The Kummer conjecture, p-th cyclotomic polynomials, the zeta function at odd integers, and all that ...

A data collection

Klaus Braun
January 2025
riemann-hypothesis.de

(1) The Kummer conjecture

(2) Kummer's connection between p-th roots of unity and the zeta function at the odd negative integers

(3) Kummer's regular and irregular primes

(4) Hurwitz quaternions and symmetry groups

(5) separable-quadratic splitting fields of quaternion algebras

(6) the integer degree (or winding number) of functions of Sobolev class $H^{1/2}$ from the circle S^1 to itself

(7) The complexification (complex polarization) of $H_{1/2}$

(8) The zeros of the Digamma function $\Psi(x) = log'\Gamma(x)$

(9) Non-harmonic Fourier series theory and Riesz basis systems $\{e^{i\lambda_\nu t}\}_{\nu\in Z}$ e.g. defined by the negative zeros of the Digamma function

(10) First thoughs about a Hilbert space based circle method to enable proofs of the Goldbach and Kummer conjecture

Vorzeichenbestimmung für quadratische Charaktere und die Kummersche Vermutung für kubische Charaktere nach einem Primzahlmodus

Hasse Helmut

3. Begriffliche Bedeutung der eigentlichen Gaußschen Summen

(HaH) p. 436: Da wir den quadratischen Fall bereits abgetan haben, bleibt somit als Kern unserer Aufgabe die explizite Bestimmung von $(\tau(\chi))^k = \omega(\chi)$ als Zahl aus $\boldsymbol{P}_k$ für Charaktere χ einer Ordnung $k \geq 3$ der primen Resklassengruppe nach einer ungeraden Primzahl $p = 1\ mod.k$.

In den Fällen, wo wir den Einheitswurzelkörper $\boldsymbol{P}_k$ auch arithmetisch beherrschen, werden wir darüber hinaus auch eine arithmetische Kennzeichnung der Zahl $\omega(\chi)$ aus $\boldsymbol{P}_k$ geben. Es sind das, da wir die Grundlagen der Arithmetik in diesem Buche in extenso nur für quadratische Zahlkörper entwickelt haben, die Fälle wo $\boldsymbol{P}_k$ quadratisch ist, also $k = 3{,}4{,}6$ mit $\boldsymbol{P}_3 = \boldsymbol{P}_6 = \boldsymbol{P}(\sqrt{-\mathbf{3}})$, $\boldsymbol{P}_4 = \boldsymbol{P}(\sqrt{-\mathbf{1}})$.

5. Vorzeichenbestimmung für quadratische Charaktere

(HaH) p. 447: Behauptung XI: Bei der analytischen Normierung $\zeta = e^{\frac{2\pi i}{f}}$ und $\sqrt{f} > 0$ gilt für die einem quadratischen Charakter χ von natürlichem Führer f zugeordnete normierte eigentliche Gaußsche Summe die Vorzeichnenbestimmung

$$\tau(\chi) = \sum_{x\ mod.f} \chi(x)\zeta^x = \begin{cases} \sqrt{f} & \text{für } \chi(-1)=1 \\ i\sqrt{f} & \text{für } \chi(-1)=-1 \end{cases}.$$

(HaH) p. 452: In dieser auf Kronecker zurückgehende Bestimmung des Vorzeichens der normierten eigentlichen quadratischen Gaußschen Summe ist, wie hervorgehoben, die Rolle der Analysis auf den Schluß beschränkt, daß der Ausdruck

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

für $x = 1, \dots, \frac{p-1}{2}$ 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 Reziprozitätgesetzes 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 Primzahlmodus

(HaH) p. 453: Der Leser wird sich längst gefragt haben, daß die eben in 5 (*5. Vorzeichenbestimmung für quadratische Charaktere*) 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 $k \geq 3$ 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 andererseits 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 $p = 1 mod. 3$ 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 gewonnenen Ergebnisse herausarbeiten und sie auch in eine von den dortigen arithmetischen Begriffsbildungen freie, ganz elementare Form setzen.

Wir beginnen mit der allgmeinen Aufrollung der Fragestellung. Es sei χ ein Charakter der Ordnung $k \geq 3$, 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 $p = 1 mod. k$ ist. Nach 3, VII ist dann die normierte eigentliche Gaußsche Summe

$$\tau(\chi) = \sum_{x\ mod.p} \chi(x)\zeta^x$$

Eine Lagrangesche Resolvente für den einzigen zyklischen Teilkörper k –ten Grades

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

des (vom Grade $p-1$ zyklischen) Einheitwurzelkörpers $\boldsymbol{P}_p$, und zwar handelt es sich um die Lagrangesche Resolvente des in 3,(3.) defininierten erzeugenden Elements

$$\vartheta = \sum_{\substack{x\ mod.p \\ \chi(x)=1}} \zeta^x = \frac{1}{k}\sum_{\substack{y\neq 0,-1\ mod.p \\ \chi(x)=1}} \zeta^{y^k}$$

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

$$\tau(\chi)^k = \omega(\chi) = \chi(-1)p \prod_{x\neq 0,-1 mod.k} \pi(\chi, \chi^x)$$

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

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

Diese Frage ist nun wieder wesentlich analytischer Natur. Zu ihrer präzisen Formulierung reicht die bloß algebraische Kenntnis von $\omega(\chi)$ als Zahl aus $\boldsymbol{P}_k$ 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 $\boldsymbol{P}_k$ 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. Damit ist jedoch im allgemeinen nicht wie in jenen Spezialfällen $\omega(\chi)$ als komplexe Zahl bekannt, nämlich deshalb nicht, weil die Primdivisorzerlegung in $\boldsymbol{P}_k$ im allgemeinen nicht eine Primzahlzerlegung ist. Nur wenn letzteres der Fall ist, d.h. nur wenn der Einheitswurzelköper $\boldsymbol{P}_k$ die Klassenzahl $h = 1$ hat, kann man demnach auf diese Weise zu einer Kenntnis von $\omega(\chi)$ als komplexe Zahl und damit zu einer präzisen Formulierung der obigen Fragestellung gelangen. Für die Spezialfälle

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

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.) hat man im kubischen Falle die arithmetische Kennzeichnung

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

mit

(1.)
$$\pi, \bar{\pi} = \frac{a \pm 3b\sqrt{-3}}{2},\ a = 1\ mod.3$$
$$p = \frac{a^2 + 27b^2}{4}\ .$$

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

(2.) π positiv-imaginär, 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 zu $\tau(\chi)$ zu π durch das *verallgemeinerte Eulersche Kriterium*

(3.) $$\chi(x) = x^{\frac{p-1}{3}} mod.\pi$$

gegeben ist.

Nach alledem kann unsere Fragestellung wie folgt präzise formuliert werden:

Sei eine Primzahl $p = 1\ mod.3$ gegeben, sei (1.) ihre normierte Primzerlegung in $\boldsymbol{P}_3$, 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

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

der komplexen Zahlenebene, und zwar wegen $|\pi| = \sqrt{p}$ auf dem Kreise vom Radius $\sqrt{p}$ um 0, und wegen der Nichtrealität von π jeweils im Inneren des betreffenden Kreisbogens (Abb. 27).

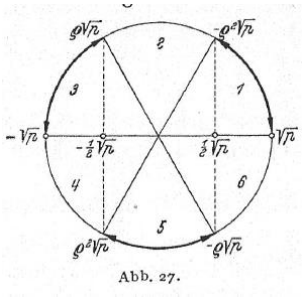

Abb. 27.

Demgemäß führt unsere Frage zu einer Einteilung aller Primzahlen $p = 1 mod. 3$ in drei Klassen p_1, p_3, p_5, je nachdem, ob die 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 $p = 1 mod. 3$ entschieden werden kann, welcher der drei Klassen p_1, p_3, 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 Sachverhaltes bemerken wir, daß die drei Klassen p_1, p_3, p_5 im kubischen Falles nicht etwas das Analog der im quadratrischen Fall hervortretenden beiden Typen $p = \pm 1 \, mod. 4$ ($p^* \lesseqgtr 0$) sind. Vielmehr legen, 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 $p = \pm 1 \, mod. 4$) in zwei Klassen p_1, 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. Quadtranten (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 p_1 angehören, während die Klasse 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 $p = 1 \, mod. 3$ einer einzigen jener drei Klassen p_1, p_3, p_5 angehören, so wird man um so mehr durch den wirklichen Sachverhalt überrascht, den KUMMER durch numerische Nachrüfung der 45 Primzahlen $p = 1 \, mod. 3$ mit $p < 500$ festgestellt hat. Er fand

24 Primzahlen

$$p_1 = 7,31,43,67,73,79,103,127,163,181,223,229,271,277,307,313,337,349,409,421,439,457,463,499,$$

14 Primzahlen

$$p_2 = 13,19,37,61,109,157,193,241,283,367,373,379,397,487,$$

7 Primzahlen

$$p_3 = 97,139,151,199,211,331,433,$$

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 $p_1, p_5 \, p_3$ gibt es unendlich viele Primzahlen, und die drei Klassen haben die Dichten $\frac{1}{2}, \frac{1}{3}, \frac{1}{6}$.*

Hinsichtlich des Dichtebegriffes verweise 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 p_1, p_3, 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 $\boldsymbol{K}$ bekannt ist, die sich in von $\boldsymbol{P}$ 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. 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 Zalhkörper $\boldsymbol{K}$; diese sind unter allen kubischen Zahlkörpern überhaupt dadurch gekennzeichnet, daß ihre Diskriminanten D keine Quadratzahl ist. Sie lassen sich in zwei übreinandergetürmte relativ-abelsche Zahlkörper einbetten, deren unterer der quadratische Zahlkörper $\boldsymbol{P}(\sqrt{D})$ ist, während der obere, ihr zugehöriger galoisscher Körper, kubisch-zyklisch über $\boldsymbol{P}(\sqrt{D}$ ist. Das Zerlegungsgesetz ist demnach bekannt. Es gibt drei unverzweigte Zerlegungstypen, nämlich

$$p \cong \mathrm{pp'p''} \text{ (Grade 1)}, \; p \cong \mathrm{p} \text{ (Grade 3)}, \; p \cong \mathrm{pp'} \text{(Grade 1,2)},$$

wo die in Klammern beigefügten Zahlen die Restklassengrade (Normexponenten) bedeuten, und diese 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 nicht-abelschen kubischem Körper $\boldsymbol{K}$ widerspiegeln, so käme, da es sich bei ihr nur um die Primzahlen $p = 1\ mod.3$ 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 $p = 1\ mod.3$ besteht. Dadurch wird aber genau jeder rein-kubische erzeugbare Körper $\boldsymbol{K} = \boldsymbol{P}(\sqrt[3]{a})$ (D rational, keine Kubikzahl) und insbesondere der einzige solche ausgeschlossen, in dessen Diskriminante nur die Primzahl 3 steckt, nämlich der Körper $\boldsymbol{K} = \boldsymbol{P}(\sqrt[3]{3})$. Es müßte sich demnach um einen kubischen Zahlkörper $\boldsymbol{K}$ 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 $= 1mod.3$) zwar von der Kummerschen Klasseneinteilung, aber nicht von der des Zerlegungsgesetzes erfaßt; dieser Einwand würde wegfallen, falls alle diese Primzahlen $q = 1mod.3$ wären – sie müßten dann notwendig schon in der Diskriminante d des quadratischen Körpers $\boldsymbol{P}(\sqrt{D}) = \boldsymbol{P}(\sqrt{d})$ 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 $\boldsymbol{K}$ 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 primenRestklassen gebildete) Primzahlmengen zu kennen, die eine Dichte besitzen. So ist die Inangriffnahme der Kummerschen Vermutung sicherlich eine lohnende 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 tranzendenter Natur sind.

