Elementare Abschätzungen für prime quadratische Reste und Nichtreste

Dissertation

der Fakultät für Mathematik und Physik
der Eberhard-Karls-Universität Tübingen
zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von
Markus Köcher, Calw
Sommersemester 2002

Tag der mündlichen Prüfung:	31. Oktober 2002
Dekan:	Prof. Dr. H. Müther
1. Berichterstatter:	Prof. Dr. P. Schmid
2. Berichterstatter:	Prof. Dr. U. Felgner

Uxori et parentibus

Inhaltsverzeichnis

Einleitung

Wie doch ein einziger Reicher so viele Bettler in Nahrung
Setzt! Wenn die Könige baun, haben die Kärrner zu tun.[1]
SCHILLER, Xenien

Wir betreten klassischen Boden. Als Carl Friedrich Gauß 1801 in Art. 303 seiner berühmten *Disquisitiones arithmeticae* [17] die Vermutung äußerte, daß die Anzahl der negativen Diskriminanten mit gleicher Geschlechter- und Klassenzahl endlich sei, ahnte er wohl kaum, welch enorme Forschungstätigkeit er damit auslösen würde. Besonders seine Vermutung, daß $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$ die einzigen negativen Diskriminanten sind, für die nur eine Äquivalenzklasse binärer quadratischer Formen existiert, hat als sogenanntes Klassenzahl-1-Problem die Aufmerksamkeit auf sich gezogen und war Antrieb für viele mathematische Untersuchungen — so auch für die vorliegende.

Bezeichnet man mit $h(D) = h(K)$ die Klassenzahl von quadratischen Formen negativer Diskriminante D bzw. die Idealklassenzahl des imaginär-quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{-d})$ mit Diskriminante D, dann besteht nämlich ein einfacher Zusammenhang zwischen der Klassenzahl $h(D)$ und primen quadratischen Resten und Nichtresten modulo D. Da für Diskriminanten $D < -8$ nur dann Klassenzahl 1 vorliegen kann, wenn $D = -p$ mit einer Primzahl $p \equiv 3\,(8)$ gilt, läßt sich dieser Zusammenhang wie folgt aussprechen: Genau dann gilt $h(D) = h(-p) = 1$, wenn alle ungeraden Primzahlen $q < \frac{p+1}{4}$ quadratische Nichtreste modulo p sind. Das heißt, es muß $h(-p) > 1$ gelten, wenn eine Primzahl $q < \frac{p+1}{4}$ existiert, die quadratischer Rest modulo p ist.

Aus diesem Grunde suchen wir in der vorliegenden Arbeit für eine vorgegebene Primzahl p nach kleinen ungeraden Primzahlen q, die quadratische Reste oder Nichtreste modulo p sind, das heißt, für die das Legendre-Symbol $\left(\frac{q}{p}\right) = 1$ oder $= -1$ ist. Wir bezeichnen mit π_p den kleinsten ungeraden primen quadratischen Rest modulo p und mit ψ_p den kleinsten ungeraden primen Nichtrest. Das Ziel sind möglichst gute obere Schranken für π_p und ψ_p in Abhängigkeit von p.

---

[1] Ursprünglich ironisches Distichon über die vielen selbsternannten Kenner und Ausleger der Kantschen Werke.

Im Falle des kleinsten Nichtrests ψ_p haben wir eine klassische Fragestellung vor uns, die schon Legendre und Gauß beschäftigt hat. Sie besitzt viele Anwendungen in der Zahlentheorie, Kodierungstheorie, Kryptologie und in anderen Bereichen. Für Primzahlen $p \equiv 1\,(8)$ zeigte Gauß selbst $\psi_p < 2\sqrt{p} + 1$, was für seinen ersten Beweis des Quadratischen Reziprozitätsgesetzes völlig ausreichte. Trygve Nagell hat den Satz von Gauß auf alle Primzahlen $p > 3$ verallgemeinert und für einzelne Restklassen modulo 8 bessere Schranken angegeben. Sehr früh schon konnte Nagell für $p \equiv 1\,(8)$ die Schranke $\psi_p < \sqrt{p}$ nachweisen, für die es viele Beweise gibt — auch einen sehr eleganten, der auf John Tate zurückgeht und bei Tsit-Yuen Lam in [27] auf S. 179 zu finden ist. Alfred Brauer konnte mit elementaren Mitteln für ψ_p obere Schranken angeben, die für große Primzahlen besser als $\sqrt{p}$ sind. Aufbauend auf der Vorarbeit von Nagell und Brauer beweisen wir im 5. Kapitel folgenden Satz:

Hauptsatz 1

Für alle Primzahlen $p > 13$ mit $p \neq 23, 59, 109, 131$ gilt $\psi_p < \sqrt{p}$.

Im einzelnen gelten die folgenden Schranken:
Ist $p \equiv 1\,(8)$, so gilt $\psi_p \leqslant \sqrt{\frac{1}{2}(p+1)}$.
Ist $p \equiv 7\,(8)$ mit $p \neq 7, 23$, so gilt $\psi_p < \sqrt{p-6}$.
Ist $p \equiv \pm 3\,(8)$ mit $p > 13$ und $p \neq 59, 109, 131$, so gilt $\psi_p < \sqrt{p}$.

Man verifiziert ohne Mühe, daß alle angegebenen Ausnahmen real sind. Der Beweis kommt mit Methoden der elementaren Zahlentheorie aus. Setzt man Methoden der analytischen Zahlentheorie ein, kann man sogar logarithmische Schranken erhalten. Ivan Vinogradov konnte beispielsweise $\psi_p < p^{1/\sqrt{4e}}(\log p)^2$ zeigen — allerdings ist diese Schranke nicht effektiv, das heißt, die Aussage gilt für Primzahlen $p > p_0$, wobei p_0 sehr groß ist und nicht angegeben werden kann. Bei Verwendung der Erweiterten Riemannschen Hypothese erhält man sogar deutlich bessere Abschätzungen, wie die Arbeit von Sebastian Wedeniwski [62] zeigt. Eine untere Schranke für ψ_p wurde von Hans Salié angegeben.

Im Mittelpunkt dieser Arbeit steht die Untersuchung der quadratischen Reste. Während der kleinste (ungerade) quadratische Nichtrest automatisch eine Primzahl ist, gilt dies für quadratische Reste nicht. Daher gestalten sich Abschätzungen für π_p nach oben viel schwieriger. Auch hier gibt es analytische Abschätzungen, zum Beispiel den Satz von Pintz, nach dem für jedes $\varepsilon > 0$ ein p_0 existiert, so daß $\pi_p < p^{1/4+\varepsilon}$ für alle Primzahlen $p > p_0$ gilt. Die Aussagen sind aber wieder nicht effektiv. Deshalb gilt unser Augenmerk den elementaren algebraischen Methoden — in der Absicht, effektive Resultate zu erzielen und die zahlentheoretischen Zusammenhänge besser zu verstehen. Meistens ist unser Beweisgang sogar konstruktiv, so daß man mit Hilfe der vorgestellten Verfahren

kleine quadratische Reste konkret ausrechnen kann. Wir beweisen im 6. Kapitel den folgenden Satz:

Hauptsatz 2

Sei $p > 11$ eine Primzahl mit $p \neq 17$.
Genau dann gilt $\pi_p < \sqrt{p}$, wenn $h(-p) > 1$ ist.

Ist $p > 7$ eine Primzahl und $h(-p) = 1$, also $p \equiv 3\,(8)$, so kann man leicht sehen, daß $\pi_p = \frac{p+1}{4}$ der kleinste ungerade prime quadratische Rest modulo p ist. (In obigem Satz muß $p = 11$ ausgenommen werden, weil $\pi_{11} = 3 = \frac{p+1}{4} < \sqrt{p}$ und $h(-11) = 1$ gleichzeitig gilt. Für $p = 17$ ist die Aussage wegen $\pi_{17} = 13 > \sqrt{p}$ und $h(-4 \cdot 17) = 4$ ebenfalls falsch.)
Da seit der Arbeit von Kurt Heegner, spätestens aber seit Alan Baker und Harold Stark das Klassenzahl-1-Problem gelöst ist, sind die Primzahlen p mit $h(-p) = 1$ bekannt. Aus dem Klassenzahl-1-Theorem erhält man also die

Folgerung

Sei $p > 7$ eine Primzahl mit $p \neq 17$.
Es gilt $\pi_p < \sqrt{p}$, es sei denn, p ist eine der Primzahlen 19, 43, 67, 163.

Je nach Kongruenzklasse von p modulo 8 läßt sich die Abschätzung für π_p etwas verbessern. Ist beispielsweise $p \equiv 3\,(8)$ und $h(-p) > 1$, so folgt aus dem Satz von Minkowski $\pi_p < \frac{2}{\pi}\sqrt{p}$. Ähnliche Abschätzungen wurden von Nagell und von Chowla-Friedlander gegeben. Ist $p \equiv 1\,(4)$, kann man p als Summe zweier Quadrate darstellen, woraus man teilweise die Abschätzung $\pi_p < \frac{1}{2}\sqrt{p-1}$ gewinnt. Eine der Schwierigkeiten beim Beweis von Hauptsatz 2 war Fall der $p \equiv 7\,(8)$. In dieser Situation ist p nicht Summe von drei Quadraten. Da $\left(\frac{2}{p}\right) = 1$ gilt, bestand das Problem vor allem darin, eine *ungerade* Primzahl mit den geforderten Eigenschaften anzugeben. In der überwiegenden Zahl der Fälle ist unser Beweis wieder konstruktiv.
Außerdem ist es uns gelungen, den Satz von Salié auf quadratische Reste zu übertragen: Es gibt eine Konstante $c > 0$ derart, daß für unendlich viele Primzahlen $\pi_p > c \cdot \log p$ gilt. Damit stellt $\log p$ eine Schranke dar, die nicht unterboten werden kann.

Unser eigentliches Interesse bestand darin, obige Folgerung soweit wie möglich ohne das Klassenzahl-1-Theorem von Heegner-Baker-Stark zu erhalten. Kann man nämlich die Abschätzung $\pi_p < \sqrt{p}$ auf elementare Weise ohne Heegner-Baker-Stark nachweisen, gewinnt man einen neuen, elementaren Zugang zum Klassenzahl-1-Theorem. Dies wäre insofern wünschenswert, als die vorliegenden Beweise dieses Theorems entweder sehr tiefliegende Methoden der analytischen oder der algebraischen Zahlentheorie (Klassen-

körpertheorie, elliptische Kurven, komplexe Multiplikation) gebrauchen. Unsere Überlegungen gehen dabei von folgender Tatsache aus: Ist $p > 7$ eine Primzahl, so existieren zwei eindeutig bestimmte ungerade natürliche Zahlen a, b mit $p = a^2 + 2b^2$. Diese Aussage geht letztlich auf Carl Friedrich Gauß zurück, ihr Beweis verwendet einfache analytische Methoden. Von hier aus gelangen wir zu einer von Heegner-Baker-Stark unabhängigen Beschreibung der Primzahlen mit Klassenzahl 1:

Hauptsatz 3

Sei $p > 7$ eine Primzahl, $h(-p) = 1$ und $p = a^2 + 2b^2$ mit $a, b \in \mathbb{N}$.
Dann gilt:

(i) $r = \frac{a^2+b^2}{2}$ *ist eine Primzahl mit* $r \equiv 1\,(4)$.

(ii) a *ist nur durch Primzahlen* $q \equiv 5, 7\,(8)$ *teilbar und*
b *ist nur durch Primzahlen* $q \equiv 3\,(4)$ *teilbar.*

(iii) $a + b$ *und* $a - b$ *sind nur durch ungerade Primzahlen* $q \equiv 5, 11\,(12)$ *teilbar.*

(iv) $2a + b$ *ist für* $p > 67$ *nur durch Primzahlen* $q \equiv 3\,(4)$ *teilbar und*
$2a - b$ *ist nur durch Primzahlen* $q \equiv 3\,(4)$ *teilbar.*

(v) $a + 2b$ *ist für* $p > 43$ *nur durch Primzahlen* $q \equiv 13, 17, 19, 23\,(24)$ *teilbar und*
$a - 2b$ *ist für* $p > 19$ *nur durch Primzahlen* $q \equiv 13, 17, 19, 23\,(24)$ *teilbar.*

(vi) $a + 4b$ *ist für* $p > 67$ *nur durch Primzahlen* $q \equiv 5, 7\,(8)$ *teilbar und*
$a - 4b$ *ist nur durch Primzahlen* $q \equiv 5, 7\,(8)$ *teilbar.*

Die sechs angegebenen Bedingungen sollen sicherstellen, daß kein quadratischer Rest $q < \frac{p+1}{4}$ existiert, was $h(-p) > 1$ nach sich zöge. Sie können durch weitere analoge Bedingungen ergänzt werden, in der Praxis wird dies aber unhandlich. Unter den Primzahlen im Bereich $7 < p < 10^6$ gibt es nur zwei Stück, die diese Bedingungen erfüllen und für die trotzdem $h(-p) > 1$ ist. Dabei ist $546067 = 487^2 + 2 \cdot 393^2$ der kleinste „Ausreißer“. Das ursprünglich Ziel, auf diese Weise das Klassenzahl-1-Problem zu lösen, würde erfordern, daß man zunächst einen Katalog von Bedingungen für $h(-p) = 1$ aufstellt, der keine Ausnahmen zuläßt, und anschließend nachweist, daß es keine Primzahl geben kann, welche den aufgestellten Bedingungen genügt. Davon sind wir jedoch weit entfernt. Es bleibt dennoch meine Überzeugung, daß $h(-p) > 1$ für $p > 163$ deshalb richtig ist, weil es dann immer „kleine“ Primteiler von $\mathbb{Z}$-Linearkombinationen in a und b gibt, die quadratische Reste modulo p sind.
Nach einem Satz von Frobenius-Rabinowitsch ist $h(-p) = 1$ in unserer Situation gleichwertig damit, daß $r(x) = x^2 - x + \frac{p+1}{4}$ für alle ganzen Zahlen x im Bereich $1 \leqslant x < \frac{p+1}{4}$ eine Primzahl ist. Mit Blick auf Teilaussage (i) ist bemerkenswert, daß $r = r(\frac{a+1}{2})$ gilt. Durch weitere Primforderungen an $r(x)$ läßt sich Hauptsatz 3 also verbessern. Allerdings sind Primzahltests immer aufwendig.

Gescheitert bin ich letztlich auch bei dem Versuch, das Klassenzahl-1-Problem durch sukzessive Kongruenzen oder durch Siebmethoden anzugehen. Ebensowenig hilfreich war die bekannte Zagiersche Interpretation der Dirichletschen Klassenzahlformel, wonach $h(-p) = 1$ gleichwertig damit ist, daß die Anzahl der quadratischen Reste mod p im Intervall $[1, \frac{p+1}{2}[$ ganau dreimal so groß ist wie die der Nichtreste.

Wenn das Thema einer Arbeit so stark in die Geschichte der Zahlentheorie verwoben ist wie das der vorliegenden Arbeit, dann gehört es zu ihrer Aufgabe, die bestehenden Erkenntnise zu sichten und zusammenzutragen. Dabei hat sich gezeigt, daß die Arbeit frührerer Mathematiker allzu leicht in Vergessenheit gerät oder vor dem Hintergrund neuer Begriffsbildungen als „veraltet“ angesehen und nicht weiter beachtet wird. Ein weiteres Ziel dieser Arbeit ist es daher, auf die Leistungen Trygve Nagells aufmerksam zu machen, dessen großartige Arbeiten oftmals nicht richtig gewürdigt werden. In vieler Hinsicht war Nagell der Wegbereiter für uns, an seiner klaren Argumentation und seinen brillanten Beweisansätzen haben wir uns immer wieder orientiert.

Zum Schluß ist es mir ein inneres Bedürfnis, mich bei Herrn Prof. Dr. Peter Schmid für die großartige Betreuung zu bedanken. Seine vielfältigen Anregungen und Ratschläge, mitgeteilt in zahllosen Gesprächen und e-Mails, waren eine unschätzbare Hilfe. Ebenso wichtig war für mich, daß er mich in Zeiten geringer Hoffnung ermutigt und unterstützt hat und daß er den Schwierigkeiten einer externen Promotion neben Beruf und Familie mit grenzenlosem Verständnis und Wohlwollen gegenüberstand.

Notationen

$\mathbb{N} = \{1; 2; 3; \ldots\}$	Menge der natürlichen Zahlen
$\mathbb{Z}$	Ring der ganzen Zahlen
$\mathbb{P}$	Menge der (rationalen) Primzahlen
$(a, b) = c$	Kurzform des größten gemeinsamer Teilers von a und b
$v_p(a) = e$	Der p-Anteil in der Primfaktorzerlegung von $a = p^e \prod_{p_i \neq p} p_i^{e_i}$
$a \equiv b\,(m)$	Kurzform von $a \equiv b\,(\mathrm{mod}\, m)$
$\left(\frac{a}{p}\right)$	Legendre-Symbol von a modulo p
π_p	Kleinster ungerader primer quadratischer Rest modulo p
ψ_p	Kleinster ungerader primer quadratischer Nichtrest modulo p
$f = (a, b, c)$	Kurzform der binären quadratischen Form $f(X, Y) = aX^2 + bXY + cY^2$
$h(D)$	Klassenzahl der eigentlichen Äquivalenzklassen positiv definiter quadratischer Formen mit Diskriminante D
$h(K)$	Klassenzahl der Idealklassengruppe des imaginär-quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{-d})$
R_K	Ring der ganzen Zahlen in K
$N(\alpha)$	Norm des Elements $\alpha \in K$
$\mathbb{P}_K$	Menge der Primelemente in R_K

1. Binäre quadratische Formen

Wir geben einige Sätze aus der Theorie der binären quadratischen Formen wieder, die im folgenden häufig benötigt werden und die letztlich auf Joseph Louis Lagrange, Adrien Marie Legendre oder Carl Friedrich Gauß zurückgehen.
Dazu rufen wir uns zunächst in Erinnerung, daß man unter einer *binären quadratischen Form*

$$f(X,Y) = aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y]$$

ein homogenes Polynom zweiten Grades in zwei Variablen mit Koeffizienten a, b, $c \in \mathbb{Z}$ versteht. Eine Form f soll *primitiv* heißen, falls a, b und c teilerfremd sind, das heißt, falls $(a,b,c) = 1$ gilt. Die ganze Zahl $D = b^2 - 4\,ac$ wird *Diskriminante von* f genannt, sie ist das wichtigste Unterscheidungsmerkmal quadratischer Formen.
Man sagt, daß eine Zahl $m \in \mathbb{Z}$ von der Form f *dargestellt* wird, wenn es x, $y \in \mathbb{Z}$ gibt, welche die Gleichung

$$f(x,y) = m$$

erfüllen. Wenn x und y überdies teilerfremd sind, sagt man, daß m von f *eigentlich dargestellt* wird.
Schon Lagrange hat in seinen *Recherches d'Arithmétique* den folgenden Satz bewiesen, dessen Originalbeweis z. B. auf S. 41f. in [54], einer kurzen Geschichte der Zahlentheorie von Winfried Scharlau und Hans Opolka, wiedergegeben wird:

(1.1) Satz
Wenn $m \in \mathbb{Z}$ von einer Form der Diskriminante D eigentlich dargestellt wird, dann wird auch jeder Teiler von m von einer Form der Diskriminante D eigentlich dargestellt.

Formen mit positiver Diskriminante stellen sowohl positive als auch negative Zahlen dar, sie heißen *indefinit*. Formen mit negativer Diskriminante hingegen stellen entweder ausschließlich positive oder ausschließlich negative Zahlen dar, wobei das Vorzeichen von a den Ausschlag gibt. Ist $a < 0$, erhält man *negativ definite* Formen, für $a > 0$ erhält man *positiv definite* Formen, mit denen wir uns in dieser Arbeit beschäftigen.

Der zentrale Begriff in der Theorie binärer quadratischer Formen ist der der *Äquivalenz.* Mit ihm erst lassen sich viele konkrete Probleme überhaupt lösen und systematisieren. Zwei Formen $f(X,Y)$ und $g(X,Y)$ heißen dabei *äquivalent,* wenn es α, β, γ, $\delta \in \mathbb{Z}$ mit $\alpha\delta - \beta\gamma = \pm 1$ solcherart gibt, daß

$$f(X,Y) = g(\alpha X + \beta Y, \gamma X + \delta Y)$$

gilt, das heißt, wenn f durch die umkehrbare ganzzahlige lineare Substitution

$$X \to \alpha X + \beta Y$$

$$Y \to \gamma X + \delta Y$$

aus g hervorgeht.
Quadratische Formen kann man bekanntlich auch mit Hilfe von Matrizen beschreiben:

$$f(X,Y) = aX^2 + bXY + cY^2 = (X,Y) \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

Schreibt man für die Formen f und g abkürzend $f = (a,b,c)$ und $g = (a',b',c')$, so bedeutet Äquivalenz von Formen in der Sprache der Matrizen, daß es eine 2×2-Matrix $T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$, also mit $\det T = \pm 1$ gibt, so daß

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a' & \frac{b'}{2} \\ \frac{b'}{2} & c' \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

erfüllt ist.
Gilt überdies $\det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \alpha\delta - \beta\gamma = +1$, spricht man von *eigentlicher Äquivalenz.*

Aus der Beschreibung der Äquivalenz mit Hilfe von Matrizen wird folgender zertraler Satz ersichtlich, mit dem man von einer Lösung (x,y) der Gleichung $f(x,y) = m$ eine Lösung von $g(x,y) = m$ erschließen kann, wenn f und g eigentlich äquivalent sind.

(1.2) Satz
Eigentlich äquivalente Formen stellen genau dieselben Zahlen eigentlich dar.

Die eigentliche Äquivalenz von Formen ist eine Äquivalenzrelation, welche nicht nur die Darstellbarkeit von Zahlen, sondern auch die Primitivität, die Definitheit und die Diskriminante invariant läßt, siehe hierzu beispielsweise [63] auf S. 60f. Die Äquivalenzklassen von Formen werden häufig einfach *Klassen* genannt. Die Menge aller Formen mit vorgegebener Diskriminante D zerfällt also in eine oder mehrere Klassen, deren Formen alle dieselben Werte annehmen.

Ein wesentliches Resultat der *Disquisitiones arithmeticae* ist es, daß die Menge $Cl(D)$ der eigentlich äquivalenten Klassen von Formen der Diskriminante D eine abelsche Gruppe ist. Als Verknüpfung fungiert eine genau bestimmte Produktbildung, die *Komposition von Formen*. Das zugehörige Neutralelement bildet die sogenannte *Hauptklasse*, die Klasse, in welcher die *Hauptform* $X^2 - \frac{D}{4}Y^2$ bzw. $X^2 + XY + \frac{1-D}{4}Y^2$ enthalten ist.
Daß es in jeder Klasse eine eindeutig bestimmte, leicht anzugebende Form mit sehr praktikablen Eigenschaften gibt, ist die Aussage des folgenden, nichttrivialen Satzes, der in kaum einem Lehrbuch vollständig ausgeführt wird, weil er viele kleinschrittige Rechnungen erfordert. Gute Beweisskizzen findet man beispielsweise in [4] auf S. 13–17, in [10] auf S. 27f. oder in [63] auf S. 59f.

(1.3) Satz von der reduzierten Form

In jeder eigentlichen Äquivalenzklasse von Formen negativer Dikriminante gibt es eine eindeutig bestimmte Form $f(X,Y) = aX^2 + bXY + cY^2$ *mit*

(i) $|b| \leqslant a \leqslant c$ *und*

(ii) $b \geqslant 0$, *falls* $|b| = a$ *oder* $a = c$ *gilt,*

die sogenannte reduzierte Form, *wobei* $|b| \leqslant a \leqslant \sqrt{\frac{|D|}{3}}$ *gilt.*

Bezeichnet $h(D)$ die Anzahl eigentlicher Äquivalenzklassen positiv definiter Formen mit negativer Diskriminate D, so läßt sich aus diesem Satz leicht erschließen, daß diese *Klassenzahl* $h(D)$ stets endlich ist. Die *Klassengruppe* ist somit eine endliche abelsche Gruppe der Ordnung $h(D)$.
Neben der Einteilung in Klassen gibt es noch eine übergeordnete Einteilung. Man sagt, daß zwei primitive positiv definite Formen mit Diskriminante D dasselbe *Geschlecht* haben, wenn sie dieselben Werte in $(\mathbb{Z}/D\mathbb{Z})^*$ darstellen. Aus dem oben Gesagten wird deutlich, daß immer ganze Klassen in einem Geschlecht liegen und daß für die Geschlechterzahl $g(D)$ immer $g(D) \leqslant h(D)$ gilt.
Den allgemeinen Zusammenhang zwischen quadratischen Formen und quadratischen Resten stellt folgender Satz her, der z. B. in [10] auf S. 26 beweisen wird.

(1.4) Darstellungssatz

Sei $D \equiv 0, 1\,(4)$ *eine ganze Zahl und* q *eine ungerade, zu* D *teilerfremde Zahl.*
Es gilt $\left(\frac{D}{q}\right) = 1$ *genau dann, wenn* q *durch eine quadratische Form mit Diskriminante* D *eigentlich dargestellt wird.*

2. Das Klassenzahl-1-Problem

2.1 Die klassische Formulierung von Gauß

Gauß betrachtet in den *Disquisitiones arithmeticae* [17] wie schon Legendre vor ihm Formen von der Gestalt

$$aX^2 + 2bXY + cY^2,$$

wobei er die Zahl $D = b^2 - ac$ als sogenannte *Determinante* einführt. Dieses Vorgehen brachte Schwierigkeiten mit sich: Um beispielsweise die Form $X^2+XY+5\,Y^2$ betrachten zu können, mußte Gauß ein Vielfaches bilden und auf die Form $2\,X^2 + 2\,XY + 10\,Y^2$ ausweichen. Dies zwang ihn, in Art. 226 zwischen *eigentlich primitiven* Formen, für die $(a, 2b, c) = 1$ gilt, und *uneigentlich primitiven* Formen, welche $(a, 2b, c) = 2$ erfüllen, zu unterscheiden und die Formen gemäß $(a, 2b, c)$ in *Ordnungen* einzuteilen.
Im Art. 303 macht Gauß Bemerkungen zur Geschlechter- und Klassenzahl negativer Diskriminanten. Dann folgt die entscheidende Passage:

> *Ferner scheint die Reihe der Determinanten, denen dieselbe gegebene Klasseneinteilung (d. h. eine gegebene Anzahl sowohl von Geschlechtern als auch von Klassen) entspricht, stets abzubrechen, welche ziemlich seltsame Bemerkung wir durch einige Beispiele erläutern. (Die erste, römische, Zahl zeigt die Anzahl der eigentlich primitiven positiven Geschlechter, die folgende die Anzahl der in jedem einzelnen Geschlechte enthaltenen Klassen an; dann folgt die Reihe der der Determinanten, welchen jene Klassifikation entspricht, und deren negatives Vorzeichen wir der Kürze wegen weggelassen haben.)*

I. 1	1, 2, 3, 4, 7
I. 3	11, 19, 23, 27, 31, 43, 67, 163
I. 5	47, 79, 103, 127
I. 7	71, 151, 223, 343, 463, 487
II. 1	5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58
II. 2	14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193
IV. 1	21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253
VIII. 1	105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760
XVI. 1	840, 1320,1365, 1848.

> *Analog finden sich 20 Determinanten (deren grösste gleich* -1423 *ist), welchen die die Klassifikation I. 9 entspricht; 4 (die grösste gleich* -1303*), welchen die Klassifikation I. 11 entspricht, u. s. w. [...] Da die Tafel, aus welcher diese Beispiele entnommen sind, weit über die grössten hier vorkommenden Determinanten hinaus fortgesetzt ist, so scheint es nicht zweifelhaft zu sein, dass die hingeschriebenen Reihen in der That abbrechen und diesen Schluss werden wir der Analogie gemäß auch auf andere Klassifikationen ausdehnen dürfen. [...] Die strengen Beweise dieser Bemerkungen aber scheinen sehr schwierig zu sein.*

Gauß hat hier also explizit folgende Vermutung ausgesprochen:

(2.1) Allgemeines Klassenzahl-Problem
Für jedes $n \in \mathbb{N}$ *ist die Anzahl der Determinanten* D *mit* $h(D) = n$ *endlich.*

Implizit ist aber auch die Aufgabe enthalten, für ein vorgegebenes $n_0 \in \mathbb{N}$ sämtliche Determinanten D mit $h(D) = n_0$ konkret zu bestimmen. Für die in der Tabelle angegebenen Klassenzahlen erhebt Gauß — vorsichtig und unausgesprochen — den Anspruch der Vollständigkeit. Für $h(D) = 1$ ergibt sich damit

(2.2) Das Gaußsche Klassenzahl-1-Problem
$D = -1, -2, -3, -4, -7$ *sind die einzigen Determinanten mit* $h(D) = 1$.

Diese Vermutung konnte — was wenig bekannt ist — 1903 von Edmund Landau in [28] bewiesen werden. Der Originalbeweis ist auch heute ohne weiteres lesbar und kommt mit elementaren Mitteln aus. Ein Beweis in moderner Terminologie findet sich in dem wunderbaren Buch von David Cox [10] auf S. 31f. unter Satz 2.18.
Es sei hier noch bemerkt, daß Gauß die 65 Determinanten der Klassifikationen I. 1, II. 1, IV. 1, VIII. 1 und XVI. 1 auch deshalb angibt, weil es sich hierbei um Eulers *numeri idonei* handelt. Gauß konnte im weiteren nämlich nachweisen, daß genau dann in jedem Geschlecht eine einzige Klasse enthalten ist, wenn die zugehörige Determinante ein *numerus idoneus* ist.

2.2 Die allgemeine Formulierung

Auch wenn das Gaußsche Vorgehen bei der Beweisführung vieler Sätze deutliche Vorteile bietet, konnte es sich gegenüber der allgemeinen Definition der quadratischen Formen als $f(X, Y) = aX^2 + bXY + cY^2$ mit Diskriminante $D = b^2 - 4\,ac$ nicht durchsetzen. Denn dieses Vorgehen ist viel geeigneter, den bekannten Zusammenhang

zwischen der Klassengruppe quadratischer Formen und der Idealklassengruppe quadratischer Zahlkörper herzustellen, eine Einsicht, die wir — wie Duncan Buell in [4] auf S. 107 ausführt — vor allem Ferdinand Gotthold Eisenstein verdanken: Ist nämlich $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, ein imaginär-quadratischer Zahlkörper mit Diskriminante D_K und bezeichnet $h(K)$ die Anzahl der Idealklassen im zugehörigen Ring R_K der ganzen Zahlen, so gilt bekanntlich $h(D_K) = h(K)$, das heißt, die Anzahl der Klassen eigentlich äquivalenter quadratischer Formen der Diskriminante D_K entspricht der Anzahl der Idealklassen in R_K.
Die Konvertierung der Resultate vom Gaußschen System ins Eisensteinsche und umgekehrt ist leider kompliziert, weil sich Formen *und* Diskriminanten unterscheiden. So ist die Eisensteinsche Diskriminante das Vierfache der Gaußschen Determinante. Für die Umrechnung der Klassenzahlen ist eine diffizile Fallunterscheidung nötig, bevor man beispeilsweise Buells Satz 7.5 in [4] auf S. 118 anwenden kann. Für $D = -d$ mit $d \equiv 3\,(8)$ gilt unter bestimmten Bedingungen die Formel $h(4D) = 3\,h(D)$, so daß für die Gaußschen Determinanten in der zweiten Zeile seiner Tabelle in unserem System meist $h(D) = 1$ gilt, siehe dazu auch [56].
Von diesen Umrechnungen bleibt das allgemeine Klassenzahlproblem (2.1) unberührt, das Klassenzahl-1-Problem hingegen muß modifiziert werden:

(2.3) Klassenzahl-1-Problem
Sei $K = \mathbb{Q}(\sqrt{-d})$ ein imaginär-quadratischer Zahlkörper mit Diskriminante D_K.
Die neun Diskriminanten $D_K = -3, -4, -7, -8, -11, -19, -43, -67, -163$ sind die einzigen Diskriminanten mit $h(K) = h(D_K) = 1$.

Für $h(K) = 1$ besteht zunächst folgende notwendige Bedingung, die sich in bekannter Weise aus der Arithmetik der quadratischen Zahlkörper ergibt:

(2.4) Satz
Sei $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, ein imaginär-quadratischer Zahlkörper.
Ist $h(K) = 1$, dann gilt $d = 1, 2, 7$ oder $d = p$ mit einer Primzahl $p \equiv 3\,(8)$.

Beweis:
Sei $p \in \mathbb{P}$ kein Primelement im Ring der ganzen Zahlen $R = R_K$, das heißt, p verzweigt oder zerfällt in R. Nach der Zerlegungstheorie in quadratischen Zahlkörpern gibt es also Primideale $\mathfrak{p}$, $\mathfrak{p}' \in \mathbb{P}_K$ mit $pR = \mathfrak{p}\mathfrak{p}'$. Da aus $h(K) = 1$ folgt, daß R ein Hauptidealring und $\mathfrak{p}$ ein Hauptideal ist, existiert ein Primelement $\pi \in R\backslash R^*$ mit $pR = (\pi\bar{\pi})R$, wobei $\bar{\pi}$ das zu π (komplex) konjugierte Element ist. Wegen $\pi\bar{\pi} = N(\pi) \in \mathbb{Z}$ und $N(\pi) \neq \pm 1$ muß $p = \pi\bar{\pi}$ gelten. Wir unterscheiden drei Fälle:

1. Fall: Ist $-d \equiv 2,\, 3\,(4)$, so gilt $D_K = -4\,d$ und $R = \mathbb{Z}[\sqrt{-d}]$. Wegen $2 \mid D_K$ verzweigt $p = 2$ in R, siehe z. B. 13.1.4 in [25]. Schreibt man $\pi = r + is\sqrt{d}$ mit $r,\, s \in \mathbb{Z}$, so gilt

$$2 = \pi\bar{\pi} = (r + is\sqrt{d})(r - is\sqrt{d}) = r^2 + d\,s^2.$$

Diese Gleichung ist nur für $d = 1$ oder $d = 2$ erfüllbar.
2. Fall: Ist $-d \equiv 1\,(8)$, so gilt $D_K = -d$ und $R = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$. Wegen $2 \nmid D_K$ und $D_K \equiv 1\,(8)$ zerfällt $p = 2$ in R, siehe z. B. 13.1.4 in [25]. Schreibt man $\pi = \frac{r}{2} + i\frac{s}{2}\sqrt{d}$ mit $r,\, s \in \mathbb{Z}$ und $r \equiv s\,(2)$, so gilt

$$2 = \pi\bar{\pi} = \frac{r^2}{4} + d\,\frac{s^2}{4} \quad \text{und damit} \quad 8 = r^2 + d\,s^2.$$

Diese Gleichung ist nur für $d = 7$ erfüllbar.
3. Fall: Ist $-d \equiv 5\,(8)$, so gilt $D_K = -d$ und $R = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$. Wählt man p als kleinsten Primteiler von $d = |D_K|$, so verzweigt p in R, siehe z. B. 13.1.5 in [25]. Schreibt man $\pi = \frac{r}{2} + i\frac{s}{2}\sqrt{d}$ mit $r,\, s \in \mathbb{Z}$ und $r \equiv s\,(2)$, so gilt

$$p = \pi\bar{\pi} = \frac{r^2}{4} + d\,\frac{s^2}{4} \quad \text{und damit} \quad 4\,p = r^2 + d\,s^2.$$

Hieraus folgt, daß $d = p \in \mathbb{P}$ mit $d = p \equiv 3\,(8)$ gelten muß.
Denn wäre $d = p \cdot q$, so müßte $q > p \geqslant 3$ gelten, da 2 in dieser Situation träge in R ist und $p = q$ auf $d = p^2 \equiv 1\,(8)$ führte. q wäre überdies ungerade, woraus $q > 4$ folgte. Außerdem müßte $r^2 \geqslant 1$ und $s^2 \geqslant 1$ gelten, andernfalls erhielte man einfache Widersprüche. Hieraus ergäbe sich aber $4\,p = r^2 + d\,s^2 \geqslant 1 + p \cdot q > 1 + 4\,p$, was unmöglich ist, q. e. d.

