Der Zwei-Quadrate-Satz von Fermat

Proseminar: Das BUCH der Beweise

Fridtjof Schulte Steinberg

Institut für Informatik
Humboldt-Universität zu Berlin

29.November 2012

Allgemeines

Pierre de Fermat

- lebte Anfang des 17. Jahrhunderts.
- viele wichtige Beiträge zur Mathematik
  - kleiner Fermatscher Satz
  - großer Fermatscher Satz
  - **Zwei-Quadrate-Satz**
  - und viele mehr
- Resultate oft nur als Denksportaufgabe

Fragestellung

Welche Zahlen können als Summe von zwei Quadraten dargestellt werden?

Einige Beispiele:

$1 = 1^2 + 0^2$
$2 = 1^2 + 1^2$
$3 = ???$
$4 = 2^2 + 0^2$
$5 = 2^2 + 1^2$
$6 = ???$
$7 = ???$
$8 = 2^2 + 2^2$
$9 = 3^2 + 0^2$
$10 = 3^2 + 1^2$
$11 = ???$

Primkörper

Jede Primzahl p bildet mit der Addition und Multiplikation „modulo p“ einen endlichen Körper.

Eigenschaften

- Das additive Inverse$(-x)$ ist gegeben durch $p - x$. Falls $p > 2$ dann sind x und $-x$ sind verschiedene Elemente.
- Es gibt ein eindeutiges multiplikatives Inverses $x * \bar{x} \equiv 1(mod p)$.
- Die Quadrate $0^2, 1^2, 2^2, ...h^2$ definieren verschiedene Elemente von $\mathbb{Z}_p$, für $h = \lfloor p/2 \rfloor$.

Die Quadrate $0^2, 1^2, 2^2, \ldots h^2$ definieren verschiedene Elemente von $\mathbb{Z}_p$, für $h = \lfloor p/2 \rfloor$.

Beweis:

$x^2 \equiv y^2 \Leftrightarrow x^2 - y^2 \equiv (x+y)(x-y) \equiv 0$

Also entweder $x \equiv y$ oder $x \equiv -y$. □

Primzahlklassen

Alle Primzahlen lassen sich in 3 verschiedene Klassen unterteilen:

1. $p = 2$
2. $p = 4m + 1$
3. $p = 4m + 3$

Lemma1

Lemma

Für jede Primzahl p der Form $p = 4m + 1$ hat die Gleichung $s^2 \equiv -1 (mod p)$ zwei Lösungen, für $p = 2$ gibt es genau eine solche Lösung, während es für Primzahlen der Form $p = 4m + 3$ keine Lösung gibt.

Beweis zu Lemma1

Lemma

Für jede Primzahl p der Form $p = 4m + 1$ hat die Gleichung $s^2 \equiv -1 (mod p)$ zwei Lösungen, für $p = 2$ gibt es genau eine solche Lösung, während es für Primzahlen der Form $p = 4m + 3$ keine Lösung gibt.

Beweis

Für $p = 2$ ist $s = 1$.
Wir setzen jedes Element mit seinem additiven und multiplikativen Inversen in Relation. Die allgemeine Äquivalenzklasse sieht so aus: $\{x, -x, \bar{x}, -\bar{x}\}$.
Es sind auch kleinere Äquivalenzklassen möglich:

- $x \equiv -x$ für ungerade p unmöglich(Folgt aus den Eigenschaften des Primkörpers)
- $x \equiv \bar{x}$ äquivalent zu $x^2 \equiv 1$
  Zwei Lösungen: $x = 1$ und $x = p - 1$
- $x \equiv -\bar{x}$ äquivlaent zu $x^2 \equiv -1$
  Entweder keine oder zwei verschiedene Lösungen $x_0, p - x_0$.

Beweis Fortsetzung

Die Menge $\{1, 2, ..., p-1\}$ hat p-1 Elemente, die in 4-Tupel aufgeteilt werden, plus ein oder zwei 2-Tupel.
Für $p-1 = 4m+2$ folgt daraus, dass es nur ein Paar gibt $\{1, p-1\}$.
Daraus folgt dass $s^2 \equiv -1(modp)$ keine Lösung hat. Für $p-1 = 4m$ muss es aber ein zweites Paar geben, das enthält die Lösung $s^2 \equiv -1$. $\square$

Beispiele

Für $p = 11$ ist die Zerlegung:
$\{1, 10\}, \{2, 9, 6, 5\}, \{3, 8, 4, 7\}$

Für $p = 13$ ist sie:
$\{1, 12\}, \{2, 11, 7, 6\}, \{3, 10, 9, 4\}, \{5, 8\}$

Das Paar $\{5, 8\}$ entspricht den zwei Lösungen von $s^2 \equiv -1 (mod 13)$.

$x^2 + y^2 \equiv -1(mod p)$

Für alle Primzahlen gibt es eine Lösung der Gleichung $x^2 + y^2 \equiv -1(mod p)$.

Beweis.

Es gibt $\lfloor p/2 \rfloor + 1$ verschiedene Quadrate x^2 in $\mathbb{Z}_p$ (3.Punkt bei Primkörpern) und es gibt $\lfloor p/2 \rfloor + 1$ verschiedene Zahlen der Form $-(1 + y^2)$. Die Anzahl der beiden Mengen ist aber zu groß um disjunkt zu sein, weil es insgesamt nur p Elemente gibt, d.h. es muss x und y geben mit $x^2 \equiv -(1 + y^2)(mod p)$. □

Lemma 2

Lemma 2

Keine Zahl $n = 4m + 3$ ist eine Summe von zwei Quadraten.

