Zeitschrift: Elemente der Mathematik

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 20 (1965)

Heft: 3

Artikel: Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper

Autor: Hasse, Helmut

DOI: https://doi.org/10.5169/seals-23925

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 15.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

ELEMENTE DER MATHEMATIK

Revue de mathématiques élémentaires – Rivista di matematica elementare

Zeitschrift zur Pflege der Mathematik
und zur Förderung des mathematisch-physikalischen Unterrichts
Organ für den Verein Schweizerischer Mathematik- und Physiklehrer

Publiziert mit Unterstützung des Schweizerischen Nationalfonds
zur Förderung der wissenschaftlichen Forschung

El. Math. Band XX Heft 3 Seiten 49–72 10. Mai 1965

Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper

In einer gemeinsamen Arbeit [1][1]) haben ANKENY, CHOWLA und ich kürzlich bewiesen, dass die mit Primzahlen p der Form

$$p = 4\,n_0^2 + 1 \quad (n_0 > 1, \text{ keine Primzahl})$$

gebildeten, bekanntlich eingeschlechtigen reell-quadratischen Zahlkörper

$$K = P(\sqrt{p})$$

mehrklassig sind.

Der Beweis beruhte auf dem Hilfssatz:

Eine diophantische Gleichung der Form

$$x^2 - (n^2 + 1)\,y^2 = \pm m$$

mit nichtquadratischem m kann nur für $m \geqq 2\,n$ lösbar sein.

Dieser Hilfssatz wiederum – in einer schwächeren Gestalt bereits von DAVENPORT an ANKENY mitgeteilt – liess sich ganz einfach auf Grund der Tatsache herleiten, dass die Grundeinheit des reell-quadratischen Zahlkörpers

$$K = P\left(\sqrt{n^2 + 1}\right)$$

explizit angebbar ist, nämlich als

$$\varepsilon = n + \sqrt{n^2 + 1} \quad \text{mit der Norm} \quad N(\varepsilon) = -1\,.$$

Man brauchte dann nur zum Ausdruck zu bringen, dass – sofern die fragliche diophantische Gleichung überhaupt lösbar ist – aus ihrer kleinsten positiven Lösung x, y durch Multiplikation der zugeordneten ganzen Zahl

$$\mu = x + y\sqrt{n^2 + 1} \quad \text{von der Norm} \quad N(\mu) = \pm m$$

aus K oder vielmehr ihrer Konjugierten μ' mit der angegebenen Grundeinheit ε von K eine mindestens ebenso grosse Lösung hervorgeht.

[1]) Die Ziffern in eckigen Klammern verweisen auf das Literaturverzeichnis, Seite 59.

Wie nun bereits RICHAUD bekannt war [2] und durch DEGERT bewiesen wurde [3], ist auch noch für weitere Typen reell-quadratischer Zahlkörper

$$K = P(\sqrt{D}) \quad (D > 0, \text{ quadratfrei})$$

die Grundeinheit ε explizit angebbar. Bezeichne n das absolut-nächste Ganze zu $\sqrt{D}$, so dass also

$$D = n^2 + r \quad \text{mit} \quad -n < r \leqq n$$

ist, und sei für den *Rest* r die *Teilbarkeitsbedingung*

$$r \mid 4n$$

erfüllt. Dann hat man

$$\varepsilon = n + \sqrt{D} \qquad \text{mit} \quad N(\varepsilon) = -\operatorname{sgn} r \quad \text{für} \quad |r| = 1$$
$$\text{(ausgenommen der Fall } D = 5,\ n = 2,\ r = 1),$$

$$\varepsilon = \frac{n + \sqrt{D}}{2} \qquad \text{mit} \quad N(\varepsilon) = -\operatorname{sgn} r \quad \text{für} \quad |r| = 4,$$

$$\varepsilon = \frac{(2n^2 + r) + 2n\sqrt{D}}{|r|} \qquad \text{mit} \quad N(\varepsilon) = +1 \quad \text{für} \quad |r| \neq 1, 4$$

(während für $|r| = 1, 4$ der letztgenannte Ausdruck das Quadrat der Grundeinheit und im Ausnahmefall die angegebene Einheit $\varepsilon = 2 + \sqrt{5}$ der Kubus der Grundeinheit ist).

Der Davenport-Ankenysche Hilfssatz lässt sich auf einige dieser Richaud-Degertschen Körpertypen in nicht-trivialer (auf andere nur in trivialer) Weise verallgemeinern, und man erhält damit dann Mehrklassigkeitsnachweise. Ein solcher Nachweis ist allerdings nur für eingeschlechtige Körper K von Interesse, da ja sonst die Mehrklassigkeit von vornherein feststeht. Eingeschlechtige reell-quadratische Zahlkörper K sind nach der Geschlechtertheorie genau diejenigen, für welche D von einem der vier Typen

$$D = p, \quad q, \quad 2q, \quad qq'$$

mit Primzahlen $p \equiv 1 \bmod. 4$ und $q, q' \equiv -1 \bmod. 4$ ist[1]), von dem hier uninteressanten Einzelfall $D = 2$ abgesehen.

