Prof. Dr. Gerhard Rosenberger

Schöne Zahlen

Vortrag bei der Lehrerfortbildung

"Schönheit in der Mathematik",

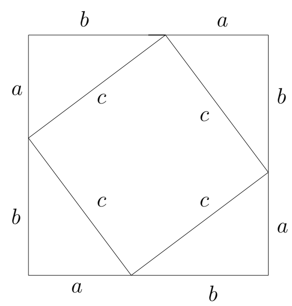
Universität Passau, 18.12.2019

Definition 1 (Pythagoreische Tripel)
Ein Tripel $(a, b; c)$ natürlicher Zahlen heißt ein *Pythagoreisches Tripel* falls $a^2 + b^2 = c^2$.

Beachte: Für ein festes c betrachten wir die Tripel $(a, b; c)$ und $(b, a; c)$ als gleich. Ein Pythagoreische Tripel heißt *primitiv* falls $\mathrm{ggT}(a, b, c) = \mathrm{ggT}(a, b) = \mathrm{ggT}(a, c) = \mathrm{ggT}(b, c) = 1$. Um alle Pythagoreische Tripel zu klassifizieren, genügt es alle primitiven zu kennen.

Wohl jeder kennt das Tripel $(3, 4; 5)$. Dies war schon in allen Frühkulturen bekannt:

1) Dialog von Kaiser Tschong Kong und dem Gelehrten Schanck Kaern (1100 BC).
2) Erwähnung im Alten Testament beim Bau der Bundeslade und dem Brandopferaltar (zweites Buch Moses und erstes Buch Könige).
3) Etliche Tripel sind erwähnt auf den Keilschrifttafeln zur Zeit des babylonischen Königs Hammurabi (1828-1530 BC); unter anderem $(12709, 13500; 18541)$. Dies gibt Hinweise auf die Konstruktion von Pythagoreischen Tripeln.
4) Das indische Baudhayana Sulbastra (600 BC) - Buch über die Kunst des Messens - enthält fünf Pythagoreische Tripel.
5) Plato (ca 428-348 BC) beschrieb Tripel der Form $(n^2 - 1, 2n; n^2 + 1)$.
6) Pythagoras (570-510 BC) beschrieb unendlich viele Pythagoreische Tripel der Form $(2n+1, 2n^2+2n; 2n^2+2n+1)$. Dies ist wahrscheinlich der Grund für die Namensgebung. Pythagoras formulierte das Problem, alle Tripel zu bestimmen. In dem Zusammenhang wurde der Satz vom rechtwinkligen Dreieck auch Satz des Pythagoras genannt.



$$(a+b)^2 = 4 \cdot \tfrac{1}{2}ab + c^2 \quad \Rightarrow a^2 + b^2 = c^2$$

Abbildung 1: China, 2000 BC

7) In der frühen Architektur wurde das Tripel $(3, 4, 5)$ zur Konstruktion von rechten Winkeln verwendet, etwa beim Bau der Pyramiden (2585 BC).

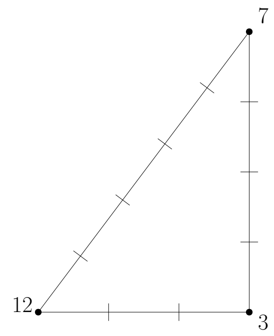


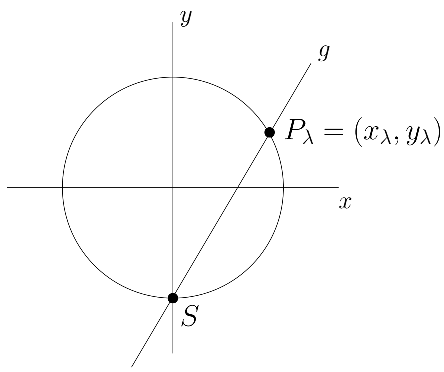
Abbildung 2: Ägyptische Seilspanner

8) Brahmagupta (628) gab eine Regel: Sei $a \in \mathbb{N}, d \in \mathbb{N}$ mit $d \mid a^2$ und $\frac{a^2}{d} - d$ gerade. Setze $b = \frac{1}{2}(\frac{a^2}{d} - d)$ und $c = \frac{1}{2}(\frac{a^2}{d} + d)$. Dann ist $(a, b; c)$ ein Pythagoreisches Tripel.

