6.4. Pythagoräische Tripel.

Man nennt ein Tripel $[x, y, z]$ natürlicher Zahlen ein *pythagoräisches Tripel,* falls gilt:

$$x^2 + y^2 = z^2.$$

Die Grundkonstruktion: Seien $a < b$ natürliche Zahlen. Dann gilt offensichtlich:

$$(2ab)^2 + (b^2 - a^2)^2 = (a^2 + b^2)^2$$

Wir sehen also: *Die Abbildung*

$$\eta\colon \{[a, b] \in \mathbb{N}^2 \mid a < b\} \longrightarrow \mathbb{N}^3, \quad \textit{mit} \quad \eta([a, b]) = [2ab, b^2 - a^2, a^2 + b^2]$$

hat als Bilder nur pythagoräische Tripel $[x, y, z]$. Zusätzlich gilt: *Die Abbildung* η *ist injektiv.*

Beweis: Sei $\eta([a, b]) = [x, y, z]$. Es ist $b^2 = \frac{1}{2}(y + z)$ und $a^2 = \frac{1}{2}(z - y)$, also folgt aus $\eta([a, b]) = \eta([a', b'])$ dass gilt $a^2 = (a')^2$ und $b^2 = (b')^2$, und demnach $a = a', b = b'$.

Aber man erhält nicht alle pythagoräischen Tripel auf diese Weise, denn

(1) Zum Beispiel erhält man nicht $[3, 4, 5]$, denn ist $\eta([a, b]) = [x, y, z]$, so ist x gerade,

(2) Zweites Beispiel: man erhält auch nicht $[12, 9, 15]$, denn 15 lässt sich nicht als Summe zweier Quadrate schreiben.

Punkt (1) ist irrelevant, denn es gilt: *Ist* $[x, y, z]$ *ein pythagoräisches Tripel, so ist mindestens eine der beiden Zahlen* x, y *gerade.*

Beweis: Wären beide Zahlen x, y ungerade, so wäre $x^2 \equiv 1$ und auch $y^2 \equiv 1$ modulo

Wir müssen uns um Punkt (2) kümmern. Offensichtlich ist $[12, 9, 15] = 3 \cdot [4, 3, 5]$ und $[4, 3, 5] = \eta([1, 2])$.

Ist $[x, y, z]$ *ein pythagoräisches Tripel, und* $d \in \mathbb{N}$*, so ist* $[dx, dy, dz]$ *ein pythagoräisches Tripel* (und auch umgekehrt gilt: Ist $[x, y, z]$ ein Tripel natürlicher Zahlen, $d \in \mathbb{N}$ und ist $[dx, dy, dz]$ pythagoräisch, so ist auch $[x, y, z]$ pythagoräisch). Um die pythagoräischen Tripel zu klassifizieren (das wollen wir jetzt tun), reicht es also, die primitiven pythagoräischen Tripel zu finden, dabei heißt ein pythagoräisches Tripel $[x, y, z]$ *primitiv*, falls $(x, y) = 1$ gilt (äquivalent dazu ist $(x, z) = 1$ und auch $(y, z) = 1$).

Ist $[x, y, z]$ *ein primitives pythagoräisches Tripel, so ist genau eine der beiden Zahlen* x, y *gerade.*

Beweis: Da $(x, y) = 1$, können x, y nicht beide gerade sein. 4, also $z^2 \equiv 2 \mod 4$. Gerade Quadratzahlen sind aber durch 4 teilbar.

Satz (Euklid) *Die Abbildung*

$$\begin{aligned}\eta\colon \{[a, b] \in \mathbb{N}^2 \mid a < b,\ (a, b) = 1,\ a \not\equiv b \mod 2\} \quad &\longrightarrow \\ \{[x, y, z] \in \mathbb{N}^3 \mid x^2 + y^2 = z^2,\ (x, y) = 1,\ x \equiv 0 \mod 2\},&\end{aligned}$$

definiert durch

$$\eta([a,b]) = [2ab, b^2 - a^2, a^2 + b^2]$$

ist eine Bijektion.