Im folgenden wird zunächst in § 1 das Davenport-Ankenysche Schlußschema ganz allgemein, ohne explizite Kenntnis der Grundeinheit ε entwickelt.

Für die Anwendung auf die eingeschlechtigen Körper K vom Richaud-Degertschen Typus wird ferner in § 2 ermittelt, welche Reste r bei diesen Körpern allein in Frage kommen.

Sodann wird in § 3 untersucht, in welchen der so resultierenden Fälle das Davenport-Ankenysche Schlußschema nicht-triviale Abschätzungen liefert und welche Mehrklassigkeitsaussagen sich aus ihnen ergeben.

---

[1]) Siehe hierzu etwa H. HASSE, Zahlentheorie, 2. Auflage, Berlin 1963, § 26, **8** und § 29, **3**. – Alle diese Körper haben ungerade Klassenzahl. Für den ersteren Typus ist dies eine wohlbekannte Tatsache (am angeführten Ort, Seite 566); für die letzteren drei Typen (am angeführten Ort, Seite 567) erkennt man es daraus, dass sonst die engere Klassengruppe mehr als einen Zyklus von 2-Potenzordnung enthielte (am angeführten Ort, Seite 499, Abb. 40c), während doch nach dem Hauptsatz über die Geschlechter (am angeführten Ort, Seite 497) bei genau zwei Diskriminantenprimteilern ($2, q$, bzw. q, q') nur ein solcher Zyklus vorhanden ist.

Schliesslich werden in § 4 über die blosse Mehrklassigkeit hinaus noch einige bemerkenswerte untere Abschätzungen für die Klassenzahl gewisser eingeschlechtiger Körper vom Richaud-Degertschen Typus gegeben.

§ 1. Das Davenport-Ankenysche Schlußschema

Je nachdem $D \equiv 1$ mod. 4 oder $D \equiv 2, 3$ mod. 4 ist, sind die ganzen Zahlen aus K bei der Darstellung durch die Basis $1, \sqrt{D}$ *mit* Nenner 2 (und ganzen mod. 2 kongruenten Koordinaten) oder *ohne* Nenner 2 (mit beliebigen ganzen Koordinaten) anzusetzen. Es sei dementsprechend

$$\varepsilon = \frac{u + v\sqrt{D}}{2} \quad \text{mit} \quad N(\varepsilon) = \frac{u^2 - Dv^2}{4} = \pm 1 \quad (u, v > 0) \tag{1a}$$

bzw.

$$\varepsilon = u + v\sqrt{D} \quad \text{mit} \quad N(\varepsilon) = u^2 - Dv^2 = \pm 1 \quad (u, v > 0) \tag{1b}$$

die Grundeinheit von K, und es bestehe für ein nicht-quadratisches m die diophantische Gleichung

$$\pm m = \frac{x^2 - Dy^2}{4} = N(\mu) \quad \text{mit} \quad \mu = \frac{x + y\sqrt{D}}{2} \quad (x, y > 0) \tag{2a}$$

bzw.

$$\pm m = x^2 - Dy^2 = N(\mu) \quad \text{mit} \quad \mu = x + y\sqrt{D} \quad (x, y > 0)\,. \tag{2b}$$

a) $D \equiv 1$ *mod.* 4

Multiplikation der Konjugierten μ' mit der Grundeinheit ε ergibt

$$\frac{\dfrac{ux - Dvy}{2} + \dfrac{vx - uy}{2}\sqrt{D}}{2} \quad \text{mit} \quad N(\varepsilon\mu') = \pm m = \frac{\left(\dfrac{ux - Dvy}{2}\right)^2 - D\left(\dfrac{vx - uy}{2}\right)^2}{4}.$$

Wird also ohne Einschränkung y als minimal vorausgesetzt, so hat man notwendig

$$\left|\frac{vx - uy}{2}\right| \geqq y\,.$$

Das bedeutet *entweder* $vx \geqq (u + 2)\,y$ und damit die Abschätzung

$$\overset{+}{(-)}m \geqq \frac{\left(\dfrac{u+2}{v}\right)^2 - D}{4}\,y^2 \geqq \frac{u^2 + 4u + 4 - Dv^2}{4v^2} = \left\{\begin{matrix} \dfrac{u+2}{v^2} & \text{für} \quad N(\varepsilon) = +1 \\ \dfrac{u}{v^2} & \text{für} \quad N(\varepsilon) = -1 \end{matrix}\right\},$$

oder $vx \leqq (u - 2)\,y$ und damit die Abschätzung

$$\overset{(+)}{-}m \leqq \frac{\left(\dfrac{u-2}{v}\right)^2 - D}{4}\,y^2 \leqq \frac{u^2 - 4u + 4 - Dv^2}{4v^2} = \left\{\begin{matrix} -\dfrac{u-2}{v^2} & \text{für} \quad N(\varepsilon) = +1 \\ -\dfrac{u}{v^2} & \text{für} \quad N(\varepsilon) = -1 \end{matrix}\right\},$$

wobei links notwendig im ersteren Falle $+m$, im letzteren Falle $-m$ steht. Damit ist bewiesen:

Hilfssatz 1a. *Aus dem Bestehen der diophantischen Gleichung* (2a) *mit nicht-quadratischem m folgt notwendig die Ungleichung*

$$m \geqq \frac{u-2}{v^2} \quad \textit{für} \quad N(\varepsilon) = +1\,, \qquad m \geqq \frac{u}{v^2} \quad \textit{für} \quad N(\varepsilon) = -1\,,$$

wo u, v die Koordinaten der Grundeinheit ε aus (1a) *sind.*

b) $D \equiv 2, 3 \; mod. \; 4$

Indem man in vorstehendem Schlußschema x, y, u, v durch $2x, 2y, 2u, 2v$ ersetzt (wobei dann die Abschätzung $y^2 \geqq 1$ durch $(2y)^2 \geqq 4$ zu ersetzen ist), erhält man ganz entsprechend:

Hilfssatz 1b. *Aus dem Bestehen der diophantischen Gleichung* (2b) *mit nicht-quadratischem m folgt notwendig die Ungleichung*

$$m \geqq \frac{2(u-1)}{v^2} \quad \textit{für} \quad N(\varepsilon) = +1\,, \qquad m \geqq \frac{2u}{v^2} \quad \textit{für} \quad N(\varepsilon) = -1\,,$$

wo u, v die Koordinaten der Grundeinheit ε aus (1b) *sind.*

§ 2. Die bei eingeschlechtigen Körpern vom Richaud-Degertschen Typus möglichen Reste

Für die Ermittlung der bei eingeschlechtigen Körpern

$$K = P(\sqrt{D})\,, \quad D = p,\, q,\, 2q,\, qq'$$

vom Richaud-Degertschen Typus

$$D = n^2 + r\,, \quad -n < r \leqq n\,, \quad r \mid 4n$$

möglichen Reste r ist zu unterscheiden, ob das nächste Ganze n zu $\sqrt{D}$ gerade oder ungerade ist. Es mag genügen, die einfachen Schlüsse, die zum Ausschluss gewisser, mit den Bedingungen nicht verträglicher Reste führen, ohne viel Text aneinanderzureihen. Für die verbleibenden Fälle werden jeweils Beispiele angegeben.

a) $D = p \equiv 1 \; mod. \; 4$

$$p = n^2 + r\,, \quad -n < r \leqq n\,, \quad r \mid 4n\,.$$

n gerade $\Rightarrow r \equiv 1 \bmod. 4,\; r \mid n,\; r \mid p,\; r = p$ oder 1.

$r = p \Rightarrow n = 0$; unmöglich.

$r = 1$ möglich; Beispiel $p = 5 = 2^2 + 1$.

n ungerade $\Rightarrow r \equiv 0 \bmod. 4,\; r/4 \mid n,\; r/4 \mid p,\; r = \pm 4p$ oder ± 4.

$r = +4p \Rightarrow -3p = n^2$; unmöglich.

$r = -4p \Rightarrow 5p = n^2,\; p = 5,\; n = 5,\; r = -4n < -n$; unmöglich.

$r = +4$ möglich; Beispiel $p = 29 = 5^2 + 4$.

$r = -4 \Rightarrow p = (n+2)(n-2),\; p = 5,\; n = 3,\; r = -4 < -3 = -n$; unmöglich.

Hilfssatz 2a. *Bei* $D = p \equiv 1 \bmod. 4$ *liegt der Richaud-Degertsche Typus nur vor für*

$$p = n^2 + 1 \quad (n \text{ gerade}), \qquad p = n^2 + 4 \quad (n \text{ ungerade}).$$

b) $D = q \equiv -1$ *mod.* 4

$$q = n^2 + r, \quad -n < r \leqq n, \quad r \mid 4n.$$

n gerade $\Rightarrow r \equiv -1 \bmod. 4$, $r \mid n$, $r \mid q$, $r = q$ oder -1.

$r = q \Rightarrow n = 0$; unmöglich.

$r = -1 \Rightarrow q = (n+1)(n-1)$, $q = 3$, $n = 2$; möglich, einziges Beispiel

$$q = 3 = 2^2 - 1.$$

n ungerade $\Rightarrow r \equiv 2 \bmod. 4$, $r/2 \mid n$, $r/2 \mid q$, $r = \pm 2q$ oder ± 2.

$r = +2q \Rightarrow -q = n^2$; unmöglich.

$r = -2q \Rightarrow 3q = n^2$, $q = 3$, $n = 3$, $r = -2n < -n$; unmöglich.

$r = \pm 2$ möglich; Beispiele $q = \begin{Bmatrix} 11 = 3^2 + 2 \\ 7 = 3^2 - 2 \end{Bmatrix}$; notwendig $q \equiv \begin{Bmatrix} 3 \bmod. 8 \\ 7 \bmod. 8 \end{Bmatrix}$ (nach zweitem Ergänzungssatz).

Hilfssatz 2b. *Bei* $D = q \equiv -1 \bmod. 4$ *liegt der Richaud-Degertsche Typus, von dem Einzelfall* $q = 3 = 2^2 - 1$ *abgesehen, nur vor für*

$$q = n^2 + 2 \quad \textit{mit} \quad q \equiv 3 \bmod. 8, \qquad q = n^2 - 2 \quad \textit{mit} \quad q \equiv 7 \bmod. 8 \quad (n \text{ ungerade}).$$

c) $D = 2q$ *mit* $q \equiv -1$ *mod.* 4

$$2q = n^2 + r, \quad -n < r \leqq n, \quad r \mid 4n.$$

n gerade $\Rightarrow r \equiv 2 \bmod. 4$, $r/2 \mid n$, $r/2 \mid q$, $r = \pm 2q$ oder ± 2.

