# §5: Diophantische Gleichungen

Diophantos von Alexandria (150 v. Chr., 350 n. Chr?)
griechischer Mathematiker — lebte in Alexandria (Ägypten)

**Def:** Eine diophantische Gleichung ist eine algebraische Gleichung (in mehreren Variablen), die in ganzen oder rationalen Zahlen gelöst werden soll. Eine algebraische Gleichung ist dabei eine Gleichung der Form $F(X_1, \dots, X_n) = 0$, wo $F \in \mathbb{Z}[X_1, \dots, X_n]$ ein Polynom mit ganzzahligen Koeffizienten ist.

**Beispiele:**
i) $2x + 4y = 5$ (Lös. in $\mathbb{Z}$)
ii) $y^2 = x^3 + 1$ (Lös. in $\mathbb{Q}$)
iii) $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 10^{10} + 1$ (Lös. in $\mathbb{Z}$)
iv) $x^n + y^n - z^n = 0$ $(n \in \mathbb{N}^*)$. (Lös. in $\mathbb{Z}^*$). Fermatsche Gleich.

## A) Diophantische Gleichungen mit nur einer Variablen

Das Polynom $F$ hat die Form $F(X) = a_n X^n + \dots + a_1 X + a_0$ $\left(a_i \in \mathbb{Z}\ \forall i \leq n,\ a_n \neq 0\right)$
Gesucht: $x \in \mathbb{Q}$ mit $F(x) = 0$.

**Satz 5.1:** Sei $\alpha \in \mathbb{Q}$ mit $F(\alpha) = 0$. Seien $r, s \in \mathbb{Z}$ mit $s \neq 0 \wedge \alpha = \frac{r}{s} \wedge \operatorname{ggT}(r, s) = 1$. Dann gelten $s \mid a_n$ und $r \mid a_0$.

Beweis: $F\left(\frac{r}{s}\right)=0 \Rightarrow a_n\frac{r^n}{s^n}+a_{n-1}\frac{r^{n-1}}{s^{n-1}}+\dots+a_1\frac{r}{s}+a_0=0 \Rightarrow$

$a_nr^n+a_{n-1}r^{n-1}s+\dots+a_1rs^{n-1}+a_0s^n=0$. Daraus folgt:

$s(a_{n-1}r^{n-1}+\dots+a_1rs^{n-2}+a_0s^{n-1})=-a_nr^n \Rightarrow s\mid a_nr^n$. $ggT(s,r)=1 \overset{AZF}{\Rightarrow}$

$s\mid a_n$. Analog zeigt man: $r\mid a_0s^n$ und $r\mid a_0$. $\square$

## B) Lineare diophantische Gleichungen

Das Polynom $F$ hat die Form $F(X_1,\dots,X_n)=a_1X_1+\dots+a_nX_n-d$ mit $a_1,\dots,a_n,d\in\mathbb{Z}$ und $n\geq 2$.

Gesucht: Die ganzzahligen Lösungen von $F(X_1,\dots,X_n)=0$, also

$$L=\{(x_1,\dots,x_n)\in\mathbb{Z}^n \mid a_1x_1+\dots+a_nx_n=d\}.$$

Die Lösungsmenge $L$ kann ganz genau beschrieben (und gerechnet) werden:

**Satz 5.2:**

1) $n=2$: Wir betrachten die Gleichung $ax+by\overset{(*)}{=}d$ mit $a,b,d\in\mathbb{Z}$ und $(a,b)\neq(0,0)$.

i) $(*)$ hat eine ganzzahlige Lösung $\Leftrightarrow ggT(a,b)\mid d$.

ii) Ang. $ggT(a,b)\mid d$. Sei $(x_0,y_0)\in\mathbb{Z}^2$ eine Lösung von $(*)$.

Dann gilt $L=\left\{(x_0,y_0)+t\left(\frac{-b}{ggT(a,b)},\frac{a}{ggT(a,b)}\right) \,\middle|\, t\in\mathbb{Z}\right\}$.

2) $\underline{n=3}$: Wir betrachten die Gleichung $ax+by+cz \overset{(*)}{=} d$ (3)
mit $a,b,c,d \in \mathbb{Z}$ und $(a,b,c) \neq (0,0,0)$.

i) $(*)$ hat eine ganzzahlige Lösung $\Leftrightarrow$ $ggT(a,b,c) \mid d$.

ii) Ang. $ggT(a,b,c) \mid d$. Dann gibt es $v_0, v_1, v_2 \in \mathbb{Z}^3$ sodass

$$L = \{v_0 + t_1 v_1 + t_2 v_2 \mid t_1, t_2 \in \mathbb{Z}\}.$$

3) $\underline{n \in \mathbb{N}, n \geq 2}$: Wir betrachten die Gleichung $a_1x_1 + \ldots + a_nx_n \overset{(*)}{=} d$
mit $a_1, \ldots, a_n, d \in \mathbb{Z}$ und $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$.

i) $(*)$ hat eine ganzzahlige Lösung $\Leftrightarrow$ $ggT(a_1, \ldots, a_n) \mid d$.

ii) Ang. $ggT(a_1, \ldots, a_n) \mid d$. Dann gibt es $v_0, v_1, \ldots, v_{n-1} \in \mathbb{Z}^n$ sodass

$$L = \{v_0 + t_1 v_1 + \ldots + t_{n-1} v_{n-1} \mid t_1, \ldots, t_{n-1} \in \mathbb{Z}\}.$$

<u>Beweis:</u>

<u>Zu 1):</u> S. Skript AZ I.

<u>Zu 2):</u>

i) "$\Rightarrow$" Sei $(x,y,z) \in \mathbb{Z}^3$ eine Lösung von $ax+by+cz=d$.

$ggT(a,b,c) \mid a,b,c \Rightarrow ggT(a,b,c) \mid ax+by+cz \Rightarrow ggT(a,b,c) \mid d$.

"$\Leftarrow$" Ang. $ggT(a,b,c) \mid d$.

$ggT(a,b,c) \overset{AZ.I}{=} ggT(ggT(a,b), c)$. AZ.I $\Rightarrow \exists \alpha, \beta \in \mathbb{Z}$ mit

$ggT(a,b) = \alpha a + \beta b$. Also $ggT(a,b,c) = ggT(\alpha a + \beta b, c)$.

A2.I $\Rightarrow \exists \gamma, \delta \in \mathbb{Z}$ mit $ggT(\alpha a+\beta b, c) = \gamma(\alpha a+\beta b)+\delta c =$
$(\gamma\alpha)a+(\gamma\beta)b+\delta c$; also $ggT(a,b,c) = (\gamma\alpha)a+(\gamma\beta)b+\delta c$.

$ggT(a,b,c) \mid d \Rightarrow \exists m \in \mathbb{Z}$ mit $m \cdot ggT(a,b,c) = d$. Daraus folgt
$m(\gamma\alpha a+\gamma\beta b+\delta c) = d$ und $\underbrace{(m\gamma\alpha)}_{\in\mathbb{Z}}a+\underbrace{(m\gamma\beta)}_{\in\mathbb{Z}}b+\underbrace{(m\delta)}_{\in\mathbb{Z}}c = d$.

$(m\gamma\alpha, m\gamma\beta, m\gamma) \in \mathbb{Z}^3$ ist eine Lösung von $ax+by+cz=d$.
Damit ist i) bewiesen.

ii) Wir rechnen zunächst ein paar Beispiele.

a) Sei $2x-y+3z=7$.

Man sieht: $x, z$ können in $\mathbb{Z}$ frei gewählt werden und dann haben wir $y = 2x+3z-7$. Also

$$L = \{(x, 2x+3z-7, z) \mid x,z \in \mathbb{Z}\} = \{(0,-7,0)+x(1,2,0)+z(0,3,1) \mid x,z \in \mathbb{Z}\}$$
$$= \{\underbrace{(0,-7,0)}_{=:v_0} + t_1\underbrace{(1,2,0)}_{=:v_1} + t_2\underbrace{(0,3,1)}_{=:v_2} \mid t_1, t_2 \in \mathbb{Z}\}.$$

b) Sei $22x+33y-7z=4$. $\quad [ggT(22,33,-7) = ggT(11,-7) = 1 \mid 4]$

Die Koeffizienten von $x, y, z$ sind $22; 33; -7$. Leider ist da kein $\pm 1$. Im Großen und Ganzen werden wir versuchen die Gleichung $22x+33y-7z=4$ umzuformen, damit eine neue Gleichung mit "kleineren Koeffizienten" entsteht. Genauer:

Sei $(x,y,z) \in \mathbb{Z}^3$ eine Lösung von $22x+33y-7z=4$.

- Die kleinste positive Zahl unter $|22|, |33|, |-7|$ ist $7 = |-7|$.

- Wir drücken $z$ in $x, y$ aus: $z = \frac{22x+33y-4}{7}$
- Wir führen die Divisionen $22:7$ und $33:7$ durch:

  $22 = 3\cdot 7+1$ ; $33 = 4\cdot 7+5$ oder (besser) $33 = 5\cdot 7+(-2)$.
- Daraus folgt: $z = \frac{(3\cdot 7+1)x+(5\cdot 7-2)y-4}{7} = \frac{7(3x+5y)+x-2y-4}{7}$

$= 3x+5y+\frac{x-2y-4}{7} \Rightarrow z = 3x+5y+w$, wo $w := \frac{x-2y-4}{7}$.

