Nachtrag (zu §5): Pythagoräische Tripel

(1) $$X^2 + Y^2 = Z^2$$

Eine Lösung $(a,b,c) \in \mathbb{N}^3$ von (1) heißt pythagoräisches Tripel. Wenn $ggT(a,b,c) = 1$, heißt es primitiv. Es genügt primitive pythagoräische Tripel zu betrachten.

F2: Die Menge der primitiven pyth. Tripel (a,b,c), bei denen (o.E.) b gerade ist, wird geliefert durch

(2) $$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

wobei (u,v) alle Paare $\in \mathbb{N}^2$ mit $ggT(u,v) = 1$, uv gerade, $u > v$ durchläuft, und zwar bijektiv.

Bew. 1) Sei $a^2 + b^2 = c^2$ mit $ggT(a,b) = 1$. $\ulcorner a,b,c \in \mathbb{N} \lrcorner$

Dann: a, b, c paarw. teilerfremd (klar)

Annahme: a, b beide ungerade, $\Rightarrow a^2 \equiv b^2 \equiv 1 \bmod 4$, $\Rightarrow$ $c^2 \equiv 2 \bmod 4$ W!

Sei (o.E) b gerade ($\Rightarrow$ a ungerade, c auch).

Man hat $b^2 = c^2 - a^2 = (c+a)(c-a)$; da $b, c+a, c-a$ gerade, folgt

(3) $$\frac{b^2}{4} = \frac{c+a}{2}\,\frac{c-a}{2} \quad \text{mit } \frac{c+a}{2}, \frac{c-a}{2}, \frac{b^2}{4} \in \mathbb{N}$$

Die Summe der beiden Faktoren auf der r.S. ist c, ihre Differenz a; wegen $(a,c) = 1$ sind die Faktoren also teilerfremd. Auf der l.S. von (3) steht aber ein Quadrat in $\mathbb{N}$ $\ulcorner$nämlich $\left(\frac{b}{2}\right)^2 \lrcorner$, also müssen beide Faktoren auf der r.S. von (3) ebenfalls Quadrate sein, d.h. es ist

(4) $$\frac{c+a}{2} = u^2, \quad \frac{c-a}{2} = v^2 \quad \text{mit } u, v \in \mathbb{N}$$

Mit (3) ist dann $b^2 = 4u^2v^2$, also $b = 2uv$. Insgesamt bestehen also die Gleichungen (2), und es ist klar, daß u, v die Bedingungen $ggT(u,v) = 1$, $u > v$ und uv gerade erfüllen. Umgekehrt folgt aus diesen Bed'n

$$ggT(u^2 - v^2, 2uv) = 1,$$

und es besteht die Gleichung

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$$

Da u, v als natürliche Zahlen durch (4) eindeutig bestimmt sind, ist F2 bewiesen. $\square$

Beispiele für pythag. Tripel:

$3^2 + 4^2 = 5^2$ — $u = 2, v = 1$

$5^2 + 12^2 = 13^2$ — $u = 3, v = 2$

$15^2 + 8^2 = 17^2$ — $u = 4, v = 1$

$21^2 + 20^2 = 29^2$ — $u = 5, v = 2$

$35^2 + 12^2 = 37^2$ — $u = 6, v = 1$

F3 (Fermat, Euler): Die Gleichung

$$X^4 + Y^4 = Z^2$$

besitzt keine Lösung $(a,b,c) \in \mathbb{N}^3$. ⌜In $\mathbb{Z}^3$ hat sie gewisse triviale Lösungen: $(0, \pm b, b^2)$, $(\pm a, 0, a^2)$⌟

Folgerung: $X^4 + Y^4 = Z^4$ hat keine Lösung in $\mathbb{N}^3$.
(Fermatvermutung für den Exponenten 4)

Bew. Ann. (1) $a^4 + b^4 = c^2$ mit $a, b, c \in \mathbb{N}$

Wähle solches Gegenbeispiel mit minimalem c.

1) Beh. a, b, c paarw. teilerfremd.
Wäre p Primteiler von zweien, so aller drei. Es folgt
$p^4 \mid c^2$, $\Rightarrow p^2 \mid c$. $\left(\frac{a}{p}\right)^4 + \left(\frac{b}{p}\right)^4 = \left(\frac{c}{p^2}\right)^2$ W zur Minimalität von c.