Insbesondere sehen wir: *Ist* $[x,y,z]$ *ein primitives pythagoräisches Tripel, so ist* z *selbst die Summe zweier Quadratzahlen!*

Der Satz steht schon bei EUKLID (Elemente, IX, § 28, 29) und war möglicherweise schon den Babyloniern bekannt (1500 v.u.Z.), jedenfalls gibt es babylonische Listen von primitiven pythagoräischen Tripeln, die darauf hindeuten. PYTHAGORAS kannte die Tripel, die man unter obiger Abbildung aus den Paaren $[a,b] = [n, n+1]$ erhält: Offensichtlich erfüllen die Paare $[n, n+1]$ die drei Bedingungen $n < n+1$, $(n, n+1) = 1$ und $n \not\equiv n+1 \mod 2$; ihnen wird zugeordnet:

$$x = 2ab = 2n^2 + 2n, \quad y = b^2 - a^2 = 2n + 1, \quad z = a^2 + b^2 = 2n^2 + 2n + 1$$

(es sind dies gerade die pythagoräischen Tripel $[x,y,z]$ mit $z = y + 1$).

Hier die Liste pythagoräischer Tripel, die man erhält, wenn man die Paare $[a,b]$ mit $a < b$, $(a,b) = 1$, und $a \not\equiv b \mod 2$ betrachtet, für die $a \leq 9$ gilt:

a	=	1	2	1	3	2	4	1	5	2	4	6	1	3	5	7	2	4	8
b	=	2	3	4	4	5	5	6	6	7	7	7	8	8	8	8	9	9	9
x	=	4	12	8	24	20	40	12	60	28	56	84	16	48	80	112	36	72	144
y	=	3	5	15	7	21	9	35	11	45	33	13	63	55	39	15	77	65	17
z	=	5	13	17	25	29	41	37	61	53	65	85	65	73	89	113	85	97	145

Beweis des Satzes. Wir beginnen mit einem Paar $[a,b]$ natürlicher Zahlen, mit $a < b$, $(a,b) = 1$, und $a \not\equiv b \mod 2$ und definieren x, y, z wie angegeben.

Wir zeigen $(x,y) = 1$. Angenommen, es gibt eine Primzahl p, die x und y teilt. Sei p ein Primteiler von $x = 2ab$, es ist $p = 2$ oder ein Teiler von a oder Wegen $a \not\equiv b$ mod 2 ist 2 kein Teiler von y, also ist p eine ungerade Primzahl. Wegen $p|x = 2ab$ ist p ein Teiler von a oder von b. Da p ein Teiler von x und y ist, ist p auch ein Teiler von z^2, also von z und demnach von $2b^2 = y + z$ und von $2a^2 = z - y$, also von a und von b (denn p ist ungerade). Dies widerspricht aber der Voraussetzung $(a,b) = 1$.

Es bleibt zu zeigen, dass die Zuordnung surjektiv ist — dies ist auch die wirklich wichtige Aussage: gesucht ist ja ein Verfahren, um alle primitiven pythagoräischen Tripel zu erhalten. Sei also $[x,y,z]$ primitives pythagoräisches Tripel, mit x gerade. Wegen $(x,y) = 1$ und $(y,z) = 1$ sind y, z beide ungerade, es gibt also $u \in \mathbb{N}$ und $v, w \in \mathbb{N}_0$ mit

$$x = 2u, \quad y = 2v + 1, \quad z = 2w + 1.$$

Setze $r = w - v$ und $s = w + v + 1$. Es ist $(r,s) = 1$, denn ist d ein Teiler von r und s, so auch von $r + s = 2w + 1 = z$ und von $s - r = 2v + 1 = y$, aber $(y,z) = 1$.

Es ist

$$x^2 = z^2 - y^2 = (z+y)(z-y) = (2w + 2v + 2)(2w - 2v) = 4rs.$$

Da r, s teilerfremd sind, sehen wir, dass beide Zahlen r, s Quadrate sind. Sei also $r = a^2, s = b^2$.

