Ungelöste Probleme der Zahlentheorie

"egy" ist ungarisch für "eins" ☺

Teil 1: Ägyptische Brüche ("Egyptian fractions") und die Erdős-Straus-Vermutung

Def. 1: Ein ägyptischer Bruch bzw. Stammbruch ist ein Bruch der Form $\frac{1}{n}$ mit $n \in \mathbb{N}$.

Jeder Bruch $\boxed{\frac{z}{n}}$ mit $1 < z < n$ kann als endl. Summe von verschiedenen Stammbrüchen der Form $\frac{1}{k}$ geschrieben werden („ägyptische Darstellung"): Man spalte den größten Stammbruch ab, so daß der Rest nichtneg. ist, und verfahre ebenso mit dem Rest.

Bsp.: $\frac{4}{17} = \frac{1}{5} + \frac{1}{29} + \frac{1}{1233} + \frac{1}{3039345}$. Oder: $\frac{31}{311} = ?$

Oft existieren ägyptische Darstellungen mit weniger Summanden und kleineren Nennern, hier etwa $\frac{4}{17} = \frac{1}{6} + \frac{1}{15} + \frac{1}{510}$. Kurze äg. Darstellungen sind sehr effektiv, da oft nur wenige Stammbrüche benötigt werden:

Sei $a(z,n)$ die Mindestzahl der Summanden in einer ägyptischen Darst. von $\frac{z}{n}$, $\operatorname{ggT}(z,n) = 1$

d.h. wir definieren $a(z,n) := \min\{k \in \mathbb{N};\ \exists m_1, \dots, m_k \in \mathbb{N} : \frac{z}{n} = \frac{1}{m_1} + \dots + \frac{1}{m_k}\}$.

(die m_i paarweise verschieden)

Dann gilt im Fall $z = 4$:

Satz 2 (Erdős): Die Menge $\{n \geq 5;\ a(4,n) > 2\}$ hat die asymptotische Dichte 0.

Beweis: Ist $p \equiv 3\ (4)$, gilt $\frac{4}{p} = \frac{1}{k} + \frac{1}{kp}$ mit $k = \frac{p+1}{4}$, $\left[\frac{4}{p+1} + \frac{4}{p(p+1)} = \frac{4p+4}{p(p+1)} = \frac{4}{p}\right]$

(OE n ungerade) also $\frac{4}{pm} = \frac{1}{km} + \frac{1}{kpm}$ für alle $m \in \mathbb{N}$.

Somit gilt $a(4,n) > 2$ nur, wenn $(p \mid n \Rightarrow p \equiv 1\ (4))$. Dann ist aber $n = a^2 + b^2$ nach Euler-Lagrange, und mit ⊛: $\frac{q(x)}{x} = O\left(\frac{1}{\sqrt{\log x}}\right) \xrightarrow[x \to \infty]{} 0$ folgt die Beh. □

Hier ist $q(x) := \#\{n \leq x;\ \exists a, b \in \mathbb{Z} : n = a^2 + b^2\}$.

Die hier verwendete Abschätzung ⊛, $q(x) = O\left(\frac{x}{\sqrt{\log x}}\right)$, kann mit dem sogenannten Selberg-Sieb, eine Methode der Siebtheorie, bewiesen werden. (vgl. frühere Vorlesung)

Satz aus der elementaren Zahlentheorie: Zahlen, die Summe zweier Quadratzahlen sind, sind genau die Zahlen, in denen Primfaktoren $\equiv 3\ (4)$ nur in gerader Potenz vorkommen.

Bem.: $a \equiv b\ (m)$
$\Leftrightarrow m \mid b - a$
$\Leftrightarrow m$ teilt $b - a$
$\Leftrightarrow a \equiv b \bmod m$

$f(x) = O(g(x))$
$:\Leftrightarrow \exists C > 0$
$\forall x : |f(x)| \leq C g(x)$

Man gelangt so zu folgender Vermutung:

Für alle $\frac{z}{n}$ mit $z \in \mathbb{N}$ fest ex. ein $n_0(z) > z$, sodaß für alle $n \geq n_0(z)$ gilt:
$\frac{z}{n}$ hat ägyptische Darstellung mit höchstens 3 Summanden.