Aufgrund dieses Satzes befinden wir uns überwiegend in folgender

(2.5) Situation
$K = \mathbb{Q}(\sqrt{-p})$ sei für eine Primzahl $p > 7$ mit $p \equiv 3\,(8)$ ein imaginär-quadratischer Zahlkörper. Da für $p \equiv 3, 7\,(8)$ stets $D_K = -p$ gilt, wird die Klassenzahl für solche Primzahlen vereinfacht mit $h(-p)$ notiert.

2.3 Die Lösungen von Heegner, Baker und Stark

Die greifbaren Bemühungen, das Klassenzahl-1-Problem in seiner allgemeinen Version zu lösen, setzten zu Beginn des 20. Jahrhunderts ein. Unmittelbar auf Landaus Erfolg bei Gauß' speziellerer Version hat Matiaš Lerch 1903 in [31] bemerkt, daß man mit diesen Methoden den allgemeinen Fall nicht angreifen kann.

1918 hat Edmund Landau dann in [29] eine Verbindung zwischen dem Klassenzahl-Problem und der ananlytischen Theorie der L-Reihen hergestellt, was eine eifrige Forschungstätigkeit auslöste, die 1934 in dem Resultat von Heilbronn und Linfoot [23] gipfelte, wonach es höchstens zehn negative Diskriminanten mit Klassenzahl 1 geben kann, das heißt außer den neun bekannten höchstens eine weitere.
1952 konnte der Gymnasiallehrer Kurt Heegner in [22] den ersten Beweis für das Klassenzahl-1-Problem (2.3) vorlegen, wobei sich die Fachwelt zunächst aber uneinig darüber war, ob der Beweis lückenhaft sei oder nicht. Erst nach Heegners Tod haben die Erläuterungen Max Deurings 1968 in [11] und Harold Starks 1969 in [59] alle Zweifel über den Beweisgang zerstreut. Die sehr tiefliegende klassenkörpertheoretische Argumentation Heegners verwendet elliptische Kurven, die komplexe Multiplikation und stützt sich wesentlich auf die Berechnung der sogenannten Weber-Funktionen. Eine ausführliche Darstellung findet man in [10] im dritten Kapitel.
1966 haben Alan Baker und Harold Stark unabhängig voneinander weitere Beweise vorgelegt. Bakers analytischer Beweis in [2] basiert auf Logarithmen algebraischer Zahlen, Starks Beweis in [58] basiert auf dem L-Reihen-Kalkül und Ideen Heegners. Die Verbindungen zwischen den Arbeiten von Heegner und Stark hat Carl Siegel in [57] dargestellt.
Es gilt also der folgende Satz, über dessen Geschichte Dorian Goldfeld in [18] einen sehr guten Überblick gibt:

(2.6) Klassenzahl-1-Theorem von Heegner-Baker-Stark
Sei $K = \mathbb{Q}(\sqrt{-d})$ *ein imaginär-quadratischer Zahlkörper mit Diskriminante* D_K.
Genau für $D_K = -3, -4, -7, -8, -11, -19, -43, -67, -163$ *gilt* $h(D_K) = 1$.

Im folgenden versuchen wir, einen elementaren Zugang zu diesem Theorem zu gewinnen in der Hoffnung, daß man auf diese Weise die algebraischen Gesetzmäßigkeiten der Arithmetik quadratischer Zahlkörper besser erkennen kann, welche von analytischen Mitteln wie dem L-Reihen-Kalkül, der Dirichletschen Klassenzahlformel etc. verdeckt werden. Wir suchen dabei nach elementareren Methoden, um für möglichst viele Primzahlen $p > 163$ die Klassenzahl 1 auszuschließen.
Es gibt nun im wesentlichen zwei Möglichkeiten, dies zu erreichen: Man kann $h(-p) = 1$ mit primen quadratischen Resten oder mit bestimmten primen Werten der Hauptform $f(X, Y) = X^2 + XY + \frac{p+1}{4}Y^2$ in Verbindung bringen. In den beiden folgenden Kapiteln werden wir diese Methoden entwickeln und feststellen, daß sie aufs engste miteinander verbunden sind.

3. Ein elementarer Lösungsansatz des Klassenzahl-1-Problems

3.1 Das Lemma von Nagell

Der Dreh- und Angelpunkt für eine elementare Lösung des Klassenzahl-1-Problems könnte im folgenden Sachverhalt zu finden sein, der schon im 19. Jahrhundert bekannt war, aber — soweit ich sehe — erst 1922 zum ersten Mal explizit ausgesprochen wurde, und zwar vom norwegischen Mathematiker Trygve Nagell in [38] auf S. 146. Es handelt sich um ein sehr einfaches Klassenzahl-1-Kriterium:

(3.1) Lemma von Nagell
Sei p eine Primzahl mit $p \equiv 3\,(8)$.
Ist $h(-p) = 1$, dann gilt $\left(\frac{q}{p}\right) = -1$ für alle Primzahlen $q < \frac{p+1}{4}$.

1. Beweis mit Hilfe quadratischer Formen (nach Nagell):
Gilt $h(-p) = 1$, so ist $f(X,Y) = X^2 + XY + \frac{p+1}{4}Y^2$ die einzige reduzierte Form mit Diskriminante $D = -p$. Ist die Primzahl $q < \frac{p+1}{4}$ und wäre $\left(\frac{q}{p}\right) = 1$, so erhielte man nach dem dem quadratischen Reziprozitätsgesetz

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

Folglich gäbe es nach dem Darstellungssatz (1.4) eine eigentliche Darstellung von q durch $f(X,Y)$, es existierten also teilerfremde $x, y \in \mathbb{Z}$ mit

$$q = x^2 + xy + \tfrac{p+1}{4}y^2,$$

wobei x, $y \neq 0$ ist. Dann folgte aber mit $|x|$, $|y| \geqslant 1$

$$q = x^2 + xy + \tfrac{p+1}{4}y^2 = \tfrac{1}{4}(2\,x + y)^2 + \tfrac{1}{4}p\,y^2 = \tfrac{p\,y^2 + (2\,x+y)^2}{4} \geqslant \tfrac{p+1}{4},$$

was ein Widerspruch zur Wahl von q wäre, q. e. d.

2. Beweis mit Hilfe von Idealen (nach Ayoub/Chowla [1]):
Ist $q < \frac{p+1}{4}$ und wäre $\left(\frac{q}{p}\right) = 1$, dann wäre wie im 1. Beweis $\left(\frac{D}{q}\right) = 1$. Nach der Zerlegungstheorie in quadratischen Zahlkörpern würde also q in R zerfallen: $qR = \mathfrak{q}\mathfrak{q}'$ mit konjugierten Primidealen $\mathfrak{q}, \mathfrak{q}' \in \mathbb{P}_K$. Wegen $h(K) = 1$ wäre R ein Hauptidealring und $\mathfrak{q}$ ein Hauptideal, es existierte demnach ein Primelement $\xi = x + y\,\frac{1+\sqrt{-p}}{2} \in R$ mit $y \neq 0$ und $\mathfrak{q} = \xi R$. Es folgte

$$q = \xi\xi' = N(\xi) = x^2 + xy + \tfrac{p+1}{4}y^2$$

und damit $4\,q = (2\,x + y)^2 + p\,y^2 \geqslant 1 + p$, also $q \geqslant \frac{p+1}{4}$, was ein Widerspruch zur Wahl von q wäre, q. e. d.

(3.2) Erster elementarer Lösungsansatz

Könnte man für jede Primzahl $p \equiv 3\,(8)$ mit $p > 163$ auf elementare Weise zeigen, daß stets eine ungerade Primzahl $q < \frac{p+1}{4}$ mit $\left(\frac{q}{p}\right) = 1$ existiert, dann müßte mit der Kontraposition des Lemmas von Nagell $h(-p) > 1$ gelten, und man hätte einen weiteren Beweis des Klassenzahl-1-Theorems.

Wir verfolgen daher in der gesamten Arbeit letztlich das Ziel, für jede Primzahl $p \equiv 3\,(8)$ mit $p > 163$ unabhängig von $h(-p)$ möglichst „kleine“ prime Reste modulo p zu finden. Diesen Weg scheint Nagell als erster wirklich konsequent beschritten zu haben, wie seine Arbeiten vor allem in den fünfziger Jahren des vorigen Jahrhunderts belegen [39, 40, 41, 42]. Ansonsten wurde diese Idee nur vereinzelt und ohne Bezugnahme auf die Vorarbeit Nagells verfolgt, so beispielsweise 1962 von Ian Connell in [9] und später von Saravadaman Chowla in Arbeiten mit verschiedenen Partnern [1, 7, 6]. Auf diese Ansätze, aus denen sich anscheinend keine intensiven Bemühungen um das Klassenzahl-1-Problem ergeben haben, werden wir im 6. Kapitel detailliert eingehen.

3.2 Erste Anwendungen

Die aus Satz (2.4) bekannte Kongruenzbedingung an p für $h(-p) = 1$ kann man mit Hilfe des Lemmas von Nagell deutlich verschärfen, indem man für kleine Primzahlen wie 3, 5 und 7 ausschließt, daß sie quadratische Reste modulo p sind. Dazu benötigen wir folgendes Lemma, das sich wie die ersten beiden Ergänzungssätze zum Quadratischen Reziprozitätsgesetz aus elementaren gruppentheoretischen Überlegungen ergibt:

(3.3) Dritter, vierter und fünfter Ergänzungssatz
Für alle Primzahlen $p \neq 3, 5, 7$ gilt:

$$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1\,(12)$$

$$\left(\frac{5}{p}\right) = 1 \iff p \equiv \pm 1, \pm 11\,(20)$$

$$\left(\frac{7}{p}\right) = 1 \iff p \equiv \pm 1, \pm 3, \pm 9\,(28)$$

Schließt man aus, daß 3 ein quadratischer Rest modulo p ist, erhält man:

(3.4) Satz
Sei $p > 11$ eine Primzahl mit $p \equiv 3\,(8)$.
Ist $h(-p) = 1$, dann gilt $p \equiv 19\,(24)$.

Beweis:
Wegen $p \equiv 3\,(8)$ muß $p \equiv 3, 11$ oder $19\,(24)$ gelten.
Wäre $p \equiv 3\,(24)$, dann könnte p wegen $p = 3 + 24\,k = 3\,(1 + 8\,k)$ keine Primzahl sein, Widerspruch!
Wäre $p \equiv 11\,(24)$, so auch $p \equiv 11\,(12)$ und damit $p \equiv -1\,(12)$. Mit (3.3) würde demnach $\left(\frac{3}{p}\right) = 1$ gelten, woraus wegen $3 < \frac{p+1}{4}$ und der Kontraposition des Lemmas von Nagell $h(-p) > 1$ folgte. Widerspruch!
Daher ist nur der Fall $p \equiv 19\,(24)$ möglich, q. e. d.

Schließt man aus, daß 5 ein quadratischer Rest modulo p ist, erhält man:

(3.5) Satz
Sei $p > 19$ eine Primzahl mit $p \equiv 3\,(8)$.
Ist $h(-p) = 1$, dann gilt $p \equiv 3, 27\,(40)$.

Beweis:
Wegen $p \equiv 3\,(8)$ muß $p \equiv 3, 11, 19, 27$ oder $35\,(40)$ gelten.
Wäre $p \equiv 11\,(40)$, so auch $p \equiv 11\,(20)$. Mit (3.3) würde demnach $\left(\frac{5}{p}\right) = 1$ gelten, woraus wegen $5 < \frac{p+1}{4}$ und der Kontraposition des Lemmas von Nagell $h(-p) > 1$ folgte. Widerspruch!
Wäre $p \equiv 19\,(40)$, so auch $p \equiv 19\,(20)$ und damit $p \equiv -1\,(20)$. Mit (3.3) würde demnach $\left(\frac{5}{p}\right) = 1$ gelten, woraus wegen $5 < \frac{p+1}{4}$ und der Kontraposition des Lemmas von Nagell $h(-p) > 1$ folgte. Widerspruch!
Wäre $p \equiv 35\,(40)$, dann könnte p wegen $p = 35 + 40\,k = 5\,(7 + 8\,k)$ keine Primzahl sein, Widerspruch!
Daher sind nur die Fälle $p \equiv 3, 27\,(40)$ möglich, q. e. d.

Schließt man aus, daß 7 ein quadratischer Rest modulo p ist, erhält man:

(3.6) Satz
Sei $p > 27$ eine Primzahl mit $p \equiv 3\,(8)$.
Ist $h(-p) = 1$, dann gilt $p \equiv 11,\ 43,\ 51\,(56)$.

Beweis:
Wegen $p \equiv 3\,(8)$ muß $p \equiv 3,\ 11,\ 19,\ 27,\ 35,\ 43$ oder $51\,(56)$ gelten.
Wäre $p \equiv 3\,(56)$, so auch $p \equiv 3\,(28)$. Mit (3.3) würde demnach $\left(\frac{7}{p}\right) = 1$ gelten, woraus wegen $7 < \frac{p+1}{4}$ und der Kontraposition des Lemmas von Nagell $h(-p) > 1$ folgte. Widerspruch!
Wäre $p \equiv 19\,(56)$, so auch $p \equiv 19\,(28)$ und damit $p \equiv -9\,(28)$. Mit (3.3) würde demnach $\left(\frac{7}{p}\right) = 1$ gelten, woraus wegen $7 < \frac{p+1}{4}$ und der Kontraposition des Lemmas von Nagell $h(-p) > 1$ folgte. Widerspruch!
Wäre $p \equiv 27\,(56)$, so auch $p \equiv 27\,(28)$ und damit $p \equiv -1\,(28)$. Mit (3.3) würde demnach $\left(\frac{7}{p}\right) = 1$ gelten, woraus wegen $7 < \frac{p+1}{4}$ und der Kontraposition des Lemmas von Nagell $h(-p) > 1$ folgte. Widerspruch!
Wäre $p \equiv 35\,(56)$, dann könnte p wegen $p = 35 + 56\,k = 7\,(5 + 8\,k)$ keine Primzahl sein, Widerspruch!
Daher sind nur die Fälle $p \equiv 11,\ 43,\ 51\,(56)$ möglich, q. e. d.

Schließt man nun sukzessive aus, daß 3 und 5 bzw. 3, 5 und 7 quadratische Reste modulo p sind, erhält man, indem man von den oben erhaltenen Restklassen den Durchschnitt bildet, die folgenden Resultate:

(3.7) Satz
Sei $p > 27$ eine Primzahl mit $p \equiv 3\,(8)$.
1. Ist $h(-p) = 1$, dann gilt $p \equiv 43,\ 67\,(120)$.
2. Ist $h(-p) = 1$, dann gilt $p \equiv 43,\ 67,\ 163,\ 403,\ 547,\ 667\,(840)$.

(3.8) Bemerkung
Klar ist, daß man mit diesem Vorgehen die Dichte δ der Primzahlen p, für die $h(-p) = 1$ möglich ist, schrittweise halbieren kann. Wegen $\varphi(120) = 32$ gilt im ersten Fall $\delta_1 = \frac{2}{32} = \frac{1}{16}$, im zweiten Fall erhält man mit $\varphi(840) = 192$ schon $\delta_2 = \frac{6}{192} = \frac{1}{32}$ usw.
Klar ist aber auch, daß man die Endlichkeit der Menge der Primzahlen mit $h(-p) = 1$ auf diesem Wege nicht zeigen kann. Man braucht andere Methoden.

4. Primwertige quadratische Formen

4.1 Quadratische Formen und quadratische Reste modulo p

Man kann zu weiteren Klassenzahl-1-Kriterien vorstoßen, indem man wie Ferdinand Frobenius und Georg Rabinowitsch binäre quadratische Formen betrachtet.

(4.1) Definition

Für eine Primzahl $p \equiv 3\,(4)$ sei

$$k(X,Y) = X^2 + p\,Y^2,$$

$$f(X,Y) = X^2 + XY + \tfrac{p+1}{4}Y^2.$$

Letzteres ist die Hauptform des Rings der ganzen Zahlen $R = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ in $\mathbb{Q}(\sqrt{-p})$. Aus diesen Formen erhält man die Polynome

$$k(X) = k(X,-1) = X^2 + p \in \mathbb{Z}[X],$$

$$r(X) = f(X,-1) = X^2 - X + \tfrac{p+1}{4} \in \mathbb{Z}[X].$$

Letzteres ist das bekannte *Rabinowitsch-Polynom*, welches schon Euler aufgefallen ist.

Zunächst stellt man folgendes fest:

(4.2) Fundamentallemma

1. *Für alle* $x, y \in \mathbb{Z}$ *gilt* $f(x,y) = \frac{1}{4}\,k(2\,x+y,y) = \frac{1}{4}((2\,x+y)^2 + p\,y^2)$.
2. *Für alle* $x \in \mathbb{N}$ *gilt* $r(x) = \frac{1}{4}\,k(2\,x-1) = \frac{1}{4}((2\,x-1)^2 + p)$.
3. *Es gilt* $r(1) = \frac{p+1}{4}$.
4. *Es gilt* $r(\frac{p+1}{4}) = (\frac{p+1}{4})^2$.

Beweis:

1. $k(2\,x+y,y) = (2\,x+y)^2 + p\,y^2 = 4\,x^2 + 4\,xy + (p+1)y^2 = 4\,f(x,y)$.
2. $k(2\,x-1) = (2\,x-1)^2 + p = 4\,x^2 - 4\,x + (p+1) = 4\,r(x)$.
3. $r(1) = 1^2 - 1 + \frac{p+1}{4} = \frac{p+1}{4}$.
4. $r(\frac{p+1}{4}) = (\frac{p+1}{4})^2 - \frac{p+1}{4} + \frac{p+1}{4} = (\frac{p+1}{4})^2$, q. e. d.

Der erwähnte Zusammenhang mit den quadratischen Resten wird durch das folgende Lemma hergestellt:

(4.3) Reste-Lemma

Sei $p \equiv 3\,(4)$ eine Primzahl.

1. *Jeder Primteiler q von $k(x) = x^2 + p$ ist quadratischer Rest modulo p:*

$$q \mid x^2 + p \Longrightarrow \left(\tfrac{q}{p}\right) = 1.$$

2. *Jeder Primteiler q von $r(x) = x^2 - x + \frac{p+1}{4}$ ist quadratischer Rest modulo p:*

$$q \mid x^2 - x + \tfrac{p+1}{4} \Longrightarrow \left(\tfrac{q}{p}\right) = 1.$$

Insbesondere ist jeder Primteiler von $\frac{p+1}{4}$ quadratischer Rest modulo p.

Beweis:

1. Aus $q \mid x^2 + p$ folgt $q\,r = x^2 + p$ und damit $p = q\,r - x^2$. Hieraus ergibt sich mit dem Quadratischen Reziprozitätsgesetz

$$\left(\tfrac{q}{p}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{p}{q}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{q\,r-x^2}{q}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{-x^2}{q}\right) = \left(\tfrac{-1}{q}\right)^2\left(\tfrac{x^2}{q}\right) = 1.$$

2. Aus $q \mid r(x)$ folgt $q\,r = x^2 - x + \frac{p+1}{4}$, was $-4\,x^2 + 4\,x - 1 + 4\,qr = p$ und damit $p = -(2\,x-1)^2 + 4\,qr$ bedeutet. Also ist

$$\left(\tfrac{q}{p}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{p}{q}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{-(2\,x-1)^2+4\,qr}{q}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{-(2\,x-1)^2}{q}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{-1}{q}\right) = 1.$$

Die Aussage folgt ebenfalls aus 1. und dem Fundamentallemma, q. e. d.

In diesen Zusammenhang gehört auch das folgende Lemma, dessen Korollar wir im letzten Kapitel in Abschnitt 6.3 benötigen:

(4.4) Lemma

Es seien s, t, u, v, $D \in \mathbb{Z}$ und D ungerade. $\frac{1}{4}(s^2 + D\,t^2)$ sei eine ganze Zahl und $|\frac{1}{4}(u^2 + D\,v^2)|$ eine Primzahl.

Ist dann $n = \dfrac{\frac{1}{4}(s^2 + D\,t^2)}{\frac{1}{4}(u^2 + D\,v^2)}$ eine ganze Zahl, so existieren x, $y \in \mathbb{Z}$ mit $n = \frac{1}{4}(x^2 + D\,y^2)$.

Beweis:

Aus den Voraussetzungen $s^2 \equiv -D\,t^2\,(4)$ und $u^2 \equiv -D\,v^2\,(4)$ erhält man durch Multiplikation $s^2u^2 - D^2\,t^2v^2 \equiv 0\,(4)$ bzw. $s^2v^2 - t^2u^2 \equiv 0\,(4)$. Also sind $\frac{1}{2}(su \pm D\,tv)$ bzw. $\frac{1}{2}(sv \mp tu)$ ganze Zahlen.

Man überzeugt sich von folgender Identität:

$$n = \frac{\frac{1}{4}(s^2 + D\,t^2)}{\frac{1}{4}(u^2 + D\,v^2)} = \frac{1}{4}\left(\frac{\frac{1}{2}(su \pm D\,tv)}{\frac{1}{4}(u^2 + D\,v^2)}\right)^2 + \frac{1}{4}D\left(\frac{\frac{1}{2}(sv \mp tu)}{\frac{1}{4}(u^2 + D\,v^2)}\right)^2.$$

Wir zeigen, daß eine der Zahlen $\frac{1}{2}(sv \mp tu)$ durch $\frac{1}{4}(u^2 + D\,v^2)$ teilbar ist. Da nun $|\frac{1}{4}(u^2+D\,v^2)|$ eine Primzahl ist, genügt es zu zeigen, daß ihr Produkt durch $\frac{1}{4}(u^2+D\,v^2)$ teilbar ist. Das Produkt ist

$$\frac{1}{4}(s^2v^2 - t^2u^2) = \frac{1}{4}v^2(s^2 + D\,t^2) - \frac{1}{4}D\,t^2v^2 - \frac{1}{4}t^2u^2 =$$

$$= v^2\,n \cdot \frac{1}{4}(u^2 + D\,v^2) - t^2 \cdot \frac{1}{4}(u^2 + D\,v^2)$$

und demnach durch $\frac{1}{4}(u^2 + D\,v^2)$ teilbar. Daher sind

$$y = \frac{\frac{1}{2}(sv \mp tu)}{\frac{1}{4}(u^2 + D\,v^2)} \text{ und folglich auch } x = \frac{\frac{1}{2}(su \pm D\,tv)}{\frac{1}{4}(u^2 + D\,v^2)}$$

ganze Zahlen, q. e. d.

Dieses Lemma findet sich in [38] auf S. 145f. Wir ergänzen es durch folgendes Korollar, das die Aussage auf die Hauptform $f(X,Y) = X^2 + XY + \frac{p+1}{4}Y^2$ überträgt:

(4.5) Korollar

Es seien s, t, u, $v \in \mathbb{Z}$ und $p \equiv 3\,(4)$ eine Primzahl. $f(s,t)$ sei eine ganze Zahl und $|f(u,v)|$ eine Primzahl.

Ist dann $\dfrac{f(s,t)}{f(u,v)}$ eine ganze Zahl, so existieren x, $y \in \mathbb{Z}$ mit $f(x,y) = \dfrac{f(s,t)}{f(u,v)}$.

Beweis:

Die Aussage folgt mit $D = p$ aus dem vorigen Lemma. Dabei ist Punkt 1 des Fundamentallemmas (4.2) zu berücksichtigen, wenn man die Substitution $s \to (2\,s - 1)$, $u \to (2\,u - 1)$, $x \to (2\,x - 1)$ anwendet, q. e. d.

4.2 Der Satz von Rabinowitsch

Wir sind nun in der Lage, das berühmte Resultat von Georg Rabinowitsch vorzustellen, welches er im August 1912 auf dem V. Internationalen Mathematikerkongreß in Cambridge vorgetragen und 1913 in [49] veröffentlicht hat. Es stellt einen Zusammenhang zwischen der Klassenzahl und den Werten des Rabinowitsch-Polynoms her, die bis zu einer bestimmten Grenze Primzahlen sein müssen:

(4.6) Satz von Rabinowitsch
Sei $p > 3$ eine Primzahl mit $p \equiv 3\,(8)$.
Es gilt $h(-p) = 1$ genau dann, wenn $r(x) = x^2 - x + \frac{p+1}{4} \in \mathbb{Z}$ für alle x mit $1 \leqslant x < \frac{p+1}{4}$ eine Primzahl ist.

Neben dem Originalbeweis, der mit dem euklidischen Algorithmus operiert, gibt es einen Standardbeweis, dessen „⇐“-Richtung sich wesentlich auf den Satz von Minkowski stützt, siehe beispielsweise die Darstellung bei Harvey Cohn in [8] auf S. 156 oder bei Paulo Ribenboim in [50]. Bei Władysław Narkiewicz in [43] auf S. 463ff. findet sich ein etwas anderes Argument, welches den Satz von Kummer-Dedekind benötigt.
Weniger bekannt ist, daß der in Rede stehende Sachverhalt nicht unbedingt zuerst von Rabinowitsch bewiesen wurde. Die „⇒“-Richtung hat 1912 auch Ferdinand Frobenius bewiesen [16], aber in allgemeinerem Rahmen, die „⇐“-Richtung findet sich in einer viel schärferen Fassung schon 1911 in einem Aufsatz von Leonard Dickson [12]. Wir werden diese Ergebnisse in Abschnitt 4.4 als Theorem formulieren und mit völlig elementaren Mitteln beweisen.
Einen Spezialfall der „⇒“-Richtung dieses Beweises haben Ayoub und Chowla 1981 in [1] veröffentlicht. Wir wollen ihn seiner Schönheit wegen hier vorab präsentieren:

Ist $h(-p) = 1$ und wäre $r(x) \notin \mathbb{P}$ für $1 \leqslant x < \frac{p+1}{4}$, dann existierte eine ungerade Primzahl q mit

$$q\,r = x^2 - x + \tfrac{p+1}{4}.$$

Dann wäre $q^2 \leqslant x^2 - x + \frac{p+1}{4} = \frac{1}{4}((2\,x-1)^2 + p)$ und damit

$$4\,q^2 \leqslant (2\,x-1)^2 + p < (\tfrac{p+1}{2} - 1)^2 + p = (\tfrac{p+1}{2})^2.$$

Aus $2\,q < \frac{p+1}{2}$ folgte $q < \frac{p+1}{4}$ und mit dem Lemma von Nagell (3.1) schließlich $\left(\frac{q}{p}\right) = -1$. Dies wäre aber ein Widerspruch, weil sich wegen $q \mid r(x)$ nach dem Reste-Lemma $\left(\frac{q}{p}\right) = 1$ ergäbe, q. e. d.

(4.7) Bemerkung
Aus dem Beweis von Ayoub und Chowla wird deutlich, daß man aus zusammengesetzten Werten des Rabinowitsch-Polynoms kleine quadratische Reste erhält: Ist $p \equiv 3\,(8)$ eine Primzahl mit $p > 3$ und $r(x)$ für $1 \leqslant x < \frac{p+1}{4}$ zusammengesetzt, so existiert ein ungerader Primteiler $q < \frac{p+1}{4}$ von $r(x)$, der nach dem Reste-Lemma (4.3) gleichzeitig ein primer quadratischer Rest modulo p ist. Die zusammengesetzten Werte des Rabinowitsch-Polynoms und die primen quadratischen Reste modulo p stehen also in einem engen Verhältnis.

Aus diesem Grunde stellt der erste Lösungsansatz (3.2) eine Implikation des folgenden Lösungsansatzes dar:

(4.8) Zweiter elementarer Lösungsansatz
Könnte man nachweisen, daß für jede Primzahl $p > 163$ mit $p \equiv 3\,(8)$ in der Menge $R = \{x^2 - x + \frac{p+1}{4} \mid 1 \leqslant x < \frac{p+1}{4}\}$ stets eine zusammengesetzte ganze Zahl enthalten ist, müßte nach dem Satz von Rabinowitsch $h(-p) > 1$ gelten, und man hätte einen weiteren Beweis des Klassenzahl-1-Theorems gefunden.

1922 hat Nagell den Satz von Rabinowitsch in [38] deutlich verschärft. Hierzu ist ein vorbereitender Satz notwendig, der eine starke Aussage über kleinste quadratische Reste macht, weshalb wir ihn erst im letzten Kapitel in Abschnitt 6.3 präsentieren wollen. Wir geben die Verschärfung hier also ohne Beweis an:

(4.9) Satz
Sei $p > 43$ eine Primzahl mit $p \equiv 3\,(8)$.
Dann sind äquivalent:

1. $h(-p) = 1$
2. $r(x) = x^2 - x + \frac{p+1}{4} \in \mathbb{Z}$ *ist für alle x mit* $1 \leqslant x \leqslant \frac{1}{2}\sqrt{\frac{p+16}{3}} - \frac{3}{2}$ *eine Primzahl.*

(4.10) Kollorar
Sei $p > 43$ eine Primzahl mit $p \equiv 3\,(8)$.
Wenn $r(x) = x^2 - x + \frac{p+1}{4} \in \mathbb{Z}$ für alle x mit $1 \leqslant x \leqslant \frac{1}{2}\sqrt{\frac{p+16}{3}} - \frac{3}{2}$ eine Primzahl ist, dann auch für alle x mit $1 \leqslant x < \frac{p+1}{4}$.

4.3 Konstruktion von kleinen quadratischen Resten

Ähnliche Ergebnisse wie der Satz von Rabinowitsch lassen sich mit Hilfe des Lemmas von Nagell (3.1) auch für das Polynom $k(X) = X^2 + p \in \mathbb{Z}[X]$ erzielen:

(4.11) Satz

Sei $p \equiv 19\,(24)$ eine Primzahl.
Dann existieren unendlich viele Zahlenpaare $(y, x) \in \mathbb{N}^2$ mit $p = y - x^2$ und $y \equiv 3\,(4)$, x gerade. Außerdem gilt:

1. *Für alle Primteiler $q \mid y = x^2 + p$ gilt $\left(\frac{q}{p}\right) = 1$.*
2. *Ist überdies $y \notin \mathbb{P}$ und $x < \sqrt{\frac{p+5}{4}}$, so gilt für alle Primteiler $q \mid y = x^2 + p$ stets $q < \frac{p+1}{4}$.*

Beweis:
Ist $p \equiv 3\,(8)$, so gilt für alle $x \in \mathbb{N}$ mit $x \equiv 2, 6\,(8)$ stets $y = x^2 + p \equiv 7\,(8)$ und für alle $x \in \mathbb{N}$ mit $x \equiv 0, 4\,(8)$ stets $y = x^2 + p \equiv 3\,(8)$. In beiden Fällen gilt $p = y - x^2$ mit $y \equiv 3\,(4)$ für alle geraden $x \in \mathbb{N}$.

1. $\left(\frac{q}{p}\right) = 1$ folgt aus dem Reste-Lemma (4.3).
2. Ist $y \notin \mathbb{P}$, so existiert $q \in \mathbb{P}$ mit $q \cdot r = y = x^2 + p$. Wegen $y \equiv 3\,(4)$ und $p \equiv 19\,(24)$ gilt $\left(\frac{3}{p}\right) = -1$, also kann 3 kein Teiler von y sein. Demnach gilt in $q \cdot r = y = x^2 + p$ stets $r \geqslant 5$ und somit $q \leqslant \frac{x^2+p}{5}$. Es folgt $q \leqslant \frac{x^2+p}{5} < \frac{p+1}{4} \iff 4\,x^2 + 4\,p < 5\,p + 5 \iff x < \sqrt{\frac{p+5}{4}}$, q. e. d.

Man beachte, daß $y \notin \mathbb{P}$ die entscheidende Bedingung ist, da immer gerade Zahlen $x < \sqrt{\frac{p+5}{4}}$ existieren. Man erhält durch diesen Satz in Verbindung mit dem Lemma von Nagell (3.1) und Satz (3.4) ein neues Klassenzahl-1-Kriterium:

(4.12) Korollar

Sei $p \equiv 19\,(24)$ eine Primzahl.
Wenn $h(-p) = 1$ ist, dann ist $k(x) = x^2 + p$ für alle geraden x mit $1 < x < \sqrt{\frac{p+5}{4}}$ eine Primzahl.

(4.13) Dritter elementarer Lösungsansatz

Könnte man zeigen, daß für jede Primzahl $p > 163$ mit $p \equiv 19\,(24)$ in der Menge $K = \{x^2 + p \in \mathbb{Z} \mid 1 < x < \sqrt{\frac{p+5}{4}},\ \text{x gerade}\}$ stets eine zusammengesetzte ganze Zahl enthalten ist, müßte nach der Kontraposition des Korollars $h(-p) > 1$ gelten, und man hätten einen weiteren Beweis des Klassenzahl-1-Theorems gefunden.

Der dritte Lösungsansatz erscheint praktikabler als der zweite Lösungsansatz, weil das Polynom k einfacher gebaut ist. Der Nachweis hingegen, daß in einer ausreichend großen, beschränkten Menge von Werten eines quadratischen Polynoms $f \in \mathbb{Z}[X]$ eine zusammengesetzte Zahl enthalten ist, scheint weit außerhalb der Möglichkeiten gegenwärtiger mathematischer Methoden zu liegen. Auch in aktuellen Monographien wie *The Development of Prime Number Theory* von Władysław Narkiewicz [44] und *Sieves in Number Theory* von George Greaves [20] sind keine Ansätze in diese Richtung erkennbar. Unserem Problem am nächsten kommen zwei Arbeiten von Kevin McCurley aus dem Jahre 1986 [35, 36], die eine Abschätzung für den kleinsten primen Wert eines Polynoms vom Typ $X^n + a$ angeben. Allerdings lauten die Sätze immer: „*Es gibt unendlich viele irreduzible Polynome $X^n + a$, so daß...*“ — was in unserem Fall nicht weiterhilft.
Das zahlentheoretische Forschungsinteresse ist offensichtlich entgegengesetzt gelagert: Seit Victor Bouniakowsky 1857 vermutet hat, daß jedes nichtkonstante irreduzible Polynom $f \in \mathbb{Z}[X]$, dessen Koeffizienten keinen gemeinsamen Teiler > 1 haben und dessen Leitkoeffizient positiv ist, unendliche viele Primzahlen darstellt — seit dieser Vermutung beschäftigen sich viele Zahlentheoretiker mit der Frage, ob bestimmte Klassen von ganzzahligen Polynomen unendlich viele prime Werte annehmen oder nicht. Hierher gehört die Landausche Vermutung, daß X^2+1 unendlich viele Primzahlen darstellt, und die viel allgemeinere Hypothese H von Andrzej Schinzel und Wacław Sierpiński, die 1958 in [55] ausgesprochen wurde. Eine andere zahlentheoretische Richtung versucht Polynome mit besonders hoher „Primzahldichte“ oder sehr langen Ketten aufeinanderfolgender primer Werte zu konstruieren, siehe die Darstellungen von Ribenboim in [51] auf S. 386–403 und von Narkiewicz in [44] auf S. 41–43.

4.4 Der Satz von Frobenius

Die bisherigen Ergebnisse finden ihre stärkste Verallgemeinerung in dem folgenden Resultat von Ferdinand Frobenius aus dem Jahre 1912, das in seiner Allgemeinheit meistens nicht richtig gewürdigt wird [16]:

(4.14) Satz von Frobenius
Sei $p \equiv 3\,(8)$ eine Primzahl und sei $f(X,Y) = X^2 + XY + \frac{p+1}{4}Y^2$ die Hauptform der Diskriminante $D = -p$.
Wenn $h(-p) = 1$ ist, dann ist $f(x,y)$ für alle teilerfremden ganzen Zahlen x, y mit $f(x,y) < (\frac{p+1}{4})^2$ eine Primzahl.

Beweis:
Gilt $h(-p) = 1$, dann ist f die einzige reduzierte Form der Diskriminante D, wobei 1 und $\frac{p+1}{4}$ die kleinsten Zahlen sind, die f (und damit alle Formen der Diskriminante D) eigentlich darstellt.
Ist $q = f(x,y) < (\frac{p+1}{4})^2$ mit $(x,y) = 1$ und wäre $q = r \cdot s$ keine Primzahl, so würde $1 < r \leqslant \sqrt{q} < \frac{p+1}{4}$ gelten, und r müßte als Teiler einer darstellbaren Zahl nach (1.1) ebenfalls eine eigentliche Darstellung besitzen. Dies wäre ein Widerspruch, q. e. d.

