7.3. Anwendung: ein Satz von Linnik

Vermutung von Vinogradov: $\forall \varepsilon>0\ \forall p>p_0(\varepsilon)\ \exists$ quadratischer Nichtrest $n \bmod p$, d.h. $\left(\frac{n}{p}\right)=-1$, mit $n<p^{\varepsilon}$.

Linnik zeigte, daß Ausnahmen zu dieser Vermutung sehr selten sind:

Satz von Linnik: Sei $\varepsilon>0$.

(i) $\#\{p\le N;\ \min\{n\in\mathbb{N};\ \left(\frac{n}{p}\right)=-1\}>N^{\varepsilon}\}\le C(\varepsilon)$.

(ii) $U(x):=\#\{p\le x;\ \min\{n\in\mathbb{N};\ \left(\frac{n}{p}\right)=-1\}>p^{\varepsilon}\}\ \ll_{\varepsilon}\ \log\log x$.

Wir beweisen den Satz als Anwendung des großen Siebs in §4.2.

Bew.: Zeigen erst (i) $\Rightarrow$ (ii): Sei $V(N):=\#\{p\in(\sqrt{N},N];\ \min\{n\in\mathbb{N};\ \left(\frac{n}{p}\right)=-1\}\ge N^{\frac{\varepsilon}{2}}\}$.

Dann: $U(x)\le\sum_{j=0}^{\infty}V(x^{2^{-j}})$. Gilt nun (i), d.h. $V(N)\le C(\frac{\varepsilon}{2})$ für jedes N.

Da $V(x^{2^{-j}})=0$ für $x^{2^{-j}}<2$, enthält die $\sum$ nur $O(\log\log x)$ viele Terme $\rightsquigarrow$ (ii). ✓

Zu (i):

Betr. $\mathcal{A}=\{1,\dots,N\}$, $\mathcal{P}:=\{3\le p<\sqrt{N};\ \forall b\le N^{\varepsilon}: \left(\frac{b}{p}\right)=1\}$,
und als Streichungsrestklassen mod p nehmen wir die $h \bmod p$ mit $\left(\frac{h}{p}\right)=-1$,
da genau die Hälfte aller primen Reste mod p quadr. Reste sind, ist
$\omega(p)=\frac{p-1}{2}\ge\frac{p}{3}$. Wollen nun $\#\mathcal{P}\le C(\varepsilon)$ zeigen.

Dazu sei $\mathcal{G}(X,Y):=\{x\in\mathbb{N};\ x\le X,\ p|x\Rightarrow p\le Y\}$
die Menge der natürlichen $x\le X$, die nur Primteiler $\le Y$ besitzen
(sogenannte Y-glatte Zahlen, wichtig auch in der algorithmischen ZT.)

Ist $n\in\mathcal{G}(N,N^{\varepsilon})$, $p\in\mathcal{P}$, so gilt für $\varepsilon\le\frac{1}{2}$: $\left(\frac{n}{p}\right)=\prod_{\tilde{p}^{\alpha}\|n}\left(\frac{\tilde{p}}{p}\right)^{\alpha}=1$,
denn aus $\alpha\ge1$ folgt $\tilde{p}\le N^{\varepsilon}$, und vgl. Def. von $\mathcal{P}$.
Somit: $n\not\equiv h\ (p)$ für $h \bmod p$ mit $\left(\frac{h}{p}\right)=-1$.

Also ist $\#\mathcal{G}(N,N^\varepsilon) \leq S(\mathcal{A},\mathcal{P},\sqrt{N}) \overset{\text{großes Sieb}}{\leq} \dfrac{N+4\pi N}{L(\sqrt{N})}$

mit $L(\sqrt{N}) \geq \sum\limits_{\substack{p<\sqrt{N}\\ p\in\mathcal{P}}} \dfrac{\omega(p)}{p-\omega(p)} \underset{\omega(p)\geq \frac{p}{3}}{\geq} \sum\limits_{\substack{p<\sqrt{N}\\ p\in\mathcal{P}}} \dfrac{\frac{p}{3}}{\frac{2}{3}p} = \frac{1}{2}\cdot\#\mathcal{P}$

folgt $\#\mathcal{G}(N,N^\varepsilon) \ll N(\#\mathcal{P})^{-1}$. Mit $\underline{\#\mathcal{G}(N,N^\varepsilon) \gg_\varepsilon N}$ $\circledast$
folgt dann die Beh. des Satzes, (i). $(\square)$

