WiSe '21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ 16: Elementare Primzahltheorie

Stichworte: Primzahlzählfunktion $\pi(x)$, Satz von Tschebyschev, Primzahlsatz, logarithmisches Integral $li(x)$, Approximation von $li(x)$, Fehlerterm bei $\pi(x) \sim li(x)$, Riemannsche Vermutung (RH), Bertrands Postulat

---

16.1. Einleitung: • Das Studium der Primzahlmenge $\mathbb{P}$ beinhaltet die Frage, wie die Aussage $\#\mathbb{P} = \infty$ spezifiziert werden kann, d.h. wie die unstetige PZ-Zählfunktion $\pi(x) = \#\{p \leq x\}$ durch eine differenzierbare Funktion approximiert werden kann.

• Euklids Beweis für $\#\mathbb{P} = \infty$ aus der Antike kann genauer zum Resultat $\pi(x) \geq \log\log(x)$ umformuliert werden, was sehr schwach ist (vgl. EZ 2.6).

• Tschebyschev bewies im Jahr 1850, dass $c_1 \frac{x}{\log(x)} \leq \pi(x) \leq c_2 \frac{x}{\log(x)}$ gilt mit Konstanten $0 < c_1 < 1 < c_2$.

Diese können, je nach Aufwand des Beweises, explizit angegeben und recht nahe an 1 "gedrückt" werden, wenn nur x genügend groß gewählt wird.

• Heute (seit 1975) hat man:

$$\frac{x}{\log(x)} \underset{x \geq 17}{\leq} \pi(x) \underset{x > 1}{\leq} 1{,}25506 \frac{x}{\log(x)}$$

Dabei drängt sich die Vermutung auf, ob $\frac{x}{\log(x)}$ die exakte Größenordnung von $\pi(x)$ in Form einer Asymptotik ist, d.h. ob $\pi(x) \sim \frac{x}{\log(x)}$ ist.

16.2. Def.: $f(x) \sim g(x)$ für $x \to \infty :\Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. "$f$ ist asymptotisch zu g" für $x \to \infty$

Landau-Symbole:

$f(x) = o(g(x))$ für $x \to \infty :\Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$

$f(x) = O(g(x))$ für $x \to \infty :\Leftrightarrow \exists C > 0\ \exists x_0 > 0\ \forall x > x_0 : |f(x)| \leq C \cdot g(x)$.

↳ "Klein oh", "groß Oh"

16.3. Bem.: Definiert man den Fehler bei dieser Approximation als $F(x) := f(x) - g(x)$, so ist $\frac{F(x)}{g(x)} = \frac{f(x)}{g(x)} - 1 \underset{x\to\infty}{\longrightarrow} 0$, wofür man auch $f(x) = \underbrace{g(x)}_{\text{Hauptterm}} + \underbrace{o(g(x))}_{\text{Fehlerterm}} = g(x)\cdot(1+o(1))$ schreibt.

D.h. hier also: $\frac{\pi(x)}{x/\log(x)} \xrightarrow{x\to\infty} 1$, bzw. $\pi(x) = \frac{x}{\log(x)} + o\left(\frac{x}{\log x}\right) = \frac{x}{\log x}\cdot(1+o(1))$.

16.4. **Bem.:** Nur durch numerische Auswertung (d.h. durch händisches Auszählen mit Primzahltabellen) wurden schon früh folgende Vermutungen aufgestellt:
- Vermutung von Legendre (1808): $\pi(x) \sim \frac{x}{\log(x) - 1.08366}$.
- Vermutung von Gauß (1849): $\pi(x) \sim li(x) := \int_2^x \frac{dt}{\log(t)}$.

16.5. **Def.:** Die Funktion $li: \mathbb{R}_{\geq 2} \to \mathbb{R}$, $li(x) := \int_2^x \frac{dt}{\log(t)}$, heißt logarithmisches Integral. (sprich: "Li von x")

16.6. **Bem.:** Die Vermutung von Gauß, $\pi(x) \sim li(x)$, ist äquivalent zur Aussage $\pi(x) \sim \frac{x}{\log(x)}$ (und somit zur Vermutung von Legendre) denn es gilt:

$$li(x) = \frac{x}{\log(x)} + o\left(\frac{x}{\log(x)}\right)$$

$$\text{wegen } li(x) = \frac{x}{\log(x)} + O\left(\frac{x}{\log^2(x)}\right) = \frac{0!\, x}{\log(x)} + \frac{1!\, x}{\log^2(x)} + O\left(\frac{x}{\log^3(x)}\right) \text{ usw.}$$

Denn es gilt folgender

16.7. **Satz:** $\forall n \in \mathbb{N}: li(x) = \sum_{k=1}^{n} \frac{(k-1)!\, x}{\log^k(x)} + n! \int_2^x \frac{dt}{\log^{n+1}(t)} + O(1)$, wo $\int_2^x \frac{dt}{\log^{n+1}(t)} = O\left(\frac{x}{\log^{n+1}(x)}\right)$.

