT erhält man die Abschätzung

$$n^*(p) = O\left((\log p)^{2+\epsilon}\right),$$

für jedes $\epsilon > 0$.

Im fünften Kapitel widmen wir uns im Gegensatz zu den bisherigen Ergebnissen den unteren Schranken für $n(p)$. HANS SALIÉ bewies im Jahre 1949, daß es eine Konstante $c > 0$ gibt, so daß für unendlich viele Primzahlen p

$$n^*(p) > c \cdot \log p$$

gilt.

Unter Voraussetzung der erweiterten Riemannschen Vermutung verschärfte HUGH MONTGOMERY 1971 diese Aussage und bewies, daß es eine Konstante c gibt, so daß für unendlich viele Primzahlen gilt

$$n^*(p) \geq c \cdot \log p \log\log p.$$

Im Jahre 1990 verbesserten S. W. GRAHAM und C. J. RINGROSE die Abschätzung von SALIÉ und bewiesen ohne ERH die Abschätzung

$$n^*(p) \geq c \cdot \log p \log\log\log p$$

für unendlich viele $p \in \mathbb{P}$ mit einem $c > 0$.

Das sechste Kapitel beschäftigt sich mit der Verteilung der kleinsten quadratischen Nichtreste, insbesondere mit der Frage, wie oft eine Primzahl q als quadratischer Nichtrest modulo einer Primzahl p auftritt. Wir werden zeigen, daß sich die Anzahl der $p \in \mathbb{P}$ mit $n(p) = q$ jedesmal ungefähr halbiert.

Auch in Anwendungen spielt der kleinste quadratische Nichtrest eine große Rolle. Dies wollen wir in Kapitel 7 anhand von zwei Beispielen zeigen. Dabei betrachten wir das Quadratwurzelziehen modulo p und einen Primzahltest.

Mein herzlicher Dank gilt Professor Wolfgang Ruppert für die sehr gute Betreuung und Unterstützung.

Kapitel 2

Quadratische Reste

Wir wollen in diesem Kapitel eine kleine Einführung in die Theorie der quadratischen Reste geben. Zunächst definieren wir das LEGENDRE-Symbol, durch das die Lösbarkeit der Gleichung $x^2 \equiv a \bmod p$ beschrieben wird. Mit dem EULER-Kriterium und dem GAUSS-Kriterium lernen wir verschiedene Wege zur Berechnung des LEGENDRE-Symbols kennen. Im Rahmen des GAUSS-Kriteriums kommen dabei das quadratische Reziprozitätsgesetz und seine beiden Ergänzungssätze ins Spiel.

2.1 Das LEGENDRE-Symbol $\left(\frac{a}{p}\right)$

Definition

Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$.

Ist die Kongruenz

$$x^2 \equiv a \ mod \ p$$

*lösbar, nennt man a einen **quadratischen Rest** modulo p, andernfalls einen **quadratischen Nichtrest** modulo p.*

Man definiert das LEGENDRE*-Symbol $\left(\frac{a}{p}\right)$ durch*

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{falls } ggT(a,p) = 1 \text{ und } a \text{ quadratischer Rest mod } p \text{ ist} \\ -1, & \text{falls } ggT(a,p) = 1 \text{ und } a \text{ quadratischer Nichtrest mod } p \text{ ist} \\ 0, & \text{falls } a \equiv 0 \ mod \ p. \end{cases}$$

*Den **kleinsten quadratischen Nichtrest**, also die kleinste natürliche Zahl, die kein quadratischer Rest modulo p ist, bezeichnen wir mit $n^*(p)$.*

Eigenschaften des LEGENDRE-Symbols

- Ist $p \nmid ab$ und $a \equiv b \bmod p$, dann ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

- Ist $p \nmid a$, dann ist $\left(\frac{a^2}{p}\right) = 1$; insbesondere ist $\left(\frac{1}{p}\right) = 1$.

2.2 Das JACOBI-Symbol

Das JACOBI-Symbol wurde von CARL GUSTAV JACOBI (*1804 †1851) eingeführt und ist eine Verallgemeinerung des LEGENDRE-Symbols.

Definition

Für eine ungerade natürliche Zahl $m \geq 1$ mit Primfaktorzerlegung $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ und $a \in \mathbb{Z}$ definieren wir das JACOBI-*Symbol $\left(\frac{a}{m}\right)$ durch*

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

wo $\left(\frac{a}{p_i}\right)$ das LEGENDRE-*Symbol bezeichnet.*

Satz

Seien $a, b \in \mathbb{Z}$ und m, n ungerade natürliche Zahlen. Dann gelten für das JACOBI-*Symbol folgende Eigenschaften:*

$$\begin{aligned}
\left(\frac{a}{m}\right) &= \left(\frac{b}{m}\right), \text{ falls } a \equiv b \bmod m, \\
\left(\frac{a \cdot b}{m}\right) &= \left(\frac{a}{m}\right) \cdot \left(\frac{b}{m}\right), \\
\left(\frac{-1}{m}\right) &= (-1)^{\frac{m-1}{2}} = \begin{cases} 1, & \text{falls } m \equiv 1 \bmod 4, \\ -1, & \text{falls } m \equiv 3 \bmod 4, \end{cases} \\
\left(\frac{2}{m}\right) &= (-1)^{\frac{m^2-1}{8}} = \begin{cases} 1, & \text{falls } m \equiv 1,\ 7 \bmod 8, \\ -1, & \text{falls } m \equiv 3,\ 5 \bmod 8, \end{cases} \\
\left(\frac{m}{n}\right) &= (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{m}\right) = \begin{cases} \left(\frac{n}{m}\right), & \text{falls } m \equiv 1 \bmod 4 \text{ oder } n \equiv 1 \bmod 4 \\ -\left(\frac{n}{m}\right), & \text{falls } m \equiv n \equiv 3 \bmod 4. \end{cases}
\end{aligned}$$

Die Aussagen ergeben sich aus den entsprechenden Eigenschaften des LEGENDRE-Symbols.

2.3 Reduktion auf Primzahlpotenzmoduln

Ist $m \in \mathbb{N}$ eine zusammengesetzte Zahl mit der Primfaktorzerlegung

$$m = \prod_{i=1}^{\infty} {p_i}^{e_i},$$

so kann man die Lösbarkeit der Gleichung $x^2 \equiv a \bmod m$, wobei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$, auf den Primzahlfall zurückführen, was im folgenden gezeigt werden soll.

Definition

Für jedes $n \in \mathbb{N}$ gibt es eine eindeutige Darstellung $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ mit $v_p(n) \in \mathbb{N}_0$, wobei fast immer $v_p(n) = 0$ ist.

Die eindeutige Primfaktorzerlegung liefert für jedes $p \in \mathbb{P}$ eine Funktion $v_p : \mathbb{N} \to \mathbb{N}_0$. Der Wert $v_p(n)$ heißt ***p-adischer Wert*** *von n.*

Lemma

Sei $f(x) \in \mathbb{Z}[x]$ ein Polynom und p eine Primzahl. Findet man ein $\omega \in \mathbb{Z}$ mit $f'(\omega) \neq 0$ und

$$v_p(f(\omega)) \geq 2 \cdot v_p\left(f'(\omega)\right) + 1,$$

so gibt es für alle $n \in \mathbb{N}$ ein $\omega_n \in \mathbb{Z}$ mit

$$f(\omega_n) \equiv 0 \ mod\ p^n \quad und \quad \omega_n \equiv \omega \ mod\ p.$$

Einen Beweis findet man in [Ser, §2, S.14].

Damit können wir nun folgenden Satz beweisen.

2.3.1 Satz

Sei $p \in \mathbb{P}$ eine Primzahl, $e \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $ggT(p, a) = 1$. Dann gilt:

$$Es\ gibt\ ein\ x \in \mathbb{Z}\ mit\ x^2 \equiv a\ mod\ p^e \iff \begin{cases} a \equiv 1\ mod\ 2 & im\ Fall\ p = 2,\ e = 1, \\ a \equiv 1\ mod\ 4 & im\ Fall\ p = 2,\ e = 2, \\ a \equiv 1\ mod\ 8 & im\ Fall\ p = 2,\ e \geq 3, \\ \left(\frac{a}{p}\right) = 1 & im\ Fall\ p \neq 2. \end{cases}$$

Beweis:

"⇒": Im Fall $p = 2$ folgt die Behauptung sofort aus $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1\ mod\ 8$. Ist $p \neq 2$, dann folgt aus der Kongruenz $x^2 \equiv a \bmod p^e$ sofort die Kongruenz $x^2 \equiv a \bmod p$, was nach Definition des LEGENDRE-Symbols äquivalent ist mit $\left(\frac{a}{p}\right) = 1$.

"⇐": Sei zunächst $p = 2$. Ist $p^e = 2,\ 4,\ 8$, dann gilt nach Voraussetzung $a \equiv 1 \bmod p^e$, also auch $1^2 \equiv a \bmod p^e$, woraus die Behauptung folgt. Nun betrachten wir den Fall $e \geq 3$. Dazu definieren wir

$$f(x) = x^2 - a.$$

Dann ist

$$f'(x) = 2x \quad \text{und} \quad v_2\left(f'(1)\right) = v_2(2) = 1.$$

Da $f(1) = 1 - a \equiv 0 \bmod 8$, ist $v_2(f(1)) \geq 3$. Also ist

$$v_2(f(1)) \geq 2 \cdot v_2\left(f'(1)\right) + 1 = 3$$

und damit ist die Voraussetzung des Lemmas erfüllt. Demnach gibt es ein $\omega_e \in \mathbb{Z}$ mit $f(\omega_e) \equiv 0 \bmod 2^e$, also $\omega_e^2 - a \equiv 0 \bmod 2^e$ und damit $\omega_e^2 \equiv a \bmod 2^e$, was die Behauptung zeigt.

Sei nun $p \neq 2$. Wir definieren wieder $f(x) = x^2 - a$. Nach Voraussetzung ist $\left(\frac{a}{p}\right) = 1$ und somit gibt es ein $\omega \in \mathbb{Z}$ mit $\omega^2 \equiv a \bmod p$. Es ist also $\omega^2 - a \equiv 0 \bmod p$ und daher

$$v_p(f(\omega)) = v_p\left(\omega^2 - a\right) \geq 1.$$

Da $\mathrm{ggT}(a, p) = 1$, ist auch $\mathrm{ggT}(\omega, p) = 1$ und daher ist

$$v_p\left(f'(w)\right) = v_p(2\omega) = 0.$$

Wir haben also

$$v_p(f(\omega)) \geq 2 \cdot v_p\left(f'(w)\right) + 1 = 1.$$

Die Voraussetzung des Lemmas ist somit wieder erfüllt und man erhält dadurch ein $\omega_e \in \mathbb{Z}$ mit $f(\omega_e) \equiv 0 \bmod p^e$ woraus schließlich $\omega_e^2 \equiv a \bmod p^e$ folgt, was die Behauptung beweist. □

Damit kann man nun die Lösbarkeit der Kongruenz $x^2 \equiv a \bmod m$ für zusammengesetze $m \in \mathbb{N}$ charakterisieren.

Folgerung

Sei $m \in \mathbb{N}$ eine natürliche Zahl mit der Primfaktorzerlegung $m = \prod_{i=1}^{\infty} {p_i}^{e_i}$ und $a \in \mathbb{Z}$ mit $ggT(a, m) = 1$. Dann gilt:

$$\text{Es gibt ein } x \in \mathbb{Z} \text{ mit } x^2 \equiv a \bmod m \iff \begin{cases} a \equiv 1 \bmod 2 & \text{im Fall } p_i = 2,\ e_i = 1, \\ a \equiv 1 \bmod 4 & \text{im Fall } p_i = 2,\ e_i = 2, \\ a \equiv 1 \bmod 8 & \text{im Fall } p_i = 2,\ e_i \geq 3, \\ \left(\frac{a}{p_i}\right) = 1 & \text{im Fall } p_i \neq 2. \end{cases}$$

Beweis:

"⇒": Die Kongruenz $x^2 \equiv a \bmod m$ impliziert natürlich die Kongruenz $x^2 \equiv a \bmod {p_i}^{e_i}$. Damit folgt die Behauptung sofort aus dem vorherigen Satz.

"$\Leftarrow$": Mit den Voraussetzungen erhalten wir aus dem letzten Satz ein $x_i \in \mathbb{Z}$ mit

$$x_i^2 \equiv a \bmod {p_i}^{e_i}.$$

Da die p_i's paarweise teilerfremd sein sollten, findet man mit dem chinesischen Restsatz ein $x \in \mathbb{Z}$ mit $x \equiv x_i \bmod {p_i}^{e_i}$ für alle i. Dann ist auch $x^2 \equiv x_i^2 \equiv a \bmod {p_i}^{e_i}$ für alle i. Also ist $x^2 \equiv a \bmod m$ und somit die Behauptung bewiesen. □

Bemerkung

Für $m \in \mathbb{N}$ bezeichnet man die primen Restklassen modulo m mit $\varphi(m)$. Diese Funktion heißt EULERSCHE φ – Funktion. Es ist $\varphi(m) = \#\{a \in \mathbb{N} : 1 \leq a \leq m \text{ und } \mathrm{ggT}(a,m) = 1\} = \#(\mathbb{Z}/m\mathbb{Z})^*$. Es gilt $\varphi(1) = 1$ und $\varphi(p) = p - 1$, wenn p eine Primzahl ist.

Eine ganze Zahl g heißt ***Primitivwurzel*** modulo p, wobei $p \in \mathbb{P}$ und $p \neq 2$, wenn sie die maximal mögliche Ordnung $\varphi(p) = p-1$ besitzt, also wenn $g^{p-1} = 1$ und $g^m \neq 1$ für $m < p-1$ gilt. Sie ist also ein Erzeuger der zyklischen Gruppe $\mathbf{F}_p^*$. Für $m, n \in \mathbb{Z}$ gilt genau dann $g^m = g^n$, wenn $m \equiv n \bmod p-1$ ist. Wegen $1 = g^{p-1} = \left(g^{\frac{p-1}{2}}\right)^2$ folgt, daß $g^{\frac{p-1}{2}}$ das einzige Element der Ordnung 2 ist, also gilt $g^{\frac{p-1}{2}} = -1$.

2.3.2 Satz von EULER-FERMAT

Ist $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ *mit* $ggT(a,m) = 1$, *dann gilt*

$$a^{\varphi(m)} \equiv 1 \ mod\ m.$$

Einen Beweis findet man in [Sche, S. 142].

Die spezielle Form des Satzes für $m = p$, also $\varphi(m) = p - 1$, geht auf FERMAT zurück.

2.3.3 Kleiner Satz von FERMAT

Ist p *eine Primzahl und* $a \in \mathbb{Z}$ *mit* $ggT(a,p) = 1$, *dann gilt*

$$a^{p-1} \equiv 1 \ mod\ p.$$

Für diesen Satz gab EULER auch einen kurzen Beweis durch Induktion an (vgl. [Sche, S. 142]).

Lemma

Ist p eine ungerade Primzahl und g eine Primitivwurzel modulo p, dann gilt für $m \in \mathbb{Z}$

$$\left(\frac{g^m}{p}\right) = 1 \iff m \equiv 0 \ mod\ 2,$$

das heißt $\left(\frac{g^m}{p}\right) = (-1)^m$.

Beweis:

" $\Rightarrow$ " : Ist g^m quadratischer Rest modulo p, dann gibt es ein $g^n \in \mathbf{F}_p$ mit $(g^n)^2 = g^m$, also gilt $m \equiv 2n \bmod p-1$. Daraus folgt sofort $m \equiv 0 \bmod 2$.

" $\Leftarrow$ " : Ist $m \equiv 0 \bmod 2$, also $m = 2n$, dann gilt $g^m = (g^n)^2$. Also ist g^m quadratischer Rest modulo p. □

Folgerung

Aus dem Lemma ergibt sich, daß $g^2,\ g^4, \ldots,\ g^{p-1}$ quadratische Reste und $g^1,\ g^3, \ldots,\ g^{p-2}$ quadratische Nichtreste sind. Folglich gibt es $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste mod p. Insbesondere gilt also $\left(\frac{g}{p}\right) = -1$ für eine Primitivwurzel g mod p.

2.4 Das EULER-Kriterium

2.4.1 Satz von EULER

Ist p eine ungerade Primzahl und $a \in \mathbb{Z}$, dann gilt

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

Beweis:

Ist $a \equiv 0 \bmod p$, ist nichts zu zeigen.

Sei nun $a \not\equiv 0 \bmod p$ und g eine Primitivwurzel modulo p.

Dann gibt es $m \in \mathbb{N}$ mit $a \equiv g^m \bmod p$ und damit folgt aus den vorherigen Betrachtungen

$$\left(\frac{a}{p}\right) = \left(\frac{g^m}{p}\right) = (-1)^m \equiv \left(g^{\frac{p-1}{2}}\right)^m = (g^m)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p.$$

□

Satz

Ist p eine ungerade Primzahl und $a, b \in \mathbb{Z}$, mit $ggT(a,p) = ggT(b,p) = 1$, dann gilt

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

Beweis:

Seien $a, b \in \mathbf{F}_p^*$. Dann gilt

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p.$$

Da das LEGENDRE-Symbol nur die Werte $0, 1, -1$ annehmen kann, folgt die Gleichung auch in $\mathbb{Z}$. □

Bemerkung

Die Formel ergibt folgendes Multiplikationsschema:

a quadr. Rest mod p,	b quadr. Rest mod p,	$\Rightarrow$	$a \cdot b$ quadr. Rest mod p,
a quadr. Nichtrest mod p,	b quadr. Rest mod p,	$\Rightarrow$	$a \cdot b$ quadr. Nichtrest mod p,
a quadr. Rest mod p,	b quadr. Nichtrest mod p,	$\Rightarrow$	$a \cdot b$ quadr. Nichtrest mod p,
a quadr. Nichtrest mod p,	b quadr. Nichtrest mod p,	$\Rightarrow$	$a \cdot b$ quadr. Rest mod p.

Somit hat eine zusammengesetzte ganze Zahl, die quadratischer Nichtrest modulo p ist, mindestens einen Primteiler, der ebenfalls quadratischer Nichtrest modulo p ist. Dies wird in Kapitel 3 bei den Abschätzungen für $n^*(p)$ bzw. $n(p)$ sehr hilfreich sein.

2.5 Das GAUSS-Kriterium

2.5.1 GAUSS'sches Lemma

Ist $a \in \mathbb{Z} \setminus \{0\}$, p eine ungerade Primzahl mit $p \nmid a$, und μ die Anzahl der Zahlen j mit $1 \leq j \leq \frac{p-1}{2}$, für welche der betragsmäßig kleinste Rest von $aj \bmod p$ negativ ist, dann gilt

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

Beweis:

Wir bezeichnen den betragsmäßig kleinsten Rest von $aj \bmod p$ mit $r(aj)$. Also ist

$$-\frac{p-1}{2} \leq r(aj) \leq \frac{p-1}{2}.$$

Für $i,\ j$ mit $1 \leq i,\ j \leq \dfrac{p-1}{2}$ und $i \neq j$, gilt natürlich

$$\begin{aligned} i &\not\equiv j \bmod p \\ \Longrightarrow\ ai &\not\equiv aj \bmod p \\ \Longrightarrow\ r(ai) &\not\equiv r(aj) \bmod p. \end{aligned} \tag{2.1}$$

Außerdem folgt aus $0 < i + j < p$

$$\begin{aligned} a(i+j) &\not\equiv 0 \bmod p \\ \Longrightarrow\ ai + aj &\not\equiv 0 \bmod p \\ \Longrightarrow\ ai &\not\equiv -aj \bmod p \\ \Longrightarrow\ r(ai) &\not\equiv -r(aj) \bmod p. \end{aligned} \tag{2.2}$$

Somit erhält man aus (2.1) und (2.2)

$$\begin{aligned} |r(ai)| &\not\equiv |r(aj)| \bmod p \\ \Longrightarrow\ |r(ai)| &\neq |r(aj)|. \end{aligned}$$

Daher ist

$$\left\{ |r(aj)| \text{ mit } 1 \leq j \leq \frac{p-1}{2} \right\} = \left\{ 1,\ 2, \ldots,\ \frac{p-1}{2} \right\}.$$

Also gilt

$$\prod_{j=1}^{\frac{p-1}{2}} r(aj) = (-1)^{\mu} \left(\frac{p-1}{2} \right)!$$

Andererseits hat man

$$\prod_{j=1}^{\frac{p-1}{2}} r(aj) \equiv \prod_{j=1}^{\frac{p-1}{2}} aj \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2} \right)! \bmod p,$$

und somit

$$a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \bmod p.$$

Aus 2.4.1 folgt $\left(\dfrac{a}{p}\right) \equiv (-1)^{\mu} \bmod p$ und daher $\left(\dfrac{a}{p}\right) = (-1)^{\mu}$. □

Beispiel

Wir wollen das LEGENDRE-Symbol $\left(\dfrac{7}{13}\right)$ berechnen. Also ist $p = 13$ und $a = 7$. Da $\dfrac{p-1}{2} = 6$, ist $1 \leq j \leq 6$. Wir erhalten folgende Tabelle:

j	1	2	3	4	5	6
$7j \bmod 13$	7	1	8	2	9	3
bzw.	-6	-12	-5	-11	-4	-10
$r(7j)$	-6	1	-5	2	-4	3

Somit ist für $j = 1,\ 3,\ 5$ der betragsmäßig kleinste Rest $r(7j)$ von $7j \bmod 13$ negativ. Man hat also $\mu = 3$ und erhält damit $\left(\frac{7}{13}\right) = (-1)^3 = -1$.

Ein weiteres Beispiel für die Anwendung des Lemmas ist die Berechnung des LEGENDRE-Symbols $\left(\frac{2}{p}\right)$ in 2.5.4.

2.5.2 Das quadratische Reziprozitätsgesetz

Sind p und q verschiedene ungerade Primzahlen, so gilt

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

Es ist also

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

Beweis:

Für den Beweis benutzen wir das GAUSS'sche Lemma. Dazu bezeichnen wir mit

μ die Anzahl der i mit $1 \le i \le \frac{q-1}{2}$, für die der betragskleinste Rest von pi modulo q negativ ist, und mit

ν die Anzahl der j mit $1 \le j \le \frac{p-1}{2}$, für die der betragskleinste Rest von qj modulo p negativ ist.

Nach 2.5.1 ist dann $\left(\frac{p}{q}\right) = (-1)^\mu$ und $\left(\frac{q}{p}\right) = (-1)^\nu$, also

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

Es muß somit gezeigt werden, daß $\mu + \nu$ genau dann ungerade ist, wenn $p \equiv q \equiv 3 \bmod 4$. Dazu zählt man nach einer Idee von FERDINAND GOTTHOLD EISENSTEIN die Gitterpunkte (x, y) mit $0 < x < \frac{p+1}{2}$ und $0 < y < \frac{q+1}{2}$, für die gilt

$$y < \frac{q}{p}\cdot x + \frac{1}{2} \quad \text{und} \quad x < \frac{p}{q}\cdot y + \frac{1}{2}.$$

Diese Punkte liegen in einem Parallelstreifen um die Gerade g mit der Gleichung $qx - py = 0$. Wir bezeichnen die Menge dieser Gitterpunkte mit Γ.

Liegt der Punkt (x, y) in Γ, dann auch der Punkt $\left(\frac{p+1}{2} - x,\ \frac{q+1}{2} - y\right)$, denn mit

$$\begin{aligned}
\frac{p}{q} \cdot \left(\frac{q+1}{2} - y\right) + \frac{1}{2} &= \frac{pq + p - 2py + q}{2q} = \frac{q\,(p+1) - p\,(2y-1)}{2q} \\
&= \frac{p+1}{2} - \frac{p}{q} \cdot \left(y - \frac{1}{2}\right) \\
&> \frac{p+1}{2} - \frac{p}{q} \cdot \left(\frac{q}{p} \cdot x + \frac{1}{2} - \frac{1}{2}\right) \\
&= \frac{p+1}{2} - x
\end{aligned}$$

und

$$\begin{aligned}
\frac{q}{p} \cdot \left(\frac{p+1}{2} - x\right) + \frac{1}{2} &= \frac{qp + q - 2qx + p}{2p} = \frac{p\,(q+1) - q\,(2x-1)}{2p} \\
&= \frac{q+1}{2} - \frac{q}{p} \cdot \left(x - \frac{1}{2}\right) \\
&> \frac{q+1}{2} - \frac{q}{p} \cdot \left(\frac{p}{q} \cdot y + \frac{1}{2} - \frac{1}{2}\right) \\
&= \frac{q+1}{2} - y
\end{aligned}$$

sind die Bedingungen für die Gitterpunkte erfüllt.

Das bedeutet, daß die Gitterpunkte aus Γ immer paarweise auftreten und ihre Anzahl genau dann ungerade ist, wenn man den Fall

$$(x, y) = \left(\frac{p+1}{2} - x,\ \frac{q+1}{2} - y\right)$$

hat. Dieser Fall tritt genau dann auf, wenn $x = \frac{p+1}{2} - x$ und $y = \frac{q+1}{2} - y$, also wenn $\left(\frac{p+1}{4},\ \frac{q+1}{4}\right)$ ein Gitterpunkt ist. $\left(\frac{p+1}{4},\ \frac{q+1}{4}\right)$ ist aber genau dann ein Gitterpunkt (und liegt dann auch in Γ), wenn $p \equiv q \equiv 3 \bmod 4$.

Jetzt bleibt noch zu zeigen, daß die Anzahl der Gitterpunkte in Γ genau $\mu + \nu$ ist. Auf der Geraden g mit Gleichung $qx - py = 0$ liegt kein Gitterpunkt aus Γ, denn aus $qx - py = 0 \iff y = \frac{q}{p} \cdot x$ würde sonst $p \mid q$ folgen. Der Punkt (x, y) liegt genau dann oberhalb von g und gehört zu Γ, wenn

$$1 \le x \le \frac{p-1}{2} \quad \text{und} \quad -\frac{p-1}{2} \le qx - py < 0$$

gilt. Also liegen oberhalb der Geraden g genau ν Punkte von Γ. Entsprechend liegt der Punkt (x, y) genau dann unterhalb der Geraden g, wenn

$$1 \le y \le \frac{q-1}{2} \quad \text{und} \quad -\frac{q-1}{2} \le py - qx < 0$$

gilt. Somit liegen genau μ Punkte von Γ unterhalb von g. Insgesamt hat man in Γ also $\mu + \nu$ Gitterpunkte und wir haben gezeigt, daß $\mu+\nu$ genau dann ungerade ist, wenn $p \equiv q \equiv 3 \mod 4$.

□

2.5.3 Erster Ergänzungssatz zum quadratischen Reziprozitätsgesetz

Für eine ungerade Primzahl p gilt

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \textit{falls } p \equiv 1 \textit{ mod } 4, \\ -1, & \textit{falls } p \equiv 3 \textit{ mod } 4. \end{cases}$$

Beweis:

Die Behauptung ergibt sich sofort aus dem Satz von EULER. □

2.5.4 Zweiter Ergänzungssatz zum quadratischen Reziprozitätsgesetz

Für eine ungerade Primzahl p gilt

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \textit{falls } p \equiv 1,\ 7 \textit{ mod } 8, \\ -1, & \textit{falls } p \equiv 3,\ 5 \textit{ mod } 8. \end{cases}$$

Beweis:

Für die betragsmäßig kleinsten Reste $r(2j)$ von $2j$ modulo p mit $1 \leq j \leq \frac{p-1}{2}$ gilt genau dann $r(2j) < 0$, wenn $\frac{p-1}{2} < 2j \leq p-1$ bzw.

$$\frac{p-1}{4} < j \leq \frac{p-1}{2}.$$

Ist $p \equiv 1 \mod 4$, dann ist $\mu = \frac{p-1}{4}$, wobei μ die Anzahl der j mit $1 \leq j \leq \frac{p-1}{2}$, für die der betragsmäßig kleinste Rest von $2j \bmod p$ negativ ist (vgl. 2.5.1). Für $p \equiv 3 \mod 4$ ist $\mu = \frac{p+1}{4}$. Folglich ist μ genau dann gerade, wenn $p - 1 \equiv 0 \mod 8$ oder $p + 1 \equiv 0 \mod 8$, also wenn $p \equiv 1,\ 7 \mod 8$. □

Folgerung

Aus dem soeben bewiesenen Satz geht hervor, daß für die Primzahlen $p \equiv 3,\ 5 \mod 8$ immer $n^*(p) = 2$ gilt. Daher werden sich die Abschätzungen im nächsten Kapitel oft auf den kleinsten **ungeraden** quadratischen Nichtrest modulo p beziehen, den wir mit $n(p)$ bezeichnen wollen.

2.5.5 Satz von Fermat-Euler

Eine ungerade Primzahl p ist genau dann Summe zweier Quadrate, d.h.

$p = a^2 + b^2$ *mit* $a, b \in \mathbb{Z}$, *wenn gilt* $p \equiv 1$ *mod* 4.

Beweis:

" $\Rightarrow$ " : Sei $p = a^2 + b^2$. Dann gilt offensichtlich $\mathrm{ggT}\,(a,p) = \mathrm{ggT}\,(b,p) = 1$. Damit erhält man

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

Das heißt -1 ist quadratischer Rest mod p, also gilt $\left(\frac{-1}{p}\right) = 1$ und somit nach 2.5.3 auch $p \equiv 1 \bmod 4$.

" $\Leftarrow$ " : Sei nun $p \equiv 1 \bmod 4$.

Wir nehmen an, p läßt sich nicht als Summe zweier Quadrate schreiben und ist minimal mit dieser Eigenschaft gewählt, also alle $\tilde{p} \in \mathbb{P}$, $\tilde{p} < p$ mit $\tilde{p} \equiv 1 \bmod 4$ sind als Quadratsumme darstellbar.

Da $\left(\frac{-1}{p}\right) = 1$, existiert ein $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \bmod p$, also $x^2 + 1 = np$, $n \in \mathbb{Z}$. Es gibt also ganze Zahlen a, b mit

$$a^2 + b^2 = mp, \text{ mit } 1 \leq a, b < \frac{p}{2} \text{ und } \mathrm{ggT}\,(a,b) = \mathrm{ggT}\,(a,p) = \mathrm{ggT}\,(b,p) = 1.$$

Man kann weiter annehmen, daß m minimal mit diesen Eigenschaften ist. Aus $a^2 + b^2 < 2 \cdot \frac{p^2}{4}$ folgt $1 < m < \frac{p}{2}$.

Sei nun q ein Primteiler von m.

Ist $q = 2$, so gilt wegen $\mathrm{ggT}\,(a,b) = 1$ und $a^2 + b^2 \equiv 0 \bmod 2$ die Kongruenz $a \equiv b \equiv 1 \bmod 2$. Dann ist

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 = \frac{a^2 + b^2}{2} = \frac{m}{2} \cdot p$$

und wir haben einen Widerspruch zur Minimalität von m.

Im Fall $q \neq 2$, hat man $a^2 + b^2 \equiv 0 \bmod q$, also $a^2 \equiv -b^2 \bmod q$ und somit $\left(\frac{a}{b}\right)^2 \equiv -1 \bmod q$. Es ist also $\left(\frac{-1}{q}\right) = 1$ und $q \equiv 1 \bmod 4$. Da außerdem $q < p$, gibt es $u, v \in \mathbb{Z}$ so, daß $q = u^2 + v^2$. Daraus erhält man $\left(\frac{u}{v}\right)^2 \equiv -1 \bmod q$ und damit $\frac{u}{v} \equiv \pm\frac{a}{b} \bmod q$. O.B.d.A. sei $\frac{u}{v} \equiv \frac{a}{b} \bmod q$, d.h. $ub \equiv va \bmod q$.

Damit ergibt sich

$$ua + vb \equiv ua + \frac{ub}{a} \cdot b \equiv \frac{u}{a}\left(a^2 + b^2\right) \equiv 0 \bmod q \quad \text{und} \quad ub - va \equiv 0 \bmod q,$$

also

$$\frac{ua+vb}{q},\ \frac{ub-va}{q} \in \mathbb{Z}.$$

Die Gleichung

$$\left(\frac{ua+vb}{q}\right)^2 + \left(\frac{ub-va}{q}\right)^2 = \frac{\left(u^2+v^2\right)\left(a^2+b^2\right)}{q^2} = \frac{m}{q}\cdot p$$

liefert aber einen Widerspruch zur Minimalitätsforderung an m. Daraus folgt schließlich die Behauptung. □

Dieser Satz ist 1640 in einem Brief von FERMAT an MERSENNE ausgesprochen worden. Allerdings war er schon ALBERT GIRARD (*1595 †1632) bekannt und heißt manchmal "Satz von GIRARD". Im Jahr 1754 publizierte EULER als erster einen Beweis. Der folgende Beweis der *Eindeutigkeit* der Darstellung geht auch auf ihn zurück (vgl. [Sche, S. 217]).

2.5.6 Satz

Die Darstellung $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$, für $p \equiv 1$ mod 4 ist eindeutig.

Beweis:

Sei $a^2+b^2 = x^2+y^2 = p$, wobei man o.B.d.A. $0 < a < b < \sqrt{p}$ und $0 < x < y < \sqrt{p}$ annehmen kann. Es ist klar, daß p keine der Zahlen a, b, x, y teilt und daß $\mathrm{ggT}(a,b) = \mathrm{ggT}(x,y) = 1$ gilt. Zu zeigen ist also $a = x$ und $b = y$. Dies ist unter den obigen Annahmen gleichwertig mit $ay - bx = 0$ bzw. $p \mid ay - bx$.

Es gilt

$$\begin{aligned}(ay-bx)\cdot(ay+bx) &= a^2y^2 - b^2x^2 = \left(p-b^2\right)\cdot y^2 - b^2x^2 \\ &= py^2 - b^2\cdot\underbrace{\left(x^2+y^2\right)}_{=p} \\ &= p\cdot\left(y^2-b^2\right).\end{aligned}$$

Also gilt $p \mid ay + bx$ oder $p \mid ay - bx$.

Wir nehmen $p \mid ay + bx$ an. Dies führt wegen $0 < ay + bx < 2p$ zu $ay + bx = p$. Wegen

$$\left(a^2+b^2\right)\cdot\left(x^2+y^2\right) = (ax-by)^2 + (ay+bx)^2 \Longleftrightarrow p\cdot p = (ax-by)^2 + p^2$$

muß gelten $ax - by = 0$. Dies ist aber nicht möglich, da $ax < by$.

