KAPITEL 1

Einführung

Mit der Erfindung der kartesischen Koordinaten durch Descartes und Fermat in der ersten Hälfte des 17. Jahrhunderts wurde es möglich, geometrische Fragestellungen algebraisch zu formulieren und mit den Methoden der Algebra zu behandeln. Heutzutage lernt man bereits in der Schule, wie man einfache geometrische Gebilde wie Geraden, Parabeln, Ebenen und Kugeln durch Gleichungen beschreibt.
In der Algebraischen Geometrie studiert man nun allgemein Lösungsmengen polynomialer Gleichungen. Dazu gehören geometrische Objekte, aber auch diophantische Gleichungen.

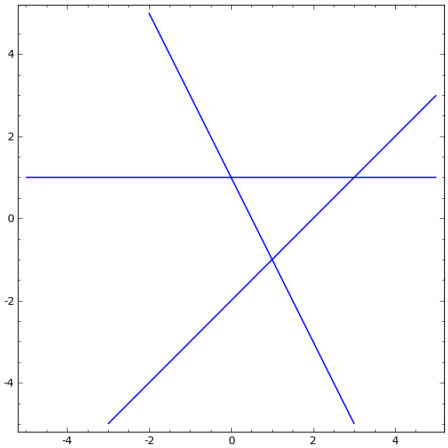
Ausgangspunkt der algebraischen Geometrie sind folgende Situationen:

- Man übersetzt geometrische Aufgabenstellungen in algebraische Gleichungen und versucht sie zu lösen.
- Man deutet algebraische Gleichungen geometrisch und versucht sie auf diese Weise besser zu verstehen.

Bevor wir richtig beginnen, wollen wir zwei einfache Beispiele für das fruchtbare Zusammenwirken von Geometrie und Algebra geben.

Beispiel: Gegeben seien die drei Geraden

$$y = x - 2, \quad y = -2x + 1, \quad y = 1.$$



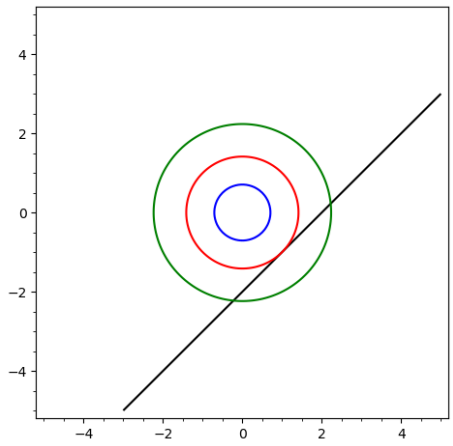
Bestimmt werden sollen alle Kreise, die alle drei Geraden berühren.

- Ein Kreis $K_r(u, v)$ mit Mittelpunkt (u, v) und Radius r wird beschrieben durch die Gleichung

$$(x - u)^2 + (y - v)^2 = w \quad \text{mit} \quad w = r^2.$$

Datei: algku1.tex. Version vom 19.7.2021

Ein Kreis und eine Gerade können sich in keinem Punkt, einem Punkt oder zwei Punkten schneiden, wie die folgende Skizze zeigt.



- **Erinnerung:** Die Diskriminante einer quadratischen Gleichung

$$ax^2 + bx + c = 0 \text{ mit } a, b, c \in \mathbb{R} \text{ und } a \neq 0$$

ist definiert als

$$D = b^2 - 4ac.$$

Es gibt drei Fälle:
  - Fall $D > 0$: Die quadratische Gleichung hat die zwei (verschiedenen) reellen Lösungen

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a}.$$

  - Fall $D = 0$: Die quadratische Gleichung hat genau eine Lösung, nämlich

$$x = \frac{-b}{2a}.$$

  - Fall $D < 0$: Die quadratische Gleichung hat keine reelle Lösung.
- Wir überlegen zunächst, wann der Kreis $K_r(u, v)$ eine der gegebenen Geraden berührt.
  - Ein Punkt (x, y) liegt genau dann im Durchschnitt der Geraden $y = x - 2$ und des Kreises $K_r(u, v)$, wenn gilt

$$\begin{aligned}
&\iff \quad y = x - 2 \text{ und } (x-u)^2 + (y-v)^2 = w \quad \iff \\
&\iff \quad y = x - 2 \text{ und } (x-u)^2 + (x-2-v)^2 = w \quad \iff \\
&\iff \quad y = x - 2 \text{ und } 2x^2 + (-2u - 2v - 4)x + (u^2 + v^2 + 4v - w + 4) = 0.
\end{aligned}$$

Die Diskriminante der quadratischen Gleichung (in x) $2x^2 + (-2u - 2v - 4)x + (u^2 + v^2 + 4v - w + 4) = 0$ ist

$$\begin{aligned}
f(u, v, w) &= (-2u - 2v - 4)^2 - 4 \cdot 2 \cdot (u^2 + v^2 + 4v - w + 4) = \\
&= -4u^2 + 8uv - 4v^2 + 16u - 16v + 8w - 16.
\end{aligned}$$

Ist $f(u, v, w) > 0$, so scheiden sich Gerade und Kreis in zwei Punkten, ist $f(u, v, w) = 0$, so gibt es genau einen Schnittpunkt, ist $f(u, v, w) < 0$, so gibt es überhaupt keine Schnittpunkte.
Wann berührt der Kreis $K_r(u, v)$ die Gerade $y = x - 2$? Genau dann, wenn sich Kreis und Gerade in genau einem Punkt schneiden (Achtung: Dies ist eine spezielle Eigenschaft von Kreisen und gilt nicht allgemein!), d.h. wenn gilt

$$f(u, v, w) = -4u^2 + 8uv - 4v^2 + 16u - 16v + 8w - 16 = 0.$$

- – Ein Punkt (x, y) liegt genau dann im Durchschnitt der Geraden $y = -2x+1$ mit dem Kreis $K_r(u, v)$ (mit $w = r^2$), wenn gilt

$$\begin{aligned}
&\iff \quad y = -2x + 1 \text{ und } (x-u)^2 + (y-v)^2 = w \quad \iff \\
&\iff \quad y = -2x + 1 \text{ und } (x-u)^2 + (-2x+1-v)^2 = w \quad \iff \\
&\iff \quad y = -2x + 1 \text{ und } 5x^2 + (-2u+4v-4)x + (u^2+v^2-2v-w+1) = 0.
\end{aligned}$$

  Die Diskriminante der quadratischen Gleichung $5x^2+(-2u+4v-4)x+(u^2+v^2-2v-w+1) = 0$ ist

$$g(u, v, w) = -16u^2 - 16uv - 4v^2 + 16u + 8v + 20w - 4.$$

  Wie eben folgt, dass die Gerade $y = -2x + 1$ genau dann den Kreis $K_r(u, v)$ (mit $w = r^2$) berührt, wenn

$$g(u, v, w) = -16u^2 - 16uv - 4v^2 + 16u + 8v + 20w - 4 = 0$$

  gilt.
- – Ein Punkt (x, y) liegt genau dann im Durchschnitt der Geraden $y = 1$ mit dem Kreis $K_r(u, v)$ (mit $w = r^2$), wenn gilt

$$\begin{aligned}
&\iff \quad y = 1 \text{ und } (x-u)^2 + (y-v)^2 = w \quad \iff \\
&\iff \quad y = 1 \text{ und } (x-u)^2 + (1-v)^2 = w \quad \iff \\
&\iff \quad y = 1 \text{ und } x^2 - 2ux + (u^2+v^2-2v-w+1) = 0.
\end{aligned}$$

