Primzahlen der Form 4k + 1 sind Summe von zwei Quadratzahlen

Bemerkungen zu einer neuen Beweisidee

von Christian Elsholtz

Christian Elsholtz, geb. 1971, hat diese Arbeit als Beitrag für den Wettbewerb „Jugend forscht" verfaßt. Sie wurde 1991 mit dem 4. Bundespreis prämiert. Er studiert zur Zeit Mathematik an der Universität Oxford.

1. Einführung und Beweisskizze

1.1 Einführung

Neben vielen interessanten Sätzen der Zahlentheorie wurde auch dieser Satz durch Fermat bekannt. Wieder einmal behauptete er, einen (nicht überlieferten) Beweis zu haben. Der erste überlieferte Beweis stammt von Euler. Seitdem sind viele verschiedene Beweise dieses Satzes veröffentlicht worden. Darüber hinaus wurde auch bewiesen, daß für jede Primzahl der Form 4k+1 genau eine Zerlegung in zwei Quadratzahlen existiert.

Im Februar 1990 veröffentlichte D. Zagier in „American Mathematical Monthly" [1] einen neuen Beweis, der auf einer völlig neuen Beweisidee beruht. Zagiers Beweis ist eine Vereinfachung eines Beweises von R. Heath-Brown, der bereits Liouvilles Ideen vereinfachte. Der Beweis ist zum einen extrem kurz, zum anderen ist die Beweisidee allgemein verständlich; die mathematischen Hilfsmittel sind elementar. Allerdings ist das Nachrechnen mühsam, so daß man den Beweis auf den ersten Blick kaum versteht. Im Rahmen des Studiums haben wir anhand eines Übungsblattes den Beweis nachvollzogen, d. h. wir haben geprüft, ob die vom Autor aufgestellten Behauptungen stimmen und das Geforderte leisten.

1.2 Beweisskizze

Im folgenden gebe ich zunächst Zagiers Beweis wieder; er ist im englischen Original nur einen Satz lang.

Man bildet die endliche Lösungsmenge der Gleichung $x^2 + 4yz = p$ ($x, y, z \in \mathbb{N}$, p Primzahl der Form 4k+1) mittels der Abbildung

$$\alpha\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{cases}\begin{pmatrix}x+2z\\z\\y-x-z\end{pmatrix}, & \text{falls } x < y-z\\ \begin{pmatrix}2y-x\\y\\x-y+z\end{pmatrix}, & \text{falls } y-z < x < 2y\\ \begin{pmatrix}x-2y\\x-y+z\\y\end{pmatrix}, & \text{falls } x > 2y\end{cases}$$

involutorisch auf sich selbst ab ($\alpha \cdot \alpha = \mathrm{id}$). Diese Abbildung hat genau einen Fixpunkt; daher hat die Lösungsmenge eine ungerade Zahl an Elementen. Bezüglich der Involution

$$\beta\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x\\z\\y\end{pmatrix}$$

existiert dann auch ein Fixpunkt.

Soweit der Beweis. Ich gebe hierzu noch einige Erläuterungen. Man will die *Existenz* einer Lösung der Gleichung $x^2 + a^2 = p = 4k + 1$ beweisen. Zunächst ist klar, daß entweder x oder a gerade sein muß, so daß man o. B. d. A. $a = 2y$ setzen kann. Nun will man die Existenz einer Lösung der Gleichung $x^2 + 4y^2 = p$ beweisen. Dazu wendet man einen Trick an, dessen Sinn man erst am Ende versteht: Man macht die Sache komplizierter und betrachtet die Lösungsmenge der Gleichung $x^2 + 4yz = p$ ($x, y, z \in \mathbb{N}$).

Man bildet diese Lösungsmenge auf zwei verschiedene Arten involutorisch auf sich selbst ab. (Bei einer Involution f ordnet man jeder Lösung bijektiv eine – nicht unbedingt verschiedene – Lösung zu, so daß gilt: $f \cdot f = \mathrm{id}$. Lösungen, die auf sich selbst abgebildet werden, heißen Fixpunkte).

Bezüglich Zagiers erster Abbildung kann man verhältnismäßig leicht zeigen, daß genau ein Fixpunkt existiert. Das bedeutet aber, daß die Lösungen der Gleichung $x^2 + 4yz = p$ paarweise zugeordnet werden können, nur für den Fixpunkt existiert kein (verschiedener) Partner, so daß die Anzahl der Lösungen ungerade ist.