(4.15) Definition
Sei $p \equiv 3\,(8)$ eine Primzahl und sei $f(X,Y) = X^2 + XY + \frac{p+1}{4}Y^2$ die Hauptform der Diskriminante $D = -p$.
Setze dann die *Frobenius-Menge*

$$F = \{f(x,y) \mid (x,y) = 1,\ f(x,y) < (\tfrac{p+1}{4})^2\}$$

sowie die *Frobenius-Faser*

$$F_{y'} = \{f(x,y') \mid (x,y') = 1,\ f(x,y') < (\tfrac{p+1}{4})^2\}$$

für eine feste ganze Zahl y'.

Damit lassen sich die bisherigen Ergebnisse wie angekündigt im folgenden Theorem zusammenfassen und verschärfen:

(4.16) Theorem
Sei $p \equiv 3\,(8)$ eine Primzahl.
Dann sind äquivalent:

(i) $h(-p) = 1$

(ii) $F = \{f(x,y) \mid (x,y) = 1,\ f(x,y) < (\frac{p+1}{4})^2\} \subseteq \mathbb{P}$

(iii) $R = \{x^2 - x + \frac{p+1}{4} \mid 1 \leqslant x < \frac{p+1}{4}\} \subseteq \mathbb{P}$

(iv) $D = \{x^2 - x + \frac{p+1}{4} \mid 1 \leqslant x \leqslant \sqrt{\frac{p}{12}} + \frac{1}{2}\} \subseteq \mathbb{P}$

Beweis:
(i) $\Longrightarrow$ (ii) ist der Satz von Frobenius.
(ii) $\Longrightarrow$ (iii) folgt aus $R = F_{-1} \subseteq F$.
(iii) $\Longrightarrow$ (iv) folgt aus $D \subseteq R$.
(iv) $\Longrightarrow$ (i) folgt aus der Theorie der reduzierten Formen: Ist $r(x) = x^2 - x + \frac{p+1}{4}$ für alle x mit $1 \leqslant x \leqslant \sqrt{\frac{p}{12}} + \frac{1}{2}$ eine Primzahl und wäre $h(-p) > 1$, so gäbe es nach dem Satz von der reduzierten Form (1.3) neben der Hauptform $(1,1,\frac{p+1}{4})$ noch eine weitere reduzierte Form (a,b,c) der Diskriminante $D = -p$ mit $|b| \leqslant a \leqslant c$, wobei $|b| \leqslant a \leqslant \sqrt{\frac{p}{3}}$

gelten würde. Wegen $-p = b^2 - 4ac$ und damit $4ac = b^2 + p$ müßte b ungerade sein, also $b = 2x - 1$. Es folgte also

$$ac = \tfrac{1}{4}((2x-1)^2 + p) = x^2 - x + \tfrac{p+1}{4} = r(x).$$

Für $b = x = 1$ erhält man mit $a = 1$ und $c = \frac{p+1}{4}$ stets die Hauptform $(1, 1, \frac{p+1}{4})$. Eine weitere reduzierte Form kann es für $b = x = 1$ nicht geben, da $\frac{p+1}{4} = r(1)$ nach Voraussetzung eine Primzahl ist. Also müßte $r(x) = ac$ für $3 \leqslant b = 2x - 1$ eine zusammengesetzte Zahl sein. Dies wäre aber ein Widerspruch zur Voraussetzung, da $3 \leqslant 2x - 1 \leqslant a \leqslant \sqrt{\frac{p}{3}}$ gerade $1 \leqslant x \leqslant \sqrt{\frac{p}{12}} + \frac{1}{2}$ bedeutet, q. e. d.

(4.17) Bemerkung

Der Beweis des Hauptsatzes ist völlig elementar, weil sowohl der Beweis des Satzes von Frobenius als auch der Beweis (iv) $\Longrightarrow$ (i) mit elementaren Mitteln auskommt. Damit gibt es auch einen elementaren Beweis des Satzes von Rabinowitsch (4.6).
Der Beweis (iv) $\Longrightarrow$ (i) stammt übrigens von Leonard Dickson, der schon im Jahre 1911 in [12] nachgewiesen hat, daß für alle Primzahlen p mit $163 < p < 1.500.000$ stets $h(-p) > 1$ gilt, das heißt, daß es für $D > -1.500.000$ nur die neun bekannten negativen Diskriminanten mit Klassenzahl 1 gibt. Dies gelang ihm mit Hilfe reduzierter Formen, durch welche er zur Bedingungung $p \equiv 43, 67\,(120)$ gelangte — ein Resultat, das wir in (3.7) auf anderem Wege erhalten haben.

(4.18) Korollar

Sei $p \equiv 3\,(8)$ eine Primzahl. Dann gilt:

1. $h(-p) = 1 \iff \left(\frac{q}{p}\right) = 1$ *für alle* $q \in F$.
2. $h(-p) = 1 \iff$ *F besteht genau aus den in R_K zerfallenden Primzahlen q mit* $\frac{p+1}{4} < q < (\frac{p+1}{4})^2$.

Beweis:
1. folgt mit $\left(\frac{D}{q}\right) = \left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)$ aus dem Darstellungssatz (1.4) für quadratische Formen.
2. folgt aus der Zerlegungstheorie von Primidealen.

(4.19) Bemerkung

Ist $h(-p) = 1$, dann besitzt jede in R_K zerfallende Primzahl eine eigentliche Darstellung durch die zugehörige Hauptform.
Ist $h(-p) > 1$, dann besitzt jede in R_K zerfallende Primzahl nach wie vor eine eigentliche Darstellung durch eine quadratische Form der Diskriminante $D = -p$, aber eben nicht notwendigerweise durch die Hauptform.

4.5 Verallgemeinerungen des Satzes von Rabinowitsch

Der Satz von Rabinowitsch ist im Laufe des 20. Jahrhunderts auf vielfältige Weise behandelt worden, bis in die jüngste Zeit hinein übt dieser Satz eine große Faszination aus, die sich in Veröffentlichungen niederschlägt.
1974 hat George Szekeres in [60] ein elementares Kriterium dafür angegeben, daß ein Wert des Rabinowitsch-Polynoms eine Primzahl ist oder nicht, indem er eine Verbindung zu einer diophantischen Gleichung zweiten Grades herstellt.
Herbert Möller hat 1976 in seiner Habilitation gezeigt [37], daß die Werte der Hauptform $f(X,Y) = X^2+XY+\frac{p+1}{4}Y^2$ in einem bestimmten Bereich nicht mehr Primfaktoren besitzen, als die sogenannte Davenport-Zahl der Klassengruppe angibt. Er hat damit über eine geometrische Interpretation dieser Werte eine untere Schranke für die Klassenzahl gegeben.
Eine ähnliche Idee hat Ryuji Sasaki 1986 in [53] vorgestellt, wo er nachweist, daß $\max\{\,\omega(x^2 - x + \frac{p+1}{4}) \mid 1 \leqslant x < \frac{p+1}{4}\}$ eine gute untere Schranke für die zugehörige Klassenzahl liefert, wobei die Primteiler-Funktion $\omega(n)$ die Anzahl der Primfaktoren von n angibt. Das bedeutet, daß die Klassenzahl um so größer ist, je mehr Primteiler ein Wert des Rabinowitsch-Polynoms besitzt.
Ein weitere Verallgemeinerung gelang 1974 Michael Hendy, der in [24] eine Verbindung zum sogenannten Klassenzahl-2-Problem herstellen konnte. Er gibt hierzu drei Typen von Polynomen an, die in einem bestimmten Bereich genau dann ausschließlich prime Werte annehmen, wenn der zugehörige imaginär-quadratische Zahlkörper die Klassenzahl 2 besitzt.
Auch zur Struktur der Klassengruppe lassen sich Verbindungen herstellen. Stéphane Louboutin beispielseise hat 1991 in [33] ein einfaches Kriterium dafür angegeben, daß die Klassengruppe eines imaginär-quadratischen Zahlkörpers den Exponenten 2 besitzt, woraus er die Polynom-Typen für die Klassenzahlen 2 und 4 ableiten konnte.
Starke Bemühungen gibt es um die Verbindung zu reellen Zahlkörpern, wo die Gaußsche Vermutung, daß es unendlich viele Zahlkörper mit $h(K) = 1$ gebe, bis heute unbewiesen ist. 1980 überträgt beispielsweise Masakazu Kutsuna in [26] die Ideen Rabinowitschs ziemlich originalgetreu auf reelle quadratische Zahlkörper.
Dongho Byeon und Harold Stark haben 2001 in [5] gezeigt, daß im reellen Fall nur endlich viele Polynome $f_m(x) = x^2+x-m$ die Rabinowitsch-Eigenschaft haben können.
Gute Überblicksartikel über den gesamten Bereich stammen von Franz Halter-Koch [21], von Louboutin, Mollin und Williams [34] und von Granville und Mollin [19].

5. Kleinste prime quadratische Nichtreste

Wir sind in dieser Arbeit nur indirekt an kleinsten quadratischen Nichtresten interessiert. Da es aus noch darzustellenden Gründen leichter ist, elementare Abschätzungen für den kleinsten quadratischen Nichtrest zu finden als für den kleinsten quadratischen Rest, gibt es hier eine Vielzahl von Beweisansätzen, deren Studium sich als lohnend erweisen kann, wenn man eine Übertragung auf quadratische Reste erreichen will. Die folgende Bezeichnung hat sich eingebürgert und ist häufig anzutreffen:

(5.1) Definition
Sei p eine Primzahl. Unter

$$\psi_p := \psi_2(p) := \min\left\{q \in \mathbb{P} \mid q \geqslant 3, \left(\tfrac{q}{p}\right) = -1\right\}$$

versteht man den *kleinsten ungeraden primen (quadratischen) Nichtrest modulo p*.

Wir geben die bekannten Abschätzungen für ψ_p in meist chronologischer Abfolge wieder, die Beweise werden angegeben, um die Übertragbarkeit auf Reste zu diskutieren.

5.1 Der Satz von Gauß

Wie in vielem ist Carl Friedrich Gauß auch hier vorausgegangen. In den *Disquisitiones arithmeticae* beweist er in Art. 129 im Zusammenhang mit dem ersten Beweis des Quadratischen Reziprozitätsgesetzes folgenden berühmten Satz, den er schon als 19jähriger gefunden hatte:

(5.2) Satz von Gauß
Ist $p \equiv 1\,(8)$ eine Primzahl, so existiert eine ungerade Primzahl $q < 2\sqrt{p} + 1$ mit

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

Das heißt, für jede Primzahl $p \equiv 1\,(8)$ gilt $\psi_p < 2\sqrt{p} + 1$.

Beweis:
Sei $p \equiv 1\,(8)$ eine Primzahl und $m \in \mathbb{Z}$ mit $1 < 2m+1 < p$ so gewählt, daß für alle ungeraden Primzahlen $q \leqslant 2m+1$ stets $\left(\frac{p}{q}\right) = 1$ gilt.
Nach dem Satz, daß für $p \equiv 1\,(\mathrm{mod}\,8)$ und $N = \prod q_i^{e_i}$ mit $(p, N) = 1$ die Kongruenz $x^2 \equiv p\,(\mathrm{mod}\,N)$ gleichbedeutend ist mit $x^2 \equiv p\,(\mathrm{mod}\,q_i)$ für jeden ungeraden Primteiler q_i von N, existiert eine ganze Zahl $x > m$ mit $x^2 \equiv p\,(\mathrm{mod}\,(2m+1)!)$. Hieraus erhält man mit einer einfachen, aber genialen Rechnung

$$\begin{aligned}(p-1^2)(p-2^2)\cdots(p-m^2) &\equiv (x^2-1^2)(x^2-2^2)\cdots(x^2-m^2)\\ &= \frac{(2m+1)!\binom{x+m}{2m+1}}{x}(\mathrm{mod}\,(2m+1)!)\end{aligned}$$

Wegen $(x, (2m+1)!) = 1$ muß x den Binomialkoeffizienten $\binom{x+m}{2m+1} \in \mathbb{Z}$ teilen, weshalb $\binom{x+m}{2m+1}/x$ eine ganze Zahl ist. Daher gilt

$$(p-1^2)(p-2^2)\cdots(p-m^2) \equiv 0\,(\mathrm{mod}\,(2m+1)!),$$

woraus sich durch geschicktes Aufteilen von $(2m+1)!$ und Ausmultiplizieren

$$\frac{(p-1^2)(p-2^2)\cdots(p-m^2)}{(2m+1)!} = \frac{1}{m+1}\cdot\frac{p-1^2}{(m+1)^2-1^2}\cdots\frac{p-m^2}{(m+1)^2-m^2} \in \mathbb{Z}$$

ergibt. Wenn man nun m so wählt, daß $m^2 < p < (m+1)^2$ gilt, müssen alle Brüche auf der rechten Seite der Gleichung im Intervall $]\,0;1\,[$ liegen, und man erhält einen Widerspruch zur Ganzzahligkeit.
Wählt man $m = \lfloor \sqrt{p} \rfloor$, gilt einerseits wie verlangt $2\lfloor \sqrt{p} \rfloor + 1 < p$, andererseits aber $m^2 < p < (m+1)^2$, was zu obigem Widerspruch führt. Folglich existiert eine ungerade Primzahl q mit

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

und $q \leqslant 2\lfloor \sqrt{p} \rfloor + 1 < 2\sqrt{p} + 1$, q. e. d.

Der Gaußsche Originalbeweis ist auch für einen heutigen Leser verhältnismäßig gut verständlich, alle späteren Wiedergaben orientieren sich deutlich an ihm, siehe beispielsweise § 50 auf S. 116f. in Dirichlets *Vorlesungen über Zahlentheorie* [13] oder S. 51f. in [47] von Herbert Piper.
Der hier wiedergegebene Beweis folgt der Darstellung von Daniel Flath in dessen sehr lesenswerter *Introduction to Number Theory*, siehe S. 77 in [15]. Darin nennt Flath den Gaußschen Beweis „the most amazing proof of this book“.
Überprüft man, ob dieser Beweis auch auf quadratische Reste übertragen werden kann, wird schnell klar, daß dies unmöglich ist. Die Übertragung scheitert daran, daß der eingangs angewandte Satz nur für quadratische Reste gilt und nicht — wie es nötig wäre — auf quadratische Nichtreste übertragen werden kann.

5.2 Die Verschärfungen von Nagell

1923 hat Trygve Nagell in [39] die Gültigkeit des Satzes von Gauß für beliebige Primzahlen nachgewiesen. Da die Arbeit schwer zugänglich ist und wichtige Hilfsmittel enthält, geben wir den Beweis ausführlich wieder, teilweise mit leicht verbesserten Schranken:

(5.3) Satz von Gauß-Nagell
Ist $p > 3$ eine Primzahl, so existiert eine ungerade Primzahl $q < 2\sqrt{p}+1$ mit $\left(\frac{q}{p}\right) = -1$. Das heißt, für jede Primzahl $p > 3$ gilt $\psi_p < 2\sqrt{p} + 1$.

Beweis:
Nach dem Satz von Gauß (5.2) gilt die Aussage für jede Primzahl $p \equiv 1\,(8)$. Wir unterscheiden die drei restlichen Fälle:
1. Fall: Ist $p \equiv 5\,(8)$ eine Primzahl, so existieren nach einem Satz von Fermat-Euler natürliche Zahlen a, b mit $p = a^2 + b^2$. Folglich gilt $a^2 - b^2 \equiv -2b^2\,(p)$ und daher

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

Ist nun ein Produkt ein quadratischer Nichtrest, muß wenigstens einer der Faktoren ein quadratischer Nichtrest sein. Da $a^2 - b^2$ ungerade ist, gibt es also einen (ungeraden) Primteiler q von $|a^2 - b^2| \geqslant 3$ mit

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

Wegen $a^2 - b^2 = (a+b)(a-b)$ gilt $q \leqslant a + b$. Da außerdem $a + b < \sqrt{2(a^2 + b^2)} = \sqrt{2p}$ äquivalent zu $0 < (a - b)^2$ ist, was in unserem Fall wegen $a \neq b$ immer erfüllt ist, gilt stets

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

2. Fall: Ist $p \equiv 7\,(8)$ eine Primzahl, so existiert eine ganze Zahl a mit $a^2 < p < (a+1)^2$. Ist a gerade, gilt $p - a^2 \equiv 3\,(4)$, die positive ganze Zahl $p - a^2$ hat demnach einen Primteiler $q \equiv 3\,(4)$, für den wegen $p = a^2 + qr$ stets

$$\left(\tfrac{q}{p}\right) = -\left(\tfrac{p}{q}\right) = -\left(\tfrac{a^2+qr}{q}\right) = -\left(\tfrac{a^2}{q}\right) = -1$$

gilt. Aus $\sqrt{p} < a + 1$ folgt $(\sqrt{p} - 1)^2 < a^2$ und hieraus

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

Ist a ungerade, gilt $\frac{1}{2}(p-a^2) \equiv 3\,(4)$, die positive ganze Zahl $\frac{1}{2}(p-a^2)$ hat demnach einen Primteiler $q \equiv 3\,(4)$, für den wegen $p = a^2 + qr'$ wie oben

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

gilt. Aus $(\sqrt{p}-1)^2 < a^2$ folgt hier

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

3. Fall: Ist $p \equiv 3\,(8)$ eine Primzahl, so existiert eine ganze Zahl a mit $a^2 < p < (a+1)^2$. Ist a gerade, gilt $\frac{1}{2}((a+1)^2-p) \equiv 3\,(4)$, die positive ganze Zahl $\frac{1}{2}((a+1)^2-p)$ hat demnach einen Primteiler $q \equiv 3\,(4)$, für den wegen $p = (a+1)^2 - qr'$ stets

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

gilt. Aus $a^2 < p$ folgt wegen $a^2 \equiv 0, 4\,(8)$ und $p \equiv 3\,(8)$ stets $a^2+3 \leqslant p$, also $a \leqslant \sqrt{p-3}$, und hieraus

$$q \leqslant \tfrac{1}{2}((a+1)^2-p) \leqslant \tfrac{1}{2}((\sqrt{p-3}+1)^2-p) = \sqrt{p-3}-1 < \sqrt{p}.$$

Ist a ungerade, gilt $\frac{1}{2}((a+2)^2-p) \equiv 3\,(4)$, die positive ganze Zahl $\frac{1}{2}((a+2)^2-p)$ hat demnach einen Primteiler $q \equiv 3\,(4)$, für den wegen $p = (a+2)^2 - qr'$ stets

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

gilt, wobei man $q < p$ aus $\frac{1}{2}((a+2)^2-p) < p$ erhält, was wegen $(a+2)^2 < 3a^2 < 3p$ für $a \geqslant 3$ und damit für $p > 3$ erfüllt ist. Aus $a^2 < p$ folgt $a^2+2 \leqslant p$ und daher $a \leqslant \sqrt{p-2}$. Hieraus ergibt sich

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

Damit gilt die Aussage in allen Fällen, q. e. d.

Wir bemerken, daß man im Fall $p \equiv 3\,(8)$, der sich später als schwierig erweisen wird, zumindest teilweise $\sqrt{p}$ als obere Schranke erhält:

(5.4) Korollar

Sei $p \equiv 3\,(8)$ eine Primzahl mit $p > 3$.
Ist die größte Quadratzahl $a^2 < p$ gerade, dann gilt stets $\psi_p < \sqrt{p}$.

(5.5) Bemerkung

In diesem Beweis ist eine Vielzahl von Ideen enthalten, deren genaue Analyse lohnend erscheint. Man stellt folgendes fest:
Die zentrale Idee im Beweis des ersten Falles ist die (bis auf Reihenfolge und Vorzeichen) eindeutige Darstellung von p als Summe zweier Quadrate a^2 und b^2, aus welchen dann

ein quadratischer Nichtrest modulo p konstruiert wird. Dieses Verfahren läßt sich prinzipiell auf die Konstruktion quadratischer Reste übertragen, wir werden es im nächsten Kapitel häufig anwenden.
Allerdings ist die Tatsache, daß ein Produkt, das Nichtrest ist, stets einen Primfaktor enthält, der ebenfalls Nichtrest ist, überhaupt nicht auf quadratische Reste übertragbar. Ein Produkt, das ein Rest ist, kann aus lauter primen Nichtresten zusammengesetzt sein. So ist beispielsweise $\left(\frac{21}{41}\right) = 1$, aber $\left(\frac{3}{41}\right) = -1$ und $\left(\frac{7}{41}\right) = -1$. Dieser Umstand erschwert den Nachweis kleiner primer Reste enorm.
Im Beweis des zweiten und dritten Falles ist die Idee von zentraler Bedeutung, p zwischen zwei benachbarte Quadratzahlen einzuschließen und einen Nichtrest als Primteiler der Differenz von Quadratzahl und p zu konstruieren. Auch dieses Vorgehen läßt sich prinzipiell auf die Konstruktion quadratischer Reste übertragen.
Allerdings gibt es auch hier ein systematisches Problem: Die Differenz wird in den Fällen $p \equiv 3\,(4)$ stets so gewählt, daß sie $\equiv 3\,(4)$ ist. Hieraus folgt nämlich, daß es einen Primteiler $q \equiv 3\,(4)$ geben muß. Dadurch erhält man bei Anwendung des Quadratischen Reziprozitätsgesetzes das gewünschte negative Vorzeichen, das letztlich auf das Ergebnis -1 führt. Bei der Konstruktion quadratischer Reste stört dieses negative Vorzeichen. Um im Quadratischen Reziprozitätsgesetz ein positives Vorzeichen zu bekommen, braucht man einen Primteiler $q \equiv 1\,(4)$. Die Existenz eines Teilers mit dieser Kongruenzeigenschaft nachzuweisen, ist aber allgemein nicht möglich. Folglich muß man $q \equiv 1\,(4)$ voraussetzen, wie dies beim Satz von Chowla-Friedlander in Abschnitt 6.4 geschieht. Dadurch geht allerdings die Allgemeingültigkeit der Aussage verloren.

(5.6) Beispiele

Im Gegensatz zum Satz von Gauß, der durch einen klassischen Widerspruchsbeweis gezeigt wird, ist der Beweis in den obigen drei Fällen vollständig konstruktiv, das heißt, daß man kleine quadratische Nichtreste „mit Bleistift und Papier“ auch konkret „ausrechnen“ kann. Einige Beispiele sollen dies verdeutlichen:

Primzahl p			q	ψ_p	$2\sqrt{p}+1$
$109 \equiv 5\,(8)$	$p = 3^2 + 10^2$	$a^2 - b^2 = -7 \cdot 13$	$q = 13$	$\psi_{109} = 11$	$21,9$
$1021 \equiv 5\,(8)$	$p = 11^2 + 30^2$	$a^2 - b^2 = -19 \cdot 41$	$q = 19$	$\psi_{1021} = 7$	$64,9$
$10069 \equiv 5\,(8)$	$p = 87^2 + 50^2$	$a^2 - b^2 = 37 \cdot 137$	$q = 37$	$\psi_{10069} = 7$	$201,7$
$103 \equiv 7\,(8)$	$10^2 < p < 11^2$	$p - a^2 = 3$	$q = 3$	$\psi_{103} = 3$	$21,3$
$1031 \equiv 7\,(8)$	$32^2 < p < 33^2$	$p - a^2 = 7$	$q = 7$	$\psi_{1031} = 7$	$65,2$
$10079 \equiv 7\,(8)$	$100^2 < p < 101^2$	$p - a^2 = 79$	$q = 79$	$\psi_{10079} = 11$	$201,8$
$107 \equiv 3\,(8)$	$10^2 < p < 11^2$	$\frac{1}{2}((a+1)^2 - p) = 7$	$q = 7$	$\psi_{107} = 5$	$21,7$
$1019 \equiv 3\,(8)$	$31^2 < p < 32^2$	$\frac{1}{2}((a+2)^2 - p) = 5 \cdot 7$	$q = 7$	$\psi_{1019} = 7$	$64,8$
$10067 \equiv 3\,(8)$	$100^2 < p < 101^2$	$\frac{1}{2}((a+1)^2 - p) = 67$	$q = 67$	$\psi_{10067} = 5$	$201,7$

Man sieht, daß dieses Verfahren leicht durchzuführen ist, aber nicht unbedingt zu sehr kleinen quadratischen Nichtresten führt.

Möglicherweise hat sich Trygve Nagell in den Kriegsjahren mit dem Thema der kleinsten quadratischen Nichtreste intensiv beschäftigt. Zu Beginn der fünfziger Jahre jedenfalls veröffentlichte er in der neuen skandinavischen Fachzeitschrift *Arkiv för Matematik* kurz hintereinander drei Arbeiten, die bessere Abschätzungen für ψ_p bieten oder Beweisvarianten darstellen. 1950 hat er die Abschätzungen in [40] für jede Restklasse modulo 8 verschärft, nur im Fall $p \equiv 3\,(8)$ konnte das Resultat von 1923 nicht verbessert werden:

(5.7) Nagellsche Abschätzungen I

1. *Ist* $p \equiv 1\,(8)$ *eine Primzahl, so gilt* $\psi_p < \sqrt{p}$.
2. *Ist* $p \equiv 3\,(8)$ *eine Primzahl mit* $p \geqslant 11$, *so gilt* $\psi_p < 2\sqrt{p} + 1$.
3. *Ist* $p \equiv 5\,(8)$ *eine Primzahl, so gilt* $\psi_p < \sqrt{2p}$.
4. *Ist* $p \equiv 7\,(8)$ *eine Primzahl mit* $p \geqslant 23$, *so gilt* $\psi_p < \sqrt{2p} - 1$.

Wir möchten auf die Beweise nicht näher eingehen, weil sie wenig Neues bieten, wenn man davon absieht, daß Nagell im Falle $p \equiv 1\,(8)$ einen Satz von Axel Thue anwendet, den er in [42] ausführlich darstellt.

Um weiter fortschreiten zu können, benötigen wir folgendes Lemma, das in vielen Aufsätzen beinahe selbstverständlich benützt, aber nirgendwo streng bewiesen wird:

(5.8) Lemma

Für jede Primzahl $p > 3$ *gilt* $\psi_p < p$.

Beweis:

Angenommen, es gäbe eine Primzahl p mit $\psi = \psi_p \geqslant p > 3$. Dividierte man ψ durch p mit Rest, gäbe es eindeutig bestimmte Zahlen k, $r \in \mathbb{N}$ mit

$$\psi = kp + r$$

und $0 < r < p < \psi$. Daher müßte $\left(\frac{r}{p}\right) = \left(\frac{\psi - kp}{p}\right) = \left(\frac{\psi}{p}\right) = -1$ gelten. Wegen $r < \psi$ könnte r keine ungerade Primzahl sein. Demnach wäre

$$r = 2^n u$$

mit ungeraden Zahlen n, $u \in \mathbb{N}$, wobei $\left(\frac{2}{p}\right) = -1$ gelten müßte und u nur Primteiler besitzen könnte, die quadratische Reste modulo p sind. Wir betrachten nun die Zahlen $\psi - 2 = kp + (r-2)$ und $(r-2) = 2(2^{n-1}u - 1)$.

Wäre $n > 1$, müßte $2^{n-1}u - 1 < \psi$ ungerade und damit ein quadratischer Rest modulo p sein. Da 2 ein Nichtrest wäre, müßte auch $r-2$ ein Nichtrest sein. Andererseits würde $\left(\frac{r-2}{p}\right) = \left(\frac{\psi - 2 - kp}{p}\right) = \left(\frac{\psi - 2}{p}\right) = 1$ gelten, Widerspruch!

Damit wäre $n = 1$ und $r = 2u$, so daß $u - 2 < \psi$ und $\psi - 4 = kp + 2(u-2) < \psi$ ungerade und daher quadratische Reste sein müßten. Da 2 Nichtrest wäre, hätte man andererseits mit $\left(\frac{\psi - 4}{p}\right) = \left(\frac{2(u-2)}{p}\right) = -1$ einen Widerspruch, q. e. d.

Im Jahre 1951 konnte Nagell in [41] obige Abschätzungen nochmals verbessern. Seine Arbeit enthält völlig neue, wahrhaft brilliante Ideen:

(5.9) Nagellsche Abschätzungen II

1. Ist $p \equiv 1\,(8)$ eine Primzahl, so gilt $\psi_p \leqslant \sqrt{\frac{1}{2}(p+1)}$.

2. Ist $p \equiv 7\,(8)$ eine Primzahl mit $p \neq 7,\ 23$, so gilt $\psi_p < \sqrt{p-6}$.

Beweis:

1. Sei $p \equiv 1\,(8)$ eine Primzahl und $\psi = \psi_p$ der kleinste ungerade Nichtrest modulo p. Es gilt stets $\left(\frac{-1}{p}\right) = 1$ und $\left(\frac{2}{p}\right) = 1$. Dividiert man p durch 2ψ mit Rest, erhält man

$$p = 2\psi k \pm r,$$

wobei $0 < r \leqslant \psi - 2$ gilt, weil $\psi - 1$ gerade ist. (Nach Lemma (5.8) gilt $\psi < p$ und damit $k \geqslant 1$.) Wegen $r < \psi$ muß r ein quadratischer Rest modulo p sein. Hieraus ergibt sich mit $\pm r = p - 2\psi k$ und

$$1 = \left(\tfrac{\pm r}{p}\right) = \left(\tfrac{p-2\psi k}{p}\right) = \left(\tfrac{-2\psi k}{p}\right) = \left(\tfrac{-2}{p}\right)\left(\tfrac{\psi}{p}\right)\left(\tfrac{k}{p}\right) = -\left(\tfrac{k}{p}\right),$$

daß k ein quadratischer Nichtrest modulo p ist, weshalb $k \geqslant \psi$ gilt. Insgesamt erhält man die Ungleichung

$$p = 2\psi k \pm r \geqslant 2\psi^2 \pm r \geqslant 2\psi^2 - \psi + 2.$$

Von $p \geqslant 2\psi^2 - \psi + 2$ aus gelangt man mit Hilfe einer quadratischen Ergänzung zu $\frac{1}{2}p \geqslant (\psi - \frac{1}{4})^2 + \frac{15}{16}$ und nach Radizieren zu

$$\psi \leqslant \sqrt{\tfrac{1}{2}p - \tfrac{15}{16}} + \tfrac{1}{4}.$$

Diese obere Schranke ist für alle Primzahlen $p \equiv 1\,(8)$ deutlich schärfer als $\sqrt{p}$. Um sie noch geringfügig zu verbessern, wählt man eine ganze Zahl $a \geqslant 0$ so, daß die Ungleichung $p \geqslant 2\psi^2 - \psi + 2$ zu einer Gleichung wird:

$$p = 2\psi^2 - \psi + 2 + 2a. \tag{1}$$

Hieraus erhält man

$$p - (2a+3)\psi = 2(\psi - 1)(\psi - 1 - a). \tag{2}$$

Wäre nun $a \leqslant \frac{1}{2}(\psi - 5)$, würde $2a + 3 \leqslant \psi - 2$ gelten. Dann müßte $(2a+3)\psi$ ein quadratischer Nichtrest modulo p sein. Da aber die rechte Seite von (2) offensichtlich ein quadratischer Rest modulo p ist, erhielte man einen Widerspruch.
Folglich muß $a \geqslant \frac{1}{2}(\psi - 3)$ gelten. Aus (1) folgt somit $p = 2\psi^2 - \psi + 2 + 2a \geqslant 2\psi^2 - \psi + 2 + \psi - 3 = 2\psi^2 - 1$ und hieraus schließlich

$$\psi \leqslant \sqrt{\tfrac{1}{2}(p+1)}.$$

2. Sei $p \equiv 7\,(8)$ eine Primzahl und $\psi = \psi_p$ der kleinste ungerade Nichtrest modulo p. Es gilt stets $\left(\frac{-1}{p}\right) = -1$ und $\left(\frac{2}{p}\right) = 1$. Dividiert man p durch ψ mit Rest, erhält man

$$p = \psi k - r,$$

wobei $0 < r \leqslant \psi - 1$ gilt. (Nach Lemma (5.8) gilt $\psi < p$ und damit $k \geqslant 1$.) Wegen $r < \psi$ muß r ein quadratischer Rest modulo p sein. Hieraus ergibt sich mit $r = \psi k - p$ und

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

daß k ein quadratischer Nichtrest modulo p ist, weshalb $k \geqslant \psi$ gilt. Insgesamt erhält man die Ungleichung

$$p = \psi k - r \geqslant \psi^2 - r \geqslant \psi^2 - \psi + 1.$$

Von $p \geqslant \psi^2 - \psi + 1$ aus gelangt man mit Hilfe einer quadratischen Ergänzung zu $p \geqslant (\psi - \frac{1}{2})^2 + \frac{3}{4}$ und nach Radizieren zu

$$\psi \leqslant \sqrt{p - \tfrac{3}{4}} + \tfrac{1}{2}.$$

Diese obere Schranke ist schlechter als $\sqrt{p}$. Um sie zu verbessern, wählt man eine ganze Zahl $a \geqslant 0$ so, daß die Ungleichung $p \geqslant \psi^2 - \psi + 1$ zu einer Gleichung wird:

$$p = \psi^2 - \psi + 1 + a.$$

Hieraus erhält man

$$p - (a + 3) = (\psi + 1)(\psi - 2). \tag{3}$$

Wegen $\psi - 2 < \psi$ und $\frac{1}{2}(\psi + 1) < \psi$ sind $\psi - 2$, $\frac{1}{2}(\psi + 1)$ und folglich auch $\psi + 1$ quadratische Reste modulo p. Auf der rechten Seite von (3) steht damit ein quadratischer Rest, woraus folgt, daß $a+3$ ein quadratischer Nichtrest modulo p sein muß. Daher gilt $a + 3 \geqslant \psi$ und damit

$$p = \psi^2 - \psi + 1 + a \geqslant \psi^2 - \psi + 1 + \psi - 3 = \psi^2 - 2.$$

Man wählt nun eine ganze Zahl $b \geqslant 0$, welche die Gleichung

$$p = \psi^2 - 2 + b$$

erfüllt. Ist $b = 0$, erhält man

$$p - 7 = (\psi + 3)(\psi - 3). \tag{4}$$

Diese Gleichung ist wegen $\psi_7 = 3$ für $p = 7$ erfüllt. Ist $p > 7$, muß $\psi > 3$ und damit $\frac{1}{2}(\psi+3) < \psi$ gelten. Folglich ist $\frac{1}{2}(\psi+3)$ und damit $\psi+3$ wie auch $\psi-3$ quadratischer Rest modulo p. Daher stellt die rechte Seite von (4) einen quadratischen Rest dar,

weshalb 7 ein quadratischer Nichtrest modulo p sein muß. Hieraus folgt $\psi \leqslant 7$ und damit $p = \psi^2 - 2 \leqslant 47$. Für $p = 23$ ist (4) erfüllt, da $\psi_{23} = 5$ gilt. Für $p = 47$ und $p = 31$ ist (4) wegen $\psi_{47} = 5$ und $\psi_{31} = 3$ hingegen nicht erfüllt, es gilt also $b > 0$. (Damit sind $p = 7$, 23 die einzigen Primzahlen $\equiv 7\,(8)$, für die $b = 0$ und damit die etwas schwächere Abschätzung $\psi_p \leqslant \sqrt{p+2}$ gilt.)
Ist nun $b > 0$, muß b gerade sein, und für $p \neq 7$, 23 gilt

$$p - (b-1) = \psi^2 - 1 = (\psi + 1)(\psi - 1).$$

Da $\psi + 1$ und $\psi - 1$ quadratische Reste modulo p sind, muß $b - 1$ ein quadratischer Nichtrest modulo p sein, woraus $b - 1 \geqslant \psi$ folgt. Hieraus erhält man

$$p = \psi^2 - 2 + b \geqslant \psi^2 - 2 + \psi + 1 = \psi^2 + \psi - 1.$$

Von $p \geqslant \psi^2 + \psi - 1$ aus gelangt man mit Hilfe einer quadratischen Ergänzung zu $p \geqslant (\psi + \frac{1}{2})^2 - \frac{5}{4}$ und nach Radizieren zu

$$\psi \leqslant \sqrt{p + \tfrac{5}{4}} - \tfrac{1}{2} < \sqrt{p-6},$$

wobei letztere Ungleichung für $p > 18,25$ aus einer einfachen Rechnung folgt, q. e. d.