  Die Diskriminante der quadratischen Gleichung $x^2 - 2ux + (u^2 + v^2 - 2v - w + 1) = 0$ ist

$$h(u, v, w) = -4v^2 + 8v + 4w - 4.$$

  Wie oben folgt, dass die Gerade $y = 1$ genau dann den Kreis $K_r(u, v)$ (mit $w = r^2$) berührt, wenn gilt

$$h(u, v, w) = -4v^2 + 8v + 4w - 4 = 0.$$

- Damit erhalten wir: Ein Kreis $K_r(u, v)$ (mit $w = r^2$) berührt genau dann alle drei gegebenen Geraden, wenn folgende Gleichungen erfüllt sind:

$$\begin{aligned}
f(u, v, w) &= -4u^2 + 8uv - 4v^2 + 16u - 16v + 8w - 16 = 0, \\
g(u, v, w) &= -16u^2 - 16uv - 4v^2 + 16u + 8v + 20w - 4 = 0, \\
h(u, v, w) &= -4v^2 + 8v + 4w - 4 = 0.
\end{aligned}$$

  Wir haben die Aufgabenstellung jetzt also auf das Lösen der drei Gleichungen in u, v, w zurückgeführt.
- Wir wollen jetzt die Lösungen des Gleichungssystems $f(u, v, w) = g(u, v, w) = h(u, v, w) = 0$ in u, v, w bestimmen. Wegen

$$h(u, v, w) = 0 \quad \iff \quad w = v^2 - 2v + 1$$

  definieren wir

$$\begin{aligned}
F(u, v) &= \frac{1}{4} f(u, v, v^2 - 2v + 1) = -u^2 + 2uv + v^2 + 4u - 8v - 2, \\
G(u, v) &= \frac{1}{16} g(u, v, v^2 - 2v + 1) = -u^2 - uv + v^2 + u - 2v + 1,
\end{aligned}$$

  denn dann gilt

$$f(u, v, w) = g(u, v, w) = h(u, v, w) = 0 \quad \iff \quad w = v^2 - 2v + 1 \text{ und } F(u, v) = G(u, v) = 0.$$

- Wir wollen nun $F(u,v) = G(u,v) = 0$ lösen. Es gilt:

$$\begin{aligned}
& F(u,v) = G(u,v) = 0 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & F(u,v) = 0 \text{ und } \frac{1}{3}(G(u,v) - F(u,v)) = 0 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & -u^2 + 2uv + v^2 + 4u - 8v - 2 = 0 \text{ und } -uv - u + 2v + 1 = 0 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & -u^2 - 2uv - v^2 + 4u - 8v - 2 = 0 \text{ und } (2-u)v = u - 1 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & v = \frac{u-1}{2-u} \text{ und } -u^2 - 2uv - v^2 + 4u - 8v - 2 = 0 \text{ und } u \neq 2 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & v = \frac{u-1}{2-u} \text{ und } -\frac{u^4 - 6u^3 + 7u^2 + 6u - 9}{(u-2)^2} = 0 \text{ und } u \neq 2 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & v = \frac{u-1}{2-u} \text{ und } u^4 - 6u^3 + 7u^2 + 6u - 9 = 0.
\end{aligned}$$

- Verwenden wir nun $w = v^2 - 2v + 1$, so folgt schließlich

$$\begin{aligned}
& f(u,v,w) = g(u,v,w) = h(u,v,w) = 0 \quad \Longleftrightarrow \\
\Longleftrightarrow \quad & u^4 - 6u^3 + 7u^2 + 6u - 9 = 0, \quad v = \frac{u-1}{2-u}, \quad w = (\frac{2u-3}{u-2})^2.
\end{aligned}$$

- Die Gleichung für u können wir numerisch lösen und erhalten dann folgende vier Lösungen:

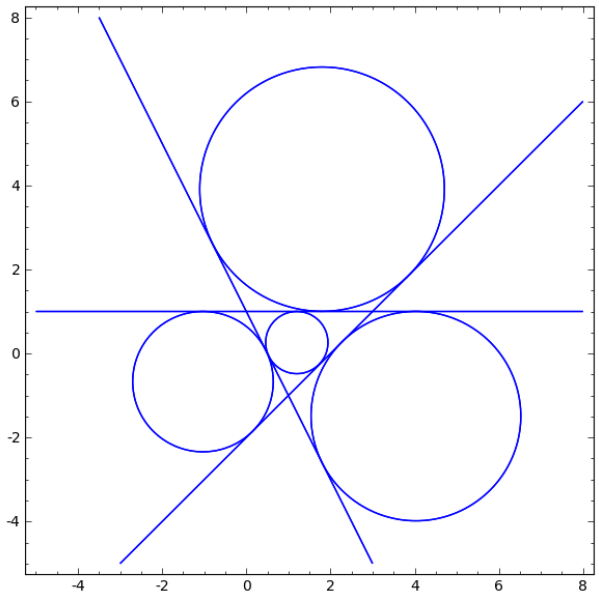
i	u_i	v_i	w_i	r_i
1	-1.03	-0.67	2.79	1.67
2	1.20	0.26	0.55	0.74
3	1.80	3.91	8.45	2.91
4	4.03	-1.49	6.21	2.49

Die vier Kreise $K_{r_i}(u_i, v_i)$ berühren also alle drei Geraden.

Mit SAGE kann man u_i, v_i, w_i, r_i wie folgt finden:

```
var("u")
f=u^4-6*u^3+7*u^2+6*u-9
U=f.roots(ring=RR)
for u,_ in U:
  v=(u-1)/(2-u)
  w=((2*u-3)/(u-2))^2
  r=w^0.5
  print(u,v,w,r)
```

-

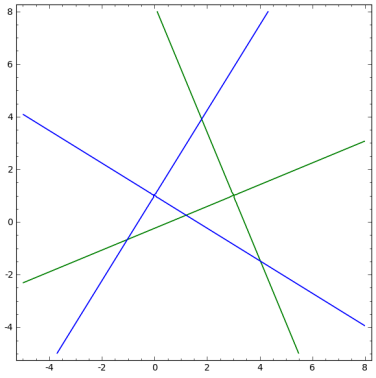


Wir haben also ein geometrisches Problem in die Algebra übersetzt, die entsprechenden Gleichungen manipuliert und gelöst. Als Ergebnis erhalten wir vier Kreise.

- Wir kommen nochmals zurück zu den Gleichungen $F(u,v) = G(u,v) = 0$, d.h.

$$-u^2 + 2uv + v^2 + 4u - 8v - 2 = 0 \text{ und } -u^2 - uv + v^2 + u - 2v + 1 = 0.$$

Wir lassen die Kurven zeichnen und erhalten folgendes Bild:



Dies legt die Vermutung nahe, dass es sich bei beiden Gleichungen um Geradenpaare handelt.

- Durch Probieren findet man die Zerlegungen

$$\begin{aligned} F(u,v) &= -u^2 + 2uv + v^2 + 4u - 8v - 2 = \\ &= (v + u - 4 + \sqrt{2}(u-3))(v + u - 4 - \sqrt{2}(u-3)) \\ G(u,v) &= -u^2 - uv + v^2 + u - 2v + 1 = \\ &= (v - \frac{1}{2}u - 1 + \frac{1}{2}\sqrt{5}u)(v - \frac{1}{2}u - 1 - \frac{1}{2}\sqrt{5}u) \end{aligned}$$

Die Schnittpunkte lassen sich hier natürlich sofort direkt ausrechnen:

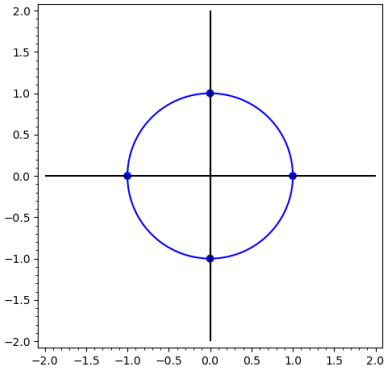
$$\begin{aligned} u_1 &= \frac{3}{2} - \sqrt{2} - \frac{1}{2}\sqrt{5}, & v_1 &= \frac{1}{2} - \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{5} - \frac{1}{2}\sqrt{2}\cdot\sqrt{5}, & w_1 &= \frac{9}{2} - 2\sqrt{2} + \frac{1}{2}\sqrt{5}, \\ u_2 &= \frac{3}{2} - \sqrt{2} + \frac{1}{2}\sqrt{5}, & v_2 &= \frac{1}{2} - \frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{5} + \frac{1}{2}\sqrt{2}\cdot\sqrt{5}, & w_2 &= \frac{9}{2} - 2\sqrt{2} - \frac{1}{2}\sqrt{5}, \\ u_3 &= \frac{3}{2} + \sqrt{2} - \frac{1}{2}\sqrt{5}, & v_3 &= \frac{1}{2} + \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{5} + \frac{1}{2}\sqrt{2}\cdot\sqrt{5}, & w_3 &= \frac{9}{2} + 2\sqrt{2} + \frac{1}{2}\sqrt{5}, \\ u_4 &= \frac{3}{2} + \sqrt{2} + \frac{1}{2}\sqrt{5}, & v_4 &= \frac{1}{2} + \frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{5} - \frac{1}{2}\sqrt{2}\cdot\sqrt{5}, & w_4 &= \frac{9}{2} + 2\sqrt{2} - \frac{1}{2}\sqrt{5}. \end{aligned}$$

(Die Nummerierung ist so gewählt, dass es zu den nummerischen Lösungen passt.)

