

Der Zwei-Quadrate-Satz von Fermat

Michael Adler

24.3.2008

Abstract. Das vorliegende Dokument ist die Ausarbeitung und Ergänzung meines Vortrages bei der TopMath-Frühlingschule auf Frauenchiemsee (30.3.2008 - 4.4.2008).

Es beschäftigt sich mit der Frage, welche natürlichen Zahlen n sich als Summe zweier Quadratzahlen schreiben lassen. Es wird sich zeigen, dass dies genau dann der Fall ist, wenn die Vielfachheit jeder Primzahl $p \equiv 3 \pmod{4}$ in der kanonischen Primfaktorzerlegung von n gerade ist. Der Schlüssel des Beweises ist Proposition 1, welche besagt, dass sich eine Primzahl $p \neq 2$ genau dann als Summe zweier Quadratzahlen schreiben lässt, wenn $p \equiv 1 \pmod{4}$. Für dieses Lemma werden 3 völlig unterschiedliche Beweise vorgestellt. Die ersten beiden Beweise sind sehr elementar und bestechen durch ihre Einfachheit, wohingegen der letzte Beweis mit (einfachen) Methoden der algebraischen Zahlentheorie geführt wird. Ferner wird die Eindeutigkeit dieser Darstellung auf zwei verschiedene Arten bewiesen (wieder elementar und mit Methoden der algebraischen Zahlentheorie)

Abschließend wird (ohne Beweis) eine Formel angegeben, die die Anzahl der Darstellungen einer natürlichen Zahl als Summe zweier Quadratzahlen zählt. Es wird bemerkt, dass sich die "wenigsten" natürlichen Zahlen als Summe zweier Quadratzahlen schreiben lassen; dies ist jedoch möglich, falls man die Anzahl der Quadrate auf 4 erhöht (der Vier-Quadrate-Satz von Lagrange).

Inhaltsverzeichnis

| | | |
|----------|--|-----------|
| 1 | Requisiten | 3 |
| 1.1 | -1 als quadratischer Rest modulo p | 3 |
| 1.2 | Der euklidische Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen | 4 |
| 2 | Primzahlen als Summe zweier Quadratzahlen | 4 |
| 2.1 | Existenz | 4 |
| 2.1.1 | Erster Beweis (nach Axel Thue) | 4 |
| 2.1.2 | Zweiter Beweis (nach Heath-Brown) | 5 |
| 2.1.3 | Dritter Beweis (Algebraische Zahlentheorie) | 7 |
| 2.2 | Eindeutigkeit | 7 |
| 2.2.1 | Erster Beweis (elementar) | 7 |
| 2.2.2 | Zweiter Beweis (algebraische Zahlentheorie) | 8 |
| 3 | Natürlichen Zahlen als Summe zweier Quadratzahlen | 8 |
| 3.1 | Der Zwei-Quadrate-Satz von Fermat | 8 |
| 4 | Ausblick | 9 |
| 4.1 | Die Anzahl der verschiedenen Darstellungen $n = x^2 + y^2$ | 9 |
| 4.2 | Die Menge aller Zahlen der Form $n = x^2 + y^2$ ist "klein" | 10 |
| 5 | Literaturverzeichnis | 11 |

Im Folgenden sei stets $\mathbb{N} = \{1, 2, 3, \dots\}$ gemeint.

1 Requisiten

1.1 -1 als quadratischer Rest modulo p

Lemma 1. Für eine Primzahl p ist die quadratische Kongruenz

$$X^2 \equiv -1 \pmod{p}$$

genau dann lösbar, wenn $p \not\equiv 3 \pmod{4}$. Für $p = 2$ gibt es genau eine Lösung (modulo p). Im Falle der Lösbarkeit nennt man -1 einen *quadratischen Rest* modulo p .