$(x,y,z)\in\mathbb{Z}^3 \Rightarrow w\in\mathbb{Z}$. $\left[w = \frac{x-2y-4}{7} \Leftrightarrow x-2y-7w = 4\right]$

Wir haben gezeigt:

- Ist $(x,y,z)\in\mathbb{Z}^3$ eine Lösung von $22x+33y-7z=4$, dann gibt es ein $w\in\mathbb{Z}$ sodass

  $(x,y,z,w)$ Lösung von $\begin{cases} z = 3x+5y+w \\ 1\cdot x-2y-7w = 4 \end{cases}$ $(+)$ ist

  gut
- Umgekehrt, wenn $(x,y,z,w)\in\mathbb{Z}^4$ das System $(+)$ erfüllt, dann ist $(x,y,z)\in\mathbb{Z}^3$ eine Lösung von $22x+33y-7z=4$. [Einfach $w$ in $(+)$ eliminieren]

Daraus folgt: $(x,y,z)\in\mathbb{Z}^3$ ist Lösung von $22x+33y-7z=4 \Leftrightarrow$ $\exists w\in\mathbb{Z}$ sodass $(x,y,z,w)$ Lösung von $(+)$ ist.

In $(+)$ können $y, w\in\mathbb{Z}$ frei gewählt werden, und dann sind $x, z$ eindeutig bestimmt:

$x = 2y+7w+4$ ; $z = 3(2y+7w+4)+5y+w = 12+11y+22w$. Also

$$L = \{(2y+7w+4;\ y;\ 12+11y+22w) \mid y, w \in \mathbb{Z}\}$$
$$= \{(4,0,12) + y(2,1,11) + w(7,0,22) \mid y, w \in \mathbb{Z}\}$$
$$= \{\underbrace{(4,0,12)}_{\overset{\shortparallel}{v_0}} + t_1\underbrace{(2,1,11)}_{\overset{\shortparallel}{v_1}} + t_2\underbrace{(7,0,22)}_{\overset{\shortparallel}{v_2}} \mid t_1, t_2 \in \mathbb{Z}\}.$$

c) Sei $35x+55y+77z=3$ $\quad [ggT(35,55,77) = ggT(5,77) = 1 \mid 3]$

Wir gehen wie in b) vor.

Sei $(x,y,z) \in \mathbb{Z}^3$ eine Lösung von $35x+55y+77z=3$.

$x = \frac{3-55y-77z}{35}$. $\quad 55 = 2\cdot 35 - 15$ ; $77 = 2\cdot 35 + 7$.

$$x = \frac{3-(2\cdot 35-15)y-(2\cdot 35+7)z}{35} = \frac{35(-2y-2z)+3+15y-7z}{35} =$$

$-2y-2z+w$, wo $w := \frac{3+15y-7z}{35} \in \mathbb{Z}$. Wie in b) erhalten wir:

$(x,y,z) \in \mathbb{Z}^3$ ist Lösung von $35x+55y+77z=3 \iff$

$\exists w \in \mathbb{Z}$ sodass $(x,y,z,w)$ Lösung von $\begin{cases} x = -2y-2z+w \\ 15y-7z-35w = -3 \end{cases}$ $(+)$ ist.

Jetzt muss die Gleichung $15y-7z-35w=-3$ gelöst werden.

Sei $(y,z,w) \in \mathbb{Z}^3$ eine Lösung von $15y-7z-35w=-3$.

$-7z = -3-15y+35w \Rightarrow z = \frac{3+15y-35w}{7}$.

$15 = 2\cdot 7 + 1$ gut ; $-35 = (-5)\cdot 7$.

$$z = \frac{3+(2\cdot 7+1)y-5\cdot 7w}{7} = \frac{7(2y-5w)+3+y}{7} = 2y-5w+u, \text{ wo}$$

$u := \frac{y+3}{7} \in \mathbb{Z}$. Daraus folgt:

$(y,z,w) \in \mathbb{Z}^3$ ist Lösung von $15y - 7z - 35w = -3 \iff$

$\exists u \in \mathbb{Z}$ sodass $(y,z,w,u)$ Lösung von $\begin{cases} z = 2y - 5w + u \\ 1y - 7u = -3 \end{cases}$ $(++)$ ist.

gut

Jetzt können wir L bestimmen.

In $(++)$ können $u, w \in \mathbb{Z}$ frei gewählt werden und dann haben wir $y = 7u - 3$ und $z = 2(7u-3) - 5w + u = -6 + 15u - 5w$.

$(+) \Rightarrow x = -2y - 2z + w = -2(7u-3) - 2(-6+15u-5w) + w = 18 - 44u + 11w$.

$$L = \{(18-44u+11w;\ -3+7u;\ -6+15u-5w) \mid u,w \in \mathbb{Z}\}$$
$$= \{(18,-3,-6) + u(-44,7,15) + w(11,0,-5) \mid u,w \in \mathbb{Z}\}$$
$$= \{\underbrace{(18,-3,-6)}_{v_0} + t_1\underbrace{(-44,7,15)}_{v_1} + t_2\underbrace{(11,0,-5)}_{v_2} \mid t_1,t_2 \in \mathbb{Z}\}.$$

<u>Beweis von 2) ii)</u>

Wir betrachten alle Gleichungen der Form $ax+by+cz=d$ mit $a,b,c,d \in \mathbb{Z}$, $(a,b,c) \neq (0,0,0)$ und $ggT(a,b,c) \mid d$.

Beweis durch Induktion über $n := \min(\{|a|,|b|,|c|\} \setminus \{0\})$.

Sei $n \in \mathbb{N}^*$ gegeben und $ax+by+cz=d$ eine Gleichung wie oben mit $n = \min(\{|a|,|b|,|c|\} \setminus \{0\})$.

I.V: Die Aussage 2) ii) gilt für alle Gleichungen $\alpha x + \beta y + \gamma z = \delta$ wie oben mit $K := \min(\{|\alpha|,|\beta|,|\gamma|\} \setminus \{0\}) < n$.

Z.z: Die Aussage 2)ii) gilt für die Gleichung $ax+by+cz=d$. (8)

OBdA, $ggT(a,b,c)=1$ und $n=|a|$.

Fall 1: $n=1$. [Also, $a=\pm 1$]

Sei $(x,y,z)\in\mathbb{Z}^3$. $ax+by+cz=d \iff \underbrace{a^2}_{=1}x+aby+acz=ad \iff$

$x=ad-aby-acz$. Daraus folgt

$$L=\{(ad-aby-acz,\ y,\ z)\mid y,z\in\mathbb{Z}\}$$

$$=\{(ad,0,0)+y(-ab,1,0)+z(-ac,0,1)\mid y,z\in\mathbb{Z}\}$$

$$=\{\underbrace{(ad,0,0)}_{=v_0}+t_1\underbrace{(-ab,1,0)}_{=v_1}+t_2\underbrace{(-ac,0,1)}_{=v_2}\mid t_1,t_2\in\mathbb{Z}\}.$$

Fall 2: $n\geq 2$.

Wir teilen b und c durch a: Seien $q_1,r_1,q_2,r_2\in\mathbb{Z}$ mit $b=q_1a+r_1$, $c=q_2a+r_2$ und $0\leq|r_1|,|r_2|<|a|=n$.

Sei $(x,y,z)\in\mathbb{Z}^3$ eine Lösung von $ax+by+cz=d$.

$$x=\frac{d-by-cz}{a}=\frac{d-(q_1a+r_1)y-(q_2a+r_2)z}{a}=\frac{a(-q_1y-q_2z)+d-r_1y-r_2z}{a}$$

$$=-q_1y-q_2z+w,\ \text{wo } w:=\frac{d-r_1y-r_2z}{a}\in\mathbb{Z}.$$

$$\left[w=\frac{d-r_1y-r_2z}{a}\iff r_1y+r_2z+aw=d\right].$$

Wir haben gezeigt:

- Wenn $(x,y,z)\in\mathbb{Z}^3$ Lösung von $ax+by+cz=d$ ist, dann gibt es ein $w\in\mathbb{Z}$ sodass

$$(x,y,z,w) \text{ Lösung von } \begin{cases} x=-q_1y-q_2z+w \\ r_1y+r_2z+aw=d \end{cases} (+) \text{ ist.}$$

- Umgekehrt, sei $(x,y,z,w) \in \mathbb{Z}^4$ eine Lösung von (+):

Dann haben wir $d = r_1 y + r_2 z + aw = r_1 y + r_2 z + a(x + q_1 y + q_2 z) =$
$ax + (q_1 a + r_1) y + (q_2 a + r_2) z = ax + by + cz$, also $ax + by + cz = d$ und
$(x,y,z)$ ist Lösung von $ax + by + cz = d$.

Daraus folgt:

$(x,y,z) \in \mathbb{Z}^3$ ist Lösung von $ax + by + cz = d \iff$

$\exists w \in \mathbb{Z}$ sodass $(x,y,z,w)$ Lösung von $\begin{cases} x = -q_1 y - q_2 z + w \\ r_1 y + r_2 z + aw = d \end{cases}$ (+) ist.

Wir betrachten die Gleichung $r_1 y + r_2 z + aw = d$.

Sei $L' := \{(y,z,w) \in \mathbb{Z}^3 \mid r_1 y + r_2 z + aw = d\}$.

Sei $K := \min(\{|r_1|, |r_2|, \underbrace{|a|}_{\neq 0}\} \setminus \{0\})$. Wir zeigen dass $K < n$.

Laut Def. haben wir $|r_1| < n$ und $|r_2| < n$. Da $ggT(a,b,c) = 1 \wedge |a| = n \geq 2$
folgt $(|r_1| > 0$ oder $|r_2| > 0)$. Also $K < n$.