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

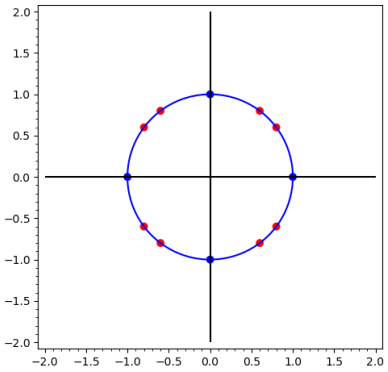
$$x^2 + y^2 = 1 \quad \text{mit} \quad x, y \in \mathbb{Q}.$$

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



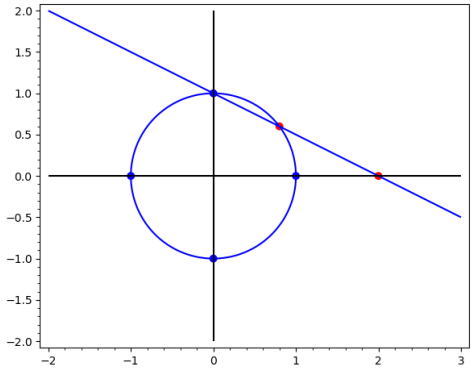
Gibt es weitere Punkte? Bekanntlich gilt $3^2+4^2=5^2$, woraus sich $(\frac{3}{5})^2+(\frac{4}{5})^2=1$ ergibt. Also ist $(\frac{3}{5},\frac{4}{5})$ ein rationaler Kreispunkt. Aus Symmetriegründen erhält man dann gleich folgende rationale Kreispunkte:

$$(\frac{3}{5},\frac{4}{5}),(\frac{3}{5},-\frac{4}{5}),(-\frac{3}{5},\frac{4}{5}),(-\frac{3}{5},-\frac{4}{5}),(\frac{4}{5},\frac{3}{5}),(\frac{4}{5},-\frac{3}{5}),(-\frac{4}{5},\frac{3}{5}),(-\frac{4}{5},-\frac{3}{5}).$$



Gibt es weitere rationale Punkte auf dem Einheitskreis?
Eine geometrische Idee:

- Wir starten mit dem Punkt $(0,1)$. Sei (x_0,y_0) irgendein, von $(0,1)$ verschiedener Kreispunkt. Wir legen eine Gerade durch $(0,1)$ und (x_0,y_0):



  Setzen wir zusätzlich $x_0\neq 0$, also $(x_0,y_0)\neq(0,-1)$ voraus, so wird die Gerade durch folgende Gleichung beschrieben:

$$\frac{y-1}{x-0}=\frac{y_0-1}{x_0-0},$$

  also

$$y=\frac{y_0-1}{x_0}x+1.$$

- Den Schnittpunkt mit der x-Achse erhalten wir, wenn wir $y=0$ setzen und nach x auflösen:

$$0=\frac{y_0-1}{x_0}x+1 \quad\Longleftrightarrow\quad \frac{y_0-1}{x_0}x=-1 \quad\Longleftrightarrow\quad x=\frac{x_0}{1-y_0}.$$

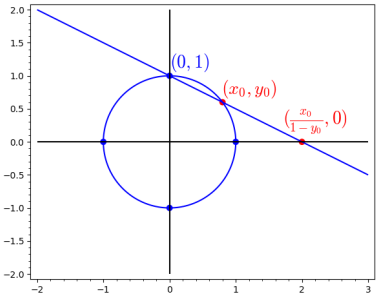
  Die Gerade schneidet die x-Achse also im Punkt

$$(\frac{x_0}{1-y_0},0).$$

  Wir ordnen jetzt jedem von $(0,1)$ verschiedenen Punkt des Kreises die x-Koordinate des Schnittpunkts der Verbindungsgeraden zu:

$$(x_0,y_0)\mapsto\frac{x_0}{1-y_0}.$$

(Diese Abbildung funktioniert auch für $(x_0, y_0) = (0, -1)$.)



- Wir nehmen nun umgekehrt irgendeinen Punkt $(t, 0)$ der x-Achse und bestimmen die Gerade durch die Punkte $(0, 1)$ und $(t, 0)$, wobei wir zunächst $t \neq 0$ voraussetzen:

$$\frac{y-1}{x-0} = \frac{1-0}{0-t} = -\frac{1}{t}$$

oder

$$y = -\frac{1}{t}x + 1.$$

Wir bemerken, dass gilt

$$t = -\frac{x}{y-1} = \frac{x}{1-y}.$$

Nun bestimmen wir den zweiten Schnittpunkt der Geraden mit dem Einheitskreis.

Dazu setzen wir die Geradengleichung in die Kreisgleichung ein:

$$\begin{aligned} x^2 + \left(-\frac{1}{t}x + 1\right)^2 = 1 \quad &\iff \quad x^2 + \frac{1}{t^2}x^2 - \frac{2}{t}x + 1 = 1 \quad \iff \\ &\iff \quad \left(1 + \frac{1}{t^2}\right)x^2 = \frac{2}{t}x \quad \overset{x\neq 0}{\iff} \\ &\iff \quad \left(1 + \frac{1}{t^2}\right)x = \frac{2}{t} \quad \iff \\ &\iff \quad x = \frac{\frac{2}{t}}{1 + \frac{1}{t^2}} = \frac{2t}{t^2+1}. \end{aligned}$$

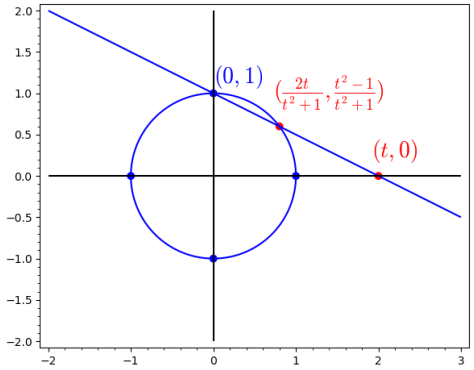
- Den zugehörigen y-Wert erhalten wir, wenn wir den x-Wert in die Geradengleichung einsetzen:

$$y = -\frac{1}{t} \cdot \frac{2t}{t^2+1} + 1 = \frac{-2}{t^2+1} + \frac{t^2+1}{t^2+1} = \frac{t^2-1}{t^2+1}.$$

Wir erhalten also als Schnittpunkt

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

(Diese Gleichung gilt auch für $t = 0$.)



Mit Hilfe unserer geometrischen Überlegungen haben wir die Kreispunkte parametrisiert. Wir formulieren das Ergebnis als Satz:

SATZ. *Die Abbildung*

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

ist bijektiv mit der Umkehrabbildung

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

(Wir verzichten hier auf einen rein algebraischen Beweis.)

Der Satz erlaubt es, beliebig viele rationale Punkte auf dem Einheitskreis anzugeben. Hier sind ein paar Beispiele.