Bew.: Induktion:

$\underline{n=1}$: $li(x) = \int_2^x \frac{dt}{\log(t)} = \int_2^x \underbrace{1}_{u'} \cdot \underbrace{\frac{1}{\log(t)}}_{v} \cdot dt \overset{p.I.}{=} \frac{t}{\log(t)}\Big|_2^x + \int_2^x \frac{t}{t \log^2(t)} dt = \frac{x}{\log(x)} + \int_2^x \frac{dt}{\log^2(t)} + O(1)$

Schritt $n \rightsquigarrow n+1$: $\int_2^x \frac{dt}{\log^n(t)} = \int_2^x \underbrace{1}_{u'} \cdot \underbrace{\frac{1}{\log^n(t)}}_{v} \cdot dt \overset{p.I.}{=} \frac{t}{\log^n(t)}\Big|_2^x + n \int_2^x \frac{t}{t \log^{n+1}(t)} dt$

$u = 1 \qquad v' = \frac{-n}{\log^{n+1}(t)}$

$$= \frac{x}{\log^n(x)} + n \int_2^x \frac{dt}{\log^{n+1}(t)} + O(1),$$

und dies in die n-te Formel einsetzen gibt die $(n+1)$-te Formel.

Beachten: $\forall n \in \mathbb{N}: \int_2^x \frac{dt}{\log^n(t)} = \int_2^{\sqrt{x}} \underbrace{\frac{1}{\log^n(t)}}_{\leq 1} dt + \int_{\sqrt{x}}^x \frac{dt}{\log^n(t)} = O(\sqrt{x}) + O\left(\frac{x}{\log^n(x)}\right) = O\left(\frac{x}{\log^n(x)}\right)$.

Integrationsweglänge $\leq x$, $\log^n(t) \geq \left(\frac{1}{2}\right)^n \cdot \log^n(x)$ ($t \geq \sqrt{x}$) □

16.8. **Bem.:** • Welche Vermutung ist die genauere/bessere? $\pi(x) \sim li(x)$ oder $\pi(x) \sim \frac{x}{\log(x)}$ oder die von Legendre, $\pi(x) \sim \frac{x}{\log(x) - A}$ mit $A = 1.08366$? Die genauere Version liefert $\pi(x) \sim li(x)$ wie numerische Daten äußerst gut bestätigen, auch im Hinblick auf die Vermutung in 16.10. [Beachten: $\frac{x}{\log(x)} \sim \frac{x}{\log(x) - A} \iff \frac{\log(x) - A}{\log(x)} \to 1$ ✓]

EZ 16

-3-

- Die <u>beste</u> Approximation an $\pi(x)$ durch eine Funktion der Gestalt $\frac{x}{\log x - A}$ wird dabei mit $A = 1$ erreicht, denn

$$li(x) \sim \frac{x}{\log x - A} \overset{16.7}{\Longleftrightarrow} \frac{x}{\log(x)} + \frac{x}{\log^2(x)} + o\left(\frac{x}{\log^2(x)}\right) \sim \frac{x}{\log(x) - A}$$

$$\Longleftrightarrow \frac{\log(x) + 1}{\log^2(x)} + o\left(\frac{1}{\log^2(x)}\right) \sim \frac{1}{\log(x) - A} \underset{\substack{1\cdot(\log(x)-A) \\ o(\ldots) \text{ rüber}}}{\Longleftrightarrow} \frac{\log(x)^2 - A\log(x) + \log x - A}{\log^2(x)} \sim 1 + \underbrace{o\left(\frac{\log(x) - A}{\log^2(x)}\right)}_{= o\left(\frac{1}{\log x}\right)}$$

$\cdot \log^2(x)$

$$\Rightarrow \log^2(x) - A\log(x) + \log(x) - A \sim \log^2(x) + o(\log x) \Rightarrow (1 - A)\log x = o(\log x),$$

was für $A \neq 1$ ein Widerspruch ist.