Die Vermutung stimmt für $z=2$ wegen $\frac{2}{n} = \frac{1}{k} + \frac{1}{kn}$ mit $k = \frac{n+1}{2}$ für $n>2$, $2 \nmid n$,
sowie für $z=3$ wegen $\frac{3}{n} = \frac{1}{k} + \frac{1}{kn}$ mit $k = \frac{n+1}{3}$ für $n>3$, $n \equiv -1 (3)$,
und $\frac{3}{n} = \frac{1}{k} + \frac{2}{kn}$ mit $k = \frac{n+2}{3}$ für $n>3$ $n \equiv +1 (3)$, ist k_n ungerade, verwende $z=2$-Fälle!

hier reichen sogar zwei Summanden

Für $z=4$ wird vermutet, dass alle $\frac{4}{n}$, $n \in \mathbb{N}$ ungerade, Summe von höchst. 3 Stammbrüchen ist. Dies heißt die Vermutung von Erdős–Straus und ist nach wie vor ungelöst.
Sie stammt aus Arbeiten von Erdös und Straus, welche um 1970 herum erschienen sind.
Sie ist mittlerweile bewiesen außer in den Fällen
$n \equiv 1^2, 11^2, 13^2, 17^2, 19^2, 23^2 \mod 840$ (vgl. Mordell/R.Guy)
sowie für alle $n \leq 10^{14}$.
Es gibt eine Vielzahl weiterer Teilergebnisse zur E-S-Vermutung.
Man kann zeigen, dass fast immer mind. 3 Summanden für ein festes z reichen:

__Satz 3:__ (Vaughan, 1970): $\boxed{\# \{ n \leq x;\ \underset{(n,z)=1}{} \frac{z}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \text{ unlösbar} \} = O\left(\frac{x}{(\log x)^{1/\varphi(z)}}\right)}$

__Satz 4:__ (Hofmeister/Stoll) (1985): $\boxed{\# \{ n \leq x;\ (n,z)=1,\ a(z,n) > 2 \} = O\left(\frac{x}{(\log x)^{1/\varphi(z)}}\right)}$ (vgl. Skript zur Siebtheorie)

(hier ist $\varphi(z) := \# \{ m \leq z;\ m \geq 1,\ \underbrace{ggT(m,z)}_{\text{schreiben auch: } (m,z)} = 1 \}$ die Eulersche φ-Funktion)

Kettenbruch: $[a_0, a_1, a_2, \dots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$

a_i heißen "Teilbrüche"

Wir untersuchen jetzt [nach Elsner / Sander / Steuding], welche Kettenbrüche sich als Summe zweier Stammbrüche schreiben lassen. Wir zeigen: Für eine Folge $a_2, \dots, a_m \in \mathbb{N}$ gibt es einen KB der Länge m, der die Folge als Teilbrüche enthält und der die Summe zweier Stammbrüche ist. Dazu folgende Konstruktion.

Sei $a_1, \dots, a_m$ eine (endl.) Folge natürlicher Zahlen.

Def 5: Muir symbol: $A_n = \langle a_n, a_{n+1}, \dots, a_m \rangle$ für $n = 1, \dots, m$, wird rekursiv def. als

$$A_{m+1} = \langle\,\rangle := 1, \quad A_m := a_m, \quad A_n := a_n A_{n+1} + A_{n+2}$$

für $n = 1, \dots, m-1$.

Klar: alle $A_n \in \mathbb{N}$, $\mathrm{ggT}(A_n, A_{n+1}) = 1$,

sowie $[0, a_1, \dots, a_m] = \frac{A_2}{A_1}$ (Vollst. Ind.)

Bsp.: Sind alle $a_i = 1$, folgt $A_{m-i} = f_{i+2}$, die $(i+2)$-ten Fibonaccizahl

Es gilt:

Satz 6: Für $m \geq 2$ seien $a_2, \dots, a_m \in \mathbb{N}$. Dann gilt für alle $k \in \mathbb{N}$, $(A_2 - 1)k > A_3$:

$$[0, (A_2 - 1)k - A_3, a_2, \dots, a_m] = \frac{1}{A_2 k - A_3} + \frac{1}{(A_2 k - A_3)(A_2 - 1)}.$$

r.S. = "rechte Seite"

Bew.: Für $a_1 \in \mathbb{N}$ ist $[0, a_1, \dots, a_m] = \frac{A_2}{A_1} = \frac{A_2}{a_1 A_2 + A_3}$, dies und die r.S. $= \frac{1}{A_2 k - A_3} + \frac{1}{(A_2 k - A_3)(A_2 - 1)}$

$= \frac{A_2}{(A_2 k - A_3)(A_2 - 1)}$ sind gleich genau wenn $a_1 = (A_2 - 1)k - A_3$, falls $(A_2 - 1)k - A_3 > 0$. $\square$

Zweck: Für Zahlen $\frac{4}{n} = [0, a_1, \dots, a_m]$ mit $a_1 = (A_2 - 1)k - A_3$ erlaubt der Satz eine Konstruktion von $\frac{4}{n}$ als Summe zweier verschiedener Stammbrüche.