Beweis. Der Fall $p = 2$ ist trivial. Sei daher $p > 2$. Für jedes $x \in \mathbb{Z}/p\mathbb{Z}^\times = \{1, 2, \dots, p-1\}$ setze man $[x] := \{x, -x, 1/x, -1/x\}$. Das liefert eine Partition und somit eine Äquivalenzrelation auf der Menge $\{1, 2, \dots, p-1\}$, wenn man jeweils alle Vertreter der Restklassen im Bereich $\{1, 2, \dots, p-1\}$ wählt. Es sind die Fälle interessant, in denen $[x]$ weniger als 4 Elemente enthält:

- (1) Die Gleichung $x \equiv -x \pmod{p}$ ist nicht möglich, da p ungerade ist.
- (2) Die Gleichung $x \equiv 1/x \pmod{p}$ ist äquivalent zu $x^2 \equiv 1 \pmod{p}$, also $x \equiv \pm 1 \pmod{p}$ mit Äquivalenzklasse $\{1, p-1\}$.
- (3) Die Gleichung $x \equiv -1/x \pmod{p}$ ist äquivalent zu $x^2 \equiv -1 \pmod{p}$. Diese Gleichung hat entweder keine Lösung oder zwei Lösungen $\pm x_0$ mit Äquivalenzklasse $\{x_0, p-x_0\}$.

Folglich gibt es genau dann zwei 2-elementige Äquivalenzklassen, wenn $X^2 \equiv -1 \pmod{p}$ lösbar ist; ansonsten gibt es genau eine 2-elementige Äquivalenzklasse.

Die Existenz zweier 2-elementiger Äquivalenzklassen ist äquivalent zu $p-1 = 4m+2+2 \equiv 0 \pmod{4}$ und die Existenz genau einer 2-elementigen Äquivalenzklasse ist äquivalent zu $p-1 = 4m+2 \equiv 2 \pmod{4}$. \square

Bemerkung. Nach dem Satz von Wilson gilt $(p-1)! \equiv -1 \pmod{p}$, falls p prim ist (es gilt auch die Umkehrung dieser Aussage); man rechnet damit leicht nach, dass im Fall $p \equiv 1 \pmod{4}$ die beiden modulo p verschiedenen Lösungen gegeben sind durch $\pm \left(\frac{p-1}{2}\right)!$.

1.2 Der euklidische Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen

Die Menge $\mathbb{Z}[i] := \mathbb{Z} + i\mathbb{Z} = \{a + ib : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ ist als Bild des Ringhomomorphismus $\mathbb{Z}[X] \longrightarrow \mathbb{C}$, $f \mapsto f(i)$ ein Integritätsring, der so genannte *Ring der ganzen Gaußschen Zahlen*. In diesem Ring lässt sich eine Division mit Rest erklären, d.h. $\mathbb{Z}[i]$ wird ein *euklidischer Ring*, indem man die Gradabbildung

$$\delta : \mathbb{Z}[i] - \{0\} \longrightarrow \mathbb{N}, \quad \alpha \longmapsto |\alpha|^2$$

eingührt: Stellt man sich nämlich $\mathbb{Z}[i]$ in der Gaußschen Zahlenebene $\mathbb{C} \cong \mathbb{R}^2$ vor, so bildet $\mathbb{Z}[i]$ ein *Gitter* in \mathbb{C} . Nach dem Satz von Pythagoras ist der Abstand zweier benachbarter Punkte aus $\mathbb{Z}[i]$ höchstens gleich der Länge $\sqrt{2}$ der Diagonalen einer *Masche*. Zu $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$ gibt es daher ein $\gamma \in \mathbb{Z}[i]$, sodass

$$|\alpha\beta^{-1} - \gamma| \leq \frac{1}{2} \cdot \sqrt{2} < 1.$$

Setzt man $\rho := \alpha - \beta\gamma$, so hat man $|\rho| < |\beta|$, also

$$\alpha = \beta\gamma + \rho \quad \text{und} \quad \delta(\rho) < \delta(\beta).$$

Insbesondere ist $\mathbb{Z}[i]$ als euklidischer Ring faktoriell, d.h. jedes Element aus $\mathbb{Z}[i] - (\mathbb{Z}[i]^\times \cup \{0\})$ lässt sich als Produkt von Primelementen aus $\mathbb{Z}[i]$ schreiben. (Dies ist eine Verallgemeinerung der wohlbekanntenen Primfaktorzerlegung des euklidischen Ringes \mathbb{Z} : Dort ist $\mathbb{Z}^\times = \{-1, 1\}$ und bekanntlich lässt sich jede Zahl $z \in \mathbb{Z} - (\mathbb{Z}^\times \cup \{0\})$ als Produkt von Primelementen aus \mathbb{Z} schreiben.)

2 Primzahlen als Summe zweier Quadratzahlen

2.1 Existenz

Proposition 1. Eine Primzahl $p \neq 2$ lässt sich genau dann als Summe zweier Quadratzahlen schreiben, $p = x^2 + y^2$, $x, y \in \mathbb{Z}$, wenn $p \equiv 1 \pmod{4}$.