Beispiele:

t	0	1	-1	2	3	4	5
$\mu(t)$	$(0,-1)$	$(1,0)$	$(-1,0)$	$(\frac{4}{5},\frac{3}{5})$	$(\frac{3}{5},\frac{4}{5})$	$(\frac{8}{17},\frac{15}{17})$	$(\frac{5}{13},\frac{12}{13})$

Wir können nun auch die im 1. Quadranten gelegenen rationalen Kreispunkte, d.h. die Punkte

$$(x,y) \text{ mit } x^2 + y^2 = 1 \text{ und } x, y \in \mathbb{Q}_{>0}$$

gut beschreiben:

FOLGERUNG. *Die Punkte (x,y) mit $x, y \in \mathbb{Q}_{>0}$ und $x^2 + y^2 = 1$ lassen sich durch die rationalen Zahlen > 1 parametrisieren. Genauer:*

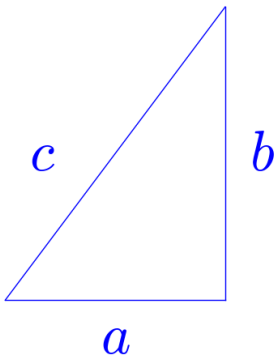
$$\begin{array}{rcl} \{(x,y) \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0} : x^2 + y^2 = 1\} & \simeq & \mathbb{Q}_{>1} \\ (x,y) & \longmapsto & \dfrac{x}{1-y} \\ (\dfrac{2t}{t^2+1}, \dfrac{t^2-1}{t^2+1}) & \longleftarrow & t \end{array}$$

Dabei sind die angegebenen Abbildungen invers zueinander.

Pythagoreische Tripel: Ein **pythagoreisches Tripel** ist ein Tripel (a,b,c) natürlicher Zahlen $a, b, c \in \mathbb{N}$, wenn gilt:

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

d.h. wenn a, b, c die Seitenlängen eines rechtwinkligen Dreiecks sind (Satz des Pythagoras). Manchmal spricht man dann auch von einem pythagoreischen Dreieck.



Ein pythagoreisches Tripel (a,b,c) nennt man **primitiv**, wenn gilt $\mathrm{ggT}(a,b,c) = 1$. Ein bekanntes Beispiel ist

$$(3,4,5).$$

Ist (a, b, c) ein pythagoreisches Tripel und $k \in \mathbb{N}$, so folgt aus

$$(ka)^2 + (kb)^2 = (kc)^2,$$

dass auch (ka, kb, kc) ein pythagoreisches Tripel ist. Man kann sich überlegen, dass sich alle pythagoreische Tripel auf diese Weise aus primitiven pythagoreischen Tripeln ergeben.
Sei nun (a, b, c) ein pythagoreisches Tripel. Dann folgt aus $a^2 + b^2 = c^2$ natürlich $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$. Also ist $(\frac{a}{c}, \frac{b}{c})$ ein im 1. Quadranten gelegener rationaler Punkt des Einheitskreises. Nach der Folgerung gibt es also einen Parameter $t \in \mathbb{Q}_{>1}$, sodass gilt

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

Der Parameter ist

$$t = \frac{\frac{a}{c}}{1 - \frac{b}{c}} = \frac{a}{c-b}.$$

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

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

Anders geschrieben:

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

- Ist m oder n gerade, wählt man $c = m^2 + n^2$, so erhält man das Tripel

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

- Sind m und n ungerade Zahlen, wählt man $c = \frac{m^2+n^2}{2}$, so ist c eine natürliche Zahl und man erhält das Tripel

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

Man kann beweisen, was wir hier nicht tun wollen, dass man auf diese Weise alle primitiven pythagoreischen Tripel erhält:

Satz (Beschreibung aller primitiven pythagoreischen 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 pythagoreischen Tripel. Dann ist die Abbildung

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

bijektiv mit der Umkehrabbildung

$$\beta : \mathbb{Q}_{>1} \to P, \quad \frac{m}{n} \mapsto \begin{cases} (2mn, m^2-n^2, m^2+n^2), & \text{falls } m, n \in \mathbb{N}, m > n, \mathrm{ggT}(m, n) = 1, \\ & m \text{ oder } n \text{ gerade}, \\ (mn, \frac{m^2-n^2}{2}, \frac{m^2+n^2}{2}), & \text{falls } m, n \in \mathbb{N}, m > n, \mathrm{ggT}(m, n) = 1, \\ & m \text{ und } n \text{ ungerade}. \end{cases}$$

Beispiele: Hier sind alle primitiven pythagoreischen Tripel (a, b, c) mit $c \leq 100$. Es gibt 32 Stück.

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

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

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 bestimmt:

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

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

Die vorangegangenen Überlegungen hatten mit der Kurve $x^2 + y^2 = 1$ zu tun. Durch die angegebene Parametrisierung sieht man, dass es unendlich viele rationale Punkte auf dieser Kurve gibt. Dies ändert sich, wenn man den Exponenten 2 durch eine größere Zahl ersetzt.

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

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

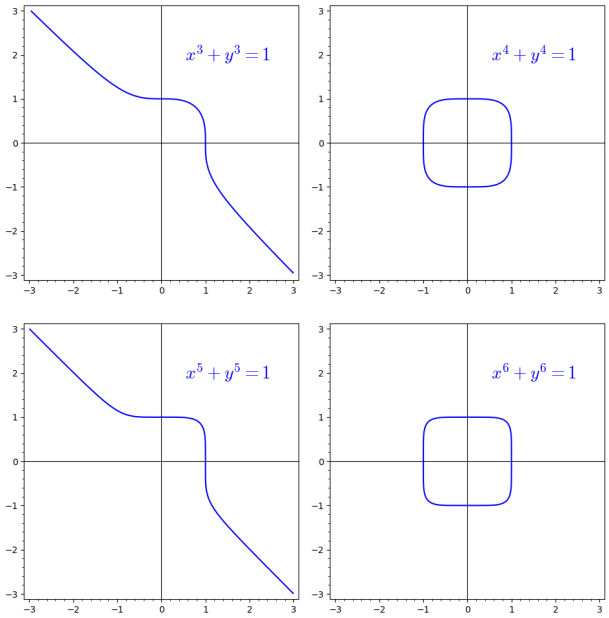
keine Lösung. Dies wurde von Fermat behauptet, von Wiles (1995) bewiesen. (Der Beweis ist nichttrivial.) Gilt $a^n + b^n = c^n$, so folgt $(\frac{a}{c})^n + (\frac{b}{c})^n = 1$, also hat man das Problem, nach rationalen Punkten (Punkten mit rationalen Koordinaten) auf der Kurve

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

zu suchen. Es wurde bewiesen, dass es nur die folgenden trivialen Lösungen gibt:

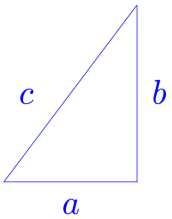
$$\begin{cases} (1,0), (-1,0), (0,1), (0,-1) & \text{für gerades } n, \\ (1,0), (0,1) & \text{für ungerades } n. \end{cases}$$

Die folgenden Bilder zeigen die reellen Kurven für einige n.



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.

Bemerkung: Eine natürliche Zahl n nennt man **quadratfrei**, wenn sie nicht durch das Quadrat einer Primzahl p teilbar ist. Jede natürlich Zahl $n \in \mathbb{N}$ lässt sich eindeutig zerlegen

$$n = k^2\ell \text{ mit } k, \ell \in \mathbb{N}, \ell \text{ quadratfrei.}$$

Man nennt ℓ auch den quadratfreien Anteil von n (SAGE: `squarefree_part`). Ein paar Beispiele:

$$1 = 1^2 \cdot 1, \quad 2 = 1^2 \cdot 2, \quad 3 = 1^2 \cdot 2, \quad 4 = 2^2 \cdot 1, \quad 5 = 1^2 \cdot 5,$$
$$6 = 1^2 \cdot 6, \quad 7 = 1^2 \cdot 7, \quad 8 = 2^2 \cdot 2,$$
$$12 = 2^2 \cdot 3, \quad 18 = 3^2 \cdot 2, \quad 20 = 2^2 \cdot 5, \quad 24 = 2^2 \cdot 6, \quad 27 = 3^2 \cdot 3,$$
$$28 = 2^2 \cdot 7, \quad 32 = 2^4 \cdot 2, \quad \ldots$$

Unsere Beschreibung der rationalen Punkte des Einheitskreises führt nun zu einer Beschreibung der Kongruenzzahlen:

SATZ.