Satz 2 (Arithmetica von Diophantos (300 BC))
Seien $n, m \in \mathbb{N}$ mit $ggT(n, m) = 1$ und $n - m > 0$ und ungerade. Dann ist $(n^2 - m^2, 2nm; n^2 + m^2)$ ein primitives Pythagoreisches Tripel, und ferner kann jedes primitive Pythagoreische Tripel in der Form erhalten werden.

Beweis: Die angegebenen Tripel sind natürlich Pythagoreische Tripel, sogar primitive. Sei nun $(a, b; c)$ ein Pythagoreisches Tripel $(a, b, c \in \mathbb{N})$, also $a^2 + b^2 = c^2$. Dann ist $x^2 + y^2 = 1$ mit $x = \frac{a}{c}, y = \frac{b}{c}$ positive rationale Zahlen.

Umgekehrt liefert jede positive rationale Lösung von $x^2 + y^2 = 1$ ein Pythagoreisches Tripel nach Bestimmung eines gemeinsamen Nenners: $x = \frac{a}{c}, y = \frac{b}{c}$. Daher reduziert sich die Bestimmung der primitiven Pythagoreischen Tripel auf die Bestimmung der positiven rationalen Lösungen von $x^2 + y^2 = 1$. Diese Gleichung beschreibt einen Kreis um $(0, 0)$ vom Radius 1, den Einheitskreis E.



Sei $g\colon y = \lambda x - 1$ eine Gerade durch $S = (0, -1)$ und Steigung $\lambda \neq 0$. Sei $P_\lambda = (x_\lambda, y_\lambda) \neq S$ der zweite Schnittpunkt von g mit E.

Die Koordinaten von P_λ erfüllen die Gleichung

$$1 = x^2 + y^2 = x^2 + (\lambda x - 1)^2.$$

Es folgt $(\lambda^2+1)x^2 - 2\lambda x = 0$. Wegen $\lambda \neq 0$ ist $x_\lambda \neq 0$. Es folgt $x_\lambda = \frac{2\lambda}{\lambda^2+1}$ und $y_\lambda = \lambda x_\lambda - 1 = \frac{\lambda^2-1}{\lambda^2+1}$. Also ist (x_λ, y_λ) eine rationale Lösung genau dann wenn

$$\lambda = \frac{y_\lambda + 1}{x_\lambda} \in \mathbb{Q}.$$

Wir wollen alle positiven rationalen Lösungen, d.h. $x_\lambda, y_\lambda > 0$. Für die ist $\lambda^2 - 1 > 0$ und $\lambda > 0$ also $\lambda > 1$. Setze $\lambda = \frac{n}{m} > 1$ mit $\mathrm{ggT}(n,m) = 1$. Einsetzen ergibt:

$$x_\lambda = \frac{2nm}{n^2+m^2} \text{ und } y_\lambda = \frac{n^2-m^2}{n^2+m^2}.$$

Wegen $\lambda > 1$ erhalten wir das Pythagoreische Tripel $(2nm, n^2-m^2; n^2+m^2)$. Dies ist primitiv genau dann wenn $n-m$ und damit auch $n+m = n-m+2m$ ungerade ist. Denn: Ist p prim mit $p \mid n$ und $p \mid n^2-m^2$, so ist $p \mid (n-m)$ oder $p \mid (n+m)$ also $p \mid m$. Dies steht im Widerspruch zu $\mathrm{ggT}(n,m) = 1$. Ist $n-m$ gerade, so ist das Tripel nicht primitiv, da dann $2 \mid (n^2-m^2)$ und $2 \mid 2nm$. □

Satz 3 (Großer Fermatscher Satz (17. Jhd))
Die Gleichung $a^n + b^n = c^n, n \in \mathbb{N}, n \geq 3$, hat keine Lösung in den natürlichen Zahlen.