Einen Zugang zur Lösung könnte man vielleicht finden, indem man die Klasseneinteilung der Primzahlen $p = 1mod.3$ auf alle nicht durch 3 teilbaren Führer f kubischer Restklassencharaktere χ, also auf alle Produkte aus lauter verschiedenen solchen Primzahlen verallgemeinert. Für einen Führer $f = p_1 \cdots p_n$ mit n verschiedenen Primzahlen $p_k = 1mod.3$ gibt es nach §13,6 im ganzen 2^{n-1} Paare konjugiert-komplexer kubischer Restklassencharaktere $\chi_k, \bar{\chi}_k$, die den 2^{n-1} verschiedenen Zerlegungen $f = \frac{a_k^2 + 27 b_k^2}{4}$ mit $a_k = 1mod.3, \quad b_k > 0$ zugeordnet sind. Es handelt sich demnach um eine Klasseneinteilung nicht der Führer allein, sondern der Paare f, a_k je nachdem, auf welchem Sektor des

Kreises vom Radius $\sqrt{f}$ um 0 die zugehörige normierte Gaußsche Summe $\tau(\chi_k)$ 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 hinreichnend 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 Defintion die normierte Primzerlegung (1.) von p in $\boldsymbol{P_3}$ nur in ihrer rationalen Form braucht, und nicht auch 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.

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

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

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 $y \equiv 0 \bmod p$ 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

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

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

$$\eta^3 - 3p\,\eta - a\,p = 0. \tag{8.}$$

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. $p = 7$. Die absolut-kleinsten kubischen Reste sind $\pm 1 \bmod 7$. 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.

$p = 13$. Die absolut-kleinsten kubischen Reste sind ± 1, $\pm 5 \bmod 13$.

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:

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

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 über-

lagert 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

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

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). Setzt man

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

also

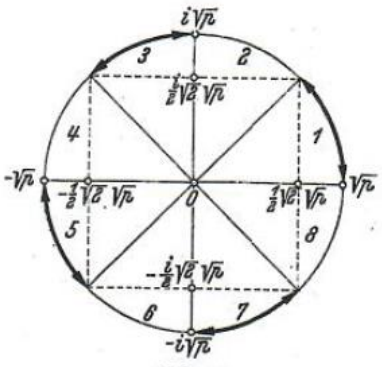

Abb. 28.

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

so kann über diese Einteilung ersichtlich auch dadurch entschieden werden, welchem der vier (offenen) Intervalle

$$-\sqrt{p} \ldots -\tfrac{1}{2}\sqrt{2}\sqrt{p} \qquad -\tfrac{1}{2}\sqrt{2}\sqrt{p} \ldots 0$$

(Klasse p_5) (Klasse p_3)

$$0 \ldots \tfrac{1}{2}\sqrt{2}\sqrt{p} \qquad \tfrac{1}{2}\sqrt{2}\sqrt{p} \ldots \sqrt{p}$$

(Klasse p_7) (Klasse p_1)

der Realteil

$$\varrho = \tfrac{1}{2}(\tau(\chi) + \tau(\bar{\chi})) \qquad \text{für } p \equiv 1 \bmod 8,$$

bzw. welchem der vier (offenen) Intervalle

$$-\sqrt{p} \ldots -\tfrac{1}{2}\sqrt{2}\sqrt{p} \qquad -\tfrac{1}{2}\sqrt{2}\sqrt{p} \ldots 0$$

(Klasse p_7) (Klasse p_5)

$$0 \ldots \tfrac{1}{2}\sqrt{2}\sqrt{p} \qquad \tfrac{1}{2}\sqrt{2}\sqrt{p} \ldots \sqrt{p}$$

(Klasse p_1) (Klasse p_3)

der Imaginärteil

$$\sigma = \tfrac{1}{2i}(\tau(\chi) + \tau(\bar{\chi})) \qquad \text{für } p \equiv 5 \bmod 8$$

angehört. Diese Reduktion auf die Summe

$$\eta = \tau(\chi) + \tau(\bar{\chi}) = \begin{cases} 2\varrho & \text{für } p \equiv 1 \bmod 8 \\ 2i\sigma & \text{für } p \equiv 5 \bmod 8 \end{cases}$$

erweist sich, wie wir sehen werden, für die numerische Durchführung der Entscheidung als zweckmäßig.

Es erhebt sich wieder die Frage, ob die so durch die Gegebenheiten (2.), (3.), (4.) eindeutig festgelegte Einteilung aller Primzahlen $p \equiv 1 \bmod 4$ jedes der beiden Typen $p \equiv 1, 5 \bmod 8$ in die vier Klassen p_1, p_3, p_5, p_7 durch ein arithmetisches Gesetz beherrscht wird, und wie gegebenenfalls dieses Gesetz beschaffen ist. Auch auf diese Frage kennt man bis heute keine Antwort.

Was die algebraische Bedeutung der Zahl η betrifft, so ist sie, wie gemäß 3,(7.) die Zahl

$$\vartheta = \tfrac{1}{4}(-1 + \sqrt{p} + \tau(\chi) + \tau(\bar{\chi})) = \tfrac{1}{4}(-1 + \sqrt{p} + \eta),$$

eine Erzeugende des (einzigen) zyklischen biquadratischen Teilkörpers K von P_p, dessen quadratischer Teilkörper notwendig $\mathsf{P}(\sqrt{p})$ ist. Nach den 4,(10a.) zugrunde liegenden Relationen hat man in der Tat

$$\begin{aligned} \eta^2 &= \tau(\chi)^2 + \tau(\bar{\chi})^2 + 2\tau(\chi)\tau(\bar{\chi}) \\ &= -\sqrt{p}(\pi^* + \bar{\pi}^*) + 2\chi(-1)p = -2a^*\sqrt{p} + 2\chi(-1)p, \end{aligned}$$

wo der dortigen Normierung (11a.) entsprechend $a^* = (-1)^{\frac{a-1}{2}} a$ und

$\pi^*, \bar{\pi}^* = (-1)^{\frac{a-1}{2}} (a \pm 2bi)$ zu verstehen ist. Demnach genügt η in bezug auf den quadratischen Teilkörper $\mathsf{P}(\sqrt{p})$ von K einer reinen quadratischen Gleichung. Für Realteil ϱ und Imaginärteil σ von $\tau(\chi)$ ergeben sich daraus nach (5.), den beiden Typen entsprechend, die über $\mathsf{P}(\sqrt{p})$ reinen quadratischen Gleichungen

$$\varrho^2 = \sqrt{p}\,\frac{-a^* + \sqrt{p}}{2} \quad \text{für } p \equiv 1 \bmod 8,$$

$$\sigma^2 = \sqrt{p}\,\frac{a^* + \sqrt{p}}{2} \quad \text{für } p \equiv 5 \bmod 8,$$

deren rechte Seite beidemal die Norm $b^2 p$ hat. Mit diesen Gleichungen ist eine algebraische Erzeugung des zyklischen biquadratischen Teilkörpers $\mathsf{K} = \mathsf{P}(\vartheta) = \mathsf{P}(\eta) = \mathsf{P}(\varrho)$ bzw. $\mathsf{P}(i\sigma)$ von P_p explizit angegeben.

Analytisch stellt sich die Zahl η in der Form

$$\eta = 2 \sum_{\substack{x \bmod p \\ \psi(x) = 1}} \chi(x) \zeta^x$$

dar, wo $\psi = \chi^2 = \bar{\chi}^2$ wieder den quadratischen Charakter mod. p bezeichnet; denn für $\psi(x) = 1$ ist $\chi(x) + \bar{\chi}(x) = 2\chi(x)$ und für $\psi(x) = -1$ ist $\chi(x) + \bar{\chi}(x) = 0$. Daraus ergeben sich für Realteil ϱ bzw. Imaginärteil σ von $\tau(\chi)$ nach (5.) die Darstellungen

$$\varrho = 2 \sum_{\substack{\pm x \bmod p \\ \psi(x) = 1}} \chi(x) \cos \frac{2\pi x}{p} \quad \text{für } p \equiv 1 \bmod 8,$$

$$\sigma = 2 \sum_{\substack{\pm x \bmod p \\ \psi(x) = 1}} \chi(x) \sin \frac{2\pi x}{p} \quad \text{für } p \equiv 5 \bmod 8.$$

Beispiele. $p = 5$. Die absolut-kleinsten quadratischen Reste sind $\pm 1 \bmod 5$, und es ist $\chi(1) = 1$. Daher wird

$$\sigma = 2 \sin \frac{2\pi}{5}.$$

Die einfache Abschätzung

$$\sigma = 2 \sin \frac{2\pi}{5} > 2 \sin \frac{2\pi}{6} = \sqrt{3} > \frac{1}{2}\sqrt{2}\sqrt{5}$$

zeigt hier ohne Zuhilfenahme von Tabellen, daß σ dem Intervall $\frac{1}{2}\sqrt{2}\sqrt{5} \ldots \sqrt{5}$, also 5 der Klasse p_3 angehört.

$p = 17$. Die absolut-kleinsten quadratischen Reste sind ± 1, ± 2, ± 4, $\pm 8 \bmod 17$, und es ist $\chi(1) = 1, \chi(2) = -1, \chi(4) = 1, \chi(8) = -1$. Daher wird

$$\varrho = 2\left[\cos \frac{2\pi}{17} - \cos \frac{4\pi}{17} + \cos \frac{8\pi}{17} - \cos \frac{16\pi}{17}\right].$$

Durch numerische Ausrechnung findet man, daß ϱ dem Intervall $0 \ldots \frac{1}{2}\sqrt{2}\sqrt{17}$, also 17 der Klasse p_7 angehört.

Auf meine Anregung hin hat KALUZA auf Grund dieser Formeln für die 37 Primzahlen $p \equiv 1 \bmod. 8$ und die 43 Primzahlen $p \equiv 5 \bmod. 8$ mit $p < 1000$ die Verteilung auf die Klassen p_1, p_3, p_5, p_7 numerisch bestimmt. Das Ergebnis ist in der nachstehenden Tabelle zusammengestellt.

Klasse/Typus	Primzahlen	Anzahlen	
$p_1 \equiv 1 \bmod. 8$	73, 113, 193, 409, 449, 521, 593, 673, 937, 977	10	21
$p_1 \equiv 5 \bmod. 8$	13, 109, 149, 229, 373, 397, 557, 797, 829, 853, 997	11	
$p_3 \equiv 1 \bmod. 8$	41, 97, 233, 281, 433, 809, 881, 953	8	23
$p_3 \equiv 5 \bmod. 8$	5, 37, 61, 181, 197, 269, 293, 389, 541, 613, 653, 661, 677, 757, 877	15	
$p_5 \equiv 1 \bmod. 8$	137, 241, 617, 761, 929	5	12
$p_5 \equiv 5 \bmod. 8$	53, 157, 317, 421, 461, 709, 733	7	
$p_7 \equiv 1 \bmod. 8$	17, 89, 257, 313, 337, 353, 401, 457, 569, 577, 601, 641, 769, 857	14	24
$p_7 \equiv 5 \bmod. 8$	29, 101, 173, 277, 349, 509, 701, 773, 821, 941	10	
$p \equiv 1 \bmod. 8$		37	80
$p \equiv 5 \bmod. 8$		43	

Dies numerische Material umfaßt zwar die doppelte Spanne wie das Kummersche. Immerhin erscheint es gewagt, auf Grund der Tatsache, daß das Anzahlverhältnis in den vier Klassen beider Typen zusammen (und nicht ganz so genau für die beiden Typen einzeln) ungefähr 2:2:1:2 ist, eine bestimmte Vermutung über die Dichten auszusprechen, zumal bei diesen Verhältnissen der dem biquadratischen Fall fremdartige Hauptnenner 7 auftreten würde. Jedenfalls möchte ich glauben:

Analogon zur Kummerschen Vermutung. *Für jeden der beiden Typen $p \equiv 1, 5 \bmod. 8$ gibt es in jeder der vier Klassen p_1, p_3, p_5, p_7 unendlich viele Primzahlen, und diese Klassen haben Dichten, die für beide Typen übereinstimmen.*