Die Richtung “ \Rightarrow ” ist leicht einzusehen: Wegen $x^2 \equiv 0, 1 \pmod{4}$ für alle $x \in \mathbb{Z}$ gilt $x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$ für alle $x, y \in \mathbb{Z}$. Da p prim ist, muss $p \equiv 1 \pmod{4}$ gelten.

2.1.1 Erster Beweis (nach Axel Thue)

Beweis. “ \Leftarrow ”: Die Menge $M := \{0, 1, \dots, \lfloor \sqrt{p} \rfloor\}^2$ hat $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$ Elemente. Nach dem Schubfachprinzip gibt es daher zu jedem $s \in \mathbb{Z}$ zwei voneinander verschiedene Paare

$(x', y'), (x'', y'') \in M$ mit

$$x' - sy' \equiv x'' - sy'' \pmod{p}, \quad \text{d.h.} \quad x' - x'' \equiv s(y' - y'') \pmod{p}.$$

Man setze $x := |x' - x''|$, $y := |y' - y''|$. Dann gilt $(x, y) \in M \setminus \{(0, 0)\}$ und mit einem geeigneten Vorzeichen $x \equiv \pm sy \pmod{p}$. Nach Lemma 1 ist -1 ein quadratischer Rest modulo p , d.h. man kann s so wählen, dass $s^2 \equiv -1 \pmod{p}$. Dann gilt $x^2 \equiv s^2 y^2 \equiv -y^2 \pmod{p}$. Es gilt also

$$(x, y) \in \mathbb{Z}^2 \quad \text{mit} \quad 0 < x^2 + y^2 < 2p \quad \text{und} \quad x^2 + y^2 \equiv 0 \pmod{p}.$$

Aber p ist die einzige Zahl zwischen 0 und $2p$, die durch p teilbar ist. Daher muss $x^2 + y^2 = p$ gelten. \square

2.1.2 Zweiter Beweis (nach Heath-Brown)

Beweis. “ \Leftarrow ”: Man setze

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

$$T := \{(x, y, z) \in S : z > 0\}$$

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

S ist eine endliche Menge, denn aus $x \geq 1$, $y \geq 1$ folgt $y \leq \frac{p}{4}$ und $x \leq \frac{p}{4}$. Umgekehrt gibt es zu jedem Paar (x, y) höchstens zwei Werte für z , derart dass $(x, y, z) \in S$. Der Beweis lässt sich in 3 Schritte gliedern:

(1) T und U haben dieselbe Kardinalität, d.h. $|T| = |U|$.

Die lineare Involution

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

hat keine Fixpunkte (aus $z = 0$ folgt $p = 4xy$) und ist injektiv, folglich bijektiv. Also bildet f die endliche Menge T auf

$$\{(x, y, z) \in S : z < 0\} = \{(x, y, z) \in S : z \leq 0\} = S \setminus T$$

ab. Weiter gilt

$$S \setminus U = \{(x, y, z) \in S : (x - y) + z \leq 0\} = \{(x, y, z) \in S : (x - y) + z < 0\},$$

denn aus $(x - y) + z = 0$ folgt $p = 4xy + z^2 = 4xy + (x - y)^2 = (x + y)^2$. Da f die Vorzeichen von $x - y$ und z gleichzeitig vertauscht, d.h. aus $(x - y) + z > 0$ wird $(x' - y') + z' < 0$, wenn $(x', y', z') = f(x, y, z)$ gesetzt ist, bildet f die Menge U auf $S \setminus U$ ab. Insgesamt ergibt sich somit $|T| = \frac{1}{2}|S| = |U|$.

(2) Die Kardinalität von U ist ungerade. Dazu betrachte man die Involution

$$g : U \longrightarrow U, \quad (x, y, z) \longmapsto (x - y + z, y, 2y - z).$$

Ist $(x, y, z) \in U$ und $(x', y', z') := g(x, y, z)$ gesetzt, so gilt $x' = x - y + z > 0$, $y' = y > 0$ und

$$4x'y' + z'^2 = 4(x - y + z)y + (2y - z)^2 = 4xy + z^2 = p,$$

also $g(x, y, z) = (x', y', z') \in S$. Aus $x' - y' + z' = (x - y + z) - y + (2y - z) = x > 0$ folgt schließlich $g(x, y, z) \in U$. Ferner hat man

$$g(x', y', z') = g(x - y + z, y, 2y - z) = ((x - y + z) - y + (2y - z), y, 2y - (2y - z)) = (x, y, z),$$

also $g^2 = \text{id}$. Es gilt

$$g(x, y, z) = (x - y + z, y, 2y - z) = (x, y, z)$$

genau dann, wenn $y = z$. Die Gleichung $p = 4xy + y^2 = (4x + y)y$ zeigt, dass dies nur für $y = z = 1$ und $x = \frac{p-1}{4}$ gelten kann. g ist also eine Involution auf U mit genau einem Fixpunkt. Folglich ist $|U|$ ungerade.