Dieser Satz wurde erst 1994 von Andrew Wiles (in Teilen mit Richard Taylor) bewiesen. Im Laufe der Jahre wurde die Aussage für einige Spezialfälle auch schon früher nachgewiesen:

- $n = 4$ Fermat
- $n = 3$ und $n = 6$: Euler (1770)
- $n = 5$: Legendre (1825)
- $n = 7$: Launé (1839)

Im folgenden findet sich ein Beweis für den Fall $n = 4$, also für die Aussage: $x^4 + y^4 = z^2$ hat keine Lösung in den natürlichen Zahlen.

Beweis: Wir nehmen an, es gibt eine Lösung $(x_0, y_0; z_0)$ über $\mathbb{N}$. Ohne Einschränkung sei $\mathrm{ggT}(x_0, y_0, z_0) = 1$. Wir konstruieren eine Lösung (x_1, y_1, z_1) mit $z_1 < z_0$ in den natürlichen Zahlen. Es ist $(x_0^2, y_0^2; z_0)$ ein primitives Pythagoreisches Tripel. Wir können also annehmen, dass

$$x_0^2 = a^2 - b^2, \quad y_0^2 = 2ab, \quad z_0 = a^2 + b^2$$

mit $\mathrm{ggT}(a,b) = 1, a > b, a^2 - b^2$ ungerade (dann ist auch $a - b$ ungerade).
a kann nicht gerade sein, da sonst $x_0^2 = 4k^2 - b^2, b$ ungerade also $x_0^2 = 4l - 1$, was nicht geht. Also ist a ungerade. Da x_0^2 auch ungerade ist, ist b notwendig gerade.

Wegen $\operatorname{ggT}(a,b) = 1$ und $x_0^2 + b^2 = a^2$ gibt es c, d mit $\operatorname{ggT}(c,d) = 1, c > d$ und $c - d$ ungerade mit $x_0 = c^2 - d^2$, $b = 2cd$, $a = c^2 + d^2$.

Wegen $\operatorname{ggT}(a,b) = 1$ folgt $\operatorname{ggT}(c,d) = \operatorname{ggT}(c, c^2+d^2) = \operatorname{ggT}(d, c^2+d^2) = 1$. Es folgt $y_0^2 = 2ab = 4cd(c^2+d^2)$ also $(\frac{1}{2}y_0)^2 = cd(c^2+d^2)$. Nach Euklids Lemma gibt es x_1, y_1, z_1 mit $x_1^2 = c, y_1^2 = d, z_1^2 = c^2 + d^2$, also $z_1^2 = c^2 + d^2 = x_1^4 + y_1^4$. Es ist

$$z_1 \leq z_1^2 = c^2 + d^2 = a < a^2 + b^2 = z_0.$$

Wir machen so weiter und erhalten eine Folge von Lösungen $(x_k, y_k; z_k), k = 0, 1, 2, \ldots$ mit $z_0 > z_1 > z_2 > \cdots > 0$. Dies steht im Widerspruch zur Tatsache, dass jede nicht-leere Teilmenge der natürlichen Zahlen ein kleinstes Element enthält, also hat $x^4 + y^4 = z^2$ keine Lösung über $\mathbb{N}$. $\square$

Weitere Beispiele für die geometrische Methode:

1) Pell's Gleichung: $x^2 - Dy^2 = 1$ mit $D > 0, D$ quadratfrei. Es gibt die offensichtlichen Lösungen $(1,0)$ und $(-1,0)$.

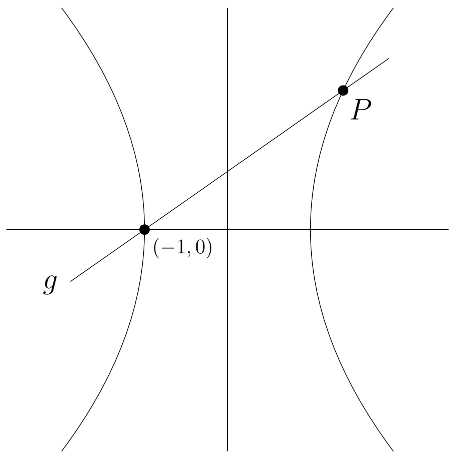


Abbildung 3: Graph von $x^2 - Dy^2 = 1$.

