Vorlesung Zahlentheorie II (Analytische ZT)

SoSe '23, hhu
K. Halupczok

a17: Siebmethoden

Stichworte: Konzept Sieb, Siebfunktion PZ Zwillingssieb, Polignac-Vermutung, Satz von Brun/Chen, Pentium-Bug, große und kleine Siebe, Quasiquadrate, kl. quNR

17.1. Einleitung: Wir führen das Konzept eines mathematischen Siebs ein.

Vorbild: Sieb des Eratosthenes: Sei $x>0$ und $\mathcal{A} := \{n \le x\}$, etwa $x = 25$: ($\sqrt{25}=5$)

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

Für jede PZ $p \le \sqrt{x}$ 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 $\le x$ einen Primteiler $\le \sqrt{x}$ besitzen).

17.2. Formalisierung eines Siebproblems: Sei $\mathcal{A}$ eine endliche Menge. Sei $\mathcal{P}$ die Menge der PZen p, für die es eine bestimmte Teilmenge $\mathcal{A}_p \subseteq \mathcal{A}$ gibt.
Problem: Bestimme gute o.S. und u.S. für die Kardinalität der gesiebten Menge $\mathcal{S}(\mathcal{A},\mathcal{P}) := \mathcal{A} \setminus \bigcup_{p\in\mathcal{P}} \mathcal{A}_p$, der Siebfunktion $\#\mathcal{S}(\mathcal{A},\mathcal{P})$.
Mathematisch praktikabel ist die folgende, moderne Notation für ein Siebproblem (eine endl. Folge $(a_n)_{n\le x}$ als $\mathcal{A}$ zu nehmen erlaubt Wiederholungen in der "Liste" der zu streichenden Objekte/Zahlen):

17.3. Def.: Sei $\mathcal{A}=(a_n)_{n\le x}$ eine endliche Folge (typischerweise nat. Zahlen), $\mathcal{P} \subseteq \mathbb{P}$. Für ein $z>1$ reell def. $P(z) := \prod_{\substack{p\in\mathcal{P}\\ p<z}} p$. Die Daten $(\mathcal{A},\mathcal{P},z)$ heißen Sieb.

17.4. Bsp.: Im Eratosthenes-Sieb: $\mathcal{P}=\mathbb{P}$, $a_n = n$, $z=\sqrt{x}$. Die Vielfachen a_n von $p<z$ werden "gestrichen", "mit 0 überschrieben", "fallen durch das Sieb". Im Sieb "übrig" bleiben alle ungestrichenen $a_n = n \le x$, das sind die $n \le x$, wo $ggT(n, P(z)) = 1$.

17.5. **Def.:** In einem Sieb heißt $S(\mathcal{A},\mathcal{P},z) := \sum_{\substack{n\le x\\ (a_n,P(z))=1}} 1$ die Siebfunktion.

17.6. **Bsp.:** Im Eratosthenes-Sieb ist $S(\mathcal{A},\mathcal{P},\sqrt{x})$ die Kardinalität der ungestrichenen Zahlen zwischen $\sqrt{x}$ und x, genau: $S(\mathcal{A},\mathcal{P},\sqrt{x}) = \pi(x) - \pi(\sqrt{x})$.
[Wähle $a_1=0$, sonst $a_n=n$ für $n>1$. Ist $\sqrt{x}\in\mathbb{Z}$, nimm $z=\sqrt{x}+\frac{1}{2}$.]

17.7. **Bsp.:** PZ Zwillingssieb: $a_n := n(n+2)$, $\mathcal{P}=\mathbb{P}$, $x>2$, $z\ge 2$.
Sei $S(\mathcal{A},\mathcal{P},z) = \#\{n\le x;\ (a_n, P(z))=1\}$ die Siebfunktion.
Ist $z>\sqrt{x}+2$, zählen wir mit der Siebfunktion alle PZen p, für die auch $p+2$ PZ ist, d.h. die gesiebte Menge besteht zwischen $\sqrt{x}$ und x genau aus den Primzahlzwillingen $p\in\mathbb{P}$, für die auch $p+2\in\mathbb{P}$ ist.

