KAPITEL 1

Einführung

Gegeben seien Polynome $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_n]$. Ein Grundproblem in der Zahlentheorie ist die Bestimmung der Mengen

$$X_{\mathbb{Z}} = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n : f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0\}$$

und

$$X_{\mathbb{Q}} = \{(a_1, \ldots, a_n) \in \mathbb{Q}^n : f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0\},$$

d.h. das Lösen des diophantischen Gleichungssystems $f_1 = \cdots = f_r = 0$ in ganzen und rationalen Zahlen. Betrachtet man die Lösungen der Gleichungen in $\mathbb{R}^n$ und $\mathbb{C}^n$, also

$$X_{\mathbb{R}} = \{(a_1, \ldots, a_n) \in \mathbb{R}^n : f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0\}$$

und

$$X_{\mathbb{C}} = \{(a_1, \ldots, a_n) \in \mathbb{C}^n : f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0\},$$

so erhält man geometrische Objekte in $\mathbb{R}^n$ und $\mathbb{C}^n$, und natürlich gilt

$$X_{\mathbb{Z}} \subseteq X_{\mathbb{Q}} \subseteq X_{\mathbb{R}} \subseteq X_{\mathbb{C}}.$$

$X_{\mathbb{C}}$ wird in der algebraischen Geometrie untersucht. Man stellt fest, dass die Geometrie von $X_{\mathbb{C}}$ einen wesentlichen Einfluss auf die zahlentheoretischen Mengen $X_{\mathbb{Z}}$ und $X_{\mathbb{Q}}$ hat. Damit beschäftigt sich die diophantische Geometrie.

Im Folgenden werden wir ein paar Beispiele behandeln.

Pythoagoräische Tripel: Ein Tripel (a, b, c) natürlicher Zahlen wird pythagoräisches Tripel genannt, wenn gilt

$$a^2 + b^2 = c^2,$$

d.h. wenn a, b, c Seitenlängen eines rechtwinkligen Dreiecks sind. Die ersten Tripel findet man durch Probieren, wobei wir o.E. $a \leq b$ voraussetzen können:

$$(3,4,5), \quad (6,8,10), \quad (5,12,13), \quad (9,12,15), \quad (8,15,17), \quad (12,16,20), \quad (15,20,25), \quad \ldots$$

Da mit (a, b, c) und $m \in \mathbb{N}$ auch (ma, mb, mc) ein pythagoräisches Tripel ist, können wir auch $\mathrm{ggT}(a, b, c) = 1$ voraussetzen. Dann findet man folgende Tripel mit $c \leq 200$:

$$(3,4,5), \quad (5,12,13), \quad (8,15,17), \quad (7,24,25), \quad (20,21,29), \quad (12,35,37), \quad (9,40,41), \quad (28,45,53),$$
$$(11,60,61), \quad (33,56,65), \quad (16,63,65), \quad (48,55,73), \quad (36,77,85), \quad (13,84,85), \quad (39,80,89),$$
$$(65,72,97), \quad (20,99,101), \quad (60,91,109), \quad (15,112,113), \quad (44,117,125), \quad (88,105,137),$$
$$(24,143,145), \quad (17,144,145), \quad (51,140,149), \quad (85,132,157), \quad (119,120,169), \quad (52,165,173),$$
$$(19,180,181), \quad (104,153,185), \quad (57,176,185), \quad (95,168,193), \quad (28,195,197).$$

Kann man diese Tripel irgendwie beschreiben?
Gilt $a^2 + b^2 = c^2$ mit $a, b, c \in \mathbb{N}$, so ist

$$(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1 \quad \text{mit} \quad \frac{a}{c}, \frac{b}{c} \in \mathbb{Q},$$

d.h. $(\frac{a}{c}, \frac{b}{c})$ ist ein Punkt mit rationalen Koordinaten des Einheitskreises. Wir beschäftigen uns daher zunächst mit nachfolgendem Problem:

Datei: dg_einf.tex. Version vom 25.4.2019

Rationale Kreispunkte: Wir suchen nach Punkten (x, y) des Einheitskreises mit rationalen Koeffizienten, d.h. nach Lösungen der Gleichung

$$x^2 + y^2 = 1 \quad \text{mit} \quad x, y \in \mathbb{Q}.$$

Es gibt einige „triviale“ Lösungen der Gleichung, beispielsweise $(-1, 0)$.

(1) Ist (x_0, y_0) ein von $(-1, 0)$ verschiedener Kreispunkt mit $x_0, y_0 \in \mathbb{Q}$, so gibt es genau eine Gerade durch $(-1, 0)$ und (x_0, y_0), nämlich

$$y = t(x + 1) \quad \text{mit} \quad t = \frac{y_0}{x_0 + 1} \in \mathbb{Q}.$$

Die Gerade schneidet den Kreis genau in den beiden Punkten.

(2) Sei umgekehrt

$$y = t(x + 1)$$

eine Gerade durch $(-1, 0)$ mit rationaler Steigung t. Wir bestimmen die Schnittpunkte der Geraden mit dem Kreis, indem wir die Geradengleichung in $x^2 + y^2 - 1 = 0$ einsetzen:

$$\begin{aligned} 0 &= x^2 + t^2(x+1)^2 - 1 = x^2 + t^2(x^2 + 2x + 1) - 1 = (t^2+1)x^2 + 2t^2x + t^2 - 1 = \\ &= (t^2+1)\left(x^2 + \frac{2t^2}{t^2+1}x + \frac{t^2-1}{t^2+1}\right) = (t^2+1)\left(x^2 + \frac{(t^2+1)+(t^2-1)}{t^2+1}x + \frac{t^2-1}{t^2+1}\right) = \\ &= (t^2+1)\,(x+1)\left(x + \frac{t^2-1}{t^2+1}\right) = (t^2+1)\Big(x - (-1)\Big)\left(x - \frac{1-t^2}{1+t^2}\right). \end{aligned}$$

Der erste Schnittpunkt ist $(-1, 0)$, der zweite (x_t, y_t) mit

$$x_t = \frac{1-t^2}{1+t^2}, \quad y_t = t(x_t + 1) = t\left(\frac{1-t^2}{1+t^2} + 1\right) = \frac{2t}{1+t^2}.$$

Offensichtlich gilt $x_t, y_t \in \mathbb{Q}$ wegen $t \in \mathbb{Q}$ und $x_t \neq -1$.