2) Wegen $(a^2)^2 + (b^2)^2 = c^2$ ist (a^2, b^2, c) prim. pyth. Tripel.
O.E. b^2 gerade, d.h. b gerade, $\Rightarrow$ a ungerade. Nach F1:

(2) $a^2 = u^2 - v^2$, $b^2 = 2uv$, $c = u^2 + v^2$ mit
$u, v \in \mathbb{N}$, uv gerade, $ggT(u,v) = 1$, $u > v$.

$u^2 = a^2 + v^2$, $\Rightarrow$ v gerade (sonst $u^2 \equiv 2 \bmod 4$)

Wieder nach F1:

(3) $a = x^2 - y^2$, $v = 2xy$, $u = x^2 + y^2$ mit $x, y \in \mathbb{N}$, $ggT(x,y) = 1$.

(3)&(2) $\Rightarrow b^2 = 4(x^2+y^2)xy$, $\left(\frac{b}{2}\right)^2 = (x^2+y^2)xy$ $\xRightarrow[ggT(x,y)=1]{ggT(xy,\,x^2+y^2)=1}$

x^2+y^2, x, y Quadrate: $x = r^2$, $y = s^2$, $x^2+y^2 = t^2$, also

$$\boxed{r^4 + s^4 = t^2} \quad \text{mit } r, s, t \in \mathbb{N}.$$

$c = u^2 + v^2$

Aber $t \leq t^4 \overset{(3)}{=} u^2 \overset{(2)}{<} c$. W! zur Minimalität von c. □

Pythagoräische Quadrupel

Wir fragen nach allen Quadern mit ganzzahligen Kantenlängen $a, b, c > 0$, deren Raumdiagonale ebenfalls ganzzahlige Länge $d > 0$ hat. Wir suchen also nach allen Quadrupeln $(a,b,c,d) \in \mathbb{N}^4$ mit

$$(1) \qquad d^2 = a^2 + b^2 + c^2,$$

und zwar o.E. nur nach primitiven, d.h. solchen mit $ggT(a,b,c,d) = 1$, was gleichbedeutend mit $ggT(a,b,c) = 1$ ist. Von den Zahlen a, b, c kann höchstens eine ungerade sein, denn sonst ist $d^2 \equiv 2$ oder 3 mod 4. Wegen $ggT(a,b,c) = 1$ sind a, b, c nicht alle gerade. Wir setzen daher o.E. voraus, daß

a ungerade, aber b, c gerade

sind. Nach (1) ist d ungerade, also sind $a+d$ und $a-d$ gerade; daher schreibe (1) in der Form

$$(2) \qquad \frac{d+a}{2}\,\frac{d-a}{2} = \frac{b^2+c^2}{4} = (b/2)^2 + (c/2)^2$$

Es liegt so nahe, nach einer Zerlegung

$$(3) \qquad b/2 + i\,c/2 = (p+qi)(u+iv)$$

in $\mathbb{Z}[i]$ zu suchen, die bei Normbildung in (2) übergeht, die also

$$(4) \qquad N(p+qi) = \frac{d+a}{2} \quad \text{und} \quad N(u+iv) = \frac{d-a}{2}$$

erfüllt, d.h. $\frac{d+a}{2} = p^2+q^2$ und $\frac{d-a}{2} = u^2+v^2$, mithin

$$(5) \qquad d = p^2+q^2+u^2+v^2, \qquad a = p^2+q^2-u^2-v^2$$

Wegen $(p+qi)(u+iv) = (pu-qv) + (qu+pv)i$ ist andererseits (3) äquivalent mit

$$(6) \qquad b = 2(pu-qv), \qquad c = (2qu+pv)$$

Um zu einer Zerlegung (3), die (4) erfüllt, zu gelangen, gehen wir von der Primfaktorzerlegung von $b/2 + i\,c/2$ in $\mathbb{Z}[i]$ aus. Diese notieren wir in der Gestalt

$$(7) \qquad b/2 + i\,c/2 = \varepsilon\, n\, \pi_1^{\nu_1} \bar{\pi}_1^{\nu_1'} \cdots \pi_r^{\nu_r} \bar{\pi}_r^{\nu_r'}\; \pi_{r+1}^{\nu_{r+1}} \cdots \pi_s^{\nu_s},$$

