Daher wird

$$\eta = 1 + 6\cos\frac{2\pi}{13} + 6\cos\frac{10\pi}{13}.$$

Hier zeigen die Abschätzungen

$$\eta < 1 + 6\cos 0 + 6\cos\frac{3\pi}{4} = 1 + 6 - 3\sqrt{2} = 7 - 3\sqrt{2} < \sqrt{13},$$

$$\eta > 1 + 6\cos\frac{2\pi}{12} + 6\cos\frac{10\pi}{12} = 1 > -\sqrt{13},$$

daß η dem Intervall $-\sqrt{13} \ldots \sqrt{13}$, also 13 der Klasse p_5 angehört.

7. Analoga für bikubische und biquadratische Charaktere.

Der bikubische Fall läßt sich wie schon in 4 auf den kubischen Fall zurückführen. Man benutzt dazu am einfachsten nicht wie dort vor (10 c.) die etwas tiefer liegende Formel (7.) aus IX, sondern die Grundformel aus VIII für das Faktorensystem der Gaußschen Summen.

In den Bezeichnungen aus 4 für den kubischen und bikubischen Fall hat man danach

$$\tau(\chi\psi) = \frac{\tau(\chi)\,\tau(\psi)}{\pi(\chi,\psi)} = \chi(2)\,\frac{\tau(\chi)\,\tau(\psi)}{\pi}.$$

Hierdurch wird die Normierungsaufgabe für die sechste Wurzel aus

$$\tau(\chi\psi)^6 = p^*\bar{\pi}^4$$

auf die in 6 besprochene Normierungsaufgabe für die dritte Wurzel aus $\tau(\chi)^3 = p\,\pi$ und die in 5 durchgeführte Vorzeichenbestimmung der Quadratwurzel aus $\tau(\psi)^2 = p^*$ zurückgeführt:

$$(1.) \qquad \tau(\chi\psi) = \sqrt[6]{p^*\bar{\pi}^4} = \chi(2)\,\frac{\sqrt[3]{p\pi}\,\sqrt{p^*}}{\pi}.$$

Die zu untersuchende $\sqrt[6]{p^*\bar{\pi}^4}$ hat hier von vornherein sechs Möglichkeiten, die sich durch die sechs Sextanten des Kreises um 0 vom Radius $\sqrt{p}$ trennen lassen, nicht etwa nur durch eine alternierende Folge von sechs Zwölftelsektoren, weil die positiv-imaginäre Normierung von π keinerlei Einschränkung für die Lage von $p^*\bar{\pi}^4$ in der komplexen Ebene mit sich bringt. Rechnet man jedoch diese Sextanten, anstatt von der positiv-reellen Achse, von dem Strahl durch $\chi(2)\,\frac{\sqrt{p^*}}{\pi}$ aus, so kommen entsprechend den drei Klassen p_1, p_3, p_5 der Primzahlen $p \equiv 1 \bmod 3$ nach (1.) nur der 1., 3., 5. Sextant in Frage. Es tritt also nicht etwa, wie man hätte denken können, eine Unterteilung jener drei Klassen in je zwei Halbklassen auf. Der bikubische Fall liefert somit nichts wesentlich Neues.

Im biquadratischen Fall, dem wir uns jetzt zuwenden, tritt dagegen ein Analogon zur Kummerschen Klasseneinteilung auf, das hier noch durch eine zum quadratischen Fall analoge Typeneinteilung überlagert ist. Im Anschluß an die Ausführungen in 4 über den biquadratischen Fall und nach dem Vorbild aus 6 des kubischen Falles können wir uns kurz fassen.

Es handelt sich für eine Primzahl $p \equiv 1 \bmod 4$ nach 4, (10a.) um die Normierung der vierten Wurzel aus

$$(2.) \qquad \tau(\chi)^4 = p\,\pi^2, \quad \tau(\bar{\chi})^4 = p\,\bar{\pi}^2.$$

Dabei können wir ohne Einfluß auf die Fragestellung die arithmetische Normierung 4, (11a.) von $\pi, \bar{\pi}$ durch die analytische Normierung

$$(3.) \qquad \left\{\begin{array}{l} \pi, \bar{\pi} = a \pm 2bi \quad \text{mit} \quad a > 0,\ b > 0 \\ p = a^2 + 4b^2 \end{array}\right\}$$

ersetzen, also π im ersten Quadranten der komplexen Zahlenebene wählen, da es in (2.) auf das Vorzeichen von π nicht ankommt. Unter χ ist dann der diesem Primfaktor π von p in P_4 durch das verallgemeinerte Eulersche Kriterium

$$(4.) \qquad \chi(x) \equiv x^{\frac{p-1}{4}} \bmod \pi$$

zugeordnete biquadratische Charakter mod. p zu verstehen.

Anders als im kubischen Falle sind hier $\tau(\chi), \tau(\bar{\chi})$ nicht immer konjugiert-komplex zueinander, sondern es ist

$$\tau(\bar{\chi}) = \chi(-1)\,\overline{\tau(\chi)}$$

mit

$$\chi(-1) = (-1)^{\frac{p-1}{4}} = \left\{\begin{array}{l} 1 \text{ für } p \equiv 1 \bmod 8 \\ -1 \text{ für } p \equiv 5 \bmod 8 \end{array}\right\}.$$

Diese Alternative ergibt eine Einteilung der zu betrachtenden Primzahlen $p \equiv 1 \bmod 4$ in zwei Typen.

Bei der Normierung (3.) ist der Radikand $p\pi^2$ positiv-imaginär. Demnach verteilen sich die Primzahlen $p \equiv 1 \bmod 4$ jedes der beiden Typen auf

vier Klassen p_1, p_3, p_5, p_7,

je nachdem, ob die π wie angegeben zugeordnete normierte Gaußsche Summe

$\tau(\chi)$ im 1., 3., 5., 7. Oktanten

der komplexen Zahlenebene liegt (Abb. 28).

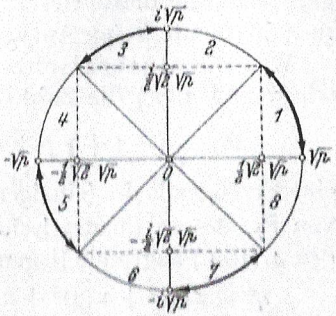

Abb. 28.

