Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K8: AKS- bzw. LP-Primzahltest

Stichworte: Funktionsweise des AKS-Primzahltests / LP-Primzahltests nach A. Granville, Beweisskizze für die Laufzeitabschätzung

---

8.1. Einleitung: Im Jahr 2002 veröffentlichten drei indische Computerspezialisten (M. Agrawal, N. Kayal und N. Saxena) einen deterministischen Primzahltest, der polynomiell schnelle Laufzeit besitzt: heute als AKS-Test bezeichnet. Dies war ein großer Durchbruch, da zuvor polynomielle Primzahltests nur probabilistisch waren (die in K7), und deterministische Primzahltests nicht polynomiell schnell waren. Die Überraschung lag vor allem darin, dass der Test schnell zu verstehen und überaus einfach zu zeigen ist.
Zur praktischen Anwendung genügt der AKS-Test nur begrenzt: Bis max. 10 000-stellige Dezimalzahlen können damit getestet werden, danach geht es zu langsam.
Wir folgen der Darstellung von A. Granville in seinem preisgekrönten Artikel "It is easy to determine whether a given integer is prime" von 2005 und zeigen die Verbesserung des AKS-Tests nach Lenstra / Pomerance "LP-Test", erschienen 2019.

8.2. AKS-Test, Originalversion: Für $N \geq 2$ sei $r \in \mathbb{N}$ mit $r < N$ so, dass $\mathrm{ord}_r(N) > \log^2(N)$. Dann ist N genau dann prim, wenn
(a) N keine (echte) Potenz ist, (echte Potenzen sind Potenzen $\neq 1$ mit Exponenten ≥ 2)
(b) N keinen Primfaktor $\leq r$ enthält,
und (c) $(X+a)^N \equiv X^N + a \mod (N, X^r - 1)$ für jedes $1 \leq a \leq r \cdot \log(N)$ gilt.

8.3. Bem.: Die letzte Bedingung bezeichnet die Gleichung $(X+a)^N = X^N + a$ im Ring $\mathbb{Z}_N[X]/(X^r - 1)$. ← herausgeteilt wird das von $X^r - 1$ erzeugte Ideal

8.4. Bem.: Der AKS-Test 8.2 hat eine Laufzeit von $\tilde{O}(\log^{7.5}(N))$.
Wir behandeln die Verbesserung von Lenstra / Pomerance ("LP-Test") mit Laufzeit $\tilde{O}(\log^6(N))$ [mit effektiv berechenbarer impl. Konstante!], die hinsichtlich des AKS-Tests optimal ist: Da $r > \log^2(N)$ und die Laufzeit von (c) nicht unter $\tilde{O}(r^{3/2}\log^3(N))$ möglich ist, kann der AKS-Test prinzipiell nicht schneller als $\tilde{O}(\log^6(N))$ [#Bit-op.] laufen.

8.5. **Bem.:** • Zur Bezeichnung "Soft-Oh": Wir schreiben $\tilde{O}(y)$ für $O(y \log^{O(1)}(y))$.
Eine Division $a \bmod b$ benötigt dann die Laufzeit $\tilde{O}(\ell)$, falls a, b Binärlänge $\leq \ell$ haben.

• Die Größe von r ist für die Laufzeit $\tilde{O}(r^{3/2}\log^3(N))$ entscheidend; mit tieferen ZT-Ergebnissen konnte $r = \tilde{O}(\log^3(N))$ gezeigt werden, was auf $\tilde{O}(\log^{\frac{9}{2}+3}(N)) = O(\log^{7.5}(N))$ führt.

• Eine randomisierte Version des AKS-Tests läuft in $O(\log(N)^{4+o(1)})$, daran wird derzeit geforscht [s. §6 in Granvilles Artikel]. Dies wäre schneller als der Miller-Rabin-Test mit $O(\log^5(N))$!