Betrachte $g : y = m(x+1)$. Für die Koordinaten von P gilt: $x^2 - Dm^2(x+1)^2 = 1$. Es folgt

$$(1 - Dm^2)x^2 - (2Dm^2)x - (Dm^2 + 1) = 0.$$

Eine Lösung ist $x = -1$, die andere ist

$$x = \frac{1 + Dm^2}{1 - Dm^2}$$

Das gibt

$$y = m\left(\frac{1 + Dm^2}{1 - Dm^2} + 1\right) = \frac{2m}{1 - Dm^2}$$

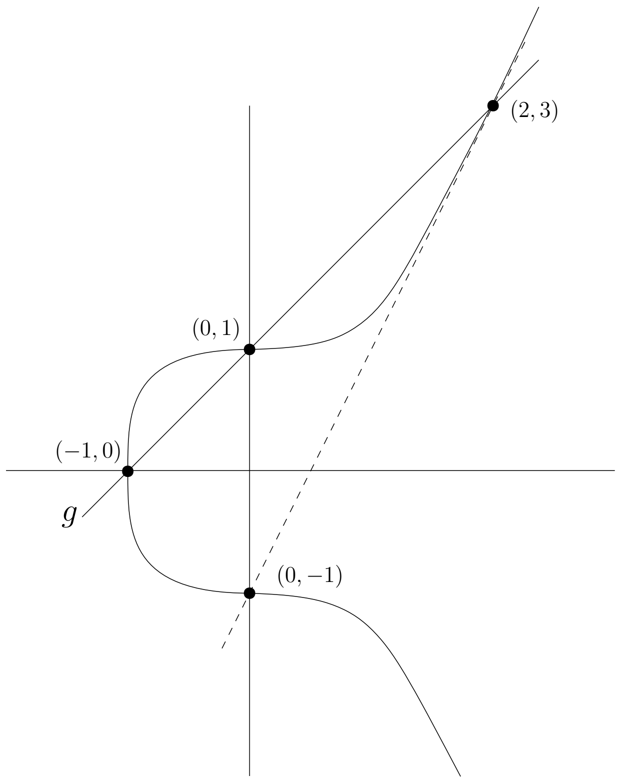
Dies beweist auch den folgenden Satz.

Satz 4
Jede Lösung (x, y) *von* $x^2 - Dy^2 = 1$ *ungleich* $(-1, 0)$ *ist ausdrückbar als*

$$x = \frac{1 + Dm^2}{1 - Dm^2}, \quad y = \frac{2m}{1 - Dm^2}.$$

Man kann jetzt ganzzahlige Lösungen für $X^2 - DY^2 = Z^2$ finden.
Beispiel: Für $m = 2$ ist $(x, y) = (-\frac{13}{11}, -\frac{4}{11})$. Also $(X, Y, Z) = (-13, -4, 11)$.

2. Die Gleichung $y^2 = x^3 + 1$ beschreibt eine elliptische Kurve.



Die Gleichung hat die offensichtlichen Lösungen $(0, 1)$ und $(-1, 0)$. Diese beiden Punkte $(0, 1)$ und $(-1, 0)$ werden durch die Gerade $g\colon\ y = x + 1$ verbunden. Der dritte Punkt auf g und der elliptischen Kurve ist $(2, 3)$. Die Tangente durch $(2, 3)$ erfüllt die Gleichung

$$2yy' = 3x^2$$

Die Steigung der Tangente durch $(2, 3)$ ist $m = 2$.

$$y' = \frac{1}{2} \cdot \frac{1}{\sqrt{x^3 + 1}} \cdot 3 \cdot x^2$$

Also $y'(2) = m = 2$. Die Gleichung der Tangente ist gegeben durch $y = 2x - 1$, denn aus $h\colon\ y = 2x + n$ und $(2,3) \in h$ folgt $n = -1$. Der Schnitt dieser Tangente mit dem Graphen von $y^2 = x^3 + 1$ ist der Punkt $(0, -1)$. Man kann zeigen, dass die Gleichung $y^2 = x^3 + 1$ nur endlich viele rationale Lösungspaare (x, y) hat.