Kehrt man die Argumentation um, so muß bezüglich jeder anderen Involution eine ungerade Anzahl an Fixpunkten existieren. Es gibt also mindestens einen Fixpunkt!

Zagiers zweite Abbildung

$$\beta\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x\\z\\y\end{pmatrix}$$

ist eine Involution. Für den Fixpunkt gilt dann aber $y = z$, so daß

$$x^2 + 4yz = x^2 + 4y^2 = x^2 + (2y)^2 = p = 4k+1$$

folgt. Soweit die eigentliche Beweisidee.

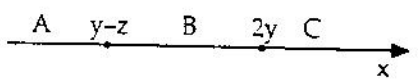
Zagier hat dem Leser Arbeit überlassen:

Der Beweis funktioniert nur, wenn die Lösungsmenge endlich ist; dies ist jedoch dadurch gewährleistet, daß eine (durch p) nach oben beschränkte Summe positiver Zahlen vorliegt.

Der Nachweis, daß α eine Involution ist, ist etwas aufwendiger:

Die Lösungsmenge der Gleichung $x^2 + 4yz = p$ wird durch $x < y - z$; $y - z < x < 2y$; $x > 2y$ in drei disjunkte Teilmengen A, B und C zerlegt.

(Eine Lösung der Gleichung, für die $x < y - z$ gilt, liege in A usw.)



$x = y - z$ und $x = 2y$ kann nicht gelten, da sonst $x^2 + 4yz$ keine Primzahl wäre.

Jede Lösung $\begin{pmatrix}x\\y\\z\end{pmatrix}$ der Gleichung liegt also in genau einer der Teilmengen A; B und C.

Der Nachweis, daß α eine Involution ist, wird leichter, nachdem man erkannt hat, daß Lösungen aus A auf Lösungen aus C (und umgekehrt) abgebildet werden; Lösungen aus B werden auf Lösungen aus B abgebildet. Dies sei hier nur für eine Lösung aus A durchgeführt:

$$\alpha_A\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x+2z\\z\\y-x-z\end{pmatrix}.$$

Es gilt also $x' > 2y'$ und $x', y', z' \in \mathbb{N}$ und

$$(x')^2 + 4y'z' = x^2 + 4xz + 4z^2 + 4yz - 4xz - 4z^2 = x^2 + 4yz.$$

Daher bildet α Elemente aus A nach C ab.

$$\alpha_C\begin{pmatrix}x'\\y'\\z'\end{pmatrix} = \begin{pmatrix}x'-2y'\\x'-y'+z'\\y'\end{pmatrix}$$

$$= \begin{pmatrix}x+2z-2z\\x+2z-z+y-x-z\\z\end{pmatrix} = \begin{pmatrix}x\\y\\z\end{pmatrix}$$

Nochmalige Anwendung von α führt also wieder zur Ausgangslösung. Ein Fixpunkt von α kann dann natürlich nur in B liegen:

$$\alpha_B\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}2y-x\\y\\x-y+z\end{pmatrix}\overset{!}{=}\begin{pmatrix}x\\y\\z\end{pmatrix}.$$

Dies ist nur gegeben, wenn $x = y$.

Damit $x^2 + 4yz = x^2 + 4xz = x(x + 4z)$ = Primzahl, muß aber $x = y = 1$ gelten. Es folgt $z = k$. Der einzige Fixpunkt von α ist also

$$\begin{pmatrix}1\\1\\k\end{pmatrix}.$$

2. Vorüberlegungen zur Bestimmung der Abbildung

Bisher handelt es sich nicht um meine eigene Leistung, denn zum einen stammt weder die Beweisidee noch der Beweis von mir, zum anderen ist die bisherige Beweisskizze anhand eines Übungsblattes während des Studiums entstanden.

Antrieb zur weiteren Beschäftigung mit diesem Thema war für mich die Frage:

Wie kann man auf einen solchen Beweis, insbesondere auf diese merkwürdige Abbildung α kommen?

Gibt es nicht eine einfachere Abbildung, die dasselbe leistet, d. h. nachweist, daß die Anzahl der Lösungen von $x^2 + 4yz = p$ ungerade ist?