Es ist
$$a^2 = r = w - v \leq w < w + v + 1 < s = b^2,$$
also ist auch $a < b$. Wegen $(r, s) = 1$ ist $(a, b) = 1$. Modulo 2 erhalten wir $s = w + v + 1 \not\equiv w + v \equiv w - v = r \mod 2$, also ist auch $a \not\equiv b \mod 2$. Dies zeigt, dass $[a, b]$ alle geforderten Bedingungen erfüllt.

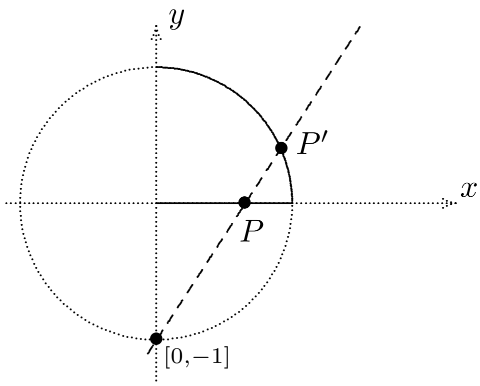
Zu zeigen bleibt, dass $[a, b]$ unter unserer Zuordnung auf $[x, y, z]$ abgebildet wird. Es ist $a^2 + b^2 = r + s = z$. Es ist $(2ab)^2 = 4a^2b^2 = 4rs = x^2$. Da $2ab$ und x positiv sind, folgt $2ab = x$. Schließlich ist $b^2 - a^2 = s - r = 2v + 1 = y$. Damit ist der Satz bewiesen.

Geometrische Interpretation: Wir überlegun uns zuerst, dass die primitiven pythagoräischen Tripel $[x, y, z]$ bijektiv den Punkten im ersten Quadranten auf dem Einheitskreis entsprechen, die rationale Koordinaten haben, unter der Abbildung
$$[x, y, z] \mapsto [\tfrac{x}{z}, \tfrac{y}{z}].$$

Schneide nun den Einheitskreis $\{[x, y] \mid x^2 + y^2 = 1\}$ mit der Geraden g, die durch die Punkte $[0, -1]$ und $P = [q, 0]$ geht, sie ist (für $q \neq 0$) durch die Gleichung
$$y = \tfrac{1}{q}x - 1$$
gegeben.

Die Gerade g schneidet den Einheitskreis im Punkt $(0, -1)$ und in einem weiteren Schnittpunkt:
$$P' = \left[\frac{2q}{1+q^2}, \frac{1-q^2}{1+q^2}\right].$$
Zum Beweis brauchen wir nur zu zeigen:
$$\frac{1}{q} \cdot \frac{2q}{1+q^2} - 1 = \frac{2}{1+q^2} - \frac{1+q^2}{1+q^2} = \frac{1-q^2}{1+q^2}.$$
Setzt man $q = \frac{a}{b}$, so erhält man
$$\frac{2\frac{a}{b}}{1+\frac{a^2}{b^2}} = \frac{2ab}{a^2+b^2}$$
$$\frac{1-\frac{a^2}{b^2}}{1+\frac{a^2}{b^2}} = \frac{b^2-a^2}{a^2+b^2}$$
also
$$P' = \left[\frac{2ab}{a^2+b^2}, \frac{b^2-a^2}{a^2+b^2}\right].$$

Zeichnung:



Die Zuordnung $P \mapsto P'$ heißt *stereographische Projektion*, sie bildet das Intervall $]0,1[$ auf den Kreisbogen des Einheitskreises im Inneren des ersten Quadranten ab. Dabei gehen rationale Zahlen auf Punkte in $\mathbb{R}^2$ mit rationalen Koeffizienten. Umgekehrt gilt auch: Ist das Bild P' von P unter der stereographischen Projektion ein Punkt mit rationalen Koordinaten, so ist P selbst eine rationale Zahl. Es ist also die Zuordnung

$$P = \frac{a}{b} \mapsto P' = \left[\frac{2ab}{a^2+b^2}, \frac{b^2-a^2}{a^2+b^2}\right] = \left[\frac{x}{z}, \frac{y}{z}\right]$$

mit

$$x = 2ab, \quad y = b^2 - a^2, \quad z = a^2 + b^2.$$