- *Ist N eine quadratfreie Kongruenzzahl, so gibt es $m, n, k \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$, $m > n$ und*
$$N = \frac{(m^2 - n^2)mn}{k^2}.$$
- *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
$$a = \frac{2mn}{k}, \quad b = \frac{m^2 - n^2}{k}, \quad c = \frac{m^2 + n^2}{k}.$$

Beweis:

- Sei N eine Kongruenzzahl, d.h. $N = \frac{1}{2}ab$ und $a^2 + b^2 = c^2$ mit $a, b, c \in \mathbb{Q}_{>0}$. Dann ist $(\frac{a}{c}, \frac{b}{c})$ ein rationaler Kreispunkt im 1. Quadranten, es gibt also $m, n \in \mathbb{N}$ mit $m > n$, $\mathrm{ggT}(m, n) = 1$ und
$$\frac{a}{c} = \frac{2mn}{m^2 + n^2}, \quad \frac{b}{c} = \frac{m^2 - n^2}{m^2 + n^2},$$
also
$$a = 2mn \cdot \frac{c}{m^2 + n^2}, \quad b = (m^2 - n^2) \cdot \frac{c}{m^2 + n^2}.$$
Dann ist
$$N = \frac{1}{2}ab = \frac{1}{2} \cdot 2mn \cdot \frac{c}{m^2 + n^2} \cdot (m^2 - n^2) \cdot \frac{c}{m^2 + n^2} = mn(m^2 - n^2) \cdot \left(\frac{c}{m^2 + n^2}\right)^2.$$
Wir schreiben
$$\frac{c}{m^2 + n^2} = \frac{\ell}{k} \text{ mit } \ell, k \in \mathbb{N}, \mathrm{ggT}(\ell, k) = 1$$
und erhalten dann
$$N = mn(m^2 - n^2) \cdot \frac{\ell^2}{k^2}, \quad \text{also} \quad Nk^2 = mn(m^2 - n^2) \cdot \ell^2.$$
Da N quadratfrei sein soll, folgt aus $\mathrm{ggT}(k, \ell) = 1$ sofort $\ell = 1$, und damit
$$Nk^2 = mn(m^2 - n^2).$$
Es ist dann
$$\frac{c}{m^2 + n^2} = \frac{1}{k},$$
woraus sich
$$a = \frac{2mn}{k}, \quad b = \frac{m^2 - n^2}{k}, \quad c = \frac{m^2 + n^2}{k}$$
ergibt.
- 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 (mit $m > n$ und $\mathrm{ggT}(m,n) = 1$), zerlegt $mn(m^2 - n^2) = Nk^2$ mit quadratfreiem N. Dann ist N eine Kongruenzzahl.

Beispiel: Wir wählen $m = 2021$ und $n = 1000$. Dann gilt mit den Bezeichnungen des vorangegangenen Satzes

$$\begin{aligned} Nk^2 &= mn(m^2-n^2) = 6233655261000 = 2^3 \cdot 3 \cdot 5^3 \cdot 19 \cdot 43 \cdot 47 \cdot 53 \cdot 1021 = \\ &= (2 \cdot 3 \cdot 5 \cdot 19 \cdot 43 \cdot 47 \cdot 53 \cdot 1021) \cdot (2 \cdot 5)^2 = 62336552610 \cdot 10^2. \end{aligned}$$

Daher ist

$$N = 62336552610$$

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

$$a = \frac{2mn}{k} = 404200, \quad b = \frac{m^2-n^2}{k} = \frac{3084441}{10}, \quad c = \frac{m^2+n^2}{k} = \frac{5084441}{10}.$$

Beispiele: Nach dem eben beschriebenen Verfahren haben wir m bis 10000 laufen lassen. Dabei wurden folgende quadratfreien Kongruenzzahlen $N \leq 50$ gefunden:

N	(a,b,c)	m	n	k
5	$\left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348}\right)$	2401	961	1494696
5	$\left(\frac{20}{3}, \frac{3}{2}, \frac{41}{6}\right)$	5	4	6
5	$\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$	9	1	12
5	$\left(\frac{4920}{1519}, \frac{1519}{492}, \frac{3344161}{747348}\right)$	1681	720	747348
6	$(3,4,5)$	3	1	2
6	$(4,3,5)$	2	1	1
6	$\left(\frac{120}{7}, \frac{7}{10}, \frac{1201}{70}\right)$	25	24	70
6	$\left(\frac{3404}{1551}, \frac{4653}{851}, \frac{7776485}{1319901}\right)$	2738	529	1319901
6	$\left(\frac{4653}{851}, \frac{3404}{1551}, \frac{7776485}{1319901}\right)$	3267	2209	2639802
6	$\left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}\right)$	49	1	140
7	$\left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right)$	16	9	60
7	$\left(\frac{35}{12}, \frac{24}{5}, \frac{337}{60}\right)$	25	7	120
13	$\left(\frac{323}{30}, \frac{780}{323}, \frac{106921}{9690}\right)$	361	289	19380
13	$\left(\frac{780}{323}, \frac{323}{30}, \frac{106921}{9690}\right)$	325	36	9690
14	$\left(\frac{21}{2}, \frac{8}{3}, \frac{65}{6}\right)$	9	7	12
14	$\left(\frac{21840}{3713}, \frac{3713}{780}, \frac{21914881}{2896140}\right)$	4225	2016	2896140
14	$\left(\frac{3713}{780}, \frac{21840}{3713}, \frac{21914881}{2896140}\right)$	6241	2209	5792280
14	$\left(\frac{8}{3}, \frac{21}{2}, \frac{65}{6}\right)$	8	1	6
15	$\left(4, \frac{15}{2}, \frac{17}{2}\right)$	4	1	2
15	$\left(\frac{15}{2}, 4, \frac{17}{2}\right)$	5	3	4
15	$\left(\frac{161}{68}, \frac{2040}{161}, \frac{141121}{10948}\right)$	529	49	21896
15	$\left(\frac{2040}{161}, \frac{161}{68}, \frac{141121}{10948}\right)$	289	240	10948
21	$\left(12, \frac{7}{2}, \frac{25}{2}\right)$	4	3	2
21	$\left(\frac{4200}{527}, \frac{527}{100}, \frac{503521}{52700}\right)$	625	336	52700
21	$\left(\frac{527}{100}, \frac{4200}{527}, \frac{503521}{52700}\right)$	961	289	105400
21	$\left(\frac{7}{2}, 12, \frac{25}{2}\right)$	7	1	4
22	$\left(\frac{140}{3}, \frac{33}{35}, \frac{4901}{105}\right)$	50	49	105
22	$\left(\frac{33}{35}, \frac{140}{3}, \frac{4901}{105}\right)$	99	1	210