Folglich war unsere Annahme falsch und es gilt $p \mid ay - bx$, was wir zeigen wollten. □

2.5.7 Lemma

Ist $m \geq 3$ eine natürliche Zahl, die kein Quadrat ist, und

$$x = \min\left\{k \in \mathbb{N}_{>0} \mid \left(\frac{k}{m}\right) = -1\right\}, \tag{2.3}$$

dann ist x eine Primzahl.

Für jede Primzahl $p \geq 3$ ist somit der zugehörige kleinste positive quadratische Nichtrest $n(p)$ eine Primzahl.

Beweis:

Ist m eine Primzahl, dann ist es klar, daß mindestens ein $k \in \mathbb{N}_{>0}$ existiert mit $\left(\frac{k}{m}\right) = -1$. Mit dem chinesischen Restsatz folgt dies schließlich auch für $m \notin \mathbb{P}$.

Wir nehmen nun an, daß x zusammengesetzt ist. Dann existieren natürliche Zahlen $a, b > 1$ mit $x = a \cdot b$. Daraus erhalten wir

$$-1 = \left(\frac{x}{m}\right) = \left(\frac{a \cdot b}{m}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{b}{m}\right),$$

was bedeutet, daß entweder $\left(\frac{a}{m}\right) = -1$ oder $\left(\frac{b}{m}\right) = -1$ gilt. Dies liefert allerdings einen Widerspruch zu (2.3). Also muß x eine Primzahl sein. □

Beispiele

In Tabelle 2.1 sind für die Primzahlen $3 \leq p < 100$ die kleinsten quadratischen Nichtreste $n^*(p)$ angeführt:

$n^*(3) = 2$	$n^*(13) = 2$	$n^*(29) = 2$	$n^*(43) = 2$	$n^*(61) = 2$	$n^*(79) = 3$
$n^*(5) = 2$	$n^*(17) = 3$	$n^*(31) = 3$	$n^*(47) = 5$	$n^*(67) = 2$	$n^*(83) = 2$
$n^*(7) = 3$	$n^*(19) = 2$	$n^*(37) = 2$	$n^*(53) = 2$	$n^*(71) = 7$	$n^*(89) = 3$
$n^*(11) = 2$	$n^*(23) = 2$	$n^*(41) = 3$	$n^*(59) = 2$	$n^*(73) = 5$	$n^*(97) = 5$

Tabelle 2.1: Kleinste quadratische Nichtreste für $3 \leq p < 100$

Da 2 quadratischer Nichtrest aller Primzahlen der Form $8n \pm 3$ ist, wollen wir in Tabelle 2.2 die kleinsten ungeraden quadratischen Nichtreste für die Primzahlen $3 \leq p < 100$ angeben:

$n(3) = 5$	$n(13) = 5$	$n(29) = 3$	$n(43) = 3$	$n(61) = 7$	$n(79) = 3$
$n(5) = 3$	$n(17) = 3$	$n(31) = 3$	$n(47) = 5$	$n(67) = 3$	$n(83) = 5$
$n(7) = 3$	$n(19) = 3$	$n(37) = 5$	$n(53) = 3$	$n(71) = 7$	$n(89) = 3$
$n(11) = 7$	$n(23) = 5$	$n(41) = 3$	$n(59) = 11$	$n(73) = 5$	$n(97) = 5$

Tabelle 2.2: Kleinste ungerade quadratische Nichtreste für $3 \leq p < 100$

Kapitel 3

Elementare Abschätzungen

Mit den Ergebnissen des vorhergehenden Kapitels können wir nun beginnen, in diesem Kapitel die verschiedenen elementaren Abschätzungen für den kleinsten quadratischen Nichtrest anzugeben. Die unterschiedlichen Ergebnisse nehmen ihren Anfang bei GAUSS, der sich schon im Alter von 18 Jahren damit beschäftigte. Weitere Fortschritte erzielte TRYGVE NAGELL, der zunächst die Aussage von GAUSS verallgemeinerte und fast 30 Jahre später seine Abschätzungen noch zweimal verschärfte. Seine Ergebnisse wurden von L. RÉDEI und BENGT STOLT verfeinert. Kurz und elegant lassen sich die Abschätzung von IVAN NIVEN, HERBERT S. ZUCKERMAN und HUGH L. MONTGOMERY sowie der Satz von SEBASTIAN WEDENIWSKI beweisen. Sehr gute Abschätzungen bieten die drei Sätze von ALFRED BRAUER, die zeitlich sogar vor NAGELL liegen. Auch LARS FJELLSTEDT glaubte eine gute Abschätzung für den kleinsten quadratischen Nichtrest bewiesen zu haben, jedoch stellte sich sein Beweis als fehlerhaft heraus.

Vorbemerkung

In den beiden Ergänzungssätzen zum quadratischen Reziprozitätsgesetz haben wir gesehen, daß man für eine Primzahl $p \geq 3$ in einigen Fällen explizit einen quadratischen Nichtrest angeben kann. Zum Beispiel

$$p \equiv 7 \bmod 8 \overset{2.3.3}{\Longrightarrow} \left(\frac{-1}{p}\right) = -1,$$
$$p \equiv 3,\ 5 \bmod 8 \overset{2.3.4}{\Longrightarrow} \left(\frac{2}{p}\right) = -1.$$

Es bleiben jedoch die Primzahlen $p \equiv 1 \bmod 8$, für die man auf Anhieb keinen quadratischen Nichtrest angeben kann.

3.1 Abschätzung von GAUSS

Als erster hat sich GAUSS mit dem Problem der Primzahlen $p \equiv 1 \bmod 8$ beschäftigt und bewies in den *Disquisitiones arithmeticae* in Art. 129 folgenden Satz zur Abschätzung des kleinsten quadratischen Nichtrestes für eine Primzahl der Form $8n + 1$.

3.1.1 Satz von Gauss

Ist p eine Primzahl der Form $8n+1$, dann existiert mindestens eine ungerade Primzahl q mit

$$q < 2\sqrt{p}+1 \quad \textit{und} \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1.$$

Das heißt, für jede Primzahl $p \equiv 1$ mod 8 gilt

$$n(p) \leq 2\lfloor\sqrt{p}\rfloor + 1.$$

Beweis:

Wir nehmen an, daß alle Primzahlen $q \leq 2\lfloor\sqrt{p}\rfloor + 1$ quadratische Reste modulo p sind, also $\left(\frac{q}{p}\right) = 1$ gilt. Damit wollen wir dann einen Widerspruch herleiten.

Zuerst setzen wir

$$m = \lfloor\sqrt{p}\rfloor.$$

Dann ist $m \geq 1$. Da $p \equiv 1$ mod 8, ist $p \geq 17$ und daher gilt

$$\begin{array}{rrcl} & \sqrt{p} & > & 1+\sqrt{2} \\ \iff & \sqrt{2} & < & \sqrt{p}-1 \\ \iff & 2 & < & p-2\sqrt{p}+1 \\ \iff & 2\sqrt{p}+1 & < & p \\ \implies & 2m+1 & < & p. \end{array}$$

Insgesamt erhält man also

$$1 < 2m+1 < p.$$

Nun setzen wir

$$M = (2m+1)!$$

Für alle ungeraden Primteiler q von M gilt dann $q \leq 2m+1 < p$. Daher ist ggT $(p, M) = 1$. Wegen unserer Voraussetzung gilt nun $\left(\frac{q}{p}\right) = 1$ und da $p \equiv 1$ mod 8, folgt $\left(\frac{p}{q}\right) = 1$. Nach Satz 2.3.1 gibt es also für jedes $n \in \mathbb{N}$ ein $x_{q,n} \in \mathbb{Z}$ mit

$$x_{q,n}^2 \equiv p \bmod q^n.$$

Wegen $p \equiv 1$ mod 8 liefert Satz 2.3.1 für alle $n \in \mathbb{N}$ eine ganze Zahl $x_{2,n}$ mit

$$x_{2,n}^2 \equiv p \bmod 2^n.$$

Mit dem chinesischen Restsatz findet man schließlich ein $x \in \mathbb{Z}$, das die Kongruenz

$$x^2 \equiv p \bmod M$$

erfüllt, wobei wir o.B.d.A. $0 \leq x \leq M-1$ annehmen können. Aus $\mathrm{ggT}(p, M) = 1$ folgt auch $\mathrm{ggT}(x, M) = 1$ und somit $2m+2 \leq x \leq M-1$.

Wir rechnen modulo M und erhalten

$$x\left(p-1^2\right)\left(p-2^2\right)\cdots\left(p-m^2\right) \equiv x\left(x^2-1^2\right)\left(x^2-2^2\right)\cdots\left(x^2-m^2\right) \equiv$$

$$\equiv (x-m)(x-m+1)\cdots(x-1)\,x\,(x+1)\cdots(x+m-1)(x+m) \mod M. \tag{3.1}$$

Mit $x \geq 2m+2$ ergibt sich

$$(x-m)(x-m+1)\cdots(x-2)(x-1)\,x\,(x+1)(x+2)\cdots(x+m-1)(x+m) =$$

$$= \frac{1\cdot 2\cdot \ldots \cdot (x+m)}{1\cdot 2\cdot \ldots \cdot (x-m-1)} = \frac{(x+m)!}{(x-m-1)!} = \frac{(x+m)!}{(x-m-1)!\,(2m+1)!}\cdot(2m+1)! = \binom{x+m}{2m+1}\cdot M.$$

Daraus folgt

$$(x-m)(x-m+1)\cdots(x-2)(x-1)\,x\,(x+1)(x+2)\cdots(x+m-1)(x+m) \equiv 0 \mod M$$

und nach (3.1) auch

$$x\left(p-1^2\right)\left(p-2^2\right)\cdots\left(p-m^2\right) \equiv 0 \mod M.$$

Da $\mathrm{ggT}(x, M) = 1$ war, erhält man

$$\left(p-1^2\right)\left(p-2^2\right)\cdots\left(p-m^2\right) \equiv 0 \mod M$$

und damit

$$M \mid \prod_{i=1}^{m}\left(p-i^2\right).$$

Also ist

$$c := \frac{1}{M}\cdot\prod_{i=1}^{m}\left(p-i^2\right) \in \mathbb{Z}. \tag{3.2}$$

Es gilt

$$\begin{aligned}
M &= (2m+1)! = 1\cdot 2\cdot \ldots \cdot (m-1)\cdot m\cdot (m+1)\cdot (m+2)\cdot (m+3)\cdot \ldots \cdot 2m\cdot (2m+1)\\
&= (m+1)\cdot[m(m+2)]\cdot[(m-1)(m+3)]\cdot \ldots \cdot [2\cdot(2m)]\cdot[1\cdot(2m+1)]\\
&= (m+1)\cdot\left(m^2+2m\right)\cdot\left(m^2+2m-3\right)\cdot \ldots \cdot 4m\cdot(2m+1)\\
&= (m+1)\cdot\left[(m+1)^2-1^2\right]\cdot\left[(m+1)^2-2^2\right]\cdot \ldots \cdot\left[(m+1)^2-(m-1)^2\right]\cdot\left[(m+1)^2-m^2\right]\\
&= (m+1)\cdot\prod_{i=1}^{m}\left[(m+1)^2-i^2\right].
\end{aligned}$$

Man erhält also

$$c = \frac{1}{M}\cdot\prod_{i=1}^{m}\left(p-i^2\right) = \frac{1}{m+1}\cdot\prod_{i=1}^{m}\frac{p-i^2}{(m+1)^2-i^2}$$

Wegen $m = \lfloor\sqrt{p}\rfloor$ gilt für $i \in \{1, 2, \ldots, m\}$ die Ungleichung $i < \sqrt{p}$, also $i^2 < p$ und damit $p - i^2 > 0$. Außerdem gilt natürlich $(m+1)^2 - i^2 > 0$. Aus $m = \lfloor\sqrt{p}\rfloor$ folgt auch $\sqrt{p} < m + 1$ und somit $p < (m+1)^2$. Schließlich erhält man

$$0 < p - i^2 < (m+1)^2 - i^2,$$

was zu

$$0 < \frac{p - i^2}{(m+1)^2 - i^2} < 1$$

führt. Dies bedeutet aber, daß

$$0 < \frac{1}{m+1} \cdot \prod_{i=1}^{m} \frac{p - i^2}{(m+1)^2 - i^2} < 1, \quad \text{also} \quad 0 < c < 1,$$

was jedoch einen Widerspruch zur Aussage $c \in \mathbb{Z}$ aus (3.2) liefert. Demnach muß die zu Beginn gemachte Annahme falsch sein und somit existiert eine ungerade Primzahl q mit

$$q \leq 2\lfloor\sqrt{p}\rfloor + 1 < 2\sqrt{p} + 1 \quad \text{und} \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = -1.$$

□

3.2 Die Abschätzungen von NAGELL

Im Jahre 1923 gelang es TRYGVE NAGELL, die Gültigkeit des Satzes von GAUSS für beliebige Primzahlen nachzuweisen. Sein Beweis ist in die drei Fälle $p \equiv 5 \bmod 8$, $p \equiv 7 \bmod 8$ und $p \equiv 3 \bmod 8$ unterteilt und ist im Gegensatz zum Widerspruchsbeweis von GAUSS vollständig konstruktiv. In den einzelnen Fällen ergeben sich teilweise sogar bessere Schranken als $2\sqrt{p}+1$.

Im ersten Fall benutzt er die eindeutige Darstellung von p als Summe zweier Quadrate, die in 2.5.5 und 2.5.6 bewiesen wurde, um daraus einen quadratischen Nichtrest modulo p zu konstruieren.

Der Beweis der beiden anderen Fälle stützt sich auf die Idee, daß p zwischen zwei Quadratzahlen liegt. Aus der Differenz von Quadratzahl und p, die immer als $\equiv 3 \bmod 4$ gewählt wird, erhält man dann einen Primteiler $q \equiv 3 \bmod 4$. Da auch $p \equiv 3 \bmod 4$ gilt, entpuppt sich q mit dem quadratischen Reziprozitätsgesetz als gewünschter Nichtrest modulo p.

Da die Originalarbeit von NAGELL schwer zugänglich ist, orientiert sich der folgende Beweis an [Köch, S. 31].

3.2.1 Satz von GAUSS-NAGELL

Ist $p > 3$ eine Primzahl, dann existiert mindestens eine ungerade Primzahl $q < 2\sqrt{p} + 1$ mit $\left(\frac{q}{p}\right) = -1$, d.h. für jede Primzahl $p > 3$ gilt

$$n(p) < 2\sqrt{p} + 1.$$

Beweis:

- Für $p \equiv 1 \bmod 8$ gilt die Aussage nach dem Satz von GAUSS.

Es bleiben also noch die Fälle $p \equiv 5 \bmod 8$, $p \equiv 7 \bmod 8$ und $p \equiv 3 \bmod 8$ zu zeigen.

- Sei $p \equiv 5 \bmod 8 \implies p \equiv 1 \bmod 4$.
  Nach 2.5.5 $\exists\, a, b \in \mathbb{N},\ a \neq b$ mit $p = a^2 + b^2$

$$\implies a^2 - b^2 = p - b^2 - b^2 \equiv -2b^2 \bmod p$$

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

  Ist ein Produkt quadratischer Nichtrest modulo p, muß mindestens einer der Faktoren ebenfalls quadratischer Nichtrest sein. Da $a^2 - b^2 = p - 2b^2 \equiv p \equiv 1 \bmod 2$, existiert ein ungerader Primteiler q von $\left|a^2 - b^2\right| \geq 3$ mit

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

  Da $a^2 - b^2 = (a+b)(a-b)$ gilt $q \leq a + b$. Außerdem ist $a + b < \sqrt{2p}$, denn

$$\begin{aligned} a + b &< \sqrt{2\left(a^2 + b^2\right)} = \sqrt{2p} \\ \iff a^2 + 2ab + b^2 &< 2a^2 + 2b^2 \\ \iff 0 &< a^2 - 2ab + b^2 \\ \iff 0 &< (a-b)^2, \end{aligned}$$

  was wegen $a \neq b$ immer erfüllt ist. Man erhält also

$$q \leq a + b < \sqrt{2p}.$$

- Sei $p \equiv 7 \bmod 8$. Es existiert ein $a \in \mathbb{N}$ mit $a^2 < p < (a+1)^2$.
  Es ist

$$0^2 \equiv 4^2 \equiv 0 \bmod 8 \quad \text{und} \quad 2^2 \equiv 6^2 \equiv 4 \bmod 8,$$

  sowie

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8.$$

  Für alle geraden $a \in \mathbb{Z}$ gilt also $a^2 \equiv 0,\ 4 \bmod 8$ und für alle ungeraden a gilt $a^2 \equiv 1 \bmod 8$.
  Fall 1: a gerade
  Mit $a \equiv 0 \bmod 2$ ist $a^2 \equiv 0,\ 4 \bmod 8$ und damit $a^2 \equiv 0 \bmod 4$. Wegen $p \equiv 7 \bmod 8$ ist auch $p \equiv 3 \bmod 4$. Daraus erhält man $p - a^2 \equiv 3 \bmod 4$. Folglich hat die positive ganze Zahl $p - a^2$ einen Primteiler $q \equiv 3 \bmod 4$ für den mit $p = a^2 + qs,\ s \in \mathbb{Z}$ gilt

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

Aus $\sqrt{p} < a+1$ folgt $\left(\sqrt{p}-1\right)^2 < a^2$ und somit gilt

$$q \leq p - a^2 < p - (\sqrt{p}-1)^2 = 2\sqrt{p} - 1.$$

Fall 2: a ungerade
Man hat also

$$\begin{aligned} & a^2 && \equiv && 1 \bmod 8 \\ \Longrightarrow \quad & p - a^2 && \equiv && 7 - 1 \equiv 6 \bmod 8 \\ \Longrightarrow \quad & p - a^2 && = && 8k + 6,\ k \in \mathbb{Z} \\ \Longrightarrow \quad & \frac{1}{2}\left(p - a^2\right) && = && 4k + 3 \\ \Longrightarrow \quad & \frac{1}{2}\left(p - a^2\right) && \equiv && 3 \bmod 4. \end{aligned}$$

Demnach hat $\frac{1}{2}\left(p - a^2\right)$ einen Primteiler $q \equiv 3 \bmod 4$ für den mit $p = a^2 + qs',\ s' \in \mathbb{Z}$ gilt

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

Wie oben folgt aus $\left(\sqrt{p}-1\right)^2 < a^2$

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

- Sei $p \equiv 3 \bmod 8$. Es existiert auch hier ein $a \in \mathbb{N}$ mit $a^2 < p < (a+1)^2$.
  Fall 1: a gerade

$$\begin{aligned} \Longrightarrow \quad & a + 1 && \equiv && 1 \bmod 2 \\ \Longrightarrow \quad & (a+1)^2 && \equiv && 1 \bmod 8 \\ \Longrightarrow \quad & (a+1)^2 - p && \equiv && 1 - 3 \equiv -2 \equiv 6 \bmod 8 \\ \Longrightarrow \quad & \frac{1}{2}\left((a+1)^2 - p\right) && \equiv && 3 \bmod 4. \end{aligned}$$

Folglich gibt es einen Primteiler $q \equiv 3 \bmod 4$ von $\frac{1}{2}\left((a+1)^2 - p\right)$, so daß $p = (a+1)^2 - qt,\ t \in \mathbb{Z}$. Auch hier gilt

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

Da $a^2 < p$, gilt wegen $a^2 \equiv 0,\ 4 \bmod 8$ und $p \equiv 3 \bmod 8$ stets $a^2 + 3 \leq p$ und somit $a \leq \sqrt{p-3}$.
Insgesamt ergibt sich

$$q \leq \frac{1}{2}\left((a+1)^2 - p\right) \leq \frac{1}{2}\left(\left(\sqrt{p-3}+1\right)^2 - p\right) = \sqrt{p-3} - 1 < \sqrt{p},$$

also

$$q < \sqrt{p}.$$

Fall 2: a ungerade

$$\begin{aligned} \Longrightarrow \quad a+2 &\equiv 1 \bmod 2 \\ \Longrightarrow \quad (a+2)^2 &\equiv 1 \bmod 8 \\ \Longrightarrow \quad (a+2)^2 - p &\equiv 1-3 \equiv -2 \equiv 6 \bmod 8 \\ \Longrightarrow \quad \frac{1}{2}\left((a+2)^2 - p\right) &\equiv 3 \bmod 4. \end{aligned}$$

Nun hat $\frac{1}{2}\left((a+2)^2 - p\right)$ einen Primteiler $q \equiv 3 \bmod 4$ mit $p = (a+2)^2 - qt',\ t' \in \mathbb{Z}$ und somit

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

Da $a^2 < p$ und beide Seiten ungerade sind, folgt $a^2 + 2 \leq p$ und damit $a \leq \sqrt{p-2}$. Daraus erhält man

$$q \leq \frac{1}{2}\left((a+2)^2 - p\right) \leq \frac{1}{2}\left(\left(\sqrt{p-2}+2\right)^2 - p\right) = 2\sqrt{p-2} + 1 < 2\sqrt{p} + 1.$$

Also gilt die Aussage für alle Primzahlen $p > 3$. □

Bemerkung und Beispiele

Setzt man in 3.2.1 die Bedingung $q \equiv 3 \bmod 4$, so ist z.B. für die Primzahlen $p = 11,\ 83,\ 227$ der Wert $2\lfloor\sqrt{p}\rfloor + 1 = 7,\ 19, 31$ jeweils tatsächlich die kleinste Primzahl $\equiv 3 \bmod 4$, die quadratischer Nichtrest modulo p ist.

Da die Verfahren im Beweis des Satzes von GAUSS-NAGELL leicht durchzuführen sind, wollen wir in den Tabellen 3.1, 3.2 und 3.3 die verschiedenen Konstruktionen der quadratischen Nichtreste an einigen Beispielen verdeutlichen:

p	$p = a^2 + b^2$		q	$n(p)$	$2\sqrt{p}+1$
61	$61 = 5^2 + 6^2$	$a^2 - b^2 = -11$	11	7	16,6
349	$349 = 5^2 + 18^2$	$a^2 - b^2 = -13 \cdot 23$	13	7	38,4
1381	$1381 = 15^2 + 34^2$	$a^2 - b^2 = -19 \cdot 49$	19	11	75,3

Tabelle 3.1: Nichtrest-Konstruktion von NAGELL für $p \equiv 5 \bmod 8$

p	$a^2 < p < (a+1)^2$		q	$n(p)$	$2\sqrt{p}+1$
79	$8^2 < 79 < 9^2$	$p - a^2 = 15 = 3 \cdot 5$	3	3	18,8
599	$24^2 < 599 < 25^2$	$p - a^2 = 23$	23	7	49,9
1559	$39^2 < 1559 < 40^2$	$\frac{1}{2}(p - a^2) = 19$	19	17	79,9

Tabelle 3.2: Nichtrest-Konstruktion von NAGELL für $p \equiv 7 \bmod 8$

p	$a^2 < p < (a+1)^2$		q	$n(p)$	$2\sqrt{p}+1$
43	$6^2 < 43 < 7^2$	$\frac{1}{2}\left((a+1)^2 - p\right) = 3$	3	3	14,1
467	$21^2 < 467 < 22^2$	$\frac{1}{2}\left((a+2)^2 - p\right) = 31$	31	5	44,2
1811	$42^2 < 1811 < 43^2$	$\frac{1}{2}\left((a+1)^2 - p\right) = 19$	19	19	86,1

Tabelle 3.3: Nichtrest-Konstruktion von NAGELL für $p \equiv 3 \bmod 8$

Man findet also recht einfach quadratische Nichtreste modulo p, aber nicht immer sehr kleine quadratische Nichtreste.

3.2.2 Die Verschärfungen von NAGELL I

Anfang der fünfziger Jahre veröffentlichte TRYGVE NAGELL in der skandinavischen Fachzeitschrift *Arkiv för Matematik* kurz hintereinander drei Arbeiten, in denen er teilweise verbesserte Abschätzungen für $n(p)$ darstellte. So verschärfte er 1950 die Abschätzungen für jede Restklasse modulo 8. Nur für die Primzahlen $p \equiv 3 \bmod 8$ konnte das Ergebnis $n(p) < 2\sqrt{p}+1$ von 1923 nicht verbessert werden.

Satz

1. *Ist p eine Primzahl der Form $8n+1$, dann gilt $n(p) < \sqrt{p}$.*
2. *Ist p eine Primzahl der Form $8n+5$, dann gilt $n(p) < \sqrt{2p}$.*
3. *Ist $p > 7$ eine Primzahl der Form $8n-1$, dann gilt $n(p) < \sqrt{2p} - 1$.*
4. *Ist $p > 3$ eine Primzahl der Form $8n+3$, dann existiert eine Primzahl $q \equiv 3$ mod 4, $q < 2\sqrt{p}+1$, so daß $\left(\frac{q}{p}\right) = -1$. Das heißt $n(p) < 2\sqrt{p}+1$.*

Für den Beweis benötigen wir die folgenden Lemmata, deren Beweis man in [Nag1] findet.

Lemma 1

Sei p eine Primzahl. Ist $a \in \mathbb{Z}$, mit $ggT(a,p) = 1$, dann gibt es zwei ganze positive Zahlen $x < \sqrt{p}$ und $y < \sqrt{p}$ mit

$$a \cdot y \equiv \pm x \bmod p$$

für eines der beiden Vorzeichen.

Lemma 2

Ist p eine Primzahl der Form $12t-1$, dann gibt es zwei ganze positive Zahlen u und v, so daß

$$p = 3 \cdot v^2 - u^2$$

mit

$$u < \sqrt{\frac{1}{2} \cdot p}, \qquad v < \sqrt{\frac{1}{2} \cdot p}$$

gilt.

Beweis des Satzes:

1. Sei a ein quadratischer Nichtrest modulo p. Dann gibt es nach Lemma 1 zwei ganze Zahlen x und y, so daß
$$a \cdot y \equiv \pm x \bmod p$$
mit $0 < x < \sqrt{p}$, $0 < y < \sqrt{p}$ und $\mathrm{ggT}(x,y) = 1$. Außerdem ist $\left(\frac{-1}{p}\right) = 1$, da $p \equiv 1 \bmod 4$. Damit ist
$$\left(\frac{x}{p}\right) = \left(\frac{\pm x}{p}\right) = \left(\frac{a \cdot y}{p}\right) = \underbrace{\left(\frac{a}{p}\right)}_{=-1} \cdot \left(\frac{y}{p}\right) = -\left(\frac{y}{p}\right).$$
Da $\left(\frac{x}{p}\right)$ bzw. $\left(\frac{y}{p}\right)$ nur die Werte -1, 1 annehmen kann, ist entweder x oder y ein quadratischer Nichtrest modulo p. Somit besitzt eine der beiden Zahlen einen Primteiler q, der ebenfalls quadratischer Nichtrest ist. Da $q < \sqrt{p}$, haben wir die Behauptung bewiesen.

2. Wurde bereits in 3.2.1 bewiesen.

3. Da $p \equiv -1 \bmod 8$, ist $p \equiv -1,\ 7 \bmod 24$. Für $p \equiv 7 \bmod 24$ gilt
$$\left(\frac{3}{p}\right) \overset{p \equiv 3 \bmod 4}{=} -\left(\frac{p}{3}\right) \overset{p \equiv 1 \bmod 3}{=} -\left(\frac{1}{3}\right) = -1,$$
also ist für diese Primzahlen 3 ein quadratischer Nichtrest. Daher genügt es, die Aussage für $p \equiv -1 \bmod 24$ zu zeigen. Nach Lemma 2 gibt es positive ganze Zahlen u und v, $u < \sqrt{\frac{1}{2} \cdot p}$, $v < \sqrt{\frac{1}{2} \cdot p}$, so daß
$$p = 3 \cdot v^2 - u^2.$$
Aus
$$3 \cdot \left(v^2 - u^2\right) = p - 2 \cdot u^2 > p - 2 \cdot \sqrt{\frac{1}{2} \cdot p} = 0$$

folgt $v^2 - u^2 > 0$ und, da u, v positiv sind, auch $v > u$.
Außerdem gilt

$$\left(\frac{p - 2 \cdot u^2}{p}\right) = \left(\frac{-2}{p}\right) = \underbrace{\left(\frac{-1}{p}\right)}_{=-1} \cdot \underbrace{\left(\frac{2}{p}\right)}_{=-1} = -1$$

und damit

$$-1 = \left(\frac{3 \cdot \left(v^2 - u^2\right)}{p}\right) = \left(\frac{v^2 - u^2}{p}\right),$$

da

$$\left(\frac{3}{p}\right) \overset{p \equiv 3 \bmod 4}{=} -\left(\frac{p}{3}\right) \overset{p \equiv 2 \bmod 3}{=} -\left(\frac{2}{3}\right) = 1.$$

Somit ist $v^2 - u^2$ ein quadratischer Nichtrest modulo p, der mindestens einen Primteiler q besitzt, der ebenfalls quadratischer Nichtrest ist. Für q gilt die Ungleichung

$$q \leq v + u \leq \left\lfloor \sqrt{\frac{1}{2} \cdot p} \right\rfloor + \left\lfloor \sqrt{\frac{1}{2} \cdot p} \right\rfloor - 1 < \sqrt{2p} - 1,$$

was wir beweisen wollten.

4. Wurde bereits in 3.2.1 bewiesen. □

3.2.3 Die Verschärfungen von NAGELL II

Für die Fälle $p \equiv 1 \bmod 8$ und $p \equiv 7 \bmod 8$ konnte NAGELL im Jahre 1951 die ein Jahr vorher veröffentlichten Abschätzungen nochmals verbessern.

Wir wollen jedoch zunächst folgendes Lemma beweisen, das wir im folgenden benötigen werden.

Lemma

Für alle Primzahlen $p > 3$ gilt $n(p) < p$.

Beweis:

Wir nehmen an, es gäbe eine Primzahl p mit $n(p) \geq p > 3$ und führen diese Aussage zum Widerspruch. Teilt man nun $n(p)$ durch p, so findet man $k, r \in \mathbb{N}$, so daß

$$n(p) = k \cdot p + r$$

gilt, mit $0 < r < p < n(p)$. Somit wäre

$$\left(\frac{r}{p}\right) = \left(\frac{n(p) - k \cdot p}{p}\right) = \left(\frac{n(p)}{p}\right) = -1.$$

Da $r < n(p)$, kann r keine ungerade Primzahl sein und es muß daher

$$r = 2^m \cdot u$$

mit ungeraden Zahlen $m, u \in \mathbb{N}$ gelten. Dabei muß $\left(\frac{2}{p}\right) = -1$ sein und u darf nur Primteiler besitzen, die quadratische Reste modulo p sind.

Nun betrachten wir die Zahlen

$$n(p) - 2 = k \cdot p + (r-2) \quad \text{und} \quad (r-2) = 2 \cdot \left(2^{m-1} \cdot u - 1\right).$$

Angenommen es würde $m > 1$ gelten, dann wäre $2^{m-1} \cdot u - 1 < n(p)$ ungerade und damit ein quadratischer Rest modulo p. Da $\left(\frac{2}{p}\right) = -1$ gelten muß, würde

$$\left(\frac{r-2}{p}\right) = \left(\frac{2 \cdot \left(2^{m-1} \cdot u - 1\right)}{p}\right) = -1$$

gelten, also wäre $r-2$ ein Nichtrest. Andererseits ist aber

$$\left(\frac{r-2}{p}\right) = \left(\frac{n(p) - 2 - k \cdot p}{p}\right) = \left(\frac{n(p)-2}{p}\right) = 1,$$

was einen Widerspruch liefert.