Betrachten wir die Kurve $y^2 = x^3 + 17$, so sehen wir, dass die Punkte $(-1, 4)$ und $(2, 5)$ auf der Kurve liegen. Die Gleichung für die Gerade durch diese Punkte ist

$$y = \tfrac{1}{3}x + \tfrac{13}{3}$$

Der weitere Schnittpunkt der Geraden mit der Kurve ist $(-\frac{8}{9}, \frac{109}{27})$. Fährt man so fort, so erhält man unendlich viele Paare rationaler Zahlen, die $y^2 = x^3 + 17$ erfüllen.

Eine andere Strategie ist, einen Punkt und eine (abstrakte) Steigung der Kurve in dem Punkt anzugeben. Beispiel: $y^2 = -x^3 - 1$. Es gibt die Lösung $(0, 1)$. Die Gerade durch diesen Punkt mit Steigung m ist $G : y = m(x + 1)$. Wir erhalten dann die Gleichung

$$m^2(x + 1)^2 + x^3 + 1 = 0.$$

Dies gibt

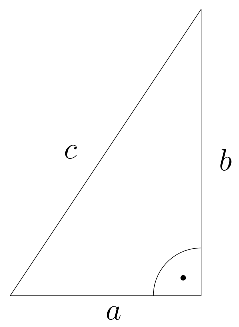
$$x^3 + m^2x^2 + 2m^2x + (1 + m)^2 = 0.$$

Da $(-1, 0)$ auf g liegt, ist die linke Seite durch $(x + 1)$ teilbar. Das ergibt

$$(x + 1)(x^2 + (m^2 - 1)x + (m^2 + 1)) = 0.$$

Die Diskriminante von $x^2 + (m^2 - 1)x + (m^2 + 1)$ ist $\tau^2 = (m^2 - 1)^2 - 4(m^2 + 1) = m^4 - 6m^2 - 3$. Diese Gleichung hat aber einen höheren Grad als die ursprüngliche Gleichung.

Wie sieht die Länge der Hypotenuse eines rechtwinkligen Dreiecks mit ganzzahligen Katheten aus?



Es gilt $c^2 = a^2 + b^2$, also $c = \sqrt{a^2 + b^2}$. Wann ist $n = c \in \mathbb{N}$? Also, wann lässt sich $n \in \mathbb{N}$ darstellen als $n = x^2 + y^2$ mit $x, y \in \mathbb{Z}$?

Wir können uns auf die primitiven Gleichungen beschränken, d.h. auf $n = x^2 + y^2$ mit $\mathrm{ggT}(x, y) = 1$. Dann ist -1 quadratischer Rest mod n. Das ist genau der Inhalt des Satzes von Fermat:

Satz 5
$n = x^2 + y^2$ mit $ggT(x, y) = 1$, wenn -1 quadratischer Rest $\pmod n$ ist, d.h. wenn es q und $p \in \mathbb{Z}$ gibt mit $-1 = q^2 - pn$.

Beweis: Das lässt sich so zeigen. Sei $\Gamma = \left\{\pm \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{Z},\ ad - bc = 1\right\}$.
Per Hand oder mit dem Rechner kann man direkt zeigen:

1) Sei $A = \pm \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. Dann hat A die Ordnung 2 genau dann, wenn $a + d = 0$.

