Zwei-Quadrate-Satz von Fermat

Ahmed Sato

January 26, 2020

in dieser Lektion werden wir sehen, welche Primzahl als Summe von zwei Quadraten dargestellt werden können und welche nicht.

Introduction: Die Primzahlen lassen sich in 3 verschiedene Klassen unterteilen:

$P = 2 = 1^1 + 1^1$
$P = 4m + 1$
$P = 4m + 3$

Lemma 1: Kein Zahl $n = 4m + 3$ ist eine Summe von zwei Quadraten.

Beweis: Das Quadrat einer geraden Zahl ist $(2k)^2 = 4k^2 = 0(modp)$. Das Quadert einer ungeraden Zahl ist $(2k + 1)^2 = 4(k^2 + k) + 1 = 1(mod4)$. damit ist die Summe von zwei Quadraten $0, 1$ oder $2(mod4)$.

Lemm 2: Jede Primzahl der Form $P = 4m + 1$ ist eine Summe von 2 Quadraten, sie kann also als $P = x^2 + y^2$ dargestellt werden, mit $x, y \in N$.

Der erste Beweis stammt von Axel Thue.
Wir betrachten die Paare(x', y') von ganzen Zahlen mit $x', y' \in \{0, 1, ..., \lfloor\sqrt{p}\rfloor\}$.
Es gibt genau $(\lfloor\sqrt{p}\rfloor + 1)^2$ solcher Paare, $\lfloor\sqrt{x}\rfloor + 1 > x$ für $x = \sqrt{p} \quad \Rightarrow x^2 > p$.

Also können für ein festes $s \in Z_p$ die Werte $x's y'$, die man aus den Paaren(x', y') erzeugt, nicht alle modulo p verscheiden sein. Also gibt es für jedes s zwei verschiedene Paar:

$(x', y'), (x'', y'') \in \{0, 1, ..., \sqrt{p}\}^2$ mit $x' - sy' \equiv x'' \equiv sy''\ (modp)$.
Nun bilden wir die Differenzen: $x' - x'' \equiv s(y' - y'')(modp)$ und definieren $x := |x' - x''|; y := |y' - y''|$.
Dann erhalten wir:

$$x = \pm sy(modp) \quad ; (x, y) \in \{0, 1, ..., \lfloor\sqrt{p}\rfloor\}^2$$

x und y können nicht beide Null sein, weil die Paare $(x\prime; y\prime)$ und $(x''; y'')$ verschieden sind.

Sei nun s eine Lösung von $x^2 \equiv s^2y^2 \equiv -y^2\ (modp)\ (x; y) \in Z$ mit $0 < x^2 + y^2 < 2p$ und $x^2 + y^2 \equiv 0\ (modp)$. Die Primzahl p ist aber die einzige Zahl zwischen 0 und $2p$, die durch p teilbar ist. Also gilt $x^2 + y^2 = p$.

Der zweite Beweis von Heath-Brown basiert auf drei Involutionen.
Beweis(2): wir untersuchen die Menge:

$$S := \{(x, y, z) \in Z^3 : 4xy + z^2 = p, \quad x > 0, y > 0\}$$

Diese Menge ist endlich: aus $x \geq 1$ und $y \geq 1$ folgt nämlich $y \leq \frac{p}{4}$ und $x \leq \frac{p}{4}$.
Damit gibt es aber nur endlich viele mögliche Werte für x und y , und für gegebenes x und y gibt es höchstens zwei Werte für z .

. 1. Die erste lineare Involution ist:

$$f : S \to S, \quad (x, y, z) \to (y, x, -z)$$

also vertausche x und y und negiere z. Dies bildet ganz offensichtlich S auf sich selbst ab, und es ist eine Involution: Zweimal angewendet, ergibt es die Identität.
Dieses f hat offenbar keine Fixpunkte, weil aus $z = 0$ sofort $p = 4xy$ folgen würde, was nicht sein kann.