wobei wir in n alle Primfaktoren zusammenfassen, die zu Primzahlen $q \equiv 3 \bmod 4$ gehören, während zu jedem der Primelemente π_i Primzahlen

$$p_i = N(\pi_i) = \pi_i \bar{\pi}_i$$

mit $p_i \equiv 1 \bmod 4$ oder $p_i = 2$ gehören; im letzteren Fall ist $\bar{\pi}_i \mathrel{\hat=} \pi_i \mathrel{\hat=} 1+i$, während für $p_i \neq 2$ stets $\bar{\pi}_i \mathrel{\not\hat=} \pi_i$ gilt. Die π_i mit $1 \le i \le r$ bezeichnen genau die Primteiler π_i mit $\bar{\pi}_i \mathrel{\not\hat=} \pi_i$, für die auch $\bar{\pi}_i$ in $b/2 + i\,c/2$ aufgeht. – Per Normbildung geht (7) über in

$$(8) \qquad (b/2)^2 + (c/2)^2 = n^2\, p_1^{\nu_1+\nu_1'} \cdots p_r^{\nu_r+\nu_r'}\; p_{r+1}^{\nu_{r+1}} \cdots p_s^{\nu_s}$$

<u>Lemma</u>: Jede Primzahl $q \equiv 3 \bmod 4$ geht in $d+a$ bzw. $d-a$ mit <u>gerader</u> Vielfachheit auf.

Beweis: Sei $q \equiv 3 \bmod 4$ ein Primteiler von $d+a$. Wir behaupten, daß q nicht in $d-a$ aufgeht. Angenommen, das sei doch der Fall. Dann ist q auch Teiler von $(d+a)-(d-a) = 2a$, also von a. Aber b ist prim zu q, denn sonst würde q nach (2) auch c teilen, im Widerspruch zu $ggT(a,b,c) = 1$. Ebenso ist c prim zu q.

---

*) natürlich ist auch $r=0$ möglich.

Doch q muß wegen (2) in b^2+c^2 aufgehen, mithin gilt

$$b^2+c^2 \equiv 0 \bmod q \quad \text{mit} \quad b, c \not\equiv 0 \bmod q$$

Dann wäre aber -1 ein quadratischer Rest mod q, im Widerspruch zu $q \equiv 3 \bmod 4$. – Es folgt nun
$w_q(d+a) = w_q((d+a)(d-a)) = w_q(b^2+c^2) =$ gerade, vgl. (8).
Analog für $d-a$. □
Nach dem Lemma haben die Faktoren $\frac{d+a}{2}$ und $\frac{d-a}{2}$ in (2) mit Blick auf (8) die Darstellungen

$$\frac{d+a}{2} = n_1^2 p_1^{\lambda_1} \cdots p_s^{\lambda_s}, \quad \frac{d-a}{2} = n_2^2 p_1^{\mu_1} \cdots p_s^{\mu_s} \text{ mit}$$

(9) $$n_1, n_2 \in \mathbb{N};\ \lambda_i, \mu_i \geq 0 \text{ und } \lambda_i + \mu_i = \nu_i + \nu_i' \text{ für } 1 \leq i \leq r,$$

$$\lambda_i + \mu_i = \nu_i \text{ für } r+1 \leq i \leq s;\ n_1^2 n_2^2 = n^2, \text{ d.h. } n_1 n_2 = n.$$

Ausschlaggebend ist nun die folgende Feststellung: Für $1 \leq i \leq r$ geht p_i nicht in beiden der Zahlen $\frac{d+a}{2}, \frac{d-a}{2}$ auf. Denn sonst wäre p_i ein Teiler von a und d; andererseits geht $p_i = \pi_i \bar{\pi}_i$ nach (7) in b und c auf, im Widerspruch zu $ggT(a,b,c)=1$. Unter den p_i mit $1 \leq i \leq r$ bezeichnen nun o.E. $p_1, \dots, p_m$ genau die p_i, die in $\frac{d+a}{2}$ aufgehen. Dann gilt in (9) genauer:

$$\frac{d+a}{2} = n_1^2 p_1^{\nu_1+\nu_1'} \cdots p_m^{\nu_m+\nu_m'} \, p_{r+1}^{\lambda_{r+1}} \cdots p_s^{\lambda_s}$$

