Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 34 (1979)
Heft: 4

Artikel: Die irreduziblen Zahlen des Bereichs Z [Formel]
Autor: Wilker, Peter
DOI: https://doi.org/10.5169/seals-33804

rungen, aber auch von seinen Lehrern und Schülern verlangte er hohe Leistungen. Seine Strenge im Fachlichen war jedoch gepaart mit Milde im menschlichen Bereich. Auch war ihm die Förderung begabter Kinder aus einfachen Volkskreisen ein besonderes Anliegen.
Seit seinem Rücktritt hat sich am MNG einiges geändert, aber in wesentlichen Strukturen erkennt man noch immer den Einfluss seines ersten Leiters. Viele Lehrer und Generationen von ehemaligen Schülern erinnern sich in grosser Dankbarkeit an das Wirken ihres Rektors und Lehrers Paul Buchner.

R. Conzelmann

Die irreduziblen Zahlen des Bereichs $\mathbf{Z}[\sqrt{-5}]$

1. Die Existenz von Zahlbereichen, in denen jedes Element zwar als Produkt irreduzibler Zahlen geschrieben werden kann, die Produktdarstellung aber nicht eindeutig ist, wurde von Eduard Kummer um 1844 erkannt, obwohl sich diese Tatsache schon aus der Theorie der quadratischen Formen von Gauss ergab (vgl. [3]). Der Bereich $\mathbf{Z}[\sqrt{-5}]$, d.h. die Menge der komplexen Zahlen der Form $u+v\sqrt{-5}$ $(u, v \in \mathbf{Z})$, dient als einfaches Beispiel. In ihm sind 3, 7, $1+2\sqrt{-5}$, $1-2\sqrt{-5}$ irreduzibel, und es gilt $21=3\cdot 7=(1+2\sqrt{-5})(1-2\sqrt{-5})$. Dieses und ähnliche Beispiele findet man in allen gängigen Lehrbüchern der Zahlentheorie beschrieben. Der vorliegende Artikel soll die Frage beantworten, welches ganz allgemein die irreduziblen Zahlen von $\mathbf{Z}[\sqrt{-5}]$ sind und wie man andere oder sogar «alle» Beispiele nicht eindeutiger Zerlegbarkeit konstruieren kann. Darüber findet man in der Literatur im allgemeinen nichts oder nichts unmittelbar Ersichtliches, was aber leicht erklärlich ist. In Bereichen mit eindeutiger Faktorzerlegung wie $\mathbf{Z}$ oder $\mathbf{Z}[\sqrt{-1}]$ sind ja die irreduziblen Zahlen mit den Primzahlen identisch und stellen die «Bausteine der Arithmetik» dieser Bereiche dar. In Bereichen wie $\mathbf{Z}[\sqrt{-5}]$ ist dies nicht der Fall, und die irreduziblen Zahlen spielen eine weit geringere Rolle. Zudem ist es in den erstgenannten Bereichen - wie sogleich angedeutet werden soll - verhältnismässig leicht, die Bedingungen anzugeben, denen die irreduziblen Zahlen des Bereichs genügen müssen, während in den andern Bereichen tiefer liegende Hilfsmittel der algebraischen Zahlentheorie angewendet werden müssen.
Wir führen im Bereich der ganzen algebraischen Zahlen eines quadratischen Zahlkörpers $\mathbf{Q}(\sqrt{d})$ die üblichen Begriffe «konjugiert» und «Norm» ein (vgl. dazu etwa [4] und [6]). Konjugiert zu $a=u+v\sqrt{d}$ ist $\bar{a}=u-v\sqrt{d}$; die Norm von a ist $N(a)=a\bar{a}=u^2-dv^2$. Es ist leicht zu kontrollieren, dass $N(\alpha\beta)=N(\alpha)N(\beta)$. Wir erinnern zudem an die Begriffe Einheit: Zahl x mit $x \mid 1$; irreduzible Zahl: Zahl x, keine Einheit, mit ausschliesslich trivialen Teilern x und Einheiten; Primzahl: Zahl x mit $x \mid a$ oder $x \mid b$, falls $x \mid ab$.
Im Bereich $\mathbf{Q}(\sqrt{d})$ gelte nun die Eindeutigkeit der Zerlegbarkeit in irreduzible, das sind gleichzeitig Primzahlen. Sei a irreduzibel mit Norm m und sei m in rationale Primzahlen zerlegt, etwa $m=\pm p_1 p_2 \cdots p_k$. Da $a \mid m$ und da a prim ist, muss schon $a \mid p_i$ für einen Primfaktor p_i von m gelten. Jede irreduzible Zahl des