Nach I.V. gibt es $\tilde{v}_0, \tilde{v}_1, \tilde{v}_2 \in \mathbb{Z}^3$ sodass

$$L' = \{ \underbrace{\tilde{v}_0}_{(\tilde{v}_{00}, \tilde{v}_{01}, \tilde{v}_{02})} + t_1 \underbrace{\tilde{v}_1}_{(\tilde{v}_{10}, \tilde{v}_{11}, \tilde{v}_{12})} + t_2 \underbrace{\tilde{v}_2}_{(\tilde{v}_{20}, \tilde{v}_{21}, \tilde{v}_{22})} \mid t_1, t_2 \in \mathbb{Z} \}.$$

Wir drücken $y, z, w, x$ in $t_1, t_2$ aus:

$y = \tilde{v}_{00} + t_1 \tilde{v}_{10} + t_2 \tilde{v}_{20}$; $z = \tilde{v}_{01} + t_1 \tilde{v}_{11} + t_2 \tilde{v}_{21}$; $w = \tilde{v}_{02} + t_1 \tilde{v}_{12} + t_2 \tilde{v}_{22}$.

Aus (+) folgt $x = -q_1 y - q_2 z + w =$

$-q_1(\tilde{v}_{00} + t_1 \tilde{v}_{10} + t_2 \tilde{v}_{20}) - q_2(\tilde{v}_{01} + t_1 \tilde{v}_{11} + t_2 \tilde{v}_{21}) + \tilde{v}_{02} + t_1 \tilde{v}_{12} + t_2 \tilde{v}_{22} =$

$-q_1\tilde{v}_{00} - q_2\tilde{v}_{01} + \tilde{v}_{02} + t_1(-q_1\tilde{v}_{10} - q_2\tilde{v}_{11} + \tilde{v}_{12}) + t_2(-q_1\tilde{v}_{20} - q_2\tilde{v}_{21} + \tilde{v}_{22})$. Also

$$(x,y,z) = (-q_1\tilde{v}_{00} - q_2\tilde{v}_{01} + \tilde{v}_{02} + t_1(-q_1\tilde{v}_{10} - q_2\tilde{v}_{11} + \tilde{v}_{12}) + t_2(-q_1\tilde{v}_{20} - q_2\tilde{v}_{21} + \tilde{v}_{22}); \tilde{v}_{00} + t_1\tilde{v}_{10} + t_2\tilde{v}_{20}; \tilde{v}_{01} + t_1\tilde{v}_{11} + t_2\tilde{v}_{21})$$

$$= \underbrace{(-q_1\tilde{v}_{00} - q_2\tilde{v}_{01} + \tilde{v}_{02}; \tilde{v}_{00}; \tilde{v}_{01})}_{=:v_0} + t_1\underbrace{(-q_1\tilde{v}_{10} - q_2\tilde{v}_{11} + \tilde{v}_{12}; \tilde{v}_{10}; \tilde{v}_{11})}_{=:v_1} + t_2\underbrace{(-q_1\tilde{v}_{20} - q_2\tilde{v}_{21} + \tilde{v}_{22}; \tilde{v}_{20}; \tilde{v}_{21})}_{=:v_2}$$

Also $L = \{v_0 + t_1v_1 + t_2v_2 \mid t_1, t_2 \in \mathbb{Z}\}$ hat die gewünschte Form.

Damit ist die Aussage 2)ii) bewiesen.

<u>Bem</u>: In $L = \{v_0 + t_1v_1 + t_2v_2 \mid t_1, t_2 \in \mathbb{Z}\}$ sind die Vektoren $v_0, v_1, v_2 \in \mathbb{Z}^3$ bei weitem nicht eindeutig bestimmt. Aber es gilt immer:

- $v_0$ ist eine partikuläre Lösung von $ax + by + cz = d$.
- $v_1, v_2$ sind Lösungen von $ax + by + cz = 0$.
- $v_1, v_2$ sind über $\mathbb{Q}$ linear unabhängig.

<u>Bspl</u>: Für die Gleichung $22x + 33y - 7z = 4$ (s. S. 4-5-6) haben wir $L = \{\underbrace{(4,0,12)}_{v_0} + t_1\underbrace{(2,1,11)}_{v_1} + t_2\underbrace{(7,0,22)}_{v_2} \mid t_1, t_2 \in \mathbb{Z}\}$ gerechnet:

$v_0 = (4,0,12)$ ist Lösung von $22x + 33y - 7z = 4$. $[22\cdot 4 - 7\cdot 12 = 88 - 84 = 4]$

$v_1 = (2,1,11)$ und $v_2 = (7,0,22)$ sind Lösungen von $22x + 33y - 7z = 0$.

$v_1, v_2$ sind linear unabh. über $\mathbb{Q}$.

<u>Zu 3)</u>: Der Beweis verläuft analog wie für 2).

Damit ist Satz 5.2 bewiesen. $\square$

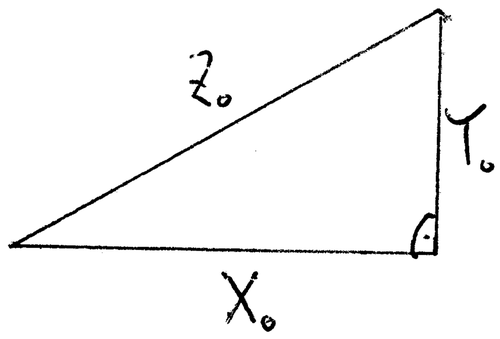
## c) Die Gleichung $X^2+Y^2=Z^2$

Die Gleichung $X^2+Y^2 \overset{(1)}{=} Z^2$ hat offensichtlich ganzzahlige Lösungen: zum Beispiel $(3,4,5)$ und $(5,-12,13)$.

Bem: Ist $(X_0, Y_0, Z_0)$ eine ganzzahlige Lösung von (1), dann auch $(tX_0, tY_0, tZ_0)$ $\forall t \in \mathbb{Z}$. Z.B: $(9,12,15)$ ist auch Lösung von (1).

Def: i) Ein pythagoreisches Tripel ist eine Lösung $(X,Y,Z) \in \mathbb{Z}^3$ von (1) mit $Z \neq 0$.

ii) Ein pythagoreisches Tripel $(X_0, Y_0, Z_0)$ heisst primitiv wenn $ggT(X_0, Y_0, Z_0) = 1$.




Bem: Ist $(X_0, Y_0, Z_0)$ ein primitives pythagoreisches Tripel, dann gelten $ggT(X_0, Y_0) = ggT(X_0, Z_0) = ggT(Y_0, Z_0) = 1$.

Ziel: Alle primitiven pythagoreischen Tripel zu finden.

Lemma: Sei $(X,Y,Z)$ ein primitives pythagoreisches Tripel. Dann gilt $2 \mid X,\ 2 \nmid Y,\ 2 \nmid Z$ oder $2 \nmid X,\ 2 \mid Y,\ 2 \nmid Z$.

Beweis: • Ang. $2 \mid X \wedge 2 \mid Y$. Dann ist $ggT(X,Y) \geq 2 > 1$ ↯

• Ang. $2 \nmid X \wedge 2 \nmid Y$. $(X \equiv 1 \bmod 2 \wedge Y \equiv 1 \bmod 2) \Rightarrow (X^2 \equiv 1 \bmod 4 \wedge Y^2 \equiv 1 \bmod 4)$.

Also $Z^2 = X^2 + Y^2 \equiv 1+1 = 2 \bmod 4$, ↯

Also haben $X$ und $Y$ verschiedene Paritäten. Es folgt dass $X^2+Y^2$ ungerade ist. $Z^2 = X^2+Y^2 \Rightarrow 2 \nmid Z^2 \Rightarrow 2 \nmid Z$.

$\square$

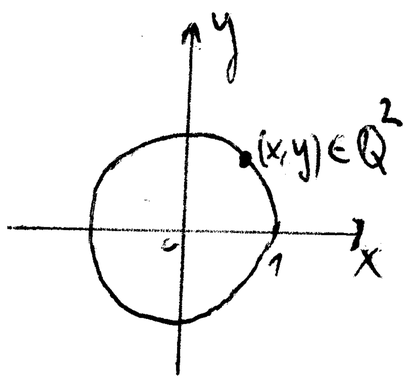
**Satz 5.3:** Die primitiven pythagoreischen Tripel mit $Z > 0$ haben die Form $(X,Y,Z) = (2ST, S^2-T^2, S^2+T^2)$ oder
$(X,Y,Z) = (S^2-T^2, 2ST, S^2+T^2)$, mit
$S,T \in \mathbb{Z}$ teilerfremd und von verschiedenen Paritäten.

**Beweis:** i) Sei $(X,Y,Z) = (2ST, S^2-T^2, S^2+T^2)$ mit $S,T \in \mathbb{Z}$ teilerfremd und von verschiedenen Paritäten.