Kummer E. E.,
Eine Aufgabe betreffend die Theorie der cubischen Reste,

Journal für die reine und angewandte Mathematik, 23, S. 285-286, 1842

Eine Aufgabe, betreffend die Theorie der cubischen Reste

Journal für die reine und angewandte Mathematik 23, 285–286 (1842)

Wenn p eine Primzahl von der Form $3n+1$ ist, und g eine primitive Wurzel derselben, so kann die Reihe $1, g, g^2, g^3, \ldots g^{p-2}$ in drei verschiedene Reihen geordnet werden, nämlich $1, g^3, g^6, \ldots g^{p-4}$, ferner $g, g^4, g^7, \ldots g^{p-3}$ und $g^2, g^5, g^8, \ldots g^{p-2}$. Die Reste der ersten Reihe für den Modul p sind die cubischen Reste, von denen wir einen beliebigen mit α bezeichnen; die Reste der zweiten und dritten Reihe, welche wir resp. mit β und γ bezeichnen, sind die cubischen Nichtreste. Wenn nun α, β und γ die angegebene Bedeutung haben, so sind, wie *Gauſs* gezeigt hat, folgende drei Reihen:

$$z_1 = \sum_0^{p-1}{}_k \cos\frac{2\alpha k^3\pi}{p}, \quad z_2 = \sum_0^{p-1}{}_k \cos\frac{2\beta k^3\pi}{p}, \quad z_3 = \sum_0^{p-1}{}_k \cos\frac{2\gamma k^3\pi}{p}$$

die drei Wurzeln von folgender cubischen Gleichung:

$$z^3 = 2pz + pt,$$

wo t durch die in ganzen Zahlen aufzulösende Gleichung $4p = t^2 + 27u^2$ und durch die Bedingung, daſs es positiv oder negativ zu nehmen sei, je nachdem es die Form $3h+1$ oder $3h-1$ hat, vollständig bestimmt ist. Die drei Reihen z_1, z_2, z_3 spielen in der Theorie der cubischen Reste eine sehr wichtige Rolle, sind aber durch diese cubische Gleichung noch nicht genau bestimmt, da es ganz unentschieden bleibt, welche der drei Wurzeln dieser Gleichung einer jeden dieser Reihen gleich ist; mit dieser Unbestimmtheit sind daher auch alle Resultate behaftet, welche man mit Hülfe dieser Reihen über cubische Reste gewinnt. Ich habe nun die Aufgabe, diese Unbestimmtheit aufzuheben, allerdings in einem gewissen Sinne gelöset, aber die Lösung genügt nicht recht, weil sie die Kenntniſs der Summe aller cubischen Reste, welche kleiner sind als $\frac{1}{2}p$, und eben so die Kenntniſs der Summen der beiden verschiedenen Arten von Nichtresten voraussetzt. Aus diesen berechneten Summen habe ich denn auch

die Werthe der drei Reihen z_1, z_2, z_3 für alle Primzahlen von der Form $3n+1$, unter 400, vollständig bestimmt und will die Resultate hier mittheilen, damit vielleicht ein Anderer durch Induction das allgemeine Gesetz finden könne, welches mir noch verborgen geblieben ist.

Zunächst bemerke ich, dafs, da t in den Grenzen $-2\sqrt{p}$ und $+2\sqrt{p}$ liegt, die drei Wurzeln der cubischen Gleichung stets in folgenden drei Intervallen enthalten sein müssen: die eine in den Grenzen $-2\sqrt{p}$ und $-\sqrt{p}$, eine der andern in den Grenzen $-\sqrt{p}$ und $+\sqrt{p}$ und die dritte in den Grenzen $+\sqrt{p}$ und $+2\sqrt{p}$. Ferner bemerke ich, dafs, wenn eine der drei Reihen vollständig bestimmt ist, die Bestimmung der beiden anderen keine Schwierigkeiten weiter hat, da diese sich rational durch jene ausdrücken lassen; daher bestimme ich hier nur die Reihe $z_1 = \sum_0^{p-1}{}_k \cos\frac{2\alpha k^3\pi}{p}$, in welcher auch $\alpha = 1$ genommen werden kann. Diese Reihe aber liegt nach meiner Berechnung

1) in den Grenzen $-2\sqrt{p}$ und $-\sqrt{p}$ für die Primzahlen
97, 139, 151, 199, 211, 331;

2) in den Grenzen $-\sqrt{p}$ und $+\sqrt{p}$ für die Primzahlen
13, 19, 37, 61, 109, 157, 193, 241, 283, 367, 373, 379, 397;

3) in den Grenzen $+\sqrt{p}$ und $+2\sqrt{p}$ für die Primzahlen
7, 31, 43, 67, 73, 79, 103, 127, 163, 181, 223, 229, 271, 277, 307, 313, 337, 349.

Es käme nun darauf an, zu suchen, welche Eigenthümlichkeiten jede dieser drei Reihen habe, die keine Primzahl der beiden anderen Reihen theilte. Die lineäre Form der Primzahlen scheint hierbei keine Bedeutung zu haben, wohl aber die quadratische Form $4p = t^2 + 27u^2$; vielleicht auch die Form $p = r^2 + 3.s^2$. Da ich aber auch aus diesen kein Gesetz entdecken konnte, so nahm ich meine Zuflucht zu den Zahlen, welchen $\beta^{\frac{p-1}{3}}$ und $\gamma^{\frac{p-1}{3}}$ congruent sind, aber mit eben so wenig Erfolg; auch ob gewisse Zahlen, namentlich 2 und 3 cubische Reste sind, oder nicht, entschied hierbei nichts. Jedenfalls scheint das Gesetz etwas tief zu liegen, genauer Nachforschungen aber wohl werth zu sein.

Eine Aufgabe betreffend die Theorie der cubischen Reste
(KuE)
(translation by the author)

If p is a prime in the form $p = 3n + 1$ and g a primitive root of it, then the series $1, g^1, g^2, g^3, \dots g^{n-2}$ can be ordered into the three different series $1, g^3, g^6, \dots g^{p-4}$, $g^4, g^7, \dots g^{p-3}$, $g^2, g^5, g^8 \dots g^{p-2}$. The remainders of the first series for the module p are the cubics remainders, from which we note an arbitrary one with α; the remainders of the second and third series, which we denote with β and γ, are the cubic non-remainders. The related Gaussian series

$$z_1 = \sum_0^{p-1} \cos\left(\frac{2\alpha k^3 \pi}{p}\right),\ z_2 = \sum_0^{p-1} \cos\left(\frac{2\beta k^3 \pi}{p}\right),\ z_3 = \sum_0^{p-1} \cos\left(\frac{2\gamma k^3 \pi}{p}\right).$$

are the three roots of the following cubic equation:

$$z^3 = 2pz + pt$$

where t is uniquely determined by the whole integer solution of the equation $4p = t^2 + 27u^2$ and t being positive resp. negative if it is in the form $3h + 1$ resp. $3h - 1$. … The three series are not uniquely determined by the cubic equation as it is not decided, which of the three roots correspond to the which of the three series. …. I have solved this vagueness in a certain sense, but this solution is insufficient, as it requires the knowledge of the sum of all cubic remainders (and also the sums of both cubic non-remainders) smaller than $\frac{1}{2}p$. …. From those calculated sums I have determined the values of z_1, z_2, z_3 for all primes of the form $3n + 1$ less than 400 and I am publishing those, that another person can find a common law by induction, which was hidden from me. First I notice, that because t lies in the interval $-2\sqrt{p}$ and $2\sqrt{p}$, the three roots of the cubic equation have to lie in the following three intervals $I_1 := (-2\sqrt{p}, -\sqrt{p})$, $I_2 := (-\sqrt{p}, \sqrt{p})$, $I_3 := (\sqrt{p}, 2\sqrt{p})$. I further note, that if one of the three series is known the other two can be rationally expressed out by it; therefore I determine only the series $z_1 = \sum_0^{p-1} \cos\left(\frac{2\alpha k^3 \pi}{p}\right)$ where one can choose $\alpha := 1$. This series lies in the intervals

I_1 : for the primes $97, 139, 151, 199, 211, 331$

I_2 : for the primes $13, 19, 37, 61, 109, 157, 193, 241, 283, 367, 373, 379, 397$

I_3 : for the primes $7, 31, 43, 67, 73, 79, 103, 127, 163, 181, 223, 229, 271, 277, 307, 313, 337, 349.$

It would now be a matter of searching which peculiarity each of those three have, where no primes is part of the other two series. The linear form of the primes seem to have no meaning, but the quadratic form $4p = t^2 + 27u^2$; perhaps also the form $p = r^2 + 3s^2$. Because I can't discover any law from this, I tried numbers, which are congruent to $\beta^{\frac{p-1}{3}}$ and $\gamma^{\frac{p-1}{3}}$; but also with little success; also, the case if the numbers 2 and 3 are either cubic remainders or not, gave me no hint. In any case the law seems to be built on deeper reasons being worth researching.

Exponential sums over primes
(DuA)

Kummer studied the distribution of the cubic exponential sums

$$S_p = \sum_{n=1}^{p} e(\frac{n^3}{p}),\ e(x) \coloneqq e^{2\pi i x}$$

with $p = 1 \bmod 3$ prime. The bound $|S_p| \leq 2\sqrt{p}$ is well known, and we can consequently write

$$\frac{S_p}{2\sqrt{p}} = \cos(2\pi\theta_p),\ \theta_p \in [0,1] \qquad (1.1).$$

This specifies the value $\theta_p - 1/2$ up to sign. This sign ambiguity can be resolved by noticing that (1.1) is the real part of an explicit root of unity (given by a normalized Gauss sum over Eisenstein integers) with range $(-1,1)$. To probe whether θ_p is equidistributed, Kummer computed the frequency with which $\cos(2\pi\theta_p)$ lay in the intervals interval $I_1 \coloneqq \left[\frac{1}{2}, 1\right]$ than in $I_2 \coloneqq \left[-\frac{1}{2}, \frac{1}{2}\right]$ or $I_3 \coloneqq \left[-1, -\frac{1}{2}\right]$, for $p \leq 500$. Kummer observed that $\cos(2\pi\theta_p)$ tened to lay more frequently in I_1 than in I_2 or I_3 (the ratio he observed was $3 : 2 : 1$ respectively). If this bias persisted, then the angles θ_p are not uniformly distributed. …. The Patterson conjecture explained the bias observed by Kummer, (PaS):

Patterson conjecture: As $X \to \infty$

$$\sum_{\substack{p \leq X \\ p=1 \,(\mathrm{mod}\, 3)}} \frac{S_p}{2\sqrt{p}} \sim \frac{2(2\pi)^{2/3}}{5\Gamma(\frac{2}{3})} \cdot \frac{(X)^{5/6}}{\log X}$$

where p runs through primes. …

… Some 20 years later, in 2000, Health-Brown sharpened his earlier result with Patterson and obtained unconditionally the nealy tight upper bound, (HeD),

$$\sum_{\substack{p \leq X \\ p=1 \,(\mathrm{mod}\, 3)}} \frac{S_p}{2\sqrt{p}} \ll_\varepsilon X^{\frac{5}{6}+\varepsilon} \text{ for any } \varepsilon > 0.$$

Remarks: By appealing to a heuristic form of the circle method Patterson's heuristic fell short of a proof of his conjecture explaining the bias observed by Kummer (DuA). This was due to insufficent bounds for the minor arcs. There is also a refinement from the Patterson conjecture that features an error term capturing square root cancellation. In (DuA) the Patterson conjecture is confirmed conditionally on the assumption of the Generalized Riemann Hypothesis, i.e. all non-trivial zeros of all Dirichlet L –functions have real part equal to $1/2$.

