(I) Einführung

§0: Notationen, Vereinbarungen

- $\mathbb{P} := \{p \in \mathbb{N};\ p \text{ prim}\}$ die Menge der Primzahlen (kurz: PZen)
- $\mathbb{P}_k := \{n \in \mathbb{N};\ n$ hat in Primfaktorzerlegung höchst. k viele Primfaktoren$\}$
  die Menge der Fastprimzahlen des Typs k / Ordnung k
- $A = O(B) \iff A \ll B \iff B \gg A :\iff \exists c > 0 : |A| \leq c \cdot B$
  (A komplexwertige Funktion, B Funktion mit reellen positiven Werten)
  O-Notation bzw. Vinogradov-Notation
- $\#\mathcal{A}$ Kardinalität einer endl. Menge $\mathcal{A}$

§1: Motivation, Einführung in Siebprobleme

Einige Fragestellungen, die als Siebproblem formuliert werden können:

(1) Ist jede gerade Zahl $n \geq 2$ Summe zweier PZen?
(Goldbachsche Vermutung)

(2) Gibt es ∞ viele PZpaare (p, q) mit $q = p + 2$?
(Primzahlzwillingsvermutung)

(3) Gibt es beliebig lange arithmetische Progressionen $\{a, a+q, a+2q, \dots, a+rq\}$, die nur aus PZen bestehen?

(4) Gibt es ∞ viele PZen der Form $n^2 + 1$, $n \in \mathbb{N}$?

(5) Gibt es für jedes $n \in \mathbb{N}$ eine Primzahl p mit $n^2 < p < (n+1)^2$?

(6) Gibt es für jedes $\varepsilon > 0$ eine Zahl $N(\varepsilon) \in \mathbb{N}$, so daß für jedes $N > N(\varepsilon)$ das Intervall $[N, N + N^{\varepsilon}]$ eine quadratfreie Zahl m (mit $d^2 | m \Rightarrow d = 1$) enthält?

(7) Gibt es für ein $\gamma \leq \frac{1}{4}$ und jedes genügend große $x > 0$ ein Paar $(m, n) \in \mathbb{N}^2$ mit $x \leq m^2 + n^2 < x + x^{\gamma}$?

Die Siebtheorie hat auf diese Fragen folgende (Teil-)Antworten:

(1): $\#\{(p,p')\in\mathbb{P}^2;\ p+p'=2n\} \ll \frac{\sigma(n)}{n}\cdot\frac{n}{(\log n)^2}$,

wobei $\sigma(n):=\sum_{t\mid n} t$ die Teilersummenfunktion bezeichnet.

Vermutet wird, daß auch „$\gg$" anstelle „$\ll$" gilt

Weiter (Chen 1973):

$\#\{(p,p')\in(\mathbb{P},\mathbb{P}_2);\ p+p'=2n\} \gg \frac{n}{(\log n)^2}$

und

(2): $\#\{p\in\mathbb{P};\ p\le x,\ p+2\in\mathbb{P}_2\} \gg \frac{x}{(\log x)^2}$.

Brun (1915): $\#\{p\in\mathbb{P};\ p\le x,\ p+2\in\mathbb{P}\} \ll \frac{x}{(\log x)^2}\cdot(\log\log x)^2$

woraus $\sum_{\substack{p\in\mathbb{P},\\ p+2\in\mathbb{P}}}\frac{1}{p}<\infty$ folgt (Beweis später, mit partieller Summation)

(4): Iwaniec (1978): $\#\{n\le x;\ n^2+1\in\mathbb{P}_2\} \gg \frac{x}{\log x}$

(3): Heath-Brown (1978): $\#\{n\equiv l \pmod k;\ n\in\mathbb{P}_2,\ n\le k^2\}$

$$\ge \frac{k^2}{\varphi(k)\log k}$$ für k groß genug und $(l,k)=1$.

Die Frage in (3) wurde positiv beantwortet von Green/Tao (2004). Alle anderen Fragen sind bis heute offen.

Weitere Teilantworten liefert die Siebtheorie. Diese findet mittlerweile auch in anderen Bereichen der Mathematik Anwendungen.

Wie können obige Fragestellungen als Siebproblem formuliert werden?