- $(2ST)^2 + (S^2-T^2)^2 = 4S^2T^2 + S^4 - 2S^2T^2 + T^4 = S^4 + 2S^2T^2 + T^4 = (S^2+T^2)^2$.
- Sei $p$ prim mit $p \mid 2ST$, $p \mid S^2-T^2$, $p \mid S^2+T^2$.
  $p \neq 2$ denn $S^2+T^2$ ist ungerade. $p \mid 2ST \overset{\text{OBdA}}{\Longrightarrow} p \mid S$. $p \mid S \Rightarrow p \mid S^2 \Rightarrow$ $p \mid T^2$ (denn $p \mid S^2+T^2$). Daraus folgt $p \mid T$ und $ggT(S,T) \geq p > 1$ ↯.
  Also $ggT(X,Y,Z) = 1$ und $(X,Y,Z)$ ist ein primitives pythagoreisches Tripel.
  Analog für $(X,Y,Z) = (S^2-T^2, 2ST, S^2+T^2)$ mit $S,T \in \mathbb{Z}$ teilerfremd und von verschiedenen Paritäten.

ii) Sei $(X,Y,Z)$ ein primitives pythagoreisches Tripel mit $Z > 0$.
Seien $x := \frac{X}{Z}$ und $y := \frac{Y}{Z}$. $x,y \in \mathbb{Q}$ und $x^2+y^2 = \frac{X^2}{Z^2} + \frac{Y^2}{Z^2} = 1$.
Daher eine Abbildung

$$\left\{\begin{matrix}\text{primitive pythagoreische Tripel} \\ (X,Y,Z) \text{ mit } Z>0\end{matrix}\right\} \xrightarrow{\varphi} \left\{\begin{matrix}\text{rationale Lösungen} \\ \text{von } x^2+y^2=1\end{matrix}\right\}.$$




$$(X,Y,Z) \longmapsto \left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

Wir zeigen, dass $f$ bijektiv ist.

• Injektivität: Ang. $f(X,Y,Z) = f(X',Y',Z')$. Dann gilt $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{X'}{Z'}, \frac{Y'}{Z'}\right)$, also $\frac{X}{Z} = \frac{X'}{Z'}$ und $\frac{Y}{Z} = \frac{Y'}{Z'}$. Da $ggT(X,Z) = ggT(X',Z') = 1$

$\underset{Z,Z'>0}{\Rightarrow}$ $X = X'$ und $Z = Z'$. Daraus folgt $Y = Y'$ und $(X,Y,Z) = (X',Y',Z')$.

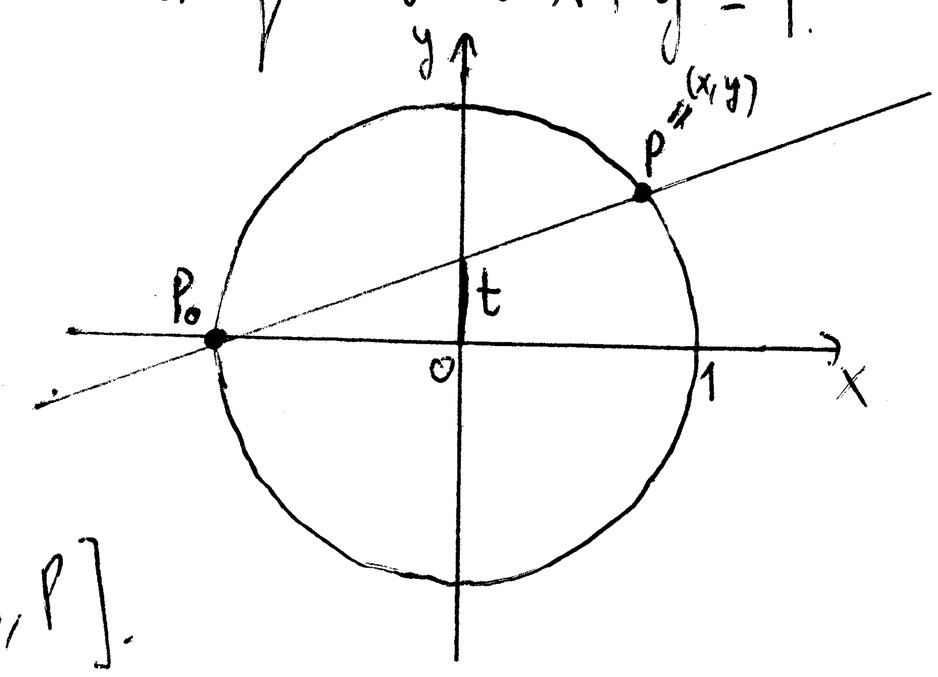
• Surjektivität: Sei $(x,y) \in \mathbb{Q}^2$ mit $x^2+y^2=1$. Sei $Z \in \mathbb{N}^*$ minimal sodass $\exists X, Y \in \mathbb{Z}$ mit $x = \frac{X}{Z}$ und $y = \frac{Y}{Z}$. $x^2+y^2=1 \Rightarrow X^2+Y^2=Z^2$.

Die Minimalität von $Z \Rightarrow ggT(X,Y,Z) = 1 \Rightarrow (X,Y,Z)$ ist ein primitives pythagoreisches Tripel und $f(X,Y,Z) = (x,y)$.

Damit ist gezeigt, dass $f$ bijektiv ist.

Wir bestimmen jetzt die rationalen Lösungen von $x^2+y^2=1$.

Sei $P_0 := (-1,0)$ und $P = (x,y) \neq P_0$ eine rationale Lösung von $x^2+y^2=1$.




Sei $t := y/x+1$. $x,y \in \mathbb{Q} \Rightarrow t \in \mathbb{Q}$.

[$t$ ist die Steigung der Geraden durch $P_0, P$].

Wir wollen $x,y$ in $t$ ausdrücken.

$$y = t(x+1) \Rightarrow 0 = x^2+y^2-1 = x^2+t^2(x+1)^2-1 = x^2-1+t^2(x+1)^2 = (x-1)(x+1)+t^2(x+1)^2$$
$$= (x+1)(x-1+t^2(x+1)) \underset{x\neq -1}{\Rightarrow} x-1+t^2(x+1) = 0 \Rightarrow x(t^2+1) = 1-t^2 \Rightarrow x = \frac{1-t^2}{1+t^2}.$$

$$y = t(x+1) = t\left(\frac{1-t^2}{1+t^2} + \frac{1+t^2}{1+t^2}\right) = \frac{2t}{1+t^2}.$$

Also $(x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ für ein $t \in \mathbb{Q}$.

Umgekehrt ist für jedes $t \in \mathbb{Q}$ der Punkt $(x,y) := \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ eine rationale Lösung von $x^2+y^2=1$.

Also $\left\{\begin{matrix}\text{rationale Lösungen} \\ \text{von } x^2+y^2=1\end{matrix}\right\} \overset{(*)}{=} \left\{\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \middle| t \in \mathbb{Q} \cup \{\infty\}\right\}$. $\left[t=\infty \Rightarrow \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \underset{\text{Konvention oder } t\to\infty}{=} (-1,0) = P_0\right]$

Mit Hilfe der Bijektion $f$ und $(*)$ können wir die primitiven pythagoreischen Tripel bestimmen.

Sei $(X,Y,Z)$ ein primitives pythagoreisches Tripel mit $Z>0$.

Fall 1: $f(X,Y,Z) = \left(\frac{X}{Z}, \frac{Y}{Z}\right) = (-1,0)$. Dann haben wir $Y=0$ und $Z=-X$.
Daraus folgt $(X,Y,Z) = (-1,0,1) = (S^2-T^2, 2ST, S^2+T^2)$ mit $S=0$ und $T=1$.

Fall 2: $f(X,Y,Z) = \left(\frac{X}{Z}, \frac{Y}{Z}\right) \neq (-1,0)$.
Dann gibt es ein (eindeutiges) $t \in \mathbb{Q}$ mit $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.
Seien $U, V \in \mathbb{Z}$ mit $t = U/V$ und $ggT(U,V)=1$.

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = \left(\frac{1-U^2/V^2}{1+U^2/V^2}, \frac{2U/V}{1+U^2/V^2}\right) = \left(\frac{V^2-U^2}{V^2+U^2}, \frac{2UV}{V^2+U^2}\right).$$

Daraus folgt $\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \left(\frac{V^2-U^2}{V^2+U^2}, \frac{2UV}{V^2+U^2}\right)$.

Fall 2a: $U, V$ haben verschiedene Paritäten.

$ggT(U,V)=1 \Rightarrow$ der Bruch $\frac{V^2-U^2}{V^2+U^2}$ ist gekürzt. Da $ggT(X,Z)=1$ und $\frac{X}{Z} = \frac{V^2-U^2}{V^2+U^2}$ folgt $X = V^2-U^2$ und $Z = V^2+U^2$. $\frac{Y}{Z} = \frac{2UV}{U^2+V^2} \Rightarrow Y = 2UV$.

Also $(X,Y,Z) = (V^2-U^2, 2UV, V^2+U^2)$ hat die gewünschte Form.

Fall 2b: $U, V$ sind ungerade. [$U, V$ gerade unmöglich denn $ggT(U,V)=1$]

Seien $S, T \in \mathbb{Z}$ mit $V+U=2S$ und $V-U=2T$

- $\frac{X}{Z} = \frac{V^2-U^2}{V^2+U^2} = \frac{(V-U)(V+U)}{\frac{1}{2}((V+U)^2+(V-U)^2)} = \frac{2\cdot 2T\cdot 2S}{4S^2+4T^2} = \frac{2ST}{S^2+T^2}$.
- $\frac{Y}{Z} = \frac{2UV}{V^2+U^2} = \frac{(V+U)^2-(V-U)^2}{(V+U)^2+(V-U)^2} = \frac{4S^2-4T^2}{4S^2+4T^2} = \frac{S^2-T^2}{S^2+T^2}$.
- $ggT(U,V)=1 \Rightarrow ggT(S,T)=1$.
- $S, T$ haben verschiedene Paritäten, sonst hätten wir $2|V$ und $2|U$ ↯ [$V=S+T$, $U=S-T$]
- ($ggT(S,T)=1$ und $S,T$ haben verschiedene Paritäten) $\Rightarrow$ die Brüche $\frac{2ST}{S^2+T^2}$ und $\frac{S^2-T^2}{S^2+T^2}$ sind gekürzt.