$r = +2q \Rightarrow n = 0$; unmöglich.

$r = -2q \Rightarrow 4q = n^2$; unmöglich.

$r = \pm 2$ möglich; Beispiele $2q = \begin{Bmatrix} 2 \cdot 3 = 2^2 + 2 \\ 2 \cdot 7 = 4^2 - 2 \end{Bmatrix}$; notwendig $q \equiv \begin{Bmatrix} 3 \bmod. 8 \\ 7 \bmod. 8 \end{Bmatrix}$ (nach zweitem Ergänzungssatz).

n ungerade $\Rightarrow r \equiv -3 \bmod. 8$, $r \mid n$, $r \mid q$, $r = -q$ mit $q \equiv 3 \bmod. 8$,

$3q = n^2$, $q = 3$, $n = 3$, $r = -n$; unmöglich.

Hilfssatz 2c. *Bei* $D = 2q$ *mit* $q \equiv -1 \bmod. 4$ *liegt der Richaud-Degertsche Typus nur vor für*

$$2q = n^2 + 2 \quad \textit{mit} \quad q \equiv 3 \bmod. 8, \qquad 2q = n^2 - 2 \quad \textit{mit} \quad q \equiv 7 \bmod. 8 \quad (n \text{ ungerade}).$$

d) $D = qq'$ *mit* $q, q' \equiv -1$ *mod.* 4

$$qq' = n^2 + r, \quad -n < r \leqq n, \quad r \mid 4n.$$

n gerade $\Rightarrow r \equiv 1 \bmod. 4$, $r \mid n$, $r \mid qq'$, $r = qq', -q, -q', 1$.

$r = qq' \Rightarrow n = 0$; unmöglich.

$r = -q \Rightarrow q(q'+1) = n^2$, $q \mid n$, $q < n$, $q' \geqq n$ möglich;

Beispiel $q\,q' = 3 \cdot 11 = 6^2 - 3$; notwendig $q < q'$.

$r = 1$ unmöglich (nach erstem Ergänzungssatz).

n ungerade $\Rightarrow r \equiv 0 \bmod. 4$, $r/4 \mid n$, $r/4 \mid q\,q'$, $r = \pm 4\,q\,q'$, $\pm 4\,q$, $\pm 4\,q'$, ± 4.

$r = +4\,q\,q' \Rightarrow -3\,q\,q' = n^2$; unmöglich.

$r = -4\,q\,q' \Rightarrow 5\,q\,q' = n^2$; unmöglich.

$r = \pm 4\,q$ möglich; Beispiele $q\,q' = \left\{\begin{matrix} 3 \cdot 79 = 15^2 + 12 \\ 3 \cdot 71 = 15^2 - 12 \end{matrix}\right\}$; notwendig $q < q'$ (denn mit $n = q\,n_0$ hat man $q' = q\,n_0^2 \pm 4$ mit $4\,q \leqq n$, also $4 \leqq n_0$, und daher $q' \geqq 16\,q - 4 \geqq 14\,q + (2\,q - 4) \geqq 14\,q + 2$).

$r = +4$ unmöglich (nach erstem Ergänzungssatz).

$r = -4$ möglich; Beispiel $q\,q' = 3 \cdot 7 = 5^2 - 4$.

Hilfssatz 2d. *Bei $D = q\,q'$ mit $q, q' \equiv -1 \bmod. 4$ und $q < q'$ liegt der Richaud-Degertsche Typus nur vor für*

$$q\,q' = n^2 - q \quad (n \text{ gerade}), \qquad q\,q' = n^2 \pm 4\,q \quad (n \text{ ungerade}), \qquad q\,q' = n^2 - 4 \quad (n \text{ ungerade}).$$

§ 3. Mehrklassigkeitsaussagen

Bekanntlich ist $K = P(\sqrt{D})$ nur dann einklassig, wenn für jede in K zerlegte Primzahl m, also für jede Primzahl m mit $(D/m) = 1$, die diophantische Gleichung

$$\frac{x^2 - Dy^2}{4} = \pm m \; (D \equiv 1 \bmod. 4) \qquad \text{bzw.} \qquad x^2 - Dy^2 = \pm m \; (D \equiv 2, 3 \bmod. 4)$$

lösbar ist. In den Hilfssätzen 1a, b wurde nun für die Körper K vom Richaud-Degertschen Typus eine durch die Grundeinheit ε von K bestimmte Schranke s derart angegeben, dass bei Lösbarkeit jener Gleichung notwendig $m \geqq s$ ist. Um K als mehrklassig zu erweisen, genügt es demnach, die Existenz einer Primzahl m festzustellen, die den folgenden beiden Forderungen genügt:

$$\left(\frac{D}{m}\right) = 1\,, \qquad m < s\,.$$

Nachstehend wird für die eingeschlechtigen Körper K vom Richaud-Degertschen Typus, wie sie in den Hilfssätzen 2a, b, c, d ermittelt wurden, jeweils die Schranke s aus der nach RICHAUD-DEGERT bekannten Grundeinheit ε gebildet. Soweit s mit D gross wird, ergeben sich dann durch auf der Hand liegende Erfüllung der angegebenen beiden Forderungen Mehrklassigkeitsaussagen, die jeweils durch das kleinste Zahlenbeispiel belegt werden.