Vorbild: <u>Sieb des Eratosthenes:</u> (275 – 195 v.u.Z.)

Sei $x > 0$ und $\mathcal{A} := \{n \leq x\}$,
etwa $x = 25$: $(\sqrt{25} = 5)$

$$(1)\ \cancel{2}\ \cancel{3}\ \cancel{4}\ \cancel{5}\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}\ \cancel{21}\ \cancel{22}\ 23\ \cancel{24}\ \cancel{25}$$

Für jede PZ $p \leq \sqrt{x}$ streiche alle $\lfloor \frac{x}{p} \rfloor$ Vielfachen von p, in der Liste verbleiben alle Primzahlen zwischen $\sqrt{x}$ und x

(Funktioniert, da zusammengesetzte Zahlen $\leq x$ einen Primteiler $\leq \sqrt{x}$ besitzen).

<u>Formalisierung eines Siebproblems:</u>

Die Grundmenge $\mathcal{A}$ sei eine endliche Folge nichtnegativer reeller Zahlen, also

$$\mathcal{A} = (a_n)_{n \leq x},$$

gelegentlich nimmt man auch einfach irgendeine endliche Menge (diese kann also irgendwelche Objekte enthalten), Folgen können aber wegen der erlaubten Wiederholungen praktischer sein.

Gegeben sei weiter eine allgemeine Menge $\mathcal{P} \subseteq \mathbb{P}$ von Primzahlen.
Für ein $z > 1$ reell definiert man

$$\boxed{P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p}$$

Im Eratosthenes-Bsp.: $\mathcal{P} = \mathbb{P}$, $z = \sqrt{x}$.
Idee: übrigbehalten werden alle ungestrichenen $n \leq x$, d.h. die mit <u>$\mathrm{ggT}(n, P(z)) = 1$.</u>
$\leadsto$ PZen zwischen $\sqrt{x}$ und x

Üblicherweise möchte man die Elemente der gesiebten Menge <u>zählen</u> und betrachtet daher die

Siebfunktion: $$S(\mathcal{A},\mathcal{P},z) := \sum_{\substack{n\in\mathcal{A}\\ (n,P(z))=1}} 1$$

Es gilt: $S(\mathcal{A},\mathcal{P},z) = \#\{n\in\mathcal{A};\ p\mid n \Rightarrow p\geq z \text{ für } p\in\mathcal{P}\}$.

In der Formulierung mit einer Folge $\mathcal{A}=(a_n)_{n\leq x}$: $$S(\mathcal{A},\mathcal{P},z) := \sum_{\substack{n\leq x\\ (n,P(z))=1}} a_n$$

Im Eratosthenes-Bsp.:

$\mathcal{A}=\{n\leq x\}$ bzw. $\mathcal{A}=(a_n)_{n\leq x}$ mit $a_n:=1$ für alle n.

Es gilt dann $S(\mathcal{A},\mathcal{P},\sqrt{x}) = \pi(x)-\pi(\sqrt{x})$ mit der <u>Primzahlzählfunktion</u> $\pi(x) := \#\{p\leq x;\ p\in\mathbb{P}\}$.

Ist $\sqrt{x}<z\leq x$, so ist $S(\mathcal{A},\mathcal{P},z) = \pi(x)-\pi(z)$.

$\rightsquigarrow$ zählen PZen in Intervallen!

Meist ist (a_n) die charakteristische Funktion einer Menge $\mathcal{A}\subseteq\mathbb{N}$, dann muß nicht zwischen „Mengen“ und „Folgen“ unterschieden werden.

In Siebproblemen hat man immer das Problem, gute Abschätzungen für die Siebfunktion zu finden. Siebsätze liefern diese unter bestimmten Voraussetzungen, die ein Sieb erfüllen muß.

Zur Formulierung der Probleme (1) & (7) als Siebproblem:

Zu (1): $\mathcal{A} = \{ n(2N-n);\ n \in \mathbb{N},\ 2 \le n \le 2N-2 \}$, $\mathcal{P} = \mathbb{P}$.