Schlielich bildet f die Lösungen in: $T := \{(x, y, z) \in S \quad : z > 0\}$ auf die Lösungen in $S \setminus T$ ab, die $z < 0$ erfüllen.
Also vertauscht f die Vorzeichen von $x - y$ und von z , und bildet somit auch die Lösungen in:

$$U := \{(x, y, z) \in S \quad : (x - y) + z > 0\}$$

auf die Lösungen in $S \setminus U$ ab.
Dafür müssen wir nur überprüfen, dass es keine Lösungen gibt, mit $(x - y) + z = 0$.
Aber die gibt es nicht, weil daraus sofort $p = 4xy + z^2 = 4xy + (x - y)^2 = (x + y)^2$ folgen würde. Was liefert uns nun die Analyse von f ? Die hauptschliche Beobachtung ist, dass f die Mengen T und U mit ihren Komplementen $S \setminus T$ bzw. $S \setminus U$ in Bijektion setzt; deshalb haben T und U beide die halbe Kardinalitaet von S also haben T und U dieselbe Kardinalität.

2. Die zweite Involution, die wir betrachten wollen, lebt auf der Menge U :

$$g : U \to U, \quad (x, y, z) \to (x - y + z, y, 2y - z)$$

Zunächst überprüfen wir, dass dies überhaupt eine wohldefinierte Abbildung ist:
Wenn $(x, y, z) \in U$ ist, dann gilt $x - y + z > 0, y > 0$ und $4(xy + z)y + (2y - z)^2 = 4xy + z^2 = p$, also $g(x, y, z) \in S$.
Mit $(x - y + z) - y + (2y - z) = x > 0$ liefert dies $g(x, y, z) \in U$.

Weiterhin ist g eine Involution: $g(x, y, z) = (xy + z, y, 2yz)$
wird durch g auf $((xy + z)y + (2yz), y, 2y(2yz)) = (x, y, z)$ abgebildet.

Und schließlich hat g genau einen Fixpunkt: $(x, y, z) = g(x, y, z) = (x - y + z, y, 2y - z)$
gilt genau dann, wenn $y = z$ ist.
Dann haben wir aber: $p = 4xy + y^2 = (4x + y)y$,was nur für $y = 1 = z$ und $x = \frac{p-1}{4}$ gelten kann.
Und wenn g eine Involution auf U ist, die genau einen Fixpunkt hat, dann hat U ungerade Kardinalität.

3. Die dritte Involution lebt auf der Menge T, und sie vertauscht einfach x und y:

$$h : T \to T, \quad (x, y, z) \to (y, x, z)$$

Diese Abbildung ist nun ganz offensichtlich wohldefiniert und sie ist eine Involution.
Wir kombinieren jetzt das Wissen, das wir aus den beiden anderen Involutionen abgeleitet haben:
T hat dieselbe Kardinalitt wie U , und die ist ungerade.
Aber da h somit eine Involution Auf einer endlichen Menge mit ungerader Kardinalität ist, hat jede Involution mindestens einen Fixpunkt.
Es gibt einen Punkt $(x, y, z) \in T$, mit $x = y$, also eine Lösung von $p = 4x^2 + z^2 = (2x)^2 + z^2$

.

Literatur:
1. A. AIGNER: Zahlentheorie, de Gruyter, Berlin 1975.
2. F. W. CLARKE, W. N. EVERITT, L. L. LITTLEJOHN , S. J. R. VORSTER: H. J. S. Smith and the Fermat Two Squares Theorem, Amer. Math. Monthly 106 (1999), 652-665.

3. D. R. HEATH-BROWN: Fermats two squares theorem, Invariant (1984), 2-5. LATEX version, with appendix on history, January 2008, at eprints.maths.ox.ac. uk/677/1/invariant.pdf.
4. H. RIESEL: Prime Numbers and Computer Methods for Factorization, Second edition, Progress in Mathematics 126, Birkhuser, Boston MA 1994.
5. M. RUBINSTEIN , P. SARNAK: Chebyshevs bias, Experimental Mathematics 3 (1994), 173-197.
6. A. THUE: Et par antydninger til en taltheoretisk metode, Kra. Vidensk. Selsk. Forh. 7 (1902), 57-75.
7. S. WAGON: Editors corner: The Euclidean algorithm strikes again, Amer. Math. Monthly 97 (1990), 125-129. [8] D. ZAGIER: A one-sentence proof that every prime $p \equiv 1(mod 4)$ is a sum of two squares, Amer. Math. Monthly 97 (1990), 144.