Also muß $m = 1$ und damit $r = 2 \cdot u$ sein. Damit wären

$$u - 2 < n(p) \quad \text{und} \quad n(p) - 4 = k \cdot p + 2 \cdot (u-2) < n(p)$$

ungerade und quadratische Reste modulo p. Mit $\left(\frac{2}{p}\right) = -1$ erhält man jedoch

$$\left(\frac{n(p)-4}{p}\right) = \left(\frac{2 \cdot (u-2)}{p}\right) = -1$$

und damit einen Widerspruch. Daher ist die zu Beginn gemachte Annahme falsch und die Behauptung bewiesen. □

Satz

1. *Ist p eine Primzahl der Form $8n+1$, dann gilt $n(p) \leq \sqrt{\frac{1}{2} \cdot (p+1)}$.*
2. *Ist p eine Primzahl der Form $8n+7$ mit $p \neq 7,\ 23$, dann gilt $n(p) \leq \sqrt{p-6}$.*

Beweis:

1. Zunächst dividieren wir p durch $2 \cdot n(p)$ und erhalten

   $$p = 2 \cdot n(p) \cdot k \pm s,$$

   mit $s \in \mathbb{Z}$, $0 \leq s \leq n(p) - 2$. Nach dem vorherigen Lemma gilt $n(p) < p$ und damit $k \geq 1$. Es ist s ein quadratischer Rest modulo p und mit $\left(\frac{-1}{p}\right) = 1$ ist

   $$1 = \left(\frac{s}{p}\right) = \left(\frac{p \pm s}{p}\right) = \underbrace{\left(\frac{2}{p}\right)}_{=1} \cdot \left(\frac{n(p)}{p}\right) \cdot \left(\frac{k}{p}\right) = -1 \cdot \left(\frac{k}{p}\right).$$

Somit ist k quadratischer Nichtrest, also $k \geq n(p)$, und damit erhält man die Ungleichung

$$p \geq 2 \cdot n(p)^2 - n(p) + 2.$$

Daraus ergibt sich

$$n(p) \leq \frac{1}{4} + \frac{1}{4} \cdot \sqrt{8p - 15}.$$

Wir wollen jedoch dieses Ergebnis noch verbessern und

$$n(p) \leq \sqrt{\frac{1}{2} \cdot (p+1)}$$

zeigen. Da $n(17) = 3$, gilt diese Ungleichung für $p = 17$ und damit für alle Primzahlen $p > 17$, für die $n(p) = 3$ ist. Daher können wir $n(p) \geq 5$ voraussetzen.
Wir setzen

$$p = 2 \cdot n(p)^2 - n(p) + 2 + 2 \cdot a, \tag{3.3}$$

wobei $a \in \mathbb{Z}$, $a \geq 0$ gilt. Durch Umformen erhalten wir

$$\begin{aligned} p - (2 \cdot a + 3) \cdot n(p) &= 2 \cdot n(p)^2 - 4 \cdot n(p) - 2 \cdot a \cdot n(p) + 2 + 2 \cdot a \\ &= 2 \cdot (n(p) - 1) \cdot (n(p) - 1 - a). \end{aligned}$$

Angenommen, es gilt $a \leq \frac{1}{2} \cdot (n(p) - 5)$, dann ist $2 \cdot a + 3 \leq n(p) - 2$. Also ist $2 \cdot a + 3$ ein quadratischer Rest und $(2 \cdot a + 3) \cdot n(p)$ ein quadratischer Nichtrest modulo p. Damit und mit $\left(\frac{-1}{p}\right) = 1$ erhält man

$$\begin{aligned} -1 &= \left(\frac{(2 \cdot a + 3) \cdot n(p)}{p}\right) = \left(\frac{p - (2 \cdot a + 3) \cdot n(p)}{p}\right) \\ &= \underbrace{\left(\frac{2}{p}\right)}_{=1} \cdot \underbrace{\left(\frac{n(p) - 1}{p}\right)}_{=1} \cdot \underbrace{\left(\frac{n(p) - 1 - a}{p}\right)}_{=1} \\ &= 1, \end{aligned}$$

was jedoch einen Widerspruch liefert. Daher muß $a \geq \frac{1}{2} \cdot (n(p) - 3)$ gelten. Damit erhält man aus (3.3)

$$\begin{aligned} p &\geq 2 \cdot n(p)^2 - n(p) + 2 + n(p) - 3 \\ &= 2 \cdot n(p)^2 - 1 \end{aligned}$$

und schließlich die gewünschte Ungleichung

$$n(p) \leq \sqrt{\frac{1}{2} \cdot (p+1)}.$$

2. Wir teilen p durch $n(p)$ und erhalten

$$p = n(p) \cdot k - r,$$

wobei $r \in \mathbb{Z}$, $0 \leq r \leq n(p) - 1$. Somit ist r ein quadratischer Rest modulo p. Wegen des vorherigen Lemmas gilt wieder $k \geq 1$. Damit ergibt sich

$$1 = \left(\frac{r}{p}\right) = \left(\frac{p+r}{p}\right) = \left(\frac{n(p)}{p}\right) \cdot \left(\frac{k}{p}\right) = -1 \cdot \left(\frac{k}{p}\right),$$

also muß k ein quadratischer Nichtrest sein, d.h. es gilt $k \geq n(p)$. Somit ist

$$p \geq n(p)^2 - n(p) + 1$$

und man erhält

$$n(p) \leq \frac{1}{2} + \frac{1}{2} \cdot \sqrt{4p - 3}.$$

Wir setzen nun $p > 23$ voraus und wollen das Egebnis verbessern. Wir setzen

$$p = n(p)^2 - n(p) + 1 + a, \tag{3.4}$$

wobei $a \geq 0$. Dann ist

$$\begin{aligned} p - (a+3) &= n(p)^2 - n(p) - 2 \\ &= (n(p) + 1) \cdot (n(p) - 2) \\ &= 2 \cdot \frac{1}{2} \cdot (n(p) + 1) \cdot (n(p) - 2) \end{aligned}$$

Wegen $\frac{1}{2} \cdot (n(p) + 1) < n(p)$ und $(n(p) - 2) < n(p)$, sind diese Zahlen quadratische Reste modulo p und man erhält

$$\begin{aligned} \left(\frac{p-(a+3)}{p}\right) &= \underbrace{\left(\frac{-1}{p}\right)}_{=-1} \cdot \left(\frac{a+3}{p}\right) \\ &= \underbrace{\left(\frac{2}{p}\right)}_{=1} \cdot \underbrace{\left(\frac{\frac{1}{2} \cdot (n(p)+1)}{p}\right)}_{=1} \cdot \underbrace{\left(\frac{n(p)-2}{p}\right)}_{=1} = 1, \end{aligned} \tag{3.5}$$

also muß $\left(\frac{a+3}{p}\right) = -1$ und damit $a + 3$ ein quadratischer Nichtrest modulo p sein. Dann ist $a + 3 \geq n(p)$ und mit (3.4) folgt

$$\begin{aligned} p &\geq n(p)^2 - n(p) + 1 + n(p) - 3 \\ \iff p &\geq n(p)^2 - 2. \end{aligned}$$

Nun setzen wir

$$p = n(p)^2 - 2 + b \tag{3.6}$$

und unterscheiden zwei Fälle.
Ist $b > 0$, dann ist

$$\begin{aligned} p - (b-1) &= n(p)^2 - 1 \\ &= (n(p) + 1) \cdot (n(p) - 1) \\ &= 2 \cdot \frac{1}{2} \cdot (n(p) + 1) \cdot (n(p) - 1). \end{aligned}$$

Da $\frac{1}{2}\cdot(n(p)+1) < n(p)$ und $(n(p)-1) < n(p)$, sind diese Zahlen wieder quadratische Reste und wie in (3.5) ergibt sich, daß $b-1$ ein quadratischer Nichtrest modulo p ist. Also folgt mit $b-1 \geq n(p)$ und (3.6)

$$\begin{aligned} & p \geq n(p)^2 - 2 + n(p) + 1 \\ \Longleftrightarrow\ & p \geq n(p)^2 + n(p) - 1. \end{aligned} \tag{3.7}$$

Für $b = 0$ erhalten wir

$$\begin{aligned} p-7 &= n(p)^2 - 9 \\ &= (n(p)+3)\cdot(n(p)-3). \end{aligned} \tag{3.8}$$

Wegen $\frac{1}{2}\cdot(n(p)+3) < n(p)$ ist diese Zahl und damit auch die rechte Seite von (3.7) ein quadratischer Rest modulo p. Aus

$$\left(\frac{p-7}{p}\right) = \underbrace{\left(\frac{-1}{p}\right)}_{=-1}\cdot\left(\frac{7}{p}\right) = \left(\frac{[n(p)+3]\cdot[n(p)-3]}{p}\right) = 1$$

folgt, daß 7 quadratischer Nichtrest modulo p ist, also $n(p) \leq 7$. Aus (3.6) folgt damit $p = n(p)^2 - 2 \leq 47$. Da $n(47) = 5$, gilt die Gleichung (3.8) nur für die Primzahlen $p = 7$ und $p = 23$.
Somit erhält man aus (3.7), daß für alle Primzahlen $p \equiv -1 \bmod 8$, $p \neq 7,\ 23$ gilt

$$n(p) \leq -\frac{1}{2} + \frac{1}{2}\cdot\sqrt{4p+5}.$$

Für $p \geq 55$ gilt die Ungleichung $-\frac{1}{2} + \frac{1}{2}\cdot\sqrt{4p+5} \leq \sqrt{p-6}$ und damit die Behauptung. Für $p = 31,\ 47$ ist

$$\begin{aligned} n(31) &= 3 \leq \sqrt{25} \\ n(47) &= 5 \leq \sqrt{41} \end{aligned}$$

und damit haben wir die Behauptung bewiesen. □

In seiner Arbeit bemerkt NAGELL, daß man mit ähnlichen Methoden auch die beiden folgenden Aussagen beweisen kann, einen konkreten Beweis gibt er jedoch nicht an:

Ist p eine Primzahl mit $p \equiv 5$ mod 8, dann gilt $n(p) < \sqrt{p}$, außer für $p = 5,\ 13,\ 109$.

Ist p eine Primzahl mit $p \equiv 3$ mod 8, dann gilt $n(p) < \sqrt{p} + 4$, außer für $p = 131$.

3.3 Satz von RÉDEI

Auf NAGELLS Arbeit aufbauend veröffentlichte L. RÉDEI im Jahre 1953 in der Zeitschrift *Acta Scientiarum Mathematicarum* einen Artikel, in dem er die Abschätzungen von NAGELL leicht verschärfte.

Satz

Für jede ungerade Primzahl

$$p \neq 3, 5, 7, 11, 13, 23, 59, 109, 131 \tag{3.9}$$

gibt es eine ungerade Primzahl $q < \sqrt{p}$ *mit* $\left(\frac{q}{p}\right) = -1$.

Beweis:

Da die Aussage für die Primzahlen $p \equiv 1 \bmod 8$ schon von NAGELL bewiesen wurde, geben wir nur den Beweis für die Primzahlen $p \equiv 3,\ 5,\ 7 \bmod 8$ an.

Daß die Zahlen in (3.9) wirklich Ausnahmefälle sind, zeigt uns Tabelle 3.4.

p	q	$\lfloor\sqrt{p}\rfloor$
3	5	1
5	3	2
7	3	2
11	7	3
13	5	3
23	5	4
59	11	7
109	11	10
131	17	11

Tabelle 3.4: Primzahlausnahmen von RÉDEI

Im folgenden nehmen wir schon an, daß (3.9) gilt.

Sei nun e die größte ganze Zahl $< \sqrt{p}$. Da $\sqrt{p} \notin \mathbb{Z}$, gilt einerseits $e = \lfloor\sqrt{p}\rfloor$, andererseits auch $e < \sqrt{p} < e + 1$, also $e^2 < p < (e+1)^2$. Daraus folgt $0 < p - e^2 < 2 \cdot e + 1$. Aus der rechten Ungleichung erhalten wir $p - e^2 \leq 2 \cdot e$. Für $p - e^2 = 2 \cdot e$ ist $p = e \cdot (e + 2)$, was jedoch nur für $e = 1$, also $p = 3$ möglich ist. Da dieser Fall aber in (3.9) ausgeschlossen wird, muß $p - e^2 < 2 \cdot e$ gelten. Daraus ergibt sich also insgesamt

$$0 < p - e^2 < 2 \cdot e. \tag{3.10}$$

Wegen (3.9) ist

$$e \geq 4. \tag{3.11}$$

Nun genügt es zu zeigen, daß sich unter den ungeraden Zahlen

$$1,\ 3,\ 5, \ldots,\ (\leq e) \tag{3.12}$$

ein quadratischer Nichtrest mod p befindet, da dieser dann mindestens einen ungeraden Primteiler besitzt, der ebenfalls quadratischer Nichtrest mod p ist.

Dazu nehmen wir nun an, daß alle Zahlen in (3.12) quadratische Reste mod p sind und führen diese Annahme dann in jedem der Fälle $p \equiv 3,\ 5,\ 7 \bmod 8$ zu einem Widerspruch.

Fall 1 : $p \equiv 7 \bmod 8$

Wir bezeichnen mit P, Q zwei Zahlen, die gleich einem Produkt von je zwei Zahlen aus

$$1,\ 2, \ldots,\ e$$

sind. Es genügt zu zeigen, daß ein Paar P, Q mit $P+Q = p$ existiert, denn wegen $\left(\frac{-1}{p}\right) = -1$ gilt dann

$$\left(\frac{P}{p}\right) = \left(\frac{p-Q}{p}\right) = \left(\frac{-Q}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{Q}{p}\right) = -\left(\frac{Q}{p}\right).$$

Also ist entweder $\left(\frac{P}{p}\right) = -1$ oder $\left(\frac{Q}{p}\right) = -1$. Wir nehmen o.B.d.A. $\left(\frac{P}{p}\right) = -1$ an. Ist nun P ungerade, hat P mindestens einen ungeraden Primteiler, der quadratischer Nichtrest mod p ist und wir sind fertig. Ist P gerade, dann ist

$$\left(\frac{P}{p}\right) = \left(\frac{2^k \cdot u}{p}\right) = \left(\frac{2^k}{p}\right) \cdot \left(\frac{u}{p}\right) = -1$$

mit $k \geq 1$ und $u \leq e$, u ungerade. Wegen $\left(\frac{2}{p}\right) = 1$ folgt $\left(\frac{u}{p}\right) = -1$ und wir haben unter den Zahlen in (3.12) einen quadratischen Nichtrest gefunden, was uns den gewünschten Widerspruch liefert.

Wir unterscheiden nun die folgenden Fälle:

Fall $2 \nmid e$:

Wegen (3.10) ist $\frac{\left(p-e^2\right)}{2} < e$ und daher erfüllen

$$P = e^2 \quad \text{und} \quad Q = 2 \cdot \frac{p-e^2}{2}$$

die oben genannten Bedingungen.

Für den Fall $2 \mid e$ gilt $e \geq 8$. Denn sonst wäre wegen (3.11) entweder $e = 4$ und damit $p = 23$, was aber wegen (3.9) nicht sein kann, oder $e = 6$ und $p = 47$, wobei aber $\left(\frac{5}{47}\right) = -1$ einen Widerspruch zur Annahme liefert.

Ist $e \equiv 0 \bmod 2$, dann gilt

$$\begin{aligned} p - (e-1)\cdot(e-3) &= p - \left(e^2 - 4e + 3\right) \equiv 4 + e^2 - 4 \\ &\equiv 0 \bmod 4. \end{aligned} \tag{3.13}$$

Wir unterscheiden nun zwei weitere Fälle.

Fall $2 \mid e,\ 8 \mid p-(e-1)\cdot(e-3)$:

Ein geeignetes Paar ist

$$P = (e-1)\cdot(e-3) \quad \text{und} \quad Q = 8\cdot\frac{p-P}{8},$$

da der Faktor $\dfrac{p-P}{8}$ ganz ist und wegen (3.10)

$$\frac{p-(e-1)\cdot(e-3)}{8} = \frac{p-e^2+4e-3}{8} < \frac{6e-3}{8} < e$$

gilt.

Fall $2 \mid e$, $8 \nmid p-(e-1)\cdot(e-3)$:

Wegen $p-(e-1)\cdot(e-3) \not\equiv 0 \bmod 8$ und (3.13) ist $p-(e-1)\cdot(e-3) \equiv 4 \bmod 8$ und man erhält

$$\begin{aligned} p-(e-3)\cdot(e-5) &= p-(e-1)\cdot(e-3)-\underbrace{4\cdot(e-3)}_{\equiv 4 \bmod 8} \\ &\equiv 0 \bmod 8. \end{aligned}$$

Gilt nun sogar

$$16 \mid p-(e-3)\cdot(e-5)\,, \tag{3.14}$$

dann ist

$$P = (e-3)\cdot(e-5) \quad \text{und} \quad Q = 16\cdot\frac{p-P}{16}$$

ein passendes Paar, da nach (3.10) der letzte Faktor $< \dfrac{10e-15}{16} < e$ ist.

Ist die Bedingung (3.14) falsch, dann gilt wegen $p-(e-3)\cdot(e-5) \equiv 0 \bmod 8$ die Kongruenz $p-(e-3)\cdot(e-5) \equiv 8 \bmod 16$ und damit

$$\begin{aligned} p-(e-1)\cdot(e-7) &= p-(e-3)\cdot(e-5)+8 \\ &\equiv 0 \bmod 16. \end{aligned}$$

Damit genügt das Paar

$$P = (e-1)\cdot(e-7) \quad \text{und} \quad Q = 16\cdot\frac{p-P}{16}$$

den Anforderungen, da der letzte Faktor wie oben $< e$ ist.

Fall 2 : $p \equiv 3 \bmod 8$

In diesem Falle wollen wir eine ungerade ganze Zahl N mit $0 < N \le e$ finden, für die $\left(\dfrac{N}{p}\right) = -1$ gilt. Dafür werden wir N in der Form

$$N = \frac{u\cdot v-p}{2^{2k+1}\cdot 3^l} \quad \text{oder} \quad N = \frac{p-u\cdot v}{2^{2k+2}\cdot 3^l}$$

angeben, wobei $k,\ l = 0,\ 1$ und $u,\ v = 1,\ 3,\ 5, \ldots$ gelten soll. Da $p \equiv 3 \bmod 8$, haben wir $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = -1$ und nach unserer Annahme, daß alle Zahlen in (3.12) quadratische Reste sind, gilt $\left(\frac{3}{p}\right) = 1$. Dann ist

$$\left(\frac{2^{2k+1} \cdot 3^l}{p}\right) = \left(\frac{2}{p}\right)^{2k+1} \cdot \left(\frac{3}{p}\right)^l = -1 \tag{3.15}$$

und

$$\left(\frac{2^{2k+2} \cdot 3^l}{p}\right) = \left(\frac{2}{p}\right)^{2k+2} \cdot \left(\frac{3}{p}\right)^l = 1. \tag{3.16}$$

Außerdem schränken wir $u,\ v$ durch

$$\left(\frac{u}{p}\right) = \left(\frac{v}{p}\right) \tag{3.17}$$

ein, indem wir für

$$u = v \quad \text{oder} \quad u,\ v \le e \quad \text{oder} \quad u \le e,\ v \le 3e,\ 3 \mid v$$

sorgen. In den letzteren beiden Fällen gilt dann wegen unserer Annahme sogar $\left(\frac{u}{p}\right) = \left(\frac{v}{p}\right) = 1$. Mit (3.15), (3.16) und (3.17) erhalten wir dann

$$\begin{aligned} -\left(\frac{\frac{u\cdot v-p}{2^{2k+1}\cdot 3^l}}{p}\right) &= \left(\frac{2^{2k+1}\cdot 3^l}{p}\right)\cdot\left(\frac{\frac{u\cdot v-p}{2^{2k+1}\cdot 3^l}}{p}\right) = \left(\frac{2^{2k+1}\cdot 3^l\cdot\frac{u\cdot v-p}{2^{2k+1}\cdot 3^l}}{p}\right) \\ &= \left(\frac{u\cdot v-p}{p}\right) = \left(\frac{u\cdot v}{p}\right) = \left(\frac{u}{p}\right)\cdot\left(\frac{v}{p}\right) = 1, \end{aligned}$$

woraus

$$\left(\frac{\frac{u\cdot v-p}{2^{2k+1}\cdot 3^l}}{p}\right) = -1$$

folgt. Außerdem gilt auch

$$\begin{aligned} \left(\frac{\frac{p-u\cdot v}{2^{2k+2}\cdot 3^l}}{p}\right) &= \left(\frac{2^{2k+2}\cdot 3^l}{p}\right)\cdot\left(\frac{\frac{p-u\cdot v}{2^{2k+2}\cdot 3^l}}{p}\right) = \left(\frac{2^{2k+2}\cdot 3^l\cdot\frac{p-u\cdot v}{2^{2k+2}\cdot 3^l}}{p}\right) \\ &= \left(\frac{p-u\cdot v}{p}\right) = \left(\frac{-u\cdot v}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{u}{p}\right)\cdot\left(\frac{v}{p}\right) = -1. \end{aligned}$$

Somit gilt für die gewählte Darstellung von N in jedem Fall $\left(\frac{N}{p}\right) = -1$. Wir unterscheiden nun mehrere Fälle.

Fall $2 \mid e$:

Wir wählen

$$N = \frac{(e+1)^2 - p}{2},$$

also $u = v = e + 1$. Offensichtlich ist $N \in \mathbb{Z}$ und $N > 0$. Wegen (3.10) gilt außerdem

$$N = \frac{1}{2}\left(e^2 + 2 \cdot e + 1 - p\right) < \frac{1}{2}\left(2 \cdot e + 1\right) = e + \frac{1}{2},$$

also $N \leq e$ und damit sind alle Bedingungen an N erfüllt.

Fall $4 \mid e - 1$:

Für $u = e$ und $v = e - 2$ betrachten wir

$$N = \frac{p - e \cdot (e - 2)}{4}.$$

Mit (3.10) ist

$$N = \frac{1}{4}\left(p - e^2 + 2 \cdot e\right) > \frac{e}{2} > 0 \quad \text{und} \quad N = \frac{1}{4}\left(p - e^2 + 2 \cdot e\right) < \frac{1}{4} \cdot 4 \cdot e = e,$$

womit wieder alle an N gestellten Forderungen erfüllt sind.

Es bleibt noch der Fall $4 \mid e + 1$, den wir in weitere Fälle untergliedern werden.

Fall $4 \mid e + 1,\ 3 \mid e$:

Wir nehmen zunächst

$$e > 18 \tag{3.18}$$

an und betrachten die Zahlen

$$a = \frac{e \cdot (e + 6) - p}{8} \quad \text{und} \quad b = \frac{(e - 6) \cdot (e + 12) - p}{8}.$$

Es ist

$$a = b + 9.$$

Die Zahlen $a,\ b$ sind ganz, denn aus $e + 1 = 4 \cdot k$, also $e = 4 \cdot k - 1$ folgt

$$\begin{aligned} e \cdot (e + 6) - p &= (4 \cdot k - 1) \cdot (4 \cdot k + 5) - p = 16 \cdot k^2 + 16 \cdot k - 5 - p \\ &\equiv 3 - p \equiv 0 \bmod 8 \end{aligned}$$

und damit $a \in \mathbb{Z}$. Aus $a = b + 9$ folgt schließlich auch $b \in \mathbb{Z}$. Außerdem ergibt sich aus $a = b + 9$, daß eine der beiden Zahlen ungerade ist. Zudem liegen beide zwischen 0 und e, denn aus (3.10) und (3.18) folgt

$$a > b = \frac{1}{8}\left(e^2 + 6 \cdot e - 72 - p\right) > \frac{1}{8}\left(4 \cdot e - 72\right) > 0$$

und

$$b < a = \frac{1}{8}\left(e^2 + 6 \cdot e - p\right) < \frac{6 \cdot e}{8} < e.$$

Somit ist a oder b eine passende Zahl N.

Gilt (3.18) nicht, dann kommt wegen $e \geq 4$ nur $e = 15$ und damit $p = 227$ und $p = 251$ in Betracht. Wegen $\left(\frac{5}{227}\right) = -1$ und $\left(\frac{11}{251}\right) = -1$ scheiden diese Fälle jedoch auch aus.

Fall $4 \mid e+1,\ 3 \mid e-1$:

Diesmal nehmen wir

$$e > 40 \tag{3.19}$$

an. Wir betrachten die vier Zahlen

$$a = \frac{p-(e-4)\cdot(e+2)}{16}, \qquad b = \frac{p-(e-12)\cdot(e+2)}{16},$$
$$c = \frac{p-(e-22)\cdot(e+20)}{16}, \qquad d = \frac{p-(e-16)\cdot(e+14)}{16}$$

mit

$$b = a + \frac{e+1}{2} + \frac{1}{2}, \quad c = a + 27, \quad d = a + 13 + \frac{1}{2}.$$

Es ist wieder $e = 4\cdot k - 1$ und damit

$$\begin{aligned} p-(e-4)\cdot(e+2) &= p-(4\cdot k-5)\cdot(4\cdot k+1) = p-16\cdot k^2+16\cdot k+5 \\ &\equiv p+5 \equiv 3+5 \equiv 0 \bmod 8. \end{aligned}$$

Somit ist der Zähler von a durch 8 teilbar, also $a \in \frac{1}{2}\mathbb{Z}$, was bedeutet, daß a entweder ganzzahlig ist, oder den Nenner 2 hat.

Für $a \in \mathbb{Z}$ gilt auch $c \in \mathbb{Z}$ und $c \equiv a+1 \bmod 2$, weshalb eine der beiden Zahlen a oder c ungerade und ganzzahlig sein muß.

Ist $a \notin \mathbb{Z}$, dann hat a den Nenner 2 und wegen $\frac{e+1}{2} \in \mathbb{Z}$ folgt daraus $b, d \in \mathbb{Z}$. Da $d - b = 13 - 2\cdot k \equiv 1 \bmod 2$, muß entweder b oder d ungerade und ganzzahlig sein.

Die kleinste dieser Zahlen ist a, die größte ist b oder c. Nach (3.10) und (3.19) gilt

$$\begin{aligned} a &= \frac{1}{16}\left(p-e^2+2\cdot e+8\right) > \frac{1}{16}\left(2\cdot e+8\right) > 0, \\ b &= \frac{1}{16}\left(p-e^2+10\cdot e+24\right) < \frac{1}{16}\left(12\cdot e+24\right) < e, \\ c &= \frac{1}{16}\left(p-e^2+2\cdot e+440\right) < \frac{1}{16}\left(4\cdot e+440\right) < e. \end{aligned}$$

Damit liegen die Zahlen a, b, c, d zwischen 0 und e und daher ist die ungerade ganze Zahl unter a, b, c, d eine passende Zahl N.

Wenn (3.19) nicht gilt, kommen nur $e = 7,\ 19,\ 31$ und damit $p = 59,\ 379,\ 971,\ 1019$ in Frage. Wegen (3.9) scheidet $p = 59$ aus. Für die übrigen erhalten wir durch

$$\left(\frac{3}{379}\right) = \left(\frac{11}{971}\right) = \left(\frac{7}{1019}\right) = -1$$

den gewünschten Widerspruch.

Fall $4 \mid e+1,\ 3 \mid e+1$:

Nun nehmen wir

$$e > 30 \tag{3.20}$$

an und betrachten die Zahlen

$$a = \frac{p-(e-30)\cdot(e-4)}{48}, \qquad b = \frac{p-(e-24)\cdot(e-10)}{48},$$
$$c = \frac{p-(e-18)\cdot(e-16)}{48}, \qquad d = \frac{p-(e-12)\cdot(e-22)}{48}.$$

Nach unserer Annahme gilt $\left(\frac{3}{p}\right) = 1$. Mit $p \equiv 3 \bmod 4$ und dem quadratischen Reziprozitätsgesetz folgt daraus $\left(\frac{p}{3}\right) = -\left(\frac{3}{p}\right) = -1$, was sofort $p \equiv 2 \bmod 3$ impliziert. Mit dem chinesischen Restsatz folgt schließlich $p \equiv 11 \bmod 24$.

Es gilt $e + 1 \equiv 0 \bmod 12$, also können wir $e = 12 \cdot k - 1$ schreiben und erhalten damit

$$\begin{aligned} p-(e-30)\cdot(e-4) &= p-(12\cdot k-31)\cdot(12\cdot k-5) \equiv p-(12\cdot k-7)\cdot(12\cdot k-5) \\ &\equiv p-144\cdot k^2+144\cdot k-35 \equiv 11-11 \equiv 0 \bmod 24. \end{aligned}$$

Somit ist der Zähler von a durch 24 teilbar und es gilt wieder $a \in \frac{1}{2}\mathbb{Z}$.

Wegen

$$b = a - 3 + \frac{1}{2}, \quad c = a - 4 + \frac{1}{2}, \quad d = a - 3,$$

folgt ähnlich wie im vorherigen Fall, daß eine der vier Zahlen eine ungerade ganze Zahl ist. Sie ist eine passende Zahl N, wenn sie zwischen 0 und e liegt. Dies gilt in der Tat wegen (3.10) und (3.20), da

$$a = \frac{1}{48}\left(p - e^2 + 34\cdot e - 120\right) < \frac{1}{48}\left(36\cdot e - 120\right) < e.$$

Ist $e \le 30$, kommen $e = 11,\ 23$, also $p = 131,\ 139,\ 547,\ 563,\ 571$ in Betracht. Wegen (3.9) scheidet $p = 131$ aus, die übrigen Fälle fallen weg wegen

$$\left(\frac{3}{139}\right) = \left(\frac{3}{547}\right) = \left(\frac{5}{563}\right) = \left(\frac{3}{571}\right) = -1.$$

Fall 3 : $p \equiv 5 \bmod 8$

Wegen $p \equiv 1 \bmod 4$ gilt $\left(\frac{-1}{p}\right) = 1$ und deshalb genügt es, eine ungerade ganze Zahl N zu finden mit $-e \le N \le e$ und $\left(\frac{N}{p}\right) = -1$. Dieser Fall wird dem vorherigen sehr ähnlich, allerdings vereinfachen wir ihn dadurch, daß wir N in der Form

$$N = \frac{p - u\cdot v}{2^{2k+1}}$$

angeben können, wobei für $k,\ u,\ v$ dasselbe gilt wie vorher. Da $\left(\frac{2}{p}\right) = -1$, ist $\left(\frac{2^{2k+1}}{p}\right) = -1$ und damit

$$\begin{aligned} -\left(\frac{\frac{p-u\cdot v}{2^{2k+1}}}{p}\right) &= \left(\frac{2^{2k+1}}{p}\right)\cdot\left(\frac{\frac{p-u\cdot v}{2^{2k+1}}}{p}\right) = \left(\frac{p-u\cdot v}{p}\right) \\ &= \left(\frac{-1}{p}\right)\cdot\left(\frac{u}{p}\right)\cdot\left(\frac{v}{p}\right) = 1, \end{aligned}$$

also gilt

$$N = \left(\frac{\frac{p-u\cdot v}{2^{2k+1}}}{p} \right) = -1.$$

Wir unterscheiden wieder verschiedene Fälle.

Fall $2 \nmid e,\ 3 \mid e$:

Wir setzen

$$e > 10 \tag{3.21}$$

voraus und wählen

$$N = \frac{p - (e-4)\cdot(e+6)}{2}.$$

Es ist also $u = e-4$ und $v = e+6$. Wegen $2 \nmid e$ gilt $u \equiv v \equiv 1 \bmod 2$, außerdem gilt $1 \leq u \leq e$, $1 \leq v$. Aus der Voraussetzung $e \equiv 0 \bmod 3$ folgt $v \equiv 0 \bmod 3$ und $v = e+6 \leq 3 \cdot e$. Damit sind die Bedingungen an u und v erfüllt.

Aus (3.10) folgt

$$\begin{aligned} N &= \frac{1}{2}\left(p - e^2 - 2\cdot e + 24\right) > \frac{1}{2}\left(-2\cdot e + 24\right) > -e, \\ N &< 12,\ N \leq 11 \leq e. \end{aligned}$$

Also ist N wegen $-e \leq N \leq e$ eine passende Zahl.

Gilt (3.21) nicht, bleibt wegen (3.11) noch $e = 9$. Da aber zwischen 81 und 100 keine Primzahl $p \equiv 5 \bmod 8$ liegt, scheidet dieser Fall aus.

Fall $2 \nmid e,\ 3 \mid e-1$:

Die Zahl

$$N = \frac{p - e\cdot(e+2)}{2}$$

erfüllt unsere Voraussetzungen, da wegen (3.10)

$$N = \frac{1}{2}\left(p - e^2 - 2e\right) > -e \quad \text{und} \quad N = \frac{1}{2}\left(p - e^2 - 2e\right) < 0$$

gilt.

Fall $2 \nmid e,\ 3 \mid e+1$:

Eine passende Zahl ist diesmal

$$N = \frac{p - (e-2)\cdot(e+4)}{2},$$

denn aus (3.10) und (3.11) folgt

$$N = \frac{1}{2}\left(p - e^2 - 2e + 8\right) > \frac{1}{2}\left(-2e + 8\right) > -e \quad \text{und} \quad N < 4 \leq e.$$

Fall $2 \mid e,\ 3 \mid e$:

Wir betrachten die Zahl

$$N = \frac{p - (e-3)\cdot(e+3)}{2}.$$

Wegen (3.10) und $e \geq 4$ gilt $N = \frac{1}{2}\left(p - e^2 + 9\right) > \frac{9}{2} > -e$. Ist $N \leq e$ falsch, so ist $N \geq e+1$ und damit

$$p \geq e^2 + 2\cdot e - 7. \tag{3.22}$$

Aus (3.10) folgt $e^2 < p < e^2 + 2\cdot e$. Da $e^2 + 2\cdot e \equiv 4 + 4 \equiv 0 \bmod 8$, müßte wegen $p \equiv 5 \bmod 8$ und (3.22)

$$p = e^2 + 2\cdot e - 3$$

gelten. Dies ist jedoch ein Widerspruch, denn wegen $e^2 + 2\cdot e - 3 = (e-1)\cdot(e+3)$ kann die rechte Seite keine Primzahl sein. Somit muß $N \leq e$ gelten und wir haben ein passendes N gefunden.

Fall $2 \mid e$, $3 \mid e+1$:

Offenbar ist

$$N = \frac{p - (e-1)\cdot(e+1)}{2}$$

eine passende Zahl.

Fall $2 \mid e$, $3 \mid e-1$:

Wir setzen

$$e > 15 \tag{3.23}$$

und betrachten die Zahlen

$$a = \frac{p - (e-7)\cdot(e+5)}{8} \quad \text{und} \quad b = \frac{p - (e-11)\cdot(e+17)}{8}.$$

Wegen $e^2 \equiv 2\cdot e \equiv 6\cdot e \equiv 0,\ 4 \bmod 8$ ist

$$p - (e-7)\cdot(e+5) = p - e^2 + 2\cdot e + 35 \equiv 0 \bmod 8$$

und

$$p - (e-11)\cdot(e+17) = p - e^2 - 6\cdot e + 187 \equiv 0 \bmod 8,$$

also sind beide Zahlen ganz. Da

$$b = a - e + 19, \tag{3.24}$$

ist eine der beiden Zahlen ungerade. Außerdem ist nach (3.10), (3.23) und (3.24)

$$a > 0, \qquad b > -e$$

und

$$\begin{aligned} a &= \frac{1}{8}\left(p - e^2 + 2\cdot e + 35\right) < \frac{1}{8}\left(4\cdot e + 35\right) < e, \\ b &= \frac{1}{8}\left(p - e^2 - 6\cdot e + 187\right) < \frac{1}{8}\left(-4\cdot e + 187\right) < e. \end{aligned}$$

Somit haben wir ein passendes N gefunden.

Ist $e > 15$ falsch, kommen nur $e = 4,\ 10$ und damit $p = 101,\ 109$ in Betracht. Dabei ist $p = 109$ wegen (3.9) nicht möglich und wegen $\left(\frac{3}{101}\right) = -1$ scheidet auch $p = 101$ aus. Damit haben wir den Satz bewiesen. □

3.4 Satz von Stolt

Ein Jahr später, 1954, verbessert Bengt Stolt die Aussage von Rédei und publiziert in seiner Arbeit den folgenden Satz, dessen Beweis sich sehr an dem von Rédei orientiert.

Satz

Wenn p eine Primzahl $\equiv 5$ mod 8 ist, besteht die Ungleichung

$$n(p) < \left(\frac{p}{2}\right)^{\frac{1}{2}},$$

außer für $p = 5, 13, 37, 61, 109$.

Beweis:

In einer kleinen Tabelle wollen wir zunächst wieder zeigen, daß der Satz für $p = 5, 13, 37, 61, 109$ nicht gilt.

p	$n(p)$	$\left\lfloor \left(\frac{p}{2}\right)^{\frac{1}{2}} \right\rfloor$
5	3	1
13	5	2
37	5	4
61	7	5
109	11	7

Tabelle 3.5: Primzahlausnahmen von Stolt

Wir bezeichnen mit e die größte natürliche Zahl $< \sqrt{\frac{p}{2}}$. Wegen $\sqrt{\frac{p}{2}} \notin \mathbb{Z}$ ist dann $e < \sqrt{\frac{p}{2}} < e+1$, also $2 \cdot e^2 < p < 2 \cdot (e+1)^2$. Daraus erhalten wir schließlich

$$0 < p - 2 \cdot e^2 < 4 \cdot e + 2. \tag{3.25}$$

Es ist

$$e \geq 5,$$

denn für $e < 5$ ist $p = 29$ die einzige Primzahl für die der Satz wegen $n(29) = 3 < \sqrt{\frac{29}{2}} \approx 3,81$ gilt.