8.6. **Def.:** Sei $f(x) \in \mathbb{Z}[x]$ ein geg. normiertes Polynom vom Grad d, und $N \in \mathbb{N}$.
Der Ring $\mathbb{Z}[x]/(N, f(x)) \cong \mathbb{Z}_N[x]/(f(x))$ heißt **Pseudokörper**, falls (i) $f(x^N) \equiv 0 \bmod (N, f(x))$, (ii) $x^{N^d} - x \equiv 0 \bmod (N, f(x))$,
und (iii) $x^{N^{d/q}} - x$ in $\mathbb{Z}[x]/(N, f(x))$ eine Einheit ist für alle Primteiler q von d.

8.7. **Bem.:** Ist N prim und $f(x)$ irreduzibel mod N, sind diese Kriterien erfüllt und $\mathbb{Z}[x]/(N, f(x))$ ist ein endlicher Körper.

8.8. **AKS-Test nach Lenstra/Pomerance [LP-Test]:** Sei $N \geq 2$ und $\log^2(N) < d < N$ so, dass für ein normiertes Polynom $f(x)$ vom Grad d in $\mathbb{Z}[x]$ der Ring $\mathbb{Z}[x]/(N, f(x))$ ein Pseudokörper ist.
Dann ist N genau dann prim, wenn (a) N keine (echte) Potenz ist,
(b) N keinen Primfaktor $\leq d$ enthält,
und (c) $(x+a)^N \equiv x^N + a \bmod (N, f(x))$ für alle $1 \leq a \leq \sqrt{d}\log(N)$ gilt.

8.9. **Bew.:** Sei $A := \sqrt{d}\log(N)$ und $B := \lfloor A \rfloor \in \mathbb{N}$. „$\Rightarrow$" klar, z.z. nur „$\Leftarrow$". Dazu sei N zus'gesetzt so, dass die Bedingungen (a), (b) und (c) erfüllt sind.
Sei $p \mid N$ prim und $h(x)$ ein irred. Faktor von $f(x)$ mod p, so dass $\mathbb{F} \cong \mathbb{Z}[x]/(p, h(x))$ ein endlicher Körper ist (nämlich $\cong \mathbb{F}_{p^m}$, $m = \deg h$).
Sei $\mathcal{F} := \mathbb{Z}[x]/(p, f(x)) \supseteq \mathbb{F}$, da $(p, h(x)) \supseteq (p, f(x))$ da $h(x) \mid f(x)$.
Sei $r := \mathrm{ord}_{\mathcal{F}}(x)$ laut Def. (ii), (iii) in 8.6, so dass $d = \mathrm{ord}_r(N)$ folgt.
[in $\mathcal{F}$: • $x^{N^d} = x$ laut (i) $\rightsquigarrow \mathrm{ord}_r(N) \mid d$,
• $x^{N^{d/q}} \neq x$ für alle $q \mid d$, q prim, laut (iii) $\rightsquigarrow$ „$<$" nicht möglich.]

$\rightsquigarrow$ Es sind $\underbrace{x^{N^0}}_{=x}, x^{N^1}, \ldots, x^{N^{d-1}}$ in $\mathcal{F}$ p.w.v., und ebenso in $\mathbb{F}$.
Daher hat $g(T) := \prod_{i=0}^{d-1}(T - x^{N^i}) \in \mathbb{F}[T]$ p.w.v. Nullstellen in $\mathbb{F}$.

Außerdem gilt $g(x^p) \doteq g(x)^p = 0$ in $\mathbb{F}$, da $\mathrm{char}\,\mathbb{F} = p$: $(z+y)^p = \sum_{j=0}^{p} \binom{p}{j} z^j y^{p-j} = z^p + y^p$ (f. in. Satz; $\binom{p}{j} \equiv 0 \ (p)$ für $1 \le j \le p-1$, induktiv mehrere Summanden),
daher muss x^p gleich einem $x^{N^{i_0}}$ sein in $\mathbb{F}$, also auch in $\mathfrak{F}$.
Dies impliziert $p \equiv N^{i_0} \ (r)$ für ein $i_0 \in \{0, \dots, d-1\}$.
Ist nun $R \le \mathbb{Z}_r^\times$ mit $R := \langle N, p \rangle$, folgt bereits $R = \langle N \rangle$ und $\#R = d$.