Es muß noch $\circledast$ bewiesen werden.
Dazu zeigen wir sogar eine asymptotische Formel für $\#\mathcal{G}(X,Y)$, die auch bei anderen Fragen der ZT wichtiges Hilfsmittel ist.
Wir benutzen ab jetzt die gängige Bezeichnung $\underline{\Psi(x,y) := \#\mathcal{G}(x,y)}$.

Lemma 7.4:
Es gibt genau eine stetige Funktion $\varrho : (0,\infty) \to \mathbb{R}$, die auf $(1,\infty)$ diff'bar ist und für die gilt:
$\underline{\varrho(u) = 1 \text{ für } 0<u\leq 1,}$ $\quad \underline{u\varrho'(u) = -\varrho(u-1) \text{ für } u>1.}$ $\oplus$
Es gilt $0<\varrho(u)<1$ für $u>1$, dort ist ϱ streng monoton fallend.
Ist $c\in\mathbb{R}$ mit $0<c<1$ geg., so gilt für $x\geq 2$ und $y\geq x^c$ die Asymptotik

$$\boxed{\Psi(x,y) = x\,\varrho\left(\frac{\log x}{\log y}\right) + O\left(\frac{x}{\log x}\right).}$$

⌈Bem.: Aus der Asymptotik folgt $\circledast$ wegen $\Psi(N,N^\varepsilon) = N\varrho(\frac{1}{\varepsilon}) + o(N) \gg_\varepsilon N$.⌋

Bem.: Die Funktion ϱ heißt auch <u>Dickman-Funktion</u>.
Die Bedingungen $\oplus$ sind ein Beispiel für eine
<u>Differenzen-Differentialgleichung</u>. Die Lösung ist auf $(0,1]$ vorgegeben und sukzessive erklärbar im IV $u\in(k,k+1]$, $k\in\mathbb{N}$, durch

$$\varrho(u) = \varrho(k) - \int_k^u \frac{1}{t}\varrho(t-1)\,dt.$$

Die Ex.+Eind. von ϱ ist damit klar.

Bew.: Es gen. z.z.: die Asymptotik für $\Psi(x,y)$. ⌜Aus $0 \le \Psi(x,y) \le x$ folgt $\varrho(u) \in [0,1]$ für $u>0$.
Aus ⊛: ϱ fällt streng monoton für $u>1$. Da $\varrho(u) \ge 0$, ist ϱ nirgends $=0$, also $\varrho(u) \in (0,1)$ für $u>1$. ⌟

Für $x \ge 2$, $z \ge y \ge 2$, gilt die Gleichung

$$\boxed{\Psi(x,y) = \Psi(x,z) - \sum_{y<p\le z} \Psi\left(\tfrac{x}{p}, p\right).}$$

(„Buchstab-Identität")

⌜ OE y,z prim, denn $\Psi(x,y)$ ändert sich nicht, wenn y durch die größte PZ $\le y$ ersetzt wird. Weiter OE ($p \in [y,z]$ prim $\Rightarrow p=y \vee p=z$), der allg. Fall folgt aus sukzessiver Anwendung dieses Spezialfalls. Schreibe dafür $z=p=\min\{p' \in \mathbb{P} : p'>y\}$, zeige $\Psi(x,p) - \Psi(x,y) = \Psi\left(\tfrac{x}{p}, p\right)$: die l.S. $= \#(\mathcal{G}(x,p) \setminus \mathcal{G}(x,y))$, und jedes $n \in \mathcal{G}(x,p) \setminus \mathcal{G}(x,y)$ ist schreibbar als $n = pm$ mit $m \in \mathcal{G}\left(\tfrac{x}{p}, p\right)$ ✓. ⌟

Sei $u = \dfrac{\log x}{\log y}$, zeigen Asymptotik mit VI über $k \in \mathbb{N}$ für $u \le k$.