3) Hat $A = \pm \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ die Ordnung 2, so gibt es $X = \pm \left(\begin{smallmatrix} x & y \\ u & v \end{smallmatrix}\right) \in \Gamma$ mit $A = \pm X \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) X^{-1}$

   Sei $-1 = q^2 - pn$. Bilde $A = \left(\begin{smallmatrix} q & n \\ -p & -q \end{smallmatrix}\right)$. Dann ist $\pm A \in \Gamma$ und

$$\pm \left(\begin{smallmatrix} q & n \\ -p & -q \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} x & y \\ u & v \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} v & -y \\ -u & x \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} -(yv+xu) & x^2+y^2 \\ -(u^2+v^2) & (yv+xu) \end{smallmatrix}\right) \qquad \square$$

Sei p eine Primzahl. Dann ist $p = x^2 + y^2, x, y, \in \mathbb{Z}$, genau dann wenn $p = 2$ oder $p \equiv 1 \pmod 4$. Mit $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (bc + ad)^2$ kann man explizite Darstellungen für $n \in \mathbb{N}$ finden, wenn man die Primfaktorzerlegung von n kennt.

Definition 6 (Kongruenzzahl)
Eine *Kongruenzzahl* ist eine natürliche Zahl, die der Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seiten ist.

Wir wissen: Ist $\triangle$ ein rechtwinkliges Dreieck mit natürlichen, paarweise teilerfremden Seiten a, b, c (mit Hypotenuse c), so ist $(a, b; c) = (n^2 - m^2, 2nm; n^2 + m^2)$ mit $\mathrm{ggT}(n, m) = 1$, $n > m$ und $n - m$ ungerade. Der Flächeninhalt solch eines Dreiecks ist dann gegeben durch $s = \frac{1}{2}ab = nm(n^2 - m^2)$. Wann ist s selbst ein Quadrat?

Angenommen $s = t^2$, dann haben wir $a^2 + b^2 = c^2$ und $ab = 2t^2$. Da a oder b gerade ist, etwa $a = 2k$, folgt $kb = t^2$. Da k und b teilerfremd sind, gilt $k = p^2$ und $b = q^2$ wegen $a = 2k^2 = 2p^2$. Die Pythagoreische Gleichung lautet dann

$$4k^4 + q^4 = c^2.$$

Diese Gleichung hat aber keine natürliche Lösung. Dies folgt analog wie oben bei Fermats Gleichung, wenn wir den Beweis mit dem Pythagoreischen Tripel $(2k^2, q^2; c)$ starten; s kann also kein Quadrat aus $\mathbb{N}$ sein.

Es ist sehr schwer, die $n \in \mathbb{N}$ zu finden, die Kongruenzzahlen sind.

Starten wir mit rationalen Seiten, so können wir mit dem Hauptnenner multiplizieren. Es folgt, dass 1 keine Kongruenzzahl ist. Die kleinste Kongruenzzahl ist 5, denn 5 ist der Flächeninhalt des rechtwinkligen Dreiecks mit den rationalen Seiten $\frac{20}{3}, \frac{3}{2}, \frac{41}{6}$.

Bemerkung 7
Sei nun $n \in \mathbb{N}$ fest. Es gibt eine Bijektion zwischen den Mengen

$$V_1 = \{(a,b,c) \in \mathbb{Q}^3 \mid a^2 + b^2 = c^2,\ \tfrac{ab}{2} = n\}$$

und

$$V_2 = \{(x,y) \in \mathbb{Q}^2 \mid y^2 = x^3 - n^2,\ xy \neq 0\}.$$

Die Bijektion ist gegeben durch $f_1\colon V_1 \to V_2$, $(a,b,c) \mapsto (\frac{nb}{c-a}, \frac{2n^2}{c-a})$ und $f_2\colon V_2 \to V_1$, $(x,y) \mapsto (\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y})$. Die Gleichung $y^2 = x^3 - n^2x$ hat die trivialen Lösungen $(0,0)$ und $(\pm n, 0)$. In beiden Fällen ist $xy = 0$.

Damit ist eine natürliche Zahl n eine Kongruenzzahl genau dann, wenn $y^2 = x^3 - n^2x$ eine nicht-triviale Lösung (d.h. $xy \neq 0$) hat.