Hingegen erhalten wir ein eindeutiges Kriterium, wann ein Kettenbruch Summe zweier Stammbrüche ist, wie folgt:

(Bis auf das Auffinden von Teilern von A_1^2 ist das Kriterium algorithmisch machbar.)

PFZ = Primfaktorzerlegung

Satz 7: Seien $a_1,\dots,a_m \in \mathbb{N}$. Dann ist $[0,a_1,\dots,a_m]$ die Summe zweier Stammbrüche genau wenn $A_1 + \prod_{j=1}^{r} p_j^{\mu_j} \equiv 0 \mod A_2$ gilt für gewisse $0 \le \mu_j \le 2\nu_j$, wobei $A_1 = \prod_{j=1}^{r} p_j^{\nu_j}$ die PFZ von A_1 ist.

Bem.: $\prod_j p_j^{\mu_j}$ ist Teiler von A_1^2.

Bew.:
Es ist $[0,a_1,\dots,a_m] = \frac{1}{x} + \frac{1}{y}$ für $x,y \in \mathbb{N}$
genau wenn $A_2 x(z-x) = A_1 z$, $z := x+y$.
Also ist $z = A_2 \omega$ für ein $\omega \in \mathbb{N}$, da $(A_1,A_2)=1$, und die Identität ist äquivalent zu $(A_2 x - A_1)\omega = x^2$.

Jetzt benutzen wir zur Lösbarkeit dieser Identität (in x) folgendes
Lemma 8: (damit ist der Beweis von Satz 7 dann vollendet)
Vor.: $a,b \in \mathbb{N}$, $(a,b)=1$.
Beh.: $\left(\exists x \in \mathbb{N},\ x > \frac{a}{b} : bx-a \mid x^2\right) \iff \left(\exists\, 0 \le \beta_j \le 2\nu_j\ (1 \le j \le r) : b \mid a + \underbrace{\prod_{j=1}^{r} p_j^{\beta_j}}_{\text{Teiler von } a^2}\right)$

wo $a = \prod_{j=1}^{r} p_j^{\nu_j}$ die PFZ von a ist.

Bew.: „⇒": Sei $(bx-a)\omega = x^2$ mit $x = \prod_j p_j^{e_j} \cdot q$, wo $(q,a)=1$ und die $e_j \ge 0$.
Dann: $bx - a = \frac{x^2}{\omega} = \frac{q^2}{\omega} \cdot \prod_j p_j^{2e_j}$,

also $bq \prod_j p_j^{e_j} = \frac{q^2}{\omega} \cdot \prod_j p_j^{2e_j} + a$. ⊛ z.z.: $\frac{q^2}{\omega} \overset{!}{=} 1$.
Ann.: $p \mid \frac{q^2}{\omega}$, p prim, $\forall j : p \ne p_j$.
Dann ist $p \mid q$ und wegen ⊛ folgt $q \mid a$, im ↯ zu $(q,a)=1$. Also ist $\omega = q^2$.
• Weiter folgt $\underbrace{bq \prod_j p_j^{e_j}}_{x} - \underbrace{\prod_j p_j^{2e_j}}_{\leadsto \beta_j := 2e_j} = \underbrace{\prod_j p_j^{\nu_j}}_{a}$, also $e_j \le \nu_j$. Es folgt die Beh.

„⇐": Sei $bt = a + \prod_j p_j^{\beta_j}$, die $\beta_j \le 2\nu_j$. Da $(a,b)=1$, ist $\forall j : p_j^{\min(\nu_j,\beta_j)} \mid t$,
also ist $bt - a = \prod_j p_j^{\beta_j} \mid t^2$, denn $\beta_j \le \min(2\nu_j, 2\beta_j) = 2\min(\nu_j,\beta_j)$. □