Also haben wir $\frac{X}{Z} = \frac{2ST}{S^2+T^2}$, $\frac{Y}{Z} = \frac{S^2-T^2}{S^2+T^2}$ mit $ggT(X,Z) = ggT(2ST, S^2+T^2) = 1$ und $ggT(Y,Z) = ggT(S^2-T^2, S^2+T^2) = 1$.

Daraus folgt $X = 2ST$, $Z = S^2+T^2$ und $Y = S^2-T^2$.

Also hat $(X,Y,Z) = (2ST, S^2-T^2, S^2+T^2)$ die gewünschte Form.

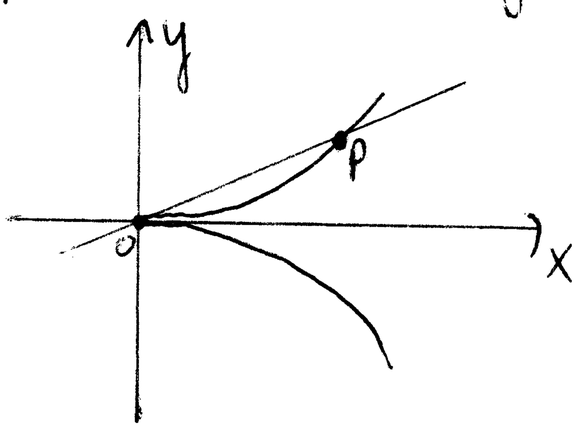
Damit ist Satz 5.3 bewiesen.

# D) Elliptische Kurven über $\mathbb{Q}$

Hauptziel: Untersuchung von $y^2 = x^3 + ax^2 + bx + c$ $(a, b, c \in \mathbb{Q})$ auf rationale Lösungen.

Beispiele: (1) $y^2 = x^3$

In $\mathbb{R}$:




Sei $P := (x, y) \in \mathbb{Q}^2$ eine Lösung von (1), $P \neq (0,0)$.

Sei $t := y/x$. $t \in \mathbb{Q}$ und $y = tx$.

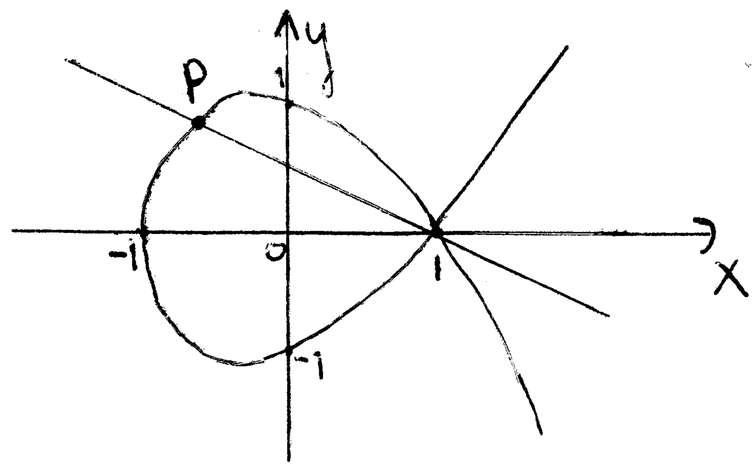
$y^2 = x^3 \Rightarrow t^2x^2 = x^3 \Rightarrow x = t^2 \Rightarrow y = tx = t^3$.

Also $(x, y) = (t^2, t^3)$ für ein $t \in \mathbb{Q}$. Umgekehrt ist $(t^2, t^3)$ eine rationale Lösung von (1) für alle $t \in \mathbb{Q}$.

Die rationalen Lösungen von (1) sind der Form $(t^2, t^3)$ mit $t \in \mathbb{Q}$.

(2) $y^2 = (x+1)(x-1)^2$

In $\mathbb{R}$:




Sei $P := (x, y) \in \mathbb{Q}^2$ eine Lösung von (2), $P \neq (1,0)$.

Sei $t := y/x-1$ [$t$ ist die Steigung der Geraden durch $P$ und $(1,0)$]

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

$\Rightarrow y = t(t^2-1-1) = t(t^2-2)$. Also $(x, y) = (t^2-1, t(t^2-2))$ für ein $t \in \mathbb{Q}$. Umgekehrt ist für jedes $t \in \mathbb{Q}$ der Punkt $(t^2-1, t(t^2-2))$ eine rationale Lösung von (2).

Die rationalen Lösungen von (2) sind der Form $(t^2-1, t(t^2-2))$; $t \in \mathbb{Q}$.

Bem: $x^3$ hat 0 als dreifache Nullstelle und $(x+1)(x-1)^2$ hat 1 als doppelte Nullstelle. Allgemein: Falls $p(x) := x^3+ax^2+bx+c$ $(a,b,c \in \mathbb{Q})$ eine doppelte oder dreifache Nullstelle besitzt, dann ist es einfach die rationalen Lösungen von $y^2 = p(x)$ zu bestimmen.

Ab jetzt wird vorausgesetzt, dass $p(x) = x^3+ax^2+bx+c$ nur einfache Nullstellen besitzt [d.h. die 3 komplexen Nullstellen von $p$ sind paarweise verschieden].

Die Bedingung dafür ist (s. §1):

$$\Delta := -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0.$$

[Wenn $a=0$, dann ist $\Delta = -4b^3 - 27c^2$]

Def: Eine elliptische Kurve über $\mathbb{Q}$ ist eine Gleichung der Form $E: y^2 = x^3+ax^2+bx+c$ mit $a,b,c \in \mathbb{Q}$ und $\Delta \neq 0$.

[NB: Bei der Bestimmung der Länge von Ellipsen treten Ausdrücke auf, die $\sqrt{x^3+ax^2+bx+c}$ enthalten]

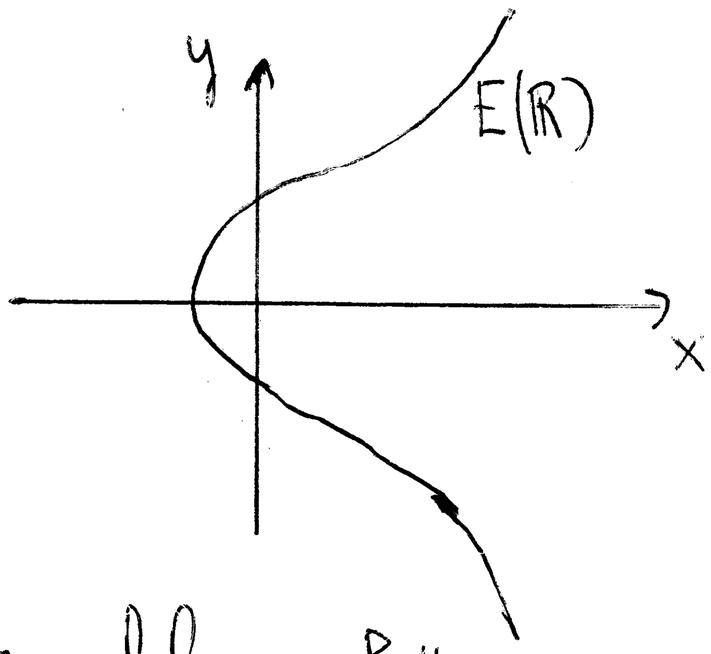
Def: Sei $E: y^2 = x^3+ax^2+bx+c$ eine elliptische Kurve über $\mathbb{Q}$. Sei $K \supseteq \mathbb{Q}$ ein Körper. $E(K) := \{(x,y) \in K^2 \mid y^2 = x^3+ax^2+bx+c\} \cup \{\mathcal{O}\}$.

$E(\mathbb{Q})$ ist also die Menge der rationalen Lösungen von $y^2 = x^3+ax^2+bx+c$, plus $\{\mathcal{O}\}$.

Punkt im Unendlichen

## Beispiele:

i) $E: y^2 = x^3 + 17$



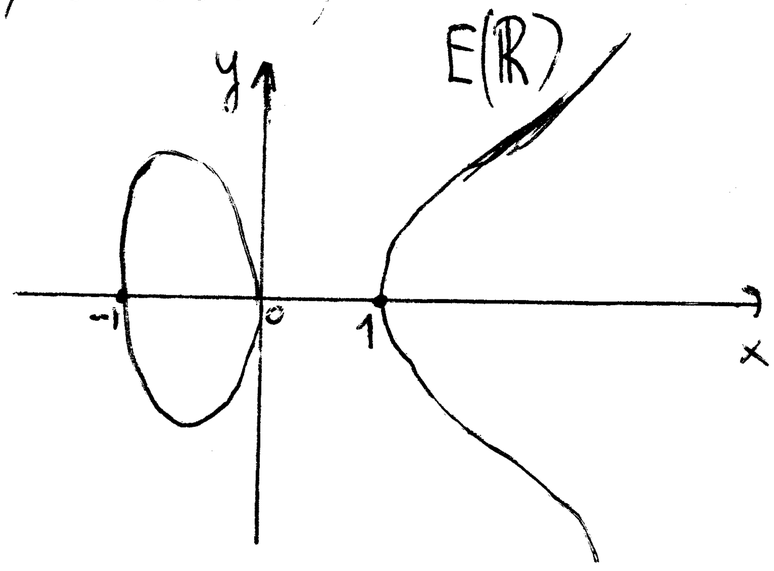

$\Delta = -27 \cdot 17^2 < 0.$

[$p(x) := x^3 + 17$ hat nur eine reelle Nullstelle]

E hat genau 16 ganzzahlige Lösungen, unter anderen $(-1,4)$, $(-2,3)$, ..., $(5234, 378661)$.

ii) $E: y^2 = x^3 - x = x(x-1)(x+1).$

$E(\mathbb{Q}) = \{(0,0), (-1,0), (1,0), \mathcal{O}\}.$




$\Delta = -4(-1)^3 > 0$

[$p(x)$ hat 3 verschiedene reelle Nullstellen]

Sei $E: y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve über $\mathbb{Q}$ und $K \supseteq \mathbb{Q}$ ein Körper.