Bei meinen Überlegungen will ich versuchen, folgende „Beweismotive" anzuwenden:

1. Die Einfachheit: Wenn ich die Wahl zwischen Alternativen habe, werde ich die wählen, die mir am einfachsten erscheint. So einfach wie möglich, so kompliziert wie nötig.
2. Das Spiegel- bzw. Symmetrieprinzip: Wenn ein Problem nicht von vorne lösbar ist, dann vielleicht von hinten. Oder: untersuche ich ein Objekt X und stelle Eigenschaft Y fest, so frage ich: Wie muß X aussehen, damit Eigenschaft Y erfüllt ist?
3. Ich übernehme von Zagier das Invarianzprinzip in bezug auf die Parität (gerade – ungerade).

Im folgenden werde ich mich in Zagiers Lage hineinversetzen, d. h. vom Ziel ausgehend überlegen, welchen Weg ich zu wählen habe. Natürlich wußte er, daß Primzahlen der Form $p = 4k+1$ im wesentlichen auf genau eine Weise in zwei Quadratzahlen zerlegt werden können. Die Gleichung $x^2 + a^2 = p$ hat aber die beiden Lösungen (x, a) und (a, x); da nun x oder a gerade sein muß, betrachtet man o. B. d. A. mit $a = 2y$ die Gleichung $x^2 + 4y^2 = p$, die nur noch genau eine Lösung hat. Es ist aber nicht ohne weiteres möglich, etwas über die Lösung auszusagen, da sie, abhängig von der Primzahl p, sehr unregelmäßig ist.

Manchmal ist es sinnvoll, ein vorgegebenes Problem als Spezialfall eines allgemeineren anzusehen. Aussagen über den allgemeinen Fall gelten erst recht für den Spezialfall. Hier bietet es sich an, die Gleichung etwas zu modifizieren. Verallgemeinerungen führen oft eine zusätzliche Variable ein. Wenn man sich an das Invarianzprinzip bezüglich der Parität erinnert, wäre es schön, wenn die neue Gleichung eine ungerade Anzahl an Lösungen hätte, vorausgesetzt, daß die Behauptung, es existiere genau eine Lösung, stimmt!

Modifiziert man die Gleichung $x^2 + 4y^2 = p$ z. B. zu $x^2 + 4y^2 + z = p$ kann man dies nicht auf einen Blick gewährleisten. Bei $x^2 + 4yz = p$ ist das aber möglich (Einfachheitsprinzip)! Denn Lösungen mit $y \neq z$ erhält man paarweise durch Vertauschen von y und z, und es gibt (setzt man die Behauptung voraus) nur eine Lösung mit $y = z$. Die nähere Untersuchung der Gleichung $x^2 + 4yz = p$ erscheint also gerechtfertigt. Wenn man nachweisen kann, daß die Anzahl der Lösungen ungerade ist, ist man am Ziel. Da wir nicht voraussetzen, sondern nachweisen wollen, gehen wir – nach dem Spiegelprinzip – andersherum vor. Eine Analyse liefert, daß die Vertauschung von y und z die Involution

$$\begin{pmatrix}x\\y\\z\end{pmatrix}\rightarrow\begin{pmatrix}x\\z\\y\end{pmatrix}$$

mit dem unbekannten Fixpunkt

$$\begin{pmatrix}x\\y\\y\end{pmatrix}\text{ ist.}$$

Gehen wir andersherum vor, dann suche ich zu einem bekannten (einfachen) Fixpunkt eine Abbildung, mit der ich die Parität der Lösungsmenge untersuchen kann. Da man an den Fixpunkten einer Involution die Parität der Lösungsmenge direkt ablesen kann, suche ich eine Involution (Einfachheitsprinzip). Aus diesem Prinzip folgt auch, daß die Abbildung linear sein sollte, da man sie bequem als Matrix schreiben kann. Einfachheitshalber sollten in der Matrix nur ganze Zahlen stehen, die konstant, also unabhängig von p, sind. Als Fixpunkt gebe ich die einfachste Lösung von $x^2 + 4yz = p$ vor.

Dies ist $\begin{pmatrix}1\\1\\k\end{pmatrix}$.

Also suche ich

- eine lineare Abbildung
- eine Involution
- mit genau einem Fixpunkt $\begin{pmatrix}1\\1\\k\end{pmatrix}$
- mit ganzen Zahlen in der Matrix; Matrix unabhängig von p
- Lösung von $x^2 + 4yz = p$ soll auf Lösung derselben Gleichung abgebildet werden.