(3) Es gibt einen Punkt $(x, y, z) \in T$ mit $x = y$, d.h. p ist Summe zweier Quadrate,

$$p = 4x^2 + z^2 = (2x)^2 + z^2.$$

Hierzu betrachte man die Involution

$$h : T \longrightarrow T, \quad (x, y, z) \longmapsto (y, x, z).$$

Da $|T| = |U|$ ungerade ist, muss h einen Fixpunkt $(x, y, z) \in T$ besitzen; für diesen gilt $x = y$. □

2.1.3 Dritter Beweis (Algebraische Zahlentheorie)

Beweis. “ \Leftarrow ”: Es genügt zu zeigen, dass p in $\mathbb{Z}[i]$ kein Primelement bleibt: Dann gibt es eine Zerlegung $p = \alpha\beta$ in zwei Nichteinheiten $\alpha, \beta \in \mathbb{Z}[i]^\times$. Bezeichnet $N(z)$ das Quadrat der Norm einer komplexen Zahlen z , also $N(z) = |z|^2$, so gilt

$$p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta). \quad (*)$$

Da α, β keine Einheiten sind, gilt $N(\alpha), N(\beta) \neq 1$: Angenommen, es wäre etwa $N(\alpha) = 1$, so folgte $a^2 + b^2 = 1$, wenn $\alpha = a + ib$ gesetzt ist. Entweder es gilt dann $a = \pm 1, b = 0$ oder $a = 0, b = \pm 1$; aber jedes der Elemente $\pm 1, \pm i$ ist offensichtlich eine Einheit.

Wegen $N(\alpha), N(\beta) \neq 1$ folgt aus $(*)$ die Darstellung $p = N(\alpha) = a^2 + b^2$, d.h. p ist Summe zweier Quadrate.

Auf Grund der Voraussetzung $p \equiv 1 \pmod{4}$ ist -1 ein quadratischer Rest modulo p nach Lemma 1, d.h. es gibt ein $x \in \mathbb{Z}$ mit $p|x^2 + 1 = (x + i)(x - i)$. Wäre p prim, so müsste $p|x + i$ oder $p|x - i$ folgen, aber $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$, d.h. p ist nicht prim. \square

2.2 Eindeutigkeit

Die Darstellung aus Proposition 1 ist bis auf die Reihenfolge der Summanden eindeutig.

2.2.1 Erster Beweis (elementar)

Beweis. Angenommen, man hätte zwei verschiedene Darstellungen $p = x^2 + y^2 = \tilde{x}^2 + \tilde{y}^2$ mit $x, \tilde{x}, y, \tilde{y} \in \mathbb{Z}$. O.B.d.A. gelte $1 \leq x, y, \tilde{x}, \tilde{y}$ und o.B.d.A. seien x, \tilde{x} gerade, y, \tilde{y} ungerade und $\tilde{x} > x$. Dann ist $y > \tilde{y}$ und es gibt zwei natürliche Zahlen s, t mit $\tilde{x} = 2s + x$ und $\tilde{y} = y - 2t$. Aus

$$p = \tilde{x}^2 + \tilde{y}^2 = (2s + x)^2 + (y - 2t)^2 = p + 4sx + 4s^2 - 4ty + 4t^2$$

folgt $s(x + s) = t(y - t)$ $(*)$. Setze $d := \text{ggT}(s, t)$. Für $\tilde{s} := s/d$ und $\tilde{t} := t/d$ gilt $\text{ggT}(\tilde{s}, \tilde{t}) = 1$. Aus $(*)$ folgt $\tilde{s}(x + s) = \tilde{t}(y - t)$ $(**)$. Wegen der Teilerfremdheit von \tilde{s} und \tilde{t} gilt daher $\tilde{t}|x + s$, d.h. es gibt ein $m \in \mathbb{N}$, sodass $x + s = m\tilde{t}$. Setzt man dies in $(**)$ ein, so erhält man $m\tilde{s} = y - t$. Unter Verwendung von $s = d\tilde{s}$ und $t = d\tilde{t}$ hat man daher die beiden Gleichungen $m\tilde{t} = x + d\tilde{s}$ und $m\tilde{s} = y - d\tilde{t}$. Es folgt

$$p = x^2 + y^2 = (m\tilde{t} - d\tilde{s})^2 + (m\tilde{s} + d\tilde{t})^2 = (m^2 + d^2)(\tilde{s}^2 + \tilde{t}^2).$$