17.8. PZ Zwillingsvermutung: Es gibt unendl. viele PZ Zwillinge.
Diese Vermutung ist bis heute unbewiesen! Die Siebtheorie kennt Teilantworten, die wir in diesem Kapitel besprechen möchten. Eine Verfeinerung von 17.8 lautet:

17.9. PZ Zwillingsvermutung nach Hardy-Littlewood: Sei $\pi_2(x) := \#\{p\le x;\ p,p+2\in\mathbb{P}\}$.
Dann gilt $\pi_2(x) \sim 2C_2 \int_2^x \frac{dt}{\log^2(t)} \sim 2C_2 \frac{x}{\log^2(x)}$ mit $C_2 := \prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right) = 0.66016\ldots$
Die Konstante $C_2>0$ heißt Zwillingskonstante.

Zur Abschätzung von Siebfunktionen kennt man Siebsätze.
Dazu gehören klassischerweise das Brunsche Sieb und das Selberg-Sieb.
Da das große Sieb eines der neueren ist und stärker als die genannten, wollen wir dieses hier besprechen und zeigen, dass damit die meisten gängigen Anwendungen zu bewerkstelligen sind.
So zeigen wir in a20.10 das folgende Ergebnis (nur für $n=2$, allg. $n\in\mathbb{N}_{\ge 2}$ analog).

17.10. **Satz:** Sei $\pi_n(x) := \#\{p\in\mathbb{P};\ p\le x,\ p+n\in\mathbb{P}\}$ für $2\mid n$,
insb. ist $\pi_2(x)$ die Anzahl der PZ Zwillinge $\le x$.
Dann ist $\pi_n(x) \ll \frac{x}{\log^2(x)} \prod_{p\mid n}\left(1+\frac{1}{p}\right)$ mit absoluter impliziter Konstante. [Nathanson, Thm. 7.2]

17.11. **Bem.:** Die Vermutung von de Polignac (1849) besagt $\pi_n(x) \xrightarrow{x\to\infty} \infty$ für alle geraden $n \in \mathbb{N}$.

Für den Fall $n=2$ hatten wir fest (und gilt nach a20.10):

17.12. **Kor.:** Es ist $\pi_2(x) \ll \frac{x}{\log^2(x)}$.

17.13. **Kor./Satz von Brun:** Sei p_n die (aufsteigende) Folge der PZ Zwillinge p_n (mit $p_n+2 \in \mathbb{P}$).
Dann ist $\sum_{n\geq 1} \left(\frac{1}{p_n} + \frac{1}{p_n+2}\right)$ konvergent. (Bew. $\sum_{n\geq 1} \frac{1}{p_n}$ kgt.)

Bew.: $n = \pi_2(p_n) \ll \frac{p_n}{\log^2(p_n)}$, also ist $\frac{1}{p_n} \ll \frac{1}{n \log^2(p_n)} \ll \frac{1}{n \log^2(n)}$,
und daher

$$\sum_{n\geq 1} \frac{1}{p_n} \ll \sum_{n\geq 1} \frac{1}{n \log^2(n)}, \text{ was kgt.} \qquad \square$$

Brun zeigte diesen Satz 1920 mit einem anderen Siebsatz, der Brunsches Sieb heißt.

17.14. **Bem.:** Der Satz von Brun besagt, dass es deutlich weniger PZ Zwillinge gibt als Pzen. Die offene Frage, ob $\pi_2(x)$ divergiert, d.h. 17.8, bleibt damit aber ungeklärt.

17.15. **Def.:** Die Konstante $\sum_{\substack{p,\, p+2 \\ \text{prim}}} \left(\frac{1}{p} + \frac{1}{p+2}\right) = 1{,}9021604 \pm 5 \cdot 10^{-7}$ heißt auch Brunsche Konstante.

17.16. Beim Versuch, diesen numerischen Wert genauer zu bestimmen, fand T. Nicely im Jahr 1995 einen Bug (= Programmierfehler) im damaligen Intel Pentium Computer Chip. Die Behebung dieses Fehlers hat die Firma Intel viele Millionen Dollar gekostet.

Als bisher bestes Resultat in Richtung PZ Zwillingsvermutung wird folgendes Resultat von 1973 angesehen:

17.17. **Satz von Chen:** Es gibt unendl. viele $p \in \mathbb{P}$, so dass $\Omega(p+2) \leq 2$ gilt, wobei $\Omega(n) := \sum_{p^\alpha \mid n} 1$ die Anzahl der Primfaktoren von n bezeichnet.

Der Beweis dieses Satzes erfordert stark verfeinerte, umfangreiche Siebmethoden. Er kann z.B. nachgelesen werden in [Nathanson, Additive Number Theory – The Classical Bases, Chap. 9 & 10].