$k=1$: $u \le 1 \iff y \ge x$, was $\Psi(x,y) = \lfloor x \rfloor = x + O(1)$ impliziert. ✓

$k \to k+1$: Sei die Asymptotik für $u \le k \iff y \ge x^{1/k}$ bekannt.

Für $k < u \le k+1$ folgt aus der Buchstab-Identität:

$$\Psi(x,y) = \Psi(x, x^{1/k}) - \sum_{y<p\le x^{1/k}} \Psi\left(\tfrac{x}{p}, p\right).$$

Ind.vor. anw. auf r.S., da $\dfrac{\log(\frac{x}{p})}{\log p} = \dfrac{\log x}{\log p} - 1 \le k$ für $p > y \ge x^{1/(k+1)}$.

Falls $k=1$, ist $\Psi\left(\tfrac{x}{p}, p\right) = \lfloor \tfrac{x}{p} \rfloor$ für $x^{1/2} < p \le x$, also

$$\Psi(x,y) = x\Big(1 - \underbrace{\sum_{y<p\le x} \tfrac{1}{p}}_{= \log\log x - \log\log y + O\left(\frac{1}{\log y}\right)}\Big) + O\left(\tfrac{x}{\log x}\right),$$

d.h. $\Psi(x,y) = x(1 - \log u) + O_k\left(\frac{x}{\log x}\right)$,

also $\varrho(u) = 1 - \log u$ für $1 < u \le 2$.

Falls $k \ge 2$, ist für $p \le x^{1/k}$ dann $\log \frac{x}{p} \gg \log x$.

Buchstab-Identität, Fall $k=1$; Ind.vor.:

$$\Psi(x,y) = \varrho(k)\, x - \sum_{y<p\le x^{1/k}} \left(\varrho\left(\tfrac{\log x}{\log p} - 1\right) \tfrac{x}{p} + O_k\left(\tfrac{x/p}{\log \frac{x}{p}} \right) \right) + O_k\left(\tfrac{x}{\log x}\right).$$

$$\sum_{y<p\le x^{1/k}} \frac{1}{p}\, \varrho\left(\frac{\log x}{\log p} - 1\right) \overset{\text{partielle } \Sigma}{=} \varrho(k-1) \sum_{y<p\le x^{1/k}} \frac{1}{p} - \int_y^{x^{1/k}} \Big(\sum_{y<p\le \xi} \frac{1}{p}\Big)\, \varrho'\left(\frac{\log x}{\log \xi} - 1\right) \left(\frac{d}{d\xi} \frac{\log x}{\log \xi}\right) d\xi$$

Subst. $\frac{\log x}{\log \xi} = t$:

$$= \varrho(k-1) \sum_{y<p\le x^{1/k}} \frac{1}{p} - \int_k^u \Big(\sum_{x^{1/u}<p\le x^{1/t}} \frac{1}{p} \Big)\, \varrho'(t-1)\, dt.$$

ρ, ρ' beschr. $\rightsquigarrow$ $$\sum_{y<p\le x^{1/k}} \frac{1}{p}\,\rho\left(\frac{\log x}{\log p}-1\right) = \rho(k-1)\log\frac{u}{k} + \underbrace{\int_k^u \log\frac{u}{t}\,\rho'(t-1)\,dt}_{} + O_k\left(\frac{1}{\log x}\right)$$

partielle $\int \rightarrow$ $$= -\rho(k-1)\log\frac{u}{k} + \int_k^u \frac{1}{t}\rho(t-1)\,dt$$
$$= -\rho(k-1)\log\frac{u}{k} + \rho(k) - \rho(u).$$

$\rightsquigarrow$ $\Psi(x,y) = \rho(u)\,x + O_k\left(\frac{x}{\log x}\right)$ für $y \ge x^{1/k}$.