Bereichs ist also Faktor einer und, wie man leicht sieht, auch nur einer rationalen Primzahl, und es genügt, die Zerlegungen der letzteren zu studieren.
Man bemerkt, dass bei Nichtbestehen der eindeutigen Zerlegbarkeit das vorgebrachte Argument hinfällig wird. Wie sich zeigen wird, ist auch die angeführte Tatsache nicht mehr richtig, und die Verhältnisse hängen entscheidend von der sogenannten Klassenzahl h des Körpers $\mathbf{Q}(\sqrt{d})$ ab. Wir erwähnen, dass $h=1$ notwendig und hinreichend für die Eindeutigkeit der Produktdarstellung durch irreduzible Zahlen ist und dass $\mathbf{Q}(\sqrt{-5})$ die Klassenzahl $h=2$ hat.
Im Rahmen dieses Artikels ist es natürlich nicht möglich, die zur Konstruktion der irreduziblen Zahlen von $\mathbf{Z}[\sqrt{-5}]$ benötigten Sätze der algebraischen Zahlentheorie zu begründen. Sie sollen lediglich erläutert und anschliessend soll gezeigt werden, wie man mit ihrer Hilfe auf elementarem Weg zu einer expliziten Bestimmung der irreduziblen Zahlen kommt. (Zur algebraischen Zahlentheorie vgl. z. B. [7].)

2. Wir erinnern an einige fundamentale Begriffe der Zahlen- und Ringtheorie. Sei R ein (kommutativer) Ring mit Einselement 1. Für $r \in R$ bezeichne Rr das von r erzeugte Hauptideal, bestehend aus allen Vielfachen von r. Man sieht leicht, dass $Rr=R$ gleichwertig ist damit, dass r Einheit des Ringes ist. Ein Ideal P von R heisst prim, wenn $P \neq R$ und wenn aus $ab \in P$ stets $a \in P$ oder $b \in P$ folgt. Es ist klar, dass das Ringelement r genau dann prim ist, wenn das Hauptideal Rr ein Primideal ist.
Es sei nun R der Ring der ganzen algebraischen Zahlen eines Zahlkörpers. Eine fundamentale Tatsache der algebraischen Zahlentheorie besagt, dass sich in R jedes Ideal eindeutig als Produkt von Primidealen schreiben lässt. Wir werden von dieser Tatsache vielfach, meist stillschweigend, Gebrauch machen.
Wie sofort aus der Definition folgt, gilt $\mathbf{Z} \subseteq R$. Ist P ein Primideal von R, so ist $P \cap \mathbf{Z}$, wie sich ebenfalls unmittelbar aus der Definition ergibt, ein Primideal von $\mathbf{Z}$, also ein von einer rationalen Primzahl erzeugtes Hauptideal $\mathbf{Z}p$ von $\mathbf{Z}$. Dadurch wird P eindeutig eine Primzahl p zugeordnet, und man sagt, P liege über p.
Ist umgekehrt p eine rationale Primzahl, so betrachte man das von p im ganzen Ring R erzeugte Hauptideal Rp, das sich eindeutig als Produkt von Primidealen aus R darstellen lässt. Es gilt die weitere fundamentale Tatsache, dass die bei dieser Produktdarstellung auftretenden Primideale genau die über p liegenden sind.
Für quadratische Zahlkörper lässt sich diese Produktdarstellung einfach beschreiben durch

Satz 1. *Ist p eine rationale Primzahl und ist R der Ring der ganzen algebraischen Zahlen eines quadratischen Zahlkörpers $\mathbf{Q}(\sqrt{d})$, so gibt es für die Darstellung von Rp als Produkt von Primidealen aus R drei Möglichkeiten*:

(V) $Rp=P^2$ mit einem Primideal P («p ist verzweigt»).
(Z) $Rp=P_1P_2$ mit zwei verschiedenen Primidealen P_1, P_2 («p ist zerlegt»).
(T) Rp ist selber Primideal («p ist träge»).

Es lässt sich stets angeben, welcher der drei Fälle für eine gegebene Primzahl p eintritt. Wir stellen die Kriterien gerade für den Ring $\mathbf{Z}[\sqrt{-5}]$ dar, der im folgenden kurz mit A bezeichnet werden soll.