Beweis.

Das Quadrat einer geraden Zahl ist $(2k)^2 = 4k^2 \equiv 0(mod 4)$. Das Quadrat einer ungeraden Zahl ist $(2k + 1)^2 = 4(k^2 + k) + 1 \equiv 1(mod 4)$. Damit ist die Summe von zwei Quadraten $0, 1$ oder $2(mod 4)$.

□

Das zeigt, dass die Primzahlen der Form $4m + 3$ „schlecht“ sind.

Proposition

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 $x, y \in \mathbb{N}$.

Beweis der Proposition

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 $x, y \in \mathbb{N}$.

Beweis:

- 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.
- $\lfloor x\rfloor + 1 > x$ für $x = \sqrt{p} \Rightarrow x^2 > p$
- Also können für ein festes $s \in \mathbb{Z}_p$ die Werte $x' - sy'$, die man aus den Paaren(x', y') erzeugt, nicht alle modulo p verscheiden sein. (Schubfachprinzip)

Beweis der Proposition Teil 2

- Also gibt es für jedes s zwei verschiedene Paare $(x'y'), (x'', y'') \in \{0, 1, ...\lfloor\sqrt{p}\rfloor\}^2$ mit $x' - sy' \equiv x'' - sy''(modp)$.

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

- x und y können nicht beide Null seien, weil die Paare (x', y') und (x'', y'') verschieden sind.

- Sei nun s eine Lösung von $x^2 \equiv s^2y^2 \equiv -y^2(modp)$ $(x, y) \in \mathbb{Z}$ 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 Zwei-Quadrate-Satz

Eine natürliche Zahl n kann genau dann als Summe von zwei Quadraten dargestellt werden, wenn jeder Primfaktor der Form $p = 4m + 3$ in der Primfaktorzerlegung von n mit geradem Exponenten auftritt.

.

Bezeichnung:
Eine Zahl n heißt darstellbar, wenn sie eine Summe von zwei Quadraten ist, das heißt $n = x^2 + y^2$ für ganzzahlige x, y.

Der Zwei-Quadrate-Satz: Beweis 1. Teil

n darstellbar $\Leftrightarrow$ jeder Primfaktor der Form $p = 4m + 3$ kommt in der Primfaktorzerlegung mit geradem Exponenten vor.

Beweis:

$\Rightarrow$

1. $1 = 1^2 + 0^2$ und $2 = 1^2 + 1^2$ sind darstellbar. Jede Primzahl der Form $p = 4m + 1$ ist darstellbar.

2. Das Produkt von zwei Zahlen $n_1 = x_1^2 + y_1^2$ und $n_2 = x_2^2 + y_2^2$ ist darstellbar.
   $n_1 * n_2 = (x1x2 + y1y2)^2 + (x_1y_2 - x_2y_1)^2$

3. Wenn n darstellbar ist, $n = x^2 + y^2$, dann ist auch nz^2 darstellbar.
   $nz^2 = (xz)^2 + (yz)^2$

Der Zwei-Quadrate-Satz: Beweis 2. Teil

n darstellbar $\Leftrightarrow$ jeder Primfaktor der Form $p = 4m + 3$ in der Primfaktorzerlegung mit geradem Exponenten vorkommt.

$\Leftarrow$

4. Wenn $p = 4m + 3$ eine Primzahl ist, die eine darstellbare Zahl n $n = x^2 + y^2$ teilt, dann teilt p sowohl x als auch y. Damit ist n auch durch p^2 teilbar.
   Wenn nämlich $x \not\equiv 0(modp)$ wäre, gäbe es ein $\bar{x}$ mit $x\bar{x} \equiv 1(modp)$.
   $x^2 + y^2 \equiv 0$ mit $\bar{x}^2$ multiplizieren $\Rightarrow 1 + y^2\bar{x}^2 = 1 + (\bar{x}y)^2 \equiv 0(modp)$.
   Was für $4m + 3$ nach Lemma 1 unmöglich ist.
   (Lemma 1: Es existiert keine Lösung der Gleichung $s^2 \equiv -1$ für Primzahlen der Form $4m + 3$.)
5. Wenn n darstellbar und durch $p = 4m + 3$ teilbar ist, dann ist n auch durch p^2 teilbar und n/p^2 ist ebenfalls darstellbar. Dies folgt aus 4. $\square$

Beispiele vom Anfang

Zahlen und ihre Primfaktoren:

$2 = 1^2 + 1^2$ (2)
$3 =$??? (3)
$4 = 2^2 + 0^2$ (2^2)
$5 = 2^2 + 1^2$ (5)
$6 =$??? $(2, 3)$
$7 =$??? (7)
$8 = 2^2 + 2^2$ (2^3)
$9 = 3^2 + 0^2$ (3^2)
$10 = 3^2 + 1^2$ $(2, 5)$
$11 =$??? (11)

Quellen:

Aigner, Martin; Ziegeler, Günter M.: Das BUCH der Beweise; Springer; Berlin 2002

http://upload.wikimedia.org/wikipedia/commons/f/f3/Pierre_de_Fermat.jpg(27.11.2012)