Setzt man

$$\tau(\chi) = \varrho + i\sigma, \quad \overline{\tau(\chi)} = \varrho - i\sigma,$$

also

$$(5.) \qquad \varrho = \tfrac{1}{2}\left(\tau(\chi) + \chi(-1)\,\tau(\bar{\chi})\right), \quad \sigma = \tfrac{1}{2i}\left(\tau(\chi) - \chi(-1)\,\tau(\bar{\chi})\right),$$

wie wir jetzt explizit sehen werden, allein durch die Zahlen p, a aus (1.) bestimmt ist.

Die Zahl η hängt mit der Erzeugenden ϑ des zyklischen kubischen Teilkörpers K von P_p, zu der $\tau(\chi)$ Lagrangesche Resolvente ist, durch die nach 3, (7.) bestehende Beziehung

$$\vartheta = \frac{1}{3}\left(-1 + \tau(\chi) + \tau(\bar{\chi})\right) = \frac{\eta - 1}{3}$$

zusammen, ist also wie ϑ eine Erzeugende von K. Durch die normierte primitive p-te Einheitswurzel ζ stellen sich die Konjugierten zu ϑ als die p-ten Kreisteilungsperioden dritten Grades in der Form dar:

$$(6.)\quad \left\{\begin{aligned} \vartheta &= \sum_{\substack{x \bmod p \\ \chi(x)=1}} \zeta^{x} &&= \frac{1}{3}\sum_{y \not\equiv 0 \bmod p} \zeta^{y^3} \\ \vartheta' &= \sum_{\substack{x' \bmod p \\ \chi(x')=\varrho}} \zeta^{x'} = \sum_{\substack{x \bmod p \\ \chi(x)=1}} \zeta^{rx} &&= \frac{1}{3}\sum_{y \not\equiv 0 \bmod p} \zeta^{ry^3} \\ \vartheta'' &= \sum_{\substack{x'' \bmod p \\ \chi(x'')=\varrho^2}} \zeta^{x''} = \sum_{\substack{x \bmod p \\ \chi(x)=1}} \zeta^{r^2x} &&= \frac{1}{3}\sum_{y \not\equiv 0 \bmod p} \zeta^{r^2y^3} \end{aligned}\right\},$$

wo r ein kubischer Nichtrest mod. p mit $\chi(r) = \varrho = \frac{-1+\sqrt{-3}}{2}$ ist. Die Konjugierten zu η erhält man dann, indem man in der Summation über y noch das Glied 1 mit $y \equiv 0$ mod. p hinzufügt:

$$(7.)\quad \eta = \sum_{y \bmod p} \zeta^{y^3}, \qquad \eta' = \sum_{y \bmod p} \zeta^{ry^3}, \qquad \eta'' = \sum_{y \bmod p} \zeta^{r^2y^3}.$$

Die beiden linearen Gleichungssysteme 3, (4.), (7.) lauten hier:

$$\left\{\begin{aligned} -1 &= \vartheta + \vartheta' + \vartheta'' \\ \tau(\chi) &= \vartheta + \varrho\vartheta' + \varrho^2\vartheta'' \\ \tau(\bar{\chi}) &= \vartheta + \varrho^2\vartheta' + \varrho\,\vartheta'' \end{aligned}\right\}, \qquad \left\{\begin{aligned} 0 &= \eta + \eta' + \eta'' \\ \tau(\chi) &= \frac{1}{3}(\eta + \varrho\eta' + \varrho^2\eta'') \\ \tau(\bar{\chi}) &= \frac{1}{3}(\eta + \varrho^2\eta' + \varrho\,\eta'') \end{aligned}\right\}$$

und

$$\left\{\begin{aligned} \vartheta &= \tfrac{1}{3}(-1 + \tau(\chi) + \tau(\bar{\chi})) \\ \vartheta' &= \tfrac{1}{3}(-1 + \varrho^2\tau(\chi) + \varrho\tau(\bar{\chi})) \\ \vartheta'' &= \tfrac{1}{3}(-1 + \varrho\,\tau(\chi) + \varrho^2\tau(\bar{\chi})) \end{aligned}\right\}, \qquad \left\{\begin{aligned} \eta &= \tau(\chi) + \tau(\bar{\chi}) \\ \eta' &= \varrho^2\tau(\chi) + \varrho\tau(\bar{\chi}) \\ \eta'' &= \varrho\,\tau(\chi) + \varrho^2\tau(\bar{\chi}) \end{aligned}\right\}.$$

Denkt man in den letzteren Gleichungen für $\tau(\chi)$ und $\tau(\bar{\chi})$ die richtig normierte $\sqrt[3]{p\pi}$ und ihre Konjugiert-komplexe $\sqrt[3]{p\bar{\pi}}$ eingetragen, so hat man die Cardanischen Auflösungsformeln für die zyklischen kubischen Gleichungen vor sich, denen ϑ und η genügen. Die Gleichung für η hat den zweithöchsten Koeffizienten 0; sie entsteht aus der für ϑ mit dem zweithöchsten Koeffizienten -1 durch die übliche Reduktion.

Explizit ergeben sich diese Gleichungen durch Berechnung der beiden weiteren symmetrischen Grundfunktionen von η, η', η'' wie folgt:

$$\eta\,\eta'\eta'' = \tau(\chi)^3 + \tau(\bar{\chi})^3 = p\,\pi + p\,\bar{\pi} = p\,a,$$
$$\eta\,\eta' + \eta\,\eta'' + \eta'\eta'' = -3\,\tau(\chi)\,\tau(\bar{\chi}) = -3\,p.$$

Die Gleichung für η lautet demnach

$$(8.)\qquad \eta^3 - 3p\,\eta - a\,p = 0.$$

Sie ist in der Tat nur durch die beiden Zahlen p, a aus (1.) bestimmt. Ihre Diskriminante ist

$$\frac{4p^3 - a^2p^2}{27} = b^2p^2.$$

Als Gleichung für ϑ ergibt sich

$$\vartheta^3 + \vartheta^2 - \frac{p-1}{3}\,\vartheta - \frac{ap + 3p - 1}{27} = 0.$$

Daß hierin auch der letzte Koeffizient ganzzahlig ist, erkennt man als formale Folge aus der Beziehung (1.) zwischen p und a. Mit diesen Gleichungen ist eine algebraische Erzeugung des zyklischen kubischen Teilkörpers $\mathsf{K} = \mathsf{P}(\vartheta) = \mathsf{P}(\eta)$ von P_p explizit angegeben.