Dann:

$$S(\mathcal{A}, \mathcal{P}, \sqrt{2N}) = \# \{ p \in \mathbb{P};\ 2N-p \in \mathbb{P};\ \sqrt{2N} \le p,\ 2N-p \le 2N-2 \}$$

Siebfunktion zum Goldbach-Problem

Zu (7): $\mathcal{A} = \{ n \in \mathbb{N};\ n < x \}$, $\mathcal{P} = \{ p \in \mathbb{P};\ p \equiv 3\ (4) \}$

Dann:

$$S(\mathcal{A}, \mathcal{P}, x) = \# \{ n \in \mathbb{N};\ n < x,\ p \nmid n \text{ für } p \in \mathbb{P},\ p \equiv 3\ (4) \}$$

$$\underset{\uparrow}{=} \# \{ n \in \mathbb{N};\ n < x,\ n = l^2 + m^2 \text{ für } l, m \in \mathbb{N},\ (l,m) = 1 \}$$

Satz von Euler (elementare ZT)

Siebfunktion für Summen zweier $\square$e

Ü

> Zeigen Sie: Für alle hinreichend großen x ist
> $\{ (m,n) \in \mathbb{N}^2;\ x \le m^2 + n^2 < x + 8x^{1/4} \} \ne \emptyset$.

Weiteres Einsatzgebiet der Siebtheorie:

- Artins Vermutung: Sei $m \in \mathbb{Z} \setminus \{0, 1, -1\}$ keine Quadratzahl. Gibt es dann ∞ viele PZen p, für die m eine Primitivwurzel mod p ist? (D.h. so, daß m die mult. Gruppe von $\mathbb{Z}/p$ erzeugt)

Bewiesen: • eine von drei beliebigen ganzen Zahlen a, b, c (nicht $0, \pm 1$, kein $\square$) ist PW mod p für ∞ viele PZen p.

• GRH für Dedekind-ζ-Fkt. bestimmter Kummer-Erweiterungen $\Rightarrow$ Artins V.

- Lang-Trotter-Vermutung: Analogon der Artin-Vermutung für elliptische Kurven

§2: Einige zahlentheoretische Vorbereitungen: Zahlentheoretische Funktionen

Bem.: Schreiben den ggT von $m, n \in \mathbb{N}$ als (m,n). Besteht Verwechslungsgefahr mit $(m,n) \in \mathbb{N}^2$, schreiben wir $\operatorname{ggT}(m,n)$.

Def. 1: • Zahlentheoretische Funktion: $f: \mathbb{N} \to \mathbb{C}$,
Menge: $\mathcal{F} := \{ f: \mathbb{N} \to \mathbb{C} \}$

• $f \in \mathcal{F}$ multiplikativ $:\Leftrightarrow \forall m,n \in \mathbb{N},\ (m,n)=1:$
$$f(mn) = f(m) f(n)$$

• $f \in \mathcal{F}$ additiv $:\Leftrightarrow \forall m,n \in \mathbb{N},\ (m,n)=1:$
$$f(mn) = f(m) + f(n)$$
(z.B. $f = \log$)

Def. 2: • (zahlentheoretische) Faltung: $f, g \in \mathcal{F}$, dann heißt $f * g \in \mathcal{F}$,
$$\boxed{(f*g)(n) := \sum_{d \mid n} f(d)\, g\left(\tfrac{n}{d}\right)} = \sum_{\substack{d,t \mid n \\ dt = n}} f(d) g(t)$$
die Faltung von f und g ($t = \frac{n}{d}$ „Gegenteiler" von d)

• Funktion $\varepsilon(n) := \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & n=1 \\ 0, & \text{sonst} \end{cases}$

$\mathbb{1}(n) := 1$

Bem.: Eine mult. Funktion f ist durch Angabe der Werte $f(p^k)$ bestimmt wegen $f(n) \underset{\text{PFZ}}{=} f(p_1^{k_1} \cdots p_r^{k_r}) = f(p_1^{k_1}) \cdots f(p_r^{k_r})$.