(V) tritt ein, wenn p die sogenannte Diskriminante von A teilt. Diese ist gleich -20; somit sind 2 und 5 die einzigen verzweigten Primzahlen.
(Z) tritt ein für $p \neq 2, 5$, wenn die quadratische Kongruenz $x^2 \equiv -5 \bmod p$ lösbar ist. Unter Verwendung des quadratischen Reziprozitätsgesetzes lassen sich die zugehörigen p leicht angeben. Wir verzichten auf die einfache Durchrechnung und führen nur das Resultat an: p ist zerlegt dann und nur dann, wenn $p \equiv 1, 3, 7$ oder $9 \bmod 20$ ist.
(T) tritt ein für p, wenn $x^2 \equiv -5 \bmod p$ nicht lösbar ist. Dies liefert natürlich $p \equiv 11, 13, 17$ oder $19 \bmod 20$ als träge Primzahlen.

3. Wir wollen im folgenden zur Vereinfachung der Ausdrucksweise ein Ideal von A, das nicht ein Hauptideal ist, «echt» nennen. Von der oben erwähnten Tatsache, dass die Klassenzahl von A gleich 2 ist, benötigen wir für unsere Zwecke lediglich die folgenden Tatsachen:

Satz 2. *Das Produkt zweier echter Primideale von A ist ein Hauptideal. Das Produkt eines echten Primideals mit einem Hauptideal ist ein echtes Ideal.*

Bevor wir einen für unsere Zwecke sehr nützlichen Hilfssatz ableiten, sei erwähnt, dass die Einheiten von A die Zahlen ± 1 sind. Denn eine Einheit $u + v\sqrt{-5}$ hat, weil sie 1 teilt, die Norm 1, und die Gleichung $1 = u^2 + 5v^2$ lässt nur die Lösungen $u = \pm 1$, $v = 0$ zu.

Hilfssatz 1. *Sei $\alpha \in A$ und $A\alpha = P_1 P_2 \cdots P_n$ die Zerlegung des Hauptideals $A\alpha$ in Primideale von A. α ist in A dann und nur dann irreduzibel, wenn $n = 1$ oder wenn $n = 2$ und die beiden auftretenden Primideale echt sind.*

Beweis: Sei α irreduzibel. Aus Satz 2 folgt sofort, dass die Anzahl der echten unter den Primidealen P_i gerade sein muss. Fasst man sie paarweise zusammen, so erhält man eine Darstellung von $A\alpha$ als Produkt von Hauptidealen, etwa $A\alpha = A\beta_1 A\beta_2 \cdots A\beta_m$. Dies bedeutet $\alpha = \pm \beta_1 \beta_2 \cdots \beta_m$, was aber wegen der Irreduzibilität von α nur für $m = 1$ möglich ist. Folglich ist also entweder $A\alpha$ selber ein Primideal, oder aber es ist Produkt zweier echter Primideale.
Sei umgekehrt $A\alpha = P$, ein Primideal, aber α ein Produkt, etwa $\alpha = \beta_1 \beta_2$. Dann is $A\alpha = A\beta_1 A\beta_2 = P$, so dass infolge der Eindeutigkeit der Produktdarstellung durch Primideale z. B. $A\beta_1 = P$ und $A\beta_2 = A$ sein muss. Dann ist aber β_2 eine Einheit, und die Zerlegung von α war nicht echt. α ist also irreduzibel.
Ist schliesslich $A\alpha = P_1 P_2$, mit echten Primidealen P_1 und P_2, aber wieder $\alpha = \beta_1 \beta_2$, so muss β_1 oder β_2 eine Einheit sein. Andernfalls wäre nämlich z. B. $A\beta_1 = P_1$, $A\beta_2 = P_2$, und P_1 sowie P_2 wären nicht echt.
Wir fügen hier noch einen weiteren, ganz elementaren Hilfssatz an.

Hilfssatz 2. *Seien α, β irreduzible Zahlen von A, die nicht zu $\mathbf{Z}$ gehören, während $\alpha\beta \in \mathbf{Z}$ gelte. Dann ist $\beta = \pm \bar{\alpha}$.*

Beweis: Aus $\alpha\beta = k \in \mathbf{Z}$ folgt $\alpha\bar{\alpha}\beta = N(\alpha)\beta = k\bar{\alpha}$, also $\beta = (k/N(\alpha))\,\bar{\alpha}$. $k/N(\alpha)$ ist eine rationale Zahl, und wir nehmen an, sie sei in die Form r/s mit teiler-

fremden r, s und $s>0$ gebracht. Da die Komponenten von β ganzzahlig sind, muss $\bar{\alpha}=s\gamma$ für ein $\gamma\in A$ gelten, was wegen der Irreduzibilität von α und der Voraussetzung $\alpha\notin\mathbf{Z}$ auf $s=1$ führt. Aber $\beta=r\bar{\alpha}$ ist wieder nur für $r=\pm 1$ möglich.