Natürlich sind obige Annahmen keine notwendigen Bedingungen. Aber ich hoffte, daß die einfachste Abbildung, die mir die Parität der Lösungsmenge liefert, so aussieht. Nachdem das Einfachheitsprinzip ausgereizt war, folgte nach dem Spiegelprinzip etwas Bedauerliches:

Zu der einfachen Abbildung

$$\beta\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}x\\z\\y\end{pmatrix}$$

mit dem komplizierten Fixpunkt

$$\begin{pmatrix}x\\y\\y\end{pmatrix}$$

gehört sicher eine komplizierte Abbildung α, (obwohl ich stark vereinfachende Annahmen über α gemacht habe), da der Fixpunkt einfach ist.

3. Bestimmung der Abbildung

Von nun an leite ich notwendige Bedingungen (unter obigen Voraussetzungen) her.

Die Abbildung α werde durch die Matrix

$$B=\begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix}$$

dargestellt. Also gilt

$$B\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}ax+by+cz\\dx+ey+fz\\gx+hy+iz\end{pmatrix}=\begin{pmatrix}x'\\y'\\z'\end{pmatrix}.$$

Da $x^2 + 4yz = (x')^2 + 4(y')(z')$ gelten soll, folgt:

$$(ax + by + cz)^2 + 4\,(dx + ey + fz)(gx + hy + iz) = x^2 + 4yz.$$

Koeffizientenvergleich ergibt:

für x^2:	$a^2 + 4\,dg = 1$
für xy:	$2ab + 4\,(dh + eg) = 0$
für y^2:	$b^2 + 4\,eh = 0$
für xz:	$2ac + 4\,(di + fg) = 0$
für z^2:	$c^2 + 4\,fi = 0$
für yz:	$2bc + 4\,(ei + fh) = 4.$

Weiterhin soll $B^2 = E$ (Einheitsmatrix) gelten, da wir eine Involution suchen. Durch Matrizenmultiplikation folgt:

$$\begin{aligned} a^2 + bd + cg &= 1\\ da + ed + fg &= 0\\ ga + hd + ig &= 0\\ ab + be + ch &= 0\\ db + e^2 + fh &= 1\\ gb + he + ih &= 0\\ ac + bf + ci &= 0\\ dc + ef + fi &= 0\\ gc + hf + i^2 &= 1. \end{aligned}$$

Jetzt nehmen wir die Bedingung hinzu, daß $\begin{pmatrix}1\\1\\k\end{pmatrix}$ Fixpunkt ist:

$$\begin{aligned} a\cdot 1 + b\cdot 1 + c\cdot k &= 1\\ d\cdot 1 + e\cdot 1 + f\cdot k &= 1\\ g\cdot 1 + h\cdot 1 + i\cdot k &= k \end{aligned}$$

Dies soll für alle Primzahlen $p = 4k+1$, also für verschiedene k-Werte gelten. Da nun die a, b, c, ... i konstant sind, erhält man: $c = 0$, $f = 0$, $i = 1$.

Hiermit folgt aus $2ac + 4\,(di + fg) = 0$, daß $d = 0$.

Aus $d \cdot 1 + e \cdot 1 + f \cdot k = 1$ folgt dann $e = 1$.

Wegen $a^2 + 4dg = 1$ muß $a = 1$ oder $a = -1$ gelten.

Für $a = 1$ folgt aber aus $a \cdot 1 + b \cdot 1 + c \cdot k = 1$ $b = 0$, aus $gb + he + ih = 0$ erhält man $h \cdot (e + i) = 0$, also $h = 0$ und daraus $g = 0$.

Aus $a = 1$ folgt also die Einheitsmatrix, die aber sicher mehr als einen Fixpunkt hat.

Also ist $a = -1$, daher $b = 2$. Wegen $b^2 + 4eh = 0$ gilt $h = -1$ und daher $g = 1$.

Es gilt also: $B = \begin{pmatrix}-1 & 2 & 0\\ 0 & 1 & 0\\ 1 & -1 & 1\end{pmatrix}$.

Da nun auch $x', y', z' \in \mathbb{N}$ sein soll, muß $-x + 2y > 0$ und $x - y + z > 0$ sein.