Wir kommen nun zum großen Sieb:

17.18 Motivation: • Im PZzwillingssieb werden pro PZ $p>2$ die Streichungsreste 0 und -2 mod p benutzt. (Streichen a_n, bzw. setze $a_n=0$, falls $n\equiv 0(p)$ oder $n\equiv -2(p)$ ist).
• Im Sieb des Eratosthenes wird der Streichungsrest 0 mod p benutzt.

17.19. Def.: Für eine Zahlenfolge $\mathcal{A}=(a_n)_{n\in\mathbb{N}}$, $p\in\mathcal{P}\subseteq\mathbb{P}$ ist $W_p:=\{h\ (p);\ n\equiv h(p)\Rightarrow a_n=0\}$ die Menge der Streichungsrestklassen mod p, und $w(p):=\#W_p\leq p$ ihre Anzahl.
Es Siebprobleme, die wesentlich mehr Streichungsreste verwenden:
Bsp. Quasiquadrate:

17.20. Def.: $n\in\mathbb{N}$ heißt Quasiquadrat, falls $n\equiv x^2\ (p)$ für jedes $p\leq n^{1/2}$ lösbar ist, d.h. falls n für jedes $p\leq n^{1/2}$ ein quadratischer Rest mod p ist.
Quadratzahlen sind Quasiquadrate, aber umgekehrt muss dies nicht so sein.
Man gelangt zu der Frage, wieviele Quasiquadrate im Vergleich zu Quadratzahlen es gibt. Man kann diese mit einem Sieb zählen:

17.21. Sei $\mathcal{A}=(a_n)_{n\leq x}$ eine Folge in $\mathbb{Z}$, $\mathcal{P}=\mathbb{P}$. Sei $w(p)$ die Anzahl der Streichungsrestklassen mod p. Wir nehmen an, dass $w(p)<p$ für alle $p\in\mathcal{P}$ sei.
Für Quasiquadrate: $a_n:=\begin{cases}1, & n \text{ Quasiquadrat in } [\frac{x}{2},x],\\ 0, & \text{sonst für } n\leq x.\end{cases}$
Sei $p\leq\sqrt{\frac{x}{2}}=:z$.
Für ein Quasiquadrat ist $n\equiv h\ (p)$ nicht möglich für einen Rest h mod p, wenn $\nexists\, k: h\equiv k^2\ (p)$ gilt, d.h. wenn h kein quadratischer Rest mod p.
Solche Reste sind Streichungsreste. Die Anzahl der Quasiquadrate in $[\frac{x}{2},x]$ ist dann $\sum_{n\leq x} a_n$.
Für jede PZ $p\in\mathbb{P}$ gibt es $\frac{p-1}{2}$ quadratische Reste und ebensoviele Restklassen, die es nicht sind (die quadratischen Nichtreste).
⌈Ist $H=\{1,2,\dots,\frac{p-1}{2}\}$, so hat für einen qu. Rest a mod p die (lösbare) Kongruenz $x^2\equiv a\ (p)$ genau eine Lsg. in H: $b^2\equiv a\equiv c^2\ (p)\overset{\mathbb{Z}/p \text{ Körper}}{\Longrightarrow} b\equiv\pm c\ (p)$, also $b=c$, falls $b,c\in H$.⌋
Die # der qu. Reste ist also $\#H=\frac{p-1}{2}$, die der Nichtreste $=p-1-\frac{p-1}{2}=\frac{p-1}{2}$ ✓
Somit: Die $\frac{p-1}{2}$ vielen quadratischen Nichtreste sind Streichungsrestklassen mod p, haben so $w(p)\geq\frac{p-1}{2}$ im Sieb für Quasiquadrate.

17.22. **Bezeichnung:** Ein Sieb mit $\frac{w(p)}{p} > c$ für ein $c > 0$ und alle $p \in \mathcal{P}$ heißt großes Sieb (anschaulich: mit "großen" Löchern, durch die Zahlen fallen können). Andernfalls heißt das Sieb kleines Sieb.

17.23. **Bem:** Das genannte Sieb für Quasiquadrate ist ein großes Sieb, das für PZZwillinge und das Sieb des Eratosthenes sind Beispiele für kleine Siebe. Speziell für große Siebe ist der folgende Siebsatz gut geeignet. Er geht auf Linnik (1941) zurück und wurde von Bombieri, Montgomery, Vaughan u.a. weiterentwickelt.