Die Gleichmäßigkeit in y ergibt sich wie folgt: Für $y > x^c$ sind nur die $k \le \frac{1}{c}$ zu betrachten, die impliziten O-Konstanten sind dann unabh. von k wählbar. $\square$

Bem.: Eng verwandt mit der Dickman-Fkt. ist die Buchstab-Fkt. $\omega(u)$, [nicht zu verwechseln mit der Restklassenanzahl $\omega(p)$ eines Siebs!] def. durch $u\omega(u) := 1$ für $1 \le u \le 2$, $u\omega(u) := 1 + \int_1^{u-1}\omega(v)\,dv$, $u > 2$.

Für die Fkt. $\Phi(x,y) := \#\{n \le x;\ p \mid n \Rightarrow p > y\} = \#\{n \le x;\ (n, \prod_{p\le y} p) = 1\}$. kann dann mit einer analogen Buchstab-Identität die Asymptotik
$$\Phi(x,y) = \frac{x\omega(u) - y}{\log y} + O\left(\frac{x}{\log^2 y}\right), \quad x^\varepsilon < y \le x,\ \varepsilon > 0,\ u = \frac{\log x}{\log y},$$
gezeigt werden.

Das große Sieb hat noch zahlreiche andere Anwendungen. Selbst im Fall von kleinen Sieben, d.h. wenn $\omega(p)$ klein ist wie etwa im Fall des Beweises der Brun-Titchmarsh-Unglg. (s.o., Anw. 4 des Selberg-Siebes), kann es starke Abschätzungen liefern.

Für die Anzahl PZ-Zwillinge $\le x$ kann etwa
$$\pi_2(x) \le \frac{8\mathfrak{S}x}{(\log x)^2} + o\left(\frac{x}{(\log x)^2}\right), \quad \mathfrak{S} := 2\prod_{p\ge 3}\left(1 - \frac{1}{(p-1)^2}\right),$$
gezeigt werden, was bis auf den Faktor 8 die richtige Größenordnung laut Hardy&Littlewood's Vermutung ist.

Eine weitere wichtige Anwendung der großen Sieb-Ungleichung ist die Verteilung von Primzahlen in Restklassen. Es kann gezeigt werden:

<u>Satz von Barban-Davenport-Halberstam:</u> Für $1 \le Q \le x$, $A > 0$ gilt:

$$\sum_{q \le Q} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} \left| \pi(x; q, a) - \frac{1}{\varphi(q)} \int_2^x \frac{dt}{\log t} \right|^2 \ll Qx \log x + x^2 (\log x)^{-A}.$$

Für $Q \le x (\log x)^{-A-1}$ kann damit die nichttriv. Schranke $x^2 (\log x)^{-A}$ gezeigt werden, d.h. die Gleichverteilung der Pzen in Restklassen, wie sie wegen dem Satz von Siegel-Walfisz gleichmäßig nur für $q \le (\log x)^C$ gegeben ist, gilt im Mittel für alle Restklassen mit sehr viel größeren Moduln.

Dies kann gleichmäßig für alle Reste $a \bmod q$ verschärft werden, allerdings auf Kosten der Größe der Moduln q:

<u>Satz von Bombieri-Vinogradov:</u> Sei $A \ge 1$. Dann ist

$$\sum_{q \le Q} \max_{(a,q)=1} \max_{y \le x} \left| \pi(y; q, a) - \frac{1}{\varphi(q)} \int_2^y \frac{dt}{\log t} \right| \ll x (\log x)^{-A} + Q\sqrt{x} (\log Qx)^6.$$

Hier kann also für $Q \le \sqrt{x} (\log x)^{-B(A)}$ die nichttriv. Schranke $x (\log x)^{-A}$ gezeigt werden.

Der Beweis benutzt dabei eine Variante der großen Sieb-Ungleichung für Charaktere, sowie einer kombinatorischen Identität, der <u>Vaughan-Identität.</u>

Der wichtige Satz von Bombieri-Vinogradov kann in Anwendungen oft die Annahme der allgemeinen Riemannschen Vermutung ersetzen.