4. Wir betrachten nochmals Satz 1 und wollen Kriterien dafür suchen, wann in den Fällen (V) und (Z) die auftretenden Primideale P bzw. P_1, P_2 Hauptideale sind und wann echt.
Im Falle (V) ist diese Frage leicht zu beantworten. Ist P ein Hauptideal, $P=A\alpha$, mit $\alpha=u+v\sqrt{-5}$, so gilt $Ap=(A\alpha)^2=A\alpha^2$, also $p=\pm\alpha^2$. Berechnet man beidseits die Normen, so findet man $N(p)=p^2=N(\alpha^2)=N(\alpha)^2$, also $N(\alpha)=p=u^2+5v^2$. p ist entweder 2 oder 5. Die diophantische Gleichung $2=u^2+5v^2$ ist unlösbar, hingegen hat $5=u^2+5v^2$ die Lösungen $u=0$, $v=\pm 1$. Somit ist P für 2 ein echtes Primideal, für 5 das Hauptideal $A\sqrt{-5}$.
Wann im Falle (Z) für $Ap=P_1P_2$ Hauptideale auftreten, ist eine tiefer liegende Frage. Sei $P_1=A\alpha_1$, $P_2=A\alpha_2$. Es folgt $A\alpha_1\alpha_2=Ap$, also $\alpha_1\alpha_2=\pm p\in\mathbf{Z}$, während offenbar α_1 und α_2 nicht zu $\mathbf{Z}$ gehören. Nach Hilfssatz 1 sind α_1 und α_2 irreduzibel, nach Hilfssatz 2 gilt $\alpha_2=\pm\bar{\alpha}_1$. Setzt man $\alpha_1=u+v\sqrt{-5}$, so gilt somit $p=\alpha_1\bar{\alpha}_1=u^2+5v^2$.
Damit also bei $Ap=P_1P_2$ Hauptideale auftreten können, muss $p=u^2+5v^2$ lösbar sein. Ist dies umgekehrt der Fall, ist (u,v) eine Lösung, und setzt man $\alpha=u+v\sqrt{-5}$, so wird $p=\alpha\bar{\alpha}$, $Ap=A\alpha A\bar{\alpha}$, und gemäss Satz 1 müssen $A\alpha$ und $A\bar{\alpha}$ Primideale sein.
Da wir uns im Falle (Z) befinden, gilt $p\equiv 1, 3, 7$ oder $9 \bmod 20$. Betrachtet man die Gleichung $p=u^2+5v^2$ modulo5, so bedeutet ihre Lösbarkeit, dass $u^2\equiv p \bmod 5$ gelten muss. Dies ist offenbar nur für $p\equiv 1$ oder $4 \bmod 5$ möglich, was dazu führt, dass mod20 nur $p\equiv 1$ oder 9 in Frage kommen.
Damit ist unsere Fragestellung auf die nach der Lösbarkeit der diophantischen Gleichung $u^2+5v^2=p$ für Primzahlen $p\equiv 1$ oder $9 \bmod 20$ zurückgeführt. Es gilt nun

Satz 3. *Die diophantische Gleichung $u^2+5v^2=p$ ist für eine Primzahl $p\equiv 1$ oder $9 \bmod 20$ stets lösbar.*

Satz 3 ergibt sich aus der Theorie der quadratischen Formen von Gauss (vgl. [2]) oder auch direkt mittels des Minkowskischen Satzes über Linearformen (vgl. [5]). Wir werden übrigens auf die Existenzaussage von Satz 3 am Schluss dieses Artikels zurückkommen. Aufgrund der vorstehenden Ergebnisse lassen sich bereits die rationalen Primzahlen angeben, die in A irreduzibel bleiben. Es sind dies einmal die trägen Primzahlen $p\equiv 11, 13, 17, 19 \bmod 20$ sowie diejenigen zerlegbaren, bei denen Ap das Produkt zweier echter Primideale ist. Wie gerade gezeigt, sind das die Primzahlen $p\equiv 3, 7 \bmod 20$. Schliesslich ist im Falle (V) noch 2 irreduzibel in A.
Wir fassen zusammen: Irreduzibel in A sind
(1) rationale Primzahlen $p\equiv 3, 7, 11, 13, 17, 19 \bmod 20$ sowie $p=2$.