(5.10) Bemerkung

Zunächst bemerken wir, daß Nagell im Fall $p \equiv 1\,(8)$ mit einem sehr einfachen Beweis eine relativ kleine Schranke erhält. Der Beweis ist zwar nicht konstruktiv, die Mittel sind aber völlig elementar und stehen in keinem Verhältnis zu dem Aufwand, den der Beweis von Tsit-Yuen Lam in [27] auf S. 179f. erfordert, der sich im wesentlichen auf p-adische Zahlen stützt. Bei Lam ist die Stoßrichtung aber eine andere — er möchte aus seiner Argumentation die Hilbert-Reziprozität ableiten.
Daß man mit solch einfachen Mittel auskommt, liegt vor allem daran, daß die Aussage in diesem Fall ausnahmslos gilt. Im Fall $p \equiv 7\,(8)$ hingegen gibt es Ausnahmen, weshalb eine äußerst präzise Argumentation notwendig ist.
Nagell beweist in seinem Aufsatz auch folgende Aussage, auf die wir aber nicht näher eingehen, weil die angegebene Schranke nicht kleiner als $\sqrt{p}$ ist:

Ist $p \equiv 5\,(8)$ eine Primzahl, so gilt $\psi_p < \sqrt{p-4} + 2$.

Außerdem merkt Nagell an, daß man auf dieselbe Weise auch die folgenden beiden Aussagen zeigen könne, einen Beweis gibt er aber leider nicht an:

Ist $p \equiv 5\,(8)$ eine Primzahl mit $p \neq 5$, 13, 109, so gilt $\psi_p < \sqrt{p}$.
Ist $p \equiv 3\,(8)$ eine Primzahl mit $p \neq 131$, so gilt $\psi_p < \sqrt{p} + 4$.

Auch im Falle $p \equiv 3\,(8)$ wünscht man sich eine Schranke kleiner $\sqrt{p}$. Im übernächsten Abschnitt werden für beide Fälle das schärfere Resultat $\psi_p < \sqrt{p}$ beweisen.

5.3 Die Verschärfungen von Brauer

Schon 1931 hat Alfred Brauer in [3] mit elementaren Methoden schärfere Abschätzungen gegeben als Nagell 1950 in [40]. Nagell ist offenbar später auf die Arbeit Brauers aufmerksam geworden, er erwähnt sie erst 1951 in [42].
Da die Brauerschen Beweise aus seitenlangen kleinschrittigen Rechnungen bestehen, die gut nachzuvollziehen sind, verweisen wir auf die Originalarbeit und geben nur die Ergebnisse wieder:

(5.11) Satz von Brauer

1. *Ist* $p \equiv 5\,(8)$ *eine Primzahl, so gilt* $\psi_p < \sqrt{p+4} + 2$.
2. *Ist* $p \equiv \pm 3\,(8)$ *eine Primzahl mit* $p \geqslant 5$, *so gilt* $\psi_p < 2\sqrt[5]{16p^2} + 2\sqrt[5]{4p} + 1$.
3. *Ist* $p \equiv 7\,(8)$ *eine Primzahl, so gilt für den kleinsten primen (nicht notwendig ungeraden) quadratischen Nichtrest* q *modulo* p *stets* $q < \sqrt[5]{4p^2} + 3\sqrt[5]{2p} + 1$.

(5.12) Bemerkung

Brauers Beweisidee beruht im wesentlichen darauf, daß er auf sehr geschickte Weise aus der Sequenz der quadratischen Reste 1, 3, ... $\psi_p - 2$ eine Sequenz quadratischer Nichtreste modulo p konstruiert, die er zwischen zwei benachbarte Quadratzahlen einschließt. Durch sukzessives Aufteilen in Teilintervalle und diffizile Abschätzungen gelangt Brauer zu seinen Ergebnissen.

(5.13) Beispiele

Es seien einige Beispiele tabellarisch angeführt:

Primzahl p	ψ_p	Gauß-Nagell	Nagell I	Nagell II	Brauer	$(\log p)^2$	$\log p$
$97 \equiv 1\,(8)$	$\psi_{97} = 5$	20,7	9,8	7,0	—	20,9	4,57
$103 \equiv 7\,(8)$	$\psi_{103} = 3$	21,3	13,3	10,0	18,1	21,4	4,63
$107 \equiv 3\,(8)$	$\psi_{107} = 5$	21,7	21,7	14,3	30,3	21,8	4,67
$109 \equiv 5\,(8)$	$\psi_{109} = 11$	21,9	14,8	12,2	30,5	22,0	4,69
$1009 \equiv 1\,(8)$	$\psi_{1009} = 11$	64,5	31,8	22,4	—	47,8	6,92
$1019 \equiv 3\,(8)$	$\psi_{1019} = 7$	64,8	64,8	35,9	67,2	48,0	6,93
$1021 \equiv 5\,(8)$	$\psi_{1021} = 7$	64,9	45,2	32,0	67,2	48,0	6,93
$1031 \equiv 7\,(8)$	$\psi_{1031} = 7$	65,2	63,2	32,0	36,0	48,1	6,94
$10009 \equiv 1\,(8)$	$\psi_{10009} = 7$	201,1	100,0	70,8	—	84,8	9,21
$10067 \equiv 3\,(8)$	$\psi_{10067} = 5$	201,7	201,7	104,3	156,7	85,0	9,22
$10069 \equiv 5\,(8)$	$\psi_{10069} = 7$	201,7	141,9	100,3	156,7	85,0	9,22
$10079 \equiv 7\,(8)$	$\psi_{10079} = 11$	201,8	199,8	100,4	75,5	85,0	9,22
$100019 \equiv 3\,(8)$	$\psi_{100019} = 29$	633,5	633,5	320,3	375,6	132,6	11,5
$100069 \equiv 5\,(8)$	$\psi_{100069} = 11$	633,7	447,4	316,3	375,7	132,6	11,5
$100129 \equiv 1\,(8)$	$\psi_{100129} = 11$	633,9	316,4	223,8	—	132,6	11,5
$100267 \equiv 7\,(8)$	$\psi_{100267} = 13$	634,3	446,8	316,6	167,6	132,6	11,5

Man sieht, daß die Abschätzungen nicht besonders scharf sind. Die Differenz zum exakten Wert wird bei wachsendem p immer größer, wobei die Nagellschen Abschätzungen II im Bereich bis ungefähr 500.000 meist besser sind als die Brauerschen.

Die Spalten $(\log p)^2$ und $\log p$ zeigen, daß diese Abschätzungen bei großem p besser wären, wobei $\log p$ als obere Schranke nicht selten zu klein ist. Dies wird in [52] von Hans Salié auch nachgewiesen:

(5.14) Satz von Salié für Nichtreste
Es gibt eine Konstante $c > 0$ so, daß für unendlich viele Primzahlen p

$$\psi_p > c \cdot \log p$$

gilt.

Für den Beweis sei auf die Originalarbeit verwiesen. Der Satz läßt sich auf quadratische Reste übertragen, dieses Ergebnis findet sich in Abschnitt 6.6 mit Beweis.

5.4 Die Fälle $p \equiv 3\,(8)$ und $p \equiv 5\,(8)$

In diesem Abschnitt werden die beiden noch ausstehenden Fälle $p \equiv 5\,(8)$ und $p \equiv 3\,(8)$ behandelt. Im ersten Fall konnten wir die Nagellsche Argumentation verfeinern. Dabei stellen wir im Schlußteil des Beweises einen Widerspruch zu folgender Aussage über Sequenzen von Primzahlen in arithmetischen Progressionen her:

(5.15) Satz von Cantor-Dickson
Es seien n, d, $a \geqslant 2$ ganze Zahlen und a, $a+d$, $a+2d, \ldots a+(n-1)d$ eine Sequenz von n Primzahlen (in arithmetischer Progression). Es sei q die größte Primzahl mit $q \leqslant n$. Dann ist entweder $\prod_{p \leqslant q} p$ ein Teiler von d, oder es gilt $a = q$ und $\prod_{p<q} p$ teilt d.

Ein Beweis findet sich in [51] auf S. 284.

(5.16) Beispiel
Wähle $n = 3$, $d = 2$. Dann gilt $a = 3$, folglich ist 3, 5, 7 die einzige Primzahlsequenz der Form a, $a + 2$, $a + 4$.
Wegen $n = 3$ gilt nämlich $q = 3$. Da 6 nicht $d = 2$ teilt, muß nach diesem Satz $a = q = 3$ gelten.

(5.17) Satz
Ist $p \equiv 5\,(8)$ eine Primzahl mit $p > 13$ und $p \neq 109$, so gilt $\psi_p < \sqrt{p}$.

Beweis:
Sei $p \equiv 5\,(8)$ eine Primzahl und $\psi = \psi_p$ der kleinste ungerade Nichtrest modulo p. Es gilt stets $\left(\frac{-1}{p}\right) = 1$ und $\left(\frac{2}{p}\right) = -1$. Dividiert man p durch ψ mit Rest, erhält man

$$p = \psi k + r,$$

wobei $|r| \leqslant \frac{\psi-1}{2}$ gilt, weil ψ ungerade ist. (Nach Lemma (5.8) gilt $\psi < p$ und damit $k \geqslant 1$.) Wir unterscheiden die Fälle r ungerade und r gerade.

1. Fall: r ist ungerade

In diesem Fall ist k gerade und $\left(\frac{|r|}{p}\right) = \left(\frac{r}{p}\right) = 1$ wegen $|r| < \psi$. Genau eine der vier Zahlen $3\psi + r$, $\psi + r$, $-\psi + r$ und $-3\psi + 3$ ist $\equiv 4\,(\mathrm{mod}\,8)$. Diese Zahl werde mit r_0 bezeichnet. Dann ist $\frac{1}{4}r_0$ eine ungerade ganze Zahl mit $|\frac{1}{4}r_0| < \psi$, also gilt $\left(\frac{|\frac{1}{4}r_0|}{p}\right) = 1$ und damit $\left(\frac{r_0}{p}\right) = 1$.
Definiere die ganze Zahl k_0 durch

$$p = \psi k_0 + r_0. \tag{1}$$

Dann muß $\left(\frac{k_0}{p}\right) = -1$ sein. Je nach Definition von r_0 gilt $k_0 = k-3$, $k-1$, $k+1$ oder $k+3$. k_0 ist also ungerade, und es gilt $k_0 \geqslant k - 3 > 0$. (Wäre $k_0 = k - 3 \leqslant 0$, kämen wegen $k \geqslant 1$ nur die Fälle $k_0 = -2$, -1, 0 in Frage. $k_0 = -2$ und $k_0 = 0$ ist unmöglich, da k_0 ungerade sein muß. $k_0 = -1$ ist wegen $\left(\frac{-1}{p}\right) = 1$ ausgeschlossen.)
Aus $\left(\frac{k_0}{p}\right) = -1$ und ungeradem $k_0 > 0$ folgt

$$k_0 \geqslant \psi.$$

Unterfall 1a: Ist $r_0 = 3\psi + r$, dann gilt $k_0 = k - 3 \geqslant \psi$. Mit Gleichung (1) erhält man $p = \psi k_0 + r_0 \geqslant \psi^2 + 3\psi + r > \psi^2 + 2\psi + 1 = (\psi + 1)^2$. Hieraus folgt

$$\psi < \sqrt{p} - 1.$$

Unterfall 1b: Ist $r_0 = \psi + r$, dann gilt $k_0 = k - 1 \geqslant \psi$. Mit Gleichung (1) erhält man $p = \psi k_0 + r_0 \geqslant \psi^2 + \psi + r > \psi^2$. Hieraus folgt

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

Unterfall 1c: Ist $r_0 = -\psi + r$, dann gilt $k_0 = k + 1 \geqslant \psi$.
Ist sogar $k_0 \geqslant \psi + 2$, erhält man $p \geqslant (\psi+2)\psi - \psi + r = \psi^2 + \psi + r > \psi^2$ aus Gleichung (1) und damit

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

Da $k_0 \geqslant \psi$ ungerade ist, müssen wir nur noch den Fall $k_0 = \psi$ betrachten. Wir zeigen, daß dieser Fall nur für die ausgeschlossenen Primzahlen $p = 5, 109$ eintreten kann. Ist nämlich $k_0 = \psi$, gilt gemäß (1)

$$p = \psi^2 - \psi + r = (\psi - 1)\psi + r = (\psi - 2)(\psi + 1) + (r + 2). \tag{2}$$

$\left(\frac{r}{p}\right) = 1$ impliziert demnach $\left(\frac{\psi-1}{p}\right) = -1$, also gilt $\psi - 1 = 2^n u$ mit ungeraden natürlichen Zahlen n, u, wobei jeder Primteiler von u quadratischer Rest modulo p ist. Wäre nun $n > 1$, müßte $\psi + 1 = 2(2^{n-1}u + 1)$ wegen $\left(\frac{2}{p}\right) = -1$ ein Nichtrest sein, da $2^{n-1}u + 1 < \psi$ ungerade und damit ein quadratischer Rest wäre. Da $r + 2$ ungerade ist und $|r + 2| < \psi$ gilt, ist $\left(\frac{r+2}{p}\right) = 1$. Demnach müßte auf der rechten Seite von (2) aber $\left(\frac{\psi-2}{p}\right) = -1$ gelten, was ein Widerspruch wäre.
Also gilt $n = 1$, $\psi - 1 = 2u$, und $\psi + 1 = 2(u + 1)$ ist ein quadratischer Rest, wobei der 2-Anteil $v_2(u + 1)$ von $u + 1$ ungerade sein muß. Wir betrachten nun die weiteren Darstellungen

$$p = (\psi - 3)(\psi + 2) + (r + 6) = (\psi - 4)(\psi + 3) + (r + 12). \tag{3}$$

Ist $\psi = 3$, so muß $r = -1$ und $p = \psi^2 - \psi + r = 5$ gelten, was ausgeschlossen wurde. Wir haben also $\psi > 3$. Es gilt $\psi - 3 = 2(u - 1)$ mit einem geraden 2-Anteil $v_2(u - 1)$ und daher $\left(\frac{\psi-3}{p}\right) = \left(\frac{2}{p}\right) = -1$. Wir unterscheiden zwei Fälle:
1. Ist $\left(\frac{\psi+2}{p}\right) = 1$, so muß in (3) auf der linken Seite $r + 6$ ein ein Nichtrest sein und daher $|r + 6| \geqslant \psi$. Aus der generellen Abschätzung $|r| \leqslant \frac{\psi-1}{2}$ erhält man damit $\psi \leqslant 11$ und notwendigerweise $|r| \leqslant 5$. Geht man für die Primzahlen $3 < \psi \leqslant 11$ alle zulässigen ungeraden r durch, ergibt sich in (2) nur für $\psi = 11$ und $r = -1$ eine Primzahl $p \equiv 5\,(8)$, nämlich die ausgeschlossene Primzahl $p = 11^2 - 11 - 1 = 109$.
2. Ist $\left(\frac{\psi+2}{p}\right) = -1$, so betrachten wir in (3) die rechte Seite: $\psi + 3 = 2(u + 2)$ muß ebenso wie 2 ein Nichtrest sein, $\psi - 4$ ist ungerade und deshalb ein quadratischer Rest modulo p. Folglich gilt $\left(\frac{r+12}{p}\right) = -12$ und damit $|r + 12| \geqslant \psi$, da ungerade. Aus $|r| \leqslant \frac{\psi-1}{2}$ erhält man die Abschätzung $\psi \leqslant 23$. Wegen $\left(\frac{\psi+2}{p}\right) = -1$ muß $\psi + 2$ eine Primzahl sein, sonst gäbe es einen ungeraden Primteiler $q < \psi$, der Nichtrest wäre. Folglich müssen nur solche Primzahlen $3 < \psi \leqslant 23$ betrachtet werden, für die $\psi + 2$ ebenfalls prim ist. Geht man wieder alle zulässigen Möglichkeiten durch, ergibt sich für $\psi = 11$ abermals das ausgeschlossene $p = 109$ und für $\psi = 17$ die Primzahl $p = 277$, für die sich aber wegen $\psi_{277} = 5$ ein Widerspruch ergibt. Andere Primzahlen $p \equiv 5\,(8)$ der geforderten Art existieren nicht.
Unterfall 1d: Ist $r_0 = -3\psi + r$, dann gilt $k_0 = k + 3 \geqslant \psi$.
Ist sogar $k_0 \geqslant \psi + 4$, erhält man $p \geqslant (\psi + 4)\psi - 3\psi + r > \psi^2$ aus Gleichung (1) und damit

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

Ist $k_0 \geqslant \psi + 2$, ergibt sich voraussetzungsgemäß

$$p = (\psi+2)\psi + r_0 = \psi^2 + 2\psi + r_0 \equiv 1 + 2\psi + 4 = 5 + 2\psi \not\equiv 5 \,(\mathrm{mod}\, 8)$$

und damit ein Widerspruch.
Da $k_0 \geqslant \psi$ ungerade ist, müssen wir nur noch den Fall $k_0 = \psi$ behandeln. Wir zeigen, daß dieser Fall nicht eintreten kann. Ist nämlich $k_0 = \psi$, gilt gemäß (1)

$$p = (\psi-3)\psi + r = (\psi-2)(\psi-1) + (r-2) = (\psi-4)(\psi+1) + (r+4). \qquad (4)$$

Aus $\left(\frac{r}{p}\right) = 1$ folgt auf der linken Seite $\left(\frac{\psi-3}{p}\right) = -1$. Daher ist $\psi - 3 = 2^n u$ mit ungeraden natürlichen Zahlen n, u, wobei jeder Primteiler von u quadratischer Rest modulo p ist. Betrachtet man die Mitte von Gleichung (4), so müssen $r-2$ und $\psi-2$ beides quadratische Reste sein, da ungerade und $< \psi$. Folglich gilt auch $\left(\frac{\psi-1}{p}\right) = 1$. Wäre nun $n > 1$, müßte $\psi - 1 = 2(2^{n-1}u+1)$ wegen $\left(\frac{2}{p}\right) = -1$ aber ein Nichtrest sein, da $2^{n-1}u + 1 < \psi$ ungerade und damit ein quadratischer Rest wäre. Folglich gilt $n = 1$ und $\psi - 3 = 2u$.
Wäre $\psi = 3$, erhielten wir in (4) sofort einen Widerspruch, da $r = \pm 1$. Also gilt $\psi > 3$. Auf der rechten Seite von (4) gilt sicherlich $\left(\frac{\psi-4}{p}\right) = 1$. Ferner ist $\psi + 1 = 2(u+2)$ mit ungeradem $u+2 < \psi$, also $\left(\frac{\psi+1}{p}\right) = \left(\frac{2}{p}\right) = -1$. Daher muß auch $r+4$ ein Nichtrest sein. Somit gilt $|r+4| \geqslant \psi$. Aus $|r| \leqslant \frac{\psi-1}{2}$ ergeben sich die Abschätzungen $\psi \leqslant 7$ und $|r| \leqslant 3$. Geht man für die Primzahlen $\psi = 5$, 7 alle zulässigen Möglichkeiten durch, erhält man nur für $\psi = 7$ und $r = 1$ eine Primzahl $p \equiv 5\,(8)$, nämlich $p = \psi^2 - 3\psi + r = 29$, für die sich aber wegen $\psi_{29} = 3$ ein Widerspruch ergibt.

2. Fall: r ist gerade

In diesem Fall ist k ungerade. Wir müssen drei Fälle unterscheiden:
Unterfall 2a: Ist $r \equiv 4\,(8)$, so ist $\frac{r}{4} < \psi$ ungerade und damit $\left(\frac{r}{p}\right) = \left(\frac{r/4}{p}\right) = 1$. Aus

$$p = \psi k + r$$

folgt notwendig $\left(\frac{k}{p}\right) = -1$ und somit $k \geqslant \psi$. Es ergibt sich also $p \geqslant \psi^2 + r$.
Ist $r > 0$ oder ist $r < 0$ und $k > \psi$, gilt wie behauptet

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

Wäre $r < 0$ und $k = \psi$, erhielten wir einen Widerspruch. Denn in

$$p = \psi^2 + r = \psi^2 - \psi + a = (\psi-1)\psi + a$$

mit $\psi > a = r + \psi \geqslant \frac{\psi+1}{2}$ wäre a ungerade und daher ein quadratischer Rest (mod p). Hieraus folgte, daß $\psi - 1$ ein Nichtrest wäre. In

$$p = (\psi-1)(\psi+1) + (r+1)$$

wäre $r+1 < \psi$ und ungerade, also quadratischer Rest. Folglich müßte $\psi+1$ ein Nichtrest sein. Da $\psi - 2$ ungerade und daher quadratischer Rest wäre, ergäbe sich aus

$$p = (\psi - 2)(\psi + 1) + (a + 2),$$

daß $a + 2$ ein (ungerader) quadratischer Nichtrest ist, was $a + 2 \geqslant \psi$ bedeutete. Aus $a + 2 \geqslant \psi > a = r + \psi$ folgte $r + 2 \geqslant 0 > r$ und damit $r = -2$, was ein Widerspruch zu $r \equiv 4\,(8)$ wäre.

Unterfall 2b: Ist $r \equiv 0\,(8)$, ist $\psi \pm \frac{r}{4}$ ungerade. Wir betrachten die Darstellung

$$p = (k - 4)\psi + (4\psi + r) = (k + 4)\psi - (4\psi - r). \tag{5}$$

Ist $r < 0$, gilt $\psi + \frac{r}{4} < \psi$, also ist $\psi + \frac{r}{4}$ und damit auch $4\psi + r = 4(\psi + \frac{r}{4})$ ein quadratischer Rest modulo p. Auf der linken Seite von (5) muß die ungerade Zahl $k-4$ ein quadratischer Nichtrest sein, was $k-4 \geqslant \psi$ bedeutet. Es folgt $p \geqslant \psi^2+4\psi+r > \psi^2$ und damit wie behauptet

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

Ist $r > 0$, gilt $\psi - \frac{r}{4} < \psi$, also ist $\psi - \frac{r}{4}$ und damit auch $4\psi - r = 4(\psi - \frac{r}{4})$ ein quadratischer Rest modulo p. Auf der rechten Seite von (5) muß die ungerade Zahl $k+4$ ein quadratischer Nichtrest sein, was $k+4 \geqslant \psi$ bedeutet. Ist sogar $k+4 \geqslant \psi+4$, so erhalten wir wegen $r \geqslant 8$ stets $p \geqslant \psi^2 + r > \psi^2 + 8$ und damit wie behauptet

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

Die verbleibenden Fälle $k + 4 = \psi + 2$ und $k + 4 = \psi$ führen auf Widersprüche:
Wäre $k + 4 = \psi + 2$, hätten wir wegen $p = \psi^2 - 2\psi + r \equiv 1 - 2\psi \equiv 3,\ 7\,(\mathrm{mod}\,8)$ einen Widerspruch.
Wäre $k + 4 = \psi$, hätten wir

$$p = \psi^2 - 4\psi + r = \psi(\psi - 4) + r.$$

$\psi-4$ ist ungerade und wäre deshalb ein quadratischer Rest $(\mathrm{mod}\ p)$. Es folgte $\left(\frac{r}{p}\right) = -1$. Wegen $0 < r < \psi$ müßte $r = 2^s u$ gelten, wobei $s = v_2(r)$ und u ungerade wären und u nur quadratische Reste als Primteiler besäße. Voraussetzungsgemäß gälte $s \geqslant 3$ und damit $\psi \geqslant 17$. Wir setzen

$$t = \begin{cases} 2, & \text{falls } s = 3 \\ s - 2, & \text{sonst} \end{cases}$$

und betrachten für jede ganze Zahl $0 \leqslant n < \frac{\psi-1}{2^t}$ die Identität

$$p = (\psi - 2^t n)(\psi + 2^t n - 4) + r + 2^t n(2^t n - 4).$$

Sicherlich wäre $\psi - 2^t n$ ungerade und damit quadratischer Rest modulo p. Für die 2-Anteile würde $v_2(2^t n(2^t n - 4)) > s$ und damit $v_2(r + 2^t n(2^t n - 4)) = s$ gelten. Für

$n < 2\sqrt{\psi}$ wäre nun $r + 2^t n(2^t n - 4) < 2^s \psi$ und folglich ein Nichtrest modulo p. Daher müßten auch alle $\psi_n = \psi + 2^t n - 4$ quadratische Nichtreste sein. Außerdem müßten alle ψ_n mit $\psi_n < 2\psi$ Primzahlen sein, andernfalls wäre ein Primteiler Nichtrest $< \psi$. Nach Satz (5.15) kann aber eine solch lange Primzahlsequenz wie ψ_n nicht existieren, also Widerspruch.

Unterfall 2c: Ist $r \equiv 2\,(4)$, so ist eine der beiden Zahlen $\pm 2\psi + r \equiv 4\,(8)$. Bezeichnet man mit r_0 diese Zahl, so ist $|\frac{r_0}{4}| < \psi$ und damit quadratischer Rest modulo p. Folglich ist in

$$p = k_0\psi + r_0$$

$k_0 = k \pm 2$ ein (ungerader) Nichtrest, also $k_0 \geqslant \psi$.
Ist $r_0 = 2\psi + r$, so gilt $p \geqslant \psi^2 + 2\psi + r > \psi^2 + \psi + 2$ und damit wie behauptet

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

Ist $r_0 = -2\psi + r$, haben wir $k_0 = k + 2$. Ist sogar $k_0 \geqslant \psi + 4$, erhalten wir wieder $p \geqslant (\psi + 4)\psi - 2\psi + r > \psi^2 + 2\psi + r$ und damit wie behauptet

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

Der Fall $k_0 = \psi + 2$ führt auf den Widerspruch

$$p = (\psi + 2)\psi - 2\psi + r = \psi^2 + r \equiv 1 + 2 = 3\,(\mathrm{mod}\,4).$$

Es bleibt noch der Fall $k_0 = \psi$ zu betrachten, der ebenfalls unmöglich ist. In dieser Situation hätten wir nämlich für jede ganze Zahl $0 \leqslant n \leqslant \frac{p-3}{2}$

$$p = \psi^2 - 2\psi + r = (\psi - 2n)(\psi + 2n - 2) + r + 4n(n-1).$$

Voraussetzungsgemäß würde für den 2-Anteil $v_2(r + 4n(n-1)) = v_2(r) = 1$ gelten, also wäre $r + 4n(n-1) < 2\psi$ und damit ein quadratischer Nichtrest modulo p. Da $\psi - 2n$ ein quadratischer Rest wäre, müßte $\psi_n = \psi + 2n - 2$ ein Nichtrest sein. Wegen $|r| \leqslant \frac{\psi-1}{2}$ müßten die ψ_n für $n \leqslant \sqrt{3\psi}$ Primzahlen sein. Nach Satz (5.15) wäre dies nur für $\psi = 3$ und $n \leqslant 3$ möglich. Hieraus erhielten wir $|r| \leqslant 1$, was ein Widerspruch wäre, q. e. d.

(5.18) Satz
Ist $p \equiv 3\,(8)$ eine Primzahl mit $p > 11$ und $p \neq 59, 131$, so gilt $\psi_p < \sqrt{p}$.

Der Beweis dieses Satzes kann mit denselben Mitteln wie im vorigen Fall geführt werden, er gestaltet sich aber wesentlich komplizierter, da sowohl -1 als auch 2 quadratische Nichtreste sind. Zur Abkürzung benützen wir den Computer: Ein einfaches Programm kann nachweisen, daß die Aussage für alle Primzahlen $p \equiv 3\,(8)$ mit $11 < p < 500.000$ und $p \neq 59, 131$ erfüllt ist, siehe hierzu Abschnitt 7.2 auf S. 70. Für $p > 500.000$ gilt $\psi_p < 2\sqrt[5]{16p^2} + 2\sqrt[5]{4p} + 1 < \sqrt{p}$ nach dem Satz von Brauer (5.11).

Das Hauptresultat dieses Kapitels folgt nun aus den Sätzen (5.9), (5.17) und (5.18):

Hauptsatz 1
Für alle Primzahlen $p > 13$ mit $p \neq 23, 59, 109, 131$ gilt $\psi_p < \sqrt{p}$.
Im einzelnen gelten die folgenden Schranken:
Ist $p \equiv 1\,(8)$, so gilt $\psi_p \leqslant \sqrt{\frac{1}{2}(p+1)}$.
Ist $p \equiv 7\,(8)$ mit $p \neq 7, 23$, so gilt $\psi_p < \sqrt{p-6}$.
Ist $p \equiv \pm 3\,(8)$ mit $p > 13$ und $p \neq 59, 109, 131$, so gilt $\psi_p < \sqrt{p}$.

5.5 Analytische Abschätzungen

In diesem Abschnitt geben wir zwei Resultate wieder, die mit analytischen Mitteln erzielt worden sind. Der folgende berühmte Satz wurde 1919 von Ivan M. Vinogradov bewiesen und ist 1927 in [61] der westlichen Welt bekannt geworden. Die Abschätzung ist zwar schärfer als unser Ergebnis, hat aber den Nachteil, daß sie erst oberhalb einer Schranke p_0 gilt, die sich nicht angeben läßt.

(5.19) Satz von Vinogradov
Es existiert eine Schranke $p_0 > 0$ so, daß für den kleinsten primen (nicht notwendig ungeraden) quadratischen Nichtrest q modulo p

$$q < p^{\frac{1}{2\sqrt{e}}} (\log p)^2$$

für alle $p > p_0$ gilt.

Wir schließen dieses Kapitel mit einem Satz von Sebastian Wedeniwski, der unter der Voraussetzung der Erweiterten Riemannschen Hypothese eine sehr starke effektive Abschätzung sogar für das Jacobi-Symbol liefert. Das Resultat stammt aus dem Jahre 2001 und findet sich in [62] auf S. 122:

(5.20) Satz von Wedeniwski
Sei > 1 eine ungerade ganze Zahl, die kein Quadrat ist. Für das Jacobi-Symbol $\left(\frac{\cdot}{m}\right)$ sei $\psi_m^* = \min\left\{q \in \mathbb{N} \mid \left(\frac{q}{m}\right) = -1\right\}$. Angenommen, die Erweiterte Riemannsche Hypothese ist korrekt, dann gilt

$$\psi_m^* < \tfrac{3}{2}(\log m)^2 - \tfrac{44}{5} \log m + 13.$$

6. Kleinste prime quadratische Reste

In diesem Kapitel sollen mit elementaren Mitteln Abschätzungen für den kleinsten ungeraden primen quadratischen Rest modulo einer Primzahl erarbeitet werden. Auch hier hat sich eine Bezeichnung eingebürgert, die wir beibehalten wollen:

(6.1) Definition
Sei p eine Primzahl. Unter

$$\pi_p := \pi_2(p) := \min\left\{q \in \mathbb{P} \mid q \geqslant 3,\ \left(\tfrac{q}{p}\right) = 1\right\}$$

versteht man den *kleinsten ungeraden primen (quadratischen) Rest modulo p*.

Während die kleinsten primen Nichtreste in zahlreichen Arbeiten breit erforscht sind und auch einige elementare Abschätzungen existieren, gibt es zu den kleinsten primen Resten verhältnismäßig wenig Literatur.
Eine Ursache mag sein, daß man den Nutzen solcher Abschätzungen nicht erkannt hat, ein anderer Grund ist möglicherweise darin zu suchen, daß elementare Abschätzungen in den nichttrivialen Fällen nur mit großem Aufwand zu bekommen sind, denn der Nachweis gestaltet sich, wie im vorigen Kapitel beschrieben, viel schwieriger als im Falle der Nichtreste.
Die wesentlichen Vorarbeiten gehen auch hier auf Trygve Nagell zurück, der schon 1922 mit der Formulierung von Lemma (3.1) in diese Richtung gegangen ist und in seinen Arbeiten der fünfziger Jahre schließlich konkrete Abschätzungen bewiesen hat. 1933 hat Derrick Lehmer, Starks Doktorvater, in [30] mit Siebmethoden kleinste quadratische Reste bestimmt und damit $h(-p) > 1$ für alle Primzahlen $163 < p < 5.000.000.000$ nachgewiesen. Zwar gibt es einige nicht effektive analytische Ergebnisse, Nagells Arbeit bleibt aber — ohne zitiert zu werden — bis in die siebziger und achtziger Jahre hinein die einzige Anstrengung um konkrete Abschätzungen für π_p.
Im einfachen Fall einer Primzahl $p \equiv 1\,(4)$ konstruiert man, wie in Abschnitt 6.1 ausgeführt wird, eine natürliche Zahl, bei der aufgrund ihrer Struktur jeder Primteiler ein ungerader quadratischer Rest modulo p ist. Hier macht auch die Abschätzung keine Schwierigkeiten.

Der Fall $p \equiv 7\,(8)$ bereitet erheblich mehr Schwierigkeiten, läßt sich aber dennoch meist konstruktiv lösen. In einem Fall muß man mit Hilfe des Satzes von Minkowski einen Widerspruch herleiten.
$p \equiv 3\,(8)$ ist der wirklich interessante Fall, weil nur in dieser Restklasse die Primzahlen $p > 7$ liegen, deren Klassenzahl 1 sein kann. Daher treten hier Probleme auf, denn im Falle $h(-p) = 1$ gilt nach dem Lemma von Nagell (3.1) stets $\pi_p \geqslant \frac{p+1}{4}$, während man für $h(-p) > 1$ eine wesentlich bessere Abschätzung erwarten muß. Möchte man aber in irgendeiner Weise das Klassenzahl-1-Problem angreifen, muß man nach Abschätzungen suchen, die von der Klassenzahl unabhängig sind. Dies geschieht in Abschnitt 6.4.

6.1 Der einfache Fall $p \equiv 1\,(4)$

Die ersten konkreten Abschätzungen für π_p überhaupt finden sich wie gesagt bei Nagell, und zwar 1923 in [39] und 1950 in [40]:

(6.2) Satz
Ist $p \equiv 1\,(4)$ eine Primzahl mit $p > 17$, so existiert eine ungerade Primzahl $q < \sqrt{p}$ mit

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

Das heißt, für jede Primzahl $p \equiv 1\,(4)$ mit $p > 17$ gilt $\pi_p < \sqrt{p}$.