Gaussian numbers

The prime elements of $Z[i]$ are also known as Gaussian primes. An associate of a Gaussian prime is also a Gaussian prime. The conjugate of a Gaussian prime is also a Gaussian prime; this implies that Gaussian primes are symmetric about the real and imaginary axes.

The Gaussian integers form a principal ideal domain, i.e., they form also a unique factorization domain. This implies that a Gaussian integer is irreducible (that is, it is not the product of two non-units) if and only if it is prime (that is, it generates a prime ideal).

The norm of a Gaussian integer is a sum of two squares. A whole number with norm equal one is called an unit. The norm of a prime ideal is a prime number, (HuA).

The norm of a Gaussian integer is the basis of the Euler factorization method. The sum of two squares can be factorized into Gaussian integers. The Gaussian integers can be factorizied further, (ToH).

The four-square theorem of Lagrange states that every positive integer is the sum of four squares. Its proof is based on the theorem that any prime is the sum of four squares, (HaG) 20.5. For further theorems about integral and prime quaternions we refer to (HaG1) 20.6 ff.

A positive integer is a Gaussian prime if and only if it is a prime number p that is congruent to $3 \; mod \; 4$ (that is, it may be written $4n + 3$, with n a nonnegative integer). The other prime numbers are not Gaussian primes, but each is the product of two conjugate Gaussian primes.

A Gaussian integer $a + ib$ is a Gaussian prime if and only if either its norm is a prime number, or it is the product of a unit $\{\pm 1, \pm i\}$ and a prime number of the form $4n + 3$.

It follows that there are three cases for the factorization of a prime number p in the Gaussian integers:

1. If the prime number p is congruent to $3 \; mod \; 4$, then it is a Gaussian prime
2. If p is congruent to $1 \; mod \; 4$, then p is a decomposed prime in the Gaussian integers (i.e., it is the product of a Gaussian prime by its conjugate, both of which are non-associated Gaussian primes (neither is the product of the other by a unit)
3. If $p = 2$, we have $2 = (1 + i)(1 - i) = i(1 - i)^2$; that is, 2 is the product of the square of a Gaussian prime by a unit; it is the unique ramified prime in the Gaussian integers.

In summary

Every odd prime in the form $p = 4k + 1$ and $p = 2$ can be represented as the sum of two squares of two whole (positive or negative integer) numbers a and b. This is never the case for primes in the form $q = 4k + 3$, or more generally, the sum of two squares of two whole numbers a and b is only divisible by a prime number q, if a and b are divisible by q.

Gaussian numbers and the $\zeta(s)$ function

Let $r(n)$ denote the "number of representations" function as a sum of two squares

$$r(n) \coloneqq \#\{(a,b) \in R^2 | a^2 + b^2 = n\}.$$

The Hurwitz Zeta function is the Dirichlet series defined by, (IvA) 1.8,

$$L(s,\chi) \coloneqq \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p (1 - \chi(p)p^{-s})^{-1} \text{ for } Re(s) > 1$$

Then for the character function defined by, (ZaD) §2, (HaG) 17.9,

$$\chi(s) \coloneqq \begin{cases} 1 \, for \, n = 1 \, mod \, 4 \\ -1 \, for \, n = -1 \, mod \, 4 \\ 0 \, for \, n = 0 \, mod \, 2 \end{cases}$$

the corresponding Dirichlet series results into

$$\frac{1}{4} \sum_{n=1}^{\infty} \frac{r(n)}{n^s} = \zeta(s) L(s).$$

For $L(s)$ the following representations are valid, (ZaD) S. 31,

$$L(s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \cdots = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{t^{s-1}}{e^t + e^{-t}} dt$$

with the following relationship to the Euler number

$$L(-n) = \frac{1}{2} E_n, \, L(2n+1) = \frac{(-1)^n E_{2n}}{2^{2n+2}(2n)!} \pi^{2n+1}, \, n = 0,1,2, \ldots .$$

One lemma to calculate $L(s,\chi)$ for arbitrary Dirchichlet characters $\chi \neq \chi_0$ is

Lemma (ZaD) S. 77: For $0 < \varphi < 2\pi$ it holds

$$\sum_{n=1}^{\infty} \frac{e^{n\varphi}}{n} = -\log\left(2 \sin\left(\frac{\varphi}{2}\right)\right) + i\left(\frac{\pi}{2} - \frac{\varphi}{2}\right).$$

Note:The two summands are Hilbert transforms of each other.

(CoJ) Coates J., Sujatha R., Cyclotomic Fields and Zeta Values, Springer, Berlin, Heidelberg, New York, 2006

J. Coates · R. Sujatha

Cyclotomic Fields and Zeta Values

Springer

Preface

Chihayaburu	*Mighty they are*
Kami no igaki ni	*The gods within this sacred shrine-*
Hau kuzu mo	*Yet even the vines*
Aki ni wa aezu	*Creeping in the precincts could not hold*
Utsuroinikeri	*Against the autumn's tingeing of*
	their leaves.

– Ki no Tsurayaki (Kokinshu, V : 262).

This little book is intended for graduate students and the non-expert in Iwasawa theory. Its aim is to present in full detail the simplest proof of the important theorem on cyclotomic fields, which is often called "the main conjecture". We have thought it worthwhile to write such a book, not only because this theorem is arguably the deepest and most beautiful known result about the arithmetic of cyclotomic fields, but also because it is the simplest example of a vast array of subsequent, unproven "main conjectures" in modern arithmetic geometry involving the arithmetic behaviour of motives over p-adic Lie extensions of number fields (see [CFKSV]). These main conjectures are concerned with what one might loosely call the exact formulae of number theory which conjecturally link the special values of zeta and L-functions to purely arithmetic expressions (the most celebrated example being the conjecture of Birch and Swinnerton-Dyer for elliptic curves).

The first complete proof of the cyclotomic main conjecture was given by Mazur-Wiles, but it should not be forgotten that Iwasawa himself not only discovered the main conjecture but proved an important theorem which implies it in all known numerical cases. In this book, we follow this approach to the main conjecture via Iwasawa's theorem, and complete its proof by the ingenious arguments using Euler systems, due

to Kolyvagin, Rubin and Thaine. Not only does this treatment have the advantage of using less machinery, but it also gives for example, a very simple proof of the existence of the p-adic analogue of the Riemann zeta function.

If one looks at the past evolution of algebraic number theory, there has been a tendency to discover that the ideas which initially seem special to cyclotomic fields do, in the end, turn out to have very general counterparts. To quote Iwasawa [Iw1]:

"The theory of cyclotomic fields is in a unique position in algebraic number theory. On the one hand, it has provided us with a typical example of algebraic number fields from which we have been able to develop the theory of algebraic number fields in general; and on the other hand, it has also revealed to us many beautiful properties of the cyclotomic fields which are proper to these fields and which give us deep insights into important arithmetic results in elementary number theory."

Already, it is known that the ideas discussed in this book work in some measure for elliptic curves over certain abelian p-adic Lie extensions, both for curves with complex multiplication ([CW2], [Ru], [Y]) and without complex multiplication ([Ka2], [SU]). It does not seem unreasonable to hope that this may turn out to be true in much greater generality, perhaps even in the direction of the non-abelian main conjecture made in [CFKSV].

Finally, we thank Karl Rubin for his very helpful comments on the manuscript.

1

Cyclotomic Fields

1.1 Introduction

Let p be an odd prime number. We owe to Kummer the remarkable discovery that there is a connexion between the arithmetic of the field generated over $\mathbb{Q}$ by the p-th roots of unity and the values of the Riemann zeta function at the odd negative integers. This arose out of his work on Fermat's last theorem. Almost a hundred years later, Iwasawa made the equally major discovery that the p-adic analogue of the Riemann zeta function is deeply intertwined with the arithmetic of the field generated over $\mathbb{Q}$ by all p-power roots of unity. The main conjecture, which is now a theorem (first completely proved by Mazur and Wiles [MW]), is the natural final outcome of these ideas. This main conjecture is the deepest result we know about the arithmetic of cyclotomic fields. In this first chapter, we explain more fully this background, and also give the precise statement of the main conjecture towards the end of the chapter. However, all proofs will be postponed until the later chapters.

Let μ_p denote the group of p-th roots of unity, and put

$$\mathcal{F} = \mathbb{Q}(\mu_p), \quad \varpi = \mathrm{Gal}(\mathcal{F}/\mathbb{Q}). \tag{1.1}$$

Now ϖ acts on μ_p, and thus gives an injective homomorphism

$$\theta : \varpi \hookrightarrow \mathrm{Aut}(\mu_p) = (\mathbb{Z}/p\mathbb{Z})^\times \tag{1.2}$$

In fact, θ is an isomorphism by the irreducibility of the p-th cyclotomic polynomial. Thus the powers θ^n for $n = 1, \ldots, p-1$ give all the characters of ϖ with values in $\mathbb{F}_p$. Let $\mathfrak{C}$ denote the ideal class group of $\mathcal{F}$. We stress that $\mathfrak{C}$ becomes impossible to compute numerically by naive methods once p is at all large. However, as is explained below,

we owe to Kummer the discovery of a miraculous connexion between the p-primary subgroup of $\mathfrak{C}$ and the values

$$\zeta(s) \text{ for } s = -1, -3, -5, \ldots, \tag{1.3}$$

where $\zeta(s)$ is the classical complex Riemann zeta function. We recall that $\zeta(s)$ is defined by the Euler product

$$\zeta(s) = \prod_l (1 - l^{-s})^{-1} \tag{1.4}$$

for complex s with real part greater than 1, and has an analytic continuation over the whole complex plane, apart from a simple pole at $s = 1$. It has been known since Euler that the values (1.3) are rational numbers. In fact,

$$\zeta(-n) = -\mathcal{B}_{n+1}/(n+1) \qquad (n = 1, 3, 5, \cdots) \tag{1.5}$$

where the Bernoulli numbers $\mathcal{B}_n$ are defined by the expansion

$$t/(e^t - 1) = \sum_{n=0}^{\infty} \mathcal{B}_n t^n/n!. \tag{1.6}$$

One computes easily from these equations that

$$\zeta(-1) = -\frac{1}{12}, \quad \zeta(-3) = \frac{1}{120}, \quad \zeta(-5) = -\frac{1}{252}, \cdots .$$

Definition 1.1.1. *We say that the prime number p is irregular if p divides the order of $\mathfrak{C}$.*

The first few irregular primes are $p = 37, 59, 67, 101, 103, \cdots$. It would be very difficult numerically to test whether a prime number p is irregular if we did not have the following remarkable criterion for irregularity due to Kummer.

Theorem 1.1.2. *The prime p is irregular if and only if p divides the numerator of at least one of $\zeta(-1), \zeta(-3), \cdots, \zeta(4-p)$.*

For example, we have

$$\zeta(-11) = \frac{691}{32760}, \quad \zeta(-15) = \frac{3617}{8160},$$

and thus, thanks to Kummer's theorem, we conclude that both 691 and 3617 are irregular primes. The irregularity of 37 follows from the fact that

$$\zeta(-31) = \frac{37 \times 208360028141}{16320}.$$

We point out that the numerators and denominators of these zeta values tend to grow very rapidly. For example, the numerator of $\zeta(-179)$ has 199 digits. However, fortunately Kummer's theorem basically reduces the problem of deciding whether a prime p is irregular to a question of arithmetic modulo p, and is numerically very powerful. Indeed, using computational techniques derived from Kummer's theorem, all irregular primes up to 12,000,000 have been determined [BCEMS]. One finds that, up to this limit, the percentage of regular primes is approximately 60.61 percent, which fits remarkably well with the distribution which would occur if the numerators of the zeta values occurring in Theorem 1.1.2 were random modulo p (see the discussion after Theorem 5.17 in [Wa]).