Satz 1: (1) $(\mathcal{F}, *)$ ist abelsche Halbgruppe mit neutr. El. ε

(2) $\mathcal{I} := \{f \in \mathcal{F};\ f(1) \neq 0\}$ ist mit $*$ eine abelsche Gruppe mit neutralem El. ε

(3) $\mathcal{M} := \{f \in \mathcal{F};\ f \text{ multiplikativ}\}$ ist Untergruppe von $(\mathcal{I}, *)$

(4) Das Faltungsinverse der Fkt. $\mathbb{1}$ ist die Möbiusfunktion

$$\mu(n) := \begin{cases} 1, & n = 1 \\ 0, & n \text{ durch Quadratzahl teilbar,} \\ (-1)^m, & n = p_1 \cdots p_m \text{ mit } m \text{ vielen p.w.v. Pzen } p_1, \ldots, p_m \end{cases}$$

D.h. es gilt

$$\boxed{\mu * \mathbb{1} = \varepsilon}$$

bzw.

$$\boxed{\sum_{d|n}' \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & \text{sonst} \end{cases}}$$

Bem.:

$\mu^2(n) = 1$

$\Leftrightarrow n$ ist $\square$frei

$\Leftrightarrow (d^2 | n \Rightarrow d = 1)$

Beweisskizze: Kommut.: ✓, assoz.: schreibe $(f*g)(n) = \sum_{\substack{d_1|n \\ d_2|n \\ d_1 d_2 = n}} f(d_1) g(d_2)$, rechnen ...

ε neutral: $(f*\varepsilon)(n) = f(n)$ ✓

(2), (3): Invertierbarkeit in $\mathcal{I}$ bzw. $\mathcal{M}$:

ist f geg., löse $g * f = \varepsilon$ rekursiv nach g auf (induktiv nach $n = 1, 2, \ldots$)

$\rightsquigarrow g$ mult.

$\mathbb{1} * \mu$ mult., $(\mathbb{1} * \mu)(p^k) = \mu(1) + \mu(p) = 1 - 1 = 0 \rightsquigarrow (4)$ ✓

Satz 2: **Möbiussche Umkehrformel:** $F, f \in \mathcal{F}$, dann gilt:

$$F = f * \mathbb{1} \Leftrightarrow f = F * \mu$$

Bew.: Folgt aus Satz 1, Teil (4). $\square$

Beispiele für zahlentheoretische Funktionen:

① **Eulersche φ-Fkt.:** $\varphi(n) := \#\{1 \le a \le n;\ (a,n)=1\}$

ist multiplikativ, $\varphi * 1\!\!1 = id$, d.h. $\boxed{\sum_{d|n} \varphi(d) = n}$

$\Leftrightarrow \varphi = \mu * id$

Bew.: Haben $\varphi(p^k) = p^k - p^{k-1}$.

Also: $1\!\!1 * \varphi(p^r) = 1 + \sum_{k=1}^{r} (p^k - p^{k-1}) = p^r$, d.h. $1\!\!1 * \varphi = id$,

da $1\!\!1 * \varphi$ mult. □

Eigenschaft: $\sum_{n \le N} \varphi(n) = \frac{3}{\pi^2} N^2 + O(N \log N)$

② Für $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ def. wir:

Teileranzahlfunktion:	$d(n) := (k_1+1) \cdots (k_r+1)$ $\quad d = 1\!\!1 * 1\!\!1$	mult.
Primteileranzahl:	$\nu(n) := r$	add.
Primfaktorenanzahl:	$\Omega(n) := k_1 + \ldots + k_r$	add.
Teilersummenfunktion:	$\sigma(n) := \sum_{d|n} d$, d.h. $\sigma = 1\!\!1 * id$	mult.

Auch für diese Fktn. gelten Asymptotiken für ihren Mittelwert.

③ **von Mangoldt-Funktion:** $\Lambda : \mathbb{N} \to \mathbb{R}_{\ge 0}$,

$$\Lambda(n) := \begin{cases} \log p, & n = p^m \\ 0, & n \text{ keine Primpotenz} \end{cases}$$

(weder additiv noch multiplikativ)

Es gilt: $\boxed{\Lambda * 1\!\!1 = \log}$, d.h. $\sum_{d|n} \Lambda(d) = \log n \Leftrightarrow \Lambda = \mu * \log$

Λ ist zum Studium der Anzahl bestimmter PZen oft technisch einfacher handzuhaben als die PZ-Zählfunktion π selbst.