17.24. **Satz vom großen Sieb:** Sei $\mathcal{A} = (a_n)_{n \le N}$ eine Folge in $\mathbb{C}$, $w(p)$ wie in Def. 17.19 und sei $w(p) < p$ für alle $p \in \mathcal{P}$. Setze $g_w(q) := \mu^2(q) \prod_{\substack{p \mid q \\ p \in \mathcal{P}}} \frac{w(p)}{p - w(p)}$ und $L_w := \sum_{q \le Q} g_w(q)$ für $Q \ge 1$ beliebig. Dann ist

$$\Big|\sum_{n \le N} a_n\Big|^2 \le \frac{N + Q^2}{L_w} \sum_{n \le N} |a_n|^2.$$

- Ist $\mathcal{A}$ speziell die charakteristische Fkt. einer Menge $\mathcal{M} \subseteq \mathbb{N} \cap [1, N]$ (gesiebt mit $w(p)$ vielen Restklassen mod p für alle $p \le Q$), d.h. $a_n = \begin{cases} 1, & n \in \mathcal{M}, \\ 0, & n \notin \mathcal{M}, \end{cases}$ dann folgt $\underbrace{\sum_{n \le N} a_n}_{= S(\mathcal{A}, \mathcal{P}, Q)} = \# \mathcal{M} \le \frac{N + Q^2}{L_w}$.

17.25. **Bem.:** Die Schranke hängt nur von $w(p)$ ab, nicht von der Art der benutzten Streichungsrestklassen. Ist $w(p) > cp$, ist $\frac{w(p)}{p - w(p)} = \frac{1}{p/w(p) - 1}$ groß und $\frac{1}{L_w}$ klein, die Schranke in 17.24 also gut. Der Satz gibt aber selbst für kleine Siebe meist außerordentlich gute Schranken.

Weiter ist Q nichts anderes als $Q = z$, die maximale Größe der Streichungsprimzahlen.

17.26. **Kor. / Satz über Quasiquadrate:** Ist $\mathcal{Q} = \{n \le x;\ n \text{ Quasiquadrat}\}$, so gilt $\# \mathcal{Q} \ll x^{1/2} \log(x)$ für $x \to \infty$. Die Größenordnung für die Anz Quasiquadrate ist in etwa vergleichbar mit der Anz. Quadratzahlen $\le x$. $\left[\frac{\# \mathcal{Q}}{x^{1/2}} \ll \log(x)\right]$

Bew.: Der Satz 17.24 vom großen Sieb mit $w(p) \geq \frac{p-1}{2}$, $N = x$ und a_n wie in 17.21 ergibt für die Anzahl $Q_1(x) := \sum_{\frac{x}{2} < n \leq x} a_n$ der Quasiquadrate in $[\frac{x}{2}, x]$ dann
$Q_1(x) \leq \frac{x + Q^2}{L_w}$, mit $Q := \sqrt{\frac{x}{2}}$ gibt dies $\ll \frac{x}{L_w}$.
Nun gilt für $q = p \leq Q$, dass $\frac{w(p)}{p - w(p)} \geq \frac{\frac{p-1}{2}}{p - \frac{p-1}{2}} = \frac{p-1}{p+1} \geq \frac{1}{3}$,
also $L_w \gg \sum_{p \leq Q} \frac{1}{3} \gg_{\text{Tsch.}} \frac{Q}{\log(Q)}$ und $Q_1(x) \leq \frac{x}{Q} \log(Q) \ll \sqrt{x} \log(x)$.
Für die Anzahl $\# \mathcal{Q}$ ergibt sich
$$\# \mathcal{Q} \ll \sum_{0 \leq k \leq \frac{\log(x)}{\log(2)}} Q_1\left(\frac{x}{2^k}\right) \ll \sqrt{x} \log(x) \sum_k \frac{1}{2^{k/2}} \ll \sqrt{x} \log(x).$$
□

Eine weitere Anwendung des großen Siebes 17.24 ist, damit mit quadratischen Resten zu sieben, um die Größe des kleinsten quadratischen Nichtrests mod $p \leq x$ zu bestimmen.

17.27. Def.: $n_p := \min\{n \in \mathbb{N};\ n \equiv X^2 (p) \text{ unlösbar in } X \bmod p\}$ heißt kleinster quadratischer Nichtrest.