This mysterious link given in Theorem 1.1.2 between two totally different mathematical objects, namely the ideal class group of $\mathcal{F}$ on the one hand, and the special values of the Riemann zeta function on the other, is unquestionably one of the great discoveries in number theory, whose generalization to other arithmetic situations is a major theme of modern arithmetic geometry.

We end this introduction by recalling the following remarkable congruences, which were first discovered by Kummer as part of his proof of Theorem 1.1.2, and which provide the first evidence for the existence of the p-adic analogue of $\zeta(s)$.

Theorem 1.1.3. *Let n and m be odd positive integers such that $n \equiv m \not\equiv -1 \bmod (p-1)$. Then the rational numbers $\zeta(-n)$ and $\zeta(-m)$ are p-integral, and*

$$\zeta(-n) \equiv \zeta(-m) \bmod p.$$

(CoJ) Coates J., Sujatha R., Cyclotomic Fields and Zeta Values, Springer, Berlin, Heidelberg, New York, 2006

Kummer's regular and irregular primes

Kummer introduced the concept of regular and irregular primes based on an underlying „ideal complex number" concept. There are infinitely many irregular primes congruent to $3\ mod\ 4$, ((JeK).

(Kummer) **Theorem 1.1.2** (CoJ):

> The prime p is irregular if and only if p divides the numerator of at least one of $\zeta(-1)$, $\zeta(-3), \ldots \zeta(4-p)$.

Let B_m denotes a Bernoulli number in the even-suffix notation. Then the Kummer theorem states that p is regular if and only if it does not divide the numerator of any of the Bernoulli numbers B_2, B_4, … B_{p-3}, (KuE1).

As part of his proof Kummer showed the following congruences

Theorem 1.1.3 (CoJ):

> Let n and m be odd positive integers such that $n = m \neq -1 mod(p-1)$. Then the rational numbers $\zeta(-n)$ and $\zeta(-m)$ are p -integral, and $\zeta(-n) = \zeta(-m) mod\ p$.

For the rational Bernoulli numbers it holds $B_{2k+1} = 0$; for the Euler integer numbers it holds $E_{2k-1} = 0$.

Carlitz called an odd prime prime p to be irregular with respect to the Euler numbers if it divides one of the numbers E_2, E_4, … E_{p-3}, He proved that the number of such primes is infinite, (CaL).

For any irregular prime p the pair $(p, 2k)$ is called a irregular pair, if p is irregular and $2 \leq 2k \leq p-3$.

From the Hensel lemma it follows the

Lemma:

> Let p denote an odd prime number and $a \in Z_2$ where p is not a divisor of a. Then a is a square in Z_2 iff a is a quadratic rest $mod\ p$.
>
> If $a \in Z_2$ is odd, then a is a square in Z_2 iff $a = 1 mod 8$.

Note: Q, R, C are fields, the Hamiltonian quaternions $|\boldsymbol{H}$ is a skew field.

The Fundamental Theorem of Algebra for Quaternions (EbH) p. 204

Every polynomial $X^n - a$, $a \in |\boldsymbol{H}$, of degree $n > 0$ has zeros in every plane in $|\boldsymbol{H}$ containing $0, e,$ and a.

Hurwitz quaternions

The set of Hurwitz quaternion integers provides an Euclidian ring domain (as the Gaussian integers), (HuA). The number of representations of an whole positive number n as a sum of of four quadrats is, depending if this number is odd or even, the 8-times resp. the 24-times of the sum of the odd divisors of the number n, (HuA). The unit elements of Q_{24} form the lattice of the regular, self-dual 24-cell, which does not have a regular analogue in any other dimension. We note that the 3-dimensional unit sphere S^3 contains the not abelian Q_{24} unit group of the Hurwitz quaternions.

From (HaG) 20.7, we recall:

> „If α is an integral quaternion, then one at least of its associates has integral coordinates; and if α is odd, then one at least of its associates has non-integral coordinates."

In (CoB) a "unique factorization of Hurwitz quaternions" is proposed, where any non-unit Hurwitz quaternion can be factored uniquely, up to a series of unit-migrations, meta-commutations, and re-combinations.

The quaternion rotation operator

The perhaps primary application of quaternions is the quaternion rotation operator. This is a special quaternion triple-product (unit quaternions and rotating imaginary vector) competing with the conventional (Euler) matrix rotation operator. The quaternion rotation operator can be interpreted as a frame or a point-set rotation, (KuJ). Its outstanding advantages compared to the Euler geometry are

- the axes of rotation and angles of rotation are independent from the underlying coordinate system and directly readable
- there is no need to to take care about the sequencing of the rotary axes.

The quaternion rotation operator is proposed alternatively to the Euclidian rotation.

Hurwitz quaternions and symmetry groups

For each quaternion of S^3 there is a quaternion represention as a sum of two product terms in the form $e \cdot cos\left(\frac{\omega}{2}\right) + q \cdot sin\left(\frac{\omega}{2}\right)$, where e denotes the „real" quaternion unit, q denotes a purely imaginary quaternion with norm equal one, and ω denotes an angle between zero and 2π, (EbH) 7.3. We also note that S^1 and S^3 are the only spheres with a "continuous" group structure, (EbH) 7.2. From the fundamental theorem of algebra for quaternions it follows that there are exactly n roots of any quaternion with not vanishing imaginary part, (EbH) 7.1.8.

The 1-dimensional S^1 unit sphere is isomorphic to $U(1)$; the 3-dimensional S^3 unit sphere is isomorphic to $SU(2)$.

The groups S^1 and S^3 have parameter representations, (EbH) 3.5.4(2'), 7.3.2(3). There are epimorphisms between S^3 and $SO(3)$, resp. between $S^3 \times S^3$ and $SO(4)$. The group $SO(4)$ contains isomorphic normal subgroups to the group S^3, i.e. it is a not „simple" Lie group. The groups $SO(n)$, $n > 4$, are all „simple", i.e. they have not trivial coherent normal subgroups. The groups $SO(2n+1)$ have no normal subgroup unequal (e). The groups $SO(4)$ have exactly the not trivial normal subgroup $\{e, -e\}$, (EbH) 7.3.4.

With respect to the proposed unified field theory (UFT) in (BrK1) we note that the 1-dimensional unit sphere in R^2 corresponds to the Lie group $U(1)$. The related number grid is built by the Eisenstein numbers. Regarding the characteristics of S^1 and S^3 in the context of Hurwitz quaternions and the proposed united field theory (UFT) we note a possible conceptual link to the Courant conjecture, (CoR) p. 763:

> *Families of spherical waves for arbitrary time-like lines exist only in the case of two or four variables, and then only if the differential equation is equivalent to the wave equation.*

In the context of the Teichmueller theory with respect to the Riemann & Hyperbolic surfaces we mention that the compactification of the field of complex numbers C, the Riemann sphere, is homeomorphic to S^2. In the context of the proposed Hilbert space framework we note the relationship oft he Teichmüller space with the fractional Hilbert space $H_{1/2}$.

In (AdS), (FiD) quaternionic Hilbert spaces (in particular, Krein spaces) for various applications to quantum mechanics are provided.

In (AlD) quaternionic inner product spaces including ortho-complemented subspaces are studied. The main result is that a closed uniformly positive subspace in a quaternionic Krein space is ortho-complemented.

Employing quaternionic Newton's law, in (ArI) it is shown that the energy conservation equation is the analog of Lorenz gauge in electromagnetism.

Regarding the crucial difference between the algebra based gauge theory and the analysis based GRT we quote from (BlC):

„*The correspondence between symmetries and conserved quantities is one of the most important principles of physics. The crucial difference between gauge theories and the GRT is that the symmetries of the GRT act on the space-time itself and not only on the degree of freedoms of the „internal" fields.*

The vacuum Einstein equations state that the Ricci curvature Ric(g) of a lorentzian metric g is identically zero. Recast as hamiltonian evolution equations, they become a hamiltonian system on the cotangent bundle of the manifold MΣ of smooth riemannian metrics on a manifold Σ which represents the typical Cauchy hypersurface.

As in every lagrangian field theory with symmetries, the initial data must satisfy constraints. But, unlike those of gauge theories, the constraints of general relativity do not arise as momenta of any hamiltonian group action. In this paper, (BlC), we show that the bracket relations among the constraints of general relativity are identical to the bracket relations in the Lie algebroid of a groupoid consisting of diffeomorphisms between space-like hypersurfaces in spacetimes. A direct connection is still missing between the constraints themselves, whose definition is closely related to the Einstein equations, and our groupoid, in which the Einstein equations play no role at all. We discuss some of the difficulties involved in making such a connection.

In contrast to classical mechanics and gauge field theories, the conserved quantities of the GRT do not span a symmetry algebra in the conventional sense. Instead, a so-called Hamiltonian Lie algebroid can be obtained from a naturally constructed symmetry groupoid."

About common separable-quadratic splitting fields of quaternion algebras

P. Draxl
Nachrichten der Akademie der Wissenschaften in Göttingen, II. Mathematisch-Physikalische Klasse, Jahrgang 1075, Nr. 16

Über gemeinsame separabel-quadratische Zerfällungskörper von Quaternionenalgebren

Von *Peter Draxl*, Bielefeld

Vorgelegt von Herrn M. Kneser in der Sitzung vom 4. Juli 1975

Ist k ein kommutativer Körper, dann wollen wir unter einer *k-Quaternionenalgebra* wie üblich eine einfache vierdimensionale k-Algebra mit Zentrum k verstehen (vgl. etwa M. Deuring [3]). Ziel dieser Note ist der Beweis von folgendem

Satz. *Ist das Tensorprodukt zweier k-Quaternionenalgebren kein Schiefkörper, so besitzen diese einen gemeinsamen, über k separabel-quadratischen Zerfällungskörper.*

Ist die Charakteristik von k ungleich zwei, so ist der Satz bekannt (A. Pfister [5], S. 124, Zusatz). Im allgemeinen Fall ist meines Wissens bislang nur die Existenz eines gemeinsamen quadratischen Zerfällungskörpers unter den gegebenen Voraussetzungen bekannt (A. A. Albert [1]), was im Falle $\mathrm{char}\ k \neq 2$ selbstverständlich ausreicht.

Folglich genügt es, fortan $\mathrm{char}\ k = 2$ vorauszusetzen. Bevor nun der Satz in diesem verbleibenden Fall in § 2 bewiesen wird, werden in § 1 einige Tatsachen über k-Quaternionenalgebren bei $\mathrm{char}\ k = 2$ zusammengestellt, die ich teilweise in der in § 2 benötigten Form in der Literatur nicht finden konnte. In § 3 werden dann als eine mögliche Anwendung obigen Satzes diejenigen Körper der Charakteristik zwei axiomatisch gekennzeichnet, welche bis auf Äquivalenz genau eine reguläre, quaternäre, anisotrope quadratische Form gestatten; dabei stellt sich heraus, daß die Verhältnisse völlig den schon bekannten (A. Fröhlich [4]) im Falle $\mathrm{char}\ k \neq 2$ entsprechen.

Der hier in § 2 gegebene Beweis des Satzes ist übrigens eine Verfeinerung des Albertschen Beweises, der rein algebrentheoretisch verläuft. Es erscheint einleuchtend, daß sich auch der die Theorie der quadratischen Formen wesentlich benutzende Pfistersche Beweis übertragen läßt, wenn man gewisse neuere Ergebnisse dieser Theorie auf den bislang in diesem Zusammenhang vernachlässigten Fall der Charakteristik zwei übertrüge.

Nach wie vor unentschieden bleibt die Frage, ob im Falle eines nicht-vollkommenen Körpers k mit $\mathrm{char}\ k = 2$ unter den Voraussetzungen des Satzes

auch die Existenz eines gemeinsamen über k inseparabel-quadratischen Zerfällungskörpers folgt; der Fall eines vollkommenen Körpers der Charakteristik zwei ist insofern uninteressant, als dann gar keine k-Quaternionenschiefkörper existieren (vgl. § 1).