5. Nun soll die Bestimmung der irreduziblen, aber nicht zu $\mathbf{Z}$ gehörenden Elemente

von A in Angriff genommen werden. Wir schreiben für sie generell $a=u+v\sqrt{-5}$ und gehen so vor, dass wir Aa betrachten, notwendige Bedingungen für die Irreduzibilität von a ableiten und zeigen, dass sie auch hinreichend sind.
Zur Vereinfachung der Ausdrucksweise soll im folgenden a als «Lösung» der diophantischen Gleichung $u^2+5v^2=N(a)$ betrachtet werden. Es ist klar, dass neben a auch $-a$, $\pm\bar{a}$ Lösungen sind. Sie werden als nicht wesentlich verschieden angesehen.
Das Hauptideal Aa kann selber prim sein; wir wollen das in diesem Abschnitt voraussetzen. Aa liegt dann über einer rationalen Primzahl p und wird bei der Produktdarstellung von Ap als Faktor auftreten. Die genauen Verhältnisse hängen davon ab, welcher der Bedingungen (V), (T) oder (Z) die Zahl p genügt.

(V) p ist verzweigt, d.h. $Ap=(Aa)^2=Aa^2$ und $p=\pm a^2$. Anderseits muss p gleich 2 oder 5 sein. Wie bereits gezeigt, kommt nur 5 in Frage, woraus $a=\sqrt{-5}$ folgt. Dass $\sqrt{-5}$ tatsächlich irreduzibel ist, folgt z.B. daraus, dass $N(\sqrt{-5})=5$ ist.

(T) p ist träge, d.h. Ap ist ein Primideal, $Ap=Aa$ und $a=\pm p$. Dieser Fall wurde bereits besprochen.

(Z) p ist zerlegt, d.h. $Ap=P_1P_2$ mit z.B. $Aa=P_1$. Aus Satz 2 folgt, dass auch P_2 ein Hauptideal sein muss, etwa $P_2=A\beta$. Somit gilt $Ap=Aa\,A\beta=A(a\beta)$ und $a\beta=\pm p$. Aus Hilfssatz 1 folgt die Irreduzibilität von β. a und β können nicht ganzzahlig sein, so dass nach Hilfssatz 2 gelten muss: $\beta=\pm\bar{a}$, $p=a\bar{a}=N(a)=u^2+5v^2$.

Wie in Abschnitt 4 gezeigt, ist die Lösbarkeit der diophantischen Gleichung $p=u^2+5v^2$ gleichwertig mit $p\equiv 1, 9 \bmod 20$. Sie hat übrigens nur eine Lösung a. Denn wäre γ eine weitere Lösung, $p=\gamma\bar{\gamma}$, so würde $Ap=A\gamma\,A\bar{\gamma}=P_1P_2$, also z.B. $A\gamma=P_1=Aa$ und $\gamma=\pm a$, folgen.
Man sieht nun umgekehrt sofort, dass jede Lösung a einer Gleichung der angegebenen Art in A irreduzibel ist. Denn aus $Ap=Aa\,A\bar{a}$ folgt aufgrund der Annahme, dass p zerlegbar ist, dass Aa ein Primideal sein muss, worauf man Hilfssatz 1 anwenden kann.
Bevor wir die Ergebnisse dieses Abschnitts zusammenfassen, sei bemerkt, dass wir nur einen Wert von a angeben. Stets sind auch $-a$ und $\pm\bar{a}$ zusammen mit a irreduzibel.
Irreduzibel in A sind
(2) $\sqrt{-5}$,
(3) Lösungen a der Gleichung $p=u^2+5v^2$, p eine rationale Primzahl $\equiv 1$ oder $9 \bmod 20$ (p bestimmt a eindeutig).