- Lange Zeit wurde vergeblich versucht, die Aussage $\pi(x) \sim \frac{x}{\log(x)}$ (oder eine der äquivalenten Versionen) zu beweisen.
  Tschebyschev konnte 1851 in diesem Zusammenhang immerhin zeigen:
  Falls der Grenzwert $\lim\limits_{x\to\infty} \frac{\pi(x)}{x/\log(x)}$ existiert, so muss er $= 1$ sein.

- Der endgültige Beweis gelang erst 1896 durch Hadamard und de la Vallée-Poussin (unabhängig voneinander), und ist heute als der Primzahlsatz (PZS) bekannt. Es gilt also:

16.9. <u>PZS:</u> $\pi(x) \sim \frac{x}{\log(x)}$, und die oben genannten, dazu äquivalenten Versionen, etwa $\pi(x) \sim li(x)$ bzw. $\pi(x) \sim \frac{x}{\log(x) - A}$ für jedes $A \in \mathbb{R}$.

16.10. <u>Bem.:</u> Wir kommen zur Frage nach der Größenordnung der Fehlerglieder in den PZS-Versionen.
Die beste Approximation liefert anscheinend die Version $\pi(x) \sim li(x)$, numerische Daten zeigen dies deutlich. Wie gut diese Approximation ist, ist bis heute eins der wichtigsten zentralen ungelösten Probleme der Mathematik:

16.11. <u>Riemannsche Vermutung</u> (RH) $\Longleftrightarrow \pi(x) = li(x) + O(\sqrt{x}\log(x))$.

bzw. "$O_\varepsilon(x^{1/2+\varepsilon})$ für jedes $\varepsilon > 0$" genügt auch zur (RH).

16.12. **Bem. zur (RH):** • Genauer kann man zeigen:

$$1)\ RH \Rightarrow \pi(x) = li(x) + O(\sqrt{x}\log(x)),\quad 2)\ \forall \varepsilon>0: \pi(x) = li(x) + O_\varepsilon(x^{1/2+\varepsilon}) \Rightarrow RH.$$

- Wir werden die Riemannsche Vermutung in der Vorlesung "Analytische Zahlentheorie" als eine analytische Aussage über die Lage der Nullstellen der Zetafunktion ζ formulieren. Damit kann die behauptete Äquivalenz in 16.11 gezeigt werden.
- Der Beweis der Tschebyschev-Ungleichungen und des PZSes wird standardmäßig in einer Vorlesung über analytische Zahlentheorie vorgeführt.
- Die äquivalente Umformulierung in 16.11 macht den Nutzen der RH für die Theorie zur Verteilung der PZen sehr deutlich: Nach dieser sind die PZen so gut wie nur möglich durch $li(x)$ verteilt. Dies spielt für viele Anwendungen mit Primzahlen oft eine große Rolle.

16.13. **Bem.:** Schon der Satz von Tschebyschev, dass $C_1 \frac{x}{\log(x)} \le \pi(x) \le C_2 \frac{x}{\log(x)}$ gilt, hat bereits interessante Konsequenzen, etwa

Bertrands Postulat: Zwischen n und $2n$ liegt stets (mind.) eine Primzahl p (für $n \geq 2$).

Bew.: Nimmt man etwa $C_1 = 1$, $C_2 = 1.26$ (vgl. 16.1), so folgt für $2n \geq 17$, dass

$$\sum_{n<p\le 2n} 1 = \pi(2n) - \pi(n) \geq C_1 \frac{2n}{\log(2n)} - C_2 \frac{n}{\log(n)}$$

$$= \frac{n}{\log(n)} \cdot \underbrace{\Big(C_1 \underbrace{\frac{2\log(n)}{\log(2n)}}_{\geq 1.5 \text{ für große } n \text{ (da } \to 2\text{, gilt bereits für } n \geq 8)} - C_2\Big)}_{\geq 1\cdot 1.5 - 1.26 > 0} > 0,$$

die $n \le 8$ sind klar. $\square$

Bekanntes Zitat (von N. Fine, nicht von P. Erdős):

"Chebyshev said it,
we'll say it again:
There is always a prime
between N and 2N."

Ende der Vorlesung