The integer degree (or winding number) of functions of Sobolev class $H^{1/2}$ from the circle S^1 to itself

(BoA), (BoJ), (KoJ), (NaS), (SeG)

Lemma (BoA): Let f be a function of Sobolev class $H^{1/2}$ from the circle S^1 to itself. Then there exists an integer n given by $n = \frac{1}{2\pi i}\int_{S^1} f^{-1}\frac{\partial f}{\partial x}dx$ (*), and a real function $g \in H^{1/2}$ on S^1, unique up to an integral multiple of a 2π, such that $f = z^n e^{ig}$.

It also follows, that smooth functions from S^1 to itself are dense in $H^{1/2}$ such functions, for the $H^{1/2}$ topology (one may approximate g by smooth real functions).

(*) The integral $\frac{1}{2\pi i}\int_{S^1} f^{-1}\frac{\partial f}{\partial x}dx$ is defined in the distributional sense since $f^{-1} = \bar{f} \in H^{1/2}$ and $\frac{\partial f}{\partial x} \in H^{-1/2}$.

Lemma: A continuous functions f with bounded variation is not in class $H^{1/2}$; however, the Fourier series

$$f(t) = F(e^{it}) \sim \sum_{n=-\infty}^{\infty} c_n e^{int}\ ,\ c_n = c_n(f) = \frac{1}{2\pi}\int_0^{2\pi} f(t)e^{-int}dt$$

is uniformly convergent to f while df is a complex measure; hence, its degree (index or winding) number is given by

$$windF = degF = \|f\|_{1/2}^2 = \sum_{n=-\infty}^{\infty} n|c_n|^2\ .$$

Due to the orthogonality relation

$$\sum_{n=-\infty}^{\infty} c_n\,\bar{c}_{n-k} = \frac{1}{2\pi}\int_0^{2\pi} f(t)\overline{f(t)}e^{-ikt}dt = \begin{cases}0, if\ k \neq 0\\ 1\ if\ k = 0\end{cases}$$

together with the absolute convergence of the series $\sum_{n=-\infty}^{\infty} n|c_n|^2$ the sum of the series is an integer!

Proof: It holds

$$windF = degF = \frac{1}{2\pi i}\Delta logF|_{S^1} = \frac{1}{2\pi i}\oint_{S^1}\frac{1}{F}dF = \frac{1}{2\pi i}\oint_{S^1}\bar{F}d\bar{F}$$

$$= \frac{1}{2\pi i}\int_0^{2\pi}\overline{f(t)}f'(t)dt = \sum_{n=-\infty}^{\infty} n|c_n|^2$$

$$= \|f\|_{1/2}^2\ .$$

The complexification (complex polarization) of $H_{1/2}$
(SeG), (NaS)

Let $L_2^{\#}(\Gamma)$ denotes the 2π −periodic Hilbert space of real functions of mean-value zero on the unit circle $\Gamma \coloneqq S^1(R^2)$. For $u \in L_2^{\#}(\Gamma)$ and for real $\beta \in R$, $n \in Z$, the Fourier coefficients

$$u_n \coloneqq \frac{1}{2\pi}\oint u(x)e^{inx}dx$$

enable the definition of Hilbert scales $H_\beta = H_\beta^{\#}(\Gamma)$ equipped with the norms

$$\|u\|_\beta^2 \coloneqq \sum_{n=-\infty}^{\infty}|n|^{2\beta}|u_n|^2.$$

The considered Hilbert space $H_{1/2}$ comprises functions on S^1 with vanishing mean possessing square-integrable half-order derivative.

Note: The Fourier series $f(e^{ix}) = \sum_{n=-\infty}^{\infty} u_n e^{inx}$, $u_n = \bar{u}_{-n}$ converges quasi-everywhere. It can be identified with the complex sequences space

$$l_2^{1/2} = \left\{u = (u_1, u_2, u_3, \dots)\,\middle|\,\sqrt{n}u_n \text{ is square summable}\right\}.$$

by the identity

$$\|f\|_{1/2}^2 = \|u\|_{l_2^{1/2}}^2 = 2\sum_{n=1}^{\infty}|n||u_n|^2.$$

Therefore, $H_{1/2}$ and $l_2^{1/2}$ are isometrically isomorphic separable Hilbert spaces. The Hilbert transform („conjugation“ of Fourier series)

$$H[f](e^{ix}) = -\sum_{n=-\infty}^{\infty} isgn(n)u_n e^{inx}$$

is an automorphism $H\colon H_\beta \to H_\beta$ such that $H^2 = -Id$, i.e., it is a canonical complex structure for $H_{1/2}$. This complex structure is equivalent to a structure of a Hilbert space over C, if one identifies the Hilbert transform map H with multiplication with Hilbert transform $i = \sqrt{-1}$. The pair $(H_{1/2}, H)$ is called a complex Hilbert space.

Note (Segal): A complex polarization of $H_{1/2}$ for the form S means a decomposition

$$H_{1/2;C} = W_+ \otimes W_-$$

where $H_{1/2;C}$ is the complexification of $H_{1/2}$, such that S is identically zero on W_+. (W_- denotes the complex conjugate of W_+.) Then

$$(w_1, w_2) \to \langle w_1, w_2\rangle = 2i \cdot S(\bar{w}_1, w_2)$$

is a Hermitian form on W_+. If this is positive definite, making W_+ a pre-Hilbert-space, we shall call W_+ a positive polarization.

In our case of $H_{1/2}$ there is a canonical positive polarization, in which W_+ is the space of smooth maps $f\colon S^1 \to C$ which extend to holomorphic functions on the disk $D = \left\{z \in C\,\middle|\,|z| \le 1\right\}$ (modulo constants). The spaces W_+ and W_- are isotropic for S by Cauchy's theorem, and the form $\langle w_1, w_2\rangle$ is positive definite.

In fact if $f(z) = \sum_{n>0} a_n z^n$, $g(z) = \sum_{n>0} b_n z^n$ then

$$\langle f, g\rangle = \sum_{n>0} 2n\bar{a}_n b_n = \frac{2}{\pi}\int_D \overline{f'(z)}\, g'(z)d\mu(z)$$

where μ is the Lebesgue measure on D.

Note: The symplectic bilinear form

$$S: H_{1/2} \times H_{1/2} \rightarrow R$$

$$S(f,g) = \frac{1}{2\pi}\oint_{S^1} f \cdot dg$$

makes $H_{1/2}$ to a symplectic Hilbert space.The symplectic bilinear form S is S-compatible to the inner product of $H_{1/2}$ enabled by the cononical complex structure H for $H_{1/2}$ as

$$(f,g)_{1/2} = S(f, H[g])$$

defines a positive definite inner product. On Fourier coefficients this bilinear form becomes

$$S(f,g) = 2Im(\sum_{n=1}^{\infty} nu_n\bar{v}_n) = -i\sum_{n=-\infty}^{\infty} nu_n v_{-n} \ ,$$

where $\{u_n\}$ and $\{v_n\}$ are respectively the Fourier coefficients of the (real-valued) functions f and g. This non-degenerate bilinear alternating form extends from V to the full Hilbert space $H_{1/2}$.

The important interconnection between the inner product on $H_{1/2}$, the Hilbert transform complex structure H, and the form S is encapsulated in the identity:

$$S(f, H[g]) = (f,g)_{1/2} \ \ \forall f, g \in H_{1/2}.$$

Note: The symplectic form $S: H_{1/2} \times H_{1/2} \rightarrow R$ is a continuous, in fact analytics, map on $H_{1/2} \times H_{1/2}$, (Segal)

Note: The complex Hilbert space $H_{1/2;C}$ is isomorphic to $l_2^{1/2}(C)$.

Note: The Hermitian inner product of the complex Hilbert space $H_{1/2;C}$ is derived from

$$\|f\|_{1/2}^2 = \|u\|_{l_2^{1/2}}^2 = 2\sum_{n=1}^{\infty} |n||u_n|^2$$

given by

$$\langle f,g\rangle = \sum_{n=-\infty}^{\infty} |n| u_n\bar{v}_n \ .$$

The compatible complex structure H makes $H_{1/2}$ into a Hermitian vector space (i.e. a complex inner product space) with inner product

$$h(f,g) = g(f,g) + iS(f,g).$$

The following properties are valid

$$h(f, H[g]) = ih(f,g),\ h(H[f],g) = -ih(f,g) \text{ and } h(f,f) > 0,\ v \neq 0.$$

Note: If e_n is an ONS system of , and $e_n^H = H[e_n]$. Then e_n, e_n^H is a symplectic basis, i.e.,

$$S(e_n, e_m^H) = Im(h(e_n, H[e_m]) = Im(i \cdot \big(h(e_n, e_m)\big) = \delta_{nm}$$

$$S(e_n, e_m) = Im\big(h(e_n, e_m)\big) = 0,\ S(e_n^H, e_m^H) = Im\big(h(e_n^H, e_m^H)\big) = 0$$

Note:The fundamental orthogonal decomposition of $H_{1/2;C}$, comprising the Fourier series $f(e^{ix}) = \sum_{n=-\infty}^{\infty} u_n e^{inx}$, $u_0 = 0$, is given by $H_{1/2;C} = W_+ \otimes W_-$ with

$$W_+ = \big\{f \in H_{1/2;C} | all\ negative\ index\ Fourier\ coefficients\ vanish)\big\}$$

$$W_- = \big\{f \in H_{1/2;C} | all\ positiv\ index\ Fourier\ coefficients\ vanish)\big\} = \overline{W}_+.$$

Note: The sub-spaces W_+ and W_- can be characterized as precisely the $-i$ and $+i$ eigenspaces (respectively) of the extension of the Hilbert transform.

Note: Because of

$$S(f,g) = 2Im(\sum_{n=1}^{\infty} nu_n\bar{v}_n) = -i\sum_{n=-\infty}^{\infty} nu_n v_{-n}$$

each of W_+ and W_- is isotropic for S, i.e., $S(f.g) = 0$, whenever both, f and g are from either W_+ and W_-.

Note: W_+ and W_- are positive isotropic subspaces in the following sense

(1) $(f_+, g_+) = i \cdot S(f_+, \bar{g}_+) \quad f_+, g_+ \in W_+$

(2) $(f_-, g_-) = -i \cdot S(f_-, \bar{g}_-) \quad f_-, g_- \in W_-$

Note: The formulae (1) and (2) show that one could have defined the inner product $\langle f, g\rangle$ and norm on $H_{1/2;C}$ from the symplectic form S, by using these relations to define the inner products on W_+ and W_-, and declaring W_+ to be perpendicular to W_-. Thus, for general $f, g \in H_{1/2;C}$ one has the fundamental identity

$$\langle f, g\rangle = i \cdot S(f_+, \bar{g}_+) + -i \cdot S(f_-, \bar{g}_-).$$

The Hilbert space structure of $H_{1/2;C}$ can thus be described simply in terms of the canonical symplectic form it carries and the fundamental decomposition $H_{1/2;C} = W_+ \otimes W_-$. ($f_\pm$ denotes the projection of f onto $W_{+/-}$).

Note: The Hilbert transforms of $\sin(\alpha x)$, $\cos(\alpha x)$, and $e^{i\alpha x}$ are $-\cos(\alpha x)$, $\sin(\alpha x)$, and $-i \cdot sgn(\alpha)e^{i\alpha x}$.

The zeros of the Digamma function $\Psi(x) = log'\Gamma(x)$

For the Digamma function $\Psi(x) = log'\Gamma(x)$ the following formulas are valid

i) $\Psi(x) = -\gamma - \sum_{k=0}^{\infty}(\frac{1}{x+k} - \frac{1}{1+k})$

ii) $\Psi(z) = logz + O\left(\frac{1}{|z|}\right) = log\Gamma(1+z) - log\Gamma(z) + O\left(\frac{1}{|z|}\right)$

iii) $\frac{1}{\Gamma(s)} = \Psi(s)\frac{1}{\Gamma'(s)}$ resp. $-log\Gamma(s) = log\Psi(s) - log\Gamma'(s)$.