Sei H die Menge der Elemente von $\mathfrak{F}$, die multiplikativ von
$x, x+1, x+2, \dots, x+B$ erzeugt werden, d.h. $H := \{ x^{i_0} (x+1)^{i_2} \cdots (x+B)^{i_B} ; i \in \mathbb{Z}^B \} \subseteq \mathfrak{F}$.
Diese Erzeuger sind alle $\neq 0$, denn $x+a = 0$ in $\mathfrak{F}$ zeigt $x^N + a = (x+a)^N = 0$ in $\mathfrak{F}$ laut (c),
also $x^N = -a = x$ in $\mathfrak{F}$, also $N \equiv 1 \ (r)$ und $d = 1$, im $\lightning$ zur Vor. $d > \log^2(N)$ an d.
Sei $G \le \mathbb{F}$ die UG, die von den El. $x, x+1, \dots, x+B \in \mathbb{F}$ in $\mathbb{F}$ multiplikativ erzeugt wird.
Da G eine UG eines endlichen Körpers ist, ist G zyklisch (vgl. Algebra [A21.2]).
Sei $S := \{ k \in \mathbb{N} ; \tilde{g}(x^k) = \tilde{g}(x)^k$ in $\mathfrak{F}$ für alle $\tilde{g} \in H$, $k = N^i p^j \bmod r$ für $i, j \ge 0 \}$.
(Dann ist für alle $k \in S$ auch $\tilde{g}(x^k) = \tilde{g}(x)^k$ in $\mathbb{F}$ und alle $\tilde{g} \in G$.) Klar: $p \in S$ ✓,
und $N \in S$ ✓ (wegen Vor. (c)).

1. Beh.: $a, b \in S \Rightarrow ab \in S$, d.h. S ist multiplikativ abgeschlossen.
Bew.: Falls $\tilde{g} \in H$, ist $\tilde{g}(x^b) = \tilde{g}(x)^b$ in $\mathfrak{F}$. Durch Ersetzen von x durch x^a
folgt $\tilde{g}((x^a)^b) \equiv \tilde{g}(x^a)^b \bmod (p, f(x^a))$, also auch $\bmod (p, f(x))$, da $f(x^a) = 0$ in $\mathfrak{F}$.
Haben $f(x^k) = 0$ in $\mathfrak{F}$ für alle $k \in S$, denn haben $k \equiv N^i p^j \ (r)$,
und $f(x^N) = 0$ in $\mathfrak{F}$ laut (i),
und $f(x^p) \equiv f(x)^p \ (p)$, und dies ist $= 0$ in $\mathfrak{F}$ laut Def. von $\mathfrak{F}$.
Nun x^N einsetzen in $f(x^N) = f(x) = 0$ gibt $f(x^{N \cdot N}) = f(x^N) = 0$ und induktiv $f(x^{N^\ell}) = 0$ für alle ℓ,
mit $p \equiv N^{i_0} \ (r)$ folgt $f(x^k) = 0$ in $\mathfrak{F}$ für alle k der Form $k = N^i p^j$.
Somit: $\tilde{g}(x)^{ab} = (\tilde{g}(x)^a)^b \equiv \tilde{g}(x^a)^b \equiv \tilde{g}((x^a)^b) = \tilde{g}(x^{ab}) \bmod (p, f(x))$, d.h. in $\mathfrak{F}$. □