Zusammengefasst ergibt sich folgender Satz:

Satz. *Die Abbildung*

$$\psi : \mathbb{Q} \to \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : x^2 + y^2 = 1\} \setminus \{(-1, 0)\}, \quad t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

ist bijektiv mit der Umkehrabbildung

$$\varphi : \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : x^2 + y^2 = 1\} \setminus \{(-1, 0)\} \to \mathbb{Q}, \quad (x, y) \mapsto \frac{y}{x+1}.$$

Beweis: Man kann dies auch unabhängig von den vorangegangenen Überlegungen beweisen. Dazu kann man so vorgehen:

(1) Offensichtlich ist $\psi(t)$ für alle $t \in \mathbb{Q}$ definiert. Dann zeigt man, dass das Bild von ψ tatsächlich in der angegebenen Bildmenge enthalten ist.

(2) Da in der Definitionsmenge der Punkt $(-1, 0)$ ausgeschlossen ist, kommt in der Definitionsmenge kein Punkt der Gestalt $(-1, *)$ vor. Daher ist φ sinnvoll definiert.

(3) Es gilt

$$\varphi(\psi(t)) = \varphi\left(\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)\right) = \frac{\frac{2t}{1+t^2}}{\frac{1-t^2}{1+t^2} + 1} = \frac{2t}{(1-t^2) + (1+t^2)} = t$$

und

$$\begin{aligned}\psi(\varphi((x,y)) &= \psi(\frac{y}{x+1}) = (\frac{1-(\frac{y}{x+1})^2}{1+(\frac{y}{x+1})^2}, \frac{2(\frac{y}{x+1})}{1+(\frac{y}{x+1})^2}) = (\frac{(x+1)^2-y^2}{(x+1)^2+y^2}, \frac{2y(x+1)}{(x+1)^2+y^2}) = \\ &= (\frac{(x+1)^2-(1-x^2)}{(x+1)^2+(1-x^2)}, \frac{2y(x+1)}{(x+1)^2+(1-x^2)}) = \\ &= (\frac{(x^2+2x+1)+(-1+x^2)}{(x^2+2x+1)+(1-x^2)}, \frac{2y(x+1)}{(x^2+2x+1)+(1-x^2)}) = \\ &= (\frac{2x^2+2x}{2x+2}, \frac{2y(x+1)}{2x+2}) = (x,y).\end{aligned}$$

Dies zeigt dann, dass ψ und φ invers zueinander sind. ■

Wir wenden dies jetzt auf pythagoräische Tripel an:

SATZ. (1) *Sind $a,b,c \in \mathbb{Q}$ mit $a^2+b^2=c^2$ und $c \neq -a$, schreibt man $\frac{b}{a+c} = \frac{n}{m}$ mit $n \in \mathbb{Z}$, $m \in \mathbb{N}$ und $\mathrm{ggT}(n,m)=1$, setzt man $q = \frac{c}{m^2+n^2} \in \mathbb{Q}$, so gilt*

$$a = q\cdot(m^2-n^2), \quad b = q\cdot 2mn, \quad c = q\cdot(m^2+n^2).$$

(2) *Sind $a,b,c \in \mathbb{Q}$ mit $a^2+b^2=c^2$ und $c \neq -a$, sind $n \in \mathbb{Z}$, $m \in \mathbb{N}$, $q \in \mathbb{Q}$ mit*

$$a = q\cdot(m^2-n^2), \quad b = q\cdot 2mn, \quad c = q\cdot(m^2+n^2),$$

so sind n,m,q durch a,b,c eindeutig bestimmt.

(3) *Sind $n \in \mathbb{Z}$, $m \in \mathbb{N}$ mit $\mathrm{ggT}(n,m)=1$ und $q \in \mathbb{Q}^*$ und*

$$a = q\cdot(m^2-n^2), \quad b = q\cdot 2mn, \quad c = q\cdot(m^2+n^2),$$

so gilt

$$a^2+b^2=c^2 \quad \text{und} \quad c \neq -a.$$

Beweis:

(1) Zunächst bemerken wir, dass aus $c \neq -a$ natürlich $c \neq 0$ folgt, denn $c=0$ würde wegen $a^2+b^2=c^2$ sofort $a=b=0$ liefern. Aus $a^2+b^2=c^2$ folgt $(\frac{a}{c})^2+(\frac{b}{c})^2=1$. Die Voraussetzung $c \neq -a$ liefert $(\frac{a}{c},\frac{b}{c}) \neq (-1,0)$, also gilt für

$$t = \frac{\frac{b}{c}}{\frac{a}{c}+1} = \frac{b}{a+c}$$

die Beziehung

$$(\frac{a}{c},\frac{b}{c}) = (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}).$$

Schreiben wir $t = \frac{n}{m}$ mit $n \in \mathbb{Z}$, $m \in \mathbb{Z}$, $\mathrm{ggT}(n,m)=1$, so folgt

$$\frac{a}{c} = \frac{1-(\frac{n}{m})^2}{1+(\frac{n}{m})^2} = \frac{m^2-n^2}{m^2+n^2} \quad \text{und} \quad \frac{b}{c} = \frac{2\cdot\frac{n}{m}}{1+(\frac{n}{m})^2} = \frac{2mn}{m^2+n^2}.$$

Definiert man q durch $c = q\cdot(m^2+n^2)$, so folgt

$$a = q\cdot(m^2-n^2), \quad b = q\cdot 2mn, \quad c = q\cdot(m^2+n^2),$$

wie behauptet.

(2) Zur Eindeutigkeit: Gilt $a = q\cdot(m^2-n^2)$, $b = q\cdot 2mn$, $c = q\cdot(m^2+n^2)$, so folgt

$$\frac{b}{a+c} = \frac{q\cdot 2mn}{q\cdot(m^2-n^2)+q\cdot(m^2+n^2)} = \frac{n}{m}.$$

Durch die Forderung $n \in \mathbb{Z}$, $m \in \mathbb{N}$ und $\mathrm{ggT}(n,m)=1$ sind daher n und m und damit natürlich auch q eindeutig bestimmt.