N	(a,b,c)	m	n	k
29	$\left(\frac{52780}{99}, \frac{99}{910}, \frac{48029801}{90090}\right)$	4901	4900	90090
29	$\left(\frac{99}{910}, \frac{52780}{99}, \frac{48029801}{90090}\right)$	9801	1	180180
30	$(12,5,13)$	3	2	1
30	$(5,12,13)$	5	1	2
30	$\left(\frac{119}{26}, \frac{1560}{119}, \frac{42961}{3094}\right)$	289	49	6188
30	$\left(\frac{1560}{119}, \frac{119}{26}, \frac{42961}{3094}\right)$	169	120	3094
31	$\left(\frac{720}{287}, \frac{8897}{360}, \frac{2566561}{103320}\right)$	1600	81	103320
31	$\left(\frac{8897}{360}, \frac{720}{287}, \frac{2566561}{103320}\right)$	1681	1519	206640
34	$\left(24, \frac{17}{6}, \frac{145}{6}\right)$	9	8	6
34	$\left(\frac{112}{9}, \frac{153}{28}, \frac{3425}{252}\right)$	49	32	252
34	$\left(\frac{136}{15}, \frac{15}{2}, \frac{353}{30}\right)$	17	8	30
34	$\left(\frac{15}{2}, \frac{136}{15}, \frac{353}{30}\right)$	25	9	60
34	$\left(\frac{153}{28}, \frac{112}{9}, \frac{3425}{252}\right)$	81	17	504
34	$\left(\frac{17}{6}, 24, \frac{145}{6}\right)$	17	1	12
34	$\left(\frac{3927}{248}, \frac{992}{231}, \frac{939905}{57288}\right)$	1089	833	114576
34	$\left(\frac{992}{231}, \frac{3927}{248}, \frac{939905}{57288}\right)$	961	128	57288
38	$\left(\frac{1700}{279}, \frac{5301}{425}, \frac{1646021}{118575}\right)$	1250	289	118575
38	$\left(\frac{5301}{425}, \frac{1700}{279}, \frac{1646021}{118575}\right)$	1539	961	237150
39	$\left(\frac{156}{5}, \frac{5}{2}, \frac{313}{10}\right)$	13	12	10
39	$\left(\frac{5}{2}, \frac{156}{5}, \frac{313}{10}\right)$	25	1	20
41	$\left(\frac{1023}{40}, \frac{3280}{1023}, \frac{1054721}{40920}\right)$	1089	961	81840
41	$\left(\frac{1189}{420}, \frac{840}{29}, \frac{354481}{12180}\right)$	841	41	24360
41	$\left(\frac{123}{20}, \frac{40}{3}, \frac{881}{60}\right)$	41	9	120
41	$\left(\frac{3280}{1023}, \frac{1023}{40}, \frac{1054721}{40920}\right)$	1025	64	40920
41	$\left(\frac{40}{3}, \frac{123}{20}, \frac{881}{60}\right)$	25	16	60
41	$\left(\frac{840}{29}, \frac{1189}{420}, \frac{354481}{12180}\right)$	441	400	12180
46	$\left(\frac{168}{11}, \frac{253}{42}, \frac{7585}{462}\right)$	72	49	462
46	$\left(\frac{253}{42}, \frac{168}{11}, \frac{7585}{462}\right)$	121	23	924

Die obige Tabelle enthält nicht alle (quadratfreien) Kongruenzzahlen ≤ 50, es fehlen noch die Zahlen 23, 37, 47. Die folgende Tabelle liefert passende Werte, um auch die Zahlen 23, 37, 47 als Kongruenzzahlen nachzuweisen:

N	m	n
23	24336	17689
37	777925	1764
47	14561856	2289169

Bemerkung: Fermat hat bewiesen, dass 1 und 2 keine Kongruenzzahlen sind.

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 $(a,b,c) = (\frac{7}{10}, \frac{120}{7}, \frac{1201}{70})$.

Bemerkung: Der vorangegangene Satz liefert zwar eine Möglichkeit, Kongruenzzahlen zu konstruieren. Man kann mit ihm aber nicht effektiv testen, ob eine gegebene Zahl N eine Kongruenzzahl ist oder nicht.

Der folgende Satz bringt einen neuen Kurventyp ins Spiel:

SATZ. *Für eine natürliche Zahl N gilt die Äquivalenz:*

$$N \text{ ist Kongruenzzahl} \quad \Longleftrightarrow \quad \text{es gibt } x,y \in \mathbb{Q}_{>0} \text{ mit } y^2 = x^3 - N^2 x.$$

Genauer:

- *Ist N eine Kongruenzzahl, (a,b,c) ein zugehöriges rationales rechtwinkliges Dreieck mit Flächeninhalt N, setzt man*
$$x = \frac{Na}{c-b}, \quad y = \frac{2N^2}{c-b},$$
so gilt
$$x,y \in \mathbb{Q}_{>0} \quad \text{und} \quad y^2 = x(x^2 - N^2).$$
- *Ist $(x,y) \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0}$ mit*
$$y^2 = x(x^2 - N^2),$$
setzt man
$$a = \frac{2Nx}{y}, \quad b = \frac{x^2 - N^2}{y}, \quad c = \frac{x^2 + N^2}{y},$$
so sind a,b,c die Seiten eines rationalen rechtwinkligen Dreiecks mit Flächeninhalt N, insbesondere ist also N eine Kongruenzzahl.

Man kann die vorangegangenen Punkte auch so zusammenfassen:

- *Sei*
$$D_N = \{(a,b,c) \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0} \times \mathbb{Q}_{>0} : a^2 + b^2 = c^2, N = \frac{1}{2}ab\}$$
und
$$X_N = \{(x,y) \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0} : y^2 = x^3 - N^2 x\}.$$
Die Abbildung
$$\gamma : D_N \to X_N, \quad (a,b,c) \mapsto (\frac{Na}{c-b}, \frac{2N^2}{c-b})$$
ist bijektiv mit Umkehrabbildung
$$\delta : X_N \to D_N, \quad (x,y) \mapsto (\frac{2Nx}{y}, \frac{x^2 - N^2}{y}, \frac{x^2 + N^2}{y}).$$

Beweis:

- Sei N eine Kongruenzzahl, $a,b,c \in \mathbb{Q}_{>0}$ die Seitenlängen eines zugehörigen rechtwinkligen Dreiecks. Für $t = \frac{a}{c-b}$ gilt dann

$$a = \frac{2t}{t^2+1} \cdot c, \quad b = \frac{t^2-1}{t^2+1} \cdot c$$

und

$$N = \frac{1}{2}ab = \frac{1}{2} \cdot \frac{2t}{t^2+1} \cdot c \cdot \frac{t^2-1}{t^2+1} \cdot c = \frac{t(t^2-1)}{(t^2+1)^2} \cdot c^2.$$

Wir formen die letzte Gleichung äquivalent um:

$$N = \frac{t(t^2-1)}{(t^2+1)^2} \cdot c^2 \iff N = \frac{N^4 \cdot t(t^2-1)}{N^4(t^2+1)^2} \cdot c^2 = \frac{N \cdot (Nt)((Nt)^2-N^2)}{((Nt)^2+N^2)^2} \cdot c^2 \iff$$

$$\iff \left(\frac{(Nt)^2+N^2}{c}\right)^2 = (Nt) \cdot ((Nt)^2-N^2).$$

Setzen wir

$$x = Nt, \quad y = \frac{(Nt)^2+N^2}{c},$$

so gilt

$$y^2 = x(x^2-N^2) \quad \text{und} \quad x \in \mathbb{Q}_{>0}, \quad y \in \mathbb{Q}_{>0}.$$

Wir erhalten damit die Darstellungen

$$\begin{aligned} a &= \frac{2t}{t^2+1} \cdot c = \frac{2N \cdot Nt}{(Nt)^2+N^2} \cdot c = \frac{2Nx}{y}, \\ b &= \frac{t^2-1}{t^2+1} \cdot c = \frac{(Nt)^2-N^2}{(Nt)^2+N^2} \cdot c = \frac{x^2-N^2}{y}, \\ c &= \frac{(Nt)^2+N^2}{y} = \frac{x^2+N^2}{y}. \end{aligned}$$

Mit $t = \frac{a}{c-b}$ gilt weiter

$$\begin{aligned} x &= Nt = \frac{Na}{c-b}, \\ y &= \frac{N^2(t^2+1)}{c} = \frac{N^2((\frac{a}{c-b})^2+1)}{c} = \frac{N^2(a^2+(c-b)^2)}{c(c-b)^2} = \\ &= \frac{N^2(a^2+b^2+c^2-2bc)}{c(c-b)^2} = \frac{N^2(2c^2-2bc)}{c(c-b)^2} = \frac{N^2 \cdot 2c(c-b)}{c(c-b)^2} = \\ &= \frac{2N^2}{c-b}. \end{aligned}$$

- Wir rechnen dies direkt nach. Seien also $x,y \in \mathbb{Q}_{>0}$ mit

$$y^2 = x(x^2-N^2) \quad \text{und} \quad a = \frac{2Nx}{y}, \quad b = \frac{x^2-N^2}{y}, \quad c = \frac{x^2+N^2}{y}.$$

Wegen $y > 0$ und $x > 0$ folgt $x^2 - N^2 > 0$ und damit $a,b,c > 0$. Es ist

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

und

$$\frac{1}{2}ab = \frac{1}{2} \cdot \frac{2Nx}{y} \cdot \frac{x^2-N^2}{y} = \frac{Nx(x^2-N^2)}{y^2} = \frac{Ny^2}{y^2} = N.$$

Dies beweist die Behauptung.