Wir wählen nun

$$a = \frac{p - u \cdot v}{8} \quad \text{und} \quad b = \frac{p - u' \cdot v'}{8}$$

mit

$$0 < |a| \leq e, \quad 0 < |b| \leq e, \quad a - b \text{ ungerade.}$$

Außerdem soll

$$u = 3 \cdot u_1 \quad \text{und} \quad u' = 3 \cdot u_1'$$

sowie

$$v,\ v' \leq e \quad \text{oder} \quad v = 3 \cdot v_1,\ v' \leq e \quad \text{oder} \quad v = 3 \cdot v_1,\ v' = 3 \cdot v_1'$$

gelten, wobei $u_1,\ u_1',\ v_1,\ v_1'$ ganze positive ungerade Zahlen $\leq e$ sind.

Wegen $\left(\frac{-1}{p}\right) = 1$ und $\left(\frac{2}{p}\right) = -1$ gilt dann

$$\begin{aligned} -\left(\frac{\frac{p-u\cdot v}{8}}{p}\right) &= \left(\frac{2^3}{p}\right) \cdot \left(\frac{\frac{p-u\cdot v}{8}}{p}\right) = \left(\frac{p-u\cdot v}{p}\right) = \left(\frac{-u\cdot v}{p}\right) = \left(\frac{3\cdot u_1 \cdot v}{p}\right) \\ &= \left(\frac{3}{p}\right) \cdot \left(\frac{u_1}{p}\right) \cdot \left(\frac{v}{p}\right) \end{aligned}$$

bzw.

$$-\left(\frac{\frac{p-u\cdot v}{8}}{p}\right) = \left(\frac{3}{p}\right)^2 \cdot \left(\frac{u_1}{p}\right) \cdot \left(\frac{v_1}{p}\right) = \left(\frac{u_1}{p}\right) \cdot \left(\frac{v_1}{p}\right)$$

und analog

$$-\left(\frac{\frac{p-u'\cdot v'}{8}}{p}\right) = \left(\frac{3}{p}\right) \cdot \left(\frac{u_1'}{p}\right) \cdot \left(\frac{v'}{p}\right)$$

bzw.

$$-\left(\frac{\frac{p-u'\cdot v'}{8}}{p}\right) = \left(\frac{3}{p}\right)^2 \cdot \left(\frac{u_1'}{p}\right) \cdot \left(\frac{v_1'}{p}\right) = \left(\frac{u_1'}{p}\right) \cdot \left(\frac{v_1'}{p}\right).$$

Somit muß sowohl mindestens eine der Zahlen $a,\ 3,\ u_1,\ v,\ v_1$ als auch mindestens eine der Zahlen $b,\ 3,\ u_1',\ v',\ v_1'$ ein ungerader quadratischer Nichtrest sein und einen ungeraden Primteiler besitzen, der ebenfalls quadratischer Nichtrest modulo p ist. Also gibt es unter den Zahlen

$$1,\ 3,\ 5, \ldots,\ (\leq e)$$

mindestens einen quadratischen Nichtrest modulo p.

Daß solche Zahlen $u_1,\ u_1',\ v,\ v',\ a,\ b$ existieren, zeigen wir in Tabelle 3.6. Wir unterscheiden 24 Fälle. Dabei stellen wir drei Bedingungen an e. Die Bedingung in der linken Spalte sorgt dafür, daß $u,\ u',\ v,\ v' \equiv 0 \bmod 3$ und folglich $u_1,\ u_1',\ v_1,\ v_1'$ ganzzahlig sind. Die mittlere Bedingung ist notwendig, damit $a,\ b \equiv 0 \bmod 8$ und somit $a,\ b \in \mathbb{Z}$ gilt. Aus der rechten Bedingung erhalten wir $0 < |a|, |b| \leq e$ sowie $u,\ u',\ v,\ v' \leq 3 \cdot e$ und damit $u_1,\ u_1',\ v_1,\ v_1' \leq e$.

Da die Zahlen a und b an so viele Bedingungen gebunden sind, muß man für jeden Fall prüfen, ob auch alle gestellten Forderungen wirklich erfüllt sind. Dabei wollen wir einen Fall genauer erläutern. Für den Fall $3 \mid e+1,\ e \equiv 1 \bmod 8$ gibt STOLT in seiner Originalarbeit die Zahlen

$$a = \frac{p - (2 \cdot e - 19) \cdot (e + 10)}{8} \quad \text{und} \quad b = \frac{p - (2 \cdot e + 5) \cdot (e - 4)}{8}$$

an. Wegen $p-(2\cdot e+5)\cdot(e-4)\equiv 5-7\cdot 5\equiv 1 \bmod 8$ ist jedoch $b\notin\mathbb{Z}$. Daher geben wir für diesen Fall eigene Werte für a und b an und zeigen, daß sie die geforderten Bedingungen erfüllen.

Wir wählen für $e\geq 82$ die ganzen Zahlen

$$a=\frac{p-(2\cdot e-1)\cdot(e+4)}{8}\quad\text{und}\quad b=\frac{p-(2\cdot e+29)\cdot(e-14)}{8}$$

mit $u=2\cdot e-1$, $v=e+4$, $u'=2\cdot e+29$ und $v'=e-14$. Da $e\equiv -1 \bmod 3$, sind die Bedingungen an u, u' erfüllt. Für v, v' gilt $v\leq 3\cdot e$, $v\equiv 0 \bmod 3$ und $v'\leq e$, was auch unseren Forderungen entspricht.

Wegen (3.25) und $e\geq 82$ gilt

$$a=\frac{1}{8}\left(p-2\cdot e^2-7\cdot e+4\right)<\frac{1}{8}\left(-3\cdot e+6\right)\leq e\quad\text{und}\quad a>\frac{1}{8}\left(-7\cdot e+4\right)\geq -e,$$

sowie

$$b=\frac{1}{8}\left(p-2\cdot e^2-e+406\right)<\frac{1}{8}\left(3\cdot e+408\right)\leq e\quad\text{und}\quad b>\frac{1}{8}\left(-e+406\right)\geq -e.$$

Schließlich gilt noch

$$a-b=-\frac{3\cdot e+1}{4}-50\equiv 1 \bmod 2$$

und damit haben wir passende Zahlen a, b gefunden, die uns einen gewünschten quadratischen Nichtrest $\leq e$ liefern.

In Tabelle 3.7 betrachten wir die Ausnahmewerte für e, die sich in Tabelle 3.6 ergeben. Für Primzahlen $p\equiv 13 \bmod 40$ und $p\equiv 37 \bmod 40$ erhalten wir

$$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)=\begin{cases}\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1, & \text{für } p\equiv 13 \bmod 40,\\ \left(\frac{2}{5}\right)=-1, & \text{für } p\equiv 37 \bmod 40.\end{cases}$$

Da also 5 quadratischer Nichtrest ist und $e\geq 5$, gilt der Satz für diese Primzahlen. Daher genügt es, in Tabelle 3.7 die Gültigkeit des Satzes für die Primzahlen $p\equiv 21 \bmod 40$ und $p\equiv 29 \bmod 40$ zu zeigen. Dabei sehen wir auch, daß $p=61$ und $p=109$ Ausnahmefälle sind. Damit ist der Satz bewiesen. □

Bedingungen für e	$a,\ b \in \mathbb{Z}$	$a-b$	Ausnahmen für e
$3 \mid e, \quad e \equiv 0 \bmod 8, \quad e \geq 9$	$a = \frac{1}{8}[p-(2e+3)\cdot(e-1)]$, $b = \frac{1}{8}[p-(2e+9)\cdot(e-3)]$	$a-b = \frac{1}{4}e-3$	
$3 \mid e, \quad e \equiv 2 \bmod 8, \quad e \geq 9$	$a = \frac{1}{8}[p-(2e-3)\cdot(e+3)]$, $b = \frac{1}{8}[p-(2e+9)\cdot(e-1)]$	$a-b = \frac{1}{2}e$	
$3 \mid e, \quad e \equiv 4 \bmod 8, \quad e \geq 71$	$a = \frac{1}{8}[p-(2e-15)\cdot(e+9)]$, $b = \frac{1}{8}[p-(2e+33)\cdot(e-15)]$	$a-b = -45$	12, 36, 60
$3 \mid e, \quad e \equiv 6 \bmod 8, \quad e \geq 34$	$a = \frac{1}{8}[p-(2e+27)\cdot(e-11)]$, $b = \frac{1}{8}[p-(2e+15)\cdot(e-7)]$	$a-b = -\frac{1}{2}e+24$	6, 30
$3 \mid e+1, \quad e \equiv 0 \bmod 8, \quad e \geq 98$	$a = \frac{1}{8}[p-(2e+5)\cdot(e+1)]$, $b = \frac{1}{8}[p-(2e-43)\cdot(e+25)]$	$a-b = -135$	8, 32, 56, 80
$3 \mid e+1, \quad e \equiv 2 \bmod 8, \quad e \geq 51$	$a = \frac{1}{8}[p-(2e-7)\cdot(e+1)]$, $b = \frac{1}{8}[p-(2e+23)\cdot(e-11)]$	$a-b = -\frac{3e+2}{4}-25$	26, 50
$3 \mid e+1, \quad e \equiv 4 \bmod 8, \quad e \geq 18$	$a = \frac{1}{8}[p-(2e+5)\cdot(e-3)]$, $b = \frac{1}{8}[p-(2e+17)\cdot(e-7)]$	$a-b = \frac{1}{2}e-13$	
$3 \mid e+1, \quad e \equiv 6 \bmod 8, \quad e \geq 5$	$a = \frac{1}{8}[p-(2e-1)\cdot(e+1)]$, $b = \frac{1}{8}[p-(2e+5)\cdot(e-1)]$	$a-b = \frac{e-2}{4}$	
$3 \mid e-1, \quad e \equiv 0 \bmod 8, \quad e \geq 37$	$a = \frac{1}{8}[p-(2e+13)\cdot(e-7)]$, $b = \frac{1}{8}[p-(2e+7)\cdot(e-5)]$	$a-b = -\frac{1}{4}e+7$	16
$3 \mid e-1, \quad e \equiv 2 \bmod 8, \quad e \geq 13$	$a = \frac{1}{8}[p-(2e+13)\cdot(e-5)]$, $b = \frac{1}{8}[p-(2e+7)\cdot(e-3)]$	$a-b = -\frac{e-2}{4}+5$	10
$3 \mid e-1, \quad e \equiv 4 \bmod 8, \quad e \geq 13$	$a = \frac{1}{8}[p-(2e+13)\cdot(e-3)]$, $b = \frac{1}{8}[p-(2e+7)\cdot(e-1)]$	$a-b = -\frac{1}{4}e+4$	
$3 \mid e-1, \quad e \equiv 6 \bmod 8, \quad e \geq 91$	$a = \frac{1}{8}[p-(2e-5)\cdot(e+5)]$, $b = \frac{1}{8}[p-(2e+43)\cdot(e-19)]$	$a-b = -99$	22, 46, 70
$3 \mid e, \quad e \equiv 1 \bmod 8, \quad e \geq 15$	$a = \frac{1}{8}[p-(2e+9)\cdot(e-2)]$, $b = \frac{1}{8}[p-(2e+15)\cdot(e-4)]$	$a-b = \frac{e-1}{4}-5$	9
$3 \mid e, \quad e \equiv 3 \bmod 8, \quad e \geq 101$	$a = \frac{1}{8}[p-(2e-9)\cdot(e+6)]$, $b = \frac{1}{8}[p-(2e+39)\cdot(e-18)]$	$a-b = -81$	27, 51, 75, 99
$3 \mid e, \quad e \equiv 5 \bmod 8, \quad e \geq 49$	$a = \frac{1}{8}[p-(2e-21)\cdot(e+12)]$, $b = \frac{1}{8}[p-(2e+27)\cdot(e-12)]$	$a-b = -9$	21, 45
$3 \mid e, \quad e \equiv 7 \bmod 8, \quad e \geq 15$	$a = \frac{1}{8}[p-(2e+15)\cdot(e-6)]$, $b = \frac{1}{8}[p-(2e+3)\cdot(e-2)]$	$a-b = -\frac{e-1}{2}+10$	
$3 \mid e+1, \quad e \equiv 1 \bmod 8, \quad e \geq 38$	$a = \frac{1}{8}[p-(2e-1)\cdot(e+4)]$, $b = \frac{1}{8}[p-(2e+29)\cdot(e-14)]$	$a-b = -\frac{3e+1}{4}-50$	17, 41, 65
$3 \mid e+1, \quad e \equiv 3 \bmod 8, \quad e \geq 22$	$a = \frac{1}{8}[p-(2e-13)\cdot(e+10)]$, $b = \frac{1}{8}[p-(2e+11)\cdot(e-6)]$	$a-b = -e+8$	11
$3 \mid e+1, \quad e \equiv 5 \bmod 8, \quad e \geq 11$	$a = \frac{1}{8}[p-(2e+11)\cdot(e-4)]$, $b = \frac{1}{8}[p-(2e+5)\cdot(e-2)]$	$a-b = -\frac{e-1}{4}+4$	5
$3 \mid e+1, \quad e \equiv 7 \bmod 8, \quad e \geq 11$	$a = \frac{1}{8}[p-(2e+11)\cdot(e-2)]$, $b = \frac{1}{8}[p-(2e+5)\cdot e]$	$a-b = -\frac{e-3}{4}+2$	
$3 \mid e-1, \quad e \equiv 1 \bmod 8, \quad e \geq 10$	$a = \frac{1}{8}[p-(2e+7)\cdot(e-4)]$, $b = \frac{1}{8}[p-(2e+1)\cdot(e-2)]$	$a-b = -\frac{e-1}{4}+3$	
$3 \mid e-1, \quad e \equiv 3 \bmod 8, \quad e \geq 19$	$a = \frac{1}{8}[p-(2e+19)\cdot(e-6)]$, $b = \frac{1}{8}[p-(2e+7)\cdot(e-2)]$	$a-b = -\frac{e-1}{2}+12$	
$3 \mid e-1, \quad e \equiv 5 \bmod 8, \quad e \geq 7$	$a = \frac{1}{8}[p-(2e+1)\cdot(e+2)]$, $b = \frac{1}{8}[p-(2e+7)\cdot e]$	$a-b = \frac{e-1}{4}$	
$3 \mid e-1, \quad e \equiv 7 \bmod 8, \quad e \geq 66$	$a = \frac{1}{8}[p-(2e-11)\cdot(e+8)]$, $b = \frac{1}{8}[p-(2e+37)\cdot(e-16)]$	$a-b = -63$	7, 31, 55

Tabelle 3.6: Fallunterscheidungen zum Beweis von STOLT

e	$2e^2 < p < 2(e+1)^2$	p	$n(p)$
5	$50 < p < 72$	61	**7**
6	$72 < p < 98$	–	
7	$98 < p < 128$	101	3
		109	**11**
8	$128 < p < 162$	149	3
9	$162 < p < 200$	181	7
10	$200 < p < 242$	229	7
11	$242 < p < 288$	269	7
12	$288 < p < 338$	–	
16	$512 < p < 578$	541	11
17	$578 < p < 648$	–	
21	$882 < p < 968$	941	3
22	$968 < p < 1058$	1021	7
26	$1352 < p < 1458$	1381	11
		1429	11
27	$1458 < p < 1568$	1549	13
30	$1800 < p < 1922$	1861	7
		1901	3
31	$1922 < p < 2048$	1949	3
		2029	7
32	$2048 < p < 2178$	2069	3
		2141	3
36	$2592 < p < 2738$	2621	3
41	$3362 < p < 3528$	3389	3
		3461	3
		3469	13
45	$4050 < p < 4232$	4229	3
46	$4232 < p < 4418$	4261	7
		4349	3
50	$5000 < p < 5202$	5021	3
		5101	7
		5189	3

e	$2e^2 < p < 2(e+1)^2$	p	$n(p)$
51	$5202 < p < 5408$	5261	3
		5309	3
		5381	3
55	$6050 < p < 6272$	6101	3
		6221	3
		6229	7
		6269	3
56	$6272 < p < 6498$	6301	17
		6489	3
		6421	11
		6469	13
60	$7200 < p < 7442$	7229	3
		7309	19
		7349	3
65	$8450 < p < 8712$	8461	7
		8501	3
		8581	7
		8629	7
		8669	3
70	$9800 < p < 10082$	9829	11
		9901	7
		8841	3
		9949	19
		10061	3
		10069	7
75	$11250 < p < 11552$	11261	3
		11549	3
80	$12800 < p < 13122$	12821	3
		12829	7
		12941	3
		13109	3
99	$19602 < p < 20000$	19661	3
		19709	3
		19861	11
		19949	3

Tabelle 3.7: Ausnahmewerte für e im Beweis von STOLT

3.5 Satz von NIVEN-ZUCKERMAN-MONTGOMERY

Ähnlich zu NAGELLS Abschätzungen ist die folgende Abschätzung von IVAN NIVEN, HERBERT S. ZUCKERMAN und HUGH L. MONTGOMERY aus dem Jahr 1991, die man in dem Buch *"An Introduction to The Theory of Numbers"* (vgl. [Niv/Zuc/Mon]) findet. Erstaunlich dabei ist, daß sich die Aussage sehr kurz und mit einfachen elementaren Mitteln beweisen läßt.

Satz

Sei $p \in \mathbb{P}$ eine ungerade Primzahl und $n^*(p)$ der kleinste positive quadratische Nichtrest modulo p. Dann gilt

$$n^*(p) < 1 + \sqrt{p}.$$

Beweis:

Sei m die kleinste positive Zahl für die

$$m \cdot n^*(p) > p$$

gilt. Dann ist natürlich $(m-1) \cdot n^*(p) < p$, woraus man $0 < m \cdot n^*(p) - p < n^*(p)$ erhält. Daher ist $m \cdot n^*(p) - p$ ein quadratischer Rest modulo p und es gilt

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

Das liefert sofort

$$\begin{aligned} \left(\frac{m \cdot n^*(p)}{p}\right) &= 1 \\ \Longrightarrow \left(\frac{m}{p}\right) \cdot \underbrace{\left(\frac{n^*(p)}{p}\right)}_{=-1} &= 1 \\ \Longrightarrow \left(\frac{m}{p}\right) &= -1. \end{aligned}$$

Da $n^*(p)$ der kleinste quadratische Nichtrest ist, gilt $m \geq n^*(p)$ und man erhält die Ungleichung

$$(n^*(p) - 1)^2 < (n^*(p) - 1) \cdot n^*(p) \leq (m-1) \cdot n^*(p) < p.$$

Wurzelziehen und Auflösen nach $n^*(p)$ liefert das gewünschte Ergebnis

$$n^*(p) < \sqrt{p} + 1.$$

□

3.6 Satz von Wedeniwski

In seiner Dissertation [Wed] gibt Sebastian Wedeniwski einen elementaren Beweis zu einer etwas besseren Abschätzung an. Er betrachtet jedoch nicht Primzahlen und ihre kleinsten quadratischen Nichtreste, sondern natürliche Zahlen m und die erste Zahl $x < m$, für die das Jacobi-Symbol $\left(\frac{x}{m}\right)$ gleich -1 ist.

Satz

Sei $m \geq 3$ eine natürliche Zahl, die kein Quadrat ist, und

$$x = \min\left\{k \in \mathbb{N}_{>0} \mid \left(\frac{k}{m}\right) = -1\right\},$$

dann gilt

$$x \leq 1 + \sqrt{m-1}.$$

Beweis:

Sei $t \equiv -m \bmod x$, wobei $t \geq 0$ und $s = \dfrac{t+m}{x}$. Für $t = 0$ ist allerdings $m \equiv 0 \bmod x$ und daraus folgt $\left(\dfrac{x}{m}\right) = 0$, was jedoch einen Widerspruch zur Definition von x liefert. Also muß $1 \leq t < x$ gelten. In diesem Fall ist $\left(\dfrac{t}{m}\right) = 1$ und wir erhalten damit

$$1 = \left(\frac{t}{m}\right) = \left(\frac{t+m}{m}\right) = \left(\frac{s \cdot x}{m}\right) = \left(\frac{s}{m}\right) \cdot \left(\frac{x}{m}\right) = -\left(\frac{s}{m}\right).$$

Daher ist $x \leq s < \dfrac{x+m}{x}$ und es folgt $x^2 - x - m < 0$. Daraus ergibt sich mit quadratischer Ergänzung $(x-1)^2 < \left(x - \dfrac{1}{2}\right)^2 < m + \dfrac{1}{4}$. Da x und m ganze Zahlen sind, gilt sogar $(x-1)^2 \leq m$. Da m nach Voraussetzung kein Quadrat ist, erhalten wir schließlich

$$(x-1)^2 \leq m - 1,$$

was uns die Behauptung liefert. □

3.7 Die Sätze von Brauer

Gute Ergebnisse für die Abschätzung des kleinsten quadratischen Nichtrestes erzielte auch Alfred Brauer mit elementaren Methoden. Bereits im Jahre 1931 veröffentlichte er seine drei Sätze, in denen er die Fälle $p \equiv 7 \bmod 8$, $p \equiv 5 \bmod 8$ und $p \equiv \pm 3 \bmod 8$ behandelt. Dabei waren seine Ergebnisse sogar besser als die von Nagell.

Der Beweis des ersten Satzes von Brauer beruht auf der Idee, eine Sequenz quadratischer Nichtreste zu konstruieren und diese in das Intervall zweier benachbarter Quadratzahlen einzuschließen. Dieses Intervall wird sukzessive in Teilintervalle zerlegt. Durch abschätzen der Maximallänge dieser Teilintervalle findet Brauer verschiedene Schranken für $n^*(p)$. Durch weitere Abschätzungen gelangt er schließlich durch einen Widerspruch zu seinem Ergebnis.

3.7.1 Erster Satz von Brauer

Ist p eine Primzahl der Form $8n+7$, so gilt für den kleinsten quadratischen Nichtrest $n^*(p)$

$$n^*(p) < (2p)^{\frac{2}{5}} + 3(2p)^{\frac{1}{5}} + 1.$$

Beweis:

Sei r eine beliebige ganze Zahl, die später geeignet gewählt werden wird und die Bedingung $1 < r < n^*(p)$ erfüllt. Dann ist r ein quadratischer Rest modulo p. Wegen $p \equiv 7 \bmod 8$, gilt natürlich $p \equiv 3 \bmod 4$ und somit $\left(\frac{-1}{p}\right) = -1$. Da -1 also ein quadratischer Nichtrest modulo p ist, sind die Zahlen

$$p-1,\ p-2,\ldots,\ p-n^*(p)+1$$

sämtlich Nichtreste modulo p. Da $r > 1$, ist p kein ganzzahliges Vielfaches von r. Daher sind die im Intervall $[p-n^*(p)+1, p]$ liegenden ganzzahligen Vielfache von r, die wir mit

$$k \cdot r,\ (k+1)\cdot r, \ldots,\ (k+l-1)\cdot r \qquad (l \geq 1) \tag{3.26}$$

bezeichnen, ebenfalls quadratische Nichtreste modulo p. Die l Zahlen

$$k,\ k+1,\ldots,\ k+l-1 \tag{3.27}$$

bilden daher eine Sequenz von l Nichtresten. Also kann das Intervall $[k,\ k+l-1]$ keine Quadratzahl enthalten. Man wähle $a \in \mathbb{Z}$, a positiv so, daß

$$a^2 < k \leq k+l-1 < (a+1)^2. \tag{3.28}$$

Durch den Punkt $a(a+1)$ wird das Intervall $A = \left[a^2, (a+1)^2\right]$ in die beiden Teilintervalle $A_1 = \left[a(a+1), (a+1)^2\right]$ und $A_2 = \left[a^2, a(a+1)\right]$ zerlegt.

Sei nun t_1 die größte positive ganze Zahl, für die gilt

$$(a+1)^2 - t_1^2 > a(a+1). \tag{3.29}$$

Dann ist

$$a^2+2a+1-t_1^2-a^2-a > 0 \Longleftrightarrow a+1-t_1^2 > 0$$

$$\begin{array}{lccl}
\Longleftrightarrow & t_1 < & \sqrt{a+1} & \leq t_1+1 \\
\Longleftrightarrow & t_1^2 < & a+1 & \leq t_1^2+2t_1+1 \\
\Longleftrightarrow & t_1^2 \leq & a \leq t_1^2+2t_1 & < t_1^2+2t_1+1 \\
\Longleftrightarrow & t_1 \leq & \sqrt{a} & < t_1+1.
\end{array}$$

Also ist

$$t_1 = \left\lfloor \sqrt{a} \right\rfloor . \tag{3.30}$$

Das Intervall A_1 wird wiederum durch die Punkte

$$(a+1)^2 - \nu^2, \qquad (\nu = 1, 2, \ldots, t_1) \tag{3.31}$$

in Teilintervalle zerlegt. Für die Entfernung zweier benachbarter Teilpunkte im Intervall gilt

$$\left[(a+1)^2 - \nu^2\right] - \left[(a+1)^2 - (\nu+1)^2\right] = 2\nu + 1.$$

Wegen (3.29) ist die Maximallänge s_1 dieser Teilintervalle $s_1 \leq 2t_1 + 1$. Aus (3.30) folgt daher

$$s_1 \leq 2\left\lfloor \sqrt{a} \right\rfloor + 1. \tag{3.32}$$

Nun sei t_2 die größte positive ganze Zahl, für die

$$a(a+1) - t_2(t_2+1) > a^2 \tag{3.33}$$

gilt. Dann ist $t_2^2 + t_2 < a$ und die positive Wurzel der Gleichung $t_2^2 + t_2 - a = 0$ ist $-\frac{1}{2} + \sqrt{\frac{1+4a}{4}}$. Daraus erhält man

$$t_2 < \left\lfloor -\frac{1}{2} + \sqrt{\frac{1+4a}{4}} \right\rfloor \leq \left\lfloor -\frac{1}{2} + \frac{1}{2} + \sqrt{a} \right\rfloor = \left\lfloor \sqrt{a} \right\rfloor . \tag{3.34}$$

Durch die Punkte

$$a(a+1) - \nu(\nu+1), \qquad (\nu = 1, 2, \ldots, t_2) \tag{3.35}$$

wird das Intervall A_2 in Teilintervalle zerlegt. Für die Maximallänge s_2 dieser Teilintervalle gilt wegen

$$[a(a+1) - \nu(\nu+1)] - [a(a+1) - (\nu+1)(\nu+2)] = 2\nu + 2$$

und mit (3.33) und (3.34)

$$s_2 \leq 2t_2 + 2 \leq 2\left\lfloor \sqrt{a} \right\rfloor + 2. \tag{3.36}$$

Betrachtet man nun die Teilintervalle, in die das ganze Intervall A durch die Punkte (3.31) und (3.35) eingeteilt wird, dann gilt für deren Maximallänge s wegen (3.32) und (3.36)

$$s = \max(s_1, s_2) \leq 2\left\lfloor \sqrt{a} \right\rfloor + 2. \tag{3.37}$$

Angenommen es würde nun

$$n^*(p) \geq \max(a + 2 + t_1, rs) \tag{3.38}$$

gelten, dann wären die Zahlen $1,\ 2, \ldots,\ a + 1 + t_1$ alle quadratische Reste modulo p. Daher wären für $\nu = 1,\ 2, \ldots,\ t_1$ die Zahlen

$$(a+1)^2 - \nu^2 = (a + 1 + \nu)(a + 1 - \nu)$$

und für $\nu = 0,\ 1, \ldots,\ t_2$ die Zahlen

$$a\,(a+1) - \nu\,(\nu+1) = (a+1+\nu)\,(a-\nu)$$

ebenfalls quadratische Reste, da wegen (3.30) und (3.34)

$$t_2 \leq t_1$$

gilt. Also sind die Endpunkte der Teilintervalle von A sämtlich Reste. Da die Längen der Teilintervalle $\leq s$ waren, bedeutet das, daß jedes beliebige, im Intervall A gelegene Intervall von der Länge s mindestens einen quadratischen Rest enthält. Somit kann in A keine Sequenz von s quadratischen Nichtresten liegen. Da aber wegen (3.38)

$$n^*\,(p) \geq rs$$

gilt, würden im Intervall $[p - n^*\,(p) + 1,\ p]$ mindestens s ganzzahlige Vielfache von r liegen. Nach (3.26) ist die Anzahl dieser Vielfachen gerade l und deshalb ist

$$l \geq s.$$

Folglich müßte das Intervall A wegen (3.27) und (3.28) eine Sequenz von mindestens s Nichtresten, nämlich $k,\ k+1, \ldots,\ k+l-1$ enthalten, was allerdings zu einem Widerspruch führt. Deshalb ist die Ungleichung (3.38) nicht möglich und es muß

$$n^*\,(p) < \max\,(a+2+t_1, rs)$$

gelten. Mit (3.30) und (3.37) folgt daraus

$$n^*\,(p) < \max\left\{a+2+\left\lfloor\sqrt{a}\right\rfloor, 2r\left(\left\lfloor\sqrt{a}\right\rfloor+1\right)\right\}$$

und schließlich

$$n^*\,(p) \leq \max\left\{a+1+\left\lfloor\sqrt{a}\right\rfloor, 2r\left(\left\lfloor\sqrt{a}\right\rfloor+1\right)-1\right\}.$$

Aus (3.26) erhält man

$$k+l-1 < \frac{p}{r}$$

und mit (3.28) ergibt sich

$$a < \sqrt{\frac{p}{r}},$$

es muß also

$$n^*\,(p) < \max\left\{\sqrt{\frac{p}{r}}+1+\sqrt[4]{\frac{p}{r}}, 2r\left(\sqrt[4]{\frac{p}{r}}+1\right)-1\right\} \tag{3.39}$$

gelten. Wir nehmen nun

$$n^*\,(p) \geq (2p)^{\frac{2}{5}} + 3\,(2p)^{\frac{1}{5}} + 1 \tag{3.40}$$

an und wählen für $p > 16$

$$r = \left\lfloor \left(\frac{p}{16}\right)^{\frac{1}{5}} \right\rfloor + 1,$$

was die Voraussetzung $1 < r < n^*(p)$ erfüllt. Daraus erhält man

$$\sqrt{\frac{p}{r}} < \sqrt{\frac{p \cdot 2^{\frac{4}{5}}}{p^{\frac{1}{5}}}} = 2^{\frac{2}{5}} p^{\frac{1}{2}} p^{-\frac{1}{10}} = 2^{\frac{2}{5}} p^{\frac{2}{5}} = (2p)^{\frac{2}{5}}$$

und es folgt

$$\sqrt{\frac{p}{r}} + 1 + \sqrt[4]{\frac{p}{r}} < (2p)^{\frac{2}{5}} + 1 + (2p)^{\frac{1}{5}} < (2p)^{\frac{2}{5}} + 3\,(2p)^{\frac{1}{5}} + 1$$

und

$$\begin{aligned} 2r\left(\sqrt[4]{\frac{p}{r}} + 1\right) - 1 < \left(2p^{\frac{1}{5}} \cdot 2^{-\frac{4}{5}} + 2\right)\left((2p)^{\frac{1}{5}} + 1\right) - 1 &= \left((2p)^{\frac{1}{5}} + 2\right)\left((2p)^{\frac{1}{5}} + 1\right) - 1 \\ &= (2p)^{\frac{2}{5}} + 3\,(2p)^{\frac{1}{5}} + 1. \end{aligned}$$

Nach (3.39) ist also

$$n^*(p) < (2p)^{\frac{2}{5}} + 3\,(2p)^{\frac{1}{5}} + 1$$

was allerdings ein Widerspruch zu (3.40) ist und unsere Annahme somit falsch ist.

Es gilt also

$$n^*(p) < (2p)^{\frac{2}{5}} + 3\,(2p)^{\frac{1}{5}} + 1$$

für alle Primzahlen $p > 7$ der Form $8n + 7$. Für $p = 7$ folgt die Behauptung sofort aus $\left(\frac{3}{7}\right) = -1$. □

Nach 2.5.4 ist 2 quadratischer Rest für die Primzahlen der Form $8n+7$. Daher liefert der erste Satz von BRAUER sogar eine Abschätzung für den kleinsten ungeraden Nichtrest für diese Primzahlen. Da 2 für Primzahlen der Form $8n \pm 3$ quadratischer Nichtrest ist, soll nun für diese Primzahlen der kleinste ungerade quadratische Nichtrest abgeschätzt werden.