Beweis:
Jede Primzahl $p \equiv 1\,(4)$ ist nach dem Satz von Fermat-Euler als Summe einer ungeraden und einer geraden Quadratzahl darstellbar. Es gibt also a, $b \in \mathbb{N}$ mit

$$p = a^2 + 4b^2,$$

wobei a ungerade ist.
1. Fall: Ist $a > 1$, so ist jeder Primteiler q von a ungerader quadratischer Rest modulo p, denn aus $q \mid a$ ergibt sich $p = q \cdot r + 4b^2$ und mit dem Quadratischen Reziprozitätsgesetz

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{q \cdot r + 4b^2}{q}\right) = \left(\frac{4b^2}{q}\right) = 1.$$

Aus $q \mid a$ folgt außerdem $q \leqslant a$, mit $a^2 = p - 4b^2$ und $b \geqslant 1$ gilt also

$$\pi_p \leqslant q \leqslant a = \sqrt{p - 4b^2} \leqslant \sqrt{p - 4} \leqslant \sqrt{p}.$$

2. Fall: Ist $a = 1$ und enthält b einen ungeraden Primteiler q, so ist q quadratischer Rest modulo p, denn $q \mid b$ impliziert $p = 1^2 + 4q \cdot r$ und damit

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1^2+4q\cdot r}{q}\right) = \left(\frac{1^2}{q}\right) = 1.$$

Aus $q \mid b$ folgt $q \leqslant b$, mit $b^2 = \frac{1}{4}(p-1)$ ergibt sich daraus

$$\pi_p \leqslant q \leqslant b = \tfrac{1}{2}\sqrt{p-1} \leqslant \sqrt{p}.$$

3. Fall: Ist $a = 1$ und enthält b keinen ungeraden Primteiler, so muß $4b^2 = 2^m$ und damit $p = 2^m + 1$ gelten. Zahlen dieser Form sind bekanntlich nur dann Primzahlen, wenn m eine Zweipotenz ist, das heißt, wenn $m = 2^n$ gilt und $p = 2^{2^n} + 1$ eine Fermatsche Primzahl ist. Die Fälle $n = 1, 2$ sind wegen $p > 17$ ausgeschlossen. Für $n = 3$ erhält man $p = 257$ mit $\pi_{257} = 11 < \sqrt{257}$. Sei im folgenden $n \geqslant 4$.
Zieht man aus der Gleichung $p - 1 = 2^{2^n}$ für ein beliebiges $i \in \{2, 3, \ldots, n-2\}$ die 2^{n-i}-te Wurzel, erhält man die natürliche Zahl

$$s = \sqrt[2^{n-i}]{p-1} = 2^{2^i}.$$

Jeder Primteiler q von $s+1$ ist ein ungerader quadratischer Rest modulo p. Da nämlich s eine vierte Potenz ist, gibt es ein $u \in \mathbb{N}$ mit $q \mid u^4 + 1$. Aus $u^4 + 1 \equiv 0\,(q)$ folgt $u^8 \equiv 1\,(q)$, also $\operatorname{ord}(u \bmod q) = 8$. Nach dem Satz von Fermat-Euler ergibt sich hieraus $8 \mid \operatorname{ord}(\mathbb{F}_q) = q - 1$, das heißt

$$q \equiv 1\,(8).$$

Aus $q \mid s+1$ folgt $s = q\cdot r - 1$. Damit erhält man $p-1 = s^{2^{n-i}} = (q\,r-1)^{2^{n-i}} \equiv 1\,(\mathrm{mod}\ q)$, wenn man ausmultipliziert, also

$$p \equiv 2\,(q).$$

Insgesamt ergibt sich

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

Wegen $2^{n-i} \geqslant 4$ gilt außerdem

$$\pi_p \leqslant q \leqslant \sqrt[2^{n-i}]{p-1} + 1 \leqslant \sqrt{p}$$

für jedes $p \geqslant 7$, q. e. d.

In der ersten Arbeit hat Nagell den dritten Fall des Beweises nur angedeutet, in der späteren Arbeit ist der Fall dann ausgeführt, allerdings mit einem kleinen Fehler: Das i kann unmöglich als $n - 1$ gewählt werden, wie dort angegeben ist, weil ansonsten die letzte Ungleichung ungültig würde. Daher muß $n \geqslant 4$ vorausgesetzt werden, weshalb der Fall $n = 3$ separat zu behandeln ist.
Man kann aber den dritten Fall, also den Fall einer Fermatschen Primzahl, noch viel konkreter behandeln:

(6.3) Satz

Für jede Fermatsche Primzahl $p = 2^{2^n} + 1$ mit $n \geqslant 1$ gilt:
Ist n gerade, gilt $\pi_p = 13$; ist n ungerade, gilt $\pi_p = 11$.

Beweis:

Für $n \geqslant 1$ gilt $p \equiv 1\,(4)$. Aus $p = (3-1)^{2^n} + 1$ wird $p \equiv 2\,(3)$ klar, also $p \equiv 5\,(12)$. Nach (3.3) gilt dann

$$\left(\tfrac{3}{p}\right) = \left(\tfrac{p}{3}\right) = -1.$$

Für $n > 1$ wird aus $p = (5-1)^{2^{n-1}} + 1$ stets $p \equiv 2\,(5)$ ersichtlich. Mit dem zweiten Ergänzungssatz ergibt sich

$$\left(\tfrac{5}{p}\right) = \left(\tfrac{p}{5}\right) = \left(\tfrac{2}{5}\right) = -1.$$

Da für die Ordnung $o(2 \bmod 7) = 3$ gilt, hat man $2^{2^n} \equiv 2, 4\,(7)$, also $p \equiv 3, 5\,(7)$. Damit erhält man

$$\left(\tfrac{7}{p}\right) = \left(\tfrac{p}{7}\right) = -1.$$

Hieraus folgt $\pi_p \geqslant 11$.
Es gilt $o(2 \bmod 11) = 10$ und daher $o(2^{2^n} \bmod 11) = 5$, da $n \geqslant 1$. Für ungerades n erhalten wir $2^{2^n} \equiv 3, 4\,(11)$, also $p \equiv 4, 5\,(11)$ und somit

$$\left(\tfrac{11}{p}\right) = \left(\tfrac{p}{11}\right) = 1.$$

Für gerades n erhalten wir dagegen $2^{2^n} \equiv 5, 9\,(11)$, also $p \equiv 6, 10\,(11)$ und somit

$$\left(\tfrac{11}{p}\right) = \left(\tfrac{p}{11}\right) = -1.$$

Aus $o(2 \bmod 13) = 12$ und $o(2^{2^n} \bmod 13) = 3$ folgt $2^{2^n} \equiv 3\,(13)$, woraus sich $p \equiv 4\,(11)$ und daher

$$\left(\tfrac{13}{p}\right) = \left(\tfrac{p}{13}\right) = 1$$

ergibt, q. e. d.

6.2 Der Fall $p \equiv 7\,(8)$

In [40] hat Nagell auch den Fall $p \equiv 7\,(8)$ behandelt und nachgewiesen, daß $\pi_p \leqslant 2\sqrt{p}-1$ gilt, falls $p > 7$. Möchte man dieses Resultat auf $\pi_p < \sqrt{p}$ verschärfen, muß man einen erheblich größeren Aufwand treiben.
Zunächst behandeln wir den Fall der Mersenneschen Primzahlen, bei denen sich wie bei Fermatschen Primzahlen konkrete Werte für π_p angeben lassen:

(6.4) Satz
Für jede Mersennesche Primzahl $p = 2^r - 1$ mit einer Primzahl $r \geqslant 3$ gilt:

$$\pi_p = \begin{cases} 5, & \text{falls } r \equiv 1\,(4) \\ 11 \text{ oder } 13, & \text{falls } r \equiv 3\,(4) \text{ und } r \equiv 1\,(3) \\ 7, & \text{falls } r \equiv 3\,(4) \text{ und } r \equiv 2\,(3) \end{cases}$$

Beweis: Es gilt $\pi_7 = 11$. Im weiteren sei $r > 3$. Wegen $p = (3-1)^r - 1$ gilt $p \equiv 1\,(3)$, daher also

$$\left(\tfrac{3}{p}\right) = -\left(\tfrac{p}{3}\right) = -\left(\tfrac{1}{3}\right) = -1.$$

Hieraus folgt $\pi_p \geqslant 5$.
Ist nun $r \equiv 1\,(4)$, so ergibt sich $2^{r-1} = (2^4)^{(r-1)/4} \equiv 1\,(5)$, also $p \equiv 2 \cdot 1 - 1 \equiv 1\,(5)$ und damit

$$\left(\tfrac{5}{p}\right) = \left(\tfrac{p}{5}\right) = \left(\tfrac{1}{5}\right) = 1.$$

Ist $r \equiv 3\,(4)$ und $r \equiv 2\,(3)$, ergibt sich zusammen mit $r > 3$ stets $2^{r-1} = 2 \cdot 2^{r-2} = 2(7+1)^{(r-2)/3} \equiv 2\,(7)$. Aus $p \equiv 2 \cdot 2 - 1 \equiv 3\,(7)$ folgt nun mit (3.3)

$$\left(\tfrac{7}{p}\right) = -\left(\tfrac{p}{7}\right) = -\left(\tfrac{3}{7}\right) = 1.$$

Ist $r \equiv 3\,(4)$ und $r \equiv 1\,(3)$, gilt $o(2^{r-1} \bmod 7) = 1$, also $p \equiv 2 \cdot 1 - 1 \equiv 1\,(7)$ und damit

$$\left(\tfrac{7}{p}\right) = -\left(\tfrac{p}{7}\right) = -\left(\tfrac{1}{7}\right) = -1.$$

Wegen $o(2^{r-1} \bmod 13) = 2$ muß $2^{r-1} \equiv -1\,(13)$ gelten. Hieraus erhalten wir $p \equiv 2 \cdot (-1) - 1 \equiv -3\,(13)$ und damit

$$\left(\tfrac{13}{p}\right) = \left(\tfrac{p}{13}\right) = \left(\tfrac{-3}{13}\right) = \left(\tfrac{3}{13}\right) = \left(\tfrac{1}{3}\right) = 1.$$

Daher gilt in diesem Fall $7 < \pi_p \leqslant 13$, q. e. d.

Desweiteren benötigen wir zwei Sätze, die uns einfache Abschätzungen für die Klassenzahl $h(-p)$ liefern. Das erste Resultat ist eine Folge aus dem Satz von Minkowski:

(6.5) Satz
Sei $p \equiv 7\,(8)$ eine Primzahl.
Ist $\pi_p \geqslant \frac{2}{\pi}\sqrt{p}$, so ist die Klassengruppe von $\mathbb{Q}(\sqrt{-p})$ zyklisch, und es gilt $2^{h(-p)} < \frac{4}{\pi}\sqrt{p}$.

Beweis:
Nach dem Satz von Minkowski existiert in jeder Idealklasse von $K = \mathbb{Q}(\sqrt{-p})$ ein ganzes Ideal mit Norm $< \frac{2}{\pi}\sqrt{p}$. Sei nun $q \neq 2$ eine Primzahl mit $q < \frac{2}{\pi}\sqrt{p}$ und $\mathfrak{q}$ ein Primideal von K über q. Nach Voraussetzung gilt

$$\left(\tfrac{-p}{q}\right) = \left(\tfrac{q}{p}\right) = -1,$$

q ist also träge, das heißt, $\mathfrak{q} = (q)$ ist ein Hauptideal mit $N\mathfrak{q} = q^2$ und liegt demnach in der Hauptklasse. Wegen $p \equiv 7\,(8)$ zerfällt die 2 in K, es gibt also eine Zerlegung der Form $(2) = \mathfrak{p}\mathfrak{p}'$. Daher muß in jeder Idealklasse $\neq 1$ eine Potenz von $\mathfrak{p}$ liegen, die Klassengruppe $Cl(K)$ wird also zyklisch von $\mathfrak{p}$ erzeugt. Die Potenzen $\mathfrak{p}^i$ sind die einzigen möglichen Ideale von K mit einer Norm $< \frac{2}{\pi}\sqrt{p}$, die nicht Hauptideale sind. Hieraus folgt $2^{h(-p)-1} = N(\mathfrak{p}^{h(-p)-1}) < \frac{2}{\pi}\sqrt{p}$, q. e. d.

Der folgende Satz gibt eine effektive untere Schanke für die Klassenzahl an. Er stammt von Nagell und findet sich in [38] auf S. 140f., wo er völlig elementar bewiesen wird. Gross und Zagier haben bekanntlich gezeigt, daß es für alle imaginär-quadratischen Zahlkörper eine solche effektive Schranke gibt. Im allgemeinen liefert der Satz von Brauer-Siegel nur qualitative Aussagen.

(6.6) Satz
Für jede Primzahl $p \equiv 7\,(8)$ ist $h(-p) \geqslant \log_2(p+1) - 2$.

Beweis:
Wie im vorigen Beweis sei $2 \mid \mathfrak{p}$ ein Primideal in $K = \mathbb{Q}(\sqrt{-p})$ über 2. Außerdem sei h die Ordnung der Klasse von $\mathfrak{p}$ in $Cl(K)$. Dann ist h ein Teiler von $h(-p)$ und $\mathfrak{p}^h = (\alpha)$ notwendig ein Hauptideal in K. Ist nun $\alpha = x + y\frac{1+\sqrt{-p}}{2}$ mit teilerfremden ganzen Zahlen x, y, so folgt

$$2^h = N\mathfrak{p}^h = N(\alpha) = x^2 + xy + \tfrac{p+1}{4}y^2,$$

woraus man $2^h \geqslant \frac{p+1}{4}$ und damit $h(-p) \geqslant h \geqslant \log_2(p+1) - 2$ erhält, q. e. d.

Schließlich wird ein Lemma aus der elementaren Zahlentheorie benötigt, das aus dem Henselschen Lemma und der Gruppenstruktur von $(\mathbb{Z}/2^n\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ folgt, siehe beispielsweise [25] auf S. 43–45.

(6.7) Lemma

Seien c, n ganze Zahlen mit $c \equiv 1\,(8)$ und $n \geqslant 3$.

1. *Dann hat die Kongruenz $X^2 \equiv c \pmod{2^n}$ genau vier Lösungen modulo 2^n.*
2. *Ist x_0 die kleinste positive Lösung dieser Kongruenz, so sind x_0, $2^{n-1}-x_0$, $2^{n-1}+x_0$ und $2^n - x_0$ paarweise inkongruente Lösungen modulo 2^n, und es gilt*

$$0 < x_0 < 2^{n-1} - x_0 < 2^{n-1} + x_0 < 2^n - x_0.$$

Damit können wir den zentralen Satz dieses Abschnitts beweisen:

(6.8) Satz

Für jede Primzahl $p \equiv 7\,(8)$ mit $p > 7$ gilt $\pi_p < \sqrt{p}$.

Beweis:

Wegen $p > 7$ gibt es eine natürliche Zahl $n \geqslant 3$ mit $\sqrt{p} < 2^n < 2\sqrt{p}$. Wegen $-p \equiv 1\,(8)$ besitzt die Kongruenz

$$X^2 \equiv -p\,(2^n)$$

nach Lemma (6.7) genau vier Lösungen modulo 2^n, von denen u die kleinste positive sei. Aus $u < 2^{n-1} - u$ folgt $u < 2^{n-2}$. Dann sind

$$a = \frac{p + u^2}{2^n} \quad \text{und} \quad b = \frac{p + (2^{n-1} - u)^2}{2^n}$$

positive ganze Zahlen mit

$$b - a = 2^{n-2} - u > 0.$$

Da u ungerade ist, muß auch $b - a$ ungerade sein, woraus folgt, daß genau eine der Zahlen a und b ungerade ist. Aus den Abschätzungen

$$a > \frac{p + u^2}{2\sqrt{p}} > \frac{1}{2}\sqrt{p} > 2^{n-2},$$

$$b < \frac{p + (\sqrt{p} - 1)^2}{\sqrt{p}} < 2\sqrt{p} < 2^{n+1}$$

erhält man die zentrale Ungleichungskette

$$u < 2^{n-2} < \frac{1}{2}\sqrt{p} < a < b < 2\sqrt{p} < 2^{n+1}. \tag{1}$$

Jeder ungerade Primteiler q von a bzw. von b ist ein quadratischer Rest modulo p. Mit $p \equiv 7\,(8)$ und $p \equiv -u^2\,(q)$ bzw. $p \equiv -(2^{n-1} - u)^2\,(q)$ ergibt sich nämlich aus dem Quadratischen Reziprozitätsgesetz

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

Wir schätzen nun den ungeraden Primteiler q nach oben ab:
1. Fall: Ist a ungerade, so muß b gerade sein. Wenn b keine 2-Potenz ist, existiert ein ungerader Primteiler q von b mit

$$q \leqslant \tfrac{b}{2} < \sqrt{p}.$$

Wenn b eine 2-Potenz ist, kommen nach (1) nur die Fälle $b = 2^{n-1}$ oder $b = 2^n$ in Betracht. Ist $b = 2^{n-1}$, so gilt mit (1) für jeden Primteiler q von a stets

$$q \leqslant a < b = 2^{n-1} < \sqrt{p}.$$

Ist $b = 2^n$, erhalten wir einen Widerspruch. Wäre $b = 2^n$, erhielten wir aus der Definition von b die Gleichung $p = 2^{2n} - (2^{n-1} - u)^2 = (2^n - (2^{n-1} - u))(2^n + (2^{n-1} - u))$. Wegen $u < 2^{n-2}$ wären beide Faktoren > 1, p könnte also nicht prim sein.
2. Fall: Ist b ungerade, so muß a gerade sein. Wenn a keine 2-Potenz ist, existiert ein ungerader Primteiler q von a mit

$$q \leqslant \tfrac{a}{2} < \tfrac{b}{2} < \sqrt{p}.$$

Wenn a eine 2-Potenz ist, kommen nach (1) nur die Fälle $a = 2^{n-1}$ oder $a = 2^n$ in Betracht.
Ist $a = 2^{n-1}$, so erhält man $2^{2n-1} = 2^n a = p + u^2$ aus der Definition von a und damit

$$p = 2^{2n-1} - u^2. \tag{2}$$

Setzt man dies in die Definition von b ein, gewinnt man die Gleichung $b = 3 \cdot 2^{n-2} - u$. Soll nun $b < \sqrt{p}$ gelten und setzt man (2) hierein ein, erhält man die quadratische Ungleichung $u^2 - 3 \cdot 2^{n-2}u + 2^{2n-5} < 0$. Hieraus wird ersichtlich, daß genau dann $b < \sqrt{p}$ gilt, wenn $u > 2^{n-3}(3 - \sqrt{7})$ ist. Für jeden Primteiler q von b gilt dann $b < \sqrt{p}$. Sei also im folgenden

$$1 \leqslant u \leqslant 2^{n-3}(3 - \sqrt{7}) < 2^{n-4}, \tag{3}$$

woraus $n \geqslant 5$ folgt. Wir argumentieren indirekt und nehmen an, es existiere keine ungerade Primzahl q mit $\left(\frac{q}{p}\right) = 1$. Aus (2) folgt $2^{2n-1} > p$ und damit $\log_2 p < 2n - 1$. Zusammen mit Satz (6.5), nach dem $h(-p) < 2 + \frac{1}{2}\log_2 p$ gilt, ergibt sich

$$h(-p) < \tfrac{1}{2}\log_2 p + 2 < n + \tfrac{3}{2}.$$

Aus (2) und (3) folgt $p = 2^{2n-1} - u^2 > 2^{2n-2} - 1$ und damit $\log_2(p+1) > 2n - 2$. Zusammen mit Satz (6.6) ergibt sich

$$h(-p) \geqslant \log_2(p+1) - 2 > 2n - 4.$$

Hieraus folgt insgesamt

$$2n - 4 < h(-p) < n + \tfrac{3}{2},$$

woraus man $n < 5,5$ und damit $n = 5$ erhält. Nach (3) muß also $u = 1$ gelten. Das führt nach (2) auf die Mersennesche Zahl $p = 2^9 - 1 = 511 = 7 \cdot 73$, die keine Primzahl ist, Widerspruch!
Ist $a = 2^n$, erhalten wir ebenfalls einen Widerspruch. Wäre $a = 2^n$, erhielten wir aus der Definition von a die Gleichung $p = 2^{2n} - u^2 = (2^n - u)(2^n + u)$. Wegen $u < 2^{n-2}$ wären beide Faktoren > 1, p könnte also nicht prim sein, q. e. d.

(6.9) Beispiele

Der Beweis ist bis auf den Fall $a = 2^{n-1}$ und $u \leqslant 2^{n-3}(3 - \sqrt{7})$ konstruktiv, das heißt, nach dem angegebenen Verfahren lassen sich kleine quadratische Reste konkret berechnen:

p	n	u	a	b	q
31	3	1	4	5	$5 = \pi_{31}$
71	4	3	5	6	$3 = \pi_{71}$
79	4	1	5	8	$5 = \pi_{79}$
103	4	3	7	8	$7 = \pi_{103}$
167	4	3	11	12	$3 = \pi_{167}$
223	4	1	14	17	$7 = \pi_{223}$
271	5	7	10	11	$5 = \pi_{271}$
367	5	7	13	14	$7 = \pi_{367}$
479	5	1	15	22	$3 = \pi_{479}$
487	5	5	16	19	$19 = \pi_{487}$
1103	6	7	18	27	$3 = \pi_{1103}$
1399	6	3	22	35	$5 = \pi_{1399}$
1559	6	13	27	30	$3 = \pi_{1559}$
1823	6	15	32	33	$3 = \pi_{1823}$
1831	6	5	29	40	$5 = \pi_{1831}$
2143	6	15	37	38	$19 \neq \pi_{2143}$
7351	7	29	64	67	$67 \neq \pi_{7351}$

Man sieht, daß der konstruierte Primteiler q sehr häufig mit π_p übereinstimmt, daß es hiervon aber auch Ausnahmen gibt.

(6.10) Bemerkung

Der erwähnte Fall $a = 2^{n-1}$ und $u \leqslant 2^{n-3}(3 - \sqrt{7})$, also $b \geqslant \sqrt{p}$, tritt tatsächlich auf; man kann daher auf die Anwendung der Sätze (6.5) und (6.6) nicht ohne weiteres verzichten:

p	n	u	a	b	q	$\sqrt{p}$
32647	8	11	128	$181 \in \mathbb{P}$	181	180,68
32687	8	9	128	$183 = 3 \cdot 61$	$3 = \pi_{32687}$	180,80
130783	9	17	256	$367 \in \mathbb{P}$	367	361,64
523927	10	19	512	$749 = 7 \cdot 107$	$7 = \pi_{523927}$	723,83
2094343	11	53	1024	$1483 \in \mathbb{P}$	1483	1447,18
8364583	12	155	2048	$2917 \in \mathbb{P}$	2917	2892,16

6.3 Der Fall $p \equiv 3\,(8)$ mit Klassenzahl-Bedingung

In diesem und dem folgenden Abschnitt behandeln wir den verbliebenen Fall $p \equiv 3\,(8)$. Nach Satz (2.4) können nur hier Primzahlen mit $h(-p) = 1$ vorkommen. Als erstes gewichtiges Resultat haben wir einen Satz aus dem Jahre 1922, mit welchem Nagell sein Lemma (3.1) in [38] deutlich verschärft hat:

(6.11) Satz von Nagell

Sei $p \equiv 3\,(8)$ eine Primzahl mit $p \geqslant 11$.
Dann sind äquivalent:

1. $h(-p) = 1$
2. *Es gilt* $\left(\frac{q}{p}\right) = -1$ *für alle Primzahlen* $q < \frac{p+1}{4}$.
3. *Es gilt* $\left(\frac{q}{p}\right) = -1$ *für alle Primzahlen* $q \leqslant \sqrt{\frac{p+16}{3}} - 2$.

Beweis:
1. $\Longrightarrow$ 2. ist das Lemma von Nagell (3.1).
2. $\Longrightarrow$ 3. ist wegen $\sqrt{\frac{p+16}{3}} - 2 < \frac{p+1}{4}$ für $p \geqslant 11$ klar.
3. $\Longrightarrow$ 1. Es sei

$$\pi = \pi_p = q_1,\, q_2,\, q_3,\, q_4 \ldots \tag{1}$$

die nach zunehmender Größe geordnete Folge der Primzahlen q_i mit $\left(\frac{q_i}{p}\right) = 1$. Es gilt dabei $\pi_p \leqslant \frac{p+1}{4}$, weil nach dem Reste-Lemma (4.3) jeder Primteiler von $\frac{p+1}{4}$ ein quadratischer Rest modulo p ist. Aus dem Reste-Lemma (4.3) folgt ebenfalls, daß jeder Primteiler q von

$$x^2 - x + \tfrac{p+1}{4} \quad (x \in \mathbb{Z})$$

eines der q_i aus (1) ist ($i \in \mathbb{N}$). Wegen

$$\left(\tfrac{-p}{\pi}\right) = \left(\tfrac{-1}{\pi}\right)\left(\tfrac{p}{\pi}\right) = \left(\tfrac{-1}{\pi}\right)\left(\tfrac{-1}{\pi}\right)\left(\tfrac{\pi}{p}\right) = \left(\tfrac{\pi}{p}\right) = 1$$

existiert eine ganze Zahl y mit $y^2 \equiv -p \pmod{\pi}$. Dabei kann man, da $\pi - 1$ gerade ist, y im Intervall $[-\pi + 2, \pi - 2]$ ungerade wählen. Folglich gibt es natürliche Zahlen x_0 und t, so daß $(2x_0 - 1)^2 + p = 4\pi t$ und damit

$$x_0^2 - x_0 + \tfrac{p+1}{4} = \pi t \tag{2}$$

gilt, wobei man $|2x_0 - 1| \leqslant \pi - 2$ hat. Aus letzterer Ungleichung folgt durch Quadrieren

$$\pi t \leqslant \tfrac{1}{4}(\pi^2 - 4\pi + 4 + p).$$

Nach Voraussetzung gilt nun

$$\sqrt{\tfrac{p+16}{3}} - 2 < \pi, \tag{3}$$

woraus man die Ungleichung $p < 3\pi^2+12\pi-4$ erhält, die auf $\frac{1}{4}(\pi^2-4\pi+4+p) < \pi^2+2\pi$ führt. Insgesamt erhalten wir also

$$\pi t \leqslant \tfrac{1}{4}(\pi^2 - 4\pi + 4 + p) < \pi^2 + 2\pi = \pi(\pi + 2),$$

woraus $0 < t < \pi+2$ folgt. Da $\pi+1$ gerade ist, kann t nur die Werte 1 oder π annehmen. Ist $t = 1$, erhält man aus (2)

$$x_0^2 - x_0 + \tfrac{p+1}{4} = \pi,$$

was wegen $\frac{p+1}{4} \leqslant x_0^2 - x_0 + \frac{p+1}{4} = \pi \leqslant \frac{p+1}{4}$ nur für $x_0 = 1$ und $\pi = \frac{p+1}{4}$ möglich ist. Ist $t = \pi$, erhält man aus (2)

$$x_0^2 - x_0 + \tfrac{p+1}{4} = \pi^2,$$

woraus man $p = 4\pi^2 - (2x_0 - 1)^2$ und damit $p = (2\pi + 2x_0 - 1)(2\pi - 2x_0 + 1)$ erhält. Folglich gilt $2\pi - 2x_0 + 1 = 1$, also $x_0 = \pi$ und damit ebenfalls $\pi = \frac{p+1}{4}$.
Hieraus ergibt sich also, daß $\pi = q_1$ unter der Bedingung (3) von der Hauptform $X^2 + XY + \frac{p+1}{4}Y^2$ eigentlich dargestellt wird, nämlich für $x = 1$ und $y = -1$.
Wir beweisen durch vollständige Induktion, daß alle Primzahlen der Reihe (1) durch die Hauptform eigentlich dargestellt werden. Nach dem oben Gezeigten gilt die Induktionsvoraussetzung. Nehmen wir nun an, daß die $q_1, q_2, \ldots, q_{n-1}$ von der Hauptform dargestellt werden, so muß die Hauptform auch q_n darstellen. Wie oben sieht man nämlich, daß eine ganze Zahl x_1 existiert, so daß

$$x_1^2 - x_1 + \tfrac{p+1}{4} = q_n t'$$

mit $|2x_1 - 1| \leqslant q_n - 2$ gilt. Hieraus erhält man wieder

$$q_n t' \leqslant \tfrac{1}{4}(q_n^2 - 4q_n + 4 + p).$$

Aus (3) ergibt sich nun $\frac{1}{3}(p + 16) < (\pi + 2)^2 \leqslant q_n^2$, woraus sich insgesamt

$$q_n t' \leqslant \tfrac{1}{4}(q_n^2 - 4q_n + 4 + 3q_n^2 - 16) = q_n^2 - q_n - 3 < q_n^2$$

und damit

$$t' < q_n$$

ergibt. Die natürliche Zahl t' kann demnach nur die Primteiler $q_1, q_2, \ldots, q_{n-1}$ besitzen, welche nach der Induktionsvoraussetzung von der Hauptform dargestellt werden. Durch wiederholte Anwendung von Korollar (4.5) erhält man nun

$$q_n = x^2 + xy + \tfrac{p+1}{4}y^2.$$

Daher stellt die Hauptform $X^2 + XY + \frac{p+1}{4}Y^2$ alle Primzahlen der Reihe (1) eigentlich dar, es muß also $h(-p) = 1$ gelten, q. e. d.

Es ist klar, daß in diesem Satz Abschätzungen für π_p enthalten sind, die von $h(-p)$ abhängen:

(6.12) Korollar
Für jede Primzahl $p \equiv 3\,(8)$ mit $p \geqslant 11$ gilt:
1. Ist $h(-p) = 1$, so gilt $\pi_p = \frac{p+1}{4} \in \mathbb{P}$.
2. Ist $h(-p) > 1$, so gilt $\pi_p \leqslant \sqrt{\frac{p+16}{3}} - 2$.

Wir sind nun in der Lage, das zweite Hauptresultat dieser Arbeit vorzustellen, das aus den Sätzen (2.4), (6.2), (6.8) und (6.12) folgt:

Hauptsatz 2
Sei $p > 11$ eine Primzahl mit $p \neq 17$.
Genau dann gilt $\pi_p < \sqrt{p}$, wenn $h(-p) > 1$ ist.

(6.13) Bemerkung
In der angelsächsischen Welt wurden die Aufsätze Nagells, die entweder in deutscher oder französischer Sprache abgefaßt sind, überhaupt nicht zur Kenntnis genommen. Ohne auf diese Arbeiten einzugehen, beweisen S. Chowla sowie J. und M. Cowles 1986 in [6] obiges Korollar mit einer geringfügig schwächeren Abschätzung. Den Satz (6.2) beweisen die Autoren mit einem „eiligen“ Argument nur für den Fall $p \equiv 5\,(8)$, auf die Fälle $p \equiv 1\,(8)$ sowie $p \equiv 7\,(8)$ gehen sie nicht ein.
Dies zeigt einerseits, welche Faszination von solchen elementaren Fragestellungen und einer ebenso elementaren Lösung auch heute noch ausgeht.
Andererseits wird deutlich, daß im schnellebigen mathematischen Betrieb zuweilen als vermeintlich neue Erkenntnis präsentiert wird, was lediglich in Vergessenheit geraten ist. Dies zeigt, wie wichtig der Blick zurück gerade für die „Königin der Wissenschaften“ wäre, die der historischen Betrachtungsweise immer ein wenig abschätzig gegenübersteht. Diese Bemerkung sei gestattet.

Der Beweis des Satzes von Nagell (6.11) ist zwar elementar, aber nur im Grundsatz konstruktiv. Zur Bestimmung von kleinen quadratischen Resten kann man ihn praktisch nicht verwenden. Zur konkreten Bestimmung kleiner Reste für Primzahlen $p \equiv 3\,(8)$ wenden wir ein zum Fall $p \equiv 1\,(4)$ analoges Argument an, indem wir p als Summe von drei Quadraten darstellen.
Die Erkenntnisse über die Darstellbarkeit von Zahlen als Summe von drei Quadraten gehen im wesentlichen auf Carl Friedrich Gauß zurück. In Art. 291 seiner *Disquisitiones arithmeticae* beweist er den berühmten „Drei-Quadrate-Satz“:

(6.14) Satz von Gauß
Für jede natürliche Zahl n sind äquivalent:

(i) *Es gilt die Gleichung $n = a^2 + b^2 + c^2$ mit $a, b, c \in \mathbb{N}$.*

(ii) *Die Zahl n ist nicht von der Form $4^r(8s + 7)$ mit $r, s \in \mathbb{N}$.*

Dieser Satz wird von Daniel Flath im fünften Kapitel von [15] ausführlich dargestellt und bewiesen. Dort werden auf S. 178 auch detaillierte Angaben über die Anzahl der Darstellungen gemacht. Zusammen mit der Gesamtdarstellungsformel

$$R(n) = \sum_{m|n} \chi_D(m),$$

die die Gesamtdarstellungsanzahl $R(n)$ von n durch Formen der Diskriminante D angibt und die von Don Zagier in [63] auf S. 65ff. beweisen wird, erhalten wir in unserem speziellen Fall $p \equiv 3\,(8)$:

(6.15) Satz
Für jede Primzahl $p \equiv 3\,(8)$ mit $p \geqslant 11$ gilt:

(i) *Ist $h(-p) > 1$, so existieren ganau $\frac{h(-p)-1}{2}$ Tripel $(a, b, c) \in \mathbb{N}^3$ mit $p = a^2+b^2+c^2$ und $a > b > c$ („allgemeine Darstellung“).*

(ii) *Unabhängig von der Klassenzahl $h(-p)$ existiert genau ein Zahlenpaar $(a, b) \in \mathbb{N}^2$ mit $p = a^2 + b^2 + b^2 = a^2 + 2b^2$ („spezielle Darstellung“).*

Hieraus ergibt sich eine bemerkenswerte Folgerung:

(6.16) Korollar
Sei $p \equiv 3\,(8)$ eine Primzahl mit $p \geqslant 11$.
Dann sind äquivalent:

1. $h(-p) = 1$

2. *Aus $p = a^2 + b^2 + c^2$ folgt $a^2 = b^2$ oder $a^2 = c^2$ oder $b^2 = c^2$.*

Wir benötigen außerdem folgende Kongruenzaussage:

(6.17) Lemma
Für jede Primzahl $p \equiv 3\,(8)$ mit $p \geqslant 11$ gilt:
Ist $p = a^2 + b^2 + c^2$ eine Darstellung von p mit $(a, b, c) \in \mathbb{N}^3$, so gibt es jeweils einen Primteiler $q \equiv 1\,(4)$ von $a^2 + b^2$, $b^2 + c^2$ und $a^2 + c^2$, falls $a \neq b$ bzw. $b \neq c$ bzw. $a \neq c$. In allen Fällen gilt $\left(\frac{q}{p}\right) = 1$.

Beweis:
Aus Kongruenzgründen müssen a, b und c ungerade sein. OBdA betrachten wir $b^2 + c^2$. Notwendig handelt es sich um eine gerade Zahl, es gilt also

$$b^2 + c^2 = 2n$$

mit $n \in \mathbb{N}$ und $n \equiv 1\,(4)$. Angenommen, es gäbe keinen Primteiler $q \equiv 1\,(4)$ von n. Nach einem Satz von Fermat müßte dann $n = m^2$ mit $m \in \mathbb{N}$ gelten und damit auch

$$N(b + ci) = b^2 + c^2 = 2m^2.$$

Folglich könnte $b + ci$ durch kein Primelement von $\mathbb{Z}[i]$ teilbar sein, das eine Primzahl $q \equiv 1\,(4)$ teilt. Daher erhielte man $b + ci = (1 \pm i)d$ mit einer ungeraden ganzen Zahl d, die nur Primteiler $\equiv 3\,(4)$ besitzt. Hieraus folgte $b = d = c$, was ein Widerspruch zur Voraussetzung wäre.
Daher existiert stets ein Primteiler $q \equiv 1\,(4)$ von $b^2 + c^2$. Es gilt demnach $p = a^2 + qr$, woraus mit dem Quadratischen Reziprozitätsgesetz

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

folgt, q. e. d.

Insgesamt gelangen wir zu folgendem konstruktiven Resultat, bei dem die Abschätzung allerdings unbefriedigend ist:

(6.18) Satz
Für jede Primzahl $p \equiv 3\,(8)$ mit $p \geqslant 11$ gilt:
Es gibt genau $\frac{h(-p)-1}{2}$ Tripel $(a, b, c) \in \mathbb{N}^3$ mit $p = a^2 + b^2 + c^2$ und $a > b > c$. Dabei sind a, b und c ungerade, und es gilt:

(i) Es gibt jeweils einen Primteiler q von $a^2 + b^2$, $b^2 + c^2$ und $a^2 + c^2$ mit $\left(\frac{q}{p}\right) = 1$.

(ii) Ist $q \equiv 1\,(4)$ ein Primteiler von $b^2 + c^2$ und ist $p > \frac{1}{8}c^4 + c^2 + 2$, so gilt $q < \frac{p}{4}$.

Beweis:
Die Aussagen folgen aus den Sätzen (6.14), (6.15) und (6.17). Es bleibt noch die Abschätzung aus (ii) zu beweisen:

Die Zahl $b^2 + c^2$ wird dann am größten, wenn $b = a - 2$ und damit

$$p = a^2 + (a-2)^2 + c^2$$

gilt. In diesem Falle haben wir die quadratische Gleichung $p = 2a^2 - 4a + (4 + c^2)$, aus der wir

$$a = 1 \pm \sqrt{\tfrac{1}{2}(p - c^2 - 2)}$$

erhalten. Es ist nun genau dann $a^2 > \frac{1}{2}p$, wenn

$$a^2 = \tfrac{1}{2}p \pm 2\sqrt{\tfrac{1}{2}(p - c^2 - 2)} - \tfrac{c^2}{2} > \tfrac{1}{2}p$$

gilt, was genau auf die vorausgesetzte Bedingung

$$p > \tfrac{1}{8}c^4 + c^2 + 2 \tag{1}$$

führt. Ist also (1) erfüllt, haben wir sicherlich $\frac{1}{2}p < a^2$ und damit

$$b^2 + c^2 = p - a^2 < p - \tfrac{1}{2}p = \tfrac{1}{2}p.$$

Ist nun $q \equiv 1\,(4)$ ein Primteiler von $b^2 + c^2$, so auch von $\frac{b^2+c^2}{2}$. Damit erhalten wir

$$q \leqslant \tfrac{b^2+c^2}{2} = \tfrac{p-a^2}{2} < \tfrac{1}{2} \cdot \tfrac{1}{2}p = \tfrac{p}{4}$$

als Abschätzung für q, q. e. d.