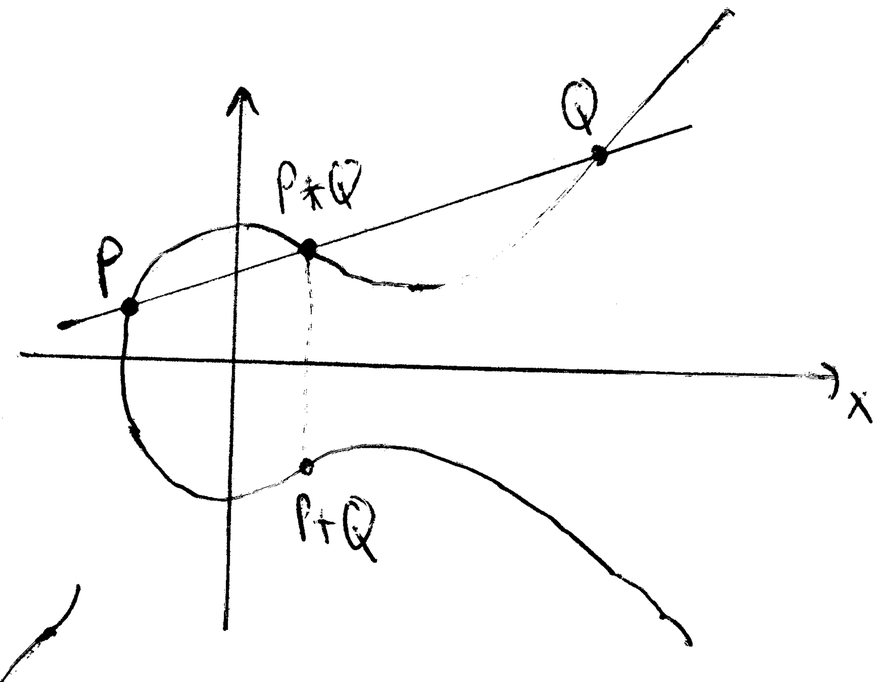
## Gruppenstruktur auf $E(K)$

Seien $P, Q \in E(K) \setminus \{\mathcal{O}\}$, $P = (x_1, y_1)$, $Q = (x_2, y_2)$.

Fall 1: $x_1 \neq x_2$.

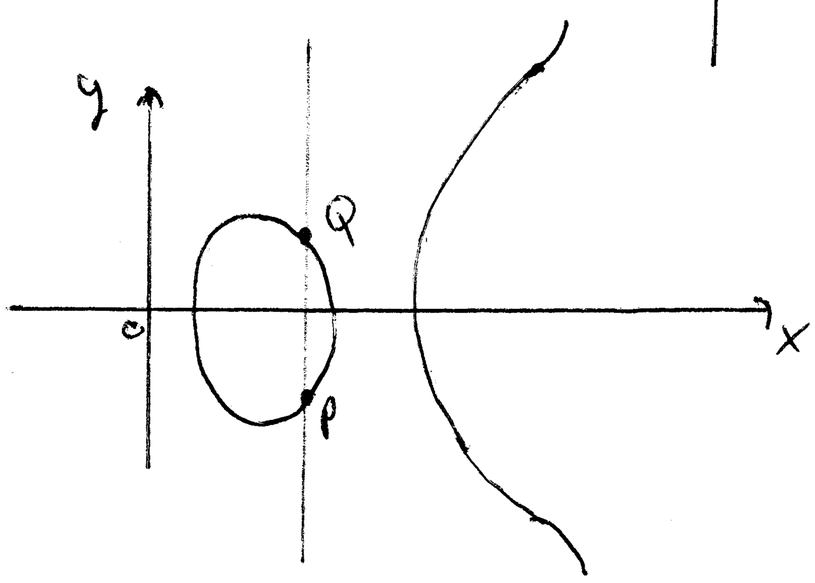
Die Gerade durch $P, Q$ trifft $E(K)$ genau in einem dritten Punkt $P * Q := (x_3, y_3)$.

Wir setzen $P + Q := (x_3, -y_3)$




Fall 2: $x_1 = x_2$, $P \neq Q$.

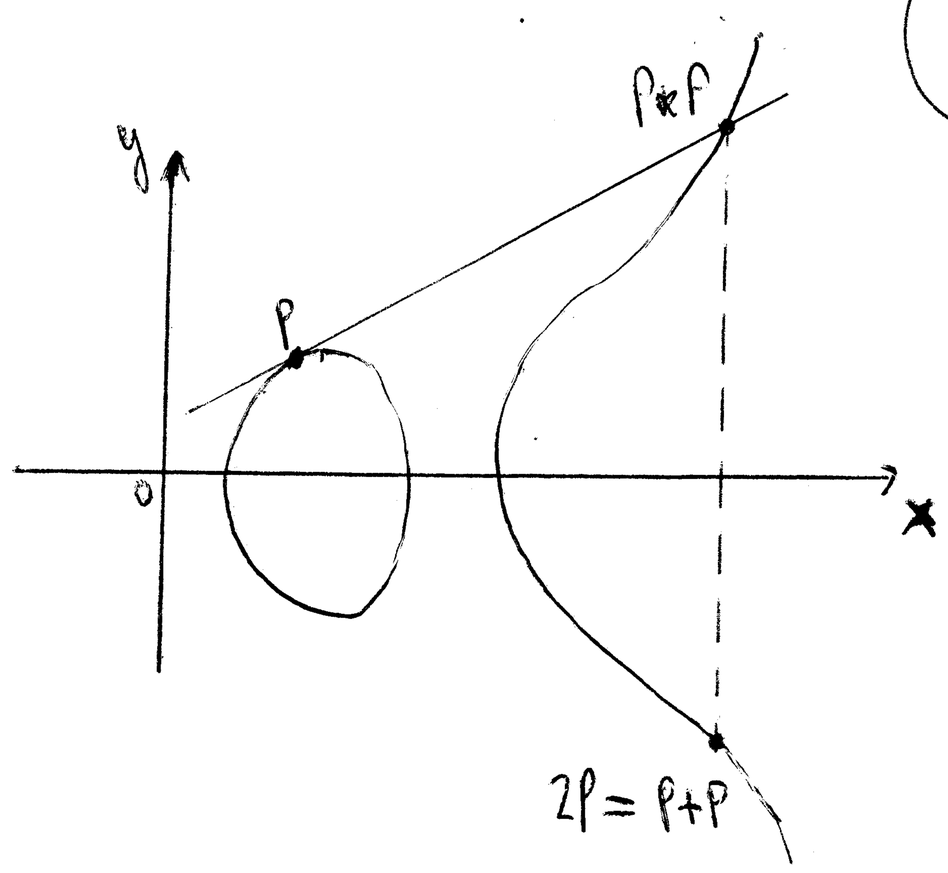
$P + Q := \mathcal{O}$ der Punkt im Unendlichen.



<u>Fall 3:</u> $P = Q$, $y_1 = y_2 \neq 0$.

Die Tangente an $E(K)$ im Punkte $P$ schneidet $E(K)$ genau in einem dritten Punkt $P * Q := (x_3, y_3)$.

Wir setzen $P + Q := (x_3, -y_3)$.




<u>Fall 4:</u> $P = Q$, $y_1 = y_2 = 0$.

Wir setzen $P + Q = 2P := \mathcal{O}$ der Punkt im Unendlichen.

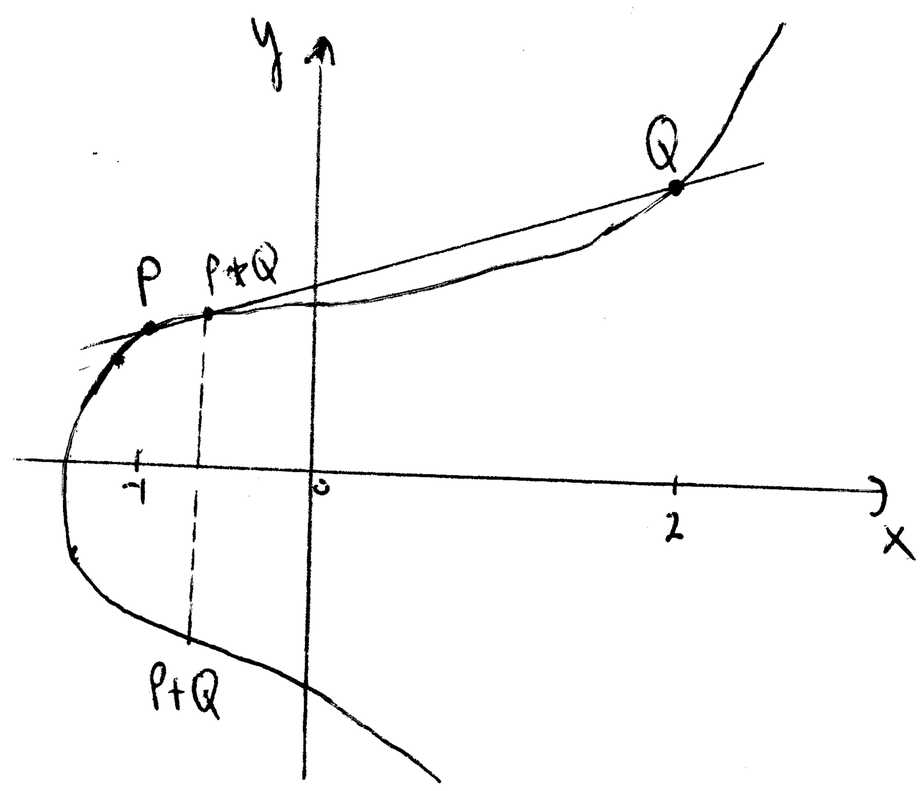
Wir wollen, dass $\mathcal{O}$ das neutrale Element ist. Also setzen wir $P + \mathcal{O} = \mathcal{O} + P = P \quad \forall P \in E(K)$.