Auf unsere Ausgangsfrage zurückkommend, können wir jetzt sagen, daß die drei Wurzeln η, η', η'' der algebraischen kubischen Gleichung (8.) in den drei Intervallen (5.) liegen, da sie ja den drei verschiedenen Normierungen von $\sqrt[3]{p\pi}$ als doppelte Realteile zugeordnet sind. Die Frage ist dann, welchem dieser Intervalle die durch (4.) analytisch normierte Wurzel η von (8.) angehört. Diese analytische Normierung (4.) kann nach (7.) in der Form

$$\eta = \sum_{y \bmod p} \zeta^{y^3} = 1 + 2\sum_{\pm\, y \bmod p} \cos\frac{2\pi y^3}{p}$$

oder nach (6.) auch

$$\eta = 1 + 3\sum_{\substack{x \bmod p \\ \chi(x)=1}} \zeta^{x} = 1 + 6\sum_{\substack{\pm x \bmod p \\ \chi(x)=1}} \cos\frac{2\pi x}{p}$$

geschrieben werden. Die letztere Form erscheint zur numerischen Entscheidung der Frage am besten geeignet.

Beispiele. $\underline{p=7}$. Die absolut-kleinsten kubischen Reste sind ± 1 mod. 7. Daher wird

$$\eta = 1 + 6\cos\frac{2\pi}{7}.$$

Die einfache Abschätzung

$$\eta > 1 + 6\cos\frac{2\pi}{6} = 1 + 3 = 4 > \sqrt{7}$$

zeigt hier ohne Zuhilfenahme von Tabellen, daß η dem Intervall $\sqrt{7} \ldots 2\sqrt{7}$, also 7 der Klasse p_1 angehört.

$\underline{p=13}$. Die absolut-kleinsten kubischen Reste sind ± 1, ± 5 mod. 13.

exponenten) bedeuten, und diese $\mathfrak{p}$ haben gerade die Dichten $\frac{1}{6}, \frac{1}{3}, \frac{1}{2}$ (in dieser Reihenfolge); dabei entspricht der letztgenannte Zerlegungstypus mit der Dichte $\frac{1}{2}$ den Primzahlen p mit $\left(\frac{D}{p}\right) = -1$. Sollte die Kummersche Klasseneinteilung das Zerlegungsgesetz in einem nichtabelschen kubischen Körper K widerspiegeln, so käme, da es sich bei ihr nur um die Primzahlen $p \equiv 1 \bmod 3$ handelt, jedenfalls nicht ein solcher in Frage, dessen Diskriminante D den quadratfreien Kern -3 hat, weil in diesem Falle der Zerlegungstypus mit der Dichte $\frac{1}{2}$ aus allen Primzahlen $p \equiv -1 \bmod 3$ besteht. Dadurch wird aber genau jeder rein-kubisch erzeugbare Körper $\mathsf{K} = \mathsf{P}(\sqrt[3]{a})$ (a rational, keine Kubikzahl) und insbesondere der einzige solche ausgeschlossen, in dessen Diskriminante D nur die Primzahl 3 steckt, nämlich der Körper $\mathsf{K} = \mathsf{P}(\sqrt[3]{3})$. Es müßte sich demnach um einen kubischen Zahlkörper K handeln, in dessen Diskriminante D von 3 verschiedene Primzahlen q stecken. Dies ist jedoch aus zwei Gründen unwahrscheinlich. Einmal würden dann diese endlich vielen Primzahlen q (soweit $\equiv 1 \bmod 3$) zwar von der Kummerschen Klasseneinteilung, aber nicht von der des Zerlegungsgesetzes erfaßt; dieser Einwand würde wegfallen, falls alle diese Primzahlen $q \equiv -1 \bmod 3$ wären — sie müßten dann notwendig schon in der Diskriminante d des quadratischen Körpers $\mathsf{P}(\sqrt{D}) = \mathsf{P}(\sqrt{d})$ stecken. Und außerdem wäre es bei der rein-kubischen Struktur der Kummerschen Klasseneinteilung höchst verwunderlich, wenn einige Primzahlen q eine Vorzugsrolle als Diskriminantenteiler des zugeordneten kubischen Zahlkörpers K spielten, ein Einwand, der in jedem Falle zutrifft; man würde sich sofort fragen, welche Primzahlen das denn sein könnten, und keinen plausiblen Grund finden, weswegen etwa die Primzahl $q = 23$ (vgl. Schluß von § 17,5) oder $q = 4027$ als Parameter etwas mit der Kummerschen Klasseneinteilung zu tun haben sollte.

Wenn es sich demnach bei der Kummerschen Klasseneinteilung auch wahrscheinlich nicht um die Widerspiegelung eines Zerlegungsgesetzes handelt, so wäre es bei dem heutigen Stande der Forschung in der Primzahltheorie doch in jedem Falle interessant, nicht-triviale (d. h. nicht aus primen Restklassen gebildete) Primzahlmengen zu kennen, die eine Dichte besitzen. So ist die Inangriffnahme der Kummerschen Vermutung sicherlich eine lohnende, reizvolle Aufgabe. Die Lösung dürfte auch nicht so schwierig sein, wie für die in § 3,8, II, III aufgeführten Primzahlfragen, die im Vergleich zu der hier gestellten, algebraisch-zahlentheoretisch fundierten, von transzendenter Natur sind.

Einen Zugang zur Lösung könnte man vielleicht finden, indem man die Klasseneinteilung der Primzahlen $p \equiv 1 \bmod 3$ auf alle nicht durch 3 teilbaren Führer f kubischer Restklassencharaktere χ, also