6. Wir wollen jetzt den Fall betrachten, dass Aa selber nicht prim ist. Nach Hilfssatz 1 ist dann Aa das Produkt zweier echter Primideale. Die beiden Ideale können gleich sein, so dass $Aa=P^2$. Wir wollen das für diesen Abschnitt voraussetzen.
P liegt über einer rationalen Primzahl p, und wieder sind die drei Möglichkeiten (T), (V) und (Z) zu berücksichtigen. (T) scheidet allerdings aus, denn ist

Ap ein Primideal, so muss $Ap=P$ gelten, und P wäre nicht echt. Aber auch (V) ist bereits erledigt, da $Ap=P^2=Aa$ auf $a=\pm p$ führt. Es bleibt also noch

(Z) p ist zerlegt, und es gilt $Ap=PQ$ mit einem weiteren echten Primideal Q. Für das Hauptideal Ap^2 ist dann $Ap^2=P^2Q^2=Aa\,Q^2$. Aufgrund von Satz 2 ist Q^2 ein Hauptideal, etwa $Q^2=A\beta$, und es folgt $a\beta=\pm p^2$. Aus Hilfssatz 1 ergibt sich β als irreduzibel, aus Hilfssatz 2 folgt $\beta=\pm\bar{a}$. Somit ist $p^2=a\bar{a}=N(a)$ $=u^2+5v^2$.

Wir wissen bereits, dass $p\equiv 3$ oder 7 mod 20 ist und müssen nun beweisen, dass die Gleichung $p^2=u^2+5v^2$ neben $u=p$, $v=0$ noch eine weitere Lösung $a\notin\mathbf{Z}$ besitzt. Dies lässt sich ohne Zuhilfenahme neuer zahlentheoretischer Sätze beweisen, indem man die soeben gegebenen Argumente rückwärts verfolgt: p ist zerlegt, also $Ap=PQ$, und P,Q sind echt wegen $p\not\equiv 1, 9$ mod 20. Es folgt Ap^2 $=P^2Q^2$, und nach Satz 2 muss $P^2=Aa$, $Q^2=A\beta$, somit $p^2=a\beta$ gelten. Wäre $a\in\mathbf{Z}$, so auch $\beta=\pm\bar{a}$, und es würde $a=\pm p$ folgen. Dann wäre aber p verzweigt, im Widerspruch zur Voraussetzung.
Wir haben damit gezeigt: Irreduzibel in A sind
(4) Lösungen a der Gleichung $p^2=u^2+5v^2$, p eine rationale Primzahl $\equiv 3$ oder 7 mod 20 (p bestimmt $a\notin\mathbf{Z}$ eindeutig).

7. Wir kommen zum letzten Fall, nämlich $Aa=P_1P_2$, beides echte und voneinander verschiedene Primideale. P_1 liege über der rationalen Primzahl p_1, P_2 über p_2. $p_1=p_2=p$ ist möglich, liefert aber keine neuen irreduziblen Zahlen. Es gilt dann nämlich $Ap=P_1P_2=Aa$, also $a=\pm p$. Wir dürfen somit $p_1\neq p_2$ annehmen.
Keine der beiden Primzahlen p_1,p_2 kann träge sein, da sonst P_1 und P_2 nicht echt wären. Somit gilt $Ap_1=P_1Q_1$, $Ap_2=P_2Q_2$ mit echten Primidealen Q_1,Q_2. Nach Satz 2 und Hilfssatz 1 ist $Q_1Q_2=A\beta$ für ein irreduzibles β, und Ap_1p_2 $=P_1Q_1P_2Q_2=Aa\,A\beta$ führt auf $a\beta=\pm p_1p_2$, $\beta=\pm\bar{a}$.
Eine der beiden Primzahlen p_i kann verzweigt sein. Ist es z.B. p_1, also $Ap_1=P_1^2$, so muss, wie bewiesen, $p_1=2$ gelten. Wegen $P_1\neq P_2$ ist dann $p_2=2$ ausgeschlossen. Setzen wir $p_2=p$, so ist p zerlegt, also gemäss Abschnitt 4 $p\equiv 3, 7$ mod 20 und a berechnet sich aus $2p=u^2+5v^2$. Dass diese Gleichung tatsächlich eine und nur eine Lösung besitzt, zeigt man wie in Abschnitt 6.
Abschliessend ist noch der Fall (Z) für p_1 wie auch p_2 zu untersuchen; beides müssen Primzahlen $\equiv 3, 7$ mod 20 sein. a genügt der Gleichung $p_1p_2=u^2+5v^2$, diesmal aber stellt es sich heraus, dass sie zwei wesentlich verschiedene Lösungen besitzt. Denn die Ausgangsbeziehung $Ap_1p_2=P_1Q_1P_2Q_2$ lässt auch die Anordnung $(P_1Q_2)(P_2Q_1)$ zu. Es wird $P_1Q_2=A\gamma, P_2Q_1=A\bar{\gamma}$, und γ ist ebenfalls Lösung von $p_1p_2=u^2+5v^2$. γ kann keine der Zahlen $\pm a$, $\pm\bar{a}$ sein, Denn ist z.B. $\gamma=a$, so auch $P_1Q_2=P_1P_2$, was auf $P_2=Q_2$ führt, d.h. p_2 wäre verzweigt. Eine dritte Lösung der Gleichung ist offenbach unmöglich.
Damit erhalten wir als letzte Serie von irreduziblen Zahlen des Bereichs A:
(5) Lösungen a der Gleichung $2p=u^2+5v^2$, p eine rationale Primzahl $\equiv 3, 7$ mod 20 (p bestimmt a eindeutig).
(6) Lösungen a der Gleichung $p_1p_2=u^2+5v^2$, p_1 und p_2 rationale Primzahlen $\equiv 3, 7$ mod 20. (Die Gleichung hat zwei wesentlich verschiedene Lösungen.)