2. Beh.: $a, b \in S$ und $a \equiv b \ (r) \Rightarrow a \equiv b \ (\#G)$.
Bew.: Für bel. $g \in \mathbb{Z}[x]$ gilt $u - v \mid g(u) - g(v)$, also: $x^r - 1 \mid x^{a-b} - 1 \mid x^a - x^b \mid g(x^a) - g(x^b)$.
Somit: $g \in H \Rightarrow g(x)^a \equiv g(x^a) \equiv g(x^b) \equiv g(x)^b \bmod (p, x^r - 1)$.
Dies gilt auch $\bmod (p, f(x))$ anstelle $\bmod (p, x^r - 1)$, da $(p, f(x)) \supseteq (p, x^r - 1)$.
$x^r - 1 = 0$ in $\mathfrak{F}$, d.h. $\bmod (p, f(x))$, so dass $x^r - 1 \in \mathbb{Z}[x] \cdot p + \mathbb{Z}[x] \cdot f(x)$.
Also: $g \in H \Rightarrow g(x)^{a-b} \equiv 1$ in $\mathbb{F}$. Da G zyklisch, wähle g als Erzeuger $\Rightarrow \#G \mid a - b$. □

8.10. **Bew.fortsetzung:** Sei $R = \langle N \rangle \leq \mathbb{Z}_r^\times$, $\#R = d$, wie oben. • Sei $a \in S$, $b \equiv a \ (N^d - 1)$.

$u - v \mid g(u) - g(v)$ gilt immer!

Nun gilt $x^{N^d} - x \equiv 0$ in $\mathbb{F}$ laut (i), also $f(x) \mid x^{N^d} - x \mid x^b - x^a \mid g(x^b) - g(x^a)$ für alle $g \in \mathbb{Z}[x]$. Falls $g \in H$, zeigt die 1. Beh., dass $g(x)^{N^d} \equiv g(x^{N^d}) \bmod (p, f(x))$ weil $N \in S$. Aber dann ist $g(x)^b \equiv g(x)^a \bmod (p, f(x))$ weil $N^d - 1 \mid b - a$ und $g(x)^{b-a} = g(x)^{\ell(N^d-1)} \equiv 1^\ell \equiv 1 \bmod (p, f(x))$.

[Gedachte $g(x^{N^d}) \overset{!}{\equiv} g(x) \bmod (p, f(x))$ wegen $f(x) \mid x^r - 1 \mid x^{N^d} - x \mid g(x^{N^d}) - g(x)$.]

Somit ist $g(x^b) \equiv g(x^a) \equiv g(x)^a \equiv g(x)^b \bmod (p, f(x))$ weil $a \in S$; dies zeigt $b \in S$.

• Nun sei $b = \frac{N}{p}$ und $a = N p^{\varphi(N^d-1)-1}$, also $a \in S$ wegen $p, N \in S$ und 1. Beh.

Ebenso ist $b \equiv a \ (N^d - 1)$, also $b = \frac{N}{p} \in S$ nach eben Gezeigtem.

Dies zeigt laut 2. Beh. (anwendbar da $r \mid N^d - 1$), dass $\#G \mid a - b$.

• Die nat. Zahlen $\left(\frac{N}{p}\right)^i p^j$ für $i, j \geq 0$ sind p.w.v., auch für $> \#R$ viele Paare mit $0 \leq i, j \leq \sqrt{\#R}$, also ex. zwei mit $\left(\frac{N}{p}\right)^i p^j \equiv \left(\frac{N}{p}\right)^I p^J \ (r)$. Laut 1. Beh. sind $\left(\frac{N}{p}\right)^i p^j$, $\left(\frac{N}{p}\right)^I p^J \in S$.