(3) $a^2+b^2=c^2$ rechnet man sofort nach. Wegen $a+c = 2qm^2$ folgt auch $c \neq -a$. ■

SATZ (Pythagoräische Tripel). (1) *Sind* $a, b, c \in \mathbb{N}$ *mit* $a^2 + b^2 = c^2$ *mit* $\mathrm{ggT}(a, b, c) = 1$*, definiert man* $m, n \in \mathbb{N}$ *durch* $\frac{b}{a+c} = \frac{n}{m}$ *mit* $\mathrm{ggT}(m, n) = 1$ *und* k *durch* $k = \begin{cases} 1, & \text{falls } m \not\equiv n \bmod 2, \\ 2, & \text{falls } m \equiv n \bmod 2, \end{cases}$ *so gilt* $m > n$ *und*

$$a = \frac{m^2 - n^2}{k}, \quad b = \frac{2mn}{k}, \quad c = \frac{m^2 + n^2}{k}.$$

$(m, n, k$ sind durch die angegebene Darstellung eindeutig bestimmt.)

(2) *Sind* $m, n \in \mathbb{N}$ *mit* $m > n$ *und* $\mathrm{ggT}(m, n) = 1$*, ist* $k = \begin{cases} 1, & \text{falls } m \not\equiv n \bmod 2, \\ 2, & \text{falls } m \equiv n \equiv 1 \bmod 2, \end{cases}$ *so erfüllen die Zahlen*

$$a = \frac{m^2 - n^2}{k}, \quad b = \frac{2mn}{k}, \quad c = \frac{m^2 + n^2}{k}$$

die Bedingungen $a, b, c \in \mathbb{N}$*,* $a^2 + b^2 = c^2$ *und* $\mathrm{ggT}(a, b, c) = 1$*.*

Beweis:

(1) Seien also $a, b, c \in \mathbb{N}$ mit $a^2 + b^2 = c^2$. Der vorangegangene Satz liefert dann eindeutig bestimmte Zahlen $n \in \mathbb{Z}$, $m \in \mathbb{N}$, $\ell \in \mathbb{Z}$, $k \in \mathbb{N}$ mit $\mathrm{ggT}(n, m) = 1$ und $\mathrm{ggT}(\ell, k) = 1$, sodass gilt

$$a = \frac{\ell}{k} \cdot (m^2 - n^2), \quad b = \frac{\ell}{k} \cdot 2mn, \quad c = \frac{\ell}{k} \cdot (m^2 + n^2).$$

Wir haben dann

$$ka = \ell \cdot (m^2 - n^2), \quad kb = \ell \cdot 2mn, \quad kc = \ell \cdot (m^2 + n^2).$$

Wegen $c \in \mathbb{N}$ folgt $\ell \in \mathbb{N}$. Wegen $\ell \mid a, b, c$ folgt $\ell = 1$. Daher gilt nun

$$ka = m^2 - n^2, \quad kb = 2mn, \quad kc = m^2 + n^2.$$

Es folgt $k \mid 2m^2$, $k \mid 2n^2$, also $k \mid \mathrm{ggT}(2m^2, 2n^2)$. Mit $ggT(m, n) = 1$ ergibt sich $k \in \{1, 2\}$. Ist $m \not\equiv n \bmod 2$, so ist $m^2 - n^2$ ungerade und es muss $k = 1$ gelten. Ist dagegen $m \equiv n \bmod 2$, so sind alle Zahlen $m^2 - n^2, 2mn, m^2 + n^2$ gerade und es muss $k = 2$ gelten. Dies zeigt die Behauptung.

(2) $a, b, c \in \mathbb{N}$, $a^2 + b^2 = c^2$ sieht man direkt. $\mathrm{ggT}(a, b, c) = 1$ sieht man mit den Überlegungen aus dem ersten Teil des Beweises. ■

SATZ (Pythagoräische Tripel). *Sei*

$$P = \{(a, b, c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} : a^2 + b^2 = c^2, \mathrm{ggT}(a, b, c) = 1\}$$

die Menge der primitiven pythagoräischen Tripel. Dann ist

$$\alpha : P \to \mathbb{Q}_{>1}, \quad (a, b, c) \mapsto \frac{a + c}{b}$$

bijektiv mit Umkehrabbildung

$$\beta : \mathbb{Q}_{>1} \to P, \quad \frac{m}{n} \mapsto \left(\frac{m^2 - n^2}{\mathrm{ggT}(2, m - n)}, \frac{2mn}{\mathrm{ggT}(2, m - n)}, \frac{m^2 + n^2}{\mathrm{ggT}(2, m, n)} \right),$$

wobei $\mathrm{ggT}(m, n) = 1$ *und* $m, n \in \mathbb{N}$ *gewählt sei.*

Beispiele: Hier sind alle primitiven pythagoräischen Tripel (a, b, c) mit $c \leq 100$. Es gibt 16 Stück.

(a, b, c)	$\alpha((a, b, c))$
$(3, 4, 5)$	2
$(4, 3, 5)$	3
$(5, 12, 13)$	$\frac{3}{2}$
$(12, 5, 13)$	5
$(8, 15, 17)$	$\frac{5}{3}$
$(15, 8, 17)$	4
$(7, 24, 25)$	$\frac{4}{3}$
$(24, 7, 25)$	7
$(20, 21, 29)$	$\frac{7}{3}$
$(21, 20, 29)$	$\frac{5}{2}$
$(12, 35, 37)$	$\frac{7}{5}$
$(35, 12, 37)$	6
$(9, 40, 41)$	$\frac{5}{4}$
$(40, 9, 41)$	9
$(28, 45, 53)$	$\frac{9}{5}$
$(45, 28, 53)$	$\frac{7}{2}$