3.7.2 Zweiter Satz von BRAUER

Ist p eine Primzahl der Form $8n+5$, so gilt für den kleinsten ungeraden quadratischen Nichtrest

$$n(p) < \sqrt{p+4} + 2.$$

Beweis:

Wir betrachten das Intervall $[p - 4 \cdot n(p)\,,\ p + 4 \cdot n(p)]$. Da die Länge dieses Intervalls

$$p + 4 \cdot n(p) - p + 4 \cdot n(p) = 8 \cdot n(p)$$

ist und

$$\begin{aligned} p - 4 \cdot n(p) &\not\equiv 0 \bmod n(p) \\ p + 4 \cdot n(p) &\not\equiv 0 \bmod n(p) \end{aligned}$$

gilt, liegen in dem Intervall $[p - 4 \cdot n(p),\ p + 4 \cdot n(p)]$ acht Vielfache von $n(p)$, also genau vier ungerade Vielfache von $n(p)$. Diese bezeichnen wir mit

$$k \cdot n(p),\ (k+2) \cdot n(p),\ (k+4) \cdot n(p) \quad \text{und} \quad (k+6) \cdot n(p). \tag{3.41}$$

Die Zahlen

$$p - (k+6) \cdot n(p),\ p - (k+4) \cdot n(p),\ p - (k+2) \cdot n(p),\ p - k \cdot n(p)$$

sind vier aufeinanderfolgende gerade Zahlen, von denen genau eine $\equiv 4 \bmod 8$ ist, d.h. sie ist durch 4, aber nicht durch 8 teilbar. Sei nun $p - k^* \cdot n(p)$ diese Zahl. Dann ist die Zahl $\dfrac{p - k^* \cdot n(p)}{4}$ ungerade. Aus (3.41) folgt nun

$$\begin{array}{rrcccl} & p - 4 \cdot n(p) & < & k^* \cdot n(p) & < & p + 4 \cdot n(p) \\ \Longleftrightarrow & -4 \cdot n(p) & < & k^* \cdot n(p) - p & < & 4 \cdot n(p) \\ \Longleftrightarrow & & & |k^* \cdot n(p) - p| & < & 4 \cdot n(p) \\ \Longleftrightarrow & & & |p - k^* \cdot n(p)| & < & 4 \cdot n(p) \end{array}$$

und somit

$$\left| \frac{p - k^* \cdot n(p)}{4} \right| < n(p). \tag{3.42}$$

Also ist $\dfrac{p - k^* \cdot n(p)}{4}$ quadratischer Rest modulo p. Folglich ist auch $k^* \cdot n(p)$ quadratischer Rest und da $n(p)$ Nichtrest ist, ist auch k^* quadratischer Nichtrest. Da aber k^* ungerade ist, gilt $k^* \geq n(p)$. Nach (3.41) gilt

$$k^* \cdot n(p) < p + 4 \cdot n(p),$$

also

$$\begin{array}{rrcl} & n(p)^2 & < & p + 4 \cdot n(p) \\ \Longleftrightarrow & (n(p) - 2)^2 & < & p + 4 \\ \Longleftrightarrow & n(p) - 2 & < & \sqrt{p+4} \end{array}$$

und damit

$$n(p) < \sqrt{p+4} + 2,$$

was wir zeigen wollten. □

Im dritten Satz von BRAUER wird das Ergebnis des zweiten Satzes noch weiter verschärft. Gleichzeitig ergibt sich dieselbe Abschätzung des kleinsten quadratischen Nichtrestes auch für die Primahlen der Form $8n + 3$.

Die Beweisidee des dritten Satzes von BRAUER ist die gleiche wie die des ersten Satzes. Hier wird aus der Sequenz $1,\ 3,\ \ldots,\ n(p) - 2$ von quadratischen Resten wieder eine Sequenz von quadratischen Nichtresten konstruiert, die zwischen zwei benachbarte Quadratzahlen eingebettet wird. Wie im Beweis des ersten Satzes von BRAUER wird nun das Intervall in Teilintervalle aufgeteilt und man erhält durch mehrere Abschätzungen die gewünschte Schranke für $n(p)$.

3.7.3 Dritter Satz von Brauer

Ist $p > 3$ eine Primzahl der Form $8n \pm 3$, so gilt für den kleinsten ungeraden quadratischen Nichtrest

$$n(p) < 2\left[(4p)^{\frac{2}{5}} + (4p)^{\frac{1}{5}}\right] + 1.$$

Beweis:

Wir betrachten die geraden Zahlen

$$p+1,\ p+3,\ \ldots,\ p+n(p)-2.$$

Da $n(p)$ der kleinste quadratische Nichtrest ist, sind diese Zahlen alle quadratische Reste modulo p. Sei r eine beliebige positive ganze Zahl, für die

$$2^{2r+1} < n(p) \tag{3.43}$$

gilt. Die im Intervall $[p,\ p+n(p)-1]$ gelegenen ganzzahligen Vielfachen von 2^{2r+1} seien

$$k \cdot 2^{2r+1},\ (k+1)\cdot 2^{2r+1},\ \ldots,\ (k+l-1)\cdot 2^{2r+1} \qquad (l \geq 1). \tag{3.44}$$

Dann gilt

$$k = \left\lfloor \frac{p}{2^{2r+1}} \right\rfloor + 1. \tag{3.45}$$

Die Zahlen in (3.44) sind sämtlich quadratische Reste. Da $p \equiv \pm 3 \bmod 8$ ist, gilt nach 2.5.4 die Gleichung $\left(\frac{2}{p}\right) = -1$, also ist 2 und damit auch 2^{2r+1} quadratischer Nichtrest. Somit bilden die Zahlen

$$k,\ k+1,\ \ldots,\ k+l-1 \tag{3.46}$$

eine Sequenz von l Nichtresten. Nun läßt sich ein $a \in \mathbb{Z}$, $a > 0$ so bestimmen, daß

$$a^2 < k \leq k+l-1 < (a+1)^2 \tag{3.47}$$

gilt. Aus (3.45) folgt dann

$$a^2 \leq \left\lfloor \frac{p}{2^{2r+1}} \right\rfloor,$$

also

$$a < \sqrt{\frac{p}{2^{2r+1}}}. \tag{3.48}$$

Nun zerlegen wir das Intervall $A = \left[a^2, (a+1)^2\right]$ in Teilintervalle. Dazu unterscheiden wir zwei Fälle.

Fall 1 : a gerade

Sei $t_1 \in \mathbb{Z}$, $t_1 > 0$ so bestimmt, daß

$$(a+1)^2 - (2t_1)^2 > a^2 > (a+1)^2 - (2t_1+2)^2 \tag{3.49}$$

gilt.[1] Aus dem ersten Teil der Ungleichung erhält man

$$\begin{array}{rcl} & (a+1)^2-(2t_1)^2 & > \quad a^2 \\ \Longleftrightarrow & (2t_1)^2 & < \quad -a^2+(a+1)^2 \\ \Longleftrightarrow & (2t_1)^2 & < \quad 2a+1 \end{array}$$

und damit

$$2t_1 \leq \left\lfloor \sqrt{2a} \right\rfloor . \tag{3.50}$$

Somit zerlegen die Punkte

$$(a+1)^2-(2\nu)^2 \qquad (\nu = 1,2,\ldots,t_1) \tag{3.51}$$

das Intervall A in Teilintervalle. Dabei ist die Entfernung zweier benachbarter Teilpunkte

$$\begin{aligned} \left[(a+1)^2-(2\nu)^2\right]-\left[(a+1)^2-(2(\nu+1))^2\right] &= -(2\nu)^2+(2\nu+2)^2 \\ &= 8\nu+4. \end{aligned} \tag{3.52}$$

Von den Teilintervallen ist entweder das Intervall

$$J_{t_1} = \left[(a+1)^2-(2t_1)^2,\ (a+1)^2-(2t_1-2)^2\right]$$

oder das Intervall

$$J_{t_1+1} = \left[a^2,\ (a+1)^2-(2t_1)^2\right]$$

das größte. Wegen (3.52) mit $\nu = t_1-1$ gilt für die Länge $|J_{t_1}|$ des Intervalls J_{t_1}

$$|J_{t_1}| = 8t_1-4. \tag{3.53}$$

Da wir a als gerade vorausgesetzt haben, ist

$$\begin{aligned} a^2-\left[(a+1)^2-(2t_1+2)^2\right] &= a^2-\left(a^2+2a+1-(2t_1)^2-8t_1-4\right) \\ &= \underbrace{-2a}_{\equiv 0}+3+\underbrace{(2t_1)^2}_{\equiv 0}+\underbrace{8t_1}_{\equiv 0 \bmod 4} \\ &\equiv 3 \bmod 4. \end{aligned}$$

Aus (3.49) folgt $a^2-\left[(a+1)^2-(2t_1+2)^2\right] > 0$ und daher

$$a^2-\left[(a+1)^2-(2t_1+2)^2\right] \geq 3.$$

Daraus erhalten wir

$$\begin{aligned} 3 &\leq a^2-\left[(a+1)^2-(2t_1+2)^2\right] = a^2-\left[(a+1)^2-(2t_1)^2-8t_1-4\right] \\ &= a^2-\left[(a+1)^2-(2t_1)^2\right]+8t_1+4 \end{aligned}$$

[1] Diese Ungleichung ist immer möglich, da ein gerades Quadrat nicht gleich der Differenz eines ungeraden und eines geraden Quadrates sein kann und hier $a \geq 2$ gilt.

also

$$\left[(a+1)^2-(2t_1)^2\right]-a^2\le 8t_1+4-3.$$

Für die Länge $|J_{t_1+1}|$ des Intervalls J_{t_1+1} gilt daher

$$|J_{t_1+1}|\le 8t_1+4-3=8t_1+1. \tag{3.54}$$

Aus (3.53), (3.54) und (3.50) ergibt sich für die Maximallänge der Teilintervalle, die wir mit s_1 bezeichnen wollen

$$s_1\le 8t_1+1\le 4\cdot\left\lfloor\sqrt{2a}\right\rfloor+1. \tag{3.55}$$

Fall 2 : a ungerade

Nun sei die nichtnegative ganze Zahl t_2 so bestimmt, daß

$$(a+1)^2-(2t_2+1)^2>a^2>(a+1)^2-(2t_2+3)^2 \tag{3.56}$$

gilt.[2] Wir betrachten wieder die linke Seite der Ungleichung und erhalten

$$\begin{array}{rrcl} & (a+1)^2-(2t_2+1)^2 & > & a^2 \\ \Longleftrightarrow & (2t_2+1)^2 & < & -a^2+(a+1)^2 \\ \Longleftrightarrow & (2t_2+1)^2 & < & 2a+1, \end{array}$$

also

$$2t_2+1\le\left\lfloor\sqrt{2a}\right\rfloor. \tag{3.57}$$

In diesem Fall wird das Intervall $A=\left[a^2,(a+1)^2\right]$ durch die Punkte

$$(a+1)^2-(2\nu+1)^2\qquad(\nu=0,1,\ldots,t_2) \tag{3.58}$$

in Teilintervalle zerlegt. Dabei beträgt die Entfernung zweier benachbarter Teilpunkte

$$\begin{aligned}(a+1)^2-(2\nu+1)^2-\left[(a+1)^2-(2\nu+3)^2\right] &= -(2\nu)^2-4\nu-1+(2\nu)^2+12\nu+9\\ &= 8\nu+8. \end{aligned}\tag{3.59}$$

Für $t_2>0$ ist entweder das Intervall

$$J_{t_2}=\left[(a+1)^2-(2t_2+1)^2,\ (a+1)^2-(2t_2-1)^2\right]$$

oder

$$J_{t_2+1}=\left[a^2,\ (a+1)^2-(2t_2+1)^2\right]$$

das größte der Teilintervalle. Für $t_2=0$ ist das größte Teilintervall

$$J_{t_2+1}=\left[a^2,\ (a+1)^2-(2t_2+1)^2\right]=\left[a^2,\ (a+1)^2-1\right].$$

Aus (3.59) ergibt sich mit $\nu=t_2-1$ für die Länge $|J_{t_2}|$ des Intervalls J_{t_2}

$$|J_{t_2}|=8t_2. \tag{3.60}$$

[2] Dies ist wieder möglich, da die Summe zweier ungeraden Quadrate kein gerades Quadrat sein kann.

Diesmal ist a ungerade und daher gilt

$$\begin{aligned} a^2 - \left[(a+1)^2 - (2t_2+3)^2\right] &= a^2 - \left[a^2 + 2a + 1 - (2t_2+3)^2\right] \\ &= \underbrace{-2a}_{\equiv 2 \bmod 4} \quad -1 + \underbrace{(2t_2+3)^2}_{\equiv 1 \bmod 4} \\ &\equiv 2 \bmod 4 \end{aligned}$$

und mit (3.56) folgt

$$a^2 - \left[(a+1)^2 - (2t_2+3)^2\right] \geq 2.$$

Es ist also

$$\begin{aligned} 2 &\leq a^2 - \left[(a+1)^2 - (2t_2+3)^2\right] = a^2 - \left[(a+1)^2 - (2t_2+1)^2 - 8t_2 - 8\right] \\ &= a^2 - \left[(a+1)^2 - (2t_2+1)^2\right] + 8t_2 + 8 \end{aligned}$$

und damit

$$\left[(a+1)^2 - (2t_2+1)^2\right] - a^2 \leq 8t_2 + 8 - 2.$$

Man erhält somit für die Länge $|J_{t_2+1}|$ von J_{t_2+1}

$$|J_{t_2+1}| \leq 8t_2 + 8 - 2 = 8t_2 + 6. \tag{3.61}$$

Für die Maximallänge s_2 der Teilintervalle ergibt sich diesmal aus (3.60), (3.61) und (3.57)

$$s_2 \leq 8t_2 + 6 \leq 4\left\lfloor\sqrt{2a}\right\rfloor + 2. \tag{3.62}$$

Wenn man also das Intervall A im Fall 1 durch die Punkte in (3.51) und im Fall 2 durch die Punkte in (3.58) in Teilintervalle zerlegt, so sind in beiden Fällen die Längen aller Teilintervalle $\leq s$, wobei

$$s = \max(s_1,\ s_2). \tag{3.63}$$

Wegen (3.55) und (3.62) ist

$$s \leq 4\left\lfloor\sqrt{2a}\right\rfloor + 2. \tag{3.64}$$

Angenommen, es würde

$$n(p) \geq \max\left\{a + 2 + \left\lfloor\sqrt{2a}\right\rfloor,\ 2^{2r+1} \cdot s\right\} \tag{3.65}$$

gelten, dann wären die ungeraden Zahlen, die $\leq a + 1 + \lfloor\sqrt{2a}\rfloor$ sind, quadratische Reste. Für den Fall, daß a gerade ist, wären wegen (3.50) für $\nu = 1, 2, \ldots, t_1$ die ungeraden Zahlen

$$(a+1)^2 - (2\nu)^2 = (a + 1 + 2\nu) \cdot (a + 1 - 2\nu) \tag{3.66}$$

als Produkt quadratischer Reste ebenfalls quadratische Reste modulo p. Ist a ungerade, dann wären mit (3.57) die ungeraden Zahlen

$$(a+1)^2 - (2\nu+1)^2 = (a + 1 + 2\nu + 1) \cdot (a + 1 - 2\nu - 1) \tag{3.67}$$

für $\nu = 0, 1, \ldots, t_1$ ebenfalls quadratische Reste.

Das bedeutet, daß das Intervall A im Fall, daß a gerade ist, durch die Punkte in (3.51) und im Fall, daß a ungerade ist, durch die Punkte in (3.58) in Teilintervalle eingeteilt wird, deren Endpunkte nach (3.66) und (3.67) alle quadratische Reste sind. Nach (3.63) sind die Längen dieser Teilintervalle $\leq s$ und daher müßte jedes beliebige in A gelegene Intervall der Länge s mindestens einen quadratischen Rest enthalten. Das heißt, daß A keine Sequenz von s Nichtresten enthalten kann.

Andererseits hatten wir aber in (3.65)

$$n(p) \geq 2^{2r+1} \cdot s$$

angenommen, und nach (3.44) folgt

$$l \geq s.$$

Wegen (3.46) und (3.47) enthielte das Intervall A eine Sequenz $k,\ k+1,\ \ldots,\ k+l-1$ von mindestens s Nichtresten. Dies ist jedoch ein Widerspruch zu dem obigen Ergebnis. Somit kann die Ungleichung (3.65) nicht möglich sein und es muß

$$n(p) < \max\left\{a + 2 + \left\lfloor\sqrt{2a}\right\rfloor,\ 2^{2r+1} \cdot s\right\} \tag{3.68}$$

gelten.

Aus (3.64) folgt

$$n(p) < \max\left\{a + 2 + \sqrt{2a},\ 2^{2r+1} \cdot \left(4\sqrt{2a} + 2\right)\right\},$$

also

$$n(p) \leq \max\left\{a + 1 + \sqrt{2a},\ 2^{2r+2} \cdot \left(2\sqrt{2a} + 1\right) - 1\right\}.$$

Mit (3.48) gilt schließlich

$$n(p) < \max\left\{\sqrt{\frac{p}{2^{2r+1}}} + 1 + \sqrt{2\sqrt{\frac{p}{2^{2r+1}}}},\ 2^{2r+2} \cdot \left(2\sqrt{2\sqrt{\frac{p}{2^{2r+1}}} + 1}\right) - 1\right\}. \tag{3.69}$$

Sei nun zunächst $p > 2^{13}$, dann ist

$$\begin{aligned} & p > 2^5 \cdot 2^8 \\ \iff \quad & 2^{-8} \cdot p > 2^5 \\ \iff \quad & 2^{-\frac{8}{5}} \cdot p^{\frac{1}{5}} > 2. \end{aligned}$$

Außerdem ist $4 \cdot 2^{-\frac{18}{5}} = 2^{-\frac{8}{5}}$, d.h. in dem Intervall $\left[2^{-\frac{18}{5}} \cdot p^{\frac{1}{5}},\ 2^{-\frac{8}{5}} \cdot p^{\frac{1}{5}}\right]$ liegen zwei Potenzen von 2, also genau eine ungerade Potenz von 2. Daher können wir eine positive ganze Zahl r_0 so bestimmen, daß

$$2^{-\frac{18}{5}} \cdot p^{\frac{1}{5}} < 2^{2r_0+1} < 2^{-\frac{8}{5}} \cdot p^{\frac{1}{5}} \tag{3.70}$$

gilt.

Wir nehmen an, daß

$$n(p) \geq 2\left[(4p)^{\frac{2}{5}} + (4p)^{\frac{1}{5}}\right] + 1 \tag{3.71}$$

ist und wollen damit einen Widerspruch herleiten.

Aus (3.70) erhält man

$$n(p) > 2^{2r_0+1},$$

also ist die Bedingung (3.43) für $r = r_0$ erfüllt und aus (3.69) folgt

$$n(p) < \max\left\{\sqrt{\frac{p}{2^{2r_0+1}}} + 1 + \sqrt{2\sqrt{\frac{p}{2^{2r_0+1}}}},\ 2^{2r_0+2}\cdot\left(2\sqrt{2\sqrt{\frac{p}{2^{2r_0+1}}}} + 1\right) - 1\right\}. \tag{3.72}$$

Andererseits folgt aus (3.70)

$$\begin{aligned}\sqrt{\frac{p}{2^{2r_0+1}}} &= \left(\frac{p}{2^{2r_0+1}}\right)^{\frac{1}{2}} = \left(2^{2r_0+1}\right)^{-\frac{1}{2}}\cdot p^{\frac{1}{2}} < \left(2^{-\frac{18}{5}}\cdot p^{\frac{1}{5}}\right)^{-\frac{1}{2}}\cdot p^{\frac{1}{2}} = 2^{\frac{18}{10}}\cdot p^{-\frac{1}{10}}\cdot p^{\frac{1}{2}} \\ &= 2^{\frac{9}{5}}\cdot p^{\frac{2}{5}}\end{aligned}$$

und

$$\begin{aligned}\sqrt{2\sqrt{\frac{p}{2^{2r_0+1}}}} &= \left(2\left(\frac{p}{2^{2r_0+1}}\right)^{\frac{1}{2}}\right)^{\frac{1}{2}} = 2^{\frac{1}{2}}\cdot\left(\left(\frac{p}{2^{2r_0+1}}\right)^{\frac{1}{2}}\right) < 2^{\frac{1}{2}}\cdot\left(2^{\frac{9}{5}}\cdot p^{\frac{2}{5}}\right)^{\frac{1}{2}} = 2^{\frac{1}{2}}\cdot 2^{\frac{9}{10}}\cdot p^{\frac{2}{10}} \\ &= 2^{\frac{7}{5}}\cdot p^{\frac{1}{5}}.\end{aligned}$$

Also ist

$$\sqrt{\frac{p}{2^{2r_0+1}}} + 1 + \sqrt{2\sqrt{\frac{p}{2^{2r_0+1}}}} < 2^{\frac{9}{5}}\cdot p^{\frac{2}{5}} + 2^{\frac{7}{5}}\cdot p^{\frac{1}{5}} + 1. \tag{3.73}$$

Ebenso folgt aus (3.70)

$$\begin{aligned}2^{2r_0+2}\cdot\left(2\sqrt{2\sqrt{\frac{p}{2^{2r_0+1}}}} + 1\right) - 1 &< 2\cdot\left(2^{-\frac{8}{5}}\cdot p^{\frac{1}{5}}\right)\cdot\left(2\cdot\left(2^{\frac{7}{5}}\cdot p^{\frac{1}{5}}\right) + 1\right) \\ &= 2^{-\frac{3}{5}}\cdot p^{\frac{1}{5}}\cdot\left(2^{\frac{12}{5}}\cdot p^{\frac{1}{5}} + 1\right) \\ &= 2^{\frac{9}{5}}\cdot p^{\frac{2}{5}} + 2^{-\frac{3}{5}}\cdot p^{\frac{1}{5}} \\ &< 2^{\frac{9}{5}}\cdot p^{\frac{2}{5}} + 2^{\frac{7}{5}}\cdot p^{\frac{1}{5}} + 1. \end{aligned}\tag{3.74}$$

Aus (3.72), (3.73) und (3.74) ergibt sich schließlich

$$n(p) < 2^{\frac{9}{5}}\cdot p^{\frac{2}{5}} + 2^{\frac{7}{5}}\cdot p^{\frac{1}{5}} + 1 = 2\left[(4p)^{\frac{2}{5}} + (4p)^{\frac{1}{5}}\right] + 1.$$

Dies ist jedoch ein Widerspruch zu (3.71), also war unsere Annahme falsch und es ist

$$n(p) < 2\left[(4p)^{\frac{2}{5}} + (4p)^{\frac{1}{5}}\right] + 1.$$

Damit ist der Satz für Primzahlen $p > 2^{13}$ der Form $8n \pm 3$ bewiesen.

Wir müssen die Behauptung nun noch für die Primzahlen $3 < p < 2^{13}$ beweisen.

Für $p > 2^{13}$ von der Form $8n+5$ folgt die Behauptung aus dem zweiten Satz von Brauer; man muß hierfür nur zeigen, daß für $p > 2^{13}$ die Ungleichung

$$\begin{aligned} \sqrt{p+4}+2 &< 2\left[(4p)^{\frac{2}{5}}+(4p)^{\frac{1}{5}}\right]+1 \\ \iff \quad p+4 &< \left(2\left[(4p)^{\frac{2}{5}}+(4p)^{\frac{1}{5}}\right]-1\right)^2 \\ \iff \quad p+4 &< \left(2^{\frac{9}{5}}\cdot p^{\frac{2}{5}}+2^{\frac{7}{5}}\cdot p^{\frac{1}{5}}-1\right)^2 \end{aligned}$$

erfüllt ist. Wir setzen

$$y := p^{\frac{1}{5}},$$

d.h. es genügt zu zeigen, daß für $1 < y < 2^{\frac{13}{5}}$

$$\begin{aligned} y^5+4 &< \left(2^{\frac{9}{5}}\cdot y^2+2^{\frac{7}{5}}\cdot y-1\right)^2 \\ \iff \quad y^5+4 &< 2^{\frac{18}{5}}\cdot y^4+2^{\frac{21}{5}}\cdot y^3-2^{\frac{12}{5}}\cdot y+1 \end{aligned}$$

gilt. Dies ist äquivalent damit, zu zeigen, daß

$$\varphi(y) = y^5-2^{\frac{18}{5}}\cdot y^4-2^{\frac{21}{5}}\cdot y^3+2^{\frac{12}{5}}\cdot y+3 < 0$$

ist für $1 < y < 2^{\frac{13}{5}}$. Die Funktion $\varphi(y)$ besitzt zwei positive Nullstellen, nämlich $y_1 \approx 0,63$ und $y_2 \approx 13,48$. Im Intervall $\left[1, 2^{\frac{13}{5}}\right]$ liegt somit keine Nullstelle und hier gilt $\varphi(y) < 0$. Damit ist die Behauptung auch für die Primzahlen $p < 2^{13}$ der Form $8n+5$ bewiesen.

Für die Primzahlen $p < 2^{13}$ der Form $8n+3$ prüft man die Behauptung leicht mit einem Programm nach. □

3.7.4 Satz von Hudson-Williams

Richard H. Hudson und Kenneth S. Williams bewiesen 1980 in einem Artikel, den sie Alfred Brauer zum 86sten Geburtstag widmeten, folgende leicht verbesserte Abschätzung.

Satz

Sei p eine ungerade Primzahl $\not\equiv 1$ mod 8 und bezeichne $n(p)$ den kleinsten ungeraden quadratischen Nichtrest von p. Dann ist

$$n(p) < p^{\frac{2}{5}}+12\cdot p^{\frac{1}{5}}+33.$$

Beweis:

Wir nehmen an, daß

$$n(p) > p^{\frac{2}{5}}+12\cdot p^{\frac{1}{5}}+33 \tag{3.75}$$

gilt und führen die Aussage zu einem Widerspruch. Für $p \le 71$ gilt $n(p) \le 11$, daher sei $p > 71$. Da $n(p) > 2$, können wir $p \equiv 7 \bmod 8$ voraussetzen.

Da $\left(\frac{2}{p}\right) = 1$ und $\left(\frac{-1}{p}\right) = -1$, ist 8 quadratischer Rest und -1 quadratischer Nichtrest modulo p. Daher sind die $n(p) - 1$ positiven ganzen Zahlen

$$p - 8(n(p) - 1),\ p - 8(n(p) - 2), \ldots, p - 8 \tag{3.76}$$

sämtlich quadratische Nichtreste, die $\equiv 7 \bmod 8$ sind.

Die Zahlen in (3.76) sind positiv, da für $p \equiv 7 \bmod 8$ und $p > 71$ nach 3.3 für $p \equiv 7 \bmod 8$ und $p > 71$ gilt

$$n(p) < \sqrt{p}.$$

Sei r eine ungerade ganze Zahl der Form

$$r = \left\lfloor p^{\frac{1}{5}} \right\rfloor + \alpha,$$

wobei α eine positive ganze Zahl ≤ 8 sein soll, die wir später wählen werden.

Aus

$$p^{\frac{1}{5}} < r \leq p^{\frac{1}{5}} + 8 \tag{3.77}$$

folgern wir mit (3.75)

$$r \leq n(p) - 1. \tag{3.78}$$

Sei nun h die einzige ganze Zahl, die die Kongruenz

$$8h \equiv 8 \cdot n(p) - p \bmod r, \qquad 1 \leq h \leq r \tag{3.79}$$

erfüllt. Dadurch können wir $k \in \mathbb{Z}$ definieren durch

$$k = \frac{p - 8 \cdot (n(p) - h)}{r}. \tag{3.80}$$

Aus (3.78) und (3.79) erhalten wir $1 \leq h \leq n(p) - 1$, was bedeutet, daß $p - 8 \cdot (n(p) - h)$ eine der Zahlen in (3.76) ist und damit k positiv ist.

Wir setzen nun $l = \left\lfloor p^{\frac{1}{5}} \right\rfloor + 4$, also gilt

$$p^{\frac{1}{5}} + 3 < l < p^{\frac{1}{5}} + 4. \tag{3.81}$$

Außerdem wählen wir

$$a = \left\lfloor \sqrt{k} \right\rfloor + 1,$$

dann ist $\sqrt{k} < a \leq \sqrt{k} + 1$ und man erhält daraus

$$(a - 1)^2 \leq k < a^2. \tag{3.82}$$

Schließlich wählen wir α so, daß

$$r \equiv 1 \bmod 8 \quad \text{falls} \quad a \equiv 0 \bmod 4 \tag{3.83}$$

und

$$r \equiv 5 \bmod 8 \quad \text{falls} \quad a \equiv 2 \bmod 4. \tag{3.84}$$

Aus (3.75), (3.77), (3.79), (3.80) und (3.81) erhalten wir

$$\begin{aligned}(k+8\cdot l-8)\cdot r &= k\cdot r+8\cdot l\cdot r-8\cdot r<p-8\cdot n\left(p\right)+8\cdot r+8\cdot r\cdot\left(p^{\frac{1}{5}}+4\right)-8\cdot r\\ &< p-8\cdot n\left(p\right)+8\cdot\left(p^{\frac{1}{5}}+8\right)\cdot\left(p^{\frac{1}{5}}+4\right)\\ &< p-8\cdot p^{\frac{2}{5}}-96\cdot p^{\frac{1}{5}}-264+8\cdot p^{\frac{2}{5}}+96\cdot p^{\frac{1}{5}}+256\\ &= p-8.\end{aligned}$$

Da also

$$(k+8\cdot l-8)\cdot r<p-8 \tag{3.85}$$

gilt, sind die ganzen Zahlen $k\cdot r,\ (k+8)\cdot r,\ldots,\ (k+8\cdot l-8)\cdot r$ unter den Zahlen in (3.75) und damit sind die l ganzen Zahlen

$$k,\ k+8,\ldots,\ k+8\cdot l-8 \tag{3.86}$$

quadratische Nichtreste.

Für den Fall, daß a gerade ist, betrachten wir die Zahlen

$$(a+1)\cdot(a-1),\ \ (a+3)\cdot(a-3),\ldots,\ \ (a+2\cdot b-1)\cdot(a-2\cdot b+1), \tag{3.87}$$

wobei b die größte ganze Zahl sein soll, so daß

$$(a+2\cdot b-1)\cdot(a-2\cdot b+1)>(a-1)^2. \tag{3.88}$$

Hieraus erhalten wir

$$\begin{aligned}&(a+2\cdot b-1)\cdot(a-2\cdot b+1) &&> &&(a-1)^2\\ \Longleftrightarrow\quad &a^2-(2\cdot b-1)^2 &&> &&a^2-2\cdot a+1\\ \Longleftrightarrow\quad &(2\cdot b-1)^2 &&< &&2\cdot a-1\\ \Longleftrightarrow\quad &2\cdot b-1 &&< &&\sqrt{2\cdot a-1}\\ \Longleftrightarrow\quad &b &&< &&\tfrac{1}{2}\sqrt{2\cdot a-1}+\tfrac{1}{2}.\end{aligned} \tag{3.89}$$

Aus $(a-1)^2\leq k<\dfrac{p}{r}<p^{\frac{4}{5}}$ folgt

$$a<p^{\frac{2}{5}}+1 \tag{3.90}$$

und mit (3.89) erhalten wir

$$a+2\cdot b-1<a+\sqrt{2\cdot a-1}<a<p^{\frac{2}{5}}+1+\sqrt{2}\cdot\left(p^{\frac{2}{5}}+1\right)<n\left(p\right), \tag{3.91}$$

was bedeutet, daß die Zahlen in (3.87) sämtlich quadratische Reste modulo p sind.

Da k quadratischer Nichtrest ist, gilt in (3.82) sogar

$$(a-1)^2<k<a^2.$$

Wegen $k\leq a^2-1$, gibt es ein $m\in\mathbb{N}$ so, daß

$$a^2-(2\cdot m+1)^2<k\leq a^2-(2\cdot m-1)^2.$$

Also ist

$$(a-1)^2 < k \leq a^2 - (2\cdot m-1)^2,$$

und somit

$$(a+2\cdot m-1)\cdot(a-2\cdot m+1) > (a-1)^2.$$

Nach Wahl von b in (3.88) erhalten wir die Ungleichung $m \leq b$.

Es ist $(2\cdot m+1)^2 \equiv (2\cdot m-1)^2 \equiv 1 \bmod 8$ und daher gilt

$$a^2-(2\cdot m+1)^2 \equiv a^2-(2\cdot m-1)^2 \equiv a^2-1 \bmod 8. \tag{3.92}$$

Die Gleichung (3.80) liefert $k\cdot r = p - 8\cdot(n(p)-h)$ und mit $p \equiv 7 \bmod 8$ folgt

$$k\cdot r \equiv -1 \bmod 8.$$

Wegen $r \equiv 1 \bmod 2$ ist $r^2 \equiv 1 \bmod 8$ und daraus folgt

$$k \equiv -r \bmod 8. \tag{3.93}$$

In (3.83) und (3.84) wurde r genau so gewählt, daß $a^2-1 \equiv -r \bmod 8$ gilt, woraus man mit (3.92) und (3.93) sofort

$$a^2-(2\cdot m+1)^2 \equiv a^2-(2\cdot m-1)^2 \equiv k \bmod 8$$

erhält. Es gibt also ein $s>0$ mit

$$k = a^2-(2\cdot m+1)^2+8\cdot s.$$

Zudem gilt natürlich

$$a^2-(2\cdot m+1)^2+8\cdot m = a^2-(2\cdot m-1)^2. \tag{3.94}$$

Wegen $k \leq a^2-(2\cdot m-1)^2$ gilt nun $s \leq m$.

Wie wir oben gezeigt haben, sind für $0 \leq j \leq l-1$ die Zahlen

$$k+8\cdot j = a^2-(2\cdot m+1)^2+8\cdot s+8\cdot j = a^2-(2\cdot m+1)^2+8\cdot(s+j)$$

quadratische Nichtreste modulo p. Da die Zahl $a^2-(2\cdot m-1)^2$ nach (3.91) quadratischer Rest modulo p ist, muß wegen (3.94) für alle $j \in \{0,\ldots,l-1\}$ die Ungleichheit $s+j \neq m$ gelten. Also ist

$$m \notin \{s, s+1, \ldots, s+l-1\}.$$

Da $s \leq m$, folgt sofort $s+l-1 < m$ und damit $s+l \leq m$. Mit $s \in \mathbb{N}$ und $m \leq b$ ergibt sich

$$1+l \leq s+l \leq m \leq b. \tag{3.95}$$

Mit (3.89) und (3.90) erhalten wir die Abschätzung

$$b < \frac{1}{2}\sqrt{2\cdot a-1}+\frac{1}{2} < \frac{1}{2}\sqrt{2\cdot p^{\frac{2}{5}}+1}+\frac{1}{2}.$$

Aus $p^{\frac{1}{5}} + 3 < l$ und $1 + l \leq b$ ergibt sich

$$p^{\frac{1}{5}} + 4 < 1 + l \leq b < \frac{1}{2}\sqrt{2 \cdot p^{\frac{2}{5}} + 1} + \frac{1}{2},$$

also

$$2 \cdot p^{\frac{1}{5}} + 7 < \sqrt{2 \cdot p^{\frac{2}{5}} + 1}.$$

Quadrieren ergibt

$$4 \cdot p^{\frac{2}{5}} + 28 \cdot p^{\frac{1}{5}} + 49 < 2 \cdot p^{\frac{2}{5}} + 1,$$

was jedoch einen Widerspruch liefert. Somit war die zu Beginn gemachte Annahme falsch und die Behauptung ist bewiesen. □

3.8 Satz von FJELLSTEDT

In seinem Artikel *"A Theorem concerning the least quadratic residue and non-residue"* [Fjel] glaubte LARS FJELLSTEDT im Jahre 1956 folgende Abschätzung für den kleinsten quadratischen Nichtrest bewiesen zu haben.