Es ist klar, dass Serie (4) ein Spezialfall von Serie (6) ist. Neben den Einzelzahlen 2 und $\sqrt{-5}$ gibt es also vier unendliche Serien irreduzibler Zahlen in $\mathbf{Z}[\sqrt{-5}]$.
Die eingangs erwähnte Frage, wie sich in $\mathbf{Z}[\sqrt{-5}]$ weitere bzw. «alle» Beispiele nicht eindeutiger Faktorzerlegung ganzer Zahlen konstruieren lassen, ist jetzt leicht zu beantworten. Offenbar muss in der rationalen Primfaktorzerlegung einer solchen Zahl ein Produkt einer der Formen $2p$ oder p_1p_2 mit $p, p_1, p_2 \equiv 3, 7 \bmod 20$ vorkommen. Die kleinsten Zahlen dieser Art sind $6 = 2 \cdot 3 = (1+\sqrt{-5})\ (1-\sqrt{-5})$, $9 = 3 \cdot 3 = (2+\sqrt{-5})\ (2-\sqrt{-5})$, $21 = 3 \cdot 7 = (1+2\sqrt{-5})\,(1-2\sqrt{-5}) = (4+\sqrt{-5})\,(4-\sqrt{-5})$.

8. Dieser letzte Abschnitt des Artikels sei einigen zusätzlichen Bemerkungen gewidmet. Es ist aufgrund unserer Ergebnisse leicht, nun auch die Primzahlen des Bereichs $\mathbf{Z}[\sqrt{-5}]$ zu charakterisieren, die ja unter den aufgefundenen irreduziblen Zahlen vorkommen müssen. Wie bereits erwähnt, muss Aa ein Primideal sein, damit a prim ist. Durchgeht man unsere Liste, so findet man sofort, dass in $\mathbf{Z}[\sqrt{-5}]$ prim sind:
(1) die trägen rationalen Primzahlen $p \equiv 11, 13, 17, 19 \bmod 20$,
(2) $\sqrt{-5}$,
(3) Lösungen a von $p = u^2 + 5v^2$, $p \equiv 1, 9 \bmod 20$.

Wird eines der «kritischen» Produkte $2p$ bzw. p_1p_2 in irreduzible, nicht ganzzahlige Faktoren zerlegt, so treten jeweils deren zwei auf. Obwohl also eine ganze Zahl m mehrere Produktdarstellungen zulassen kann, ist die Anzahl der auftretenden Faktoren bei gegebenem m stets dieselbe. Dieses Phänomen beruht ausschliesslich auf der Klassenzahl 2, denn es wurde bewiesen, dass für beliebige Zahlkörper die Konstanz der Faktorenzahl in den verschiedenen Zerlegungen einer ganzen Zahl äquivalent ist dazu, dass der Körper die Klassenzahl 1 oder 2 hat (siehe [1]).
Es ist einleuchtend, dass sich die in diesem Artikel angewandte Methode zur Bestimmung der irreduziblen Zahlen auf andere Zahlkörper $\mathbf{Q}(\sqrt{d})$ der Klassenzahl 2 und negativem d übertragen lässt. Man weiss seit kurzem, dass es genau 17 solcher Körper gibt, nämlich für $-d = 5, 6, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 267, 403, 427$ (siehe [8]).
Zum Schluss soll noch die Frage aufgegriffen werden, wie sich die irreduziblen Elemente von $\mathbf{Z}[\sqrt{-5}]$ effektiv bestimmen lassen. Dazu sind zweierlei Schritte nötig. Erstens muss der Primzahlcharakter von Zahlen festgestellt und auch entschieden werden, zu welcher Restklasse mod 20 sie gehören. Dafür sind natürlich zahlreiche Verfahren bekannt. Im weiteren ist es dann nötig, diophantische Gleichungen der Form $m = u^2 + 5v^2$ zu lösen. Das kann im Prinzip in endlich vielen Schritten geschehen, doch wird man nach einem effizienten Verfahren suchen. Für die Gleichung $m = u^2 + v^2$, deren Lösungen die irreduziblen Zahlen von $\mathbf{Z}[\sqrt{-1}]$ beherrschen, sind solche Verfahren seit langem bekannt. Der Autor hat einen Algorithmus auch zur Lösung der ersten Gleichung entwickelt, der wie bei der zweiten mit einer Spielart des euklidischen Algorithmus vorgeht. Der (nicht ganz einfache) Beweis für die Durchführbarkeit des Algorithmus liefert