- Dies folgt aus (1) und (2). Man kann dies aber auch eigenständig beweisen. ■

Beispiel: Wir wissen, dass $N = 6$ eine Kongruenzzahl ist. Ein zugehöriges rationales rechtwinkliges Dreieck ist $(a, b, c) = (3, 4, 5)$. Wir berechnen mit den Formeln des Satzes

$$x = \frac{Na}{c-b} = \frac{6 \cdot 3}{5-4} = 18, \quad y = \frac{2N^2}{c-b} = \frac{2 \cdot 6^2}{5-4} = 72$$

und erhalten damit den Punkt

$$(18, 72)$$

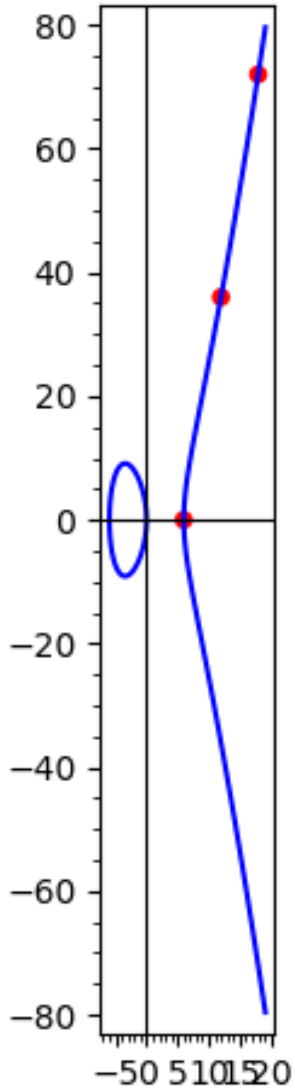
auf der Kurve $y^2 = x^3 - 36x$.
Das Dreieck $(b, a, c) = (4, 3, 5)$ führt zu

$$x = \frac{Na}{c-b} = \frac{6 \cdot 4}{5-3} = 12, \quad y = \frac{2N^2}{c-b} = \frac{2 \cdot 6^2}{5-3} = 36,$$

also den Kurvenpunkt

$$(12, 36).$$

Das folgende Bild zeigt die Kurve $y^2 = x(x^2 - 36)$ und die Kurvenpunkte $(6, 0)$, $(12, 36)$, $(18, 72)$, die alle auf der Geraden $y = 6(x - 6)$ liegen.



Beispiele: Für die Beispiele von oben haben wir nun den zum Tripel (a, b, c) gehörigen Punkte (x, y) der Kurve $y^2 = x^3 - N^2x$ aufgelistet:

N	(a, b, c)	(x, y)
5	$\left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348}\right)$	$\left(\frac{12005}{961}, \frac{1205400}{29791}\right)$
5	$\left(\frac{20}{3}, \frac{3}{2}, \frac{41}{6}\right)$	$\left(\frac{25}{4}, \frac{75}{8}\right)$
5	$\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right)$	$(45, 300)$
5	$\left(\frac{4920}{1519}, \frac{1519}{492}, \frac{3344161}{747348}\right)$	$\left(\frac{1681}{144}, \frac{62279}{1728}\right)$
6	$(3, 4, 5)$	$(18, 72)$
6	$(4, 3, 5)$	$(12, 36)$
6	$\left(\frac{120}{7}, \frac{7}{10}, \frac{1201}{70}\right)$	$\left(\frac{25}{4}, \frac{35}{8}\right)$
6	$\left(\frac{3404}{1551}, \frac{4653}{851}, \frac{7776485}{1319901}\right)$	$\left(\frac{16428}{529}, \frac{2065932}{12167}\right)$
6	$\left(\frac{4653}{851}, \frac{3404}{1551}, \frac{7776485}{1319901}\right)$	$\left(\frac{19602}{2209}, \frac{2021976}{103823}\right)$
6	$\left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}\right)$	$(294, 5040)$
7	$\left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right)$	$\left(\frac{112}{9}, \frac{980}{27}\right)$
7	$\left(\frac{35}{12}, \frac{24}{5}, \frac{337}{60}\right)$	$(25, 120)$
13	$\left(\frac{323}{30}, \frac{780}{323}, \frac{106921}{9690}\right)$	$\left(\frac{4693}{289}, \frac{192660}{4913}\right)$
13	$\left(\frac{780}{323}, \frac{323}{30}, \frac{106921}{9690}\right)$	$\left(\frac{4225}{36}, \frac{272935}{216}\right)$
14	$\left(\frac{21}{2}, \frac{8}{3}, \frac{65}{6}\right)$	$(18, 48)$
14	$\left(\frac{21840}{3713}, \frac{3713}{780}, \frac{21914881}{2896140}\right)$	$\left(\frac{4225}{144}, \frac{241345}{1728}\right)$
14	$\left(\frac{3713}{780}, \frac{21840}{3713}, \frac{21914881}{2896140}\right)$	$\left(\frac{87374}{2209}, \frac{24155040}{103823}\right)$
14	$\left(\frac{8}{3}, \frac{21}{2}, \frac{65}{6}\right)$	$(112, 1176)$
15	$\left(4, \frac{15}{2}, \frac{17}{2}\right)$	$(60, 450)$
15	$\left(\frac{15}{2}, 4, \frac{17}{2}\right)$	$(25, 100)$
15	$\left(\frac{161}{68}, \frac{2040}{161}, \frac{141121}{10948}\right)$	$\left(\frac{7935}{49}, \frac{703800}{343}\right)$
15	$\left(\frac{2040}{161}, \frac{161}{68}, \frac{141121}{10948}\right)$	$\left(\frac{289}{16}, \frac{2737}{64}\right)$
21	$\left(12, \frac{7}{2}, \frac{25}{2}\right)$	$(28, 98)$
21	$\left(\frac{4200}{527}, \frac{527}{100}, \frac{503521}{52700}\right)$	$\left(\frac{625}{16}, \frac{13175}{64}\right)$
21	$\left(\frac{527}{100}, \frac{4200}{527}, \frac{503521}{52700}\right)$	$\left(\frac{20181}{289}, \frac{2734200}{4913}\right)$
21	$\left(\frac{7}{2}, 12, \frac{25}{2}\right)$	$(147, 1764)$
22	$\left(\frac{140}{3}, \frac{33}{35}, \frac{4901}{105}\right)$	$\left(\frac{1100}{49}, \frac{7260}{343}\right)$
22	$\left(\frac{33}{35}, \frac{140}{3}, \frac{4901}{105}\right)$	$(2178, 101640)$