Lemma (NiN) p. 99: for every $\varepsilon > 0$ there is a $R > 0$ that

$$|\Psi(x) - logx| < \varepsilon \text{ for } |x| \geq R > 0.$$

Lemma (NiN) p. 99, (SeP): Let w_n denote the zeros of $\Psi(x)$ $n \in N_0$,

i) all zeros of $\Psi(x)$ are real; there is only one positive zero $w_0 \sim 1{,}461$, (AbM) 6.3.19

ii) all negative zeros w_n of $\Psi(x)$ lie in the intervals $w_n \in (-n, 1/2 - n)$.

Lemma (NiN) p. 99:

i) the sequence $y_n := n + w_n$, $n \in N$, is characterized by the relations
$\Psi(1 - w_n) = \Psi(n + 1 - y_n) = \pi\cot(\pi w_n) = \pi\cot(\pi(-n + y_n)) = \pi\cot(\pi y_n)$,
i.e.
$$y_n = \frac{1}{\pi}arctan\left(\frac{\pi}{\Psi(1-w_n)}\right)$$

ii) it holds $y_n, \frac{1}{2} - y_n \in (0, \frac{1}{2})$ and for large n
$$\pi\cot(\pi y_n) = logn + \delta_n \text{ with} \lim_{n\to\infty} \delta_n = 0,$$
resp.
$$y_n = \frac{1}{\pi}arctan\left(\frac{\pi}{logn+\delta_n}\right) = \frac{1}{logn} + \frac{\delta_n'}{logn}, \quad \lim_{n\to\infty} \delta_n' = 0$$

iii) $\frac{1}{2}\Psi(1 - w_n) = \frac{\pi}{2}\cot(\pi w_n) = \frac{\pi}{2}\cot(\pi y_n) = -\frac{1}{2y_n} - \sum_{k=0}^{\infty} s_{2k} y^{2k+1}$ (NiN)) S. 51.

Corollary: $\frac{1}{2}\Psi(1 + |w_n|) \sim \frac{1}{2|w_n|}$.

Corollary: The negative zeros w_n of $\Psi(x)$ fulfill the Kadec $-\frac{1}{4}$ condition

Note: The asymptotics of the sum of the Dawson function $D(x) := e^{-x^2}\int_0^{\infty} e^{u^2} du$ and the Digamma function $\Psi(x)$ is related to the $logx$ function by $\Psi(x) + D(x) \cong (logx - \frac{1}{2x}) + \frac{1}{2x} \cong logx$.

Riesz basis systems $\{e^{i\lambda_\nu t}\}_{\nu\in Z}$

The core theorem of non-harmonic Fourier series theory is based on the Levinson-Kadec theorems (e.g. (LeN) p. 48, (PaR) p. 113.

Levinson theorem XVIII, (LeN) p. 48: If $\{\lambda_n\}$ is a sequence and L a constant such that $|\lambda_n - n| \le L < 1/4$, then the system $\{e^{i\lambda_n x}\}_{n\in Z}$ is close in $L_2^{\#}(-\pi,\pi)$ (i.e. from $\int_{-\pi}^{\pi} f(x)e^{-inx}dx = 0$ it follows that $f(x)$ is identically zero) and possesses a unique biorthogonal set $\{h_n(x)\}$ such that for any $f \in L_2^{\#}(-\pi,\pi)$ the series

$$\sum_{-\infty}^{\infty} \frac{e^{inx}}{2\pi}\int_{-\pi}^{\pi} f(\xi)e^{-in\xi}d\xi - e^{i\lambda_n x}\int_{-\pi}^{\pi} f(\xi)h_n(\xi)d\xi$$

converges uniformly to zero over the interval $[-\pi+\delta, \pi-\delta]$ for any $\delta > 0$. Moreover the difference of weighted sums (Riesz, Abel, and so on) of the non-harmonic and ordinary Fourier series also converges uniformly to zero over $[-\pi+\delta, \pi-\delta]$.

The main ingredients to prove the Levinson theorem are the following two lemmata concerning the function

$$G(w) := G(u+iv) = (w-\lambda_0)\prod_{n=1}^{\infty}\left(1-\frac{w}{\lambda_n}\right)\left(1-\frac{w}{\lambda_{-n}}\right).$$

Lemma A (LeN) p. 55: If $\{\lambda_n\}$ fulfills the Kadec condition, then for different constants c it holds

i) $|G(w)| < c(|w|+1)e^{\pi|v|}$

ii) $|G(w)| > c|v|(|w|+1)^{-2}e^{\pi|v|}$

iii) $|G1/2 + iv)| > c.$

Lemma B (LeN) p. 57: The functions $h_n(\xi)$ defined by

$$h_n(\xi) := \int_{-\infty}^{\infty} \frac{G(u)}{(u-\lambda_n)G'(u)}e^{-iu\xi}du$$

form a sequence of biorthogonal to $\{e^{i\lambda_n x}\}$ over $(-\pi,\pi)$.

Kadec`s $\frac{1}{4}$ – Theorem (YoR) p. 36: If $\{\lambda_n\}_{n\in Z}$ is a sequence of real numbers for which $|\lambda_n - n| \le L < 1/4$, then $\{e^{i\lambda_n t}\}_{n\in Z}$ satisfy the Paley-Wiener criterion and so forms a Riesz basis for $L_2(-\pi,\pi)$.

Lemma (LeN) p. 48, (YoR) p. 100: If $\{\lambda_n\}$ is a sequence and L a constant such that

$$(*) \quad |\lambda_n - n| \le L < 1/4,$$

then the system $\{e^{i\lambda_n x}\}_{n\in Z}$ is close in $L_2^{\#}(-\pi,\pi)$ (i.e. from $\int_{-\pi}^{\pi} f(x)e^{-inx}dx = 0$ it follows that $f(x)$ is identically zero) and possesses a unique biorthogonal set $\{h_n(x)\}$ such that for any $f \in L_2^{\#}(-\pi,\pi)$ the series

$$\sum_{-\infty}^{\infty} \frac{e^{inx}}{2\pi}\int_{-\pi}^{\pi} f(\xi)e^{-in\xi}d\xi - e^{i\lambda_n x}\int_{-\pi}^{\pi} f(\xi)h_n(\xi)d\xi$$

converges uniformly to zero over the interval $[-\pi+\delta, \pi-\delta]$ for any $\delta > 0$. Moreover the difference of weighted sums (Riesz, Abel, and so on) of the non-harmonic and ordinary Fourier series also converges uniformly to zero over $[-\pi+\delta, \pi-\delta]$.

Remark (YoR) p. 36: Kadec's $\frac{1}{4}$ –theorem shows that the system $\{e^{i\lambda_n x}\}_{n\in Z}$ constitutes a Riesz basis for $L_2^{\#}(-\pi,\pi)$ whenever every μ_n is real and

$$|\lambda_n - n| \le L < 1/4,$$

but need not constitute a basis when $L = 1/4$.

Lemma, (YoR) p. 109: The system $\{e^{i\lambda_n t}\}$ is minimal in $L_2^{\#}(-\pi,\pi)$ if and only if there exists a nontrival function $f(z)$ of exponential type at most π, zeros at every λ_n, and such that

$$\int_{-\infty}^{\infty} \frac{|f(x)|^2}{1+x^2}dx < \infty.$$

A sequence of vectors in a separable Hilbert space is called complete, if its linear span is dense in the Hilbert space, resp. if the zero vector alone is perpendicular to every basis vector. A characterization of an orthogonal Schauder bases of a separable Hilbert space is that they are complete orthogonal sequences.

A complete sequence of vectors in a separable Hilbert space is a Riesz basis if and only if its moment space is equal to l^2, (YoR) p. 142.

Regarding the stability of the class of Riesz bases $\{e^{i\lambda_n t}\}$ in $L_2(-\pi,\pi)$ Kadec's theorem can be dramatically improved, first under „small" displacements of the λ_n's and then under more general „vertical" displacements, (YoR) pp. 160 ff.

> **Corollary 1** (YoR) p. 164: Let $\{\lambda_1,\lambda_2,\lambda_3,\dots.\}$ be a sequence of points lying in a strip parallel to the real axis. If the system $\{e^{iRe(\lambda_n))t}\}$ is a Riesz basis for $L_2(-\pi,\pi)$, then so is $\{e^{i\lambda_n t}\}$.
>
> **Corollary 2** (YoR) p. 164: if $\{\lambda_n\}_{n\in Z}$ be a sequence of scalars for which $sup_n|Re(\lambda_n) - n| < 1/4$ and $sup_n|Im(\lambda_n)| < \infty$, then the system $\{e^{i\lambda_n x}\}_{n\in Z}$ is a Riesz basis for $L_2^{\#}(-\pi,\pi)$.

Theorem 13 (YoR) p. 160: If the system $\{e^{i\lambda_n x}\}_{n\in N}$ is a frame in $L_2^{\#}(-\pi,\pi)$, then there is a positive constant L with the property that $\{e^{i\mu_n x}\}_{n\in N}$ is also a frame in $L_2^{\#}(-\pi,\pi)$ whenever

$$|\lambda_n - \mu_n| \le L \text{ for every } n.$$

Corollary (YoR) p. 161: If the system $\{e^{i\lambda_n x}\}_{n\in N}$ is a Riesz basis for $L_2^{\#}(-\pi,\pi)$ then there is a positive constant L with the property that $\{e^{i\mu_n x}\}_{n\in N}$ is also a Riesz basis for $L_2^{\#}(-\pi,\pi)$ whenever

$$|\lambda_n - \mu_n| \le L \text{ for every } n.$$

Theorem 14 (YoR) p. 161: let the sequence $\{\lambda_n\}_{n\in N}$ be a sequence of points lying in a strip parallel to the real axis. If the system $\{e^{iRe(\lambda_n)x}\}_{n\in N}$ is a frame in $L_2^{\#}(-\pi,\pi)$, then so is $\{e^{i\lambda_n x}\}_{n\in N}$.

A striking generalization of the Kadec theorem was discovered by Avdonin:

Avdonin's theorem of $\frac{1}{4}$ – in the mean, (YoR) p. 178: let $\lambda_n = n + \delta_n$, $n = 0,\pm1,\pm2,\dots.$, be a separated sequence of real or complex numbers. If there exists a positive integer N and a constant d, $0 \le d < \frac{1}{4}$, such that

$$\left|\sum_{k=mN+1}^{(m+1)N} \delta_k\right| \le dN$$

for all integers m, then the system $\{e^{i\lambda_n t}\}_{n\in Z}$ is a Riesz basis for $L_2^{\#}(-\pi,\pi)$.

The Paley-Wiener (separable Hilbert) space PW

The Paley-Wiener (separable Hilbert) space PW is the totality of all entire functions of exponential type at most π (i.e., $|f(z)| \leq e^{\pi|z|}$) that are square integrable on the real axis, i.e. it holds

$$|f(x+iy)| \leq e^{\pi|y|}\|f\|.$$

It is equipped with the inner product

$$(f,g) = \int_{-\infty}^{\infty} f(x)\overline{g(x)}dx.$$

Lemma (YoR) p. 90: The Paley-Wiener space PW is isometrically isomorph to $L_2^{\#}(-\pi,\pi)$. Every function $f \in PW$ can be recaptured from its values at the integers, which is achieved by the cardinal series representation of f.

A sequence of real or complex numbers $\{\lambda_n\}_{n\in N}$ is said to be an interpolating sequence for PW if the set of all sequences $\{f(\lambda_n)\}_{n\in N}$ where f ranges over PW, coincides with l^2.