(a, b, c)	$\alpha((a, b, c))$
$(11, 60, 61)$	$\frac{6}{5}$
$(60, 11, 61)$	11
$(16, 63, 65)$	$\frac{9}{7}$
$(33, 56, 65)$	$\frac{7}{4}$
$(56, 33, 65)$	$\frac{11}{3}$
$(63, 16, 65)$	8
$(48, 55, 73)$	$\frac{11}{5}$
$(55, 48, 73)$	$\frac{8}{3}$
$(13, 84, 85)$	$\frac{7}{6}$
$(36, 77, 85)$	$\frac{11}{7}$
$(77, 36, 85)$	$\frac{9}{2}$
$(84, 13, 85)$	13
$(39, 80, 89)$	$\frac{8}{5}$
$(80, 39, 89)$	$\frac{13}{3}$
$(65, 72, 97)$	$\frac{9}{4}$
$(72, 65, 97)$	$\frac{13}{5}$

Nun haben wir für alle rationalen Zahlen $\frac{m}{n} \in \mathbb{Q}_{>1}$ mit $\mathrm{ggT}(m, n) = 1$ und $m \leq 10$ die zugehörigen Tripel $\beta(\frac{m}{n})$ bestimmt:

$\frac{m}{n}$	$\beta(\frac{m}{n})$
2	$(3, 4, 5)$
3	$(4, 3, 5)$
$\frac{3}{2}$	$(5, 12, 13)$
4	$(15, 8, 17)$
$\frac{4}{3}$	$(7, 24, 25)$
5	$(12, 5, 13)$
$\frac{5}{2}$	$(21, 20, 29)$
$\frac{5}{3}$	$(8, 15, 17)$
$\frac{5}{4}$	$(9, 40, 41)$
6	$(35, 12, 37)$
$\frac{6}{5}$	$(11, 60, 61)$
7	$(24, 7, 25)$
$\frac{7}{2}$	$(45, 28, 53)$
$\frac{7}{3}$	$(20, 21, 29)$
$\frac{7}{4}$	$(33, 56, 65)$
$\frac{7}{5}$	$(12, 35, 37)$

$\frac{m}{n}$	$\beta(\frac{m}{n})$
$\frac{7}{6}$	$(13, 84, 85)$
8	$(63, 16, 65)$
$\frac{8}{3}$	$(55, 48, 73)$
$\frac{8}{5}$	$(39, 80, 89)$
$\frac{8}{7}$	$(15, 112, 113)$
9	$(40, 9, 41)$
$\frac{9}{2}$	$(77, 36, 85)$
$\frac{9}{4}$	$(65, 72, 97)$
$\frac{9}{5}$	$(28, 45, 53)$
$\frac{9}{7}$	$(16, 63, 65)$
$\frac{9}{8}$	$(17, 144, 145)$
10	$(99, 20, 101)$
$\frac{10}{3}$	$(91, 60, 109)$
$\frac{10}{7}$	$(51, 140, 149)$
$\frac{10}{9}$	$(19, 180, 181)$

FOLGERUNG. *Ist (a, b, c) ein primitives pythagoräisches Tripel, d.h. $(a, b, c) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ mit $a^2 + b^2 = c^2$ und $\mathrm{ggT}(a, b, c) = 1$, so gilt:*

$$(a, b, c) \equiv (1, 0, 1), (3, 0, 1), (0, 1, 1), (0, 3, 1) \bmod 4,$$

was auch folgendermaßen ausgedrückt werden kann:

- *Es ist* $c \equiv 1 \bmod 4$.
- *Entweder gilt* $a \equiv 1 \bmod 2$, $b \equiv 0 \bmod 4$ *oder* $a \equiv 0 \bmod 4$, $b \equiv 1 \bmod 2$.

Beweis: Ist $\alpha((a,b,c)) = \frac{m}{n}$ mit $m, n \in \mathbb{N}$, $m > n$, $\mathrm{ggT}(m,n) = 1$, so ist

$$a = \frac{m^2 - n^2}{\mathrm{ggT}(2, m-n)}, \quad b = \frac{2mn}{\mathrm{ggT}(2, m-n)}, \quad c = \frac{m^2 + n^2}{\mathrm{ggT}(2, m-n)}.$$

Wir unterscheiden zwei Fälle:

- **Fall** $m \not\equiv n \bmod 2$**:** Dann ist

  $$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

  Ist $m \equiv 1 \bmod 2$, $n \equiv 0 \bmod 2$, so folgt

  $$a \equiv 1 \bmod 4, \quad b \equiv 0 \mod 4, \quad c \equiv 1 \bmod 4.$$

  Ist $m \equiv 0 \bmod 2$, $n \equiv 1 \bmod 2$, so folgt

  $$a \equiv 3 \bmod 4, \quad b \equiv 0 \bmod 2, \quad c \equiv 1 \bmod 4.$$

- **Fall** $m \equiv n \bmod 2$**:** Wegen $\mathrm{ggT}(m,n) = 1$ gilt dann $m \equiv n \equiv 1 \bmod 2$. Damit ist

  $$a = \frac{m^2 - n^2}{2}, \quad b = mn, \quad c = \frac{m^2 + n^2}{2}.$$

  Es ist $b \equiv 1 \bmod 2$. Aus $m^2 \equiv n^2 \equiv 1 \bmod 8$ folgt $m^2 - n^2 \equiv 0 \bmod 8$ und damit

  $$a = \frac{m^2 - n^2}{2} \equiv 0 \bmod 4$$

  und analog $m^2 + n^2 \equiv 2 \bmod 8$ und damit

  $$c = \frac{m^2 + n^2}{2} \equiv 1 \bmod 4.$$

Damit ist alles gezeigt. ■

Die Fermat-Gleichung: Für $n \geq 3$ hat die Gleichung

$$a^n + b^n = c^n \quad \text{mit} \quad a, b, c \in \mathbb{N}$$

keine Lösung. Diese wurde von Fermat behauptet, von Wiles (1995) bewiesen. (Der Beweis ist nichttrivial.) Gilt $a^n + b^n = c^n$, so folgt $(\frac{a}{c})^n + (\frac{b}{c})^n = 1$, also hat man das Problem, nach Punkten mit rationalen Koordinaten auf der Kurve

$$x^n + y^n = 1$$

zu suchen. (Auch hier gibt es triviale Lösungen, beispielsweise $(x,y) = (1,0)$.)