auf alle Produkte aus lauter verschiedenen solchen Primzahlen verallgemeinert. Für einen Führer $f = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ mit n verschiedenen Primfaktoren $\mathfrak{p}_\nu \equiv 1 \bmod 3$ gibt es nach § 13,6 im ganzen 2^{n-1} Paare konjugiert-komplexer kubischer Restklassencharaktere $\chi_\nu, \bar{\chi}_\nu$, die den 2^{n-1} verschiedenen Zerlegungen $f = \frac{a_\nu^2 + 27 b_\nu^2}{4}$ mit $a_\nu \equiv 1 \bmod 3$, $b_\nu > 0$ zugeordnet sind. Es handelt sich demnach um eine Klasseneinteilung nicht der Führer f allein, sondern der Paare f, a_ν, je nachdem, auf welchem Sektor des Kreises vom Radius $\sqrt{f}$ um 0 die zugehörige normierte Gaußsche Summe $\tau(\chi_\nu)$ liegt. Sofern für diese Klasseneinteilung ein arithmetisches Gesetz vorliegt, ist anzunehmen, daß es leichter zugänglich ist als bei alleiniger Berücksichtigung der Primzahlführer $f = p$, ebenso wie ja die Tatsache, daß alle Zahlen einer primen Restklasse mod. m die Dichte $\frac{1}{\varphi(m)}$ haben (§ 4,8), leichter zu beweisen (ja trivial!) ist als bei Beschränkung auf Primzahlen (§ 14,4). Entsprechendes gilt übrigens auch für das nachher in 7 zu behandelnde biquadratische Analogon der Kummerschen Vermutung. Die arithmetischen Grundlagen über zyklische kubische und biquadratische Zahlkörper, die man zu dieser erweiterten Klasseneinteilung benötigt, habe ich ausführlich in einer kürzlich erschienenen größeren Abhandlung auseinandergesetzt, die sich an meine in § 18,3 zitierte Monographie anschließt[1]). Man würde zweckmäßig damit beginnen, sich durch numerische Nachprüfung hinreichend vieler Führer f ein Bild von dem zu erwartenden Ergebnis zu verschaffen.

Wir wollen jetzt noch die Kummersche Klasseneinteilung auf eine mehr elementare Art beschreiben. Es zeigt sich nämlich, daß man zu ihrer Definition die normierte Primzerlegung (1.) von $\mathfrak{p}$ in P_3 nur in ihrer rationalen Form braucht, und nicht auch die auf die algebraische Zahl π und die algebraischen Werte von χ bezüglichen Normierungsvorschriften (2.) und (3.).

Wie sofort ersichtlich (s. o., Abb. 27), sind nämlich die drei Klassen $\mathfrak{p}_1, \mathfrak{p}_3, \mathfrak{p}_5$ bereits dadurch unterschieden, daß für sie der doppelte Realteil

(4.) $$\eta = \tau(\chi) + \tau(\bar{\chi})$$

in den (offenen) Intervallen

(5.) $$\underset{(\text{Klasse } \mathfrak{p}_3)}{-2\sqrt{p} \cdots -\sqrt{p}} \qquad \underset{(\text{Klasse } \mathfrak{p}_5)}{-\sqrt{p} \cdots \sqrt{p}} \qquad \underset{(\text{Klasse } \mathfrak{p}_1)}{\sqrt{p} \cdots 2\sqrt{p}}$$

liegt. Hierfür spielt aber die Unterscheidung zwischen den Konjugierten $\chi, \bar{\chi}$ und $\pi, \bar{\pi}$ keine Rolle. Diese Unterscheidung in Gestalt der obigen Normierungen (2.), (3.) braucht man erst, wenn man über die Klasseneinteilung hinaus die zum Ausgang genommene Frage nach den beiden einzelnen Werten $\tau(\chi), \tau(\bar{\chi})$ beantworten will, während ihre Summe η,

[1]) H. Hasse: Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern. — Abh. Deutsche Akad. d. Wiss. Berlin, Jahrgang 1948, Nr. 2, Berlin 1950.

Inneren des betreffenden Kreisbogens (Abb. 27). Demgemäß führt unsere Frage zu einer Einteilung aller Primzahlen $p \equiv 1 \bmod 3$ in

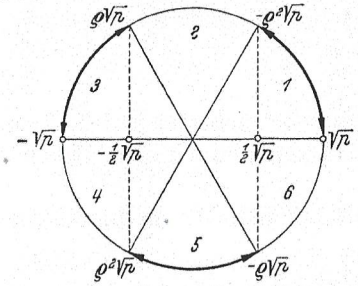

Abb. 27.

drei Klassen $\mathfrak{p}_1$, $\mathfrak{p}_3$, $\mathfrak{p}_5$,

je nachdem, ob die π wie angegeben zugeordnete normierte Gaußsche Summe

$\tau(\chi)$ im 1., 3., 5. Sextanten

der komplexen Zahlenebene liegt.

Es erhebt sich die Frage, ob es ein arithmetisches Gesetz gibt, nach dem von einer gegebenen Primzahl $p \equiv 1 \bmod 3$ entschieden werden kann, welcher der drei Klassen $\mathfrak{p}_1$, $\mathfrak{p}_3$, $\mathfrak{p}_5$ sie angehört, und wie gegebenenfalls dieses Gesetz beschaffen ist. Auf diese Frage kennt man bis heute keine Antwort.

Zur Verhütung einer falschen Vorstellung und zur Beleuchtung des Sachverhalts bemerken wir, daß die drei Klassen $\mathfrak{p}_1$, $\mathfrak{p}_3$, $\mathfrak{p}_5$ im kubischen Falle nicht etwa das Analogon der im quadratischen Falle hervortretenden beiden Typen $p \equiv \pm 1 \bmod 4$ ($p^* \lesseqgtr 0$) sind. Vielmehr liegen, vom kubischen Falle her gesehen, die Verhältnisse im quadratischen Falle folgendermaßen. Für jeden der beiden Typen ist aus $\tau(\chi)^2 = p^*$ klar, daß $\tau(\chi)$ eine der beiden Quadratwurzeln $\sqrt{p^*}$ ist. Die beiden zugehörigen Punkte auf dem Kreis vom Radius $\sqrt{p}$ um 0 sind hier das Analogon der obigen drei Sektoren. Vor Kenntnis der Vorzeichenbestimmung kann man demgemäß sagen, daß alle ungeraden Primzahlen p (ohne Rücksicht auf den Typus $p \equiv \pm 1 \bmod 4$) in zwei Klassen $\mathfrak{p}_1$, $\mathfrak{p}_3$ zerfallen, je nachdem $\tau(\chi)$ der rechte/obere oder der linke/untere Punkt ist, oder also, je nachdem $\tau(\chi)$ im 1. oder 3. Quadranten (Rand eingeschlossen!) der komplexen Zahlenebene liegt. Die Frage, ob diese Klasseneinteilung von einem Gesetz beherrscht wird, wird hier durch die Vorzeichenbestimmung in 5, XI bejaht. Das Gesetz besagt, daß alle ungeraden Primzahlen p der Klasse $\mathfrak{p}_1$ angehören, während die Klasse $\mathfrak{p}_3$ leer ist.

