Prof. Dr. Rosenberger

Fakultät für Informatik und Mathematik

Schöne Zahlen

Lehrerfortbildung – 18.12.2019

Schönheit in der Mathematik

Aufgabe 1
Geben Sie einen rein zahlentheoretischen Beweis für die Klassifikation der primitiven Pythagoreischen Tripel an.

Hinweis: Sei $a^2 + b^2 = c^2$ mit $a, b, c \in \mathbb{N}$ und $\mathrm{ggT}(a, b, c) = 1$. Schreiben Sie

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

mit a gerade (es ist notwendig a oder b gerade!). Zeigen Sie zunächst $\mathrm{ggT}(c-a, c+a) = 1$ und damit $c + a = x^2, c - a = y^2$ für $x, y \in \mathbb{N}$. Folgern Sie daraus $a = \frac{x^2-y^2}{2}$, $b = xy$ und $c = \frac{x^2+y^2}{2}$.

Beweis. Sei $a^2 + b^2 = c^2$ mit $a, b, c \in \mathbb{N}$ und $\mathrm{ggT}(a, b, c) = 1$. Zunächst ist a oder b gerade. Denn: Sind a und b beide ungerade, so ist $a^2 + b^2 \equiv 2 \pmod 4$ (Beachte: Ist $a = 2k + 1$, so ist $a^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$). Das ergibt einen Widerspruch, denn $c^2 \equiv 0 \pmod 4$ oder $c^2 \equiv 1 \pmod 4$. Es können auch nicht beide a und b gerade sein, da dann auch c gerade sein muss. Dies steht im Widerspruch zu $\mathrm{ggT}(a, b, c) = 1$. Also ist eine von a oder b gerade und die andere ungerade.

Sei ohne Einschränkung a gerade. Wir schreiben $b^2 = c^2 - a^2 = (c - a)(c + a)$. Es ist $\mathrm{ggT}(c - a, c + a) = 1$. Denn: Zunächst ist $c + a$ ungerade da a gerade ist und $\mathrm{ggT}(a, b, c) = 1$ (wäre $c+a$ gerade, so wäre c gerade, also auch b wegen $a^2+b^2 = c^2$).

Da $c + a$ ungerade ist, folgt:

$$\begin{aligned} \mathrm{ggT}(c - a, c + a) &= \mathrm{ggT}(c - a, c + a - (c - a)) = \mathrm{ggT}(c - a, 2a) \\ &= \mathrm{ggT}(c - a, a) = \mathrm{ggT}(c, a) \end{aligned}$$

Wegen $a^2 + b^2 = c^2$ und $\mathrm{ggT}(a, b, c) = 1$ ist $\mathrm{ggT}(a, c) = 1$, also $\mathrm{ggT}(c-a, c+a) = 1$.

Das Produkt der teilerfremden Zahlen $c - a$ und $c + a$ ist b^2, also ein Quadrat. Wegen der Eindeutigkeit der Primfaktorzerlegung (bis auf die Reihenfolge) müssen damit $c-a$ und $c+a$ selbst Quadrate sein. Es gibt also $x, y \in \mathbb{N}$ mit $c+a = x^2$ und $c - a = y^2$. Es folgt $2c = (c + a) + (c - a) = x^2 + y^2$, also $c = \frac{x^2+y^2}{2}$. Analog folgt $a = \frac{x^2-y^2}{2}$. Wegen $(c + a)(c - a) = b^2 = x^2y^2 = (xy)^2$ ist dann $b = xy$.

In der Tat gilt:

$$\left(\frac{x^2-y^2}{2}\right)^2 + (xy)^2 = \left(\frac{x^2+y^2}{2}\right)^2 \qquad \square$$

Bemerkung: Für $(x, y) = (3, 1)$ erhalten wir $(a, b, c) = (4, 3, 5)$; für $(x, y) = (5, 1)$ erhalten wir $(a, b, c) = (12, 5, 13)$.

Aufgabe 2

a) Eine Zahl der Form $M_n = 2^n - 1$ mit $n \in \mathbb{N}, n \geq 2$, heißt *Mersenne Zahl.* Ist M_n eine Primzahl, so nennen wir M_n eine *Mersennesche Primzahl.*

Zeigen Sie: Ist M_n eine Primzahl, so ist n selbst eine Primzahl.

