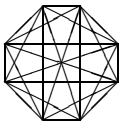
**TU CLAUSTHAL**
**INSTITUT FÜR MATHEMATIK**
**Prof. Dr. W. Klotz**



**Lineare Algebra I**
WS 1999/2000
Übungsblatt 2
Übung vom 4.11.1999

Hauptaufgabe dieser Übung ist es, den folgenden Beweis zu verstehen. Es ist ein Beweis, der mit verblüffend einfachen Methoden einen Satz beweist, der wegen seiner Eleganz als einer der schönsten Sätze der Mathematik gilt.

# A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x, y, z) \to \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \to (x, z, y)$ also has a fixed point. □

Im Februar 1990 erschien dieser Beweis in der Zeitschrift American Mathematical Monthly. Der Beweis stammt von D. Zagier, der eine Idee von D.R. Heath-Brown benutzte, der wiederum eine Idee von Liouville verwendete. Der Satz selber geht auf Girard (1625) und wenig später Fermat zurück, (der vermutlich hierfür einen Beweis kannte). Der erste überlieferte Beweis stammt von Euler (1749).

Wir werden uns dies nun schrittweise erarbeiten. Die Hauptarbeit liegt bei den Schritten 8-10. Lassen Sie die am Anfang ruhig beiseite, denn danach wird es richtig interessant!

**Satz: Jede Primzahl $p$ von der Form $p = 4k + 1, k \in \mathbb{N}$ ist Summe von zwei Quadratzahlen:**

$$\mathbf{p = a^2 + b^2.}$$

## EIN PAAR VORBEREITUNGEN DES BEWEISES

Schritt 1: Welche Zahlen $n \leq 100$ können als Summe von zwei Quadratzahlen geschrieben werden? Stimmt Ihre Beobachtung mit dem Satz überein?

Schritt 2: Wir definieren, für $p \in \mathbb{N}$, die Menge $S_p = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$. Machen Sie sich die Definition klar. Was bedeutet z.B. $(x, y, z) \in \mathbb{N}^3$ ?

Schritt 3: Berechnen Sie die Mengen $S_p$ für $p = 40, 41, 42, 43$.

Schritt 4: Beweisen Sie, daß $S_p$ für jedes $p \in \mathbb{N}$ eine endliche Menge ist.

Schritt 5: Wir zerlegen die Menge $S_p$ in drei Teilmengen:

$$\begin{aligned} A_p &= \{(x, y, z) \in S_p \mid x < y - z\}, \\ B_p &= \{(x, y, z) \in S_p \mid y - z < x < 2y\}, \\ C_p &= \{(x, y, z) \in S_p \mid x > 2y\}. \end{aligned}$$

Schritt 6: Bestimmen Sie die Mengen $A_p, B_p$ und $C_p$ für $p = 40, 41, 42, 43$. Gibt es Elemente in den Schnittmengen $A_p \cap B_p, A_p \cap C_p, B_p \cap C_p$ ? Gilt jeweils $S_p = A_p \cup B_p \cup C_p$?

Schritt 7: Beweisen Sie: Für eine Primzahl $p$ liegt jedes Element aus $S_p$ in genau einer der drei Mengen $A_p, B_p, C_p$.

Im folgenden sei $p$ eine feste Primzahl. Dann können wir z.B. $A$ statt $A_p$ schreiben.

Wenn Ihnen die folgenden Rechnungen zunächst zu abstrakt sind, dann rechnen Sie zunächst im konkreten Fall mit $p = 41$.

Schritt 8: Jetzt definieren wir eine Abbildung $\alpha$, die Elemente der Menge $S$ auf andere Elemente der Menge $S$ abbildet. Die Abbildung $\alpha$ besteht aus drei Teilabbildungen, für jede der drei Teilmengen $A, B, C$ eine.

$$\alpha : S \to S \text{ mit } \quad \alpha(x,y,z) = \begin{cases} (x+2z, z, y-x-z) & \text{falls } x < y-z \\ (2y-x, y, x-y+z) & \text{falls } y-z < x < 2y \\ (x-2y, x-y+z, y) & \text{falls } x > 2y \end{cases}$$

Zunächst einmal ist nur klar, daß $\alpha(x,y,z) \in \mathbb{N}^3$ gilt. Warum liegt für $(x,y,z) \in S$ auch $\alpha(x,y,z) \in S$?