(6.19) Beispiele

Die in (ii) geforderte Bedingung ist in fast allen Fällen erfüllt. Die einzigen Ausnahmen im Bereich $163 < p < 100000$ sind die sieben Primzahlen $p = 643$, 883, 2347, 3187, 7507, 18043 und 71443.

In allen übrigen Fällen kann man mit diesem Satz kleine quadratische Reste konkret berechnen, wie die folgende Tabelle zeigt. Es ist klar, daß man $q = \pi_p$ nur im Falle $\pi_p \equiv 1\,(4)$ erhalten kann.

p	$b^2 + c^2$	q	$\frac{p+1}{4}$	π_p
$467 = 21^2 + 5^2 + 1^2$	26	13	117	3
$467 = 17^2 + 13^2 + 3^2$	178	89	117	
$467 = 19^2 + 9^2 + 5^2$	106	53	117	
$907 = 27^2 + 13^2 + 3^2$	178	89	227	13
$1259 = 33^2 + 13^2 + 1^2$	170	5	315	3
$1259 = 35^2 + 5^2 + 3^2$	34	17	315	
$2539 = 37^2 + 33^2 + 9^2$	1170	5	635	5
$3067 = 51^2 + 21^2 + 5^2$	466	233	767	13

Ein vollständige Übersicht findet sich in Abschnitt 7.4 des Tabellen-Kapitels.

6.4 Der Fall $p \equiv 3\,(8)$ ohne Klassenzahl-Bedingung

Die erste Arbeit, in welcher für den Fall $p \equiv 3\,(8)$ der Versuch unternommen wird, unabhängig von $h(-p)$ den kleinsten primen quadratischen Rest abzuschätzen, wurde 1976 von S. Chowla und J. Friedlander in [7] veröffentlicht. In der eigentlichen Abschätzung des Rests befindet sich zwar ein Fehler, aber es wird hier zum einzigen Mal in der mir zugänglichen Literatur klar ausgesprochen, daß man auf diesem Wege das Klassenzahl-1-Theorem beweisen könnte. Es heißt dort: „A good enough upper bound might [...] provide another proof of the class number one result." Wir geben eine erweiterte und korrigierte Version wieder:

(6.20) Satz von Chowla-Friedlander

Sei $p \equiv 3\,(8)$ eine Primzahl mit $p \geqslant 11$ und a^2 die kleinste gerade Quadratzahl über p. Dann gibt es ein positives $b \equiv 1\,(4)$ mit $p = a^2 - b$, und es gilt:

(i) Ist q ein Primteiler von b mit $q \equiv 1\,(4)$, so gilt $\left(\frac{q}{p}\right) = 1$ und $q \leqslant 4\sqrt{p-1} + 3$.

(ii) Ist überdies $p \geqslant 277$, so gilt $q \leqslant b \leqslant 4\sqrt{p-1} + 3 < \frac{p+1}{4}$

Beweis:

Es ist klar, daß für $b = a^2 - p$ wegen $a^2 \equiv 0, 4\,(8)$ und $p \equiv 3\,(8)$ stets $b \equiv 1\,(4)$ gilt.

(i) Aus $q \mid b$ folgt $q \cdot r = a^2 - p$ und damit $p = a^2 - q \cdot r$. Daraus ergibt sich mit dem Quadratischen Reziprozitätsgesetz

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

(ii) Die Abschätzung erhält man folgendermaßen: b ist am größten, wenn $p-1$ eine gerade Quadratzahl ist, wenn also

$$p - 1 = (a-2)^2$$

gilt. Hieraus folgt sofort $p - 1 = a^2 - 4a + 4$ und damit $b = a^2 - p = 4a - 5$, woraus sich wegen $a = \sqrt{p-1} + 2$

$$q \leqslant b \leqslant 4\sqrt{p-1} + 3$$

ergibt. Die Ungleichung $4\sqrt{p-1} + 3 < \frac{p+1}{4}$ führt auf die quadratische Ungleichung

$$p^2 - 278p + 377 > 0,$$

die für alle $p \geqslant 277$ erfüllt ist, q. e. d.

Hieraus ergibt sich im Zusammenhang mit dem Satz von Nagell (6.11) folgendes

(6.21) Korollar

Sei $p \equiv 3\,(8)$ eine Primzahl mit $p \geqslant 277$ und a^2 die kleinste gerade Quadratzahl über p.

1. *Ist $b = a^2 - p$ eine Primzahl oder hat b einen Primteiler $q \equiv 1\,(4)$, so gilt $h(-p) > 1$.*
2. *Ist $h(-p) = 1$, so ist $b = a^2 - p$ aus einer geraden Anzahl von Primfaktoren $q \equiv 3\,(4)$ zusammengesetzt.*

(6.22) Beispiele

Mit Hilfe des Satzes von Chowla-Friedlander lassen sich leicht kleine prime quadratische Reste auffinden:

$p = a^2 - b$	$b = q_1 \cdot q_2$	q
$211 = 16^2 - 45$	$45 = 3^2 \cdot 5$	$5 = \pi_{211}$
$491 = 24^2 - 85$	$85 = 5 \cdot 17$	5
$907 = 32^2 - 117$	$117 = 3^2 \cdot 13$	$13 = \pi_{907}$
$1699 = 42^2 - 65$	$65 = 5 \cdot 13$	$5 = \pi_{1699}$
$2267 = 48^2 - 37$	$37 = 1 \cdot 37$	37
$3931 = 64^2 - 165$	$165 = 3 \cdot 5 \cdot 11$	$5 = \pi_{3931}$
$5347 = 76^2 - 429$	$429 = 3 \cdot 11 \cdot 13$	13

Es gibt aber genügend Primzahlen, welche die geforderten Bedingungen nicht erfüllen. Wir geben nur eine kleine Auswahl an:

$p = a^2 - b$	$b = q_1 \cdot q_2$
$331 = 20^2 - 69$	$69 = 3 \cdot 23$
$947 = 32^2 - 77$	$77 = 7 \cdot 11$
$1627 = 44^2 - 309$	$309 = 3 \cdot 103$
$2339 = 50^2 - 161$	$161 = 7 \cdot 23$
$3907 = 64^2 - 189$	$189 = 3^3 \cdot 7$
$5443 = 44^2 - 33$	$33 = 3 \cdot 11$

Wir kommen nun zum dritten Hauptresultat unserer Arbeit. Wie schon bei den Nichtresten versuchen wir, p als Summe von Quadratzahlen darzustellen und den gesuchten Rest als Primteiler der jeweilgen Quadrate zu gewinnen. Anders aber als im vorigen Abschnitt ist hier die Darstellung von p als Summe dreier Quadrate völlig unabhängig von der Klassenzahl $h(-p)$. Dadurch sind wir in die Lage, neue Bedingungen dafür zu formulieren, daß p eine Primzahl mit $h(-p) = 1$ ist.

(6.23) Satz

Für jede Primzahl $p \equiv 3\,(8)$ mit $p \geqslant 11$ gilt:
Es gibt genau ein Paar $(a, b) \in \mathbb{N}^2$ mit $p = a^2 + b^2 + b^2 = a^2 + 2b^2$. Dabei sind a und b ungerade, und es gilt:

(i) *Ist q ein Primteiler von a mit $q \equiv 1, 3\,(8)$, so gilt $\left(\frac{q}{p}\right) = 1$ und $q \leqslant \sqrt{p-2}$.*
Ist q ein Primteiler von b mit $q \equiv 1\,(4)$, so gilt $\left(\frac{q}{p}\right) = 1$ und $q \leqslant \sqrt{\frac{p-1}{2}}$.

(ii) *Ist $r = \frac{a^2+b^2}{2} \notin \mathbb{P}$ und q ein Primteiler von r, so gilt $\left(\frac{q}{p}\right) = 1$ und $q < \frac{p+1}{4}$.*

(iii) *Ist q Primteiler von $(a+b)(a-b)$ mit $q \equiv 1, 7\,(12)$, so gilt $\left(\frac{q}{p}\right) = 1$ und $q < \sqrt{p}$.*

(iv) *Ist q Primteiler von $(2a+b)(2a-b)$ mit $q \equiv 1\,(4)$, so gilt $\left(\frac{q}{p}\right) = 1$ und $q < \frac{11}{4}\sqrt{p}$.*

(v) *Ist q Primteiler von $(a+2b)(a-2b)$ mit $q \equiv 1, 5, 7, 11\,(24)$, so gilt $\left(\frac{q}{p}\right) = 1$ und $q < \frac{5}{2}\sqrt{p}$.*

(vi) *Ist q Primteiler von $(a+4b)(a-4b)$ mit $q \equiv 1, 3\,(8)$, so gilt $\left(\frac{q}{p}\right) = 1$ und $q < 4\sqrt{p}$.*

Beweis:
Nach Satz (6.15) exitistiert die behauptete Darstellung $p = a^2 + 2b^2$ mit $a, b \in \mathbb{N}$ unabhängig von der Klassenzahl $h(-p)$. Aus Kongruenzgründen müssen a und b ungerade sein. Zusammen mit den Grundabschätzungen $p > 2b^2$ und $p > a^2$, also

$$b < \sqrt{\tfrac{p}{2}} < \tfrac{3}{4}\sqrt{p} \quad \text{und} \quad a < \sqrt{p},$$

erhalten wir die folgenden Aussagen:

(i) Ist q ein Primteiler von a, so gilt $p = qt + 2b^2$ und damit

$$\left(\tfrac{q}{p}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{p}{q}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{2b^2+qt}{q}\right) = \left(\tfrac{-2}{q}\right) = 1 \Longleftrightarrow q \equiv 1, 3\,(8).$$

Als Abschätzung erhalten wir $q \leqslant a = \sqrt{p - 2b^2} \leqslant \sqrt{p-2}$.
Ist q ein Primteiler von b, so gilt $p = a^2 + qt$ und damit

$$\left(\tfrac{q}{p}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{p}{q}\right) = \left(\tfrac{-1}{q}\right)\left(\tfrac{a^2+qt}{q}\right) = \left(\tfrac{-1}{q}\right) = 1 \Longleftrightarrow q \equiv 1\,(4).$$

Als Abschätzung ergibt sich $q \leqslant b = \sqrt{\frac{p-a^2}{2}} \leqslant \sqrt{\frac{p-1}{2}}$.

(ii) q ein Primteiler von $r = \frac{a^2+b^2}{2}$, so ist $qt = a^2+b^2$ und damit $p = b^2+qr$. Außerdem gilt $q \equiv 1\,(4)$ nach Lemma (6.17), da $a \neq b$. Hieraus folgt

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

Ist r keine Primzahl, muß $t \geqslant 6$ gelten. Folglich erhalten wir zusammen mit den Grundabschätzungen

$$q \leqslant \frac{a^2+b^2}{t} \leqslant \frac{a^2+b^2}{6} < \frac{\frac{3}{2}p}{6} = \frac{p}{4}.$$

(iii) Ist q ein Primteiler von $(a+b)(a-b) = a^2 - b^2$, so gilt $p = qt + 3b^2$ und damit

$$\left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{3b^2+qt}{q}\right) = \left(\frac{-3}{q}\right) = 1 \Longleftrightarrow q \equiv 1, 7\,(12).$$

Da sowohl $a+b$ als auch $|a-b|$ gerade sind, erhalten wir als Abschätzungen $q \leqslant \frac{a+b}{2} < \frac{\sqrt{p}+\frac{3}{4}\sqrt{p}}{2} < \sqrt{p}$ bzw. $q \leqslant \frac{|a-b|}{2} < \frac{\sqrt{p}}{2} < \frac{1}{2}\sqrt{p}$.

(iv) Ist q ein Primteiler von $(2a+b)(2a-b) = 4a^2 - b^2$, so gilt $p = 9a^2 - qt$ und damit

$$\left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{9a^2-qt}{q}\right) = \left(\frac{-1}{q}\right) = 1 \Longleftrightarrow q \equiv 1\,(4).$$

Als Abschätzungen erhalten wir hier $q \leqslant 2a + b < 2\sqrt{p} + \frac{3}{4}\sqrt{p} < \frac{11}{4}\sqrt{p}$ bzw. $q \leqslant |2a - b| < 2\sqrt{p}$.

(v) Ist q ein Primteiler von $(a+2b)(a-2b) = a^2 - 4b^2$, so gilt $p = 6b^2 + qt$ und damit

$$\left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{6b^2+qt}{q}\right) = \left(\frac{-6}{q}\right) = 1 \Longleftrightarrow q \equiv 1, 5, 7, 11\,(24).$$

Außerdem ergibt sich $q \leqslant a + 2b < \sqrt{p} + \frac{6}{4}\sqrt{p} < \frac{5}{2}\sqrt{p}$ bzw. $q \leqslant |a - 2b| < \frac{6}{4}\sqrt{p}$.

(vi) Ist q ein Primteiler von $(a+4b)(a-4b) = a^2 - 16b^2$, so gilt $p = 18b^2 + qt$ und damit

$$\left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{18b^2+qt}{q}\right) = \left(\frac{-2}{q}\right) = 1 \Longleftrightarrow q \equiv 1, 3\,(8).$$

Wir erhalten $q \leqslant a + 4b < \sqrt{p} + 3\sqrt{p} < 4\sqrt{p}$ bzw. $q \leqslant |a - 4b| < 3\sqrt{p}$ als Abschätzungen, q. e. d.

(6.24) Beispiele

Wir geben einige wenige Beispiele an. Weitere Beispiele kann man leicht aus der Tabelle in Abschnitt 7.5 gewinnen.

$p = a^2 + 2 \cdot b^2$	$x = q_1 \cdot q_2$	q
$251 = 3^2 + 2 \cdot 11^2$	$a = 3$	$3 = \pi_{251}$
$1051 = 13^2 + 2 \cdot 21^2$	$r = 5 \cdot 61$	$5 = \pi_{1051}$
$1171 = 17^2 + 2 \cdot 21^2$	$2a + b = 5 \cdot 11$	$5 = \pi_{1171}$
$2683 = 35^2 + 2 \cdot 27^2$	$a + 4b = 11 \cdot 13$	$11 = \pi_{2683}$
$3547 = 37^2 + 2 \cdot 33^2$	$a + b = 2 \cdot 5 \cdot 7$	$7 = \pi_{3547}$
$5323 = 11^2 + 2 \cdot 51^2$	$a - 2b = -7 \cdot 13$	$7 = \pi_{5323}$
$6043 = 29^2 + 2 \cdot 51^2$	$b = 3 \cdot 17$	$17 = \pi_{6043}$
$9283 = 79^2 + 2 \cdot 39^2$	$a - 4b = -7 \cdot 11$	$11 = \pi_{9283}$

Ist eine der Bedingungen aus Satz (6.23) erfüllt, existiert also ein kleiner quadratischer Rest modulo p, und $h(-p)$ kann nach dem Lemma von Nagell (3.1) nicht 1 sein. Für eine Primzahl p mit $h(-p) = 1$ darf also keine der aufgeführten Bedingungen erfüllt sein, woraus wir das dritte Hauptresultat unserer Arbeit erhalten. (Die Schranken in (iv) bis (vi) sind für einige kleinere Primzahlen nicht kleiner als $\frac{p+1}{4}$, in diesem Fall entnimmt man die Existenz kleiner quadratischer Reste aus der Tabelle in Abschnitt 7.3.)

Hauptsatz 3

Sei $p > 7$ eine Primzahl, $h(-p) = 1$ und $p = a^2 + 2b^2$ mit $a, b \in \mathbb{N}$.
Dann gilt:

(i) $r = \frac{a^2+b^2}{2}$ *ist eine Primzahl mit* $r \equiv 1\,(4)$.

(ii) a *ist nur durch Primzahlen* $q \equiv 5, 7\,(8)$ *teilbar und*
b *ist nur durch Primzahlen* $q \equiv 3\,(4)$ *teilbar.*

(iii) $a + b$ *und* $a - b$ *sind nur durch ungerade Primzahlen* $q \equiv 5, 11\,(12)$ *teilbar.*

(iv) $2a + b$ *ist für* $p > 67$ *nur durch Primzahlen* $q \equiv 3\,(4)$ *teilbar und*
$2a - b$ *ist nur durch Primzahlen* $q \equiv 3\,(4)$ *teilbar.*

(v) $a + 2b$ *ist für* $p > 43$ *nur durch Primzahlen* $q \equiv 13, 17, 19, 23\,(24)$ *teilbar und*
$a - 2b$ *ist für* $p > 19$ *nur durch Primzahlen* $q \equiv 13, 17, 19, 23\,(24)$ *teilbar.*

(vi) $a + 4b$ *ist für* $p > 67$ *nur durch Primzahlen* $q \equiv 5, 7\,(8)$ *teilbar und*
$a - 4b$ *ist nur durch Primzahlen* $q \equiv 5, 7\,(8)$ *teilbar.*

(6.25) Gegenbeispiele

Wie schon eingangs erwähnt, gibt es unter den Primzahlen im Bereich $7 < p < 10^6$ nur zwei Stück, die die Bedingungen des Hauptsatzes erfüllen und für die trotzdem $h(-p) > 1$ ist. In der folgenden Tabelle geben wir außerdem alle „Prüfzahlen“ an:

$p = a^2 + 2 \cdot b^2$	$546067 = 487^2 + 2 \cdot 393^2$	$857707 = 707^2 + 2 \cdot 423^2$
$r = \frac{a^2+b^2}{2}$	195809	339389
$\frac{a^2-b^2}{8}$	$2^2 \cdot 5 \cdot 11 \cdot 47$	$5 \cdot 71 \cdot 113$
$4a^2 - b^2$	$71 \cdot 83 \cdot 1367$	$11 \cdot 167 \cdot 991$
$a^2 - 4b^2$	$-13 \cdot 19 \cdot 23 \cdot 67$	$-139 \cdot 1553$
$a^2 - 16b^2$	$-5 \cdot 7 \cdot 29 \cdot 31 \cdot 71$	$-5 \cdot 197 \cdot 2399$

Es bleibt eine Hoffnung von uns, daß die hier zusammengetragenen Ergebnisse dazu beitragen können, einen elementaren Beweis des Klassenzahl-1-Theorems zu finden.

6.5 Der Versuch von Fjellstedt

Im Jahre 1956 glaubte Lars Fjellstedt, in [14] folgende Aussage bewiesen zu haben:

(6.26) „Fjellstedts Traum“
Es gibt eine Schranke $p_0 > 0$ so, daß für alle Primzahlen $p > p_0$ die Abschätzung

$$\pi_p < 6 \cdot \log p$$

gilt.

Auch wenn diese Aussage möglicherweise richtig ist — für $p > 163$ konnten keine Gegenbeispiele gefunden werden —, befindet sich im Beweis ein schwerer irreparabler Fehler. In den *Mathematical Reviews* hat P. Bateman schlicht bemerkt: „The proof is incorrect“ (MR 17 (1956), S. 1056).

6.6 Der Satz von Salié

Wie schon im vorigen Kapitel angedeutet, läßt sich für den kleinsten quadratischen Rest auch eine untere Schranke angeben. Um den Satz von Hans Salié beweisen zu können, braucht man ein sehr tiefliegendes Resultat aus der analytischen Zahlentheorie, den

(6.27) Satz von Linnik
Es existiert eine Konstante $k > 0$ so, daß für alle natürlichen Zahlen $n \geqslant 2$ in jeder primen Restklasse mod n eine Primzahl $p < n^k$ liegt.

Beweis:
Siehe Kapitel X auf S. 330–370 in Karl Prachars *Primzahlverteilung* [48].

(6.28) Bemerkung
Narkiewicz führt in [44] auf S. 81f. aus, daß man nach dem aktuellen Forschungsstand für die Konstante k jede Zahl größer $5,5$ wählen kann. Außerdem findet sich dort eine Vielzahl von weiteren Literaturhinweisen.

Desweiteren benötigt man ein Lemma, das letztlich aus dem Quadratischen Reziprozitätsgesetz folgt. Ein Beweis findet sich bei David Cox in [10] auf S. 15f.:

(6.29) Lemma

Für verschiedene ungerade Primzahlen p, q gilt:

1. $\left(\frac{p}{q}\right) = 1 \Longleftrightarrow q \equiv \pm a_i^2 \,(4p)$ *für ungerade ganze Zahlen* a_i *mit* $i = 1, \ldots, \frac{1}{4}\varphi(4p)$.
2. $\left(\frac{p}{q}\right) = -1 \Longleftrightarrow q \equiv \pm a_i \,(4p)$ *für ungerade ganze Zahlen* a_i *mit* $i = 1, \ldots, \frac{1}{4}\varphi(4p)$.

Nun zum Hauptergebnis dieses Abschnitts:

(6.30) Satz von Salié für quadratische Reste

Es gibt eine Konstante $c > 0$ so, daß für unendlich viele Primzahlen p

$$\pi_p > c \cdot \log p$$

gilt.

Beweis:

Es sei $p_1, p_2, \ldots$ die Folge der Primzahlen in ihrer natürlichen Anordnung. Für jede natürliche Zahl n betrachten wir die Menge $\mathbb{P}_n$ aller Primzahlen q mit

$$p_n = \pi_q.$$

Für jedes $q \in \mathbb{P}_n$ gilt dann also

$$\begin{cases} \left(\frac{p_i}{q}\right) = -1 \quad \text{für } i = 1, \ldots, n-1 \\ \left(\frac{p_n}{q}\right) = 1 \end{cases} \tag{1}$$

Nach Lemma (6.29) wird eine Primzahl q durch jede Bedingung von (1) in genau $\frac{1}{2}\varphi(4p_i)$ verschiedene prime Kongruenzklassen modulo $4p_i$ eingeteilt. Dabei sind sämtliche n Bedingungen voneinander unabhängig. Setzt man nun

$$m = 4 \prod_{n=1}^{n} p_i, \tag{2}$$

so wird jedes $q \in \mathbb{P}_n$ durch genau eine der $\frac{1}{2^n}\varphi(m)$ primen Kongruenzklassen (mod m) festgelegt. In dieser primen Kongruenzklasse liegen nun alle der (nach Dirichlet unendlich vielen) Primzahlen aus $\mathbb{P}_n$, von denen q_n die kleinste sei. Nach dem Satz von Linnik (6.27) gibt es eine Konstante $k > 0$ mit

$$q_n < m^k,$$

also mit

$$\tfrac{1}{k} \log q_n < \log m.$$

Nach (2) gilt nun $\log m = \log 4 + \vartheta(p_n)$ mit der Tschebyscheffschen Theta-Funktion. Nach den Tschebyscheffschen Sätzen gilt außerdem $\vartheta(x) < 2x - \log 4$ für hinreichend große x, siehe z. B. [45] auf S. 267–273. Damit erhalten wir

$$\log m < 2p_n$$

für alle hinreichend große n. Insgesamt ergibt sich $\frac{1}{k} \log q_n < \log m < 2p_n$ und damit

$$\tfrac{1}{2k} \log q_n < p_n = \pi_{q_n}$$

für alle hinreichend großen n. Die Primzahlen q_n erfüllen daher die Behauptung, wenn man $c = \frac{1}{2k}$ setzt, q. e. d.

(6.31) Bemerkung
Die Konstante c kann man momentan als $\frac{1}{12}$, nicht aber größer als $\frac{1}{11}$ wählen, wie man aus den Bemerkungen von Narkiewicz in [44] auf S. 81f. über den Satz von Linnik schließen kann.

6.7 Analytische Abschätzungen

Zur Information zitieren wir zum Schluß zwei Sätze aus der analytischen Zahlentheorie, die beide starke, aber nicht-effektive Aussagen machen.

(6.32) Satz von Linnik-Vinogradov (1966)
Für jedes $\varepsilon > 0$ gibt es eine Konstante $c(\varepsilon) > 0$ so, daß

$$\pi_p < c(\varepsilon) \cdot p^{1/4+\varepsilon}$$

für alle Primzahlen p gilt.

Der Beweis findet sich in [32].

(6.33) Satz von Pintz (1977)
Für jedes $\varepsilon > 0$ gibt es eine Schranke $p(\varepsilon) > 0$ so, daß

$$\pi_p < p^{1/4+\varepsilon}$$

für alle Primzahlen $p > p(\varepsilon)$ gilt.

Der Beweis findet sich in [46].

7. Tabellen

7.1 Kleinste quadratische Nichtreste ψ_p

In der folgenden Tabelle sind für alle Primzahlen $3 \leqslant p < 2000$ die kleinsten ungeraden primen quadratischen Nichtreste ψ_p gemäß der Definition im 5. Kapitel angeführt:

$\psi_{3} = 5$	$\psi_{173} = 3$	$\psi_{397} = 5$	$\psi_{641} = 3$	$\psi_{887} = 5$	$\psi_{1163} = 5$	$\psi_{1451} = 7$	$\psi_{1721} = 3$
$\psi_{5} = 3$	$\psi_{179} = 7$	$\psi_{401} = 3$	$\psi_{643} = 3$	$\psi_{907} = 3$	$\psi_{1171} = 3$	$\psi_{1453} = 5$	$\psi_{1723} = 3$
$\psi_{7} = 3$	$\psi_{181} = 7$	$\psi_{409} = 7$	$\psi_{647} = 5$	$\psi_{911} = 7$	$\psi_{1181} = 3$	$\psi_{1459} = 3$	$\psi_{1733} = 3$
$\psi_{11} = 7$	$\psi_{191} = 7$	$\psi_{419} = 11$	$\psi_{653} = 3$	$\psi_{919} = 3$	$\psi_{1187} = 5$	$\psi_{1471} = 3$	$\psi_{1741} = 7$
$\psi_{13} = 5$	$\psi_{193} = 5$	$\psi_{421} = 13$	$\psi_{659} = 7$	$\psi_{929} = 3$	$\psi_{1193} = 3$	$\psi_{1481} = 3$	$\psi_{1747} = 3$
$\psi_{17} = 3$	$\psi_{197} = 3$	$\psi_{431} = 7$	$\psi_{661} = 7$	$\psi_{937} = 5$	$\psi_{1201} = 11$	$\psi_{1483} = 3$	$\psi_{1753} = 5$
$\psi_{19} = 3$	$\psi_{199} = 3$	$\psi_{433} = 5$	$\psi_{673} = 5$	$\psi_{941} = 3$	$\psi_{1213} = 5$	$\psi_{1487} = 5$	$\psi_{1759} = 3$
$\psi_{23} = 5$	$\psi_{211} = 3$	$\psi_{439} = 3$	$\psi_{677} = 3$	$\psi_{947} = 5$	$\psi_{1217} = 3$	$\psi_{1489} = 7$	$\psi_{1777} = 5$
$\psi_{29} = 3$	$\psi_{223} = 3$	$\psi_{443} = 5$	$\psi_{683} = 5$	$\psi_{953} = 3$	$\psi_{1223} = 5$	$\psi_{1493} = 3$	$\psi_{1783} = 3$
$\psi_{31} = 3$	$\psi_{227} = 5$	$\psi_{449} = 3$	$\psi_{691} = 3$	$\psi_{967} = 3$	$\psi_{1229} = 3$	$\psi_{1499} = 7$	$\psi_{1787} = 5$
$\psi_{37} = 5$	$\psi_{229} = 7$	$\psi_{457} = 5$	$\psi_{701} = 3$	$\psi_{971} = 11$	$\psi_{1231} = 3$	$\psi_{1511} = 11$	$\psi_{1789} = 11$
$\psi_{41} = 3$	$\psi_{233} = 3$	$\psi_{461} = 3$	$\psi_{709} = 13$	$\psi_{977} = 3$	$\psi_{1237} = 5$	$\psi_{1523} = 5$	$\psi_{1801} = 11$
$\psi_{43} = 3$	$\psi_{239} = 7$	$\psi_{463} = 3$	$\psi_{719} = 11$	$\psi_{983} = 5$	$\psi_{1249} = 7$	$\psi_{1531} = 3$	$\psi_{1811} = 19$
$\psi_{47} = 5$	$\psi_{241} = 7$	$\psi_{467} = 5$	$\psi_{727} = 3$	$\psi_{991} = 3$	$\psi_{1259} = 11$	$\psi_{1543} = 3$	$\psi_{1823} = 5$
$\psi_{53} = 3$	$\psi_{251} = 11$	$\psi_{479} = 13$	$\psi_{733} = 5$	$\psi_{997} = 5$	$\psi_{1277} = 3$	$\psi_{1549} = 13$	$\psi_{1831} = 3$
$\psi_{59} = 11$	$\psi_{257} = 3$	$\psi_{487} = 3$	$\psi_{739} = 3$	$\psi_{1009} = 11$	$\psi_{1279} = 3$	$\psi_{1553} = 3$	$\psi_{1847} = 5$
$\psi_{61} = 7$	$\psi_{263} = 5$	$\psi_{491} = 7$	$\psi_{743} = 5$	$\psi_{1013} = 3$	$\psi_{1283} = 5$	$\psi_{1559} = 17$	$\psi_{1861} = 7$
$\psi_{67} = 3$	$\psi_{269} = 3$	$\psi_{499} = 3$	$\psi_{751} = 3$	$\psi_{1019} = 7$	$\psi_{1289} = 3$	$\psi_{1567} = 3$	$\psi_{1867} = 3$
$\psi_{71} = 7$	$\psi_{271} = 3$	$\psi_{503} = 5$	$\psi_{757} = 5$	$\psi_{1021} = 7$	$\psi_{1291} = 3$	$\psi_{1571} = 11$	$\psi_{1871} = 7$
$\psi_{73} = 5$	$\psi_{277} = 5$	$\psi_{509} = 3$	$\psi_{761} = 3$	$\psi_{1031} = 7$	$\psi_{1297} = 5$	$\psi_{1579} = 3$	$\psi_{1873} = 5$
$\psi_{79} = 3$	$\psi_{281} = 3$	$\psi_{521} = 3$	$\psi_{769} = 7$	$\psi_{1033} = 5$	$\psi_{1301} = 3$	$\psi_{1583} = 5$	$\psi_{1877} = 3$
$\psi_{83} = 5$	$\psi_{283} = 3$	$\psi_{523} = 3$	$\psi_{773} = 3$	$\psi_{1039} = 3$	$\psi_{1303} = 3$	$\psi_{1597} = 5$	$\psi_{1879} = 3$
$\psi_{89} = 3$	$\psi_{293} = 3$	$\psi_{541} = 11$	$\psi_{787} = 3$	$\psi_{1049} = 3$	$\psi_{1307} = 5$	$\psi_{1601} = 3$	$\psi_{1889} = 3$
$\psi_{97} = 5$	$\psi_{307} = 3$	$\psi_{547} = 3$	$\psi_{797} = 3$	$\psi_{1051} = 3$	$\psi_{1319} = 13$	$\psi_{1607} = 5$	$\psi_{1901} = 3$
$\psi_{101} = 3$	$\psi_{311} = 11$	$\psi_{557} = 3$	$\psi_{809} = 3$	$\psi_{1061} = 3$	$\psi_{1321} = 7$	$\psi_{1609} = 7$	$\psi_{1907} = 5$
$\psi_{103} = 3$	$\psi_{313} = 5$	$\psi_{563} = 5$	$\psi_{811} = 3$	$\psi_{1063} = 3$	$\psi_{1327} = 3$	$\psi_{1613} = 3$	$\psi_{1913} = 3$
$\psi_{107} = 5$	$\psi_{317} = 3$	$\psi_{569} = 3$	$\psi_{821} = 3$	$\psi_{1069} = 7$	$\psi_{1361} = 3$	$\psi_{1619} = 7$	$\psi_{1931} = 13$
$\psi_{109} = 11$	$\psi_{331} = 3$	$\psi_{571} = 3$	$\psi_{823} = 3$	$\psi_{1087} = 3$	$\psi_{1367} = 5$	$\psi_{1621} = 17$	$\psi_{1933} = 5$
$\psi_{113} = 3$	$\psi_{337} = 5$	$\psi_{577} = 5$	$\psi_{827} = 5$	$\psi_{1091} = 17$	$\psi_{1373} = 3$	$\psi_{1627} = 3$	$\psi_{1949} = 3$
$\psi_{127} = 3$	$\psi_{347} = 5$	$\psi_{587} = 5$	$\psi_{829} = 7$	$\psi_{1093} = 5$	$\psi_{1381} = 11$	$\psi_{1637} = 3$	$\psi_{1951} = 3$
$\psi_{131} = 17$	$\psi_{349} = 7$	$\psi_{593} = 3$	$\psi_{839} = 11$	$\psi_{1097} = 3$	$\psi_{1399} = 3$	$\psi_{1657} = 5$	$\psi_{1973} = 3$
$\psi_{137} = 3$	$\psi_{353} = 3$	$\psi_{599} = 7$	$\psi_{853} = 5$	$\psi_{1103} = 5$	$\psi_{1409} = 3$	$\psi_{1663} = 3$	$\psi_{1979} = 17$
$\psi_{139} = 3$	$\psi_{359} = 7$	$\psi_{601} = 7$	$\psi_{857} = 3$	$\psi_{1109} = 3$	$\psi_{1423} = 3$	$\psi_{1667} = 5$	$\psi_{1987} = 3$
$\psi_{149} = 3$	$\psi_{367} = 3$	$\psi_{607} = 3$	$\psi_{859} = 3$	$\psi_{1117} = 5$	$\psi_{1427} = 5$	$\psi_{1669} = 7$	$\psi_{1993} = 5$
$\psi_{151} = 3$	$\psi_{373} = 5$	$\psi_{613} = 5$	$\psi_{863} = 5$	$\psi_{1123} = 3$	$\psi_{1429} = 11$	$\psi_{1693} = 5$	$\psi_{1997} = 3$
$\psi_{157} = 5$	$\psi_{379} = 3$	$\psi_{617} = 3$	$\psi_{877} = 5$	$\psi_{1129} = 11$	$\psi_{1433} = 3$	$\psi_{1697} = 3$	$\psi_{1999} = 3$
$\psi_{163} = 3$	$\psi_{383} = 5$	$\psi_{619} = 3$	$\psi_{881} = 3$	$\psi_{1151} = 13$	$\psi_{1439} = 7$	$\psi_{1699} = 3$	
$\psi_{167} = 5$	$\psi_{389} = 3$	$\psi_{631} = 3$	$\psi_{883} = 3$	$\psi_{1153} = 5$	$\psi_{1447} = 3$	$\psi_{1709} = 3$	

7.2 Kleinste quadratische Nichtreste ψ_p im Fall $p \equiv 3\,(8)$

Im folgenden geben wir von allen Primzahlen $p \equiv 3\,(8)$ mit $11 < p < 500.000$ diejenigen an, für die $\psi_p \geqslant \sqrt{p}$ gilt. Die Berechnung erfolgte mit einem MATHEMATICA-Programm:

```
For[p=13, p<500000, p++,
    If[PrimeQ[p] && Mod[p,8]==3,
      For[q=3, q<p^2, q++,
          If[PrimeQ[q],
            If[JacobiSymbol[q,p]==-1,
               If[q>=p^(1/2),
                  Print["$psi_{",p,"}="q,"$"]
                 ,];
               Break[]
            ,]
          ]
       ,]
    ]
```

$\psi_{59} = 11$
$\psi_{131} = 17$

7.3 Kleinste quadratische Reste π_p

In der folgenden Tabelle sind für alle Primzahlen $3 \leqslant p < 2750$ die kleinsten ungeraden primen quadratischen Reste π_p gemäß der Definition im 6. Kapitel angeführt:

$\pi_{3} = 7$	$\pi_{239} = 3$	$\pi_{557} = 7$	$\pi_{881} = 5$	$\pi_{1231} = 5$	$\pi_{1601} = 5$	$\pi_{1997} = 7$	$\pi_{2377} = 3$
$\pi_{5} = 11$	$\pi_{241} = 3$	$\pi_{563} = 3$	$\pi_{883} = 13$	$\pi_{1237} = 3$	$\pi_{1607} = 3$	$\pi_{1999} = 5$	$\pi_{2381} = 5$
$\pi_{7} = 11$	$\pi_{251} = 3$	$\pi_{569} = 5$	$\pi_{887} = 3$	$\pi_{1249} = 3$	$\pi_{1609} = 3$	$\pi_{2003} = 3$	$\pi_{2383} = 7$
$\pi_{11} = 3$	$\pi_{257} = 11$	$\pi_{571} = 5$	$\pi_{907} = 13$	$\pi_{1259} = 3$	$\pi_{1613} = 13$	$\pi_{2011} = 5$	$\pi_{2389} = 3$
$\pi_{13} = 3$	$\pi_{263} = 3$	$\pi_{577} = 3$	$\pi_{911} = 3$	$\pi_{1277} = 11$	$\pi_{1619} = 3$	$\pi_{2017} = 3$	$\pi_{2393} = 13$
$\pi_{17} = 13$	$\pi_{269} = 5$	$\pi_{587} = 3$	$\pi_{919} = 5$	$\pi_{1279} = 5$	$\pi_{1621} = 3$	$\pi_{2027} = 3$	$\pi_{2399} = 3$
$\pi_{19} = 5$	$\pi_{271} = 5$	$\pi_{593} = 17$	$\pi_{929} = 5$	$\pi_{1283} = 3$	$\pi_{1627} = 7$	$\pi_{2029} = 3$	$\pi_{2411} = 3$
$\pi_{23} = 3$	$\pi_{277} = 3$	$\pi_{599} = 3$	$\pi_{937} = 3$	$\pi_{1289} = 5$	$\pi_{1637} = 11$	$\pi_{2039} = 3$	$\pi_{2417} = 7$
$\pi_{29} = 5$	$\pi_{281} = 5$	$\pi_{601} = 3$	$\pi_{941} = 5$	$\pi_{1291} = 5$	$\pi_{1657} = 3$	$\pi_{2053} = 3$	$\pi_{2423} = 3$
$\pi_{31} = 5$	$\pi_{283} = 7$	$\pi_{607} = 7$	$\pi_{947} = 3$	$\pi_{1297} = 3$	$\pi_{1663} = 11$	$\pi_{2063} = 3$	$\pi_{2437} = 3$
$\pi_{37} = 3$	$\pi_{293} = 17$	$\pi_{613} = 3$	$\pi_{953} = 7$	$\pi_{1301} = 5$	$\pi_{1667} = 3$	$\pi_{2069} = 5$	$\pi_{2441} = 5$
$\pi_{41} = 5$	$\pi_{307} = 7$	$\pi_{617} = 7$	$\pi_{967} = 11$	$\pi_{1303} = 13$	$\pi_{1669} = 3$	$\pi_{2081} = 5$	$\pi_{2447} = 3$
$\pi_{43} = 11$	$\pi_{311} = 3$	$\pi_{619} = 5$	$\pi_{971} = 3$	$\pi_{1307} = 3$	$\pi_{1693} = 3$	$\pi_{2083} = 13$	$\pi_{2459} = 3$
$\pi_{47} = 3$	$\pi_{313} = 3$	$\pi_{631} = 5$	$\pi_{977} = 7$	$\pi_{1319} = 3$	$\pi_{1697} = 11$	$\pi_{2087} = 3$	$\pi_{2467} = 7$
$\pi_{53} = 7$	$\pi_{317} = 7$	$\pi_{641} = 5$	$\pi_{983} = 3$	$\pi_{1321} = 3$	$\pi_{1699} = 5$	$\pi_{2089} = 3$	$\pi_{2473} = 3$
$\pi_{59} = 3$	$\pi_{331} = 5$	$\pi_{643} = 7$	$\pi_{991} = 5$	$\pi_{1327} = 11$	$\pi_{1709} = 5$	$\pi_{2099} = 3$	$\pi_{2477} = 19$
$\pi_{61} = 3$	$\pi_{337} = 3$	$\pi_{647} = 3$	$\pi_{997} = 3$	$\pi_{1361} = 5$	$\pi_{1721} = 5$	$\pi_{2111} = 3$	$\pi_{2503} = 11$
$\pi_{67} = 17$	$\pi_{347} = 3$	$\pi_{653} = 7$	$\pi_{1009} = 3$	$\pi_{1367} = 3$	$\pi_{1723} = 11$	$\pi_{2113} = 3$	$\pi_{2521} = 3$
$\pi_{71} = 3$	$\pi_{349} = 3$	$\pi_{659} = 3$	$\pi_{1013} = 11$	$\pi_{1373} = 7$	$\pi_{1733} = 7$	$\pi_{2129} = 5$	$\pi_{2531} = 3$
$\pi_{73} = 3$	$\pi_{353} = 11$	$\pi_{661} = 3$	$\pi_{1019} = 3$	$\pi_{1381} = 3$	$\pi_{1741} = 3$	$\pi_{2131} = 5$	$\pi_{2539} = 5$
$\pi_{79} = 5$	$\pi_{359} = 3$	$\pi_{673} = 3$	$\pi_{1021} = 3$	$\pi_{1399} = 5$	$\pi_{1747} = 17$	$\pi_{2137} = 3$	$\pi_{2543} = 3$
$\pi_{83} = 3$	$\pi_{367} = 7$	$\pi_{677} = 13$	$\pi_{1031} = 3$	$\pi_{1409} = 5$	$\pi_{1753} = 3$	$\pi_{2141} = 5$	$\pi_{2549} = 5$
$\pi_{89} = 5$	$\pi_{373} = 3$	$\pi_{683} = 3$	$\pi_{1033} = 3$	$\pi_{1423} = 23$	$\pi_{1759} = 5$	$\pi_{2143} = 17$	$\pi_{2551} = 5$
$\pi_{97} = 3$	$\pi_{379} = 5$	$\pi_{691} = 5$	$\pi_{1039} = 5$	$\pi_{1427} = 3$	$\pi_{1777} = 3$	$\pi_{2153} = 7$	$\pi_{2557} = 3$
$\pi_{101} = 5$	$\pi_{383} = 3$	$\pi_{701} = 5$	$\pi_{1049} = 5$	$\pi_{1429} = 3$	$\pi_{1783} = 7$	$\pi_{2161} = 3$	$\pi_{2579} = 3$
$\pi_{103} = 7$	$\pi_{389} = 5$	$\pi_{709} = 3$	$\pi_{1051} = 5$	$\pi_{1433} = 11$	$\pi_{1787} = 3$	$\pi_{2179} = 5$	$\pi_{2591} = 3$
$\pi_{107} = 3$	$\pi_{397} = 3$	$\pi_{719} = 3$	$\pi_{1061} = 5$	$\pi_{1439} = 3$	$\pi_{1789} = 3$	$\pi_{2203} = 7$	$\pi_{2593} = 3$
$\pi_{109} = 3$	$\pi_{401} = 5$	$\pi_{727} = 7$	$\pi_{1063} = 7$	$\pi_{1447} = 7$	$\pi_{1801} = 3$	$\pi_{2207} = 3$	$\pi_{2609} = 5$
$\pi_{113} = 7$	$\pi_{409} = 3$	$\pi_{733} = 3$	$\pi_{1069} = 3$	$\pi_{1451} = 3$	$\pi_{1811} = 3$	$\pi_{2213} = 7$	$\pi_{2617} = 3$
$\pi_{127} = 11$	$\pi_{419} = 3$	$\pi_{739} = 5$	$\pi_{1087} = 17$	$\pi_{1453} = 3$	$\pi_{1823} = 3$	$\pi_{2221} = 3$	$\pi_{2621} = 5$
$\pi_{131} = 3$	$\pi_{421} = 3$	$\pi_{743} = 3$	$\pi_{1091} = 3$	$\pi_{1459} = 5$	$\pi_{1831} = 5$	$\pi_{2237} = 7$	$\pi_{2633} = 7$
$\pi_{137} = 7$	$\pi_{431} = 3$	$\pi_{751} = 5$	$\pi_{1093} = 3$	$\pi_{1471} = 5$	$\pi_{1847} = 3$	$\pi_{2239} = 5$	$\pi_{2647} = 11$
$\pi_{139} = 5$	$\pi_{433} = 3$	$\pi_{757} = 3$	$\pi_{1097} = 17$	$\pi_{1481} = 5$	$\pi_{1861} = 3$	$\pi_{2243} = 3$	$\pi_{2657} = 7$
$\pi_{149} = 5$	$\pi_{439} = 5$	$\pi_{761} = 5$	$\pi_{1103} = 3$	$\pi_{1483} = 7$	$\pi_{1867} = 7$	$\pi_{2251} = 5$	$\pi_{2659} = 5$
$\pi_{151} = 5$	$\pi_{443} = 3$	$\pi_{769} = 3$	$\pi_{1109} = 5$	$\pi_{1487} = 3$	$\pi_{1871} = 3$	$\pi_{2267} = 3$	$\pi_{2663} = 3$
$\pi_{157} = 3$	$\pi_{449} = 5$	$\pi_{773} = 11$	$\pi_{1117} = 3$	$\pi_{1489} = 3$	$\pi_{1873} = 3$	$\pi_{2269} = 3$	$\pi_{2671} = 5$
$\pi_{163} = 41$	$\pi_{457} = 3$	$\pi_{787} = 7$	$\pi_{1123} = 7$	$\pi_{1493} = 7$	$\pi_{1877} = 7$	$\pi_{2273} = 31$	$\pi_{2677} = 3$
$\pi_{167} = 3$	$\pi_{461} = 5$	$\pi_{797} = 11$	$\pi_{1129} = 3$	$\pi_{1499} = 3$	$\pi_{1879} = 5$	$\pi_{2281} = 3$	$\pi_{2683} = 11$
$\pi_{173} = 13$	$\pi_{463} = 17$	$\pi_{809} = 5$	$\pi_{1151} = 3$	$\pi_{1511} = 3$	$\pi_{1889} = 5$	$\pi_{2287} = 7$	$\pi_{2687} = 3$
$\pi_{179} = 3$	$\pi_{467} = 3$	$\pi_{811} = 5$	$\pi_{1153} = 3$	$\pi_{1523} = 3$	$\pi_{1901} = 5$	$\pi_{2293} = 3$	$\pi_{2689} = 3$
$\pi_{181} = 3$	$\pi_{479} = 3$	$\pi_{821} = 5$	$\pi_{1163} = 3$	$\pi_{1531} = 5$	$\pi_{1907} = 3$	$\pi_{2297} = 7$	$\pi_{2693} = 11$
$\pi_{191} = 3$	$\pi_{487} = 19$	$\pi_{823} = 13$	$\pi_{1171} = 5$	$\pi_{1543} = 7$	$\pi_{1913} = 7$	$\pi_{2309} = 5$	$\pi_{2699} = 3$
$\pi_{193} = 3$	$\pi_{491} = 3$	$\pi_{827} = 3$	$\pi_{1181} = 5$	$\pi_{1549} = 3$	$\pi_{1931} = 3$	$\pi_{2311} = 5$	$\pi_{2707} = 7$
$\pi_{197} = 7$	$\pi_{499} = 5$	$\pi_{829} = 3$	$\pi_{1187} = 3$	$\pi_{1553} = 23$	$\pi_{1933} = 3$	$\pi_{2333} = 7$	$\pi_{2711} = 3$
$\pi_{199} = 5$	$\pi_{503} = 3$	$\pi_{839} = 3$	$\pi_{1193} = 11$	$\pi_{1559} = 3$	$\pi_{1949} = 5$	$\pi_{2339} = 3$	$\pi_{2713} = 3$
$\pi_{211} = 5$	$\pi_{509} = 5$	$\pi_{853} = 3$	$\pi_{1201} = 3$	$\pi_{1567} = 7$	$\pi_{1951} = 5$	$\pi_{2341} = 3$	$\pi_{2719} = 5$
$\pi_{223} = 7$	$\pi_{521} = 5$	$\pi_{857} = 13$	$\pi_{1213} = 3$	$\pi_{1571} = 3$	$\pi_{1973} = 11$	$\pi_{2347} = 17$	$\pi_{2729} = 5$
$\pi_{227} = 3$	$\pi_{523} = 7$	$\pi_{859} = 5$	$\pi_{1217} = 19$	$\pi_{1579} = 5$	$\pi_{1979} = 3$	$\pi_{2351} = 3$	$\pi_{2731} = 5$
$\pi_{229} = 3$	$\pi_{541} = 3$	$\pi_{863} = 3$	$\pi_{1223} = 3$	$\pi_{1583} = 3$	$\pi_{1987} = 7$	$\pi_{2357} = 11$	$\pi_{2741} = 5$
$\pi_{233} = 7$	$\pi_{547} = 11$	$\pi_{877} = 3$	$\pi_{1229} = 5$	$\pi_{1597} = 3$	$\pi_{1993} = 3$	$\pi_{2371} = 5$	$\pi_{2749} = 3$

7.4 Die Darstellungen $p = a^2 + b^2 + c^2$ gemäß Satz (6.18)

In der folgenden Tabelle sind für alle Primzahlen $p \equiv 3\,(8)$ mit $11 \leqslant p < 5000$ die Darstellungen $p = a^2 + b^2 + c^2$ mit $a > b > c$ und $p > \frac{1}{8}c^4 + c^2 + 2$ aufgeführt. Nach Satz (6.18) gilt für jeden Primteiler $q \equiv 1\,(4)$ von $b^2 + c^2$ stets $\left(\frac{q}{p}\right) = 1$ und $q < \frac{p+1}{4}$.

$59 = 7^2 + 3^2 + 1^2$
$83 = 7^2 + 5^2 + 3^2$
$107 = 9^2 + 5^2 + 1^2$
$131 = 11^2 + 3^2 + 1^2$
$139 = 9^2 + 7^2 + 3^2$
$179 = 13^2 + 3^2 + 1^2$
$179 = 11^2 + 7^2 + 3^2$
$211 = 11^2 + 9^2 + 3^2$
$227 = 13^2 + 7^2 + 3^2$
$227 = 11^2 + 9^2 + 5^2$
$251 = 15^2 + 5^2 + 1^2$
$283 = 15^2 + 7^2 + 3^2$
$307 = 15^2 + 9^2 + 1^2$
$331 = 15^2 + 9^2 + 5^2$
$347 = 15^2 + 11^2 + 1^2$
$347 = 17^2 + 7^2 + 3^2$
$379 = 17^2 + 9^2 + 3^2$
$419 = 19^2 + 7^2 + 3^2$
$419 = 15^2 + 13^2 + 5^2$
$419 = 17^2 + 9^2 + 7^2$
$443 = 19^2 + 9^2 + 1^2$
$443 = 15^2 + 13^2 + 7^2$
$467 = 21^2 + 5^2 + 1^2$
$467 = 17^2 + 13^2 + 3^2$
$467 = 19^2 + 9^2 + 5^2$
$491 = 21^2 + 7^2 + 1^2$
$491 = 19^2 + 11^2 + 3^2$
$491 = 19^2 + 9^2 + 7^2$
$499 = 21^2 + 7^2 + 3^2$
$523 = 21^2 + 9^2 + 1^2$
$523 = 17^2 + 15^2 + 3^2$
$547 = 21^2 + 9^2 + 5^2$
$563 = 21^2 + 11^2 + 1^2$
$563 = 23^2 + 5^2 + 3^2$
$563 = 17^2 + 15^2 + 7^2$
$571 = 21^2 + 11^2 + 3^2$
$571 = 21^2 + 9^2 + 7^2$
$587 = 19^2 + 15^2 + 1^2$
$587 = 23^2 + 7^2 + 3^2$
$587 = 21^2 + 11^2 + 5^2$
$619 = 23^2 + 9^2 + 3^2$
$659 = 25^2 + 5^2 + 3^2$
$659 = 23^2 + 9^2 + 7^2$
$683 = 25^2 + 7^2 + 3^2$
$691 = 21^2 + 15^2 + 5^2$
$739 = 27^2 + 3^2 + 1^2$
$739 = 21^2 + 17^2 + 3^2$
$787 = 27^2 + 7^2 + 3^2$
$811 = 27^2 + 9^2 + 1^2$
$811 = 21^2 + 19^2 + 3^2$
$827 = 23^2 + 17^2 + 3^2$
$827 = 21^2 + 19^2 + 5^2$
$859 = 27^2 + 11^2 + 3^2$
$859 = 27^2 + 9^2 + 7^2$
$907 = 27^2 + 13^2 + 3^2$
$947 = 29^2 + 9^2 + 5^2$
$947 = 27^2 + 13^2 + 7^2$
$971 = 31^2 + 3^2 + 1^2$
$971 = 29^2 + 11^2 + 3^2$
$971 = 29^2 + 9^2 + 7^2$
$971 = 23^2 + 19^2 + 9^2$
$1019 = 27^2 + 17^2 + 1^2$
$1019 = 31^2 + 7^2 + 3^2$
$1019 = 23^2 + 21^2 + 7^2$
$1051 = 31^2 + 9^2 + 3^2$
$1051 = 23^2 + 21^2 + 9^2$
$1091 = 27^2 + 19^2 + 1^2$
$1091 = 31^2 + 11^2 + 3^2$
$1091 = 29^2 + 15^2 + 5^2$
$1091 = 31^2 + 9^2 + 7^2$
$1091 = 29^2 + 13^2 + 9^2$
$1123 = 33^2 + 5^2 + 3^2$
$1163 = 25^2 + 23^2 + 3^2$
$1163 = 33^2 + 7^2 + 5^2$
$1163 = 31^2 + 11^2 + 9^2$
$1171 = 33^2 + 9^2 + 1^2$
$1171 = 27^2 + 19^2 + 9^2$
$1187 = 31^2 + 15^2 + 1^2$
$1259 = 33^2 + 13^2 + 1^2$
$1259 = 35^2 + 5^2 + 3^2$
$1259 = 33^2 + 11^2 + 7^2$
$1283 = 29^2 + 21^2 + 1^2$
$1283 = 35^2 + 7^2 + 3^2$
$1283 = 33^2 + 13^2 + 5^2$
$1283 = 29^2 + 19^2 + 9^2$
$1291 = 29^2 + 21^2 + 3^2$
$1291 = 33^2 + 11^2 + 9^2$
$1307 = 35^2 + 9^2 + 1^2$
$1307 = 29^2 + 21^2 + 5^2$
$1307 = 33^2 + 13^2 + 7^2$
$1427 = 37^2 + 7^2 + 3^2$
$1427 = 31^2 + 21^2 + 5^2$
$1427 = 33^2 + 17^2 + 7^2$
$1427 = 35^2 + 11^2 + 9^2$
$1451 = 37^2 + 9^2 + 1^2$
$1451 = 31^2 + 21^2 + 7^2$
$1451 = 29^2 + 23^2 + 9^2$
$1459 = 37^2 + 9^2 + 3^2$
$1459 = 33^2 + 17^2 + 9^2$
$1483 = 31^2 + 21^2 + 9^2$
$1499 = 37^2 + 11^2 + 3^2$
$1499 = 37^2 + 9^2 + 7^2$
$1523 = 35^2 + 17^2 + 3^2$
$1531 = 39^2 + 3^2 + 1^2$
$1531 = 35^2 + 15^2 + 9^2$
$1571 = 39^2 + 7^2 + 1^2$
$1571 = 37^2 + 11^2 + 9^2$
$1579 = 39^2 + 7^2 + 3^2$
$1579 = 33^2 + 21^2 + 7^2$
$1619 = 33^2 + 23^2 + 1^2$
$1619 = 37^2 + 15^2 + 5^2$
$1619 = 29^2 + 27^2 + 7^2$
$1619 = 37^2 + 13^2 + 9^2$
$1627 = 33^2 + 23^2 + 3^2$
$1627 = 39^2 + 9^2 + 5^2$
$1667 = 35^2 + 21^2 + 1^2$
$1667 = 37^2 + 17^2 + 3^2$
$1667 = 39^2 + 11^2 + 5^2$
$1667 = 33^2 + 23^2 + 7^2$
$1667 = 35^2 + 19^2 + 9^2$
$1699 = 39^2 + 13^2 + 3^2$
$1699 = 33^2 + 23^2 + 9^2$
$1723 = 33^2 + 25^2 + 3^2$
$1723 = 39^2 + 11^2 + 9^2$
$1747 = 39^2 + 15^2 + 1^2$
$1747 = 35^2 + 21^2 + 9^2$
$1787 = 41^2 + 9^2 + 5^2$
$1811 = 39^2 + 17^2 + 1^2$
$1811 = 41^2 + 11^2 + 3^2$
$1811 = 41^2 + 9^2 + 7^2$
$1811 = 37^2 + 19^2 + 9^2$
$1867 = 33^2 + 27^2 + 7^2$
$1907 = 41^2 + 15^2 + 1^2$
$1907 = 43^2 + 7^2 + 3^2$
$1907 = 39^2 + 19^2 + 5^2$
$1931 = 43^2 + 9^2 + 1^2$
$1931 = 41^2 + 15^2 + 5^2$
$1931 = 39^2 + 19^2 + 7^2$
$1931 = 41^2 + 13^2 + 9^2$
$1979 = 43^2 + 11^2 + 3^2$
$1979 = 35^2 + 27^2 + 5^2$
$1979 = 43^2 + 9^2 + 7^2$
$1979 = 37^2 + 23^2 + 9^2$
$1987 = 39^2 + 21^2 + 5^2$
$1987 = 41^2 + 15^2 + 9^2$
$2003 = 37^2 + 25^2 + 3^2$
$2003 = 35^2 + 27^2 + 7^2$
$2003 = 39^2 + 19^2 + 11^2$
$2011 = 39^2 + 21^2 + 7^2$
$2011 = 33^2 + 29^2 + 9^2$
$2027 = 43^2 + 13^2 + 3^2$
$2027 = 41^2 + 15^2 + 11^2$
$2083 = 45^2 + 7^2 + 3^2$
$2083 = 39^2 + 21^2 + 11^2$
$2099 = 37^2 + 27^2 + 1^2$
$2099 = 45^2 + 7^2 + 5^2$
$2099 = 39^2 + 23^2 + 7^2$
$2099 = 43^2 + 13^2 + 9^2$
$2131 = 41^2 + 21^2 + 3^2$
$2131 = 45^2 + 9^2 + 5^2$
$2131 = 39^2 + 23^2 + 9^2$
$2179 = 37^2 + 27^2 + 9^2$
$2203 = 45^2 + 13^2 + 3^2$
$2203 = 41^2 + 21^2 + 9^2$
$2243 = 47^2 + 5^2 + 3^2$
$2243 = 45^2 + 13^2 + 7^2$
$2243 = 41^2 + 21^2 + 11^2$
$2251 = 45^2 + 15^2 + 1^2$
$2267 = 47^2 + 7^2 + 3^2$
$2267 = 35^2 + 31^2 + 9^2$
$2267 = 39^2 + 25^2 + 11^2$
$2339 = 47^2 + 11^2 + 3^2$
$2339 = 45^2 + 17^2 + 5^2$
$2339 = 47^2 + 9^2 + 7^2$
$2371 = 39^2 + 29^2 + 3^2$
$2371 = 43^2 + 21^2 + 9^2$
$2371 = 45^2 + 15^2 + 11^2$
$2411 = 49^2 + 3^2 + 1^2$
$2411 = 45^2 + 19^2 + 5^2$
$2411 = 39^2 + 29^2 + 7^2$
$2411 = 47^2 + 11^2 + 9^2$
$2411 = 43^2 + 21^2 + 11^2$
$2459 = 37^2 + 33^2 + 1^2$
$2459 = 49^2 + 7^2 + 3^2$
$2459 = 47^2 + 15^2 + 5^2$
$2459 = 41^2 + 27^2 + 7^2$
$2459 = 47^2 + 13^2 + 9^2$
$2467 = 45^2 + 21^2 + 1^2$
$2467 = 37^2 + 33^2 + 3^2$
$2467 = 45^2 + 19^2 + 9^2$
$2531 = 49^2 + 11^2 + 3^2$
$2531 = 49^2 + 9^2 + 7^2$

$2531 = 41^2 + 27^2 + 11^2$
$2539 = 37^2 + 33^2 + 9^2$
$2579 = 43^2 + 27^2 + 1^2$
$2579 = 49^2 + 13^2 + 3^2$
$2579 = 45^2 + 23^2 + 5^2$
$2579 = 47^2 + 17^2 + 9^2$
$2579 = 37^2 + 33^2 + 11^2$
$2659 = 51^2 + 7^2 + 3^2$
$2659 = 39^2 + 33^2 + 7^2$
$2659 = 43^2 + 27^2 + 9^2$
$2683 = 51^2 + 9^2 + 1^2$
$2699 = 49^2 + 17^2 + 3^2$
$2699 = 47^2 + 21^2 + 7^2$
$2699 = 43^2 + 27^2 + 11^2$
$2707 = 51^2 + 9^2 + 5^2$
$2707 = 49^2 + 15^2 + 9^2$
$2731 = 51^2 + 11^2 + 3^2$
$2731 = 51^2 + 9^2 + 7^2$
$2731 = 47^2 + 21^2 + 9^2$
$2731 = 39^2 + 33^2 + 11^2$
$2803 = 45^2 + 27^2 + 7^2$
$2803 = 51^2 + 11^2 + 9^2$
$2819 = 53^2 + 3^2 + 1^2$
$2819 = 43^2 + 31^2 + 3^2$
$2819 = 51^2 + 13^2 + 7^2$
$2819 = 47^2 + 23^2 + 9^2$
$2843 = 49^2 + 21^2 + 1^2$
$2843 = 53^2 + 5^2 + 3^2$
$2843 = 49^2 + 19^2 + 9^2$
$2851 = 49^2 + 21^2 + 3^2$
$2851 = 51^2 + 15^2 + 5^2$
$2851 = 51^2 + 13^2 + 9^2$
$2939 = 47^2 + 27^2 + 1^2$
$2939 = 53^2 + 11^2 + 3^2$
$2939 = 53^2 + 9^2 + 7^2$
$2963 = 51^2 + 19^2 + 1^2$
$2963 = 47^2 + 27^2 + 5^2$
$2963 = 49^2 + 21^2 + 11^2$
$2971 = 51^2 + 19^2 + 3^2$
$2971 = 51^2 + 17^2 + 9^2$
$3011 = 45^2 + 31^2 + 5^2$
$3011 = 51^2 + 19^2 + 7^2$
$3011 = 53^2 + 11^2 + 9^2$
$3011 = 51^2 + 17^2 + 11^2$
$3019 = 47^2 + 27^2 + 9^2$
$3067 = 51^2 + 21^2 + 5^2$
$3067 = 45^2 + 31^2 + 9^2$
$3083 = 55^2 + 7^2 + 3^2$
$3083 = 53^2 + 15^2 + 7^2$
$3083 = 51^2 + 19^2 + 11^2$
$3163 = 45^2 + 33^2 + 7^2$
$3163 = 51^2 + 21^2 + 11^2$
$3203 = 41^2 + 39^2 + 1^2$
$3203 = 55^2 + 13^2 + 3^2$
$3251 = 55^2 + 15^2 + 1^2$
$3251 = 49^2 + 29^2 + 3^2$
$3251 = 51^2 + 25^2 + 5^2$
$3251 = 41^2 + 39^2 + 7^2$
$3251 = 53^2 + 19^2 + 9^2$
$3251 = 51^2 + 23^2 + 11^2$
$3259 = 57^2 + 3^2 + 1^2$
$3259 = 55^2 + 15^2 + 3^2$
$3299 = 57^2 + 7^2 + 1^2$
$3299 = 55^2 + 15^2 + 7^2$
$3299 = 43^2 + 37^2 + 9^2$
$3307 = 57^2 + 7^2 + 3^2$
$3307 = 51^2 + 25^2 + 9^2$
$3323 = 55^2 + 17^2 + 3^2$
$3323 = 57^2 + 7^2 + 5^2$
$3323 = 49^2 + 29^2 + 9^2$
$3323 = 41^2 + 39^2 + 11^2$
$3331 = 57^2 + 9^2 + 1^2$
$3331 = 55^2 + 15^2 + 9^2$
$3347 = 53^2 + 23^2 + 3^2$
$3347 = 47^2 + 33^2 + 7^2$
$3347 = 51^2 + 25^2 + 11^2$
$3371 = 57^2 + 11^2 + 1^2$
$3371 = 49^2 + 31^2 + 3^2$
$3371 = 55^2 + 15^2 + 11^2$
$3467 = 55^2 + 21^2 + 1^2$
$3467 = 51^2 + 29^2 + 5^2$
$3467 = 57^2 + 13^2 + 7^2$
$3467 = 55^2 + 19^2 + 9^2$
$3491 = 59^2 + 3^2 + 1^2$
$3491 = 55^2 + 21^2 + 5^2$
$3491 = 51^2 + 29^2 + 7^2$
$3491 = 43^2 + 39^2 + 11^2$
$3499 = 49^2 + 33^2 + 3^2$
$3499 = 57^2 + 15^2 + 5^2$
$3499 = 57^2 + 13^2 + 9^2$
$3539 = 57^2 + 17^2 + 1^2$
$3539 = 59^2 + 7^2 + 3^2$
$3539 = 49^2 + 33^2 + 7^2$
$3539 = 57^2 + 13^2 + 11^2$
$3547 = 45^2 + 39^2 + 1^2$
$3547 = 57^2 + 17^2 + 3^2$
$3547 = 55^2 + 21^2 + 9^2$
$3571 = 59^2 + 9^2 + 3^2$
$3571 = 45^2 + 39^2 + 5^2$
$3571 = 49^2 + 33^2 + 9^2$
$3643 = 51^2 + 31^2 + 9^2$
$3659 = 59^2 + 13^2 + 3^2$
$3659 = 57^2 + 19^2 + 7^2$
$3659 = 47^2 + 37^2 + 9^2$
$3659 = 57^2 + 17^2 + 11^2$
$3691 = 57^2 + 21^2 + 1^2$
$3691 = 57^2 + 19^2 + 9^2$
$3739 = 47^2 + 39^2 + 3^2$
$3739 = 57^2 + 21^2 + 7^2$
$3779 = 57^2 + 23^2 + 1^2$
$3779 = 61^2 + 7^2 + 3^2$
$3779 = 55^2 + 27^2 + 5^2$
$3779 = 47^2 + 39^2 + 7^2$
$3779 = 57^2 + 19^2 + 13^2$
$3803 = 61^2 + 9^2 + 1^2$
$3803 = 57^2 + 23^2 + 5^2$
$3803 = 55^2 + 27^2 + 7^2$
$3851 = 61^2 + 11^2 + 3^2$
$3851 = 51^2 + 35^2 + 5^2$
$3851 = 61^2 + 9^2 + 7^2$
$3851 = 59^2 + 17^2 + 9^2$
$3851 = 47^2 + 39^2 + 11^2$
$3907 = 53^2 + 33^2 + 3^2$
$3907 = 51^2 + 35^2 + 9^2$
$3923 = 59^2 + 21^2 + 1^2$
$3923 = 53^2 + 33^2 + 5^2$
$3923 = 57^2 + 25^2 + 7^2$
$3923 = 61^2 + 11^2 + 9^2$
$3923 = 55^2 + 27^2 + 13^2$
$3931 = 59^2 + 21^2 + 3^2$
$3947 = 61^2 + 15^2 + 1^2$
$3947 = 59^2 + 21^2 + 5^2$
$3947 = 53^2 + 33^2 + 7^2$
$3947 = 55^2 + 29^2 + 9^2$
$3947 = 51^2 + 35^2 + 11^2$
$3947 = 57^2 + 23^2 + 13^2$
$4003 = 63^2 + 5^2 + 3^2$
$4003 = 57^2 + 27^2 + 5^2$
$4003 = 59^2 + 21^2 + 9^2$
$4019 = 63^2 + 7^2 + 1^2$
$4019 = 61^2 + 17^2 + 3^2$
$4019 = 51^2 + 37^2 + 7^2$
$4019 = 53^2 + 33^2 + 11^2$
$4027 = 63^2 + 7^2 + 3^2$
$4027 = 57^2 + 27^2 + 7^2$
$4027 = 61^2 + 15^2 + 9^2$
$4051 = 63^2 + 9^2 + 1^2$
$4051 = 51^2 + 37^2 + 9^2$
$4091 = 63^2 + 11^2 + 1^2$
$4091 = 61^2 + 19^2 + 3^2$
$4091 = 61^2 + 17^2 + 9^2$
$4091 = 51^2 + 37^2 + 11^2$
$4091 = 59^2 + 21^2 + 13^2$
$4099 = 63^2 + 11^2 + 3^2$
$4099 = 63^2 + 9^2 + 7^2$
$4099 = 57^2 + 27^2 + 11^2$
$4139 = 63^2 + 13^2 + 1^2$
$4139 = 55^2 + 33^2 + 5^2$
$4139 = 63^2 + 11^2 + 7^2$
$4139 = 47^2 + 43^2 + 9^2$
$4139 = 51^2 + 37^2 + 13^2$
$4211 = 59^2 + 27^2 + 1^2$
$4211 = 61^2 + 21^2 + 7^2$
$4211 = 57^2 + 29^2 + 11^2$
$4219 = 59^2 + 27^2 + 3^2$
$4219 = 63^2 + 15^2 + 5^2$
$4219 = 63^2 + 13^2 + 9^2$
$4243 = 47^2 + 45^2 + 3^2$
$4243 = 63^2 + 15^2 + 7^2$
$4243 = 61^2 + 21^2 + 9^2$
$4243 = 51^2 + 39^2 + 11^2$
$4259 = 63^2 + 17^2 + 1^2$
$4259 = 65^2 + 5^2 + 3^2$
$4259 = 47^2 + 45^2 + 5^2$
$4259 = 59^2 + 27^2 + 7^2$
$4259 = 53^2 + 37^2 + 9^2$
$4259 = 63^2 + 13^2 + 11^2$
$4259 = 57^2 + 29^2 + 13^2$
$4283 = 51^2 + 41^2 + 1^2$
$4283 = 65^2 + 7^2 + 3^2$
$4283 = 63^2 + 17^2 + 5^2$
$4283 = 47^2 + 45^2 + 7^2$
$4283 = 61^2 + 21^2 + 11^2$
$4283 = 55^2 + 33^2 + 13^2$
$4339 = 57^2 + 33^2 + 1^2$
$4339 = 63^2 + 19^2 + 3^2$
$4339 = 63^2 + 17^2 + 9^2$
$4363 = 57^2 + 33^2 + 5^2$
$4363 = 51^2 + 41^2 + 9^2$
$4363 = 63^2 + 15^2 + 13^2$
$4451 = 65^2 + 15^2 + 1^2$
$4451 = 59^2 + 31^2 + 3^2$
$4451 = 49^2 + 45^2 + 5^2$
$4451 = 63^2 + 19^2 + 11^2$
$4451 = 51^2 + 41^2 + 13^2$
$4483 = 57^2 + 35^2 + 3^2$
$4507 = 63^2 + 23^2 + 3^2$
$4507 = 49^2 + 45^2 + 9^2$
$4507 = 57^2 + 33^2 + 13^2$
$4523 = 67^2 + 5^2 + 3^2$
$4523 = 63^2 + 23^2 + 5^2$
$4523 = 57^2 + 35^2 + 7^2$
$4523 = 59^2 + 31^2 + 9^2$
$4547 = 55^2 + 39^2 + 1^2$
$4547 = 67^2 + 7^2 + 3^2$
$4547 = 63^2 + 23^2 + 7^2$
$4547 = 49^2 + 45^2 + 11^2$
$4603 = 63^2 + 25^2 + 3^2$
$4643 = 57^2 + 37^2 + 5^2$
$4643 = 63^2 + 25^2 + 7^2$
$4643 = 61^2 + 29^2 + 9^2$
$4643 = 57^2 + 35^2 + 13^2$
$4651 = 51^2 + 45^2 + 5^2$
$4651 = 59^2 + 33^2 + 9^2$
$4691 = 61^2 + 31^2 + 3^2$
$4691 = 65^2 + 21^2 + 5^2$
$4691 = 67^2 + 11^2 + 9^2$
$4691 = 59^2 + 33^2 + 11^2$
$4723 = 67^2 + 15^2 + 3^2$
$4723 = 63^2 + 27^2 + 5^2$
$4787 = 69^2 + 5^2 + 1^2$
$4787 = 67^2 + 17^2 + 3^2$
$4787 = 59^2 + 35^2 + 9^2$
$4787 = 65^2 + 21^2 + 11^2$
$4787 = 57^2 + 37^2 + 13^2$
$4931 = 69^2 + 13^2 + 1^2$
$4931 = 69^2 + 11^2 + 7^2$
$4931 = 67^2 + 19^2 + 9^2$
$4931 = 63^2 + 29^2 + 11^2$
$4987 = 69^2 + 15^2 + 1^2$

7.5 Die Darstellungen $p = a^2 + 2b^2$

In der folgenden Tabelle sind für alle Primzahlen $p \equiv 3\,(8)$ mit $11 \leqslant p < 14500$ die Darstellungen $p = a^2 + 2b^2$ aufgeführt.