Kongruenzzahlen: Eine natürliche Zahl N heißt **Kongruenzzahl**, wenn sie Flächeneinhalt eines rechtwinkligen Dreiecks mit rationalen Seitenlängen ist, d.h. wenn es $a, b, c \in \mathbb{Q}_{>0}$ gibt mit

$$N = \frac{1}{2}ab \quad \text{und} \quad a^2 + b^2 = c^2.$$

Beispielsweise ist 6 eine Kongruenzzahl, weil $6 = \frac{1}{2} \cdot 3 \cdot 4$ und $3^2 + 4^2 = 5^2$ gilt.
Ist N eine Kongruenzzahl mit $N = \frac{1}{2}ab$ und $a^2 + b^2 = c^2$, sind $r, s \in \mathbb{N}$, so gilt $N\frac{r^2}{s^2} = \frac{1}{2} \cdot \frac{r}{s}a \cdot \frac{r}{s}b$ und $(\frac{r}{s}a)^2 + (\frac{r}{s}b)^2 = (\frac{r}{s}c)^2$. Ist also $N\frac{r^2}{s^2} \in \mathbb{N}$, so ist dies ebenfalls eine Kongruenzzahl. Daher kann man sich auf die Betrachtung quadratfreier Zahlen beschränken.

Satz. (1) *Ist* N *eine quadratfreie Kongruenzzahl, so gibt es* $m, n, k \in \mathbb{N}$ *mit* $\mathrm{ggT}(m,n) = 1$, $m > n$ *und*

$$N = \frac{(m^2 - n^2)mn}{k^2}.$$

(2) *Sind $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ und $m > n$ und zerlegt man $(m^2 - n^2)mn$ in ein Quadrat k^2 und einen quadratfreien Teil N, also*

$$(m^2 - n^2)mn = Nk^2,$$

so ist N eine quadratfreie Kongruenzzahl. Ein zugehöriges rechtwinkliges Dreieck mit passenden Seitenlängen wird gegeben durch

$$a = \frac{m^2 - n^2}{k}, \quad b = \frac{2mn}{k}, \quad c = \frac{m^2 + n^2}{k}.$$

Beweis:

(1) Sei N eine Kongruenzzahl, d.h. $N = \frac{1}{2}ab$ und $a^2 + b^2 = c^2$. Dann gibt es eine Darstellung

$$a = \frac{\ell}{k} \cdot (m^2 - n^2), \quad b = \frac{\ell}{k} \cdot 2mn, \quad c = \frac{\ell}{k} \cdot (m^2 + n^2),$$

wobei wir offensichtlich $m, n \in \mathbb{N}$, $m > n$, $\mathrm{ggT}(m,n) = 1$ und $\ell, k \in \mathbb{N}$, $\mathrm{ggT}(\ell, k) = 1$ annehmen können. Wir haben dann

$$N = \frac{1}{2}ab = \frac{\ell^2}{k^2}(m^2 - n^2)mn \quad \text{und} \quad Nk^2 = \ell^2(m^2 - n^2)mn.$$

Da N quadratfrei sein soll, muss $\ell = 1$ gelten, was die Behauptung liefert.

(2) Man sieht, dass $a^2 + b^2 = c^2$, $a, b, c \in \mathbb{Q}_{>0}$ und $N = \frac{1}{2}ab$ gilt. Nach Konstruktion ist N quadratfrei, was dann die Behauptung beweist. ■

Bemerkung: Mit dem vorangegangenen Satz kann man Kongruenzahlen konstruieren: Man lässt m und n laufen, zerlegt $(m^2 - n^2)mn = Nk^2$ mit quadratfreiem N. Dann ist N eine Kongruenzzahl.

Beispiel: Wir wählen $m = 2019$ und $n = 1000$. Dann gilt mit den Bezeichnungen des vorangegangenen Satzes

$$\begin{aligned} Nk^2 &= (m^2 - n^2)mn = 6211172859000 = 2^3 \cdot 3 \cdot 5^3 \cdot 673 \cdot 1019 \cdot 3019 = \\ &= (2 \cdot 3 \cdot 5 \cdot 673 \cdot 1019 \cdot 3019) \cdot (2 \cdot 5)^2 = 62111728590 \cdot 10^2. \end{aligned}$$

Daher ist

$$N = 62111728590$$

eine (quadratfreie) Kongruenzzahl. Ein zugehöriges rechtwinkliges Dreieck mit Flächeninhalt N hat die Seitenlängen

$$a = \frac{m^2 - n^2}{k} = \frac{3076361}{10}, \quad b = \frac{2mn}{k} = 403800, \quad c = \frac{m^2 + n^2}{k} = \frac{5076361}{10}.$$

Beispiele: Nach dem eben beschriebenen Verfahren haben wir m bis 1000 laufen lassen. Dabei wurden folgende quadratfreien Kongruenzzahlen $N \leq 50$ gefunden:

N	a	b	c	k	m	n
5	$\frac{20}{3}$	$\frac{3}{2}$	$\frac{41}{6}$	12	9	1
5	$\frac{3}{2}$	$\frac{20}{3}$	$\frac{41}{6}$	6	5	4
6	3	4	5	1	2	1
6	4	3	5	2	3	1
6	$\frac{120}{7}$	$\frac{7}{10}$	$\frac{1201}{70}$	140	49	1
6	$\frac{7}{10}$	$\frac{120}{7}$	$\frac{1201}{70}$	70	25	24
7	$\frac{24}{5}$	$\frac{35}{12}$	$\frac{337}{60}$	120	25	7
7	$\frac{35}{12}$	$\frac{24}{5}$	$\frac{337}{60}$	60	16	9
13	$\frac{323}{30}$	$\frac{780}{323}$	$\frac{106921}{9690}$	9690	325	36
13	$\frac{780}{323}$	$\frac{323}{30}$	$\frac{106921}{9690}$	19380	361	289
14	$\frac{21}{2}$	$\frac{8}{3}$	$\frac{65}{6}$	6	8	1
14	$\frac{8}{3}$	$\frac{21}{2}$	$\frac{65}{6}$	12	9	7
15	4	$\frac{15}{2}$	$\frac{17}{2}$	4	5	3
15	$\frac{15}{2}$	4	$\frac{17}{2}$	2	4	1
15	$\frac{161}{68}$	$\frac{2040}{161}$	$\frac{141121}{10948}$	10948	289	240
15	$\frac{2040}{161}$	$\frac{161}{68}$	$\frac{141121}{10948}$	21896	529	49
21	12	$\frac{7}{2}$	$\frac{25}{2}$	4	7	1
21	$\frac{4200}{527}$	$\frac{527}{100}$	$\frac{503521}{52700}$	105400	961	289
21	$\frac{527}{100}$	$\frac{4200}{527}$	$\frac{503521}{52700}$	52700	625	336
21	$\frac{7}{2}$	12	$\frac{25}{2}$	2	4	3
22	$\frac{140}{3}$	$\frac{33}{35}$	$\frac{4901}{105}$	210	99	1
22	$\frac{33}{35}$	$\frac{140}{3}$	$\frac{4901}{105}$	105	50	49
30	12	5	13	2	5	1
30	5	12	13	1	3	2
30	$\frac{119}{26}$	$\frac{1560}{119}$	$\frac{42961}{3094}$	3094	169	120
30	$\frac{1560}{119}$	$\frac{119}{26}$	$\frac{42961}{3094}$	6188	289	49
34	24	$\frac{17}{6}$	$\frac{145}{6}$	12	17	1
34	$\frac{112}{9}$	$\frac{153}{28}$	$\frac{3425}{252}$	504	81	17
34	$\frac{136}{15}$	$\frac{15}{2}$	$\frac{353}{30}$	60	25	9
34	$\frac{15}{2}$	$\frac{136}{15}$	$\frac{353}{30}$	30	17	8
34	$\frac{153}{28}$	$\frac{112}{9}$	$\frac{3425}{252}$	252	49	32
34	$\frac{17}{6}$	24	$\frac{145}{6}$	6	9	8
34	$\frac{3927}{248}$	$\frac{992}{231}$	$\frac{939905}{57288}$	57288	961	128
39	$\frac{156}{5}$	$\frac{5}{2}$	$\frac{313}{10}$	20	25	1
39	$\frac{5}{2}$	$\frac{156}{5}$	$\frac{313}{10}$	10	13	12
41	$\frac{1189}{420}$	$\frac{840}{29}$	$\frac{354481}{12180}$	12180	441	400
41	$\frac{123}{20}$	$\frac{40}{3}$	$\frac{881}{60}$	60	25	16
41	$\frac{40}{3}$	$\frac{123}{20}$	$\frac{881}{60}$	120	41	9
41	$\frac{840}{29}$	$\frac{1189}{420}$	$\frac{354481}{12180}$	24360	841	41
46	$\frac{168}{11}$	$\frac{253}{42}$	$\frac{7585}{462}$	924	121	23
46	$\frac{253}{42}$	$\frac{168}{11}$	$\frac{7585}{462}$	462	72	49

(Es gibt aber noch mehr quadratfreie Kongruenzzahlen ≤ 50, nämlich: 5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47.)

Bemerkung: Ist N Kongruenzzahl, so kann es mehrere zugehörige rechtwinklige Dreiecke geben. Beispielsweise haben folgende rechtwinkligen Dreiecke alle den Flächeninhalt 6: $(a, b, c) = (3, 4, 5)$ und $(a, b, c) = (\frac{7}{10}, \frac{120}{7}, \frac{1201}{70})$.

Das folgende Lemma liefert ein Kriterium, ob eine natürliche Zahl N eine Kongruenzzahl ist:

LEMMA. *Sei* $N \in \mathbb{N}$.

(1) *Ist N Kongruenzzahl, d.h. gibt es $a, b, c \in \mathbb{Q}_{>0}$ mit $a^2 + b^2 = c^2$ und $N = \frac{1}{2}ab$, so erfüllen die Punkte*

$$(x_1, y_1) = (\frac{1}{2}a(a+c), \frac{1}{2}a^2(a+c)), \quad (x_2, y_2) = (\frac{1}{2}a(a-c), \frac{1}{2}a^2(a-c)),$$

$$(x_3, y_3) = (\frac{1}{2}b(b+c), \frac{1}{2}b^2(b+c)), \quad (x_4, y_4) = (\frac{1}{2}b(b-c), \frac{1}{2}b^2(b-c))$$

die Gleichung

$$y^2 = x^3 - N^2x$$

und es gilt $y_i \neq 0$.

(2) *Ist $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ mit $y^2 = x^3 - N^2x$ und $y \neq 0$, definiert man*

$$a = \frac{|y|}{|x|}, \quad b = \frac{2N|x|}{|y|}, \quad c = \frac{x^2 + N^2}{|y|},$$

so gilt

$$a^2 + b^2 = c^2, \quad a, b, c \in \mathbb{Q}_{>0} \quad \text{und} \quad N = \frac{1}{2}ab,$$

d.h. N ist eine Kongruenzzahl.

Beweis:

(1) Dies rechnet man einfach nach unter Benutzung der Gleichung $a^2 + b^2 = c^2$.

(2) Es gilt

$$\begin{aligned} a^2 + b^2 &= \frac{y^2}{x^2} + \frac{4N^2x^2}{y^2} = \frac{1}{y^2}\left(\frac{(y^2)^2}{x^2} + 4N^2x^2\right) = \frac{1}{y^2}\left(\frac{(x(x^2 - N^2))^2}{x^2} + 4N^2x^2\right) = \\ &= \frac{1}{y^2}\left((x^2 - N^2)^2 + 4N^2x^2\right) = \frac{1}{y^2}\left(x^4 - 2N^2x^2 + N^4 + 4N^2x^2\right) = \\ &= \frac{1}{y^2}\left(x^2 + N^2\right)^2 = c^2 \end{aligned}$$

und

$$N = \frac{1}{2}ab.$$

Wegen $a, b, c \in \mathbb{Q}_{>0}$ ist N eine Kongruenzzahl. ■

Bemerkung: Für $N \in \mathbb{N}$ definiert die Gleichung $y^2 = x^3 - N^2x$ eine sogenannte elliptische Kurve, die die „trivialen“ Puntke $(0, 0)$, $(N, 0)$, $(-N, 0)$ enthält. Das Lemma besagt, dass N genau dann eine Kongruenzzahl ist, wenn die angegebene Kurve nicht nur die angegebenen trivialen rationalen Punkte enthält. Aufbauend auf der Theorie der elliptischen Kurven gelang es Tunnell 1983, ein numerisch einfach überprüfbares Kriterium für eine Kongruenzzahl anzugeben. Dabei geht teilweise eine bis jetzt noch nicht bewiesene Vermutung (Birch-Swinnerton-Dyer-Vermutung) ein.