(10) $$\frac{d-a}{2} = n_2^2 p_{m+1}^{\nu_{m+1}+\nu_{m+1}'} \cdots p_r^{\nu_r+\nu_r'} \, p_{r+1}^{\mu_{r+1}} \cdots p_s^{\mu_s}$$

$$\text{mit } n_1 n_2 = n;\ \lambda_i, \mu_i \geq 0 \text{ und } \lambda_i + \mu_i = \nu_i \text{ für } r+1 \leq i \leq s$$

Setzen wir nun

$$p + qi := \varepsilon n_1 \pi_1^{\nu_1} \bar{\pi}_1^{\nu_1'} \cdots \pi_m^{\nu_m} \bar{\pi}_m^{\nu_m'} \, \pi_{r+1}^{\lambda_{r+1}} \cdots \pi_s^{\lambda_s}$$

$$u + vi := n_2 \pi_{m+1}^{\nu_{m+1}} \bar{\pi}_{m+1}^{\nu_{m+1}'} \cdots \pi_r^{\nu_r} \bar{\pi}_r^{\nu_r'} \, \pi_{r+1}^{\mu_{r+1}} \cdots \pi_s^{\mu_s}$$

(mit derselben Einheit ε wie in (7)), so sind in der Tat (3) wie (4) erfällt, vgl. (7). Im übrigen erhält man auch folgende <u>Eindeutigkeitsaussage:</u> $p+qi$, $u+vi$ in (3) lassen sich nur durch $\varepsilon_1(p+qi)$, $\varepsilon_2(u+iv)$ mit Einheiten $\varepsilon_1, \varepsilon_2$ ersetzen, die $\varepsilon_1\varepsilon_2 = 1$ erfüllen. Mit einem Parameter-Quadrupel

(11) $\qquad (p, q, u, v)$

sind so auch $(-p, -q, -u, -v)$, $(-q, p, v, -u)$, $(q, -p, -v, u)$ zulässige Quadrupel von Parametern, aber keine weiteren.

<u>Bem. 1</u> Für ein Parameter-Quadrupel zu a, b, c, d muß offenbar gelten:

(12) $\begin{cases} p^2+q^2 > u^2+v^2 > 0, \quad pu - qv > 0, \quad qu + pv > 0 \\ \text{Von den Parametern } p, q, u, v \text{ ist genau einer} \\ \text{ungerade oder genau einer gerade; } ggT(p,q,u,v) = 1. \end{cases}$

<u>Bem. 2</u> Für jedes Quadrupel $(p, q, u, v) \in \mathbb{Z}^4$ mit (12) liefern die Formeln (5) und (6) ein Quadrupel $(a, b, c, d) \in \mathbb{N}^4$ mit $a^2+b^2+c^2 = d^2$. (Allerdings ist (a, b, c, d) nicht notwendig primitiv; vgl. w.u.)

<u>Bew.</u> Wegen (12) sind zunächst a, b, c, d wirklich > 0. Doch (6) besagt dasselbe wie (3). Mit (5) folgt aus (3) aber die Relation (2), also (1).

<u>Bem. 3</u> Für $(4, 7, 2, -1)$ und $(8, 1, 2, 1)$ liefern (5) und (6) das gleiche Quadrupel $(a, b, c, d) = (60, 30, 20, 70)$. Aber dieses ist nicht primitiv, und man hat keinen Widerspruch zur obigen Eindeutigkeitsaussage. Außerdem verletzen

die betrachteten Quadrupel (p,q,u,v) die Paritätsbedingung in (12).

<u>Bem. 4</u> Die Quadrupel $(1,13,2,-1)$ und $(11,7,2,1)$ erfüllen jeweils alle Bedingungen in (12). Sie liefern das gleiche Quader-Quadrupel $(a,b,c,d) = (165, 30, 50, 175)$, aber dieses ist nicht primitiv. Kann es auch nicht sein, denn sonst widerspräche das ~~les~~ obigen Eindeutigkeitsaussage.

<u>Frage:</u> Kann man (12) so ergänzen, daß (p,q,u,v) eine <u>primitive</u> Lösung (a,b,c,d) liefert?