Wenn man nun in Analogie zu dieser Sachlage im quadratischen Falle erwarten sollte, daß etwa auch im kubischen Falle alle Primzahlen $p \equiv 1 \bmod 3$ einer einzigen jener drei Klassen $\mathfrak{p}_1$, $\mathfrak{p}_3$, $\mathfrak{p}_5$ angehören, so wird man um so mehr durch den wirklichen Sachverhalt überrascht, den Kummer durch numerische Nachprüfung der 45 Primzahlen $p \equiv 1 \bmod 3$ mit $p < 500$ festgestellt hat. Er fand

24 Primzahlen $\mathfrak{p}_1 =$ 7, 31, 43, 67, 73, 79, 103, 127, 163, 181, 223, 229, 271, 277, 307, 313, 337, 349, 409, 421, 439, 457, 463, 499.

14 Primzahlen $\mathfrak{p}_5 =$ 13, 19, 37, 61, 109, 157, 193, 241, 283, 367, 373, 379, 397, 487.

7 Primzahlen $\mathfrak{p}_3 =$ 97, 139, 151, 199, 211, 331, 433.

Da das Verhältnis 24:14:7 der Anzahlen in den drei Klassen ungefähr 3:2:1 ist, hat Kummer auf Grund dieses allerdings nicht sehr umfangreichen numerischen Materials die Vermutung ausgesprochen:

Kummersche Vermutung. *In jeder der drei Klassen $\mathfrak{p}_1$, $\mathfrak{p}_5$, $\mathfrak{p}_3$ gibt es unendlich viele Primzahlen, und die drei Klassen haben die Dichten* $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{6}$.

Hinsichtlich des Dichtebegriffs verweisen wir auf unsere Ausführungen in §14, 4.

Auch diese Vermutung ist bis heute weder bestätigt noch widerlegt worden. Ihre Bestätigung würde natürlich noch nicht eine Bejahung der obigen Frage nach einem arithmetischen Gesetz für die Klasseneinteilung $\mathfrak{p}_1$, $\mathfrak{p}_3$, $\mathfrak{p}_5$ bedeuten, aber doch das Vorhandensein eines solchen Gesetzes nahelegen, und ihre Widerlegung würde noch nicht ausschließen, daß dennoch ein solches Gesetz besteht.

Von besonderer Bedeutung erscheint die Bestätigung der Kummerschen Vermutung angesichts der folgenden Tatsache, die wir hier nur als Ergebnis mitteilen können. Wenn auch das Zerlegungsgesetz für endlich-algebraische Zahlkörper bisher nur im absolut-abelschen Falle (§19, 2) und für solche weiteren Körper K bekannt ist, die sich in von P aus übereinander getürmte relativ-abelsche Zahlkörper einbetten lassen, so weiß man doch allgemein, daß die Primzahlmengen der endlich vielen möglichen unverzweigten Zerlegungstypen unendlich sind und gruppentheoretisch bestimmte Dichten haben[1]). Man könnte demgemäß auf den Gedanken kommen, daß die Kummersche Klasseneinteilung das Zerlegungsgesetz in einem geeigneten algebraischen Zahlkörper widerspiegelt. In der Tat gibt es Zahlkörper, deren Primzahlzerlegungstypen gerade die von Kummer vermuteten Dichten $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{6}$ haben, und zwar leisten dies genau alle nicht-abelschen kubischen Zahlkörper K; diese sind unter allen kubischen Zahlkörpern überhaupt dadurch gekennzeichnet, daß ihre Diskriminante D keine Quadratzahl ist[2]). Sie lassen sich in zwei übereinandergetürmte relativ-abelsche Zahlkörper einbetten, deren unterer der quadratische Zahlkörper $\mathsf{P}(\sqrt{D})$ ist, während der obere, ihr zugehöriger galoisscher Körper, kubisch relativ-zyklisch über $\mathsf{P}(\sqrt{D})$ ist. Das Zerlegungsgesetz ist demnach bekannt. Es gibt drei unverzweigte Zerlegungstypen, nämlich

$$p \cong \mathfrak{p}\mathfrak{p}'\mathfrak{p}'' \text{ (Grade 1)}, \quad p \cong \mathfrak{p} \text{ (Grad 3)}, \quad p \cong \mathfrak{p}\mathfrak{p}' \text{ (Grade 1, 2)},$$

wo die in Klammern beigefügten Zahlen die Restklassengrade (Norm-

[1]) Siehe etwa meinen in § 19, 2 zitierten Bericht, Teil II, § 24.

[2]) Für die hier herangezogenen Tatsachen über kubische Zahlkörper müssen wir auf die Literatur verweisen. Siehe etwa H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. Math. Ztschr. 31 (1930), 565—582.

des (vom Grade $p-1$ zyklischen) Einheitswurzelkörpers P_p, und zwar handelt es sich um die Lagrangesche Resolvente des in 3, (3.) definierten erzeugenden Elements

$$\vartheta = \sum_{\substack{x \bmod p \\ \chi(x)=1}} \zeta^x = \frac{1}{k} \sum_{y \not\equiv 0 \bmod p} \zeta^{y^k},$$

der *normierten p-ten Kreisteilungsperiode vom Grade k*. Nach 4, (5.) ist die k-te Potenz

$$\tau(\chi)^k = \omega(\chi) = \chi(-1)\, p \prod_{x \not\equiv 0,\ -1 \bmod k} \pi(\chi, \chi^x)$$

als Zahl des (gegenüber $\mathsf{P}_k\,\mathsf{P}_p$ niederen) Einheitswurzelkörpers P_k algebraisch bekannt, und zwar ist diese Zahl unabhängig von der Normierung von ζ, da sie ja bei allen Automorphismen $\zeta \to \zeta^a$ von $\mathsf{P}_k\mathsf{P}_p/\mathsf{P}_k$ invariant ist. Dadurch ist die Zahl $\tau(\chi) = \sqrt[k]{\omega(\chi)}$ aus $\mathsf{P}_k\,\mathsf{P}_p$ genau k-deutig bestimmt. Die k verschiedenen Werte der k-ten Wurzel entsprechen wegen $\tau(\chi) \to \bar{\chi}(a)\,\tau(\chi)$ bei $\zeta \to \zeta^a$ umkehrbar eindeutig den durch die k Werte von χ unterschiedenen Nebenklassen nach der Untergruppe der k-ten Potenzreste mod. p.