Es existiert ein $p_0 > 0$, so daß für alle Primzahlen $p > p_0$ gilt

$$n(p) < 6 \cdot \log p.$$

In den *Mathematical Reviews* [Bate] jedoch bemerkt P. Bateman schlicht: "The proof is incorrect".

Beispiele

Abschließend wollen wir in Tabelle 3.8 einige Beispiele anführen, um die erzielten Ergebnisse auch miteinander vergleichen zu können.

p	$n(p)$	Gauß-Nag.	Nag. I	Nag. II	Rédei	Stolt	Niv./Zuc./Mon.	Wed.	Brauer
$29 \equiv 5 \bmod 8$	$n(29) = 3$	11,8	7,6	5,4	5,4	3,8	6,4	6,3	19,6
$41 \equiv 1 \bmod 8$	$n(41) = 3$	13,8	6,4	4,6	6,4	–	7,4	7,3	–
$71 \equiv 7 \bmod 8$	$n(71) = 7$	17,9	10,9	8,1	8,4	–	9,4	9,3	16,3
$83 \equiv 3 \bmod 8$	$n(83) = 5$	19,2	19,2	13,1	9,1	–	10,1	10,0	27,8
$113 \equiv 1 \bmod 8$	$n(113) = 3$	22,3	10,6	7,5	10,6	–	11,6	11,5	–
$251 \equiv 3 \bmod 8$	$n(251) = 11$	32,7	32,7	19,8	15,8	–	16,8	16,8	40,7
$613 \equiv 5 \bmod 8$	$n(613) = 5$	50,5	35,0	24,8	24,8	17,5	25,8	25,7	55,9
$911 \equiv 7 \bmod 8$	$n(911) = 7$	61,4	41,7	30,1	30,2	–	31,2	31,2	34,6
$1091 \equiv 3 \bmod 8$	$n(1091) = 17$	67,1	67,1	37,0	33,0	–	34,0	34,0	68,8
$1327 \equiv 7 \bmod 8$	$n(1327) = 3$	73,9	50,5	36,3	36,4	–	37,4	37,4	38,9
$1669 \equiv 5 \bmod 8$	$n(1669) = 7$	82,7	57,8	40,9	40,9	28,9	41,9	41,8	80,4
$1993 \equiv 1 \bmod 8$	$n(1993) = 5$	90,3	44,6	31,6	44,6	–	45,6	45,6	–

Tabelle 3.8: Vergleich der oberen Schranken

Wie man sieht, wurden die Abschätzungen im Laufe der Jahre teilweise verbessert, dennoch sind sie nicht besonders scharf. Mit wachsendem p werden die Ergebnisse zunehmend schlechter. Zudem zeigt sich, daß die BRAUERSCHEN Abschätzungen im niedrigen Primzahlbereich deutlich schlechter sind als die NAGELLSCHEN Abschätzungen II.

Kapitel 4

Analytische Abschätzungen

Bessere Ergebnisse als die des vorhergehenden Kapitels liefern die analytischen Abschätzungen für den kleinsten quadratischen Nichtrest, die wir nun erläutern wollen. Wir teilen dieses Kapitel in zwei Abschnitte ein, von denen der erste die Abschätzungen enthält, die ohne die erweiterte Riemannsche Vermutung auskommen. Im zweiten Abschnitt geben wir die Aussagen an, die auf ERH basieren.

4.1 Abschätzungen ohne ERH

Gute Ergebnisse wurden schon sehr früh von Ivan M. Vinogradov erzielt. Auch D. A. Burgess gibt eine gute Schranke für den kleinsten quadratischen Nichtrest an, die sich noch mit eher einfachen Mitteln beweisen läßt.

4.1.1 Die Sätze von Vinogradov

Bereits im Jahre 1919, veröffentlicht Ivan M. Vinogradov ein schärferes Ergebnis als die bisherigen bekannten, allerdings gilt seine Abschätzung erst ab einer gewissen Schranke. Um Vinogradovs Satz beweisen zu können, müssen wir noch ein bißchen Vorarbeit leisten.

4.1.1.1 Satz von Pólya-Vinogradov

Für ungerade Primzahlen p, $m \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt

$$\left| \sum_{t=m+1}^{m+n} \left(\frac{t}{p}\right) \right| < \sqrt{p} \cdot \log p.$$

Für den Beweis benötigen wir die folgenden Lemmata.

Lemma 1

Für ganze Zahlen x und t gilt

$$\sum_{a=0}^{p-1} e^{2\pi i \cdot \frac{x-t}{p} \cdot a} = \begin{cases} 0 & \text{für } x \not\equiv t \bmod p, \\ p & \text{für } x \equiv t \bmod p. \end{cases}$$

Beweis:
Für $x \not\equiv t \bmod p$ ist $\dfrac{x-t}{p} \notin \mathbb{Z}$ und damit $e^{2\pi i \cdot \frac{x-t}{p}} \neq 1$, also gilt

$$\sum_{a=0}^{p-1} e^{2\pi i \cdot \frac{x-t}{p} \cdot a} = \frac{\overbrace{e^{2\pi i \cdot \frac{x-t}{p} \cdot p}}^{=1} - 1}{e^{2\pi i \cdot \frac{x-t}{p}} - 1} = 0.$$

Ist $x \equiv t \bmod p$, so gilt $e^{2\pi i \cdot \frac{x-t}{p}} = 1$ und damit

$$\sum_{a=0}^{p-1} e^{2\pi i \cdot \frac{x-t}{p} \cdot a} = p,$$

was wir zeigen wollten. □

Lemma 2

Für $0 \leq x \leq \dfrac{1}{2}$ gilt

$$\sin(\pi x) \geq 2x.$$

Beweis:
Wir betrachten die Funktion $f(x) = \sin(\pi x) - 2x$. Dann haben wir

$$f'(x) = \pi \cdot \cos(\pi x) - 2, \quad f''(x) = -\pi^2 \cdot \sin(\pi x), \quad f(0) = f\left(\frac{1}{2}\right) = 0.$$

Im Inneren des Intervalls $\left[0, \dfrac{1}{2}\right]$ ist $f''(x) < 0$, d. h. daß $f'(x)$ dort streng monoton fallend ist. Somit kann die Funktion $f(x)$ hier kein lokales Minimum besitzen, also sind höchstens 0 und $\dfrac{1}{2}$ Minima. Dies impliziert sofort $f(x) \geq 0$, woraus die Behauptung folgt. □

Lemma 3

Für $x \geq 1$ gilt

$$\frac{1}{x} < \log \frac{2x+1}{2x-1}.$$

Beweis:

Wegen $1 < \log 3 \approx 1,099$ stimmt die Behauptung für $x = 1$.

Sei nun $f(x) = x \cdot \log \dfrac{2x+1}{2x-1}$. Wir berechnen wieder die Ableitungsfunktionen

$$f'(x) = \log \frac{2x+1}{2x-1} - \frac{4x}{(2x+1)\cdot(2x-1)}, \qquad f''(x) = \frac{8}{(2x+1)^2 \cdot (2x-1)^2}.$$

Es ist

$$f'(1) = \log 3 - \frac{4}{3} \approx -0,23 \quad \text{und} \quad \lim_{x\to\infty} f'(x) = 0. \tag{4.1}$$

Da $f''(x) > 0$ gilt, ist $f'(x)$ streng monoton steigend, was wegen (4.1) insbesondere $f'(x) < 0$ impliziert. Somit ist $f(x)$ streng monoton fallend. Wir substituieren $x = \dfrac{1}{t}$ und erhalten mit der Regel von de l'Hospital

$$\begin{aligned} \lim_{x\to\infty} f(x) &= \lim_{x\to\infty} x \cdot \log \frac{2x+1}{2x-1} = \lim_{t\to 0} \frac{\log \frac{2+t}{2-t}}{t} \\ &= \frac{\lim\limits_{t\to 0} \frac{4}{(2+t)\cdot(2-t)}}{\lim\limits_{t\to 0} 1} = 1. \end{aligned}$$

Somit gilt für $x > 1$ die Ungleichung $x \cdot \log \dfrac{2x+1}{2x-1} > 1$ und daraus folgt die Behauptung. □

Beweis des Satzes von PÓLYA-VINOGRADOV:

Mit Lemma 1 erhalten wir

$$\sum_{t=0}^{p-1} \sum_{a=0}^{p-1} \left(\frac{t}{p}\right) \cdot e^{2\pi i \cdot \frac{x-t}{p} \cdot a} = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \cdot \sum_{a=0}^{p-1} e^{2\pi i \cdot \frac{x-t}{p} \cdot a} = \sum_{t=0,\ t\equiv x \bmod p}^{p-1} \left(\frac{t}{p}\right) \cdot p = \left(\frac{x}{p}\right) \cdot p.$$

Damit ergibt sich nun

$$\begin{aligned} \sum_{t=m+1}^{m+n} \left(\frac{t}{p}\right) &= \sum_{x=m+1}^{m+n} \left(\frac{x}{p}\right) = \frac{1}{p} \sum_{x=m+1}^{m+n} \sum_{t=0}^{p-1} \sum_{a=0}^{p-1} \left(\frac{t}{p}\right) \cdot e^{2\pi i \cdot \frac{x-t}{p} \cdot a} \\ &= \frac{1}{p} \sum_{a=0}^{p-1} \sum_{x=m+1}^{m+n} \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \cdot e^{2\pi i \cdot \frac{x-t}{p} \cdot a} = \frac{1}{p} \sum_{a=0}^{p-1} \sum_{x=m+1}^{m+n} \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \cdot e^{2\pi i \cdot \frac{x-t}{p} \cdot a} \\ &= \frac{1}{p} \sum_{a=0}^{p-1} \sum_{x=m+1}^{m+n} e^{2\pi i \cdot a \cdot \frac{x}{p}} \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \cdot e^{-2\pi i \cdot a \cdot \frac{t}{p}}. \end{aligned} \tag{4.2}$$

Nun betrachten wir die sogenannte GAUSSsche Summe

$$S(a,p) = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \cdot e^{-2\pi i \cdot a \cdot \frac{t}{p}}.$$

Da es genausoviele Quadrate wie Nichtquadrate modulo p gibt, gilt

$$S(0,p) = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) = 0.$$

Für $1 \leq a \leq p-1$ gilt

$$S(a,p)^2 = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \cdot e^{-2\pi i \cdot a \cdot \frac{x}{p}} \cdot \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \cdot e^{-2\pi i \cdot a \cdot \frac{y}{p}}.$$

Wenn man für y einen anderen Repräsentanten von $y \bmod p$ wählt, dann ändert sich $\left(\frac{y}{p}\right) \cdot e^{-2\pi i \cdot a \cdot \frac{y}{p}}$ nicht. Wegen $\{y \bmod p : y = 1, \ldots, p-1\} = \{x \cdot y \bmod p : y = 1, \ldots, p-1\}$ können wir statt y also auch $x \cdot y$ einsetzen. Wir erhalten dann

$$\begin{aligned}
S(a,p)^2 &= \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \cdot e^{-2\pi i \cdot a \cdot \frac{x}{p}} \cdot \sum_{y=1}^{p-1} \left(\frac{x \cdot y}{p}\right) \cdot e^{-2\pi i \cdot a \cdot \frac{x \cdot y}{p}} \\
&= \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left(\frac{x^2 \cdot y}{p}\right) \cdot e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p}} = \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \cdot e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p}} \\
&= \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \sum_{x=1}^{p-1} e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p}} \\
&= \sum_{y=1}^{p-2} \left(\frac{y}{p}\right) \sum_{x=1}^{p-1} e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p}} + \left(\frac{p-1}{p}\right) \cdot (p-1) \\
&= \sum_{y=1}^{p-2} \left(\frac{y}{p}\right) \left(\sum_{x=0}^{p-1} e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p}} - 1 \right) + \left(\frac{p-1}{p}\right) \cdot (p-1) \\
&= \sum_{y=1}^{p-2} \left(\frac{y}{p}\right) \cdot \left(\frac{e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p} \cdot p} - 1}{e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p}} - 1} - 1 \right) + \left(\frac{p-1}{p}\right) \cdot (p-1) \\
&= \sum_{y=1}^{p-2} \left(\frac{y}{p}\right) \cdot \left(\frac{e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p} \cdot p} - e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p}}}{e^{-2\pi i \cdot a \cdot \frac{x(1+y)}{p}} - 1} \right) + \left(\frac{p-1}{p}\right) \cdot (p-1) \\
&= \sum_{y=1}^{p-2} \left(\frac{y}{p}\right) \cdot (-1) + \left(\frac{p-1}{p}\right) \cdot (p-1) \\
&= \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) \cdot (-1) + \left(\frac{p-1}{p}\right) + \left(\frac{p-1}{p}\right) \cdot (p-1) \\
&= -\sum_{y=1}^{p-1} \left(\frac{y}{p}\right) + \left(\frac{-1}{p}\right) \cdot p = \left(\frac{-1}{p}\right) \cdot p.
\end{aligned}$$

Es folgt also im Fall $a \not\equiv 0 \bmod p$:

$$S(a,p) = \begin{cases} \pm\sqrt{p} & \text{für } p \equiv 1 \bmod 4, \\ \pm i\sqrt{p} & \text{für } p \equiv 3 \bmod 4, \end{cases}$$

also gilt in jedem Fall

$$|S(a,p)| = \sqrt{p}. \tag{4.3}$$

Damit können wir (4.2) umformulieren und erhalten

$$\begin{aligned}
\sum_{t=m+1}^{m+n}\left(\frac{t}{p}\right) &= \frac{1}{p}\sum_{a=0}^{p-1}\sum_{x=m+1}^{m+n} e^{2\pi i\cdot a\cdot\frac{x}{p}}\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)\cdot e^{-2\pi i\cdot a\cdot\frac{t}{p}} \\
&= \frac{1}{p}\sum_{a=0}^{p-1}\sum_{x=m+1}^{m+n} e^{2\pi i\cdot a\cdot\frac{x}{p}}\cdot S(a,p) = \frac{1}{p}\sum_{a=1}^{p-1}\sum_{x=m+1}^{m+n} e^{2\pi i\cdot a\cdot\frac{x}{p}}\cdot S(a,p),
\end{aligned}$$

und mit (4.3) folgt

$$\begin{aligned}
\left|\sum_{t=m+1}^{m+n}\left(\frac{t}{p}\right)\right| &= \left|\frac{1}{p}\sum_{a=1}^{p-1}\sum_{x=m+1}^{m+n} e^{2\pi i\cdot a\cdot\frac{x}{p}}\cdot S(a,p)\right| \le \frac{1}{p}\sum_{a=1}^{p-1}\left|\sum_{x=m+1}^{m+n} e^{2\pi i\cdot a\cdot\frac{x}{p}}\right|\cdot|S(a,p)| \\
&= \frac{1}{p}\sum_{a=1}^{p-1}\left|\sum_{x=m+1}^{m+n} e^{2\pi i\cdot a\cdot\frac{x}{p}}\right|\cdot\sqrt{p} = \frac{1}{\sqrt{p}}\sum_{a=1}^{p-1}\left|\sum_{x=m+1}^{m+n} e^{2\pi i\cdot a\cdot\frac{x}{p}}\right| \\
&= \frac{1}{\sqrt{p}}\sum_{a=1}^{p-1}\left|\sum_{x=0}^{n-1} e^{2\pi i\cdot a\cdot\frac{(m+1+x)}{p}}\right| = \frac{1}{\sqrt{p}}\sum_{a=1}^{p-1} e^{2\pi i\cdot a\cdot\frac{m+1}{p}}\left|\sum_{x=0}^{n-1} e^{2\pi i\cdot a\cdot\frac{x}{p}}\right| \\
&= \frac{1}{\sqrt{p}}\sum_{a=1}^{p-1}\left|\sum_{x=0}^{n-1} e^{2\pi i\cdot a\cdot\frac{x}{p}}\right| = \frac{1}{\sqrt{p}}\sum_{a=1}^{p-1}\left|\frac{e^{2\pi i\cdot a\cdot\frac{n}{p}}-1}{e^{2\pi i\cdot\frac{a}{p}}-1}\right| \\
&= \frac{1}{\sqrt{p}}\sum_{a=1}^{p-1}\left|\frac{\frac{e^{\pi i\cdot a\cdot\frac{n}{p}}\left(e^{\pi i\cdot a\cdot\frac{n}{p}}-e^{-\pi i\cdot a\cdot\frac{n}{p}}\right)}{2i}}{\frac{e^{\pi i\cdot\frac{a}{p}}\left(e^{\pi i\cdot\frac{a}{p}}-e^{-\pi i\cdot\frac{a}{p}}\right)}{2i}}\right| = \frac{1}{\sqrt{p}}\sum_{a=1}^{p-1}\left|\frac{\sin\left(\frac{\pi a n}{p}\right)}{\sin\left(\frac{\pi a}{p}\right)}\right| \\
&\le \frac{1}{\sqrt{p}}\sum_{a=1}^{p-1}\frac{1}{\left|\sin\left(\frac{\pi a}{p}\right)\right|} = \frac{1}{\sqrt{p}}\sum_{a=1}^{p-1}\frac{1}{\sin\left(\frac{\pi a}{p}\right)} \\
&= \frac{1}{\sqrt{p}}\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{1}{\sin\left(\frac{\pi a}{p}\right)}+\frac{1}{\sin\left(\frac{\pi\cdot(p-a)}{p}\right)}\right) \\
&= \frac{1}{\sqrt{p}}\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{1}{\sin\left(\frac{\pi a}{p}\right)}+\frac{1}{\sin\left(\pi-\frac{\pi a}{p}\right)}\right) = \frac{2}{\sqrt{p}}\sum_{a=1}^{\frac{p-1}{2}}\frac{1}{\sin\left(\frac{\pi a}{p}\right)}.
\end{aligned}$$

Mit Lemma 2 und Lemma 3 erhalten wir nun

$$\begin{aligned}
\left|\sum_{t=m+1}^{m+n}\left(\frac{t}{p}\right)\right| &\le \frac{2}{\sqrt{p}}\sum_{a=1}^{\frac{p-1}{2}}\frac{1}{\sin\left(\frac{\pi a}{p}\right)} \le \frac{2}{\sqrt{p}}\sum_{a=1}^{\frac{p-1}{2}}\frac{1}{\frac{2a}{p}} = \sqrt{p}\sum_{a=1}^{\frac{p-1}{2}}\frac{1}{a} \\
&< \sqrt{p}\sum_{a=1}^{\frac{p-1}{2}}\log\frac{2a+1}{2a-1} = \sqrt{p}\cdot\log\left(\prod_{a=1}^{\frac{p-1}{2}}\frac{2a+1}{2a-1}\right) \\
&= \sqrt{p}\cdot\log\left(\frac{3}{1}\cdot\frac{5}{3}\cdot\frac{7}{5}\cdot\ldots\cdot\frac{p-2}{p-4}\cdot\frac{p}{p-2}\right) = \sqrt{p}\cdot\log p,
\end{aligned}$$

was wir zeigen wollten. □

Folgerung

Sei $p \in \mathbb{P}$ eine ungerade Primzahl, $m \in \mathbb{Z}$ mit $0 < m < p$ und R_m bzw. N_m die Anzahl der quadratischen Reste bzw. Nichtreste modulo p zwischen 1 und m. Dann gilt

$$\left| R_m - \frac{1}{2} \cdot m \right| = \left| N_m - \frac{1}{2} \cdot m \right| < \frac{1}{2} \cdot \sqrt{p} \cdot \log p. \tag{4.4}$$

Beweis:

Jede natürliche Zahl zwischen 1 und $p-1$ ist quadratischer Rest oder quadratischer Nichtrest modulo p. Daher gilt

$$R_m + N_m = m.$$

Ist x eine natürliche Zahl zwischen 1 und $p-1$, dann ist

$$\frac{1}{2} \cdot \left(1 + \left(\frac{x}{p}\right)\right) = \begin{cases} 1, & \text{falls } x \text{ quadratischer Rest ist,} \\ 0, & \text{falls } x \text{ quadratischer Nichtrest ist.} \end{cases}$$

Daraus erhält man

$$R_m = \sum_{x=1}^{m} \frac{1}{2} \cdot \left(1 + \left(\frac{x}{p}\right)\right) = \frac{1}{2} \cdot m + \frac{1}{2} \cdot \sum_{x=1}^{m} \left(\frac{x}{p}\right)$$

und

$$N_m = m - R_m = \frac{1}{2} \cdot m - \frac{1}{2} \cdot \sum_{x=1}^{m} \left(\frac{x}{p}\right).$$

Mit der Ungleichung von PÓLYA-VINOGRADOV folgt

$$\left| R_m - \frac{1}{2} \cdot m \right| = \left| N_m - \frac{1}{2} \cdot m \right| = \frac{1}{2} \cdot \left| \sum_{x=1}^{m} \left(\frac{x}{p}\right) \right| < \frac{1}{2} \cdot \sqrt{p} \cdot \log p$$

und damit die Behauptung. □

Folgerung

Sei p eine ungerade Primzahl, $u \in \mathbb{R}$ mit $1 < u < p$ und N_u die Anzahl der quadratischen Nichtreste modulo p zwischen 1 und u. Dann gilt

$$N_u > \frac{u - 1 - \sqrt{p} \cdot \log p}{2}.$$

Beweis:

Wir benutzen die letzte Folgerung und erhalten

$$N_u = N_{\lfloor u \rfloor} > \frac{\lfloor u \rfloor}{2} - \frac{\sqrt{p} \cdot \log p}{2} = \frac{u - (u - \lfloor u \rfloor) - \sqrt{p} \cdot \log p}{2} > \frac{u - 1 - \sqrt{p} \cdot \log p}{2},$$

was wir zeigen wollten. □

4.1.1.2 Satz von VINOGRADOV

Für hinreichend große Primzahlen p gilt für den kleinsten quadratischen Nichtrest modulo p die Ungleichung

$$n^*(p) < p^{\frac{1}{2\sqrt{e}}} \cdot (\log p)^2 .$$

Beweis:

Wir führen die Bezeichnungen

$$\begin{aligned} \delta &= \frac{1}{2\sqrt{e}} \approx 0,03, \\ u &= p^{\frac{1}{2\sqrt{e}}} \cdot (\log p)^2 , \\ v &= p^{\frac{1}{2}} \cdot (\log p)^2 \end{aligned}$$

ein und setzen $p \geq 5507$ voraus. Dann gilt $1 < u < v < p$.

Wir nehmen an, daß alle natürlichen Zahlen $1,\ 2,\ 3, \ldots,\ \lfloor u \rfloor$ quadratische Reste modulo p sind und wollen diese Annahme zum Widerspruch führen.

Sei q eine Primzahl. Es gibt genau $\left\lfloor \frac{v}{q} \right\rfloor$ natürliche Zahlen $\leq v$, die q als Teiler haben, nämlich $q,\ 2 \cdot q,\ 3 \cdot q, \ldots,\ \left\lfloor \frac{v}{q} \right\rfloor \cdot q$. Ist nun $x \in \mathbb{N},\ x \leq v$ ein quadratischer Nichtrest modulo p, dann besitzt x einen Primteiler $q \leq v$, der ebenfalls quadratischer Nichrest modulo p ist. Wegen unserer Annahme gilt $u < q$. Man kann also die Anzahl der quadratischen Nichtreste modulo p, die $\leq v$ sind durch

$$N_v \leq \sum_{u < q \leq v} \left\lfloor \frac{v}{q} \right\rfloor$$

abschätzen, wobei q nur Primzahlen durchläuft. Weiterhin gilt

$$N_v \leq \sum_{u < q \leq v} \frac{v}{q} = v \cdot \left(\sum_{q \leq v} \frac{1}{q} - \sum_{q \leq u} \frac{1}{q} \right),$$

also

$$\frac{N_v}{v} \leq \sum_{q \leq v} \frac{1}{q} - \sum_{q \leq u} \frac{1}{q}. \tag{4.5}$$

Im Zusammenhang mit dem Primzahlsatz bewies MERTENS, daß es eine reelle Zahl A und eine beschränkte reelle Funktion $c(x)$ gibt, sodaß für reelle $x \geq 2$ die Gleichung

$$\sum_{q \leq x} \frac{1}{q} = \log\log x + A + \frac{c(x)}{\log x} \tag{4.6}$$

gilt. Sei nun c eine positive reelle Zahl, die für alle x die Ungleichung $|c(x)| \leq c$ erfüllt.

Damit und mit (4.5) erhält man (im Fall $\log\log p \geq 0$)

$$\begin{aligned}\frac{N_v}{v} &\leq \log\log v - \log\log u + \frac{c\,(v)}{\log v} - \frac{c\,(u)}{\log u} \leq \log\log v - \log\log u + \frac{c}{\log v} - \frac{c}{\log u} \\ &\leq \log\log v - \log\log u + \frac{2\cdot c}{\log u} = \log\log v - \log\log u + \frac{2\cdot c}{\delta\cdot\log p + 2\cdot\log\log p} \\ &\leq \log\log v - \log\log u + \frac{2\cdot c}{\delta\cdot\log p} = \log\log v - \log\log u + \frac{4\sqrt{e}\cdot c}{\log p}. \qquad (4.7)\end{aligned}$$

Außerdem gilt

$$\begin{aligned}\log\log v - \log\log u &= \log\frac{\log v}{\log u} = \log\frac{\frac{1}{2}\cdot\log p + 2\cdot\log\log p}{\delta\cdot\log p + 2\cdot\log\log p} \\ &= \log\frac{\frac{1}{2}\cdot\log p + 2\cdot\log\log p}{\frac{1}{2\sqrt{e}}\cdot\log p + 2\cdot\log\log p} = \log\frac{\sqrt{e}\cdot(\log p + 4\cdot\log\log p)}{\log p + 4\sqrt{e}\cdot\log\log p} \\ &= \frac{1}{2} + \log\frac{\log p + 4\cdot\log\log p}{\log p + 4\sqrt{e}\cdot\log\log p} = \frac{1}{2} + \log\frac{1 + 4\cdot\frac{\log\log p}{\log p}}{1 + 4\sqrt{e}\cdot\frac{\log\log p}{\log p}} \\ &= \frac{1}{2} + \log\left(1 + 4\cdot\frac{\log\log p}{\log p}\right) - \log\left(1 + 4\sqrt{e}\cdot\frac{\log\log p}{\log p}\right). \qquad (4.8)\end{aligned}$$

Wir benutzen nun die Ungleichung $x - \frac{1}{2}x^2 \leq \log(1+x) \leq x$, die für reelle $x \geq 0$ gilt und erhalten mit (4.7) und (4.8)

$$\begin{aligned}\frac{N_v}{v} &\leq \frac{1}{2} + \log\left(1 + 4\cdot\frac{\log\log p}{\log p}\right) - \log\left(1 + 4\sqrt{e}\cdot\frac{\log\log p}{\log p}\right) + \frac{4\sqrt{e}\cdot c}{\log p} \\ &\leq \frac{1}{2} + 4\cdot\frac{\log\log p}{\log p} - 4\sqrt{e}\cdot\frac{\log\log p}{\log p} + \frac{1}{2}\cdot\left(4\sqrt{e}\cdot\frac{\log\log p}{\log p}\right)^2 + \frac{4\sqrt{e}\cdot c}{\log p} \\ &= \frac{1}{2} - 4\cdot\left(\sqrt{e} - 1\right)\cdot\frac{\log\log p}{\log p} + 8\cdot e\cdot\frac{(\log\log p)^2}{(\log p)^2} + \frac{4\sqrt{e}\cdot c}{\log p}. \qquad (4.9)\end{aligned}$$

Da die Ungleichung $(\log\log p)^2 \leq \log p$ gilt, läßt sich (4.9) umformen zu

$$\frac{N_v}{v} \leq \frac{1}{2} - 4\cdot\left(\sqrt{e} - 1\right)\cdot\frac{\log\log p}{\log p} + \frac{8\cdot e + 4\sqrt{e}\cdot c}{\log p}. \qquad (4.10)$$

Andererseits gilt nach der zweiten Folgerung die Abschätzung

$$N_v > \frac{v - 1 - \sqrt{p}\cdot\log p}{2}$$

und damit

$$\frac{N_v}{v} > \frac{1}{2} - \frac{1 + \sqrt{p}\cdot\log p}{2\cdot v} = \frac{1}{2} - \frac{1 + \sqrt{p}\cdot\log p}{2\cdot\sqrt{p}\cdot(\log p)^2}.$$

Mit der Ungleichung $\dfrac{1 + \sqrt{p}\cdot\log p}{2\cdot\sqrt{p}\cdot(\log p)^2} < \dfrac{1}{\log p}$ ergibt sich daraus

$$\frac{N_v}{v} > \frac{1}{2} - \frac{1}{\log p}. \qquad (4.11)$$

Nun setzen wir die Ungleichungen (4.10) und (4.11) zusammen und erhalten

$$\frac{1}{2} - \frac{1}{\log p} < \frac{N_v}{v} \leq \frac{1}{2} - 4 \cdot \left(\sqrt{e} - 1\right) \cdot \frac{\log\log p}{\log p} + \frac{8 \cdot e + 4\sqrt{e} \cdot c}{\log p}.$$

Daraus folgt

$$4 \cdot \left(\sqrt{e} - 1\right) \cdot \frac{\log\log p}{\log p} < \frac{1 + 8 \cdot e + 4\sqrt{e} \cdot c}{\log p}$$

und schließlich

$$4 \cdot \left(\sqrt{e} - 1\right) \cdot \log\log p < 1 + 8 \cdot e + 4\sqrt{e} \cdot c,$$

was für hinreichend große Primzahlen p einen Widerspruch liefert. Daher war unsere Annahme, daß alle Zahlen $1,\ 2,\ 3, \ldots,\ \lfloor u \rfloor$ quadratische Reste modulo p sind, falsch und wir haben die Behauptung bewiesen. □

4.1.1.3 Verallgemeinerung von VINOGRADOV

Einige Jahre später, 1926, verallgemeinert VINOGRADOV seine Abschätzung auf Nichtreste n-ten Grades und beweist in [Vin] folgende Aussage.

Satz

Ist p eine Primzahl und $n \neq 1$ ein Teiler von $p - 1$, dann ist der kleinste Nichtrest n-ten Grades modulo p kleiner als

$$p^{\frac{1}{2k}} (\log p)^2, \quad \textit{mit} \quad k = e^{\frac{n-1}{n}},$$

für alle hinreichend großen Werte von p.

4.1.2 Abschätzung von BURGESS

Aufbauend auf VINOGRADOVS Idee veröffentlichte D. A. BURGESS 1957 in der Zeitschrift *Mathematika* einen Artikel, in dem er mit ähnlichen Mitteln eine bessere Abschätzung bewies. Zunächst geben wir jedoch einen Satz an, den wir später benötigen werden. Auf den Beweis wird verzichtet, er findet sich in [Bur].

Satz

Zu $\delta > 0$ und $\varepsilon > 0$ existiert ein $p_1(\delta, \varepsilon)$, sodaß für alle Primzahlen $p \geq p_1(\delta, \varepsilon)$ die Ungleichung

$$\left| \sum_{n=1}^{H} \left(\frac{n}{p}\right) \right| < \varepsilon \cdot H \quad \textit{für alle} \quad H > p^{\frac{1}{4}+\delta} \tag{4.12}$$

erfüllt ist.

4.1.2.1 Satz von Burgess

Für hinreichend große Primzahlen p gilt für den kleinsten quadratischen Nichtrest modulo p

$$n^*(p) = O\left(p^{\alpha}\right)$$

für alle $\alpha > \dfrac{1}{4\sqrt{e}}$.

Beweis:

Für den Beweis benutzen wir den vorangegangenen Satz. Sei also ein $\varepsilon > 0$ gegeben. O.B.d.A. können wir $\varepsilon < 1$ voraussetzen. Nun wählen wir ein δ, das den Ungleichungen

$$0 < \delta < \frac{1}{4} \quad \text{und} \quad \log(1 + 8 \cdot \delta) < \frac{\varepsilon}{4}$$

genügt. Es ist

$$p^{\frac{1}{4}+2\cdot\delta} - p^{\frac{1}{4}+\delta} = p^{\frac{1}{4}+\delta}\left(p^{\delta} - 1\right).$$

Dann gibt es ein $p_2(\delta)$ so, daß für alle Primzahlen $p \geq p_2(\delta)$ eine natürliche Zahl $H = H(p)$ existiert mit

$$p^{\frac{1}{4}+\delta} < H(p) < p^{\frac{1}{4}+2\cdot\delta}.$$

Wir schreiben

$$H = p^{\frac{1}{4}+\delta'(p)} \quad \text{mit} \quad \delta < \delta'(p) < 2 \cdot \delta.$$

Da wir $\delta < \dfrac{1}{4}$ gewählt haben, ist $H < p^{\frac{1}{4}+\frac{1}{2}} < p$.

Außerdem gilt $n^*(p) < H$, da sonst $\left(\dfrac{n}{p}\right) = 1$ für alle n mit $1 \leq n \leq H$ folgen würde und damit die Ungleichung (4.12) den Widerspruch $H < \varepsilon \cdot H$ liefern würde.

Wir definieren nun die Mengen

$$\begin{aligned} A &= \left\{ n \in \mathbb{N} : 1 \leq n \leq H, \left(\frac{n}{p}\right) = -1 \right\}, \\ B &= \left\{ n \in \mathbb{N} : 1 \leq n \leq H,\ n \text{ hat Primteiler } q \text{ mit } n^*(p) \leq q \leq H \right\}, \\ B_q &= \left\{ n \in \mathbb{N} : 1 \leq n \leq H, q \mid n \right\} \text{ für eine Primzahl } q. \end{aligned}$$

Es gilt

$$A \subseteq B, \tag{4.13}$$

denn ist $n \in A$, so besitzt n einen Primteiler q mit $\left(\dfrac{q}{p}\right) = -1$, was nach Voraussetzung $n^*(p) \leq q \leq H$ impliziert, und daraus folgt $n \in B$.