Beide Faktoren auf der rechten Seite sind echt größer als 1; Widerspruch zur Primalität von p . \square

2.2.2 Zweiter Beweis (algebraische Zahlentheorie)

Beweis. Es gilt $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$. Die Inklusion “ \supseteq ” ist klar. Sei umgekehrt $\alpha \in \mathbb{Z}[i]^\times$. Dann gibt es ein $\beta \in \mathbb{Z}[i]$ mit $\alpha\beta = 1$, woraus $1 = N(\alpha\beta) = N(\alpha)N(\beta)$ folgt, also $N(\alpha) = 1$, d.h. nach 2.1.3 gilt $\alpha \in \{1, -1, i, -i\}$.

Sei nun p eine Primzahl und seien $p = x^2 + y^2 = \tilde{x}^2 + \tilde{y}^2$ zwei Darstellungen, d.h.

$$p = (x + iy)(x - iy) = (\tilde{x} + i\tilde{y})(\tilde{x} - i\tilde{y}).$$

Keiner der vier Klammersausdrücke ist Null oder eine Einheit; tatsächlich handelt es sich um Primelemente in $\mathbb{Z}[i]$. Es gelte etwa $x + iy = \alpha\beta$ mit $\alpha, \beta \in \mathbb{Z}[i]$. Dann folgt

$$p^2 = N(p) = N(x^2 + y^2) = N(x + iy)N(x - iy) = N(\alpha\beta)N(x - iy) = N(\alpha)N(\beta)(x^2 + y^2),$$

also $N(\alpha)N(\beta) = p$, d.h. entweder $N(\alpha) = 1$ oder $N(\beta) = 1$. Es ist also genau eines der Elemente α, β eine Einheit und $x + iy$ folglich irreduzibel, also prim, da $\mathbb{Z}[i]$ faktoriell ist. Zerlegungen in Primelemente sind im Wesentlichen eindeutig; daher gilt mit einer Einheit $\varepsilon \in \mathbb{Z}[i]^\times = \{1, -1, i, -i\}$ entweder $x + iy = \varepsilon(\tilde{x} + i\tilde{y})$ oder $x + iy = \varepsilon(\tilde{x} - i\tilde{y})$; ersteres impliziert $\tilde{x} - i\tilde{y} = \varepsilon(x - iy)$ und letzteres $\tilde{x} + i\tilde{y} = \varepsilon(x - iy)$.

Gilt etwa $x + iy = \varepsilon(\tilde{x} + i\tilde{y})$ mit $\varepsilon = i$, so bedeutet das $x + iy = -\tilde{y} + i\tilde{x}$, also $x = -\tilde{y}$ und $y = \tilde{x}$, d.h. $x^2 = \tilde{y}^2$, $y^2 = \tilde{x}^2$; analog behandelt man die restlichen Fälle. \square

3 Natürlichen Zahlen als Summe zweier Quadratzahlen

Die Vielfachheit $\nu_p(n) \geq 0$ einer Primzahl p in n ist definiert durch die Forderung $p^{\nu_p(n)} | n$, $p^{\nu_p(n)+1} \nmid n$, m.a.W.

$$\nu_p(n) := \max\{k \in \mathbb{N}_0 : p^k | n\}.$$

3.1 Der Zwei-Quadrate-Satz von Fermat

Satz. Für $n \in \mathbb{N}$ ist die diophantische Gleichung

$$x^2 + y^2 = n \tag{1}$$

genau dann lösbar, wenn für jede Primzahl $p \equiv 3 \pmod{4}$ ihre Vielfachheit $\nu_p(n)$ gerade ist.