gleichzeitig eine Existenzaussage für die Lösung der diophantischen Gleichung, und dies auch im Falle von Primzahlen $\equiv 1$ oder 9 mod20 (siehe oben Satz 3). Die Überlegungen sollen an anderer Stelle publiziert werden. Peter Wilker, Bern

LITERATURVERZEICHNIS

1 L. Carlitz: A characterization of algebraic number fields with class number 2. Proc. Am. Math. Soc. 11, 391-392 (1960).
2 P.G.L. Dirichlet und R. Dedekind: Vorlesungen über Zahlentheorie.
3 H.M. Edwards: The background of Kummer's proof of Fermat's Last Theorem for regular primes. Arch. Hist. Exact Sci. 14, 219-236 (1974/75).
4 G.H. Hardy und E.M. Wright: An introduction to the theory of numbers. Oxford University Press, 1954.
5 L.J. Mordell: Diophantine equations. Academic Press, 1969.
6 J. Niven und H.S. Zuckerman: An introduction to the theory of numbers. Wiley, 1960.
7 P. Ribenboim: Algebraic numbers. Wiley, 1972.
8 H.M. Stark: On complex quadratic fields with class number two. Math. Comput. *29*, 289-302 (1975).

Kleine Mitteilungen

Some equations involving the sum of divisors

Pomerance [2] considered the sets $S_k(a)=\{n:\sigma(n)=kn+a\}$ $(a,k\in\mathbf{Z})$. He observed that the sets $S_{\sigma(m)/m}(\sigma(m))$ if $m\mid\sigma(m)$ and $S_2(-1)$ are infinite and wrote: "We know of no other example." Below we give other examples of infinite $S_k(a)$.

Proposition 1. *If m is a positive integer not divisible by a prime number p and such that $\sigma(m)=(p-1)m$ then $p^k m\in S_p(-m)$ for natural k.*

Proof: $\sigma(p^k m)=\sigma(m)(p^{k+1}-1)/(p-1)=(p^{k+1}-1)m=p\cdot p^k m-m$.
For instance we have $3^k\cdot P\in S_3(-P)$, where P is a perfect number not divisible by 3, e.g. $P=28$ or $2^{19936}(2^{19937}-1)$. Similarly, $5^k\cdot Q\in S_5(-Q)$, where $\sigma(Q)=4Q$ and $5\nmid Q$, e.g. $Q=2^9\cdot 3^2\cdot 7\cdot 11\cdot 13\cdot 31$ or $2^{13}\cdot 3^2\cdot 7\cdot 11\cdot 13\cdot 43\cdot 127$ (R. Descartes).
Eleven numbers of the set $S_2(2)$ were listed in the paper [1]. We generalize the result stated there (case $b=1$).

Proposition 2. *If 2^a-2b-1 is a prime number $(b\in\mathbf{Z})$ then $2^a-2b-1)\in S_2(2b)$.*

Proof: $\sigma\left(2^{a-1}(2^a-2b-1)\right)=(2^a-1)(2^a-2b)=2^{2a}-2^{a+1}b-2^a+2b$
$=2\cdot 2^{a-1}(2^a-2b-1)+2b$.

Andrzej Makowski, Institute of Mathematics, University of Warsaw

REFERENCES

1 A. Makowski: Remarques sur les fonctions $\theta(n)$, $\varphi(n)$ et $\sigma(n)$. Mathesis *69*, 302-303 (1960).
2 C. Pomerance: On the congruences $\sigma(n)\equiv a \pmod n$ and $n\equiv a \pmod{\varphi(n)}$. Acta Arith. *26*, 265-272 (1975).