Wir behandeln noch ein paar Gleichungen.

Beispiel: $f = 2x^2 + 3y^2 + 5$. Man sieht sofort, dass $f = 0$ keine reellen, also erst recht keine rationalen Lösungen besitzt.

Beispiel: Sei $f = 2x^2 + 3y^2 - 1$ Offensichtlich ist

$$X_{\mathbb{R}} = \{(x, y) \in \mathbb{R}^2 : f(x, y) = 0\} \neq \emptyset;$$

$X_{\mathbb{R}}$ ist eine Ellipse im $\mathbb{R}^2$. Man sieht weiter:

$$X_{\mathbb{R}} \subseteq \{(x, y) \in \mathbb{R}^2 : |x| \leq \frac{1}{\sqrt{2}}, |y| \leq \frac{1}{\sqrt{3}}\},$$

woraus man sofort $X_{\mathbb{Z}} = \{(x, y) \in \mathbb{Z}^2 : f(x, y) = 0\} = \emptyset$ sieht. Wir wollen nun $X_{\mathbb{Q}} = \{(x, y) \in \mathbb{Q}^2 : f(x, y) = 0\}$ bestimmen. Wir setzen an $x = \frac{X}{Z}, y = \frac{Y}{Z}$ mit $X, Y \in \mathbb{Z}$, $Z \in \mathbb{N}$ und erhalten die Gleichung $g = 2X^2 + 3Y^2 - Z^2 = 0$. Hier müssen wir die ganzzahligen Lösungen bestimmen. Wir können $ggT(X, Y, Z) = 1$ annehmen, da die Gleichung homogen ist. Betrachtung modulo 3 liefert $X \equiv Z \equiv$

0 mod 3, d.h. $X = 3X_1, Z = 3Z_1$. Setzt man dies in $g = 0$ ein, so erhält man sofort $Y \equiv 0 \bmod 3$, also $Y = 3Y_1$, ein Widerspruch zu $ggT(X, Y, Z) = 1$. Also erhalten wir $X_{\mathbb{Q}} = \emptyset$.

Bemerkung: Wir wollen das Phänomen des letzten Beispiels etwas abstrakter formulieren: Sind $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_n]$ und definieren wir

$$X_{\mathbb{Z}} = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n : f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0\}$$

und für $N \in \mathbb{N}$ $X = \{f_1 = \cdots = f_r = 0\}$ mit ganzzahligen Polynomen $f_1, \ldots, f_r$

$$X_{\mathbb{Z}/N\mathbb{Z}} = \{(a_1, \ldots, a_n) \in (\mathbb{Z}/N\mathbb{Z})^n : f_1(a_1, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0\},$$

so erhält man durch Reduktion modulo N eine Abbildung $X_{\mathbb{Z}} \to X_{\mathbb{Z}/N\mathbb{Z}}$. Durch geschickte Wahl von N kann man manchmal Aussagen über $X_{\mathbb{Z}}$ erhalten. $X_{\mathbb{Z}/N\mathbb{Z}}$ ist eine endliche Menge. Ist $X_{\mathbb{Z}/N\mathbb{Z}} = \emptyset$, so auch $X_{\mathbb{Z}} = \emptyset$. Doch auch in anderen Fällen kann man manchmal Rückschlüsse ziehen aus obiger Abbildung. (Siehe voriges Beispiel.)

Beispiel: Sei $f = 2x^2 + 3y^2 - 5$. Man sieht schnell, dass $X_{\mathbb{Z}} = \{(x, y) \in \mathbb{Z}^2 : f(x, y) = 0\} = \{(\pm 1, \pm 1)\}$ gilt. Um die rationalen Punkte, also $X_{\mathbb{Q}} = \{(x, y) \in \mathbb{Q}^2 : f(x, y) = 0\}$ zu berechnen, legen wir eine Gerade mit Steigung t durch den bereits bekannten Punkt $(1, 1)$ (Geradengleichung $\frac{y-1}{x-1} = t$) und schneiden mit der Kurve $f = 0$, indem wir $y = 1 + t(x - 1)$ in $f = 0$ einsetzen: $2x^2 + 3(1 + t(x - 1))^2 - 5 = 0$. Dies ist eine quadratische Gleichung in x, wobei wir eine Lösung $x = 1$ bereits kennen, also sollte sich die zweite auch leicht bestimmen lassen:

$$2x^2 + 3(1 + t(x - 1))^2 - 5 = (x - 1)[(3t^2 + 2)x - (3t^2 - 6t - 2)].$$

Die zwei Schnittpunkte der Geraden mit $f = 0$ sind also $x = 1, y = 1$ und

$$x = \frac{3t^2 - 6t - 2}{3t^2 + 2}, \quad y = \frac{-3t^2 - 4t + 2}{3t^2 + 2}.$$

Damit hat man alle rationalen Lösungen parametrisiert gegeben:

$$X_{\mathbb{Q}}) = \{(\frac{3t^2 - 6t - 2}{3t^2 + 2}, \frac{-3t^2 - 4t + 2}{3t^2 + 2}) : t \in \mathbb{Q}\} \cup \{(1, 1), (1, -1)\}.$$

Bemerkung: Hat man eine quadratische Gleichung $f(x, y) = 0$ und einen Punkt $P = (x_0, y_0) \in \mathbb{Q}^2$ mit $f(P) = 0$, so kann man obiges Verfahren immer anwenden.