a) $D = p \equiv 1 \; mod. \; 4\,, \quad r = 1$

$$p = n^2 + 1 \quad (n \text{ gerade}), \qquad n = 2\,n_0\,, \qquad p = 4\,n_0^2 + 1\,.$$

$$\varepsilon = 2\,n_0 + p\,, \qquad N(\varepsilon) = -1\,, \qquad u = 4\,n_0\,, \qquad v = 2^{1)}\,.$$

$$s = \frac{u}{y^2} = n_0\,.$$

[1]) Dass dieses ε im Richaud-Degertschen Ausnahmefall $p = 5$ nicht die Grundeinheit (sondern ihr Kubus) ist, macht für die Anwendung von Hilfssatz 1a nichts aus. Jedoch entfällt dieser Ausnahmefall sowieso dadurch, dass für den Schluss auf Mehrklassigkeit $n_0 > 1$ zu fordern sein wird.

Die *erste* Forderung $(p/m) = 1$ ist ersichtlich für jeden Primteiler m von n_0 erfüllt. Bei solcher Wahl von m lässt sich auch die *zweite* Forderung $m < n_0$ erfüllen, wenn nur $n_0 > 1$ und keine Primzahl ist, also echte Primteiler besitzt. Somit gilt:

Satz 1a. *Die reell-quadratischen Zahlkörper* $P(\sqrt{p})$ *mit Primzahlen* p *der Form*

$$p = 4\,n_0^2 + 1 \qquad (n_0 > 1\,,\ \textit{keine Primzahl})$$

sind mehrklassig.

Es ist dies das eingangs zitierte Ergebnis aus [1].

Kleinstes Beispiel: $p = 257 = 16^2 + 1$ $(m = 2)$.

b) $D = p \equiv 1 \ mod.\ 4,\ r = 4$

$$p = n^2 + 4 \qquad (n \text{ ungerade})\,.$$

$$\varepsilon = \frac{n + \sqrt{p}}{2}\,, \qquad N(\varepsilon) = -1\,, \qquad u = n\,, \qquad v = 1\,.$$

$$s = \frac{u}{v^2} = n\,.$$

Die *erste* Forderung $(p/m) = 1$ ist ersichtlich für jeden Primteiler m von n (aber wegen $p \equiv 5$ mod. 8 nicht auch für $m = 2$) erfüllt. Bei solcher Wahl von m lässt sich auch die *zweite* Forderung $m < n$ erfüllen, wenn nur $n > 1$ und keine Primzahl ist, also echte Primteiler besitzt. Somit gilt:

Satz 1b. *Die reell-quadratischen Zahlkörper* $P(\sqrt{p})$ *mit Primzahlen* p *der Form*

$$p = n^2 + 4 \qquad (n > 1\,,\ \textit{keine Primzahl})$$

sind mehrklassig.

Kleinstes Beispiel: $p = 229 = 15^2 + 4$ $(m = 3$ oder $5)$.

Da die Klassenzahlen der Körper $P(\sqrt{p})$ von SCHAFFSTEIN bis 12000 tabelliert sind [4], besagen die Sätze 1a, b erst jenseits dieser Grenze etwas Neues. Beim Vergleich mit jenen Tabellen hat sich übrigens herausgestellt, dass die unter Satz 1b fallende Primzahl $p = 1229 = 35^2 + 4$ von SCHAFFSTEIN übersehen wurde.

In den Fällen

$$D = q \quad \text{oder} \quad 2\,q \quad \text{mit} \quad q \equiv -1 \text{ mod. } 4\,, \qquad r = \pm 2$$

hat man

$$\varepsilon = (n^2 \pm 1) + n\sqrt{D}\,, \qquad N(\varepsilon) = +1\,, \qquad u = n^2 \pm 1\,, \qquad v = n\,,$$

also

$$s = \frac{2\,(u-1)}{v^2} = 2\,\frac{(n^2 \pm 1) - 1}{n^2} \leqq 2\,.$$

Da demnach die Forderung $m < s$ hier für keine Primzahl m erfüllt ist, erhält man in diesen Fällen keine Mehrklassigkeitsaussagen.