Um die Abbildungsvorschrift auch für die anderen Fälle zu erhalten, bemerkt man zunächst, daß durch obige Grenzen drei disjunkte Mengen entstanden sind (wie bei der Beweisskizze). Natürlich will man jetzt auch die Menge A (mit $x < y - z$) und die Menge C (mit $x > 2y$) jeweils auf sich selbst abbilden. Dieser Versuch scheitert, denn für manche Primzahlen liegen in A und C je eine gerade, für andere jedoch je eine ungerade Anzahl von Lösungen. Im letzteren Falle würden bei einer Involution der Mengen A und C weitere Fixpunkte entstehen. Wenn man aber die Elemente von A und C gezählt hat, bemerkt man, daß beide Mengen gleich viele Elemente haben. Daher wird man versuchen, A auf C und C auf A abzubilden.

Gesucht werden also zwei Matrizen A und C mit $AC = E = CA$. Die Bestimmung dieser Matrizen gelang mir, indem ich für sehr kleine Primzahlen ($p = 13$ und $p = 17$), bei denen in der Menge A bzw. C nur je ein Element liegt, wo also die Zuordnung eindeutig ist, die zugehörigen Gleichungen aufstellte. Für $p = 29$ war die Abbildung nach einer Vorüberlegung eindeutig. Dadurch ergaben sich genügend Gleichungen zur eindeutigen Bestimmung der Matrizen A und C.

Eine andere Herleitung der Matrizen A und C ergibt sich, wenn man mit $X = \begin{pmatrix}-1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}$ $A = BX$ und $C = XB$ betrachtet:

$$A = \begin{pmatrix}1 & 0 & 2\\ 0 & 0 & 1\\ -1 & 1 & -1\end{pmatrix} \text{ und } C = \begin{pmatrix}1 & -2 & 0\\ 1 & -1 & 1\\ 0 & 1 & 0\end{pmatrix}$$

Allein aus der Überlegung, es könne eine möglichst einfache Abbildung mit den gewünschten Eigenschaften existieren, haben wir also genau Zagiers Abbildung erhalten, ohne vorher etwas von der Dreigliederung der Abbildung zu wissen. (Anm.: Die gesamte Abbildung ist also nicht mehr linear).

In gewissem Sinne ist Zagiers Abbildung also die einfachste mit diesen Eigenschaften, obwohl sie anfangs so kompliziert aussah.

Bei diesem konstruktiven Vorgehen wäre eigentlich noch zu prüfen, ob die Abbildung alle geforderten Eigenschaften hat, ob z. B. Lösungen aus A tatsächlich auf Lösungen aus C abgebildet werden, doch das ist bereits in der Beweisskizze geschehen.

4. Algorithmus zur Ermittlung des Fixpunktes

Nun beschäftige ich mich noch etwas mehr mit den Abbildungen α und β. Wendet man zweimal an ($\alpha \cdot \alpha$ = $\beta \cdot \beta$ = id), so ergibt sich nichts Neues. Wechselt man jedoch α und β ab, so ergibt sich etwas Überraschendes. Zunächst ein Beispiel für $p = 41$.

Ich starte mit $\begin{pmatrix}1\\1\\10\end{pmatrix}$, dem Fixpunkt von α.

$$\begin{pmatrix}1\\1\\10\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}1\\10\\1\end{pmatrix} \xrightarrow{\alpha} \begin{pmatrix}3\\1\\8\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}3\\8\\1\end{pmatrix}$$

$$\xrightarrow{\alpha} \begin{pmatrix}5\\1\\4\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}5\\4\\1\end{pmatrix} \xrightarrow{\alpha} \begin{pmatrix}3\\4\\2\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}3\\2\\4\end{pmatrix}$$

$$\xrightarrow{\alpha} \begin{pmatrix}1\\2\\5\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}1\\5\\2\end{pmatrix} \xrightarrow{\alpha} \begin{pmatrix}5\\2\\2\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}5\\2\\2\end{pmatrix}$$

Fixpunkt von β

$$\xrightarrow{\alpha} \begin{pmatrix}1\\5\\2\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}1\\2\\5\end{pmatrix} \xrightarrow{\alpha} \begin{pmatrix}3\\2\\4\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}3\\4\\2\end{pmatrix}$$

$$\xrightarrow{\alpha} \begin{pmatrix}5\\4\\1\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}5\\1\\4\end{pmatrix} \xrightarrow{\alpha} \begin{pmatrix}3\\8\\1\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}3\\1\\8\end{pmatrix}$$

$$\xrightarrow{\alpha} \begin{pmatrix}1\\10\\1\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}1\\1\\10\end{pmatrix}$$