Beispiel: $f = 2x^2 - 3y^2 + 1$. Man sieht sofort $(1, 1) \in X_{\mathbb{Z}} = \{(x, y) \in \mathbb{Z}^2 : f(x, y) = 0\}$. Wie eben findet man eine Parametrisierung

$$x = \frac{3t^2 - 6t + 2}{3t^2 - 2}, \quad y = \frac{-3t^2 + 4t - 2}{3t^2 - 2},$$

womit man direkt $X_{\mathbb{Q}} = \{(x, y) \in \mathbb{Q}^2 : f(x, y) = 0\}$ angeben kann. $X_{\mathbb{R}} = \{(x, y) \in \mathbb{R}^2 : f(x, y) = 0\}$ ist eine Hyperbel im $\mathbb{R}^2$, woraus man noch keine Abschätzung für die ganzzahligen Lösungen erhält. Im Bereich $|x| \leq 10^6$ erhält man durch Computersuche folgende ganzzahlige Lösungen:

$$(\pm x, \pm y) = (1, 1), (11, 9), (109, 89), (1079, 881), (10681, 8721), (105731, 86329).$$

Wir skizzieren eine Möglichkeit, wie man weiter vorgehen kann: Wir formen die Gleichung etwas um: $(2x)^2 - 6y^2 = -2$. In $\mathbb{Z}[\sqrt{6}]$ suchen wir Elemente der Norm -2. Nun ist der Ring Hauptidealring mit $5 + 2\sqrt{6}$ Grundeinheit. Es zeigt sich, dass die gesuchten Elemente $(2 + \sqrt{6})(5 + 2\sqrt{6})^n$ mit $n \geq 0$, d.h. durch

$$2x_n + y_n\sqrt{6} = (2 + \sqrt{6})(5 + 2\sqrt{6})^n$$

gegeben werden. Eine mögliche Darstellung ist

$$x_n = \frac{1}{4}[(2+\sqrt{6})(5+2\sqrt{6})^n + (2-\sqrt{6})(5-2\sqrt{6})^n], \quad y_n = \frac{1}{2\sqrt{6}}[(2+\sqrt{6})(5+2\sqrt{6})^n - (2-\sqrt{6})(5-2\sqrt{6})^n].$$

Beispiel: Sei $f = 1 + 2x - 4x^2y + 2y^3 - 5x^3$. Durch Probieren findet man $(1, -1) \in X_{\mathbb{Q}} = \{(x, y) \in \mathbb{Q}^2 : f(x, y) = 0\}$. Wie findet man weitere Punkte?
Hier gibt es das sogenannte Tangentenverfahren: Man schneidet die Tangente durch einen bekannten

Kurvenpunkt mit der Kurve. Die Tangente in $(1,-1)$ ist $f_x(1,-1)(x-1)+f_y(1,-1)(y+1)=0$, d.h. $y=\frac{5}{2}x-\frac{7}{2}$. Eingesetzt in f liefert dies

$$\frac{1}{4}(x-1)^2(65x-339),$$

woraus sich ein weiterer Schnittpunkt der Tangente mit der Kurve berechnet, nämlich $(x_1,y_1)=(\frac{339}{65},\frac{124}{13})$. Iteriert man dies, so erhält man eine Folge rationaler Punkte auf der Kurve:

$$\begin{aligned}
(x_0,y_0) &= (1,-1)\\
(x_1,y_1) &= (\frac{339}{65},\frac{124}{13})\\
(x_2,y_2) &= (-\frac{27392369757513}{66208265164861},-\frac{53999274824480}{66208265164861})\\
(x_3,y_3) &= (\frac{17558528443800805877782634909216083780845793937763395128 9}{24391974589498597212762103572800691406098852620368901790 59},\\
&\qquad \frac{74266370155643503338932738126835386128126623766195740951 2}{24391974589498597212762103572800691406098852620368901790 59})
\end{aligned}$$

Ist h_n der Logarithmus des Zählers von x_n, so findet man

$$h_0=0,\quad h_1=4.17,\quad h_2=31.82,\quad h_3=132.14,\quad h_4=534.55,\quad h_5=2139.84$$

und

$$\frac{h_2}{h_1}=7.624,\quad \frac{h_3}{h_2}=4.152,\quad \frac{h_4}{h_3}=4.045,\quad \frac{h_5}{h_4}=4.003.$$

Beispiel: Sei $f=-5+x+2x^4+2y^3+4y^4$ und $X_{\mathbb{Z}}=\{(x,y)\in\mathbb{Z}^2 : f(x,y)=0\}$. Man findet $(1,-1)\in X_{\mathbb{Q}}$. Die Menge $X_{\mathbb{R}}=\{(x,y)\in\mathbb{R}^2 : f(x,y)=0\}$ ist beschränkt im $\mathbb{R}^2$, woraus sich dann $X_{\mathbb{Z}}=\{(1,-1)\}$ ergibt. Kann man mit dem Tangentenverfahren weitere rationale Punkte konstruieren? Leider funktioniert das Tangentenverfahren hier nicht mehr: die Tangente in $(1,-1)$ ist $y=\frac{9}{10}x-\frac{19}{10}$, eingesetzt in f liefert die Gleichung

$$\frac{1}{2500}(x-1)^2(11561x^2-28637x+83526)=0.$$

Die quadratische Gleichung hat aber keine rationalen Lösungen.

Wir schließen mit ein paar Bemerkungen:

Ziele bzw. Ergebnisse: Sei $f(x,y)\in\mathbb{Z}[x,y]$ ein *schönes* Polynom vom Grad d und $X_{\mathbb{Z}}=\{(x,y)\in\mathbb{Z}^2 : f(x,y)=0\}$ und $X_{\mathbb{Q}}=\{(x,y)\in\mathbb{Q}^2 : f(x,y)=0\}$. Dann gilt:

- $d=3$:
  - $\#X_{\mathbb{Z}}<\infty$ (Siegel 1929).
  - Ist $X_{\mathbb{Q}}\neq\emptyset$, so besitzt $X_{\mathbb{Q}}$ die Struktur einer endlich erzeugten abelschen Gruppe (Mordell 1922).
- $d\geq 4$:
  - $\#X_{\mathbb{Z}}<\infty$ (Siegel 1929).
  - $\#X_{\mathbb{Q}}<\infty$ (Vermutung von Mordell 1922, bewiesen von Faltings 1983).