c) $D = q\,q'$ *mit* $q, q' \equiv -1 \ mod.\ 4$ $(q < q')$, $r = -4$

$$q\,q' = n^2 - 4 = (n-2)\,(n+2) \quad (n \text{ ungerade})\,, \qquad q = n - 2\,, \qquad q' = n + 2\,.$$

$$\varepsilon = \frac{n + \sqrt{q\,q'}}{2}\,, \qquad N(\varepsilon) = +1\,, \qquad u = n\,, \qquad v = 1\,.$$

$$s = \frac{u-2}{v^2} = n - 2\,.$$

Die *erste* Forderung $(q\,q'/m) = 1$ ist erfüllt für jeden Primteiler $m \equiv 1 \bmod. 4$ von n, aber nicht auch für $m = 2$; denn nach dem ersten bzw. zweiten Ergänzungssatz hat man

$$\left(\frac{q\,q'}{m}\right) = \left(\frac{-4}{m}\right) = \left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}, \qquad \left(\frac{q\,q'}{2}\right) = (-1)^{(q\,q'-1)/4} = (-1)^{[(n^2-1,\,4]-1} = -1\,.$$

Die *zweite* Forderung $m < n - 2$ läuft für Teiler m von n auf $m < n$ hinaus, weil ja sicherlich $n > 3$ und daher $n - 2 \nmid n$ ist. Somit gilt:

Satz 1c. *Die reell-quadratischen Zahlkörper* $\mathsf{P}\left(\sqrt{q\,q'}\right)$ *mit Primzahlen* $q, q' \equiv -1$ mod. 4 *von der Form*

$$q = n - 2\,, \qquad q' = n + 2$$

sind mehrklassig, wenn n einen echten Primteiler $m \equiv 1$ mod. 4 enthält, oder also wenn $n = (a^2 + b^2)\,t$ mit teilerfremden $a, b > 0$ und $t > 1$ ist.

Kleinstes Beispiel: $q\,q' = 43 \cdot 47 = 45^2 - 4$ $(m = 5)$.

d) $D = q\,q'$ *mit* $q, q' \equiv -1$ *mod.* 4 $(q < q')$, $r = -q$

$$q\,q' = n^2 - q \quad (n \text{ gerade})\,, \qquad n = q\,n_0\,, \qquad q' = q\,n_0^2 - 1 \quad (n_0 \text{ gerade})\,.$$

$$\varepsilon = (2\,q\,n_0^2 - 1) + 2\,n_0\sqrt{q\,q'}\,, \qquad N(\varepsilon) = +1\,, \qquad u = 4\,q\,n_0^2 - 2\,, \qquad v = 4\,n_0\,.$$

$$s = \frac{u-2}{v^2} = \frac{q\,n_0^2 - 1}{4\,n_0^2} = \frac{q - (1/n_0^2)}{4}\,.$$

Die *erste* Forderung $(q\,q'/m) = 1$ ist erfüllt für jeden Primteiler $m \neq 2$ von n_0 mit $(m/q) = 1$, sowie auch für $m = 2$, falls $q \equiv q'$ mod. 8; denn nach dem Reziprozitätsgesetz bzw. dem zweiten Ergänzungssatz hat man

$$\left(\frac{q\,q'}{m}\right) = \left(\frac{-q}{m}\right) = \left(\frac{m}{q}\right), \qquad \left(\frac{q\,q'}{2}\right) = (-1)^{(q\,q'-1)/4}.$$

Die *zweite* Forderung $m < [q - (1/n_0^2)]/4$ läuft wegen $n_0 \geqq 2$ auf $m \leqq (q-3)/4$ hinaus. Somit gilt:

Satz 1d. *Die reell-quadratischen Zahlkörper* $\mathsf{P}\left(\sqrt{q\,q'}\right)$ *mit Primzahlen* $q, q' \equiv -1$ mod. 4 $(q < q')$ *und*

$$q\,q' = n^2 - q \quad \textit{oder also} \quad q' = q\,n_0^2 - 1$$

sind mehrklassig, wenn n_0 einen ungeraden Primteiler $m \leqq (q-3)/4$ mit $(m/q) = 1$ enthält sowie auch, wenn $q \geqq 11$ und $q \equiv q'$ mod. 8 *ist.*

Kleinstes Beispiel: $q\,q' = 11 \cdot 43 = 22^2 - 11$ $(m = 2)$.

e) $D = q\,q'$ *mit* $q, q' \equiv -1$ *mod.* 4 $(q < q')$, $r = 4\,q$

$$q\,q' = n^2 + 4\,q \quad (n \text{ ungerade})\,, \qquad n = q\,n_0\,, \qquad q' = q\,n_0^2 + 4 \quad (n_0 \text{ ungerade})\,.$$

$$\varepsilon = \frac{(q\,n_0^2 + 2) + n_0\sqrt{q\,q'}}{2}\,, \qquad N(\varepsilon) = +1\,, \qquad u = q\,n_0^2 + 2\,, \qquad v = n_0\,.$$

$$s = \frac{u-2}{v^2} = q\,.$$

Die *erste* Forderung $(q\,q'/m) = 1$ ist erfüllt für jeden Primteiler m von n_0 mit $(m/q) = (-1)^{(m-1)/2}$, aber nicht auch für $m = 2$; denn nach dem Reziprozitätsgesetz bzw. dem zweiten Ergänzungssatz hat man

$$\left(\frac{q\,q'}{m}\right) = \left(\frac{4\,q}{m}\right) = \left(\frac{q}{m}\right) = (-1)^{(m-1)/2}\left(\frac{m}{q}\right), \quad \left(\frac{q\,q'}{2}\right) = (-1)^{(q\,q'-1)/4} = -1^{[(n^2-1)/4]+q} = -1\,.$$