Beweis. Sei $M_n = 2^n - 1, n \geq 2$ eine Primzahl. Angenommen $n = ab$ mit $2 \leq a, b < n$. Dann ist

$$M_n = 2^n - 1 = (2^a)^b - 1 = (2^a - 1)(1 + 2^a + \cdots + (2^a)^{b-1}).$$

Beide Faktoren auf der rechten Seite sind größer als 1. Dies ist ein Widerspruch, da M_n eine Primzahl ist. Also kann n nicht zusammengesetzt sein, d.h. n muss eine Primzahl sein. □

Bemerkung: M_p ist Primzahl für $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ und 257. Für alle anderen Primzahlen p mit $p \leq 257$ ist M_p keine Primzahl. Es ist etwa $M_{11} = 2^{11} - 1 = 23 \cdot 89$. Zur Zeit sind 51 Mersennesche Primzahlen bekannt. Die größte ist $2^{82589933} - 1$.

Bemerkung: Für Mersennesche Primzahlen gibt es den Lucas-Lehmer Test: Sei $p \geq 3$ eine Primzahl. Definiere rekursiv die Folge $(S_n)_{n\in\mathbb{N}}$ durch $S_1 = 4$ und $S_n = S_{n-1}^2 - 2$ für $n \geq 2$. Damit ist $M_p = 2^p - 1$ eine Primzahl genau dann wenn $M_p \mid S_{p-1}$.

Dieser Test ist die Grundlage für das Suchprojekt GIMPS nach großen Primzahlen.

b) Sei $n \in \mathbb{N}$ und $\sigma(n) = \sum_{\substack{d|n \\ d\geq 1}} d$ die Summe aller positiven Teiler von n.

Zeigen Sie: Für $n, m \in \mathbb{N}$ gilt $\sigma(n) \cdot \sigma(m) = \sigma(nm)$ falls $ggT(n, m) = 1$.

Beweis. Seien $m, n \in \mathbb{N}$ mit $\operatorname{ggT}(n, m) = 1$, $\sigma(n) = \sum_{\substack{d|n \\ d\geq 1}} d$ und $\sigma(m) = \sum_{\substack{d'|m \\ d'\geq 1}} d'$.

Es ist

$$\sigma(n)\sigma(m) = \left(\sum_{\substack{d|n \\ d\geq 1}} d\right)\left(\sum_{\substack{d'|m \\ d'\geq 1}} d'\right) = \sum_{\substack{d|n \\ d\geq 1}} \sum_{\substack{d'|m \\ d'\geq 1}} dd' = \sum_{\substack{dd'|nm \\ d\geq 1,\, d'\geq 1}} dd' = \sigma(nm)$$

da wegen $\operatorname{ggT}(n, m)$ jeder Teiler von nm von der Form dd' mit $d \mid n$, $d' \mid m$ und $\operatorname{ggT}(d, d') = 1$ ist. □

c) Eine Zahl $n \in \mathbb{N}$ heißt vollkommene Zahl falls $\sigma(n) = 2n$.

Beispiele: $n = 6, 28, 496, 8128$.

Charakterisierung: Sei $n = 2^{s-1}b$ mit $s, b \in \mathbb{N}, s \geq 2$ und b ungerade. Dann sind äquivalent:

(1) b ist eine Mersennesche Primzahl und $b = 2^s - 1$.

(2) n ist vollkommen.

Zeigen Sie: (1) $\Rightarrow$ (2).

Bemerkung: Der Beweis der Richtung (2) $\Rightarrow$ (1) ist etwas aufwendiger. Einen Beweis dafür findet man in dem Buch "Number Theory" von B. Fine und G. Rosenberger (Birkhäuser-Springer, 2016). Dort wird auch der Lucas-Lehmer Test explizit behandelt.

Beweis. Wir zeigen (1) $\Rightarrow$ (2). Sei $b = 2^s - 1$ eine Primzahl. Wegen $b \neq 2$ ist $n = 2^{s-1}b$ die Primfaktorzerlegung von n. Daher ist

$$\begin{aligned}\sigma(n) &= \sigma(2^{s-1})\sigma(b) \\ &= (1 + 2 + \cdots + 2^{s-1})(b + 1) \\ &= (2^s - 1) \cdot 2^s = 2 \cdot 2^{s-1}(2^s - 1) \\ &= 2n.\end{aligned}$$

□

Bemerkungen:

1) Wir zeigen nun die Implikation (2) $\Rightarrow$ (1) von Euler (1707-1783).