If, in addition, the system $\{e^{i\lambda_n t}\}_{n\in N}$ is complete in $L_2^{\#}(\Gamma)$, then $f(\lambda_n) = c_n$ has exactly one solution, provided $c_n \in l^2$, and in this case we shall call $\{\lambda_n\}_{n\in N}$ a complete interpolating sequence.

A complete interpolation sequence is „maximal“ in the sense that it is not contained in any larger interpolating sequence, and the converse is also true, (YoR) p. 142.

Putting

$$G(z) := z\prod_{k=0\to\infty}(1-\frac{z^2}{\lambda_n^2}) \text{ and } G_n(z) := \frac{G(z)}{G'(\lambda_n)(z-\lambda_n)}$$

then $G_n(z)$ belongs to the Paley-Wiener space PW and $g_n(t)$ is the inverse Fourier transform of $G_n(z)$, i.e. for almost all $t \in [-\pi,\pi]$,

$$g_n(t) := \int_{-\infty}^{\infty} G_n(z)e^{ixt}dt.$$

The exponentials $e^{i\lambda_n t}$ are transformed into the reproducing functions $K_n(z) = \frac{sin\ \pi(z-\lambda_n)}{\pi(z-\lambda_n}$, $g_n(t)$ is transformed into $G_n(z)$, while the moment problem itself becomes

$$f(\lambda_n) = 0, n = 0, \pm1, \pm2, \pm3, \ldots..,$$

since $f(\lambda_n) = (f, K_n)$. Here $c_n \in l^2$ and $f \in PW$ is to be found. By taking the Fourier transform of $\{e^{\mathrm{int}}\}_{n\in Z}$, we see that the set of functions

$$\left\{\frac{sin\ \pi(z-n)}{\pi(z-n)}\right\}_{n\in Z}$$

forms an orthogonal basis for PW. Accordingly every function f in PW has an unique expansion of the form

$$f(z) = \sum_{-\infty}^{\infty} c_n \frac{sin\ \pi(z-n)}{\pi(z-n)} \text{ with } \sum_{-\infty}^{\infty}|c_n|^2 < \infty.$$

The convergence of the series is understood to be in the metric of PW. But convergence in PW implies uniform convergence in each horizontal strip. This is an immediate consequence of the following useful estimate, (YoR) p. 90:

$$|f(x+iy)| \leq e^{\pi|y|}\|f\|.$$

First thoughs about a Hilbert space based circle method to enable proofs of the Goldbach and Kummer conjecture

The Kummer conjecture deals with cubic characters in the form $p = 3k + 1$. This set can be decomposed into

- all odd squares of $3k + 1$
- all even squares of $3k + 1$
- all remaining odd numbers
- all remaining even numbers.

The link to the related $\{4n - 3,4n - 1,2n\}$ decomposition of the set of integers is given by the fact, that the „distance" between the consecutive odd squares of $n = 3k + 1$ is $\{4l - 1\}$, and that the „distance" between the consecutive even squares of of $n = 3k + 1$ is $\{2l\}$. This property provides the conceptual data for an appropriate framework set-up of the proposed two-semicircle method with the following key differentation to the Hardy-Littlewood circle method, (BrK):

Hardy-Littlewood circle method	**Two-semicircle method**
winding number $\mathrm{n} \sim e^{2\pi i n x}$	winding number of functions of Sobolev class $H^{1/2}$ from the circle $\boldsymbol{S^1}$
Hurwitz periodic zeta function $F_s(x) = \sum_{n=1}^{\infty} \frac{e^{2\pi i n x}}{n^s} \in L_\infty(0,1)$	non-harmonic zeta function $G_{s,\nu}(x) = \sum_{n=-\infty}^{\infty} c_\nu(n) \frac{e^{2\pi i \lambda_n x}}{n^s}$ $\left\| u_\nu \sum_{n=-\infty}^{\infty} \frac{c_\nu(n)}{n} e^{2\pi i \lambda_n \cdot} \right\|_{1/2} < \infty,\ s = 1$ $\nu = 1,2,3,4$
zeros of the orthonormal system $\{e^{2\pi i n z}\}$ of $L_2(S^1)$	complex-valued zeros $\{z_n\}_{n\in N}$ of the Kummer function ${}_1F_1\left(\frac{1}{2},\frac{3}{2};z\right)$ and absolute values of their imaginary parts $\lvert Im(z_n)\rvert = 2\pi\omega_n$ and the negative zeros of the Digamma function (*), (BrK)
$\{n\}$	$\{4n - 3,4n - 1,2n\}$ (**)
Gaussian (complex) numbers and cyclotomic polynomial, (CoJ), (HaG)	the group S^3, the unit quaternions of the quaternion algebra $\lvert\boldsymbol{H}$), (***) (BrH1) p. 31
norm: sum of two squares, (MoC)	norm: sum of four squares, (MoC)
Euclidian rotations with fixed winding axis governed by the winding number n	quaternion rotation with dynamic winding axes governed by the odd and even squares of integers resp. their corresponding indices of the retarded/condensed sequence ω_n^* enjoying the Kadec condition

(*) In the context of non-harmonic Fourier series governed by Kadec's theorem and Avdonin's (generalized) theorem of ¼-in the mean we note that the "retarded" sequences of $(2k-1)$ resp. $((4k-3),(4k-1))$ resp. $((8k-7),(8k-5),(8k-3),(8k-1))$ are condensed by the factor ¼. *„It is interesting to note that Euclid's procedure to prove that the sequences of primes is infinite also works starting with* $n = 0$ *, i.e., without any knowledge about primes*", (HaH) S. 4.

(**) We note that the set of even integers is an ideal in the ring of Z. In case the Goldbach conjecture is valid this means that each even integer $2n = p + q$ is the norm of a quaternion if $p, q = 1 mod 4$.

(***) From the fundamental theorem of algebra for quaternions it follows that there are exactly n roots of any quaternion with not vanishing imaginary part, (EbH) 7.1.8; (EbH) p. 204

Every polynomial $X^n - a$, $a \in \lvert\boldsymbol{H}$, *of degree* $n > 0$ *has zeros in every plane in* $\lvert\boldsymbol{H}$ *containing* $0, e,$ *and* a.

References

(AdS) Adler S. L., Quaternionic quantum mechanics and quantum fields, Volume 88 of International Series of Monographs on Physics. The Clarendon Press Oxford University Press, New York, 1995

(AlD) Alpay D., Colombo F., Sabaini I., Inner Product Spaces and Krein Spaces in the Quarternionic Setting, in Springer, Operator Theory: Advances and Applications, pp. 33-65, 2015

(ArI) Arbab A. I.,The analogy between electromagnetism and hydrodynamics, Physics Assays 24, 2, 2011

(BlC) Blohmann C., Fernandes M. C. B., Weinstein, A., Groupoid symmetry and constraints in general relativity, Commun. Contemp. Math., 15, 25 pp. (2013), 1003.2857.pdf (arxiv.org)

(BoA)) Boutet de Monvel-Berthier A, Geogescu V., Purice R., A boundary value problem related to the Ginzburg-Landau model, Commun. Math. Phys. 142, 1-23 (1991)

(BoJ) Bourgain J., Kozma G., One cannot hear the winding number, J. Eur. Math. Soc. 9 (2007), no. 4, pp. 637–658

(BrK) Braun K., A toolbox to solve the RH and to build a non-harmonic Fourier series based two-semicircle method, www.riemann-hypothesis.de

(BrK1) Braun K., An unified field theory enabling a deductive structure of physics, www.riemann-hypothesis.de

(CaJ) Carruth J., Goncalves F., Kelly M., The Beurling-Selberg box minorant problem, arXiv:1702.04579

(CaL) Carlitz L., Note on irregular primes, Proc. Amer. Math. Soc. Vol. 82 (1954) pp. 329-331

(CoB) Coan B., Perng C., Factorization of Hurwitz Quaternions, International Mathematical Forum, Vol. 7, No.2, 2012, 2143 – 2156

(CoJ) Coates J., Sujatha R., Cyclotomic Fields and Zeta Values, Springer, Berlin, Heidelberg, New York, 2006

(CoR) Courant R., Hilbert D., Methods of Mathematical Physics, Volume II, John Wiley & Sons, New York, Chichester, Brisbane, Toronto, Singapore, 1989

(DrP) Draxl P. Über gemeinsame separabel-quadratische Zerfällungskörper von Quaternionenalgebren, Nachrichten der Akademie der Wissenschaften in Göttingen, II. Mathematisch-Physikalische Klasse, Jahrgang 1075, Nr. 16

(DuA) Dunn A., Radziwill M., Bias in cubic Gauss sums, Patterson‘s conjecture, 2109.07463.pdf (arxiv.org)

(EbH) Ebbinghaus H.-D., Numbers, Springer Science + Business Media, New York, 1991

(FiD) Finkelstein D., Jauch J. M., Schiminovich S., and D. Speiser D., Foundations of quaternion quantum mechanics. J. Mathematical Phys., 3:207–220, 1962

(HaG) Hardy G. H., Riesz M., The General Theory of Dirichlet’s Series, Cambridge University Press, Cambridge, 1915

(HaG1) Hardy G. H., Wright E. M., An Introduction to the Theory of Numbers, Oxford University Press, Oxford, 2008

(HaH) Hasse H., Vorlesungen über Zahlentheorie, Springer-Verlag, Berlin, Heidelberg, Göttingen, 1950

(HeD) Heath-Brown D. R., Kummer's conjecture for cubic Gauss sums, Israel J. Math. 120, (2000), no. Part A, pp. 97-124

(HeD1) Heath-Brown D. R., Patterson S. J., The distribution of Kummer sums at prime arguments, Journal für die reine und angewandte Mathematik 310), S. 111-130, 1979

(HeE) Hecke E., Vorlesungen über die Theorie der algebraischen Zahlen, Akademische Verlagsgesellschaft Geest & Portig K.-G., Leipzig, 1954

(HuA) Hurwitz A., Über die Zahlentheorie der Quaternionen, Springer-Verlag, Berlin, 1919
(IvA) Ivic A., The Riemann Zeta-Function, Theory and Applications, Dover Publications, Inc., Mineola, NewYork, 1985

(JeK) Jensen K. L., Om talteorestike Egenskaber ved de Bernoulliske Tal, Nyt Tidsskr. Mat. B (1915) 26, 73-83

(KoJ) Korevaar J., On a question of Brézis and Nirenberg concerning the degree of circle maps, Sel. mathNew ser. 5 (1999) 107-122

(KuE) Kummer E. E., Eine Aufgabe betreffend die Theorie der cubischen Rest, Journal für die reine und angewandte Mathematik, 23, S. 285-286, 1842

(KuE1) Kummer E. E., Allgemeiner Beweis des Fermatschen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoullischen Zahlen als Factoren nicht vorkommen, Journal für die reine und angewandte Mathematik, 40, S. 130-138, 1850

(KuJ) Kuipers J. B., Quaternions & Rotation Sequences, A Primer with Applications to Orbits, Aerospace and Virtual Reality, Princeton University Press, Princeton, New Jersey 1999

(MoC) Moreno C., Wagstaff Jr., S., Sum of Squares of Integers, Chapman & Hall/CRC, Boca Raton, London, New York, 2006

(NaS) Nag S., Sullivan D., Teichmüller theory and the universal period mapping via quantum calculus and the $H^{1/2}$ space on the circle, Osaka J. Math., 32, 1-34, 1995

(PaS) Patterson S. J., On the distribution of Kummer sums, Journal für die reine und angewandte Mathematik 303(304), S. 126-143, 1978

(PoG) Polya G., Über eine neue Weise bestimmte Integrale in der analytischen Zahlentheorie zu gebrauchen, Göttinger Nachr. (1917) 149-159

(SeG) Segal G., Unitary representations of some infinite dimensional groups, Commun. Math. Physics, 80 (1981), 301-342

(ZaD) Zagier D. B., Zetafunktionen und quadratische Körper, Springer-Verlag, Berlin, Heidelberg, New York, 1981