Die *zweite* Forderung verlangt $m < q$. Somit gilt:

Satz 1e. *Die reell-quadratischen Zahlkörper* $\mathsf{P}(\sqrt{q\,q'})$ *mit Primzahlen* $q, q' \equiv -1$ mod. 4 $(q < q')$ *und*

$$q\,q' = n^2 + 4\,q \quad \textit{oder also} \quad q' = q\,n_0^2 + 4$$

sind mehrklassig, wenn n_0 *einen Primteiler* $m < q$ *mit* $(m/q) \equiv (-1)^{(m-1)/2}$ *enthält.*

Kleinstes Beispiel: $q\,q' \equiv 7 \cdot 67 = 21^2 + 4 \cdot 7$ $(m = 3)$.

$$\text{f)}\ D = q\,q' \quad \textit{mit} \quad q, q' \equiv -1 \ \textit{mod.}\ 4\ (q < q')\,, \quad r = -4\,q$$

$$q\,q' = n^2 - 4\,q \ \ (n \text{ ungerade})\,, \quad n = q\,n_0\,, \quad q' = q\,n_0^2 - 4 \ \ (n_0 \text{ ungerade})\,.$$

$$\varepsilon = \frac{(q\,n_0^2 - 2) + n_0\sqrt{q\,q'}}{2}\,, \quad N(\varepsilon) = +1\,, \quad u = q\,n_0^2 - 2\,, \quad v = n_0\,.$$

$$s = \frac{u-2}{v^2} = \frac{q\,n_0^2 - 4}{n_0^2} = q - \frac{4}{n_0^2}\,.$$

Die *erste* Forderung $(q\,q'/m) = 1$ ist erfüllt für jeden Primteiler m von n_0 mit $(m/q) = 1$, aber nicht auch für $m = 2$; denn nach dem Reziprozitätsgesetz bzw. dem zweiten Ergänzungssatz hat man

$$\left(\frac{q\,q'}{m}\right) = \left(\frac{-4\,q}{m}\right) = \left(\frac{-q}{m}\right) = \left(\frac{m}{q}\right), \quad \left(\frac{q\,q'}{2}\right) = (-1)^{(q\,q'-1)/4} = (-1)^{[(n^2-1)/4]-q} = -1\,.$$

Die *zweite* Forderung $m < q - (4/n_0^2)$ läuft wegen $n_0 \geqq 3$ auf $m < q$ hinaus. Somit gilt:

Satz 1f. *Die reell-quadratischen Zahlkörper* $\mathsf{P}(\sqrt{q\,q'})$ *mit Primzahlen* $q, q' \equiv -1$ mod. 4 $(q < q')$ *und*

$$q\,q' = n^2 - 4\,q \quad \textit{oder also} \quad q' = q\,n_0^2 - 4$$

sind mehrklassig, wenn n_0 *einen Primteiler* $m < q$ *mit* $(m/q) = 1$ *enthält.*

Kleinstes Beispiel: $q\,q' = 11.271 \equiv 55^5 - 44$ $(m = 5)$.

§ 4. Untere Abschätzungen der Klassenzahl

Vor den Sätzen 1a, b, c wurde festgestellt, dass die Schranken u/v^2 bzw. $(u-2)/v^2$ aus Hilfssatz 1a für die in jenen Sätzen behandelten Körpertypen $\mathsf{P}(\sqrt{D})$ jeweils die Werte

$$s = \frac{n}{2}\,, \quad s = n\,, \quad s = n - 2$$

haben, also mit den Körperdiskriminanten

$$D = p = n^2 + 1\,, \quad D = p = n^2 + 4\,, \quad D = q\,q' = n^2 - 4$$

über alle Grenzen wachsen. Daraus lassen sich für jene Körpertypen $P(\sqrt{D})$ leicht untere Abschätzungen der Klassenzahl $h(D)$ gewinnen, aus denen insbesondere hervorgeht, dass $h(D)$ mit D über alle Grenzen wächst, sofern es unendlich viele Körper des betr. Typus gibt.

Satz 2a. *In der Folge der Primzahlen p von der Form*

$$p = (2\,m\,k)^2 + 1$$

mit irgendeiner festen Primzahl m besteht für die Klassenzahl $h(p)$ von $P(\sqrt{p})$ die untere Abschätzung

$$h(p) \geqq \frac{\log\sqrt{(p-1)/4}}{\log m}\,.$$

Satz 2b. *In der Folge der Primzahlen p von der Form*

$$p = (m\,k)^2 + 4$$

mit irgendeiner festen Primzahl $m \neq 2$ besteht für die Klassenzahl $h(p)$ von $P(\sqrt{p})$ die untere Abschätzung

$$h(p) \geqq \frac{\log\sqrt{p-4}}{\log m}\,.$$

Satz 2c. *In der Folge der Primzahlpaare $q, q' \equiv -1$ mod. 4 von der Form*

$$q = m\,k - 2\,, \quad q' = m\,k + 2$$

mit irgendeiner festen Primzahl $m \equiv 1$ mod. 4 besteht für die Klassenzahl $h(q\,q')$ von $P(\sqrt{q\,q'})$ die untere Abschätzung