Legt man nun wieder die analytische Normierung $\zeta = e^{\frac{2\pi i}{p}}$ zugrunde, so erhebt sich die Frage, *welcher der k verschiedenen k-ten Wurzeln aus der bekannten Zahl $\omega(\chi)$ die Zahl $\tau(\chi)$ gleich ist.*

Diese Frage ist wieder wesentlich analytischer Natur. Zu ihrer präzisen Formulierung reicht die bloß algebraische Kenntnis von $\omega(\chi)$ als Zahl aus P_k nicht aus; man muß vielmehr $\omega(\chi)$ auch analytisch, d. h. als komplexe Zahl kennen, um ihre k-ten Wurzeln überhaupt unterscheiden zu können. Diese Schwierigkeit trat im Spezialfall $k=2$ nicht auf, weil dort $\omega(\chi) = \chi(-1)\, p = p^*$ rational und damit trivialerweise als komplexe Zahl bekannt ist. Sie kann behoben werden, indem man für $\omega(\chi)$ eine arithmetische Kennzeichnung von der Art gibt, wie wir das in 4 für die Spezialfälle $k = 3, 4, 6$ getan haben; die dortigen arithmetischen Kennzeichnungen legen ja $\omega(\chi)$ ersichtlich auch als komplexe Zahl fest.

Nun kennt man zwar auch für beliebige Ordnung k eine arithmetische Kennzeichnung von $\omega(\chi)$, nämlich durch Angabe einerseits der Primdivisorzerlegung in P_k und andrerseits der zu 5, (6.) analogen Kongruenzeigenschaft; diese Angaben legen, zusammen mit der Tatsache, daß $|\omega(\chi)| = \sqrt{p^k}$ ist, die Zahl $\omega(\chi)$ eindeutig fest[1]). Damit ist jedoch im allgemeinen nicht wie in jenen Spezialfällen $\omega(\chi)$ als komplexe Zahl bekannt, nämlich deshalb nicht, weil die Primdivisorzerlegung in P_k im allgemeinen nicht eine Primzahlzerlegung ist. Nur wenn letzteres der Fall ist, d. h. *nur wenn der Einheitswurzelkörper P_k die Klassenzahl $h=1$ hat, kann man demnach auf diese Weise zu einer Kenntnis von $\omega(\chi)$*

[1]) Siehe dazu die in 4 zitierte Arbeit von Davenport-Hasse.

als komplexe Zahl und damit zu einer präzisen Formulierung der obigen Fragestellung gelangen. Für die Spezialfälle

$$k = 3, 4, 6 \text{ mit } \mathsf{P}_3 = \mathsf{P}_6 = \mathsf{P}(\sqrt{-3}) \text{ bzw. } \mathsf{P}_4 = \mathsf{P}(\sqrt{-1})$$

trifft das zu.

Wir wenden uns nunmehr dem von Kummer betrachteten kubischen Fall $k=3$ zu; auf die Fälle $k=6$ und $k=4$ kommen wir anschließend in 7 zu sprechen.

Nach 4, (10b.), (11b_2.) hat man im kubischen Falle die arithmetische Kennzeichnung

$$\tau(\chi)^3 = p\pi, \qquad \tau(\bar{\chi})^3 = p\bar{\pi}$$

mit

$$\text{(1.)} \qquad \left\{ \begin{array}{l} \pi, \bar{\pi} = \dfrac{a \pm 3b\sqrt{-3}}{2}; \quad a \equiv 1 \bmod 3 \\ \\ p = \dfrac{a^2 + 27b^2}{4} \end{array} \right\}.$$

An Stelle einer arithmetischen Unterscheidung der beiden Konjugierten $\pi, \bar{\pi}$, die man, analog zu der in §18, 5, (29.) für den biquadratischen Fall gegebenen, auch hier durchführen kann, braucht man für die zu behandelnde Frage die durch die Vorschrift

$$\text{(2.)} \qquad \pi \text{ positiv-imaginär}, \quad \text{also } b>0$$

gegebene analytische Unterscheidung. Es genügt, die eine, π zugeordnete Gaußsche Summe $\tau(\chi)$ zu betrachten, da dann die andere $\tau(\bar{\chi})$ als die Konjugiert-komplexe bestimmt ist. Ganz analog, wie in §18, 5, (28.) für den biquadratischen Fall, zeigt man auch hier, daß diese umgekehrte Zuordnung von χ und damit $\tau(\chi)$ zu π durch das *verallgemeinerte Eulersche Kriterium*

$$\text{(3.)} \qquad \chi(x) \equiv x^{\frac{p-1}{3}} \bmod \pi$$

gegeben ist.

Nach alledem kann unsere Fragestellung wie folgt präzise formuliert werden:

Sei eine Primzahl $p \equiv 1$ mod. 3 gegeben, sei (1.) *ihre normierte Primzerlegung in P_3, und sei χ der dem nach* (2.) *normierten Primfaktor π gemäß* (3.) *zugeordnete kubische Restcharakter mod. p.*

Welcher der drei komplexen Zahlen $\sqrt[3]{p\pi}$ ist dann die normierte Gaußsche Summe $\tau(\chi)$ gleich?

Bei der Normierung (2.) liegen nun die drei Kubikwurzeln

$$\sqrt[3]{p\pi} \text{ im 1., 3., 5. Sextanten}$$

der komplexen Zahlenebene, und zwar wegen $|\pi| = \sqrt{p}$ auf dem Kreise vom Radius $\sqrt{p}$ um o, und wegen der Nichtrealität von π jeweils im

Setzt man daher

$$\frac{1}{\mu!} = \frac{g_\mu}{m!} \qquad (\mu = 0, 1, \ldots, m)$$

mit ganzrationalen g_μ, so werden die ganzen Zahlen

$$\binom{x}{\mu} \equiv -(-1)^m m!\, g_\mu\, x(x-1) \cdots (x-(\mu-1)) \bmod p,$$

wo nunmehr rechts ganzzahlige Polynome μ-ten Grades stehen und insbesondere $g_m = 1$ ist. Diese Kongruenzwerte der $\binom{x}{\mu}$ mod. p dürfen in die für $\tau(\chi)$ mod. π^{m+1} erhaltene Kongruenz eingetragen werden; es wird also

$$\tau(\chi) \equiv -(-1)^m m! \cdot \sum_{\mu=0}^{m} \Big(\sum_{x \bmod p} x^m \cdot x(x-1) \cdots (x-(\mu-1))\, g_\mu (-1)^\mu \pi^\mu \Big) \bmod \pi^{m+1}.$$