<u>Satz 5.4:</u> $(E(K), +)$ ist eine abelsche Gruppe.

Alles trivial, ausser der Assoziativität. Das neutrale Element ist $\mathcal{O}$, und das Inverse von $P = (x, y) \in E(K)$ ist $-P := (x, -y)$

[Spiegelung an der x-Achse]

<u>Beispiele:</u> Sei $E: y^2 = x^3 + 17$




1) Seien $P := (x_1, y_1) = (-1, 4)$, $Q := (x_2, y_2) = (2, 5)$.

Geradengleichung durch $P, Q$:

$$y = \frac{5-4}{2-(-1)}(x+1) + 4 = \frac{1}{3}x + \frac{13}{3}.$$

Schnittpunkt zwischen $E(\mathbb{Q})$ und $\overline{PQ}$: $y^2 = x^3 + 17 \Rightarrow$

$$\left(\frac{1}{3}x + \frac{13}{3}\right)^2 = x^3 + 17 \Leftrightarrow x^3 - \left(\frac{x}{3} + \frac{13}{3}\right)^2 + 17 = 0.$$

Da $x^3 - \left(\frac{x}{3} + \frac{13}{3}\right)^2 + 17 = 0$ für $x = -1$ und $x = 2$ haben wir

$x^3-\left(\frac{x}{3}+\frac{13}{3}\right)^2+17=(x+1)(x-2)(x-x_3).$ $\qquad x_3=?$ $\qquad$ (20)

Koeffizienten von $x^2$ gleichsetzen: $-\left(\frac{1}{3}\right)^2=1-2-x_3 \Rightarrow x_3=1-2+\frac{1}{9}=-\frac{8}{9}.$

$y_3=\frac{1}{3}\left(-\frac{8}{9}\right)+\frac{13}{3}=-\frac{8}{27}+\frac{117}{27}=\frac{109}{27}.$ Daraus folgt

$P*Q=(x_3,y_3)=\left(-\frac{8}{9},\frac{109}{27}\right)$ und $P+Q=\left(-\frac{8}{9},-\frac{109}{27}\right).$

ii) $P=Q=(-1,4).$ $\quad 2P=P+P=?$

Tangente an $y^2=x^3+17$ im Punkte $(-1,4)$: $\quad y^2=x^3+17 \Rightarrow$

$2yy'=3x^2 \Rightarrow y'=\frac{3x^2}{2y}.$ $\qquad y'(-1)=\frac{3(-1)^2}{2\cdot 4}=\frac{3}{8}.$

Die Tangentengleichung lautet $y=\frac{3}{8}(x+1)+4=\frac{3}{8}x+\frac{35}{8}.$

Schnittpunkt zwischen $E(\mathbb{Q})$ und der Tangenten: $y^2=x^3+17 \Rightarrow$

$\left(\frac{3}{8}x+\frac{35}{8}\right)^2=x^3+17 \Rightarrow x^3-\left(\frac{3}{8}x+\frac{35}{8}\right)^2+17=0 \Rightarrow$

$x^3-\left(\frac{3}{8}x+\frac{35}{8}\right)^2+17=(x+1)^2(x-x_3)=(x+1)(x+1)(x-x_3).$

$-1$ ist doppelte Nullstelle von $x^3-\left(\frac{3}{8}x+\frac{35}{8}\right)^2+17$

Koeffizienten von $x^2$ gleichsetzen: $-\frac{9}{64}=1+1-x_3 \Rightarrow x_3=\frac{137}{64}.$

$y_3=\frac{3}{8}(x_3+1)+4=\frac{3}{8}\left(\frac{137}{64}+1\right)+4=\frac{2651}{512}.$

Also $2P=(x_3,-y_3)=\left(\frac{137}{64},-\frac{2651}{512}\right).$

Sei $E: y^2=x^3+ax^2+bx+c$ eine elliptische Kurve über $\mathbb{Q}$.

Seien $P=(x_1,y_1)$ und $Q=(x_2,y_2)$ Punkte aus $E(K)\setminus\{\mathcal{O}\}$. [$K$ Körper $\supseteq \mathbb{Q}$]

Sei $\lambda$ die Steigung $\begin{cases} \text{der Geraden } PQ \text{ wenn } x_1\neq x_2 \\ \text{der Tangente an } P \text{ wenn } P=Q \text{ und } y_1=y_2\neq 0. \end{cases}$

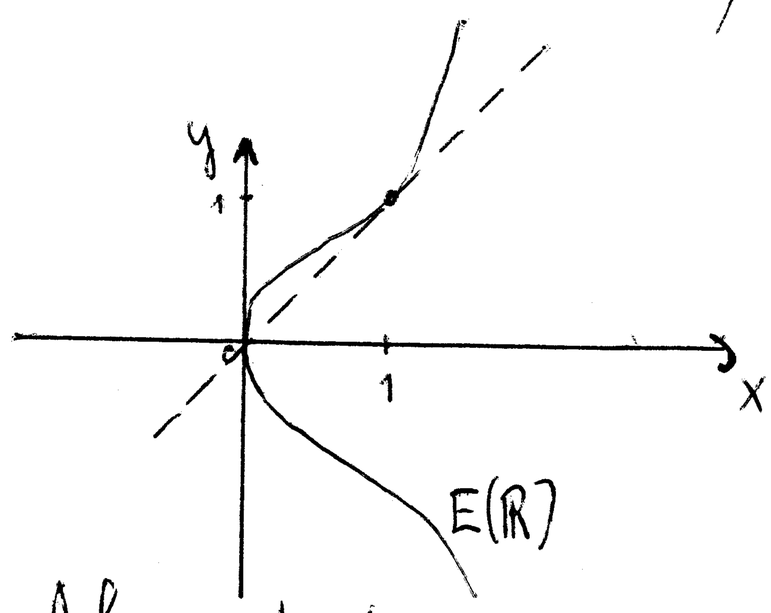
Dann gilt $\boxed{P+Q=(x_3,-y_3) \text{ mit } \begin{cases} x_3=\lambda^2-a-x_1-x_2 \\ y_3=\lambda(x_3-x_1)+y_1. \end{cases}}$

## Ergebnisse über die Gruppe $(E(\mathbb{Q}),+)$:

**Satz 5.5:** (Nagell-Lutz, 1937)

Sei $E: y^2=x^3+ax^2+bx+c$ eine elliptische Kurve über $\mathbb{Q}$.
Der Einfachheit halber setzen wir $a,b,c\in\mathbb{Z}$ voraus.
Sei $P=(x,y)\in E(\mathbb{Q})$ von endlicher Ordnung.
Dann sind $x,y\in\mathbb{Z}$ und $(y=0$ oder $y^2\mid\Delta=-4a^3c+a^2b^2+18abc-4b^3-27c^2)$. D

**Beispiele:** 1) $E: y^2=x^3-x^2+x=x(x^2-x+1)$.




Sei $(x,y)\in E(\mathbb{Q})$ von endlicher Ordnung.
Dann sind $x,y\in\mathbb{Z}$ und $(y=0$ oder $y^2\mid\Delta)$.

- Falls $y=0$, $x^3-x^2+x=x(x^2-x+1)=0 \underset{x\in\mathbb{Z}}{\Rightarrow} x=0$. Also ist $(0,0)$ ein Kandidat. Trivialerweise ist $(0,0)$ von Ordnung 2.
- Falls $y^2\mid\Delta$, dann $y^2\mid(-1)^2\cdot1^2-4\cdot1^3=-3 \Rightarrow y=\pm1$.

$y^2=x^3-x^2+x \Rightarrow x^3-x^2+x=1 \Rightarrow x^3-x^2+x-1=0 \Rightarrow (x^2+1)(x-1)=0 \underset{x\in\mathbb{Z}}{\Rightarrow}$
$x=1$. $(1,1)$ und $(1,-1)$ sind Kandidaten.

Da $(1,1)+(1,1)=(0,0)$ [s. Bild oder Üb] ist $(1,1)$ der Ordnung 4.

Die Elemente von $E(\mathbb{Q})$ von endlicher Ordnung sind

$(1,1)$; $(0,0)$; $(1,-1)$; $\mathcal{O}$.

2) $E: y^2 = x^3 - 2$. Sei $P = (3,5)$. $P \in E(\mathbb{Q})$ denn $5^2 = 3^3 - 2$.

$2P \overset{\text{rechnen}}{=} \left(\frac{129}{100}, \frac{-383}{1000}\right)$. $\frac{129}{100} \notin \mathbb{Z} \overset{5.5}{\Rightarrow}$ $2P$ ist nicht von endlicher Ordnung $\Rightarrow$ $P$ ist nicht von endlicher Ordnung $\Rightarrow$ $P$ ist von Ordnung $\infty$. Insbesondere ist die Gruppe $(E(\mathbb{Q}), +)$ unendlich.