$$h(q\,q') \geqq \frac{\log(\sqrt{q\,q'+4}-2)}{\log m}\,.$$

Beweis. Für die zu betrachtenden Diskriminanten

$$D = p = (2\,m\,k)^2 + 1\,, \quad D = p = (m\,k)^2 + 4\,, \quad D = q\,q' = (m\,k)^2 - 4$$

hat die feste Primzahl m, wie bereits vor den Sätzen 1a, b, c festgestellt, die Eigenschaft $(D/m) = 1$, zerfällt also in den Körpern $P(\sqrt{D})$ in zwei (zueinander konjugierte) Primdivisoren. Sei e die Ordnung von deren (zueinander reziproken) Klassen, also der kleinste positive Exponent, für den die diophantische Gleichung

$$\pm m^e = \frac{x^2 - Dy^2}{4}$$

lösbar ist. Nach Hilfssatz 1a hat man dann notwendig $m^e \geqq s$, also in den einzelnen Fällen

$$m^e \geqq m\,k = \frac{p-1}{4}\,, \quad m^e \geqq m\,k = p - 4\,, \quad m^e \geqq m\,k - 2 = q\,q' + 4 - 2\,.$$

Da die Klassenzahl $h(D)$ ein Vielfaches der Ordnung e ist, gelten diese Abschätzungen erst recht mit dem Exponenten $h(D)$ statt e. Das ergibt durch Logarithmierung die Behauptungen.

Schlussbemerkung (gemeinsam mit S. CHOWLA). Beachtet man, dass die Zähler rechts in den Abschätzungen aus den Sätzen 2a, b, c jeweils asymptotisch gleich $\log\sqrt{D}$ sind, so erhält man aus jenen *präzisen* unteren Abschätzungen die *asymptotischen* unteren Abschätzungen

$$\liminf_{D\to\infty} \frac{h(D)}{\log\sqrt{D}} \geqq \frac{1}{\log m},$$

gültig in den betrachteten Diskriminantenfolgen, sofern diese nicht abbrechen, das heisst sofern es unendlich viele Primzahlen p bzw. Primzahlpaare q, q' des betr. Typus gibt. In dieser asymptotischen Form besagen die in Rede stehenden Abschätzungen nichts Neues. Vielmehr hat ja SIEGEL ganz allgemein die asymptotische untere Abschätzung

$$h(D)\log\varepsilon = \frac{1}{2}\sum_{n=1} \frac{1}{n}\left(\frac{D}{n}\right) > D^{(1/2)-\theta} \quad \text{für} \quad D > D_0(\theta)$$

bei beliebigem $\theta > 0$ bewiesen [5], und in den hier betrachteten Richaud-Degertschen Fällen ist die Grundeinheit $\varepsilon < 2\sqrt{D}$ (bzw. sogar $< \sqrt{D}$), also $\log\varepsilon = O(\log\sqrt{D}) = O(D^{\theta})$ für beliebiges $\theta > 0$, so dass in diesen Fällen $h(D)$ mindestens von der Ordnung $O(D^{(1/2)-\theta})$ (statt nur $O(\log\sqrt{D})$) unendlich wird. Während aber bei SIEGEL die Schranke $D_0(\theta)$, oberhalb derer die asymptotische Abschätzung gilt, nicht effektiv angegeben wird, sind die präzisen Abschätzungen aus den Sätzen 2a, b, c von dieser Unbestimmtheit frei, geben also über das Siegelsche Ergebnis hinausgehende Informationen.

HELMUT HASSE, Hamburg

LITERATURVERZEICHNIS

[1] N. C. ANKENY, S. CHOWLA und H. HASSE, *On the class-number of the real subfield of a cyclotomic field.* J. reine angew. Math. *217*, 217–220 (1965).

[2] C. RICHAUD, *Sur la résolution des équations* $x^2 - A\,y^2 = \pm 1$. Atti Accad. pontif. Nuovi Lincei *1866*, 177–182.

[3] G. DEGERT, *Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper.* Abh. math. Sem. Univ. Hamburg *22*, 92–97 (1958).

[4] K. SCHAFFSTEIN, *Tafel der Klassenzahlen der reellen quadratischen Zahlkörper mit Primzahldiskriminante unter 12000 und zwischen 100000–101000 und 1000000–1001000.* Math. Ann. *99*, 745–748 (1928).

[5] C. L. SIEGEL, *Über die Classenzahl quadratischer Zahlkörper.* Acta arithmetica *1*, 83–86 (1935).

Packing of 18 Equal Circles on a Sphere

The largest possible angular diameter of 18 (or 19) equal circles which can be packed on the surface of a sphere has not yet been determined. Suggested values for 17 and 20 circles have been published [1] [2] [1]). These values serve as bounds for the possible values to be derived for 18 and 19 circles.

The best known arrangement for 20 circles is shown in Figure 1. If the circles at the poles are removed, then the remaining 18 circles are still locked in static equilibrium. If, in addition, the adjacent rings of 3 circles are removed, then 6 circles can be replaced to form the stable arrangement shown in Figure 2. Surprisingly, the

[1]) Numbers in brackets refer to References, page 61.