Laut 2. Beh. ist $\#G \mid \left(\frac{N}{p}\right)^i p^j - \left(\frac{N}{p}\right)^I p^J$, also $\#G \leq \left| \left(\frac{N}{p}\right)^i p^j - \left(\frac{N}{p}\right)^I p^J \right| \leq \left(\frac{N}{p} \cdot p\right)^{\sqrt{\#R}} - 1$

$= N^{\sqrt{\#R}} - 1$. ⊠

3. Beh.: Seien $f(x), g(x) \in \mathbb{Z}[x]$ mit $f = g$ in $\mathbb{F} = \mathbb{Z}[x]/(p, h(x))$.

Die Reduktionen von f und g in $\mathbb{F}$ seien Elemente von H. Falls $\deg(f), \deg(g) < \#R$, dann ist $f(x) \equiv g(x) \ (p)$ [in $\mathbb{Z}_p[x]$].

Bew.: Sei $\Delta(y)$ die Reduktion von $f(y) - g(y) \in \mathbb{Z}[y]$ in $\mathbb{F}$.

Für $k \in S$ ist $\Delta(x^k) = f(x^k) - g(x^k) = f(x)^k - g(x)^k = 0$ in $\mathbb{Z}[x]/(p, h(x))$, d.h. in $\mathbb{F}$.

Nun hat x Ordnung r in $\mathbb{F}$ [denn $\mathrm{ord}_{\mathbb{F}}(x) = r$, also $x^{r/t} \neq 1$ in $\mathbb{F}$, sonst $= 1$ in $\mathbb{F}$ $\not\downarrow$]

also sind die El. von $\{x^k; k \in R\}$ alle p.w.v. Nullst. von $\Delta(y)$ mod $(p, h(x))$, da $\#R < r$.

Da $\deg \Delta(y) < \#R$ [wegen $x^r = 1$ in $\mathbb{F}$ ist der größtmögliche Grad $r - 1 < r$], aber $\geq \#R$ Nullst. mod $(p, h(x))$ ex, ist $\Delta(y) \equiv 0 \ (p, h(x))$. Also ist $\Delta(y) \equiv 0 \ (p)$, da die Koeff. von Δ unabh. von x sind. □

8.11. **Beweisfortsetzung:** Die (Kontraposition der) 3. Beh. implizieret, dass die Produkte $\prod_{a \in T} (x + a) \in G$ für jede echte Teilmenge T von $\{0, 1, 2, \ldots, B\}$ verschiedene Elemente von G ergeben.

Dies zeigt $\#G \geq 2^{B+1} - 1$ mit $B = \lfloor A \rfloor = \lfloor \sqrt{d} \log(N) \rfloor$,

also $\#G > N^{\sqrt{\#R}} - 1$ im $\not\downarrow$ zu ⊠. □

8.12. **Konstruktion von f:** • Für r prim sei $\zeta_r := e^{2\pi i/r}$ die erste r-te EW.
Für $q \mid r-1$ sei $\eta := \sum_{j\in J} \zeta_r^j$ mit $J := \{j(r);\ j^{(r-1)/q} \equiv 1\ (r)\}$
eine Gaußsche Periode.