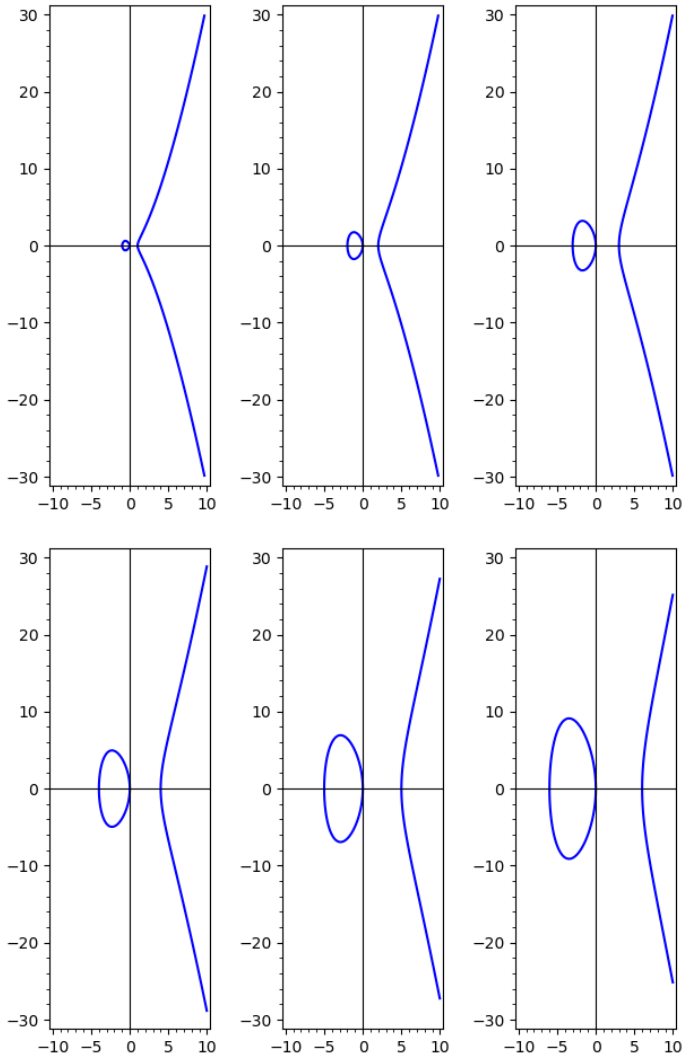
N	(a, b, c)	(x, y)
29	$\left(\frac{52780}{99}, \frac{99}{910}, \frac{48029801}{90090}\right)$	$\left(\frac{142129}{4900}, \frac{1082367}{343000}\right)$
29	$\left(\frac{99}{910}, \frac{52780}{99}, \frac{48029801}{90090}\right)$	$(284229, 151531380)$
30	$(12, 5, 13)$	$(45, 225)$
30	$(5, 12, 13)$	$(150, 1800)$
30	$\left(\frac{119}{26}, \frac{1560}{119}, \frac{42961}{3094}\right)$	$\left(\frac{8670}{49}, \frac{795600}{343}\right)$
30	$\left(\frac{1560}{119}, \frac{119}{26}, \frac{42961}{3094}\right)$	$\left(\frac{169}{4}, \frac{1547}{8}\right)$
31	$\left(\frac{720}{287}, \frac{8897}{360}, \frac{2566561}{103320}\right)$	$\left(\frac{49600}{81}, \frac{11032280}{729}\right)$
31	$\left(\frac{8897}{360}, \frac{720}{287}, \frac{2566561}{103320}\right)$	$\left(\frac{1681}{49}, \frac{29520}{343}\right)$
34	$\left(24, \frac{17}{6}, \frac{145}{6}\right)$	$\left(\frac{153}{4}, \frac{867}{8}\right)$
34	$\left(\frac{112}{9}, \frac{153}{28}, \frac{3425}{252}\right)$	$\left(\frac{833}{16}, \frac{18207}{64}\right)$
34	$\left(\frac{136}{15}, \frac{15}{2}, \frac{353}{30}\right)$	$\left(\frac{289}{4}, \frac{4335}{8}\right)$
34	$\left(\frac{15}{2}, \frac{136}{15}, \frac{353}{30}\right)$	$\left(\frac{850}{9}, \frac{23120}{27}\right)$
34	$\left(\frac{153}{28}, \frac{112}{9}, \frac{3425}{252}\right)$	$(162, 2016)$
34	$\left(\frac{17}{6}, 24, \frac{145}{6}\right)$	$(578, 13872)$
34	$\left(\frac{3927}{248}, \frac{992}{231}, \frac{939905}{57288}\right)$	$\left(\frac{2178}{49}, \frac{65472}{343}\right)$
34	$\left(\frac{992}{231}, \frac{3927}{248}, \frac{939905}{57288}\right)$	$\left(\frac{16337}{64}, \frac{2069529}{512}\right)$
38	$\left(\frac{1700}{279}, \frac{5301}{425}, \frac{1646021}{118575}\right)$	$\left(\frac{47500}{289}, \frac{10071900}{4913}\right)$
38	$\left(\frac{5301}{425}, \frac{1700}{279}, \frac{1646021}{118575}\right)$	$\left(\frac{58482}{961}, \frac{11046600}{29791}\right)$
39	$\left(\frac{156}{5}, \frac{5}{2}, \frac{313}{10}\right)$	$\left(\frac{169}{4}, \frac{845}{8}\right)$
39	$\left(\frac{5}{2}, \frac{156}{5}, \frac{313}{10}\right)$	$(975, 30420)$
41	$\left(\frac{1023}{40}, \frac{3280}{1023}, \frac{1054721}{40920}\right)$	$\left(\frac{44649}{961}, \frac{4437840}{29791}\right)$
41	$\left(\frac{1189}{420}, \frac{840}{29}, \frac{354481}{12180}\right)$	$(841, 24360)$
41	$\left(\frac{123}{20}, \frac{40}{3}, \frac{881}{60}\right)$	$\left(\frac{1681}{9}, \frac{67240}{27}\right)$
41	$\left(\frac{3280}{1023}, \frac{1023}{40}, \frac{1054721}{40920}\right)$	$\left(\frac{42025}{64}, \frac{8598315}{512}\right)$
41	$\left(\frac{40}{3}, \frac{123}{20}, \frac{881}{60}\right)$	$\left(\frac{1025}{16}, \frac{25215}{64}\right)$
41	$\left(\frac{840}{29}, \frac{1189}{420}, \frac{354481}{12180}\right)$	$\left(\frac{18081}{400}, \frac{1023729}{8000}\right)$
46	$\left(\frac{168}{11}, \frac{253}{42}, \frac{7585}{462}\right)$	$\left(\frac{3312}{49}, \frac{139656}{343}\right)$
46	$\left(\frac{253}{42}, \frac{168}{11}, \frac{7585}{462}\right)$	$(242, 3696)$

Bemerkung: Die Kurven

$$y^2 = x(x^2 - N^2) \quad \text{oder auch} \quad y^2 = x^3 - N^2x \quad \text{oder auch } y^2 = x(x - N)(x + N)$$

sind Beispiele von sogenannten **elliptischen Kurven**. Diese Kurven enthalten immer die Punkte $(0, 0)$, $(N, 0)$, $(-N, 0)$.

Die folgenden Bilder zeigen die Kurven für $N = 1, 2, 3, 4, 5, 6$.



Bemerkung: Die Beschäftigung mit Kongruenzzahlen hat eine lange Geschichte. Zwar sind viele Ergebnisse bekannt, es gibt aber auch eine Reihe offener Fragen. Ein neueres Ergebnis ist das folgende [**Tunnell**]:

Satz (Tunnell 1983). *Sei N eine quadratfreie natürliche Zahl,*

$$A = \begin{cases} \{(x,y,z) \in \mathbb{Z}^3 : 4x^2 + y^2 + 8z^2 = \frac{N}{2}, z \text{ gerade}\}, & \text{falls } N \text{ gerade}, \\ \{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = N, z \text{ gerade}\}, & \text{falls } N \text{ ungerade} \end{cases}$$

und

$$B = \begin{cases} \{(x,y,z) \in \mathbb{Z}^3 : 4x^2 + y^2 + 8z^2 = \frac{N}{2}, z \text{ ungerade}\}, & \text{falls } N \text{ gerade}, \\ \{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = N, z \text{ ungerade}\}, & \text{falls } N \text{ ungerade} \end{cases}$$

Dann gilt:

$$N \text{ Kongruenzzahl} \quad \Longrightarrow \quad \#A = \#B$$
$$N \text{ Kongruenzzahl} \quad \overset{BSD\text{-}Vermutung}{\Longleftarrow} \quad \#A = \#B$$

(Dabei steht BSD-Vermutung für eine Vermutung von Birch und Swinnerton-Dyer.)