Beweis. Jede natürliche Zahl n , für die (1) lösbar ist, werde im Folgenden *darstellbar* genannt. Vorüberlegungen:

- (1) $1 = 1^2 + 0^2$ und $2 = 1^2 + 1^2$ sind darstellbar. Jede Primzahl $p \equiv 1 \pmod{4}$ ist darstellbar.
- (2) Das Produkt zweier darstellbarer Zahlen $n = x^2 + y^2$ und $\tilde{n} = \tilde{x}^2 + \tilde{y}^2$ ist darstellbar, denn $n\tilde{n} = (x\tilde{x} + y\tilde{y})^2 + (x\tilde{y} - \tilde{x}y)^2$.

“ \Leftarrow ”: Ist für jede Primzahl $p \equiv 3 \pmod{4}$ die Vielfachheit $\nu_p(n)$ gerade, so ist

$$n_0 := \prod_{p \equiv 3 \pmod{4}} p^{\nu_p(n)} = \left(\prod_{p \equiv 3 \pmod{4}} p^{\nu_p(n)/2} \right)^2 + 0^2$$

darstellbar. Mit (1) und (2) folgt, dass n darstellbar ist.

“ \Rightarrow ”: Sei $n = x^2 + y^2$ eine darstellbare Zahl und $p \equiv 3 \pmod{4}$ eine Primzahl mit $p|n$. Dann gilt auch $p^2|n$: Angenommen, es wäre $x \not\equiv 0 \pmod{p}$. Dann ist x modulo p invertierbar und aus $x^2 + y^2 \equiv 0 \pmod{p}$ folgt durch Multiplikation mit $(1/x)^2$ die Gleichung $1 + (y/x)^2 \equiv 0 \pmod{p}$. Nach Lemma 1 ist aber -1 kein quadratischer Rest modulo $p \equiv 3 \pmod{4}$. Folglich gilt $p|x$ und analog $p|y$, also $p^2|x^2 + y^2 = n$.

Mithin ist n/p^2 darstellbar. Also gilt $\nu_p(n) \equiv 0 \pmod{2}$ für alle Primzahlen $p \equiv 3 \pmod{4}$. \square

4 Ausblick

4.1 Die Anzahl der verschiedenen Darstellungen $n = x^2 + y^2$

Setzt man $d_{r,4}(n) := \#\{t \in \{1, 2, \dots, n\} : t|n \text{ und } t \equiv r \pmod{4}\}$, so hat die Gleichung $n = x^2 + y^2$ mit $n \in \mathbb{N}$ und $x, y \in \mathbb{Z}$ genau

$$c_n := 4(d_{1,4}(n) - d_{3,4}(n))$$

verschiedene Lösungen. (Zwei Lösungen $n = x^2 + y^2 = \tilde{x}^2 + \tilde{y}^2$ werden hierbei genau dann als verschieden bezeichnet, wenn $(x, y) \neq (\tilde{x}, \tilde{y})$.)

4.2 Die Menge aller Zahlen der Form $n = x^2 + y^2$ ist “klein”

Sei D die Menge aller darstellbaren natürlichen Zahlen. (Eine natürliche Zahl wurde darstellbar genannt, wenn sie sich als Summe zweier Quadratzahlen schreiben lässt.) Offenbar sind D und $\mathbb{N} \setminus D$ zwei unendliche Mengen. Beispielsweise ist keine Zahl $\equiv 3 \pmod{4}$ darstellbar. Setzt man $D(x) := \#\{n \in \mathbb{N} : n \leq x, n \in D\}$, so gilt nach einer Arbeit von Landau $D(x) \sim c \frac{x}{\sqrt{\log x}}$ bei $x \rightarrow \infty$ mit einer reellen Konstanten $c > 0$. Daraus folgt

$$\lim_{x \rightarrow \infty} \frac{D(x)}{x} = 0,$$

d.h. es lassen sich (in diesem Sinne) die “wenigsten” natürlichen Zahlen als Summe zweier Quadrate schreiben. Allerdings lässt sich jede natürliche Zahl als Summe vierer Quadrate schreiben (Satz von Lagrange).

5 Literaturverzeichnis

- [1] Aigner M., Ziegler G.M. „Das BUCH der Beweise“. Berlin Heidelberg. Springer. ²2004.
- [2] Bosch. „Algebra“. Berlin Heidelberg. Springer. ⁶2006.
- [3] Bundschuh. „Einführung in die Zahlentheorie“. Springer. Berlin Heidelberg. ³1996.
- [4] Neukirch, Jürgen. „Algebraische Zahlentheorie“. Berlin Heidelberg. Springer. 1992.