Natürlich gilt

$$B = \bigcup_{\substack{n^*(p) \leq q \leq H, \\ q \text{ prim}}} B_q. \tag{4.14}$$

Außerdem gilt

$$B_q = \left\{ q, 2 \cdot q, 3 \cdot q, \ldots, \left\lfloor \frac{H}{q} \right\rfloor \cdot q \right\}$$

und damit ist

$$\#B_q = \left\lfloor \frac{H}{q} \right\rfloor \leq \frac{H}{q}.$$

Mit (4.13) und (4.14) erhalten wir daraus

$$\begin{aligned} \#A &\leq \#B \leq \sum_{n^*(p) \leq q \leq H} \#B_q \leq \sum_{n^*(p) \leq q \leq H} \frac{H}{q} = H \cdot \sum_{n^*(p) \leq q \leq H} \frac{1}{q} \\ &= H \cdot \left(\sum_{q \leq H} \frac{1}{q} - \sum_{q \leq n^*(p)} \frac{1}{q} + \frac{1}{n^*(p)} \right). \end{aligned}$$

Mit (4.6) ergibt sich wie im Beweis von VINOGRADOV

$$\begin{aligned} \#A &\leq H \cdot \left(\sum_{q \leq H} \frac{1}{q} - \sum_{q \leq n^*(p)} \frac{1}{q} + \frac{1}{n^*(p)} \right) \\ &= H \cdot \left(\log\log H + \frac{c(H)}{\log H} - \log\log n^*(p) - \frac{c(n^*(p))}{\log n^*(p)} + \frac{1}{n^*(p)} \right) \\ &\leq H \cdot \left(\log\log H - \log\log n^*(p) + \frac{c}{\log H} + \frac{c}{\log n^*(p)} + \frac{1}{n^*(p)} \right) \\ &\leq H \cdot \left(\log\log H - \log\log n^*(p) + \frac{2 \cdot c + 1}{\log n^*(p)} \right). \end{aligned} \tag{4.15}$$

Es gilt nun mit $H < p$ und mit (4.15)

$$\begin{aligned} \sum_{n=1}^{H} \left(\frac{n}{p} \right) &= H - 2 \cdot \#A \\ &\geq H - 2 \cdot H \cdot \left(\log\log H - \log\log n^*(p) + \frac{2 \cdot c + 1}{\log n^*(p)} \right) \\ &= H \cdot \left[1 - 2 \cdot \left(\log\log H - \log\log n^*(p) + \frac{2 \cdot c + 1}{\log n^*(p)} \right) \right]. \end{aligned}$$

Mit dem vorherigen Satz erhalten wir nun

$$\begin{aligned} \varepsilon &> \frac{1}{H} \cdot \left| \sum_{n=1}^{H} \left(\frac{n}{p} \right) \right| \geq \frac{1}{H} \cdot \sum_{n=1}^{H} \left(\frac{n}{p} \right) = 1 - 2 \cdot \frac{\#A}{H} \\ &\geq 1 - 2 \cdot \left(\log\log H - \log\log n^*(p) + \frac{2 \cdot c + 1}{\log n^*(p)} \right) \end{aligned}$$

und damit

$$\log\log H - \log\log n^*(p) + \frac{2 \cdot c + 1}{\log n^*(p)} > \frac{1}{2} \cdot (1 - \varepsilon).$$

Nun setzen wir $n^*(p) = H^{\frac{1}{\beta}}$ und damit ist

$$\log\log H - \log\log H^{\frac{1}{\beta}} + \frac{2\cdot c+1}{\log n^*(p)} = \log\frac{\log H}{\log H^{\frac{1}{\beta}}} + \frac{2\cdot c+1}{\log n^*(p)} = \log\beta + \frac{2\cdot c+1}{\log n^*(p)}$$

also

$$\log\beta + \frac{2\cdot c+1}{\log n^*(p)} > \frac{1}{2}\cdot(1-\varepsilon)$$

und somit

$$\log\beta > \frac{1}{2} - \varepsilon.$$

Daraus folgt nun

$$\beta > e^{\frac{1}{2}-\varepsilon},$$

also insbesondere

$$\beta \geq \sqrt{e}.$$

Unsere Wahl von $H = p^{\frac{1}{4}+\delta'(p)}$ liefert uns nun

$$\begin{aligned} n^*(p) &= H^{\frac{1}{\beta}} = \left(p^{\frac{1}{4}+\delta'(p)}\right)^{\frac{1}{\beta}} \\ &\leq \left(p^{\frac{1}{4}+\delta'(p)}\right)^{\frac{1}{\sqrt{e}}} = p^{\frac{1}{4\sqrt{e}}+\frac{\delta'(p)}{\sqrt{e}}}, \end{aligned}$$

somit ist $n^*(p) = O(p^\alpha)$ für alle $\alpha > \dfrac{1}{4\sqrt{e}}$, was wir zeigen wollten. □

4.2 Abschätzungen mit ERH

Unter Annahme von ERH erreichten NESMITH ANKENY und ERIC BACH sehr gute Ergebnisse, die wir nun in diesem Abschnitt angeben wollen. In seiner Dissertation bewies auch SEBASTIAN WEDENIWSKI eine Abschätzung zum kleinsten quadratischen Nichtrest, die die Gültigkeit der ERH voraussetzt. Auf Beweise wird hier verzichtet, wir wollen aber am Ende des Abschnitts zeigen, wie man aus einem Primzahlsatz fast die Abschätzung von ANKENY erhält.

4.2.1 Einführung

Definition

Eine zahlentheoretische Funktion χ mit komplexen Werten heißt ein ***Charakter modulo*** *n, wenn gilt*

$$\begin{aligned} \chi(a) &= \chi(b),\ \textit{falls } a \equiv b \bmod n, \\ \chi(a\cdot b) &= \chi(a)\cdot\chi(b)\ \textit{für alle } a,b\in\mathbb{N}, \\ \chi(a) &= 0,\ \textit{falls } ggT(a,n) \neq 1, \\ \chi(a) &\neq 0,\ \textit{falls } ggT(a,n) = 1. \end{aligned}$$

Der Charakter χ_1 mit $\chi_1(a) = 1$ für alle $a \in \mathbb{N}$ mit $ggT(a,n) = 1$ heißt ***Hauptcharakter*** *mod n. χ heißt* ***von ψ induziert****, wenn $\chi(a) = \chi_1(a) \cdot \psi(a)$, wobei ψ ein Charakter mod r und r ein Teiler von n ist. χ heißt* ***primitiver Charakter****, wenn χ nicht von einem anderen Charakter mit kleinerem Modul induziert wird. Also wird jeder Charakter von einem primitiven Charakter induziert.*

Eigenschaften von Charakteren

Da χ vollständig multiplikativ ist und χ nicht die Nullfunktion ist, folgt daraus $\chi(1) = 1$. Mit dem Satz von EULER-FERMAT erhält man

$$\chi(a)^{\varphi(n)} = \chi\left(a^{\varphi(n)}\right) = \chi(1) = 1 \text{ für } \mathrm{ggT}(a,n) = 1,$$

also ist $\chi(a)$ für $\mathrm{ggT}(a,n) = 1$ eine $\varphi(n)$-te Einheitswurzel.

Definition

Eine Reihe der Form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

wobei $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen ist und $s \in \mathbb{C}$ mit $s = \sigma + it$, heißt **DIRICHLET-*Reihe***.

Beispiele

1. Die **RIEMANNSCHE ZETAFUNKTION** $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ konvergiert für $\mathrm{Re}\, s > 1$. BERNHARD RIEMANN findet 1859 eine Fortsetzung von $\zeta(s)$ in die gesamte komplexe Ebene. Bei $s = 1$ hat ζ einen Pol erster Ordnung vom Residuum 1. In $\mathrm{Re}\, s < 0$ sind $-2,\ -4,\ -6, \ldots$ Nullstellen erster Ordnung. Für reelle $s \in [0,1)$ ist $\zeta(s) < 0$. RIEMANN definiert die Funktion

   $$\xi(s) := \frac{s}{2}(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

   Anstelle von ξ arbeitet er jedoch mit der Funktion $\xi\left(\frac{1}{2} + it\right)$ und bemerkt 1859, daß alle nicht-trivialen Nullstellen von ξ, und damit auch von ζ, auf der Geraden $\mathrm{Re}(s) = \frac{1}{2}$ liegen. Diese Bemerkung ist in dieser Form als **RIEMANNSCHE Vermutung** in die Mathematikgeschichte eingegangen.

2. **DIRICHLETSCHE L-Reihen** $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ mit einem Charakter χ. $L(s,\chi)$ konvergiert für $\sigma > 1$. Wie für die RIEMANNSCHE Zetafunktion wird auch für alle L-Funktionen angenommen, daß sich $L(s,\chi)$ meromorph fortsetzen läßt und die nicht-trivialen Nullstellen sämtlich auf der Geraden $\sigma = \frac{1}{2}$ liegen. Diese Annahme wird als **erweiterte RIEMANNSCHE Vermutung** bezeichnet.

4.2.2 Abschätzung von ANKENY

Bereits im Jahre 1952 bewies Ankeny unter Voraussetzung der erweiterten Riemannschen Vermutung die bis heute beste Abschätzung für den kleinsten quadratischen Nichtrest.

Satz von ANKENY

Sei $n \in \mathbb{N}$ und G eine Untergruppe der multiplikativen Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ mit $G \neq (\mathbb{Z}/n\mathbb{Z})^*$. Dann ist, unter Voraussetzung der erweiterten Riemannschen Vermutung, die kleinste positive ganze Zahl außerhalb G ein $O\left((\log n)^2\right)$.

Folgerung

Gilt die erweiterte Riemannsche Vermutung, so ist

$$n^*(p) = O\left((\log p)^2\right),$$

d.h. es gibt ein M so, daß für alle ungeraden Primzahlen p für den kleinsten quadratischen Nichtrest $n^*(p)$ modulo p gilt

$$n^*(p) \leq M (\log p)^2.$$

Vermutung von Ankeny

Zwei Jahre später, 1954, veröffentlichte ANKENY einen Artikel in der Zeitschrift *Duke Math. Journal*, in dem er einen Beweis für die folgende Aussage angab.

Sei p eine Primzahl mit $p \equiv 3$ mod 4. Dann gilt für alle $\epsilon > 0$ und $p > p_0(\epsilon)$

$$n^*(p) < p^{\epsilon}.$$

In den *Mathematical Reviews* [Erd] schreibt PAUL ERDÖS einen kurzen Bericht, in dem er die Aussage als bewiesen sieht. Später bemerkt K. A. RODOSSKIĬ ebenfalls in den *Mathematical Reviews* [Rod], daß der Beweis von ANKENY einen Fehler enthält.

4.2.3 Abschätzung von BACH

In seiner Dissertation [Bach] gibt ERIC BACH eine Abschätzung von P. WEINBERGER an, der 1981 zeigte, daß, falls die erweiterte Riemannsche Vermutung stimmt, die Abschätzung

$$n^*(p) \leq 4 \cdot (\log p)^2$$

gilt. BACH selbst gibt sogar eine bessere Schranke an.

Satz von Bach

Sei n eine natürliche Zahl und G eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ mit $G \neq (\mathbb{Z}/n\mathbb{Z})^*$. Ist x das kleinste Element in $(\mathbb{Z}/n\mathbb{Z})^* - G$, dann gilt unter Annahme der ERH

$$x \leq 2 \cdot (\log n)^2 .$$

Folgerung

Gilt die erweiterte Riemannsche Vermutung, dann ist

$$n^* (p) \leq 2 \cdot (\log p)^2 . \tag{4.16}$$

4.2.4 Abschätzung von Wedeniwski

Eine sehr gute Abschätzung für den kleinsten quadratischen Nichtrest, die auch die erweiterte Riemannsche Vermutung voraussetzt, gibt Sebastian Wedeniwski in seiner Dissertation 2001 an, vgl. [Wed, Kap. 6.9, S. 122].

Satz von Wedeniwski

Wir nehmen an, daß die erweiterte Riemannsche Vermutung gilt. Sei $m > 1$ eine ungerade positive ganze Zahl, mit $m \neq n^2$ für $n \in \mathbb{N}$, und

$$x = \min \left\{ k \in \mathbb{N} \mid \left(\frac{k}{m} \right) \neq 1 \right\} .$$

Dann gilt

$$x < \frac{3}{2} \cdot \log (m)^2 - \frac{44}{5} \cdot \log m + 13.$$

Überprüft man jedoch die Aussage für alle Zahlen $m < 10000$, stellt man fest, daß die Abschätzung für die Zahlen $7, 11, 13, 15, 17, 19, 21, 23, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 51, 53, 55, 57, 63, 65, 71, 73, 95, 97, 119$ nicht erfüllt ist. Dies liegt vor allem daran, daß für $m \leq 57$ die rechte Seite < 2 ist, während $x \geq 2$ gilt.

4.2.5 Satz von Bach-Shallit

In [Bac/Sha, Theorem 8.4.6, S. 217] findet man folgenden Primzahlsatz, aus dem man fast die Abschätzung von Ankeny erhält.

Satz

Gilt die erweiterte Riemannsche Vermutung, so gibt es eine Konstante M mit folgender Eigenschaft:

- *Ist n eine natürliche Zahl und $\rho_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ die Reduktion modulo n,*
- *ist G eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ vom Index d,*
- *ist C eine Nebenklasse der Untergruppe G in $(\mathbb{Z}/n\mathbb{Z})^*$,*
- *ist für reelle $x > 1$*
$$\pi_C(x) = \#\{p \leq x : \rho_n(p) \in C\},$$
d.h. $\pi_C(x)$ ist die Anzahl der Primzahlen $p \leq x$, sodaß p mod n in C liegt,

so gibt es eine reelle Funktion $M_C(x)$ für reelle $x > 1$ mit

$$\pi_C(x) = \frac{1}{d} li(x) + M_C(x) \cdot \sqrt{x} \cdot (\log x + \log n) \quad \textit{und} \quad |M_C(x)| \leq M,$$

wobei $li(x) = \displaystyle\int_2^x \frac{dt}{\log t}$.

Daraus kann man nun folgende Abschätzung für den kleinsten quadratischen Nichtrest herleiten.

Folgerung

Gilt die erweiterte Riemannsche Vermutung, so ist für jedes $\epsilon > 0$

$$n^*(p) = O\left((\log p)^{2+\epsilon}\right),$$

d.h. es gibt ein M_ϵ, sodaß für alle ungeraden Primzahlen p für den kleinsten quadratischen Nichtrest $n^*(p)$ modulo p gilt

$$n^*(p) \leq M_\epsilon (\log p)^{2+\epsilon}.$$

Beweis:

Sei p eine ungerade Primzahl, G die Untergruppe der Quadrate in $(\mathbb{Z}/p\mathbb{Z})^*$ und C die Nebenklasse der Nichtquadrate. Es ist $\text{ord}\,(\mathbb{Z}/p\mathbb{Z})^* = p - 1$ und da es genau $\dfrac{p-1}{2}$ Quadrate gibt, ist $\text{ord}G = \dfrac{p-1}{2}$. Nach dem Satz von LAGRANGE gilt für den Index d von G

$$d = \frac{\text{ord}\ (\mathbb{Z}/p\mathbb{Z})^*}{\text{ord}G} = 2.$$

Mit dem vorangegangenen Satz folgt dann

$$\pi_C(x) = \frac{1}{2}\text{li}(x) + M_C(x) \cdot \sqrt{x} \cdot (\log x + \log p).$$

Für $7 < x \leq p$ ist

$$\mathrm{li}\,(x) > \frac{x}{\log x}$$

und wir erhalten damit die Ungleichungen

$$\begin{aligned}
\pi_C\,(x) &> \frac{x}{2 \cdot \log x} + M_C\,(x) \cdot \sqrt{x} \cdot (\log x + \log p) \\
&\geq \frac{x}{2 \cdot \log x} - M \cdot \sqrt{x} \cdot (\log x + \log p) \\
&\geq \frac{x}{2 \cdot \log x} - M \cdot \sqrt{x} \cdot (\log p + \log p) \\
&\geq \frac{x}{2 \cdot \log x} - 2 \cdot M \cdot \sqrt{x} \cdot \log p
\end{aligned}$$

und daher

$$\frac{\pi_C\,(x)}{\sqrt{x} \cdot \log p} \geq \frac{\sqrt{x}}{2 \cdot \log x \cdot \log p} - 2 \cdot M.$$

Für $x = (\log p)^{2+\epsilon}$ folgt daraus

$$\begin{aligned}
\frac{\pi_C\left((\log p)^{2+\epsilon}\right)}{\sqrt{(\log p)^{2+\epsilon}} \cdot \log p} &\geq \frac{(\log p)^{1+\frac{\epsilon}{2}}}{2 \cdot \log\,(\log p)^{2+\epsilon} \cdot \log p} - 2 \cdot M \\
&= \frac{(\log p)^{\frac{\epsilon}{2}}}{2 \cdot (2+\epsilon) \cdot \log\log p} - 2 \cdot M.
\end{aligned}$$

Für hinreichend große p ist der letzte Ausdruck > 0 und damit ist $\pi_C\left((\log p)^{2+\epsilon}\right) > 0$, d.h. es gibt mindestens eine Primzahl $\leq (\log p)^{2+\epsilon}$, die quadratischer Nichtrest modulo p ist, also gilt

$$n^*\,(p) \leq (\log p)^{2+\epsilon}.$$

Dies beweist die Behauptung. □

Kapitel 5

Untere Schranken

Außer den vielen unterschiedlichen oberen Schranken für $n^*(p)$ bzw. $n(p)$ ist es auch interessant, nach unteren Schranken für den kleinsten quadratischen Nichtrest zu suchen. Mit diesem Thema hat sich unter anderem HANS SALIÉ im Jahre 1949 beschäftigt. 1971 lieferte HUGH MONTGOMERY ein besseres Ergebnis als SALIÉ. Allerdings basiert der Beweis seiner Abschätzung darauf, daß die erweiterte Riemannsche Vermutung richtig ist. Ohne ERH kommt die Verschärfung von SALIÉS Abschätzung aus, die 1990 von S. W. GRAHAM und C. J. RINGROSE veröffentlicht wurde.

5.1 Abschätzung von SALIÉ

Im Jahre 1949 hat HANS SALIÉ eine untere Schranke für den kleinsten quadratischen Nichtrest angegeben. Um seine Aussage beweisen zu könnnen, benötigen wir die beiden folgenden Sätze.

5.1.1 DIRICHLETSCHER Primzahlsatz

Sind n und a natürliche Zahlen mit $ggT(n,a) = 1$, so gibt es unendlich viele Primzahlen p mit

$$p \equiv a \ mod \ n,$$

d.h. die Folge natürlicher Zahlen

$$a,\ a+n,\ a+2n,\ a+3n,\ a+4n,\ a+5n, \ldots$$

enthält unendlich viele Primzahlen.

Beweis: Siehe [Sche, S. 354-366].

5.1.2 Satz von LINNIK

Für jede natürliche Zahl $n \geq 2$ existiert in jeder primen Restklasse mod n eine Primzahl $q < n^k$, wobei $k > 0$ eine absolute (von n unabhängige) Konstante ist.

Beweis: Siehe [Pra, S. 330-370].

5.1.3 Satz von Salié

Es ist

$$n^*(p) \neq o(\log p),$$

d.h. es gibt eine positive Konstante c und unendlich viele Primzahlen q mit

$$n^*(q) > c \cdot \log q.$$

Beweis:

Sei $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11, \ldots$ die Folge der Primzahlen und sei $m \in \mathbb{N}$, $m \geq 2$. Mit dem chinesischen Restsatz findet man ein $a_m \in \mathbb{Z}$ so, daß für eine ganze Zahl x die Äquivalenz

$$x \equiv \begin{cases} 1 \bmod 8, \\ 1 \bmod p_i \text{ für } 2 \leq i \leq m-1\ , \\ n(p_m) \bmod p_m \end{cases} \iff x \equiv a_m \bmod 8p_2p_3\cdots p_m \tag{5.1}$$

gilt. Dabei gilt $\operatorname{ggT}(a_m, 8p_2p_3\cdots p_m) = 1$. Nach 5.1.1 gibt es dann ein $q \in \mathbb{P}$ mit $q \equiv a_m \bmod 8p_2p_3\cdots p_m$. Aus (5.1) folgt

$$q \equiv 1 \bmod 8, \quad q \equiv 1 \bmod p_2, \quad \ldots, \quad q \equiv 1 \bmod p_{m-1}, \quad q \equiv n(p_m) \bmod p_m$$

und mit 2.5.4 erhält man daraus $\left(\frac{2}{p}\right) = 1$. Da $q \equiv 1 \bmod 4$, folgt mit dem quadratischen Reziprozitätsgesetz $\left(\frac{p_i}{q}\right) = \left(\frac{q}{p_i}\right)$ für $2 \leq i \leq m$ und damit ist

$$\left(\frac{p_i}{q}\right) = \left(\frac{q}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1 \text{ für } 2 \leq i \leq m-1 \quad \text{und} \quad \left(\frac{p_m}{q}\right) = \left(\frac{q}{p_m}\right) = \left(\frac{n(p_m)}{p_m}\right) = -1.$$

Daraus erhält man sofort

$$n(q) = p_m.$$

Für die Tschebyscheff-Funktion $\vartheta(x) = \ln \prod_{p \leq x} p$ gilt nach [Har/Wri, Theorem 415] die Abschätzung

$$\vartheta(n) < 2 \cdot \ln 2 \cdot n \qquad \forall\, n \geq 1.$$

Setzt man $n = p_m$, erhält man

$$\ln(2p_2p_3\cdots p_m) < 2 \cdot \ln 2 \cdot p_m.$$

Sei nun q_m die kleinste Primzahl q, die die obigen Eigenschaften erfüllt. Dann gilt nach dem Satz von Linnik

$$q_m < (8p_2p_3\cdots p_m)^k,$$

und damit

$$\begin{aligned} \ln q_m &< k \cdot (2 \cdot \ln 2 + \ln (2 p_2 p_3 \cdots p_m)) \\ &< k \cdot (2 \cdot \ln 2 + 2 \cdot \ln 2 \cdot p_m) \\ &= 2 \cdot \ln 2 \cdot k \cdot (1 + p_m) \,. \end{aligned}$$

Daraus folgt

$$p_m > \frac{\ln q_m}{2 \cdot \ln 2 \cdot k} - 1$$

und mit $n(q_m) = p_m$ schließlich

$$n(q_m) > \frac{1}{2 \cdot k \cdot \ln 2} \cdot \ln q_m - 1.$$

Da $n(q_m) = p_m$, ist $q_2,\ q_3,\ q_4, \ldots$ eine Folge von verschiedenen Primzahlen mit $\lim\limits_{m \to \infty} q_m = \infty$. Daher gilt

$$\liminf_{m \to \infty} \frac{n(q_m)}{\ln q_m} \geq \frac{1}{2 \cdot k \cdot \ln 2}$$

und damit die Behauptung. □

Bemerkung

Der Beweis des vorangegangenen Satzes liefert uns eine Möglichkeit, wie man sich eine Primzahl q_m mit $n^*(q_m) = p_m$ konstruieren kann. Es ist also jede Primzahl kleinster quadratischer Nichtrest einer anderen Primzahl.

Beispiel

Wir wählen $m = 5$, dann ist $p_5 = 11$ und $n^*(11) = 2$. Aus den Kongruenzen

$$x \equiv 1 \bmod 8,\ x \equiv 1 \bmod 3,\ x \equiv 1 \bmod 5,\ x \equiv 1 \bmod 7,\ x \equiv 2 \bmod 11$$

erhalten wir mit dem chinesischen Restsatz die Bedingung

$$x \equiv 2521 \bmod 9240 \quad \text{mit} \quad 9240 = 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11.$$

Nun suchen wir die erste Primzahl unter den Zahlen

$$2521,\ 2521 + 9240,\ 2521 + 2 \cdot 9240,\ 2521 + 3 \cdot 9240,\ \ldots$$

Das liefert uns die Zahl $q_5 = 2521$.

In der folgenden Tabelle 5.1 wurde die im Beweis angegebene Zahl q_m mit einer Maple-Funktion explizit konstruiert.

m	q_m	$n^*(q_m)$
2	17	3
3	97	5
4	241	7
5	2521	11
6	157081	13
7	1921921	17
8	144984841	19
9	3453089641	23
10	2677114441	29
11	232908956281	31
12	72201776446801	37
13	5580395077377121	41
14	380921329936066921	43
15	9628912340109142081	47
16	848547899972118145801	53
17	30894522236376162404041	59
18	306872551884612337195 5721	61
19	51606887798139067232638801	67
20	28038491294254392855376593121	71

Tabelle 5.1: Primzahlen q_m mit $n^*(q_m) = p_m$

5.2 Abschätzung von MONTGOMERY

Im Jahre 1971 bewies HUGH MONTGOMERY in seinem Buch *"Topics in Multiplicative Number Theory"* (vgl. [Mon]) folgenden Satz, aus dem wir eine untere Schranke für $n^*(p)$ folgern können.

Satz

Gilt die erweiterte Riemannsche Vermutung für alle L-Funktionen von reellwertigen Charakteren χ, dann existiert eine Konstante c, so daß für unendlich viele reellwertige primitive Charaktere χ modulo m

$$n_\chi \geq c \cdot \log m \log\log m$$

gilt. Dabei ist n_χ das kleinste n für das $\chi(n) \neq 1$ und $\chi(n) \neq 0$ gilt.

Einen Beweis findet man in [Mon, S.122].

Bemerkung

Das LEGENDRE-Symbol definiert durch $\chi(p) = \left(\frac{n}{p}\right)$ einen Charakter χ modulo p mit den Eigenschaften

$$\begin{aligned} \chi(n) = 0 &\iff p \mid n, \\ \chi(n) = 1 &\iff p \nmid n \text{ und } n \text{ ist quadratischer Rest mod } p, \\ \chi(n) = -1 &\iff p \nmid n \text{ und } n \text{ ist quadratischer Nichtrest mod } p. \end{aligned}$$

Mit dem obigen Satz erhalten wir daraus folgende Abschätzung für den kleinsten quadratischen Nichtrest.

Folgerung

Es gibt eine Konstante $c > 0$, so daß unter Annahme der erweiterten Riemannschen Vermutung für unendlich viele $p \in \mathbb{P}$ gilt

$$n^*(p) \geq c \cdot \log p \log\log p.$$

5.3 Abschätzung von GRAHAM und RINGROSE

Besser als SALIÉ, aber etwas schlechter als MONTGOMERY ist folgendes Ergebnis aus dem Jahre 1990, das allerdings ohne die erweiterte Riemannsche Vermutung auskommt. Auf den Beweis wird verzichtet, er findet sich in [Gra/Rin].

Satz

Es existiert eine Konstante $c > 0$, so daß für unendlich viele Primzahlen p gilt

$$n^*(p) \geq c \cdot \log p \log\log\log p.$$

Kapitel 6

Verteilung der kleinsten quadratischen Nichtreste

In seinem Artikel *"The Euclidean algorithm strikes again"* [Wag2] erwähnt STAN WAGON ein von ihm durchgeführtes Experiment, in dem er den kleinsten quadratischen Nichtrest $n^*(p)$ für die ersten 418 Primzahlen $> 10^{15}$ berechnet. Ihm fällt auf, daß der erste Nichtrest nie größer ist als 29 und für nur 19 der betrachteten Primzahlen $n^*(p)$ außerhalb der Menge $\{2,\ 3,\ 5,\ 7\}$ liegt. Außerdem vergleicht WAGON seine Ergebnisse mit der Abschätzung von ERIC BACH, wonach unter Annahme der verallgemeinerten Riemannschen Vermutung $n^*(p) < 2 \cdot (\log p)^2$ gilt (vgl. 4.2.3) und bemerkt, daß für Primzahlen $p \equiv 1 \bmod 4$ und $p < 1000000$ der kleinste quadratische Nichtrest höchstens 37 ist, während die Schranke $2 \cdot (\log p)^2$ für Primzahlen, die in der Nähe von 1000000 liegen, ungefähr 381 ist. Für die untersuchten 418 Primzahlen $> 10^{15}$ läge die Schranke von BACH ungefähr bei 2385.

Dies führt auch zu der interessanten Frage, wie oft eine Primzahl q als quadratischer Nichtrest modulo einer Primzahl p auftritt. Dazu wollen wir zeigen, welche Ergebnisse man erhält, wenn man mit einem C++-Programm für jeweils 1000000 aufeinanderfolgende Primzahlen p den kleinsten quadratischen Nichtrest modulo p berechnet und zählt, wie oft ein Nichtrest auftritt. Wir wollen in Tabelle 6.1 zwei Beispiele angeben.

Dabei wurden in der linken Tabelle die ersten 10^6 Primzahlen ab 10^{50} untersucht, in der Tabelle auf der rechten Seite sind die Ergebnisse für die ersten 10^6 Primzahlen $> 10^{100}$ angegeben.

Bei Betrachtung der beiden Tabellen fällt auf, daß sich die Anzahl der Primzahlen jedesmal ungefähr halbiert. Es liegt also die Vermutung nahe, daß für circa $\frac{1}{2}$ der Primzahlen $n^*(p) = 2$, für ungefähr $\frac{1}{4}$ der Primzahlen $n^*(p) = 3$, für etwa $\frac{1}{8}$ der Primzahlen $n^*(p) = 5$ gilt, usw.

Wir wollen nun dieses Verhalten erklären.

q	$\#\{p \in \mathbb{P},\ \text{mit } n^*(p) = q\}$
2	500199
3	250215
5	124406
7	62643
11	31270
13	15668
17	7716
19	3969
23	2006
29	940
31	489
37	255
41	102
43	59
47	34
53	13
59	7
61	5
67	1
71	3

q	$\#\{p \in \mathbb{P},\ \text{mit } n^*(p) = q\}$
2	499984
3	250152
5	125089
7	62317
11	31084
13	15755
17	7828
19	3875
23	1983
29	978
31	498
37	235
41	113
43	52
47	27
53	16
59	7
61	3
67	3
71	1

Tabelle 6.1: Verteilung von $n^*(p)$

Vorbemerkung

Nach 2.5.4 gilt für eine ungerade Primzahl p offensichtlich

$$n^*(p) = 2 \iff \left(\frac{2}{p}\right) = -1 \iff p \equiv 3,\ 5 \bmod 8.$$

Da die ungeraden Primzahlen nach dem DIRICHLETSCHEN Primzahlsatz einigermaßen gleichmäßig auf die vier Restklassen 1, 3, 5, 7 modulo 8 verteilt sind, sollte also für etwa die Hälfte der Primzahlen $n(p) = 2$ gelten. Wir werden dies in den folgenden Überlegungen verallgemeinern.

Wir betrachten zunächst ein Lemma, das zwei Eigenschaften des JACOBI-Symbols angibt.

Lemma

Seien $a, b \in \mathbb{N}$.

(1) *Im Fall* $ggT(2, a) = ggT(2, b) = 1$ *gilt*

$$a \equiv b \ mod\ 8 \implies \left(\frac{2}{a}\right) = \left(\frac{2}{b}\right).$$

(2) *Ist p eine ungerade Primzahl und $ggT(2\cdot p, a) = ggT(2\cdot p, b) = 1$, so gilt*

$$a \equiv b \ mod\ 4\cdot p \quad \Longrightarrow \quad \left(\frac{p}{a}\right) = \left(\frac{p}{b}\right).$$

Beweis:

(1) folgt sofort aus der Äquivalenz $\left(\frac{2}{a}\right) = 1 \Longleftrightarrow a \equiv \pm 1 \bmod 8$.

Zu (2):

Ist $p \equiv 1 \bmod 4$, so erhält man mit $a \equiv b \bmod p$ und dem quadratischen Reziprozitätsgesetz die Gleichung $\left(\frac{p}{a}\right) = \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{p}{b}\right)$.

Ist $p \equiv 3 \bmod 4$ und $a \equiv 1 \bmod 4$, dann folgt $b \equiv 1 \bmod 4$ und das quadratische Reziprozitätsgesetz liefert die letzte Gleichung, also $\left(\frac{p}{a}\right) = \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{p}{b}\right)$.

Ist $p \equiv 3 \bmod 4$ und $a \equiv 3 \bmod 4$, so folgt $b \equiv 3 \bmod 4$ und das quadratische Reziprozitätsgesetz ergibt $\left(\frac{p}{a}\right) = -\left(\frac{a}{p}\right) = -\left(\frac{b}{p}\right) = \left(\frac{p}{b}\right)$. □

Lemma

Sei $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11, \ldots$ die Folge der Primzahlen, $r \geq 1$ und $n = 8p_2p_3\cdots p_r$. Dann definiert

$$\psi_r : (\mathbb{Z}/n\mathbb{Z})^* \to \{\pm 1\} \times \{\pm 1\} \times \cdots \times \{\pm 1\}, \qquad a \mapsto \left\{\left(\frac{2}{a}\right), \ \left(\frac{3}{a}\right), \ \ldots, \left(\frac{p_r}{a}\right)\right\}$$

einen surjektiven Gruppenhomomorphismus. Ist

$$N_r = \psi^{-1}\left(\{(1, 1, \ldots, 1, -1)\}\right) \subseteq (\mathbb{Z}/n\mathbb{Z})^*,$$

dann gilt für eine Primzahl p die Äquivalenz

$$n(p) = p_r \quad \Longleftrightarrow \quad p \ mod\ n \ liegt\ in\ N_r.$$

Außerdem gilt

$$\frac{\#N_r}{\#(\mathbb{Z}/n\mathbb{Z})^*} = \frac{1}{2^r}.$$

Beweis:

Mit dem vorangegangenen Lemma erhalten wir aus der Kongruenz $a_1 \equiv a_2 \bmod 8p_2p_3\cdots p_r$ die Gleichungen

$$\left(\frac{2}{a_1}\right) = \left(\frac{2}{a_2}\right), \ \left(\frac{3}{a_1}\right) = \left(\frac{3}{a_2}\right), \ \ldots, \left(\frac{p_r}{a_1}\right) = \left(\frac{p_r}{a_2}\right).$$

Somit ist die Abbildung ψ_r wohldefiniert.[1] Die Multiplikativität des JACOBI-Symbols zeigt, daß ψ_r ein Gruppenhomomorphismus ist. Die Surjektivität überlegt man sich mit dem chinesischen Restsatz.