Über die Größe von n_p gibt es folgende Vermutung:

17.28. Vermutung (von Vinogradov): $n_p \ll p^\varepsilon$ für alle $\varepsilon > 0$.
Bisher bekannt: Dies gilt für alle $\varepsilon > \frac{1}{4\sqrt{e}} = 0.1516\ldots$

17.29. Satz von Ankeny: GRH (für alle $L(s,\chi)$ mit $\chi \bmod p$) $\Rightarrow n_p \ll \log^2(p)$.
Für die algorithmische ZT spielt dies eine große Rolle. [Bew. in Vorl. Kryptographie]
[Polya-Vinogradov $\rightsquigarrow n_p \ll \sqrt{p} \log(p)$ laut Ü]

In diesem Zusammenhang zeigte Linnik (wofür er das große Sieb entwickelte):

17.30. Satz von Linnik: Die Anzahl der $p \leq x$ mit $n_p > x^\varepsilon$ ist beschränkt durch eine Konstante $C_\varepsilon > 0$. (D.h. Ausnahmen zur Vermutung 17.28 sind selten.)

Bew.: Betr. das Sieb $\mathcal{A} = (a_n)_{n \leq x}$ mit $a_n = n$, als Streichungs-P-menge nehmen wir diesmal $\mathcal{P} := \{p \in \mathbb{P};\ n \equiv X^2 (p) \text{ lösbar für alle } n \leq x^\varepsilon\}$,
und Streichungsrestklassen sind die $h \bmod p$, für die $h \equiv X^2 (p)$ unlösbar ist (d.h. qu. Nichtrest), haben also $w(p) \geq \frac{p-1}{2}$. Die gesiebte Menge ist $\mathcal{S}(\mathcal{A}, \mathcal{P}, \sqrt{x}) = \{n \leq x;\ n \equiv X^2 (p) \text{ lösbar für alle } p \in \mathcal{P}, p \leq \sqrt{x}\}$,
sei $S(\mathcal{A}, \mathcal{P}, \sqrt{x}) := \# \mathcal{S}(\mathcal{A}, \mathcal{P}, \sqrt{x})$.

Die Menge $\mathcal{S}(\mathcal{A},\mathcal{P},\sqrt{x})$ enthält insb. alle $m \le x$, die frei von Primteilern $> x^{\varepsilon}$ sind.
⌈Ist $m = p_1 \cdots p_r$, die $p_i \le x^{\varepsilon}$, so ist jede Kongruenz $p_i \equiv X^2 (p)$ lösbar, da $p_i \le x^{\varepsilon}$ und $p \in \mathcal{P}$, etwa mit X_i mod $p \rightsquigarrow X := X_1 \cdots X_r$ löst $m = p_1 \cdots p_r \equiv X^2 (p)$. Also: $m \in \mathcal{S}(\mathcal{A},\mathcal{P},\sqrt{x})$.⌋
Insb.: alle $m = n\, p_1 \cdots p_k \le x$ mit $x^{\varepsilon - \varepsilon^2} < p_j < x^{\varepsilon}$ für $1 \le j \le k = \lfloor \frac{1}{\varepsilon} \rfloor$, ein $n \in \mathbb{N}$.
(Beachte $n \le \frac{x}{p_1 \cdots p_k} \ll \frac{x}{x^{(\varepsilon-\varepsilon^2)/\varepsilon}} = \frac{x}{x^{1-\varepsilon}} = x^{\varepsilon}$, d.h. $p \mid m \Rightarrow p < x^{\varepsilon}$.)

Es folgt $S(\mathcal{A},\mathcal{P},\sqrt{x}) \ge \sum_{p_1 \cdots p_k} \left\lfloor \frac{x}{p_1 \cdots p_k} \right\rfloor \gg x \sum_{p \in [x^{\varepsilon-\varepsilon^2}, x^{\varepsilon}]} \frac{1}{p} \underset{\text{Mertens}}{\gg} x \underbrace{(\log\log x^{\varepsilon} - \log\log x^{\varepsilon-\varepsilon^2})}_{= \log \varepsilon - \log(\varepsilon - \varepsilon^2) = \log \frac{1}{1-\varepsilon} = C_{\varepsilon} > 0} \gg x.$

Das große Sieb zeigt andererseits, dass $S(\mathcal{A},\mathcal{P},\sqrt{x}) \ll \frac{x}{\sum_{\substack{p \in \mathcal{P} \\ p < \sqrt{x}}} 1}$,
denn $\frac{\omega(p)}{p - \omega(p)} = \frac{\frac{p-1}{2}}{p - \frac{p-1}{2}} = \frac{p-1}{p+1} \ge \frac{1}{3}$,

insg. folgt $\sum_{\substack{p \in \mathcal{P} \\ < \sqrt{x}}} 1 \ll \frac{x}{S(\mathcal{A},\mathcal{P},\sqrt{x})} \ll 1$, also $\#\mathcal{P} \ll_{\varepsilon} 1$. $\square$