Dabei ist $J = J_{r,q}$ die Menge der reduzierten Restklassen mod q, die q-te Potenzen mod r sind. Es ist J eine UG der zyklischen Gruppe $\mathbb{Z}_r^\times$, also $J = \{g^{qi};\ 0 \le i < \frac{r-1}{q}\}$ für einen Erzeuger g von $\mathbb{Z}_r^\times$.
Weiter hat J insg. q viele Nebenklassen in $\mathbb{Z}_r^\times$, nämlich $g^i J$ für $0 \le i \le q-1$.
Dabei hat $\eta = \eta_0$ die Konjugierten $\eta_i := \sum_{j\in J} \zeta_r^{g^i j}$ für $0 \le i \le q-1$. [Antos $\zeta_r \mapsto \zeta_r^k$ von $\mathbb{Q}(\zeta_r)$, $1 \le k \le r-1$.]
Das Mipo von η über $\mathbb{Q}$ ist also $f(x) := \prod_{i=0}^{q-1} (x - \eta_i) \in \mathbb{Z}[x]$.
• Sei $p \neq r$ prim. Im Zahlring von $\mathbb{Q}(\zeta_r)$, nämlich $\mathbb{Z}[\zeta_r]$, [vgl. ZT I, 29.10] zerfällt (p) in ein Produkt von Primidealen [vgl. ZT I, Z13.4]. Sei $\mathcal{P}$ ein solches Primideal.
Auch $f(x)$ kann mod p zerfallen, also sei $g(x)$ irreduzibler Faktor von $f(x) \in \mathbb{F}_p[x]$ mit $g(\eta) = 0$. Nun gilt in $\mathbb{F}_p$ ja $g(x^p) = g(x)^p$ (p), also mod $\mathcal{P}$, also $g(\eta^p) = g(\eta)^p \equiv 0$ mod $\mathcal{P}$. Daher ist $\eta^p \equiv \eta_{i_2}$ (p), wo $\eta_{i_2} \in g^{i_2} J$ eine Nst. von $g(x)$ mod $\mathcal{P}$ ist, und analog $\eta_i \equiv \eta_{i_k}$ mod q ebenso für $0 \le i \le q-1$. Diese Nst. sind p.w.v. genau wenn $\mathrm{ord}_r(p^{(r-1)/q}) = q$. Daraus kann hergeleitet werden: $f(x)$ irred. mod p $\Leftrightarrow$ $\mathrm{ord}_r(p^{(r-1)/q}) = q$.
• Auf diese Art konstruieren wir ein irred. Polynom vom Grad q über $\mathbb{F}_p$, das Mipo von η.
Weiter betr. mehrere PZen $r_1, \dots, r_k$ und p.w. teilerfremde $q_1, q_2, \dots, q_k \in \mathbb{N}$ mit $q_i \mid r_i - 1$ für jedes i. Sei $f(x)$ das Mipo von $\eta_1 \eta_2 \cdots \eta_k$ über $\mathbb{Q}$, dieses hat Grad $q_1 q_2 \cdots q_k$ und ist irred. mod p genau wenn $\mathrm{ord}_{r_i} p^{(r_i-1)/q_i} = q_i$ für alle i ist.
So konstruieren wir f: Zu geg. N seien q_i, r_i wie oben, wo p durch N ersetzt ist.
Wenn N prim ist, ist $\mathbb{Z}[x]/(N, f(x))$ ein Pseudokörper.
Wenn N zusgesetzt ist, dann ist $\mathbb{Z}[x]/(N, f(x))$ kein Pseudokörper [dies belegt die Zusgesetztheit von N; die Bedingungen (i)–(iii) in 8.6 sind schnell überprüfbar],
alles dies ist ein Pseudokörper, so dass der AKS-Test 8.9 von Lenstra/Pomerance greift, vorausgesetzt dass $q_1 q_2 \cdots q_k > \log^2(N)$, mit dem N auf Primalität getestet werden kann.

8.13. **Satz (zur Existenz passender f):** Es gibt eine berechenbare Konstante N_0 so, dass für $N > N_0$ Primzahlen $r_1, r_2, \dots, r_k < \log^2(N)$ und p.w. teilerfremde $q_1, q_2, \dots, q_k \in \mathbb{N}$ existieren mit $q_i \mid r_i - 1$ und $\mathrm{ord}_{r_i}(N^{(r_i-1)/q_i}) = q_i$ für alle i, wobei $\log^2(N) < q_1 q_2 \cdots q_k < 4\log^2(N)$ gilt.

8.14. **Bem.:** • Zur Prüfung von $\operatorname{ord}_r(N^{(r_i-1)/q_i}) = q_i$: checke nur ob $N^{r_i-1} \equiv 1 \ (r_i)$ und $N^{(r_i-1)/q_i} \not\equiv 1 \ (r_i)$.