Denkt man die Polynome $(m+\mu)$-ten Grades in der inneren Summe entwickelt und wendet die Formeln aus §10, 4 für den Kongruenzwert der Summen $\sum_{x \bmod p} x^r$ mod. p (mit $r \geqq 1$) an, so bleibt nur für $\mu = m$ ein Beitrag $\not\equiv 0$ mod. p stehen, nämlich der vom höchsten Glied herrührende Beitrag -1 mod. p. So ergibt sich unter Beachtung von $g_m = 1$ der gesuchte Kongruenzwert zu

$$\tau(\chi) \equiv m!\, \pi^m \bmod \pi^{m+1}. \tag{6.}$$

Der Vergleich der Ergebnisse (5.) und (6.) zeigt, daß in der Tat die Kongruenz (3.) mit $\omega = \pi^{m+1}$ besteht.

Daß auch die Bedingung (4.) für $\omega = \pi^{m+1}$ erfüllt ist, ersieht man daraus, daß sonst $2\delta \equiv 0$ mod. π^{m+1}, also auch

$$\delta \equiv (p+1)\,\delta \equiv \frac{p+1}{2} \cdot 2\delta \equiv 0 \bmod \pi^{m+1}$$

wäre, entgegen der zuvor festgestellten Tatsache, daß δ nicht mehr durch π^{m+1} teilbar ist.

Nach dem Gesagten ist damit die Gleichung (2.) bewiesen und der Beweis von XI vollendet.

In dieser auf KRONECKER zurückgehenden Bestimmung des Vorzeichens der normierten eigentlichen quadratischen Gaußschen Summe ist, wie hervorgehoben, die Rolle der Analysis auf den Schluß beschränkt, daß der Ausdruck

$$\zeta_2^x - \zeta_2^{-x} = 2i \sin\left(\frac{2\pi x}{p}\,\frac{p+1}{2}\right) = 2i \sin\left(\frac{\pi x}{p} + \pi x\right)$$

für $x = 1, \ldots, \frac{p-1}{2}$ abwechselnd negativ- und positiv-imaginär ist. Es gibt auch andere Beweise für die Vorzeichenregel XI, bei denen im Gegenteil die Rolle der Arithmetik möglichst weitgehend zurückgedrängt

oder sogar völlig durch analytische Schlußweisen ersetzt ist, welch' letztere dann allerdings nicht mehr denselben elementaren Charakter wie die eben angegebene analytische Tatsache haben. So hat man die Theorie der Fourierschen Reihen und auch Integrale für diesen Beweis herangezogen.

Während wir uns im ersten reduzierenden Teil des Beweises auf das quadratische Reziprozitätsgesetz gestützt haben, hat schon GAUSS selbst umgekehrt diesen Zusammenhang zu einem Beweise des quadratischen Reziprozitätsgesetzes benutzt, der sich auf eine für quadratische Charaktere mit beliebigem Führer durchgeführte, analytische Vorzeichenbestimmung seiner Summen stützt.

6. Die Kummersche Vermutung für kubische Charaktere nach einem Primzahlmodul.

Der Leser wird sich längst gesagt haben, daß die eben in 5 für die Gaußschen Summen $\tau(\chi)$ zu quadratischen Charakteren χ behandelte Fragestellung nicht auf diesen Spezialfall $k=2$ beschränkt ist, sondern ihr Analogon auch für die Gaußschen Summen $\tau(\chi)$ zu Charakteren χ von höherer Ordnung $k \geqq 3$ haben wird. Das ist in der Tat der Fall. Jedoch ist dann einerseits schon die Formulierung der Frage mit arithmetischen Schwierigkeiten verbunden, die wir nachher kurz streifen werden; und andrerseits ist ihre Beantwortung bisher nicht einmal im nächsthöheren Fall $k=3$ der kubischen Charaktere gelungen.

Das Einzige, was bisher in dieser Hinsicht vorliegt, ist eine von KUMMER für die kubischen Gaußschen Summen nach einem Primzahlmodul $p \equiv 1$ mod. 3 ausgesprochene, interessante Vermutung, die allerdings wenig Beachtung gefunden hat, obwohl ihre Bearbeitung für die Zahlentheorie vielleicht fruchtbarer wäre, als die Bemühungen so vieler Fachleute und Laien um die große Fermatsche Vermutung (§ 3, 8). Wir wollen diese Vermutung hier im Anschluß an die bereits in 4 über die kubischen Gaußschen Summen gewonnenen Ergebnisse herausarbeiten und sie auch in eine von den dortigen arithmetischen Begriffsbildungen freie, ganz elementare Form setzen.

Wir beginnen mit der allgemeinen Aufrollung der Fragestellung. Es sei χ ein Charakter der Ordnung $k \geqq 3$, von dem wir auf Grund der Komponentenzerlegung 2, VI und nach der Schlußbemerkung in 3 ohne wesentliche Einschränkung voraussetzen können, daß der Führer eine Primzahl $p \equiv 1$ mod. k ist. Nach 3, VII ist dann die normierte eigentliche Gaußsche Summe

$$\tau(\chi) = \sum_{x \bmod p} \chi(x)\, \zeta^x$$

eine Lagrangesche Resolvente für den einzigen zyklischen Teilkörper k-ten Grades

$$\mathsf{K} = \mathsf{P}(\vartheta)$$

Berichtigung.