<u>Satz 5.6:</u> (Mazur, 1977)

Sei $E: y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve über $\mathbb{Q}$. Ist $P = (x,y) \in E(\mathbb{Q})$ von endlicher Ordnung $m$, dann ist $m \leq 10$ oder $m = 12$. $\square$

<u>Satz 5.7:</u> (Mordell, 1922)

Sei $E: y^2 = x^3 + ax^2 + bx + c$ eine elliptische Kurve über $\mathbb{Q}$. Dann ist $E(\mathbb{Q})$ eine endlich erzeugte abelsche Gruppe, also $\exists r \in \mathbb{N}$ und eine endliche Gruppe $T$ mit $E(\mathbb{Q}) \simeq \mathbb{Z}^r \times T$. $r$ heißt der Rank von $E$ [$r, T$ sind eindeutig bestimmt] $\square$

<u>Bem:</u> i) $r$ ist sehr schwer zu berechnen; ob $r$ beliebig groß sein kann ist offen.

ii) $T$ besteht aus den Elementen von $E(\mathbb{Q})$, die endliche Ordnung haben: $T = \{P \in E(\mathbb{Q}) \mid P \text{ ist von endlicher Ordnung}\}$

iii) $E(\mathbb{Q})$ ist endlich $\Leftrightarrow$ $r = 0$.

# Anwendungen von elliptischen Kurven

## i) Elliptischen Kurven über $K = \mathbb{Q}$

Sie spielen eine wichtige Rolle im Beweis des letzten fermatschen Satzes: Hier eine extrem grobe Beweisskizze:

Ang. $\exists a, b, c \in \mathbb{N}^*$ mit $ggT(a,b,c) = 1$ und eine Primzahl $p \geq 5$ mit $a^p + b^p = c^p$.

Sei $E_{a,b,c}: y^2 = x(x-a^p)(x+b^p)$. [$E_{a,b,c}$ ist eine elliptische Kurve über $\mathbb{Q}$]

Dann wurde gezeigt:

- $E_{a,b,c}$ ist semistabil und nicht modular
- Jede semistabile elliptische Kurve über $\mathbb{Q}$ ist modular

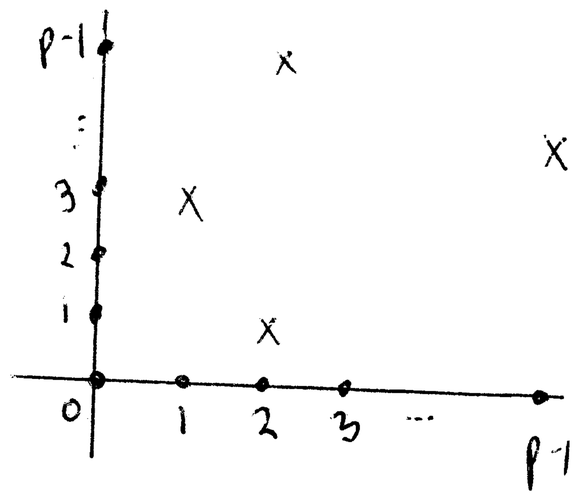
[Wiles, 1993]

## ii) Elliptische Kurven über $K = \mathbb{Z}_p$ ($p$ prim $\geq 3$)

$y^2 = x^3 + ax^2 + bx + c$, $a, b, c \in \mathbb{Z}_p$, $\Delta \neq 0$.

$E(\mathbb{Z}_p) = \{(x,y) \in \mathbb{Z}_p^2 \mid y^2 = x^3 + ax^2 + bx + c\} \cup \{O\}$.

Punkt im Unendlichen




$(E(\mathbb{Z}_p), +)$ ist eine abelsche Gruppe:

[die Formeln zur Addition von Kurvenpunkten gelten auch für elliptische Kurven über endlichen Körpern].

Anwendungen: Primzahltests
Schnelle Faktorisierung natürlicher Zahlen
Verschlüsselungsverfahren

# E) Reduktion modulo n

Zur Erinnerung: $\mathbb{Z} \to \mathbb{Z}_n$, $x \mapsto x \bmod n$ ist ein Ringhomomorphismus ($n \in \mathbb{N}$).

Reduktion modulo n (für ein geeignetes $n \geq 2$) erlaubt einem ab und zu zu zeigen, dass eine diophantische Gleichung $F(x_1, \dots, x_m) = 0$ (mit $F(X_1, \dots, X_m) \in \mathbb{Z}[X_1, \dots, X_m]$) <u>keine</u> ganzzahlige (oder nichttriviale ganzzahlige) Lösung hat. [Nichttrivial bedeutet $\neq (0, 0, \dots, 0)$]

<u>Beispiele:</u> (1) $x^2 + y^2 = 7z^2$.

Hat diese Gleichung eine nichttriviale Lösung in $\mathbb{Z}$?

Ang. $(x_0, y_0, z_0) \in \mathbb{Z}^3$ ist eine nichttriviale Lösung von $x^2 + y^2 = 7z^2$.

Sei $d := ggT(x_0, y_0, z_0)$ und $(x, y, z) := \left(\frac{x_0}{d}, \frac{y_0}{d}, \frac{z_0}{d}\right)$. Dann ist $(x, y, z)$ eine nichttriviale Lösung von (1) und $ggT(x, y, z) = 1$.

$ggT(x, y, z) = 1 \Rightarrow x, y, z$ können nicht alle 3 durch 7 teilbar sein

Ab jetzt arbeiten wir in $\mathbb{Z}_7$.

$x^2 + y^2 = 7z^2 \Rightarrow x^2 + y^2 = 0$.

Quadrate mod 7 sind 0, 1, 2, 4:

| $w \bmod 7$ | $-3$ | $-2$ | $-1$ | $0$ | $1$ | $2$ | $3$ |
|---|---|---|---|---|---|---|---|
| $w^2 \bmod 7$ | 2 | 4 | 1 | 0 | 1 | 4 | 2 |

Summe von 2 Quadraten in $\mathbb{Z}_7$:

| $x^2 + y^2$ | 0 | 1 | 2 | 4 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 4 |
| 1 | 1 | 2 | 3 | 5 |
| 2 | 2 | 3 | 4 | 6 |
| 4 | 4 | 5 | 6 | 1 |

Man sieht: $x^2 + y^2 = 0 \Rightarrow x^2 = y^2 = 0$. Und

$x^2 = y^2 = 0 \Rightarrow x = y = 0$.

$\mathbb{Z}_7$ Körper

Zurück in $\mathbb{Z}$: $x = y = 0$ in $\mathbb{Z}_7$ bedeutet $7|x$ und $7|y$.

Daraus folgt $49|x^2$, $49|y^2$ und $49|x^2+y^2$. $x^2+y^2 = 7z^2 \Rightarrow 49|7z^2$

$\Rightarrow 7|z^2 \underset{7 \text{ prim}}{\Rightarrow} 7|z$. Also $7|x$, $7|y$, $7|z$. Dies widerspricht

$ggT(x,y,z) = 1$. Damit ist bewiesen, dass $x^2+y^2=7z^2$ keine nichttriviale Lösung in $\mathbb{Z}$ hat.

(2) $x^4+y^4-z^4=3$.

Hat diese Gleichung eine ganzzahlige Lösung?

Ang. $(x,y,z) \in \mathbb{Z}^3$ ist eine Lösung von $x^4+y^4-z^4=3$.

Ab jetzt arbeiten wir in $\mathbb{Z}_5$.

| $w$ mod 5 | $-2$ | $-1$ | $0$ | $1$ | $2$ |
|---|---|---|---|---|---|
| $w^2$ mod 5 | 4 | 1 | 0 | 1 | 4 |
| $w^4$ mod 5 | 1 | 1 | 0 | 1 | 1 |

Die Tabelle zeigt, dass jede 4-te Potenz in $\mathbb{Z}_5$ ist 0 oder 1.

Also $x^4+y^4-z^4 = \begin{cases} 0+0-0=0 & \text{oder} \\ 0+0-1=-1 & \text{oder} \\ 0+1-0=1 & \text{oder} \\ 0+1-1=0 & \text{oder} \\ 1+0+0=1 & \text{oder} \\ 1+0-1=0 & \text{oder} \\ 1+1-0=2 & \text{oder} \\ 1+1-1=1. \end{cases}$

D.h. $x^4+y^4-z^4 \in \{0,1,2,4\}$.

Also $x^4+y^4-z^4 \neq 3$ in $\mathbb{Z}_5$.

Das impliziert

$x^4+y^4-z^4 \neq 3$ in $\mathbb{Z}$. $\lightning$

Die Gleichung $x^4+y^4-z^4=3$ hat keine ganzzahlige Lösung.

## F) Der Satz von Matiyasevich

Gibt es einen Algorithmus (Verfahren), der für jedes gegebene Polynom $F \in \mathbb{Z}[X_1, \dots, X_n]$ ($n \in \mathbb{N}^*$ beliebig) Auskunft darüber gibt, ob die Gleichung $F(x_1, \dots, x_n) = 0$ ganzzahlige Lösungen hat oder nicht?

**Satz 5.8:** (Matiyasevich, 1970) [Das zehnte Hilbert-Problem]
Ein solcher Algorithmus existiert nicht.

$\square$

Bem: Wenn wir nur Polynome mit einer Variablen $F \in \mathbb{Z}[X]$ betrachten, dann gibt es einen solchen Algorithmus (s. A), S. 1,2).