⇝ Mit Satz 8.13 kann die Bestimmung der r_i und q_i in $O(\log^3(N))$ Schritten erfolgen.

[Anzahl der r_i ist $O(\log^2(N))$, für jedes i checke Ordnungsbed. in $O(\log(N))$ Schritten.]

Mit der Laufzeit $O(d^{3/2}\log^3(N))$ mit $d = q_1 q_2 \cdots q_k = O(\log^2(N))$ für (c) folgt die behauptete Laufzeit.

Zum Beweis von 8.13 wird folgendes Lemma benötigt.

8.15. **Lemma:** Ist $S \subseteq \mathbb{R}_{>0}$ offene Teilmenge, die abg. bzgl. $+$ ist so, dass $\int_{\substack{0 \le t \le u \\ t \in S}} \frac{dt}{t} > u$ ist für ein $u \in]0,1]$, dann ist $1 \in S$. [Bew.: [LP, §9]]

Beweisskizze von Satz 8.13: Sei $x = (\log(N))^{1+3\eta}$ mit $\eta = \frac{1}{\log\log\log(N)}$.

• Für die meisten Pzen r ist $r-1$ aus großen Primteilern zusammengesetzt, d.h. $\prod_{\substack{q \mid r-1 \\ q > x^{\eta^2}}} q > x^{1-\eta}$ für alle bis auf $O(\frac{x}{\log^3(N)})$ viele Pzen $r \le x$.

Mit solchem r ist es sehr wahrscheinlich, dass $\operatorname{ord}_r(N^{(r-1)/q}) = q$ für solch ein $q \mid r-1$. Denn wenn nicht, hat N Ordnung $< x^{\eta}$ mod r; aber es gibt wenig solcher r:

• Sei $Q := \{q \in]x^{\eta^2}, x^{1/2}] : \exists r \le x, r \text{ prim}, r \equiv 1 \ (q), \operatorname{ord}_r(N^{(r-1)/q}) = q\}$.

Obiges zeigt dann $\sum_{q \in Q} \frac{1}{q} > \frac{3}{11} - o(1)$. Dafür werden stärkere Methoden der analytischen ZT eingesetzt: einmal die Ungl. von Brun-Titchmarsh [ZT II, a19.3], sowie eine effektive Version des Satzes von Bombieri-Vinogradov [ZT II, a21.12], die den Einfluss der Siegelnullstelle und zugeh. Modul berücksichtigt [in [LP] bewiesen].

• Sei $\varepsilon := \frac{\eta^2}{2\log\log(N)}$. Für jedes $q \in Q$ sei $\tau_q := \frac{\log(q)}{2\log\log(N)}$ und $S_0 := \bigcup_{q \in Q}]\tau_q - \varepsilon, \tau_q[$, und S der Abschluss von S_0 bzgl. $+$.

Lemma PZS/Mertens ist $\sum_{\substack{x^{\alpha} < q < x^{\beta} \\ q \text{ prim}}} \frac{1}{q} \sim \log\left(\frac{\beta}{\alpha}\right) = \int_{\alpha}^{\beta} \frac{dt}{t}$, woraus folgt, dass

$\int_{\substack{0 \le t \le \frac{1}{4}+\eta \\ t \in S}} \frac{dt}{t} > (1+o(1)) \sum_{q \in Q} \frac{1}{q} > \frac{3}{11} - o(1)$ folgt. Mit Lemma 8.15 folgt $1 \in S$,

also ex. $V \subseteq S_0$ mit $\sum_{v \in V} v = 1$. Sei $U := \{q \in Q : v \in]\tau_q - \varepsilon, \tau_q[\text{ für ein } v \in V\}$.

[OE: verschiedene v geben verschiedene q; die Argumentation kann derart modifiziert werden.]

Somit ist $0 < \sum_{q \in U} \log(q) - 2\log\log(N) < 2$, wie für Satz 8.13 verlangt.

□