   Sei $n = 2^{s-1}b$ mit $s \geq 2$, b ungerade, eine (gerade) vollkommene Zahl. Die positiven Teiler von n sind von der Form $2^t m$ mit $0 \leq t < s$ und $m \mid b$. Es folgt

   $$\sigma(n) = (1 + 2 + \cdots + 2^{s-1})\,\sigma(b) = (2^s - 1)\,\sigma(b).$$

   Da n vollkommen ist, folgt $\sigma(n) = 2n$, also erhalten wir $2^s b = (2^s - 1)\,\sigma(b)$. Damit muss $\sigma(b)$ gerade sein, denn b und $2^s - 1$ sind ungerade. Wir erhalten $b = (2^s - 1)a$ und $\sigma(b) = 2^s a, a \in \mathbb{N}$, nach Euklids Lemma:

   Sind $x, y, z \in \mathbb{Z} \setminus \{0\}$, $x \mid yz$ und $\mathrm{ggT}(x, y) = 1$, so gilt $x \mid z$. (Der Euklidische Algorithmus liefert eine Darstellung $ux + vy = 1$ mit $u, v \in \mathbb{Z}$; also ist $uxz + vyz = z$. Aus $x \mid yz$ und $x \mid x$ folgt $x \mid z$).

   Die Zahl b hat die Teiler a und $(2^s - 1)a > a$. Ihre Summe ist $2^s a = \sigma(b)$. Dies ist nur möglich, wenn $b = (2^s - 1)a$ keine anderen positiven Teiler hat. Dies bedeutet $a = 1$ und $2^s - 1$ ist eine Primzahl, und nach a) muss s eine Primzahl sein. Also ist $b = 2^s - 1$ eine Mersennesche Primzahl.

2) Es bleiben die Fragen: Gibt es unendlich viele gerade vollkommene Zahlen und damit unendlich viele Mersennesche Primzahlen? Gibt es ungerade vollkommene Zahlen?

d) Die m-te Dreieckszahl $T_m, m \in \mathbb{N}$, ist definiert durch

$$T_m = \sum_{k=1}^{m} k = \frac{m(m+1)}{2}.$$

Zeigen Sie: Ist n eine gerade vollkommene Zahl, so ist n eine Dreieckszahl.

Bemerkung: Es ist nicht bekannt, ob es ungerade vollkommene Zahlen gibt.

Beweis. Sei n eine gerade vollkommene Zahl. Wegen c) können wir $n = 2^{p-1}(2^p - 1)$ für $p \in \mathbb{N}$ und $p \geq 2$ schreiben. Setze $m = 2^p - 1$. Dann ist

$$T_m = \frac{m(m+1)}{2} = \frac{(2^p-1) \cdot 2^p}{2} = n.$$

□

Aufgabe 3

Wir setzen $f_0 = 0$, $f_1 = 1$ und $f_2 = 1$, und für $n \geq 3$ sei f_n die Anzahl aller $0-1$ Folgen der Länge $n-2$, bei denen keine zwei Einsen nebeneinander stehen. Zeigen Sie:

a) $f_n = f_{n-1} + f_{n-2}$ für $n \geq 3$.

Beweis. Wir haben $f_0 = 0, f_1 = f_2 = 1$. Sei nun $n \geq 3$. Sei M_n die Menge aller $0-1$ Folgen der Länge $n-2$, bei denen keine zwei Einsen nebeneinander stehen.
Damit ist $|M_3| = f_3 = 2$, da wir genau die Folgen 0 und 1 haben. Ferner ist $|M_4| = f_4 = 3$, da wir genau die Folgen 00, 01 und 10 haben. Sei nun $n \geq 5$ und die Behauptung sei richtig für alle k mit $3 \leq k < n$. Es ist $M_n = M_n^{(0)} \dot\cup M_n^{(1)}$ eine disjunkte Vereinigung von $M_n^{(0)}$, die Menge aller Folgen in M_n, die mit einer 0 enden, und $M_n^{(1)}$, die Menge aller Folgen in M_n, die mit einer 1 enden. Jede Folge in $M_n^{(1)}$ muss nach der Definition mit 01 enden. Daher ist

$$f_n = |M_n| = |M_n^{(0)}| + |M_n^{(1)}| = |M_{n-1}| + |M_{n-2}| = f_{n-1} + f_{n-2}.$$

Also gilt allgemein $f_n = f_{n-1} + f_{n-2}$ für $n \geq 3$ nach dem zweiten Induktionsprinzip (dies ist äquivalent zum ersten Induktionsprinzip "vollständige Induktion"). □

b) $f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ für $n \geq 1$, wobei $\alpha = \frac{1+\sqrt{5}}{2}$ die Goldene-Schnitt-Zahl ist und $\beta = -\alpha^{-1} = \frac{1-\sqrt{5}}{2}$.