Wir begannen mit dem Fixpunkt von α und haben die gesamte Lösungsmenge von $x^2 + 4yz = 41$ erzeugt, insbesondere haben wir den Fixpunkt von β erhalten. Wenn ich letzteres allgemein beweise, ergänze ich Zagiers Existenzbeweis zu einem konstruktiven Beweis. Zagier schrieb in einer Nachbemerkung: „Note that the proof is not constructive: it does not give a method to actually find the representation of p as a sum of two squares".

Beweis: Wir beginnen mit $\begin{pmatrix}1\\1\\k\end{pmatrix}$, dem Fixpunkt von α; nach einigen Iterationen werden wir wieder zu diesem Fixpunkt kommen. Da nämlich die Lösungsmenge von $x^2 + 4yz = p$ endlich ist, entsteht bei der Iteration eine Periode. Eine Vorperiode kann es nicht geben, da bei einer Involution ein eindeutig bestimmtes Inverses existiert (**Abb. 1**).

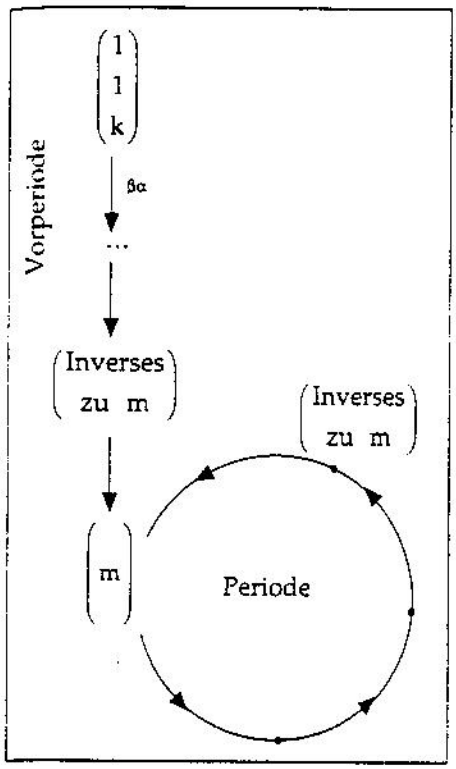


Abb. 1: Bei einer Vorperiode hätte m zwei Inverse!

Mit welcher Abbildung aber kommen wir wieder zu $\begin{pmatrix}1\\1\\k\end{pmatrix}$?

Da $\begin{pmatrix}1\\1\\k\end{pmatrix}$ ja Fixpunkt von α ist, kommen wir mit β wieder zu $\begin{pmatrix}1\\1\\k\end{pmatrix}$.

Dann aber ist die Anzahl der Lösungen in einer Periode gerade, und die Periode ist spiegelsymmetrisch zur Mitte. Dort muß also ein Fixpunkt liegen; es kann nur ein Fixpunkt von β sein, da α genau einen Fixpunkt hat.

$$\begin{pmatrix}1\\1\\k\end{pmatrix} \xrightarrow{\beta} \begin{pmatrix}1\\k\\1\end{pmatrix} \xrightarrow{\alpha} \dots \xrightarrow{\alpha} \begin{pmatrix}x\\y\\y\end{pmatrix}$$

$$\text{spiegelsymmetrisch} \quad \downarrow \beta$$

$$\begin{pmatrix}1\\1\\k\end{pmatrix} \xleftarrow{\beta} \begin{pmatrix}1\\k\\1\end{pmatrix} \xleftarrow{\alpha} \dots \xleftarrow{\alpha} \begin{pmatrix}x\\y\\y\end{pmatrix}$$

Dieser Algorithmus ist für die Praxis ungeeignet, zumindest für kleine Primzahlen erzeugt er häufig die gesamte Lösungsmenge der Gleichung $x^2 + 4yz = p$. Er ist langsamer als eine systematische Suche nach der Zerlegung in zwei Quadrate.