S. 17, Zeile 12 v. o. lies: $aA = bB = \dots$

S. 23, Zeile 16 v. u. lies: nach

S. 51, Zeile 11 v. u. lies: vorkommt

S. 62, Zeile 3 v. u. lies: $\dots + \frac{a_k}{m^k}$

S. 63, Zeile 4 v. o. lies: $a_1 \cdots a_k$

S. 98, Zeile 5 v. o. lies: $\prod_{q \neq 2}$

S. 109, Zeile 16 v. u. lies: § 19, 3

S. 137, Zeile 19 v. o. lies: $\chi_p(-1) =$ oder -1

S. 175, Zeile 1 v. u. lies: $\prod_{t \mid m}$

S. 177, Zeile 10 v. o. lies (2 mal): p_r

S. 178, Zeile 4 v. o. lies: $q^\mu \mid \varphi(p)$

S. 178, Zeile 5 v. u. lies: $x^m - 1 = \prod_{a \bmod m} (x - \zeta^a)$

S. 217, Zeile 19 v. o. lies: außerdem

S. 232, Abb. 6b setze über die rechte Vertikale: $\underline{mod.\ m_p}$

S. 238, Zeile 15 v. o. lies: mit wachsendem n

S. 242, Zeile 1 v. u. lies: (3.)

S. 243, Zeile 6 v. o. lies: $\int_1^x$

S. 254, Zeile 13 v. u. lies: $\sum_n$

S. 257, Zeile 4 v. u. lies: $\sum_{x \bmod f} \zeta_f^{x(l-1)}$

S. 281, Zeile 3 v. o. lies: $\frac{\omega_1 - \omega_1'}{2}$

S. 287, Zeile 19 v. o. lies: letzteren

S. 311, Zeile 24 v. o. lies: befriedigt

S. 344, Zeile 9 v. o. lies: e_p

S. 378, Abb. 23 (unten) lies: ζ^{-x}

S. 382, Zeile 6 v. o. lies: 2^{-k_0+1}

S. 403, Zeile 10 v. o. lies (2 mal): $\prod_{x=1}^{2n}$

S. 413, Zeile 4 v. u. lies: $\mathfrak{G}/\mathfrak{H}$

S. 428, Zeile 3 v. u. lies: (g_i, m_i)

Erster Abschnitt.

Grundlagen.

§ 1. Primzerlegung.

1. Natürliche, ganze und rationale Zahlen.

Gegenstand der elementaren Zahlentheorie sind in erster Linie die *natürlichen Zahlen* 1, 2, 3, ... Nach KRONECKER hat sie der liebe Gott geschaffen, nach DEDEKIND der menschliche Geist. Das ist je nach Weltanschauung ein unlösbarer Widerspruch oder ein und dasselbe. Für die Zahlentheorie ist es gleichgültig, wer die natürlichen Zahlen geschaffen hat. Sie stellt sich auf den Standpunkt, daß sie jedenfalls da sind und uns wohlbekannt sind.

Wir wollen etwas genauer sagen, was wir hier mit dem Wohlbekanntsein meinen. Wir setzen als bekannt voraus: 1. die Definitionen und die Gesetze des Rechnens mit den natürlichen Zahlen nach den drei ersten elementaren Rechenoperationen (Addition, Subtraktion, Multiplikation) und auch nach der vierten (Division), soweit diese im Bereich der natürlichen Zahlen ausführbar ist, 2. die Definitionen und die Gesetze der Anordnung der natürlichen Zahlen nach ihrer Größe, 3. die zwischen dem Rechnen und der Anordnung bestehenden Gesetze (wie Größeres mit Größerem addiert oder multipliziert gibt Größeres).

Wir setzen hier ferner auch als bekannt voraus die Erweiterung des Bereichs der natürlichen Zahlen zu dem in bezug auf die ersten drei elementaren Rechenoperationen geschlossenen *Integritätsbereich* $\mathfrak{r}$ *der ganzen Zahlen*:

$$\dots, -3, -2, -1, 0, 1, 2, 3, \dots$$

und dessen Erweiterung zu dem in bezug auf die vier elementaren Rechenoperationen geschlossenen *Körper* $\mathfrak{P}$ *der rationalen Zahlen*:

$$0;\ \pm 1;\ \pm 2,\ \pm\tfrac{1}{2};\ \pm 3,\ \pm\tfrac{1}{3};\ \pm 4,\ \pm\tfrac{3}{2},\ \pm\tfrac{2}{3},\ \pm\tfrac{1}{4};\ \dots,$$

sowie die Übertragung der Anordnung (einschließlich des absoluten Betrages) nebst ihren Gesetzen auf diese Erweiterungen.

Die eingeführten Bezeichnungen $\mathfrak{r}$, $\mathfrak{P}$ für den Bereich der ganzen bzw. rationalen Zahlen werden wir durchweg ohne jedesmalige neue Erklärung verwenden.

§ 9. Die Jacobische Verallgemeinerung.

§ 10. Verteilungsfragen über quadratische Reste nach einer Primzahl.

Dritter Abschnitt.

Der Dirichletsche Primzahlsatz.

§ 11. Elementare Sonderfälle.

§ 12. Die Methode von Dirichlet.

§ 13. Die Charaktere endlicher abelscher Gruppen, Restklassencharaktere.

§ 14. Der Beweis von Dirichlet.

§ 15. Das Nichtverschwinden der L-Reihen.

Vierter Abschnitt.

Quadratische Zahlkörper.

§ 16. Elementare Teilbarkeitslehre.

§ 17. Divisorentheorie.

§ 18. Bestimmung der Klassenzahl.

§ 19. Quadratische Zahlkörper und quadratisches Reziprozitätsgesetz.

Inhaltsverzeichnis.

Erster Abschnitt.

Grundlagen.

§ 1. Primzerlegung.

§ 2. Größter gemeinsamer Teiler.

§ 3. Vollkommene Zahlen, Mersennesche und Fermatsche Primzahlen.

§ 4. Kongruenz, Restklassen.

§ 5. Die Struktur der primen Restklassengruppen.

Zweiter Abschnitt.

Quadratische Reste.

§ 6. Definition, Reduktionen, Kriterien.

§ 7. Das quadratische Reziprozitätsgesetz: Elementarer Beweis.

§ 8. Das quadratische Reziprozitätsgesetz: Beweis mit Gaußschen Summen.

DIE GRUNDLEHREN DER

MATHEMATISCHEN WISSENSCHAFTEN

IN EINZELDARSTELLUNGEN MIT BESONDERER BERÜCKSICHTIGUNG DER ANWENDUNGSGEBIETE

HERAUSGEGEBEN VON

W. BLASCHKE · R. GRAMMEL · E. HOPF · F. K. SCHMIDT
B. L. VAN DER WAERDEN

BAND LIX

VORLESUNGEN
ÜBER ZAHLENTHEORIE

VON

HELMUT HASSE

SPRINGER-VERLAG
BERLIN / GÖTTINGEN / HEIDELBERG
1950

VORLESUNGEN ÜBER ZAHLENTHEORIE

VON

HELMUT HASSE
O. PROFESSOR AN DER HUMBOLDT-UNIVERSITÄT
BERLIN

MIT 28 ABBILDUNGEN

SPRINGER-VERLAG
BERLIN / GÖTTINGEN / HEIDELBERG
1950