Hinweis: α und β sind die Lösungen der Gleichung $x^2 = x + 1$, also gilt für $n \geq 1$:

$$\alpha^{n+2} = \alpha^{n+1} + \alpha^n \text{ und } \beta^{n+2} = \beta^{n+1} + \beta^n$$

Beweis. Die Zahlen α und β sind die beiden Lösungen der Gleichung $x^2 - x - 1 = 0$, d.h. es ist $\alpha^2 = \alpha + 1$ und $\beta^2 = \beta + 1$. Das ergibt $\alpha^{n+2} = \alpha^{n+1} + \alpha^n$ und $\beta^{n+2} = \beta^{n+1} + \beta^n$ nach Multiplikation mit α^n bzw. β^n.
Es ist $\alpha - \beta = \sqrt{5} \neq 0$. Für $n = 1$ ist $1 = \frac{\alpha-\beta}{\alpha-\beta} = f_1$ und für $n = 2$ ist $1 = \frac{\alpha^2-\beta^2}{\alpha-\beta} = \alpha + \beta = f_2$. Nach dem zweiten Induktionsprinzip folgt allgemein für $n \geq 1$:

$$\begin{aligned} f_{n+2} = f_{n+1} + f_n &= \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} + \frac{\alpha^n - \beta^n}{\alpha - \beta} \\ &= \frac{\alpha^{n+1} + \alpha^n - (\beta^{n+1} + \beta^n)}{\alpha - \beta} = \frac{\alpha^{n+2} - \beta^{n+2}}{\alpha - \beta} \end{aligned}$$ □

Bemerkung: Die Zahlen f_n, $n \geq 0$, heißen die *Fibonacci-Zahlen.* Diese haben viele Eigenschaften, etwa:

(1) $f_1 + f_2 + \ldots + f_n = f_{n+2} - 1$ für $n \geq 1$.

(2) $f_1^2 + \ldots + f_n^2 = f_n f_{n+1}$ für $n \geq 1$.

(3) $f_{n+m} = f_{n-1} f_m + f_n f_{m+1}$ für $n, m \geq 1$.

(4) $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$, und damit insbesondere $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$ für $n \geq 1$.

(5) $ggT(f_n, f_m) = f_{ggT(n,m)}$ für $n, m \geq 1$.

Beweise hierfür findet man in dem Buch "Number Theory" von B. Fine und G. Rosenberger (Birkhäuser-Springer, 2016).

c) Zeigen Sie die Eigenschaften (2) und (4).

Beweis. Zu (2): Es ist $f_1^2 = 1 = f_1 f_2$. Sei nun $n \geq 2$ und die Behauptung richtig für $n - 1$. Dann folgt

$$f_1^2 + \cdots + f_n^2 = (f_1^2 + \cdots + f_{n-1}^2) + f_n^2 = f_{n-1} f_n + f_n^2 = f_n(f_n + f_{n-1}) = f_n f_{n+1}.$$

Zu (4): Es ist $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^1 = \begin{pmatrix} f_2 & f_1 \\ f_1 & f_0 \end{pmatrix}$. Sei nun $n \geq 2$ und die Behauptung richtig für $n - 1$. Dann folgt

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_n & f_{n-1} \\ f_{n-1} & f_{n-2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} f_n + f_{n-1} & f_n \\ f_{n-1} + f_{n-2} & f_{n-1} \end{pmatrix} = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}. \end{aligned}$$

Sei $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Dann gilt $\det A = -1$ für die Determinante von A. Nach der Multiplikationsregel für Determinanten folgt $\det A^n = (\det A)^n = (-1)^n$ für $n \geq 1$. Wegen $A^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$ gilt $\det A^n = f_{n+1} f_{n-1} - f_n^2$ für $n \geq 1$. Das ergibt die Behauptung: $f_{n+1} f_{n-1} - f_n^2 = \det(A^n) = (\det A)^n = (-1)^n$. $\square$

Bemerkung: Die Eigenschaften (1) und (3) folgen ähnlich durch Induktion (bei (3) nehme man ein beliebiges, aber festes m). Die Eigenschaft (5) ist hingegen nicht so einfach zu zeigen.