<u>Elliott-Halberstam-Vermutung:</u> Die Schranke $x (\log x)^{-A}$ gilt für $Q = x^{1-\varepsilon}$, $\varepsilon > 0$.

Für noch größere Q ist diese Vermutung jedoch widerlegt worden.

Wir zeigen exemplarisch als eine Anwendung des Satzes von Bombieri-Vinogradov:

<u>**Satz (Titchmarsh):**</u> Mit $C := \prod_p \left(1 + \frac{1}{p(p-1)}\right)$ gilt
$$\sum_{p \le x} d(p+1) = Cx + O\left(x \frac{\log\log x}{\log x}\right).$$

<u>Bew.:</u> Schreiben
$$\sum_{p\le x} d(p+1) = \sum_{p \le x} \sum_{\substack{u,v \\ uv = p+1}} 1 = 2 \sum_{p\le x} \sum_{\substack{uv=p+1 \\ u<v}} 1 + \sum_{p\le x} \sum_{u,\, u^2 = p+1} 1$$

Die Glg. $u^2 = p+1$ hat wegen $u^2 - 1 = (u-1)(u+1)$ nur die Lösung $u=2, p=3$, die letzte Doppelsumme ist daher $O(1)$.

Weiter ist $u < v \iff u < \sqrt{p+1}$, also ist
$$\sum_{p\le x} d(p+1) = 2 \sum_{p\le x} \sum_{\substack{u < \sqrt{p+1} \\ p \equiv -1 (u)}} 1 + O(1) = 2 \sum_{u \le \sqrt{x+1}} \left(\pi(x; u, -1) - \pi(u^2-1; u, -1)\right) + O(1).$$

Sei OE $u > 1$, der Term für $u = 1$ ist $O\left(\frac{x}{\log x}\right)$.

Aufspalten der $\sum$: $\quad \sum_{p\le x} d(p+1) = 2(\Sigma_1 + \Sigma_2) + O\left(\frac{x}{\log x}\right)$

mit der Summationsbedingung $2 \le u \le U$ für Σ_1 und $U < u \le \sqrt{x+1}$ für Σ_2,

wobei $U = \sqrt{x} \cdot (\log x)^{-A}$ mit einem fixierten $A > 20$.

Schreiben $D(y, q, a) := \pi(y, q, a) - \frac{1}{\varphi(q)} \int_2^y \frac{dt}{\log t}$ und erhalten
$$\Sigma_1 = \underbrace{\sum_{2 \le u \le U} \frac{1}{\varphi(u)} \int_{u^2-1}^{x} \frac{dt}{\log t}}_{= \frac{x}{\log x} \cdot \sum_{2 \le u \le U} \frac{1}{\varphi(u)} + O\left(\frac{x}{\log x}\right)} + O\Big(\underbrace{\sum_{u \le U} \max_{y \le x} |D(y, u, -1)|}_{\ll x (\log x)^{-2} \text{ nach dem } \underline{\text{Satz von B-V}}}\Big),$$

also $\Sigma_1 = \frac{C}{2} x + O\left(\frac{x \log\log x}{\log x}\right)$ wegen $\sum_{u \le x} \frac{1}{\varphi(u)} = C \log x + O(1)$.

Für Σ_2 zeigt die <u>Brun-Titchmarsh-Unglg.</u>:
$$\Sigma_2 \ll \sum_{U < u \le \sqrt{x+1}} \pi(x; u, -1) \underset{BT}{\ll} \sum_{U < u \le \sqrt{x+1}} \frac{x}{\varphi(u) \log \frac{x}{u}} \ll \frac{x}{\log x} \underbrace{\sum_{U < u \le \sqrt{x+1}} \frac{1}{\varphi(u)}}_{\substack{= C \log \sqrt{x} - C \log \frac{\sqrt{x}}{(\log x)^A} + O(1) \\ = O(\log\log x)}} \ll \frac{x \log\log x}{\log x}.$$

$\pi(u^2 - 1; u, -1) \le \pi(x; u, -1)$ für $u \le \sqrt{x+1}$

$\square$

ENDE