Anregungen für weitere Untersuchungen:
- Eine Beschleunigung des obigen Algorithmus ist möglich, indem man die über weite Strecken offensichtlichen Schritte überspringt. Der Algorithmus ist dann äquivalent zur Reduzierung indefiniter, binärer, quadratischer Formen (siehe [5], Art. 265 und [6], Kapitel 3).
- Eindeutigkeit der Zerlegung in zwei Quadrate mittels des Algorithmus. Es reicht zu zeigen, daß es keinen Zyklus mit zwei Fixpunkten von β geben kann. Mir ist das bisher nicht gelungen.
- Geometrische Interpretation der Abbildung auf einem einschaligen Hyperboloid.
- Es gelten folgende Gleichungen für die Matrizen:
  $A^3 = C^3 = -E$, $A^6 = C^6 = B^2 = E$,
  $AB = BC$ und $BA = CB$.
  Die Matrizen A und B erzeugen eine zur Diedergruppe D_6 isomorphe Gruppe.

Zum Abschluß sei gesagt, daß Mitteilungen und Anmerkungen über weiterführende Untersuchungen oder Berichte von Lehrern, die das Thema im Unterricht behandelt haben, mir willkommen wären.

5. Dank und Literaturhinweise

Den Herren Prof. Dr. Artmann, Dr. Heath-Brown, Dipl. Math. Klein und Dr. Spalt danke ich für verschiedene Anregungen.

Zagiers Beweis findet man in
[1] American Mathematical Monthly, Februar 1990.
Einen schönen, allgemein verständlichen Beweis findet man in
[2] Spektrum der Wissenschaft, Dezember 1990.
Weitere Beweise oder verwandte Sätze findet man in:
[3] Aigner, A.: Zahlentheorie, Berlin 1975
[4] Hardy, G. H. und Wright, E. M.: An Introduction to the Theory of Numbers, Oxford 1960.
Über binäre, quadratische Formen berichten:
[5] Gauß, C. F.: Disquisitiones Arithmetical, 1801.
[6] Buell, D. A.: Binary Quadratic Forms, New York 1989.

Rezensionen

U. Drews/ E. Fuhrmann/ W. Reich/ H. Weck: Ratschläge für Lehrer, 256 S., 33 Abb., Kart., Aulis-Verlag, Köln 1987, DM 22,00.
ISBN 3-7614-0996-6
Die hier zusammengestellten Hinweise und Tips stammen aus einer Taschenbuchserie, die die Akademie der Pädagogischen Wissenschaften der DDR herausgab, um den Lehrern bei der Bewältigung des oft mühsamen Schulalltags zu helfen. Bei allen prinzipiellen Unterschieden sehen sich die Lehrer in beiden Teilen Deutschlands mit ähnlichen pädagogischen Problemen konfrontiert; so wurde der Text überarbeitet bzw. terminologisch unserer Situation angepaßt. Mit jeder Seite spürt der Leser die große Erfahrung und die Praxisnähe der Autoren, die sich mit drei Hauptthemen beschäftigen: Gestaltung einer guten Unterrichtsstunde, Erreichen von Disziplin im Unterricht, Bewertung und Zensierung. Durch die geschickte Art der Darstellung in Wort und Bild findet neben dem Berufsanfänger auch der „alte Hase" noch viele neue Tips und Anregungen für die eigene Situation in diesem preiswürdigen Buch.

H. Drewelow/ D. Hess/ E. Rausch u. a.: Hausaufgaben, Sprache, Zensuren, 256 S., 32 Abb., Kart., Aulis Verlag, Köln 1989, DM 22,00.
ISBN 3-7614-0118-1
Mit diesem Folgeband von „Ratschläge für Lehrer" werden die Hilfen für den Unterricht um drei neue wichtige Problemkreise ergänzt, die im praktischen Schulalltag täglich berührt werden. Zunächst wird geschickt auf die richtige „Dosierung" der Hausaufgaben eingegangen; anschließend werden Tips aus der großen Erfahrung der Autoren für die „goldene Mitte" bei der Verwendung von Fach- und Umgangssprache im Unterricht gegeben. Im letzten Teil wird die Problematik der Zensurengebung im Spannungsfeld „unterrichtliches Verhalten – fachliche Leistung" durchleuchtet. Wie schon der erste Band zeichnet sich auch dieser durch die gelungene Anordnung von Text und Bildern und die große Praxisnähe aus.

Karl-Hermann Waid