Schritt 9: Nehmen Sie ein Element $(x,y,z)$ aus der Teilmenge $A$. In welcher Teilmenge liegt das Element $\alpha(x,y,z)$? Gehen Sie für $(x,y,z) \in B$ und $(x,y,z) \in C$ analog vor.

Schritt 10: Berechnen Sie für ein Element $(x,y,z) \in A$ das Element $\alpha(\alpha(x,y,z))$. Gehen Sie für $(x,y,z) \in B$ und $(x,y,z) \in C$ analog vor. Beweisen Sie so, daß gilt $\alpha \circ \alpha = id_S$.

Eine Abbildung mit dieser letzteren Eigenschaft nennt man eine Involution.

DER BEWEIS

Die Hauptschwierigkeit ist bereits überwunden. Jetzt wollen wir den Lohn unserer Arbeit einholen! Sei $p$ also eine Primzahl der Form $4k+1$.

Schritt 11: Ein Fixpunkt der Abbildung $\alpha$ ist eine Element $(x,y,z) \in S$ mit $\alpha(x,y,z) = (x,y,z)$.

Zeigen Sie: $\alpha$ hat genau einen Fixpunkt. Berechnen Sie ihn!

Schritt 12: Sei $|X|$ die Anzahl der Elemente der Menge $X$. Können Sie jetzt mit Begründung angeben, ob $|S| = |A|+|B|+|C|$ gerade oder ungerade ist?

Schritt 13: Wir haben jetzt eine komplizierte Abbildung $\alpha$ mit genau einem Fixpunkt. Wir nehmen jetzt eine ganz einfache Abbildung $\beta : S \to S$ mit $\beta(x,y,z) = (x,z,y)$.

Zeigen Sie analog zu oben, aber es ist ja diesmal viel leichter, daß für $(x,y,z) \in S$ auch $\beta(x,y,z) \in S$ und daß $\beta \circ \beta = id_S$ gilt.

Schritt 14: Warum hat $\beta$ mindestens einen Fixpunkt? Kann $\beta$ mehr als einen Fixpunkt haben?

Schritt 15: Wie liefert uns der Fixpunkt von $\beta$ unmittelbar, daß $p = 4k+1$ Summe von zwei Quadratzahlen ist?

Versuchen Sie, in eigenen Worten die Beweisidee zusammenzufassen und jemand anderem zu erklären!

Hier noch einige (kürzere!) Aufgaben zur Gruppentheorie.

1. Es sei $U$ eine Untergruppe der Gruppe $(G, \cdot)$. Man zeige, daß durch

$$a \sim_r b \Leftrightarrow ab^{-1} \in U, \; a \sim_1 b \Leftrightarrow a^{-1}b \in U$$

Äquivalenzrelationen $\sim_r$ und $\sim_1$ auf $G$ definiert werden. Die Äquivalenzklassen haben die Gestalt:

$$Ub = \{ub | u \in U\} \text{ bzw. } aU = \{au | u \in U\}.$$

Sie heißen Rechts- bzw. Linksnebenklassen von $U$ in $G$. $U$ hat gleichviele Rechts- wie Linksnebenklassen. Diese gemeinsame Anzahl heißt der Index $[G:U]$ von $U$ in $G$. Für eine endliche Gruppe $G$ zeige man

$$|Ub| = |aU| = |U|$$

und folgere daraus durch Abzählen der Elemente von $G$ die Gleichung von Lagrange:

$$|G| = |U| \cdot [G:U].$$

2. Es sei $(G, \cdot)$ eine Gruppe mit dem Einselement $e$. Man zeige:

a) $aG = \{ag | g \in G\} = G$ für alle $a \in G$.
b) Ist $G$ endlich, dann gilt der 'Kleine Fermatsche Satz' der Gruppentheorie:

$$a^{|G|} = e \text{ für alle } a \in G.$$

3. Man zeige, daß jede Untergruppe einer zyklischen Gruppe zyklisch ist. Man bestimme alle Untergruppen der Gruppe $(\mathbb{Z}, +)$.