$11 = 3^2 + 2 \cdot 1^2$
$19 = 1^2 + 2 \cdot 3^2$
$43 = 5^2 + 2 \cdot 3^2$
$59 = 3^2 + 2 \cdot 5^2$
$67 = 7^2 + 2 \cdot 3^2$
$83 = 9^2 + 2 \cdot 1^2$
$107 = 3^2 + 2 \cdot 7^2$
$131 = 9^2 + 2 \cdot 5^2$
$139 = 11^2 + 2 \cdot 3^2$
$163 = 1^2 + 2 \cdot 9^2$
$179 = 9^2 + 2 \cdot 7^2$
$211 = 7^2 + 2 \cdot 9^2$
$227 = 15^2 + 2 \cdot 1^2$
$251 = 3^2 + 2 \cdot 11^2$
$283 = 11^2 + 2 \cdot 9^2$
$307 = 17^2 + 2 \cdot 3^2$
$331 = 13^2 + 2 \cdot 9^2$
$347 = 3^2 + 2 \cdot 13^2$
$379 = 19^2 + 2 \cdot 3^2$
$419 = 9^2 + 2 \cdot 13^2$
$443 = 21^2 + 2 \cdot 1^2$
$467 = 15^2 + 2 \cdot 11^2$
$491 = 21^2 + 2 \cdot 5^2$
$499 = 7^2 + 2 \cdot 15^2$
$523 = 19^2 + 2 \cdot 9^2$
$547 = 23^2 + 2 \cdot 3^2$
$563 = 15^2 + 2 \cdot 13^2$
$571 = 11^2 + 2 \cdot 15^2$
$587 = 3^2 + 2 \cdot 17^2$
$619 = 13^2 + 2 \cdot 15^2$
$643 = 25^2 + 2 \cdot 3^2$
$659 = 9^2 + 2 \cdot 17^2$
$683 = 21^2 + 2 \cdot 11^2$
$691 = 23^2 + 2 \cdot 9^2$
$739 = 17^2 + 2 \cdot 15^2$
$787 = 25^2 + 2 \cdot 9^2$
$811 = 19^2 + 2 \cdot 15^2$
$827 = 27^2 + 2 \cdot 7^2$
$859 = 29^2 + 2 \cdot 3^2$
$883 = 1^2 + 2 \cdot 21^2$
$907 = 5^2 + 2 \cdot 21^2$
$947 = 15^2 + 2 \cdot 19^2$
$971 = 27^2 + 2 \cdot 11^2$
$1019 = 21^2 + 2 \cdot 17^2$
$1051 = 13^2 + 2 \cdot 21^2$
$1091 = 33^2 + 2 \cdot 1^2$
$1123 = 31^2 + 2 \cdot 9^2$
$1163 = 21^2 + 2 \cdot 19^2$
$1171 = 17^2 + 2 \cdot 21^2$
$1187 = 33^2 + 2 \cdot 7^2$
$1259 = 3^2 + 2 \cdot 25^2$
$1283 = 15^2 + 2 \cdot 23^2$
$1291 = 29^2 + 2 \cdot 15^2$
$1307 = 27^2 + 2 \cdot 17^2$
$1427 = 33^2 + 2 \cdot 13^2$
$1451 = 27^2 + 2 \cdot 19^2$
$1459 = 1^2 + 2 \cdot 27^2$
$1483 = 5^2 + 2 \cdot 27^2$
$1499 = 21^2 + 2 \cdot 23^2$
$1523 = 39^2 + 2 \cdot 1^2$
$1531 = 37^2 + 2 \cdot 9^2$
$1571 = 39^2 + 2 \cdot 5^2$
$1579 = 11^2 + 2 \cdot 27^2$
$1619 = 39^2 + 2 \cdot 7^2$
$1627 = 13^2 + 2 \cdot 27^2$
$1667 = 33^2 + 2 \cdot 17^2$
$1699 = 41^2 + 2 \cdot 3^2$
$1723 = 29^2 + 2 \cdot 21^2$
$1747 = 17^2 + 2 \cdot 27^2$
$1787 = 27^2 + 2 \cdot 23^2$
$1811 = 33^2 + 2 \cdot 19^2$
$1867 = 43^2 + 2 \cdot 3^2$
$1907 = 15^2 + 2 \cdot 29^2$
$1931 = 3^2 + 2 \cdot 31^2$
$1979 = 27^2 + 2 \cdot 25^2$
$1987 = 23^2 + 2 \cdot 27^2$
$2003 = 9^2 + 2 \cdot 31^2$
$2011 = 43^2 + 2 \cdot 9^2$
$2027 = 45^2 + 2 \cdot 1^2$
$2083 = 25^2 + 2 \cdot 27^2$
$2099 = 39^2 + 2 \cdot 17^2$
$2131 = 41^2 + 2 \cdot 15^2$
$2179 = 1^2 + 2 \cdot 33^2$
$2203 = 5^2 + 2 \cdot 33^2$
$2243 = 39^2 + 2 \cdot 19^2$
$2251 = 37^2 + 2 \cdot 21^2$
$2267 = 45^2 + 2 \cdot 11^2$
$2339 = 33^2 + 2 \cdot 25^2$
$2347 = 13^2 + 2 \cdot 33^2$
$2371 = 47^2 + 2 \cdot 9^2$
$2411 = 27^2 + 2 \cdot 29^2$
$2459 = 3^2 + 2 \cdot 35^2$
$2467 = 17^2 + 2 \cdot 33^2$
$2531 = 9^2 + 2 \cdot 35^2$
$2539 = 19^2 + 2 \cdot 33^2$
$2579 = 39^2 + 2 \cdot 23^2$
$2659 = 47^2 + 2 \cdot 15^2$
$2683 = 35^2 + 2 \cdot 27^2$
$2699 = 51^2 + 2 \cdot 7^2$
$2707 = 23^2 + 2 \cdot 33^2$
$2731 = 43^2 + 2 \cdot 21^2$
$2803 = 25^2 + 2 \cdot 33^2$
$2819 = 9^2 + 2 \cdot 37^2$
$2843 = 51^2 + 2 \cdot 11^2$
$2851 = 49^2 + 2 \cdot 15^2$
$2939 = 51^2 + 2 \cdot 13^2$
$2963 = 15^2 + 2 \cdot 37^2$
$2971 = 53^2 + 2 \cdot 9^2$
$3011 = 33^2 + 2 \cdot 31^2$
$3019 = 29^2 + 2 \cdot 33^2$
$3067 = 5^2 + 2 \cdot 39^2$
$3083 = 45^2 + 2 \cdot 23^2$
$3163 = 11^2 + 2 \cdot 39^2$
$3187 = 55^2 + 2 \cdot 9^2$
$3203 = 39^2 + 2 \cdot 29^2$
$3251 = 57^2 + 2 \cdot 1^2$
$3259 = 53^2 + 2 \cdot 15^2$
$3299 = 57^2 + 2 \cdot 5^2$
$3307 = 43^2 + 2 \cdot 27^2$
$3323 = 51^2 + 2 \cdot 19^2$
$3331 = 17^2 + 2 \cdot 39^2$
$3347 = 57^2 + 2 \cdot 7^2$
$3371 = 3^2 + 2 \cdot 41^2$
$3467 = 27^2 + 2 \cdot 37^2$
$3491 = 57^2 + 2 \cdot 11^2$
$3499 = 59^2 + 2 \cdot 3^2$
$3539 = 33^2 + 2 \cdot 35^2$
$3547 = 37^2 + 2 \cdot 33^2$
$3571 = 23^2 + 2 \cdot 39^2$
$3643 = 59^2 + 2 \cdot 9^2$
$3659 = 51^2 + 2 \cdot 23^2$
$3691 = 53^2 + 2 \cdot 21^2$
$3739 = 61^2 + 2 \cdot 3^2$
$3779 = 9^2 + 2 \cdot 43^2$
$3803 = 21^2 + 2 \cdot 41^2$
$3851 = 51^2 + 2 \cdot 25^2$
$3907 = 55^2 + 2 \cdot 21^2$
$3923 = 15^2 + 2 \cdot 43^2$
$3931 = 59^2 + 2 \cdot 15^2$
$3947 = 45^2 + 2 \cdot 31^2$
$4003 = 31^2 + 2 \cdot 39^2$
$4019 = 63^2 + 2 \cdot 5^2$
$4027 = 43^2 + 2 \cdot 33^2$
$4051 = 1^2 + 2 \cdot 45^2$
$4091 = 27^2 + 2 \cdot 41^2$
$4099 = 7^2 + 2 \cdot 45^2$
$4139 = 21^2 + 2 \cdot 43^2$
$4211 = 63^2 + 2 \cdot 11^2$
$4219 = 13^2 + 2 \cdot 45^2$
$4243 = 65^2 + 2 \cdot 3^2$
$4259 = 39^2 + 2 \cdot 37^2$
$4283 = 51^2 + 2 \cdot 29^2$
$4339 = 17^2 + 2 \cdot 45^2$
$4363 = 59^2 + 2 \cdot 21^2$
$4451 = 33^2 + 2 \cdot 41^2$
$4483 = 55^2 + 2 \cdot 27^2$
$4507 = 67^2 + 2 \cdot 3^2$
$4523 = 51^2 + 2 \cdot 31^2$
$4547 = 63^2 + 2 \cdot 17^2$
$4603 = 61^2 + 2 \cdot 21^2$
$4643 = 15^2 + 2 \cdot 47^2$
$4651 = 67^2 + 2 \cdot 9^2$
$4691 = 63^2 + 2 \cdot 19^2$
$4723 = 41^2 + 2 \cdot 39^2$
$4787 = 33^2 + 2 \cdot 43^2$
$4931 = 57^2 + 2 \cdot 29^2$
$4987 = 53^2 + 2 \cdot 33^2$
$5003 = 69^2 + 2 \cdot 11^2$
$5011 = 31^2 + 2 \cdot 45^2$
$5051 = 51^2 + 2 \cdot 35^2$
$5059 = 71^2 + 2 \cdot 3^2$
$5099 = 69^2 + 2 \cdot 13^2$
$5107 = 65^2 + 2 \cdot 21^2$
$5147 = 27^2 + 2 \cdot 47^2$
$5171 = 57^2 + 2 \cdot 31^2$
$5179 = 61^2 + 2 \cdot 27^2$
$5227 = 5^2 + 2 \cdot 51^2$
$5323 = 11^2 + 2 \cdot 51^2$
$5347 = 73^2 + 2 \cdot 3^2$
$5387 = 45^2 + 2 \cdot 41^2$
$5419 = 37^2 + 2 \cdot 45^2$
$5443 = 49^2 + 2 \cdot 39^2$
$5483 = 69^2 + 2 \cdot 19^2$
$5507 = 33^2 + 2 \cdot 47^2$
$5531 = 27^2 + 2 \cdot 49^2$
$5563 = 19^2 + 2 \cdot 51^2$
$5651 = 63^2 + 2 \cdot 29^2$
$5659 = 59^2 + 2 \cdot 33^2$
$5683 = 65^2 + 2 \cdot 27^2$
$5779 = 73^2 + 2 \cdot 15^2$
$5827 = 25^2 + 2 \cdot 51^2$
$5843 = 15^2 + 2 \cdot 53^2$
$5851 = 53^2 + 2 \cdot 39^2$
$5867 = 75^2 + 2 \cdot 11^2$
$5923 = 71^2 + 2 \cdot 21^2$
$5939 = 39^2 + 2 \cdot 47^2$
$5987 = 57^2 + 2 \cdot 37^2$
$6011 = 69^2 + 2 \cdot 25^2$
$6043 = 29^2 + 2 \cdot 51^2$
$6067 = 55^2 + 2 \cdot 39^2$

$6091 = 77^2 + 2 \cdot 9^2$
$6131 = 9^2 + 2 \cdot 55^2$
$6163 = 31^2 + 2 \cdot 51^2$
$6203 = 75^2 + 2 \cdot 17^2$
$6211 = 73^2 + 2 \cdot 21^2$
$6299 = 51^2 + 2 \cdot 43^2$
$6323 = 39^2 + 2 \cdot 49^2$
$6379 = 77^2 + 2 \cdot 15^2$
$6427 = 35^2 + 2 \cdot 51^2$
$6451 = 49^2 + 2 \cdot 45^2$
$6491 = 21^2 + 2 \cdot 55^2$
$6547 = 7^2 + 2 \cdot 57^2$
$6563 = 81^2 + 2 \cdot 1^2$
$6571 = 37^2 + 2 \cdot 51^2$
$6619 = 11^2 + 2 \cdot 57^2$
$6659 = 81^2 + 2 \cdot 7^2$
$6691 = 79^2 + 2 \cdot 15^2$
$6763 = 61^2 + 2 \cdot 39^2$
$6779 = 27^2 + 2 \cdot 55^2$
$6803 = 81^2 + 2 \cdot 11^2$
$6827 = 45^2 + 2 \cdot 49^2$
$6883 = 41^2 + 2 \cdot 51^2$
$6899 = 81^2 + 2 \cdot 13^2$
$6907 = 83^2 + 2 \cdot 3^2$
$6947 = 57^2 + 2 \cdot 43^2$
$6971 = 3^2 + 2 \cdot 59^2$
$7019 = 51^2 + 2 \cdot 47^2$
$7027 = 23^2 + 2 \cdot 57^2$
$7043 = 9^2 + 2 \cdot 59^2$
$7187 = 15^2 + 2 \cdot 59^2$
$7211 = 69^2 + 2 \cdot 35^2$
$7219 = 71^2 + 2 \cdot 33^2$
$7243 = 85^2 + 2 \cdot 3^2$
$7283 = 81^2 + 2 \cdot 19^2$
$7307 = 75^2 + 2 \cdot 29^2$
$7331 = 63^2 + 2 \cdot 41^2$
$7411 = 47^2 + 2 \cdot 51^2$
$7451 = 3^2 + 2 \cdot 61^2$
$7459 = 31^2 + 2 \cdot 57^2$
$7499 = 69^2 + 2 \cdot 37^2$
$7507 = 73^2 + 2 \cdot 33^2$
$7523 = 9^2 + 2 \cdot 61^2$
$7547 = 75^2 + 2 \cdot 31^2$
$7603 = 49^2 + 2 \cdot 51^2$
$7643 = 45^2 + 2 \cdot 53^2$
$7691 = 27^2 + 2 \cdot 59^2$
$7699 = 79^2 + 2 \cdot 27^2$
$7723 = 35^2 + 2 \cdot 57^2$
$7867 = 37^2 + 2 \cdot 57^2$
$7883 = 21^2 + 2 \cdot 61^2$
$7907 = 87^2 + 2 \cdot 13^2$
$7963 = 5^2 + 2 \cdot 63^2$
$8011 = 53^2 + 2 \cdot 51^2$
$8059 = 11^2 + 2 \cdot 63^2$
$8123 = 69^2 + 2 \cdot 41^2$
$8147 = 87^2 + 2 \cdot 17^2$
$8171 = 27^2 + 2 \cdot 61^2$
$8179 = 41^2 + 2 \cdot 57^2$
$8219 = 51^2 + 2 \cdot 53^2$
$8243 = 81^2 + 2 \cdot 29^2$
$8291 = 87^2 + 2 \cdot 19^2$
$8363 = 75^2 + 2 \cdot 37^2$
$8387 = 63^2 + 2 \cdot 47^2$
$8419 = 79^2 + 2 \cdot 33^2$
$8443 = 91^2 + 2 \cdot 9^2$
$8467 = 23^2 + 2 \cdot 63^2$
$8539 = 67^2 + 2 \cdot 45^2$
$8563 = 25^2 + 2 \cdot 63^2$
$8627 = 87^2 + 2 \cdot 23^2$
$8699 = 93^2 + 2 \cdot 5^2$
$8707 = 47^2 + 2 \cdot 57^2$
$8731 = 91^2 + 2 \cdot 15^2$
$8747 = 93^2 + 2 \cdot 7^2$
$8779 = 29^2 + 2 \cdot 63^2$
$8803 = 89^2 + 2 \cdot 21^2$
$8819 = 87^2 + 2 \cdot 25^2$
$8867 = 57^2 + 2 \cdot 53^2$
$8923 = 61^2 + 2 \cdot 51^2$
$8963 = 39^2 + 2 \cdot 61^2$
$8971 = 77^2 + 2 \cdot 39^2$
$9011 = 81^2 + 2 \cdot 35^2$
$9043 = 95^2 + 2 \cdot 3^2$
$9059 = 9^2 + 2 \cdot 67^2$
$9067 = 83^2 + 2 \cdot 33^2$
$9091 = 71^2 + 2 \cdot 45^2$
$9187 = 95^2 + 2 \cdot 9^2$
$9203 = 15^2 + 2 \cdot 67^2$
$9227 = 93^2 + 2 \cdot 17^2$
$9283 = 79^2 + 2 \cdot 39^2$
$9323 = 75^2 + 2 \cdot 43^2$
$9371 = 93^2 + 2 \cdot 19^2$
$9403 = 85^2 + 2 \cdot 33^2$
$9419 = 21^2 + 2 \cdot 67^2$
$9467 = 45^2 + 2 \cdot 61^2$
$9491 = 87^2 + 2 \cdot 31^2$
$9539 = 33^2 + 2 \cdot 65^2$
$9547 = 5^2 + 2 \cdot 69^2$
$9587 = 63^2 + 2 \cdot 53^2$
$9619 = 41^2 + 2 \cdot 63^2$
$9643 = 11^2 + 2 \cdot 69^2$
$9739 = 91^2 + 2 \cdot 27^2$
$9787 = 43^2 + 2 \cdot 63^2$
$9803 = 99^2 + 2 \cdot 1^2$
$9811 = 17^2 + 2 \cdot 69^2$
$9851 = 99^2 + 2 \cdot 5^2$
$9859 = 97^2 + 2 \cdot 15^2$
$9883 = 19^2 + 2 \cdot 69^2$
$9907 = 95^2 + 2 \cdot 21^2$
$9923 = 81^2 + 2 \cdot 41^2$
$9931 = 83^2 + 2 \cdot 39^2$
$10067 = 33^2 + 2 \cdot 67^2$
$10091 = 3^2 + 2 \cdot 71^2$
$10099 = 89^2 + 2 \cdot 33^2$
$10139 = 99^2 + 2 \cdot 13^2$
$10163 = 9^2 + 2 \cdot 71^2$
$10211 = 57^2 + 2 \cdot 59^2$
$10243 = 71^2 + 2 \cdot 51^2$
$10259 = 81^2 + 2 \cdot 43^2$
$10267 = 85^2 + 2 \cdot 39^2$
$10331 = 93^2 + 2 \cdot 29^2$
$10427 = 75^2 + 2 \cdot 49^2$
$10459 = 91^2 + 2 \cdot 33^2$
$10499 = 39^2 + 2 \cdot 67^2$
$10531 = 73^2 + 2 \cdot 51^2$
$10627 = 103^2 + 2 \cdot 3^2$
$10651 = 101^2 + 2 \cdot 15^2$
$10667 = 3^2 + 2 \cdot 73^2$
$10691 = 57^2 + 2 \cdot 61^2$
$10723 = 65^2 + 2 \cdot 57^2$
$10739 = 9^2 + 2 \cdot 73^2$
$10771 = 103^2 + 2 \cdot 9^2$
$10859 = 99^2 + 2 \cdot 23^2$
$10867 = 97^2 + 2 \cdot 27^2$
$10883 = 15^2 + 2 \cdot 73^2$
$10891 = 37^2 + 2 \cdot 69^2$
$10939 = 83^2 + 2 \cdot 45^2$
$10979 = 81^2 + 2 \cdot 47^2$
$10987 = 67^2 + 2 \cdot 57^2$
$11003 = 45^2 + 2 \cdot 67^2$
$11027 = 105^2 + 2 \cdot 1^2$
$11059 = 103^2 + 2 \cdot 15^2$
$11083 = 101^2 + 2 \cdot 21^2$
$11131 = 77^2 + 2 \cdot 51^2$
$11171 = 33^2 + 2 \cdot 71^2$
$11243 = 75^2 + 2 \cdot 53^2$
$11251 = 1^2 + 2 \cdot 75^2$
$11299 = 7^2 + 2 \cdot 75^2$
$11411 = 63^2 + 2 \cdot 61^2$
$11443 = 79^2 + 2 \cdot 51^2$
$11467 = 107^2 + 2 \cdot 3^2$
$11483 = 99^2 + 2 \cdot 29^2$
$11491 = 103^2 + 2 \cdot 21^2$
$11579 = 51^2 + 2 \cdot 67^2$
$11587 = 97^2 + 2 \cdot 33^2$
$11699 = 57^2 + 2 \cdot 65^2$
$11731 = 47^2 + 2 \cdot 69^2$
$11779 = 23^2 + 2 \cdot 75^2$
$11827 = 73^2 + 2 \cdot 57^2$
$11867 = 3^2 + 2 \cdot 77^2$
$11923 = 49^2 + 2 \cdot 69^2$
$11939 = 9^2 + 2 \cdot 77^2$
$11971 = 89^2 + 2 \cdot 45^2$
$11987 = 87^2 + 2 \cdot 47^2$
$12011 = 93^2 + 2 \cdot 41^2$
$12043 = 109^2 + 2 \cdot 9^2$
$12107 = 45^2 + 2 \cdot 71^2$
$12163 = 65^2 + 2 \cdot 63^2$
$12203 = 69^2 + 2 \cdot 61^2$
$12211 = 31^2 + 2 \cdot 75^2$
$12227 = 57^2 + 2 \cdot 67^2$
$12251 = 99^2 + 2 \cdot 35^2$
$12323 = 111^2 + 2 \cdot 1^2$
$12347 = 93^2 + 2 \cdot 43^2$
$12379 = 101^2 + 2 \cdot 33^2$
$12451 = 97^2 + 2 \cdot 39^2$
$12491 = 3^2 + 2 \cdot 79^2$
$12539 = 99^2 + 2 \cdot 37^2$
$12547 = 55^2 + 2 \cdot 69^2$
$12611 = 81^2 + 2 \cdot 55^2$
$12619 = 37^2 + 2 \cdot 75^2$
$12659 = 111^2 + 2 \cdot 13^2$
$12739 = 79^2 + 2 \cdot 57^2$
$12763 = 109^2 + 2 \cdot 21^2$
$12899 = 111^2 + 2 \cdot 17^2$
$12907 = 107^2 + 2 \cdot 27^2$
$12923 = 21^2 + 2 \cdot 79^2$
$12979 = 71^2 + 2 \cdot 63^2$
$13003 = 59^2 + 2 \cdot 69^2$
$13043 = 111^2 + 2 \cdot 19^2$
$13099 = 43^2 + 2 \cdot 75^2$
$13147 = 5^2 + 2 \cdot 81^2$
$13163 = 99^2 + 2 \cdot 41^2$
$13171 = 7^2 + 2 \cdot 81^2$
$13187 = 87^2 + 2 \cdot 53^2$
$13219 = 113^2 + 2 \cdot 15^2$
$13259 = 51^2 + 2 \cdot 73^2$
$13267 = 73^2 + 2 \cdot 63^2$
$13291 = 13^2 + 2 \cdot 81^2$
$13331 = 57^2 + 2 \cdot 71^2$
$13339 = 109^2 + 2 \cdot 27^2$
$13411 = 17^2 + 2 \cdot 81^2$
$13451 = 93^2 + 2 \cdot 49^2$
$13499 = 99^2 + 2 \cdot 43^2$
$13523 = 81^2 + 2 \cdot 59^2$
$13619 = 87^2 + 2 \cdot 55^2$
$13627 = 107^2 + 2 \cdot 33^2$
$13691 = 117^2 + 2 \cdot 1^2$
$13723 = 85^2 + 2 \cdot 57^2$
$13763 = 105^2 + 2 \cdot 37^2$
$13859 = 9^2 + 2 \cdot 83^2$
$13883 = 45^2 + 2 \cdot 77^2$
$13907 = 57^2 + 2 \cdot 73^2$
$13931 = 117^2 + 2 \cdot 11^2$
$13963 = 29^2 + 2 \cdot 81^2$
$14011 = 67^2 + 2 \cdot 69^2$
$14051 = 63^2 + 2 \cdot 71^2$
$14083 = 31^2 + 2 \cdot 81^2$
$14107 = 115^2 + 2 \cdot 21^2$
$14243 = 111^2 + 2 \cdot 31^2$
$14251 = 101^2 + 2 \cdot 45^2$
$14323 = 119^2 + 2 \cdot 9^2$
$14347 = 35^2 + 2 \cdot 81^2$
$14387 = 105^2 + 2 \cdot 41^2$
$14411 = 117^2 + 2 \cdot 19^2$
$14419 = 89^2 + 2 \cdot 57^2$

Literaturverzeichnis

[1] **Ayoub, Raymond G./Chowla, Saravadaman**: *On Euler's Polynomial.* J. Number Theory 13 (1981), 443–445.

[2] **Baker, Alan**: *Linear forms in the logarithms of algebraic numbers.* Mathematika 13 (1966), 204–216.

[3] **Brauer, Alfred**: *Über den kleinsten quadratischen Nichtrest.* Math. Zeitschr. 33 (1931), 161–176.

[4] **Buell, Duncan A.**: *Binary Quadratic Forms. Classical Theory and Modern Computations.* Springer, Berlin, Heidelberg, New York, 1989.

[5] **Byeon, Dongho/Stark, Harold M.**: *On the finiteness of certain Rabinowitsch polynomials.* To appear: J. Number Theory, 2003.

[6] **Chowla, Saravadaman/Cowles, John R./Cowles, Mary J.**: *The Least Prime Quadratic Residue and the Class Number.* J. Number Theory 22 (1986), 1–3.

[7] **Chowla, Saravadaman/Friedlander, J.**: *Class Numbers and Quadratic Residues.* Glasgow Math. J. 17 (1976), 47–52.

[8] **Cohn, Harvey**: *A Second Course in Number Theory.* John Wiley & Sons, New York, 1962.

[9] **Connell, Ian G.**: *On algebraic number fields with unique factorization.* Canad. Math. Bull. 5 (1962), 151–166.

[10] **Cox, David A.**: *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication.* John Wiley & Sons, New York, 1989.

[11] **Deuring, Max**: *Imaginäre quadratische Zahlkörper mit Klassenzahl 1.* Inventiones math. 5 (1968), 169–179.

[12] **Dickson, Leonard Eugene**: *On the negative discriminants for which there is a single class of positive primitive binary quadrtic forms.* Bulletin American Math. Soc. 17 (1911), 534–537.

[13] **Dirichlet, Gustav Peter Lejeune**: *Vorlesungen über Zahlentheorie. Hrsg. und mit Zusätzen versehen von R. Dedekind.* Vierte Auflage. Friedrich Vieweg und Sohn, Braunschweig, 1894.

[14] **Fjellstedt, Lars**: *A theorem concerning the least quadratic residue and non-residue.* Ark. Mat. 3 (1956), 287–291.

[15] **Flath, Daniel E.**: *Introduction to Number Theory.* John Wiley & Sons, New York, 1989.

[16] **Frobenius, Ferdinand Georg**: *Über quadratische Formen, die viele Primzahlen darstellen.* Sitzungsberichte der Kgl. Preuß. Akad. Wiss. Berlin (1912), 966–980.
[= Gesammelte Abhandlungen, Band III, 573–587, Springer, Berlin, Heidelberg, New York, 1968].

[17] **Gauß, Carl Freidrich**: *Disquisitiones arithmeticae.* G. Fleischer, Leipzig, 1801.
[Dt. Übersetzung von H. Maser: *Untersuchung über höhere Arithmetik.* Springer, Berlin, 1889].

[18] **Goldfeld, Dorian**: *Gauss' class number problems for imaginary quadratic fields.* Bulletin American Math. Soc. (new series) 1 (1985), 23–37.

[19] **Granville, Andrew/Mollin, Richard A.**: *Rabinowitsch revisited.* Acta Arithmetica 96 (2000), 139–153.

[20] **Greaves, George**: *Sieves in Number Theory.* Springer, Berlin, Heidelberg, New York, 2001.

[21] **Halter-Koch, Franz**: *Prime-producing quadratic polynomials and class numbers of quadratic orders*, 1989. In: Computational Number Theory. Proceedings of the Colloquium on Computational Number Theory held at Kossoth Lajos University, Debrecen (Hungary), September 4–9, 1989. Walter de Gruyter, Berlin, New York, 1991.

[22] **Heegner, Kurt**: *Diophantische Analysis und Modulfunktionen.* Math. Zeitschr. 56 (1952), 227–253.

[23] **Heilbronn, Hans/Linfoot, E. H.**: *On the imaginary quadratic corpora of class-number one.* Quart. J. Math. Oxford (2nd series) 5 (1934), 293–301.

[24] **Hendy, Michael D.**: *Prime qaudratics associated with complex quadratic fields of class number two.* Proc. American Math. Soc. 43 (1974), 253–260.

[25] **Ireland, Kenneth/Rosen, Michael**: *A Classical Introduction to Modern Number Theory.* 2nd Edition. GTM 84. Springer, Berlin, Heidelberg, New York, 1990.

[26] **Kutsuna, Masakazu**: *On a criterion for the class number of a quadratic number field to be one.* Nagoya Math. J. 79 (1980), 123–129.

[27] **Lam, Tsit-Yuen**: *The Algebraic Theory of Quadratic Forms.* W. A. Benjamin, Reading, 1973.

[28] **Landau, Edmund**: *Über die Klassenzahl der binären quadratischen Formen von negativer Diskriminante.* Math. Annalen 56 (1903), 671–676.

[29] **Landau, Edmund**: *Über die Klassenzahl imaginär-quadratischer Zahlkörper.* Göttinger Nachrichten (1918), 285–295.
[= Gesammtelte Schriften, Band 7, 150-160].

[30] **Lehmer, Derrick Henry**: *On imaginary quadratic fields whose class number is unity.* Bulletin American Math. Soc. 39 (1933), 360.

[31] **Lerch, Matiaš**: *Über die arithmetische Gleichung* $Cl(-\Delta) = 1$. Math. Annalen 57 (1903), 568–571.

[32] **Linnik, Yurij V./Vinogradov, A. I.**: *Hyperelliptic curves and the least prime quadratic residue.* Doklady Akad. Nauk SSSR 168 (1966), 259–261.

[33] **Louboutin, Stéphane**: *Extensions du théorème de Frobenius-Rabinovitsch.* C. R. Acad. Sci. Paris 312, Série I (1991), 711–714.

[34] **Louboutin, Stéphane/Mollin, Richard A./Williams H. C.**: *Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials and quadratic residue covers.* Can. J. Math. 44, 4th series (1992), 824–842.

[35] **McCurley, Kevin S.**: *Polynomials with no small prime values.* Proc. American Math. Soc. 97 (1986), 393–395.

[36] **McCurley, Kevin S.**: *The smalles prime value of* $x^n + a$. Can. J. Math. 38 (1986), 925–936.

[37] **Möller, Herber**: *Verallgemeinerung eines Satzes von Rabinowitsch über imaginär-quadratische Zahlkörper.* J. reine angew. Math. 285 (1976), 100–113.

[38] **Nagell, Trygve**: *Über die Klassenzahl imaginär-quadratischer Zahlkörper.* Abh. Math. Sem. Hamb. Univ. 1 (1922), 140–150.

[39] **Nagell, Trygve**: *Zahlentheoretische Notizen II.* Videnskapsselskapets Skrifter. I. Mat.-naturv. Klasse, Nr. 13 (1923), 7–10.
[Signatur der UB Tübingen: Kc 121.4;MANA-1923].

[40] **Nagell, Trygve**: *Sur les restes et les non-restes quadratiques suivant un module premier.* Ark. Mat. 1 (1950), 185–193.

[41] **Nagell, Trygve**: *Sur le plus petit non-reste quadratique impair.* Ark. Mat. 1 (1951), 573–578.

[42] **Nagell, Trygve**: *Sur un théorème d'Axel Thue.* Ark. Mat. 1 (1951), 489–496.

[43] **Narkiewicz, Władysław**: *Elementary and Analytic Theory of Algebraic Numbers.* 2nd Edition. Springer, Berlin, Heidelberg, New York, 1990.

[44] **Narkiewicz, Władysław**: *The Development of Prime Number Theory. Fraom Euclid to Hardy and Littlewood.* Springer, Berlin, Heidelberg, New York, 2000.

[45] **Nathanson, Melvyn B.**: *Elementary Methods in Number Theory.* GTM 195. Springer, Berlin, Heidelberg, New York, 2000.

[46] **Pintz, János**: *Elementary methods in the theory of L-functions VI. On the least prime quadratic residue* $(\mathrm{mod}\, p)$. Acta Arithmetica 32 (1977), 173–178.

[47] **Piper, Herbert**: *Variationen über ein zahlentheoretisches Thema von Carl Friedrich Gauss.* Birkhäuser, Basel, Boston, Berlin, 1978.

[48] **Prachar, Karl**: *Primzahlverteilung.* GdMW 91. Springer, Berlin, Heidelberg, New York, 1957.

[49] **Rabinowitsch, Georg**: *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern.* J. reine angew. Math. 142 (1913), 153–164.

[50] **Ribenboim, Paulo**: *Euler's famous prime generating polynomial and the class number of imaginary quadratic fields.* L'Enseignement Math. 34 (1988), 23–42.

[51] **Ribenboim, Paulo**: *The New Book of Prime Number Records. 3rd edition.* Springer, Berlin, Heidelberg, New York, 1996.

[52] **Salié, Hans**: *Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl.* Math. Nachr. 3 (1949), 7–8.

[53] **Sasaki, Ryuji**: *On a Lower Bound for the Class Number of an Imaginary Quadratic Field.* Proc. Japan Acad. 62, Ser. A (1986), 37–39.

[54] **Scharlau, Winfried/Opolka, Hans**: *Von Fermat bis Minkowski. Eine Vorlesung über Zahlentheorie und ihre Entwicklung.* Springer, Berlin, Heidelberg, New York, 1980.

[55] **Schinzel, Andrzej/Sierpiński, Wacław**: *Sur certaines hypothèses concernant les nombres premiers.* Acta Arithmetica 4 (1958), 185–208.

[56] **Shanks, Daniel**: *On Gauss's Class Number Problems.* Math. of Computation 23 (1969), 151–163.

[57] **Siegel, Carl Ludwig**: *Zum Beweise des Starkschen Satzes*. Inventiones math. 5 (1968), 180–191.

[58] **Stark, Harold M.**: *A complete determination of complex quadratic fields with class-number one*. Michigan Math. J. 14 (1967), 1–27.

[59] **Stark, Harold M.**: *On the „Gap“ in a theorem of Heegner*. J. Number Theory 1 (1969), 16–27.

[60] **Szekeres, Georges**: *On the Number of Divisors of* $x^2 + x + A$. J. Number Theory 6 (1974), 434–442.

[61] **Vinogradov, Ivan M.**: *On the bound of the least non-residue of n-th powers*. Trans. American Math. Soc. 29 (1927), 218–226.

[62] **Wedeniwski, Sebastian**: *Primality Tests on Commutator Curves*. Dissertation der Eberhard-Karls-Universität Tübingen, 2001.

[63] **Zagier, Don Bernard**: *Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*. Springer, Berlin, Heidelberg, New York, 1981.