Für eine Primzahl p gilt

$$\begin{aligned} n(p) = p_r &\iff \left(\frac{2}{p}\right) = 1,\ \left(\frac{3}{p}\right) = 1,\ \ldots,\ \left(\frac{p_{r-1}}{p}\right) = 1, \left(\frac{p_r}{p}\right) = -1 \\ &\iff \psi_r(p \bmod n) = (1, 1, \ldots, 1, -1) \\ &\iff p \bmod n \text{ liegt in } N_r. \end{aligned}$$

Da ψ_r surjektiv ist und N_r eine Nebenklasse des Kerns ist, erhält man die letzte Behauptung aus

$$\frac{\#(\mathbb{Z}/n\mathbb{Z})^*}{\#N_r} = \frac{\#(\mathbb{Z}/n\mathbb{Z})^*}{\#\text{Kern}(\psi_r)} = \#\text{Bild}(\psi_r) = 2^r.$$

□

Bemerkung

Für Funktionen f, g schreiben wir $f(x) \sim g(x)$ ("f und g verhalten sich für $x \to \infty$ asymptotisch gleich"), wenn

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Satz

Ist $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11, \ldots$ die Folge der Primzahlen, $r \in \mathbb{N}$ und

$$f_r(x) = \#\{p \le x : n(p) = p_r\},$$

(d.h. $f_r(x)$ ist die Anzahl der Primzahlen $\le x$, deren kleinster quadratischer Nichtrest p_r ist), so gilt

$$\lim_{x\to\infty} \frac{f_r(x)}{\pi(x)} = \frac{1}{2^r},$$

wobei $\pi(x) = \#\{p \le x\}$ die Primzahlzählfunktion bezeichnet.

Beweis:

Wir verwenden die Bezeichnungen des vorangegangenen Lemmas. Sei $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ und

$$\pi(x, n, a) = \#\{p \le x : p \equiv a \bmod n\}.$$

Nach dem DIRICHLETSCHEN Primzahlsatz gilt die Beziehung (vgl. [Sche, S. 463])

$$\pi(x, n, a) \sim \frac{1}{\varphi(n)} \cdot \frac{x}{\log x}, \tag{6.1}$$

[1] In dem Lemma wurde $n = 8p_2p_3\cdots p_r$ gewählt, weil bei Wahl von $n = 2 \cdot p_2p_3\cdots p_r$ oder $n = 4p_2p_3\cdots p_r$ die entsprechende Abbildung ψ_r nicht wohldefiniert wäre.

wobei $\varphi(n) = \#\{a \in \mathbb{N} : 0 \leq a < n \text{ und } \mathrm{ggT}(a,n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^*$ die EULERSCHE φ – Funktion bezeichnet.

Der Primzahlsatz besagt (vgl. [Sche, S. 337])

$$\pi(x) \sim \frac{x}{\log x}$$

und mit (6.1) erhält man

$$\lim_{x\to\infty} \frac{\pi(x,n,a)}{\pi(x)} = \frac{1}{\varphi(n)}.$$

Dann gilt

$$\begin{aligned} f_r(x) &= \#\{p \leq x : n(p) = p_r\} \\ &= \#\{p \leq x : p \bmod n \text{ liegt in } N_r\} \\ &= \sum_{a\in N_r} \#\{p \leq x : p \equiv a \bmod n\} \\ &= \sum_{a\in N_r} \pi(x,n,a). \end{aligned}$$

Daraus erhält man

$$\begin{aligned} \lim_{x\to\infty} \frac{f_r(x)}{\pi(x)} &= \lim_{x\to\infty} \sum_{a\in N_r} \frac{\pi(x,n,a)}{\pi(x)} = \sum_{a\in N_r} \lim_{x\to\infty} \frac{\pi(x,n,a)}{\pi(x)} \\ &= \sum_{a\in N_r} \frac{1}{\varphi(n)} = \frac{\#N_r}{\#(\mathbb{Z}/n\mathbb{Z})^*} \\ &= \frac{1}{2^r}, \end{aligned}$$

was wir zeigen wollten. □

Kapitel 7

Anwendungen

Nachdem wir viele verschiedene Abschätzungen für den kleinsten quadratischen Nichtrest gefunden haben, wollen wir nun zeigen, daß kleine quadratische Reste auch in Anwendungen eine große Rolle spielen. Im folgenden Kapitel geben wir zwei Beispiele dafür an, wo kleine quadratische Reste nützlich sind. Zunächst zeigen wir, daß man mit Hilfe eines Nichtrestes schnell Quadratwurzeln modulo p ziehen kann. Im zweiten Teil zeigen wir am Beispiel des MILLER-RABIN-Primzahltests, daß quadratische Nichtreste eine wichtige Rolle spielen beim Testen einer Zahl auf Zerlegbarkeit.

7.1 Quadratwurzelziehen modulo p

In 2.1 haben wir das LEGENDRE-Symbol definiert, mit dessen Hilfe man schnell testen kann, ob für eine ungerade Primzahl p und ein $a \in (\mathbb{Z}/p\mathbb{Z})^*$ die Gleichung $x^2 = a$ in $(\mathbb{Z}/p\mathbb{Z})^*$ lösbar ist oder nicht. Nehmen wir an, wir wissen, daß $\left(\frac{a}{p}\right) = 1$ gilt. Dann existiert also ein x, so daß $x \equiv a \bmod p$. Aber wie findet man dieses x?

Für die Primzahlen $p \equiv 3 \bmod 4$ gibt es dafür eine einfache Lösung. In diesem Fall ist eine Lösung gegeben durch

$$x \equiv a^{\frac{p+1}{4}} \bmod p.$$

Da a ein quadratischer Rest ist, gilt nach dem Satz von EULER $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ und damit erhält man

$$x^2 \equiv a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}} \equiv a \bmod p,$$

wie gewünscht.

Eine ähnlich einfache Lösung findet man für die Primzahlen $p \equiv 5 \bmod 8$. Da nun wieder $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ gilt und ± 1 die einzigen Quadratwurzeln von 1 in $\mathbb{Z}/p\mathbb{Z}$ sind, haben wir

$$a^{\frac{p-1}{4}} \equiv \pm 1 \bmod p.$$

Ist nun $a^{\frac{p-1}{4}} \equiv 1 \bmod p$, dann erfüllt

$$x \equiv a^{\frac{p+3}{8}} \bmod p$$

das Gewünschte. Es ist dann nämlich

$$x^2 \equiv a^{\frac{p+3}{4}} = a \cdot a^{\frac{p-1}{4}} \equiv a \bmod p.$$

Es bleibt also wieder der Fall $p \equiv 1 \bmod 8$, für den man keine einfache Lösung für x angeben kann.

In einem Verfahren von Tonelli und Shanks wird gezeigt, daß man für die Gleichung $x^2 = a$ schnell eine Lösung angeben kann, bzw. die Nichtlösbarkeit zeigen kann, wenn man einen quadratischen Nichtrest modulo p, also ein $n \in (\mathbb{Z}/p\mathbb{Z})^*$ mit $\left(\frac{n}{p}\right) = -1$, kennt.

Die multiplikative Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ ist zyklisch von Ordnung $p-1$. Nun zerlegen wir

$$p - 1 = 2^s \cdot u \quad \text{mit} \quad s \geq 1 \text{ und } u \equiv 1 \bmod 2$$

und definieren die Untergruppen

$$G = \left\{b \in (\mathbb{Z}/p\mathbb{Z})^* : b^{2^s} = 1\right\} \quad \text{und} \quad U = \left\{c \in (\mathbb{Z}/p\mathbb{Z})^* : c^u = 1\right\}.$$

Dabei ist G zyklisch von Ordnung 2^s und U zyklisch von Ordnung u. Man kann explizit einen Isomorphismus

$$\lambda : (\mathbb{Z}/p\mathbb{Z})^* \quad \to \quad G \times U$$

beschreiben. Mit dem erweiterten euklidischen Algorithmus findet man nämlich $A, B \in \mathbb{Z}$, so daß

$$1 = A \cdot 2^s + B \cdot u.$$

Dann gilt für $a \in (\mathbb{Z}/p\mathbb{Z})^*$

$$a = a^{A \cdot 2^s + B \cdot u} = \left(a^{B \cdot u}\right) \cdot \left(a^{A \cdot 2^s}\right) \quad \text{mit} \quad \left(a^{B \cdot u}\right) \in G, \ \left(a^{A \cdot 2^s}\right) \in U,$$

denn mit dem kleinen Satz von FERMAT erhält man

$$\left(a^{B \cdot u}\right)^{2^s} = a^{B \cdot u \cdot 2^s} = a^{B \cdot (p-1)} = \underbrace{\left(a^{p-1}\right)}_{\equiv 1 \bmod p}{}^{B} = 1$$

und analog $\left(a^{A \cdot 2^s}\right)^u = 1$. Also ist

$$\lambda(a) = \left(a^{B \cdot u}, a^{A \cdot 2^s}\right).$$

Hat man ein Element aus U, so kann man daraus schnell die eindeutig bestimmte Wurzel ziehen. Denn für $c \in U$ gilt $c^u = 1$ und damit

$$c = c^{u+1} = \left(c^{\frac{u+1}{2}}\right)^2.$$

Es bleibt also die Frage, wie man Wurzeln aus Elementen von G zieht. Wir geben ein Verfahren an, für das man jedoch einen Erzeuger g der zyklischen Gruppe G benötigt. Dazu bemerken wir:

Ist $n \in (\mathbb{Z}/p\mathbb{Z})^*$, dann ist $n^u \in G$ und es gilt

$$n^u \text{ erzeugt } G \iff \left(\frac{n}{p}\right) = -1.$$

Hat man also einen quadratischen Nichtrest modulo p, so erhält man auch schnell einen Erzeuger g der Gruppe G.

Sei nun g ein Erzeuger von G und $b \in G$. Dann existiert ein eindeutig bestimmtes $k \in \mathbb{Z}$ mit

$$b = g^k \quad \text{und} \quad 0 \leq k < 2^s.$$

Wie erhält man nun die Zahl k? Dazu geben wir die eindeutige Zerlegung in der Binärdarstellung an

$$k = 2^{l_1} + 2^{l_2} + \ldots + 2^{l_m} \quad \text{mit} \quad 0 \leq l_1 < l_2 < \ldots < l_m < s.$$

Nun definieren wir

$$b_i = g^{2^{l_i} + 2^{l_{i+1}} + \ldots + 2^{l_m}}$$

und haben dann

$$b_1 = b, \quad b_{i+1} = b_i \cdot g^{-2^{l_i}}, \quad b_{m+1} = 1.$$

Ist $t_i \geq 0$ minimal mit der Eigenschaft $b_i^{2^{t_i}} = 1$, so ist $\operatorname{ord}(b_i) = 2^{t_i}$. Da aber auch $\operatorname{ord}(b_i) = 2^{s-l_i}$ gilt, ist $l_i = s - t_i$. Für gegebenes b und g erhält man damit folgendes Verfahren zur Bestimmung von k:

1. Setze $b_1 = b$, $i = 1$.
2. Bestimme durch Probieren das minimale $t_i \geq 0$ mit $b_i^{2^{t_i}} = 1$ und setze $l_i = s - t_i$.
3. Berechne $b_{i+1} = b_i \cdot g^{-2^{l_i}}$.
4. Ist $b_{i+1} = 1$, so ist man fertig und hat

   $$k = 2^{l_1} + 2^{l_2} + \ldots + 2^{l_i}.$$

   Im anderen Fall ersetzt man i durch $i + 1$ und geht zu 2.

Wenn man nun die Darstellung $b = g^k$ für $b \in G$ kennt, dann gilt:

- Ist $k \equiv 1 \bmod 2$, so ist b kein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^*$.
- Ist $k \equiv 0 \bmod 2$, so ist

  $$b = \left(\pm g^{\frac{k}{2}}\right)^2$$

  ein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^*$ und man hat auch gleich die Quadratwurzeln bestimmt.

Um das Verfahren etwas zu verdeutlichen, wollen wir ein Beispiel angeben.

Beispiel

Wir wählen $p = 12289$, dann ist $p - 1 = 12288 = 2^{12} \cdot 3$. Es gilt $\left(\frac{11}{p}\right) = -1$, also wird die Untergruppe G von $g = 11^3 = 1331$ erzeugt. Nun wollen wir $b = 4770$ als Potenz von g schreiben. Wir wenden also das obige Verfahren an und erhalten:

i	b_i	t_i	l_i
1	4770	11	1
2	192	10	2
3	2548	8	4
4	7969	7	5
5	3542	5	7
6	1305	4	8
7	5146	3	9
8	1479	2	10
9	1		

Damit erhält man

$$k = 2^1 + 2^2 + 2^4 + 2^5 + 2^7 + 2^8 + 2^9 + 2^{10} = 1974 \quad \text{und} \quad b = g^k.$$

Da $k \equiv 0 \bmod 2$, ist b also ein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^*$.

Bemerkung

Wenn man eine Quadratwurzel aus $a \in (\mathbb{Z}/p\mathbb{Z})^*$ ziehen will, muß man nicht explizit die Zerlegung $\lambda(a) = (b, c)$ bestimmen. Wegen

$$a = \left(a^{\frac{u+1}{2}}\right)^2 \cdot a^{-u} \quad \text{und} \quad a^{-u} \in G$$

muß man nämlich nur die Quadratwurzel aus a^{-u} ziehen.

7.2 Primzahltests

Als Anwendung des Satzes von ERIC BACH betrachten wir einen Primzahltest. In seinem Artikel *"Riemann's Hypothesis and Tests for Primality"* (vgl. [Mil]) zeigt GARY MILLER, daß, unter Annahme der erweiterten Riemannschen Vermutung, Primzahltests in polynomialer Zeit möglich sind. Die Idee dabei ist, daß eine Zahl uns sagen kann, daß eine andere Zahl zusammengesetzt ist, ohne dabei zu verraten, wie man diese Zahl faktorisiert. Wenn wir also testen, ob eine Zahl n prim ist, dann suchen wir statt dessen nach einem Zeugen für die Zerlegbarkeit von n. Nach BACHS Abschätzung impliziert die erweiterte Riemannsche Vermutung, daß der letzte Zeuge für die Zerlegbarkeit von n, falls einer existiert, ein $O(\log n)^2$ ist. Die folgenden Ergebnisse orientieren sich an dem Artikel *"Primality testing"* von STAN WAGON [Wag1].

Der MILLER-RABIN-Test

Sei n eine ungerade natürliche Zahl und $n-1 = 2^s \cdot m$, wobei $s \geq 1$ und m ungerade. Weiter sei $b \in (\mathbb{Z}/n\mathbb{Z})^*$. Gilt

$$b^m \equiv 1 \bmod n \quad \text{oder} \quad b^{2^k \cdot m} \equiv -1 \bmod n \text{ für ein } k \text{ mit } 0 \leq k \leq s-1,$$

dann sagen wir, n erfüllt den MILLER-RABIN-*Test zur Basis b. Erfüllt n den Test nicht, so ist n zusammengesetzt.*

Wenn eine Zahl n einen MILLER-RABIN-Test besteht, dann hofft man, daß die Zahl prim ist. Allerdings gibt es auch zusammengesetzte Zahlen, die einen solchen Test bestehen.

Definitionen

- *Eine zusammengesetzte ungerade natürliche Zahl n, die den* MILLER-RABIN-*Test zur Basis b besteht, heißt* ***starke Pseudoprimzahl*** *zur Basis b.*
- *Erfüllt n den Test zur Basis b nicht, dann heißt b ein* ***Zeuge für die Zerlegbarkeit von*** *n.*
- *Wir bezeichnen die $s+1$ Zahlen b^m, b^{2m}, $\ldots$, $b^{n-1} \bmod n$ als die b-***Sequenz*** *von n. Wir sagen, die Sequenz ist vom Typ 1, wenn entweder alle Einträge gleich 1 sind, oder ein Eintrag vor dem letzten Eintrag gleich -1 ist (wobei die restlichen dann natürlich gleich 1 sind). Sonst heißt die Sequenz vom Typ 2. Es gibt also 5 Möglichkeiten, die wir in Tabelle 7.1 aufführen (dabei bezeichnen $*$ eine Zahl ungleich ± 1).*

b^m	b^{2m}	b^{4m}	.	.	.	.	.	b^{n-1}	
1	1	1	1	1	1		$\cdots$	1	*Typ* 1
$*$	$*$	$*$	$\cdots$	$*$	-1	1	$\cdots$	1	*Typ* 1
$*$	$*$	$*$	$\cdots$	$*$	1	1	$\cdots$	1	*Typ* 2
$*$	$*$	$*$	$*$	$*$	$*$	$\cdots$	$*$	$*$	*Typ* 2
$*$	$*$	$*$	$*$	$*$	$*$	$\cdots$	$*$	-1	*Typ* 2

Tabelle 7.1: Sequenz-Typen für den MILLER-RABIN-Algorithmus

Beispiele

- 2047 ist eine starke Pseudoprimzahl zur Basis 2 mit der 2-Sequenz $1, 1$.
- 1373653 ist eine starke Pseudoprimzahl zur Basis 2 mit der 2-Sequenz $890592, -1, 1$ und zur Basis 3 mit der 3-Sequenz $1, 1, 1$.

Betrachten wir die Abschätzung von ERIC BACH, die unter Voraussetzung der erweiterten Riemannschen Vermutung gilt, erhalten wir folgendes Verfahren:

1. Berechne für jedes $b \leq 2\,(\log n)^2$ die b-Sequenz von n.

2. Ist die b-Sequenz von n vom Typ 2, gib n als zusammengesetzt aus.

3. Sonst gib n als prim aus.

Ist also n eine ungerade zusammengesetzte Zahl, so existiert nach BACHS Abschätzung ein Zeuge $p \in \mathbb{P}$ für die Zerlegbarkeit von n mit $p \leq 2\,(\log n)^2$.

Beweis:

Falls n eine Primzahl ist, gilt nach dem kleinen Satz von FERMAT

$$b^{n-1} \equiv 1 \bmod n.$$

Da ± 1 die einzigen Quadratwurzeln von 1 in $\mathbb{Z}/n\mathbb{Z}$ sind, muß also der Weg zur 1 in der b-Sequenz von n vom Typ 1 sein.

Sei nun n eine Primzahlpotenz, aber keine Primzahl. Für diesen Fall zeigt H. W. LENSTRA in seinem Artikel *"Miller's primality test"* (vgl. [Len]), daß $b^{n-1} \not\equiv 1 \bmod n$ für ein $b < 2 \cdot (\log n)^2$ gilt und damit die b-Sequenz von n vom Typ 2 ist.

Nun sei n eine zusammengesetzte Zahl, aber keine Primzahlpotenz, mit $n - 1 = 2^s \cdot m$, wobei $s \geq 1$ und m ungerade. Wir unterscheiden jetzt zwei Fälle:

Fall 1 : n hat mindestens zwei unterschiedliche Primfaktoren p, q, für die

$$v_2\,(q-1) < v_2\,(p-1) \tag{7.1}$$

gilt.

Nach der Abschätzung von BACH existiert ein $b \leq 2\,(\log p)^2$ mit $\left(\frac{b}{p}\right) = -1$. Wegen 2.4.1 gilt dann

$$b^{\frac{p-1}{2}} \equiv -1 \bmod p, \quad \text{also} \quad b^{p-1} \equiv 1 \bmod p.$$

Also ist $\mathrm{ord}_p\,(b) = p - 1$ und es gilt natürlich

$$v_2\,(\mathrm{ord}_p\,(b)) = v_2\,(p-1)\,. \tag{7.2}$$

Nun nehmen wir an, daß

$$b^m \equiv 1 \bmod n$$

gilt. Dann ist auch $b^m \equiv 1 \bmod p$, woraus folgt, daß $\mathrm{ord}_p\,(b)$ ungerade ist. Dies ist jedoch ein Widerspruch zu (7.2). Also muß die Kongruenz $b^m \equiv 1 \bmod n$ falsch sein.

Weiter nehmen wir an, daß

$$b^{2^k m} \equiv -1 \bmod n \text{ für ein } k \in [1, s-1]\,.$$

Dann ist $b^{2^k m} \equiv -1 \bmod p$ und $b^{2^k m} \equiv -1 \bmod q$, also $b^{2^{k+1} m} \equiv 1 \bmod p$ und $b^{2^{k+1} m} \equiv 1 \bmod q$. Somit erhält man

$$v_2\,(\mathrm{ord}_p\,(b)) = v_2\,(\mathrm{ord}_q\,(b)) = k + 1. \tag{7.3}$$

Da $\mathrm{ord}_q(b)$ entweder gleich $q-1$ oder ein Teiler davon ist, gilt $v_2(\mathrm{ord}_q(b)) \leq v_2(q-1)$. Mit (7.1) und (7.2) erhält man schließlich

$$v_2(\mathrm{ord}_p(b)) = v_2(p-1) > v_2(q-1) \geq v_2(\mathrm{ord}_q(b)),$$

was aber einen Widerspruch zu (7.3) liefert.

Also ist die b-Sequenz von n vom Typ 2, was nach MILLERS Algorithmus bedeutet, daß n zusammengesetzt ist.

Fall 2 : n hat mindestens zwei verschiedene Primteiler p, q mit

$$v_2(q-1) = v_2(p-1).$$

Wir wählen ein b, für das o.B.d.A.

$$\left(\frac{b}{p}\right) = -1 \quad \text{und} \quad \left(\frac{b}{q}\right) = 1$$

gilt. Nach dem EULER-Kriterium ist dann

$$b^{\frac{p-1}{2}} \equiv -1 \bmod p \quad \text{und} \quad b^{\frac{q-1}{2}} \equiv 1 \bmod q.$$

Also ist $\mathrm{ord}_p(b) = p-1$ und damit

$$v_2(\mathrm{ord}_p(b)) = v_2(p-1). \tag{7.4}$$

Außerdem ist $\mathrm{ord}_q(b) \leq \frac{q-1}{2}$, also ist $\mathrm{ord}_q(b)$ ein Teiler von $q-1$ und es gilt

$$v_2(\mathrm{ord}_q(b)) \leq v_2(q-1). \tag{7.5}$$

Wir nehmen wieder

$$b^m \equiv 1 \bmod n$$

an und erhalten mit $b^m \equiv 1 \bmod p$ und damit $\mathrm{ord}_p(b) \equiv 1 \bmod 2$ einen Widerspruch zu (7.4).

Die Annahme

$$b^{2^k m} \equiv -1 \bmod n \text{ für ein } k \in [1, s-1]$$

führt wieder zu

$$v_2(\mathrm{ord}_p(b)) = v_2(\mathrm{ord}_q(b)) = k+1,$$

was aber wegen

$$v_p(\mathrm{ord}_p(b)) = v_2(p-1) = v_2(q-1) \geq v_2(\mathrm{ord}_q(b))$$

einen Widerspruch liefert.

Somit ist auch in diesem Fall die b-Sequenz von n vom Typ 2, was wieder zeigt, daß n zusammengesetzt ist. □

Findet man also "schnell" kleine quadratische Nichtreste, so kann man mit dem MILLER-RABIN-Algorithmus schnell zeigen, daß eine zusammengesetzte natürliche Zahl zusammengesetzt ist.

In seinem Artikel erwähnt STAN WAGON auch eine Berechnung von Carl Pomerance, J. L. Selfridge und Samuel S. Wagstaff, die mittels Computer alle Zahlen $n < 25 \cdot 10^9$ geprüft und festgestellt haben, daß man für diese Zahlen schon sehr kleine Zeugen für die Zerlegbarkeit findet. Nach dem Satz von BACH gibt es für eine zusammengesetzte Zahl $n < 25 \cdot 10^9$ einen Zeugen $b < 1147$ für die Zerlegbarkeit von n. Bei dem Versuch hat sich herausgestellt, daß ein $b \leq 11$ schon genügt. Die folgende Tabelle zeigt, daß der erste Zeuge näher bei $\log_{10} n$ liegt, als bei $2 \cdot (\log n)^2$. Dabei ist n die erste zusammengesetzte Zahl für die b der kleinste Zeuge für die Zerlegbarkeit von n ist.

b	n	$2 \cdot (\log n)^2$	$\log_{10} n$
3	2047	117	3,3
5	1373653	400	6,1
7	25326001	582	7,4
11	3215031751	959	9,5

Tabelle 7.2: Versuch von Pomerance, Selfridge und Wagstaff

Da der kleinste quadratische Nichtrest damit zusammenhängt, bezieht sich STAN WAGON auch auf eine Berechnung von D. H. Lehmer, Emma Lehmer und Daniel Shanks, die für Primzahlen $p \leq 2 \cdot 10^{12}$ den kleinsten quadratischen Nichtrest angegeben haben. In einer Graphik vergleicht er die Treppenfunktion $f(N) = \max\limits_{M \leq N} \{n^*(M)\}$ mit der Funktion $2 \log N \log \log N$. Er bemerkt, daß die erweiterte Riemannsche Vermutung $f(N) < 2 \cdot (\log N)^2$ impliziert, jedoch $2 \log N \log \log N$ eine bessere Schranke zu sein scheint. Auf jeden Fall ist $2 \cdot (\log N)^2$ als obere Schranke ausreichend, um Primzahltests in polynomialer Zeit durchführen zu können.

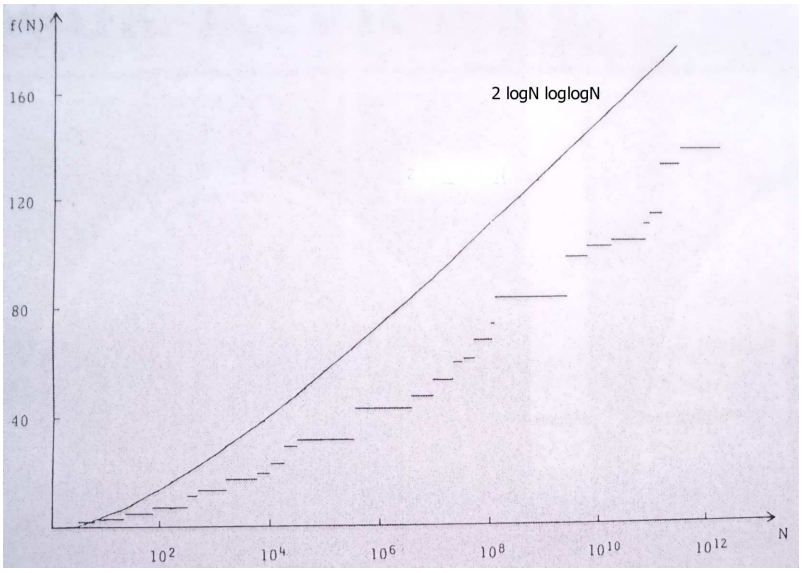

Abbildung 7.1: Vergleich von $f(N) = \max\limits_{M \leq N} \{n^*(M)\}$ mit $g(N) = 2 \log N \log \log N$

Symbolverzeichnis

$\mathbb{N}$	Menge der natürlichen Zahlen
$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{P}$	Menge der Primzahlen
$\left(\frac{a}{p}\right)$	LEGENDRE-Symbol
$a \equiv b \bmod p$	Kongruenz
$a \mid b$	a teilt b
$a \nmid b$	a teilt nicht b
$\mathrm{ggT}\,(a, b)$	größter gemeinsamer Teiler von a, b
$n^*\,(p)$	kleinster quadratischer Nichtrest modulo p
$n\,(p)$	kleinster ungerader quadratischer Nichtrest modulo p
$\#$	Mächtigkeit
$v_p\,(n)$	p-adischer Wert von n
$\varphi\,(n)$	Eulersche φ-Funktion
$\square$	Beweisende
$\lfloor x \rfloor$	GAUSS-Klammer, größte ganze Zahl $\leq x$
$o\,(\ldots)\,,\ O\,(\ldots)$	LANDAU-Symbole
$\log n$	bezeichnet immer den natürlichen Logarithmus $\ln n$
$\mathrm{ord}G$	Ordnung einer Gruppe
$\mathbb{Z}/m\mathbb{Z}$	zyklische Gruppe der Ordnung m
$\chi\,(n)$	Restklassencharakter
$L\,(s, \chi)$	DIRICHLETSCHE L-Reihe
$\zeta\,(s)$	RIEMANNSCHE ζ-Funktion
$\pi\,(x)$	Primzahlzählfunktion, $\pi\,(x) = \#\,\{p \leq x \mid p \in \mathbb{P}\}$

Literaturverzeichnis

[Ank1] **Ankeny, Nesmith C.,** *The least quadratic non residue.* Annals of Mathematics (2), 55 (1952), 65-72

[Ank2] **Ankeny, Nesmith C.,** *Quadratic Residues.* Duke Math. Journal, 21 (1954), 107-112

[Bach] **Bach, Eric,** *Analytic Methods in the analysis and design of number-theoretic algorithms.* Dissertation, MIT Press, London, 1984

[Bac/Sha] **Bach, Eric/ Shallit, Jeffrey O.,** *Algorithmic Number Theory, Volume 1: Efficient Algorithms.* MIT Press 1996

[Bate] **Bateman, P.,** Review zu "Fjellstedt, Lars, *A theorem concerning the least quadratic residue and non-residue.* Arkiv för Matematik 3 (1956), 287-291". *Mathematical Reviews* 17 (1956), 1056

[Brau] **Brauer, Alfred,** *Über den kleinsten quadratischen Nichtrest.* Mathematische Zeitschrift 33 (1931), 161-176

[Brü] **Brüdern, Jörg,** *Einführung in die analytische Zahlentheorie.* Springer-Verlag, Berlin, 1995

[Bund] **Bundschuh, Peter,** *Einführung in die Zahlentheorie.* Springer-Verlag, Berlin, 1988

[Bur] **Burgess, D. A.,** *The Distribution of quadratic residues and non-residues.* Mathematika 4 (1957), 106-112

[Coh] **Cohen, Henri,** *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin, 1995

[Cox] **Cox, David A.,** *Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication.* John Wiley & Sons, New York, 1989

[Dir] **Dirichlet, P. G. Lejeune,** *Vorlesungen über Zahlentheorie. Hrsg. und mit Zusätzen versehen von R. Dedekind.* Vierte Auflage. Friedrich Vieweg und Sohn, Braunschweig, 1894

[Erd] **Erdös, Paul,** Review zu "Ankeny, Nesmith C., *Quadratic Residues.* Duke Math. Journal, 21 (1954), 107-112". *Mathematical Reviews* 15 (1954), 777

[Fjel] **Fjellstedt, Lars,** *A theorem concerning the least quadratic residue and non-residue.* Arkiv för Matematik 3 (1956), 287-291

[Gau] **Gauß, Carl Friedrich,** *Disquisitiones arithmeticae.* Übersetzung von Arthur A. Clarke, S. J., Yale University Press, London, 1966

[Godw] **Godwin, H. J.** *On the least quadratic non-residue.* Proceedings of the Cambridge Philosophical Society 61 (1965), 671-672

[Gra/Rin] **Graham, S. W./ Ringrose, C. J.,** *Lower Bounds for Least Quadratic Non-Residues,* Prog. Math. 85 (1990), 269-309

[Har/Wri] **Hardy, G. H./ Wright, E. M.,** *An Introduction to the Theory of Numbers.* 5th edition, 1979

[Has] **Hasse, Helmut,** *Vorlesungen über Zahlentheorie.* Zweite Auflage. Springer-Verlag, Berlin, 1964

[Hua] **Hua, Loo Keng,** *Introduction to Number Theory.* Springer-Verlag, Berlin, 1982

[Huds] **Hudson, Richard H.** *On the least quadratic non-residue of a prime* $p \equiv 3$ *mod* 4. Journal für reine und angewandte Mathematik 318 (1980), 106-109

[Köch] **Köcher, Markus,** *Elementare Abschätzungen für prime quadratische Reste und Nichtreste.* Dissertation der Eberhard-Karls-Universität Tübingen, 2002

[Len] **Lenstra, H. W.,** *Miller's primality test.* Information Processing Letters 8 (1979), S. 86-88

[Mat] **Prof. Dr. Matzat, B. H.,** *Skript zur Vorlesung Elementare Zahlentheorie.* Universität Heidelberg, SS 1992

[Mil] **Miller, Gary,** *Riemann's Hypothesis and Tests for Primality.* Journal of Computer and System Sciences 13 (1976), 300-317

[Mon] **Montgomery, Hugh,** *Topics in Multiplicative Number Theory.* Springer-Verlag, Berlin, 1971

[Nag1] **Nagell, Trygve,** *Sur les restes et les non-restes quadratiques suivant un module premier.* Arkiv för Matematik 1 (1950), 185-193

[Nag2] **Nagell, Trygve,** *Sur le plus petit non-reste quadratique impair.* Arkiv för Matematik 1 (1951), 573-578

[Niv/Zuc/Mon] **Niven, Ivan/ Zuckerman, Herbert S./ Montgomery, Hugh L.,** *An Introduction to The Theory of Numbers.* 5th edition, John Wiley & Sons, Inc., New York, 1991

[Pra] **Prachar, Karl,** *Primzahlverteilung.* Springer-Verlag, Berlin, 1957

[Red] **Rédei, L.,** *Die Existenz eines ungeraden quadratischen Nichtrestes mod p im Intervall* $1, \sqrt{p}$. Acta Scientiarum Mathematicarum Szeged 15 (1953), 12-19

[Rem/Ull] **Remmert, Reinhold/ Ullrich, Peter,** *Elementare Zahlentheorie.* Birkhäuser-Verlag, Basel, 1987

[Rod] **Rodosskiĭ, K. A.,** Review zu "Ankeny, Nesmith C., *Quadratic Residues.* Duke Math. Journal, 21 (1954), 107-112". *Mathematical Reviews* 17 (1956), 713

[Rup] **Ruppert, Wolfgang,** *Skript zur Vorlesung Kryptographie.* Universität Erlangen/Nürnberg, WS 2000/01

[Sal] **Salié, Hans,** *Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl.* Mathematische Nachrichten 3 (1949), 7-8

[Ser] **Serre, Jean-Pierre,** *A course in arithmetic.* Springer-Verlag, Berlin, 1973

[Sche] **Scheid, Harald,** *Zahlentheorie.* BI-Wissenschaftsverlag, 1991

[Sto] **Stolt, Bengt,** *Über den kleinsten positiven quadratischen Nichtrest.* Mathematica Scandinavica 2 (1954), 187-192

[Vin] **Vinogradov, Ivan Matveevich,** *On the bound of the least non-residue of n-th powers.* Transactions of the American Mathematical Society 29 (1927), 218-226

[Wag1] **Wagon, Stan,** *Primality testing.* The Mathematical Intelligencer Vol. 8, No. 3 (1986), 58-61

[Wag2] **Wagon, Stan,** *The Euclidean algorithm strikes again.* American Mathematical Monthly 97 (1990), 125-129

[Wed] **Wedeniwski, Sebastian,** *Primality Tests on Commutator Curves.* Dissertation der Eberhard-Karls-Universität Tübingen, 2001

[Wei] **Weil, André,** *Number Theory - An approach through history.* Birkhäuser, Boston, 1984

Erklärung

Hiermit erkläre ich, daß ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Literatur erstellt habe.

Erlangen, den 29. April 2004 Harriet Fakesch