Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K7: Primzahltests, Pseudo-Primzahlen

Stichworte: Probab. Pz test, Pseudo-Pz, Carmichael-Zahlen, Miller-Rabin-Test, Satz von Ankeny und die (GRH), Artinsche Primitivwurzel-Vermutung

---

7.1. **Primzahltestproblem:** Teste ob ein zufällig gewähltes, großes $N \in \mathbb{N}$, $N>2$, (mit hoher Wahrscheinlichkeit) eine Primzahl ist. In der Praxis (für industrielle Zwecke) werden probabilistische Tests benutzt: ein solcher Test erkennt sicher ein zusammengesetztes N, andernfalls liefert er, dass N sehr wahrscheinlich prim ist. Solche Tests sind polynomiell schnell. Für die üblichen Krypto-Anwendungen reichen probabilistische Primzahltests aus, um große Pzen zu erzeugen (Zahlen N, die sehr wahrscheinlich prim sind): Man erzeugt zufällig eine ungerade Zahl N im gewünschten Bereich und testet. Falls N zus'ges., testet man $N+2$, dann $N+4$ usw. Man erwartet laut Pz Satz bis $N+C$ etwa $\sim \log(N)$ viele Pzen, da $p_m \sim m \log(m)$, vgl. a20.13 (ZT II). Man muss also nicht lange warten, bis der Test anschlägt.
Der erste solche Test war [1974, Solovay-Strassen]. Eine bis heute benutzte Verfeinerung ist der Miller-Rabin-Test 7.6, die wir vollständig beweisen.

7.2. **Grundlage / Heuristik:** Hintergrund ist der Kleine Fermatsche Satz, d.h.
p prim $\Rightarrow$ Für alle $a \in \mathbb{Z}$ mit $p \nmid a$ gilt $a^{p-1} \equiv 1 \ (p)$.
Man kann hier versucht sein, die Umkehrung zu raten; hier ist „$\Leftarrow$" zwar i.a. falsch, aber dennoch oft richtig: Ist $N = p \cdot q$ zus'gesetzt mit $p \neq q$ prim, und $U := \{a \in \mathbb{Z}_N^\times ;\ a^{N-1} \equiv 1 \ (N)\}$, so ist $U = \ker(f)$, wo $f: a \mapsto a^{N-1}$.
Also ist U eine UG von $\mathbb{Z}_N^\times$, also $\#U \leq \frac{1}{2} \#(\mathbb{Z}_N^\times) = \frac{\varphi(N)}{2}$,
Sofern ein $a \in \mathbb{Z}_N^\times \setminus U$ überhaupt existiert.

7.3. Eine Verbesserung dieser Idee ist bereits der Solovay-Strassen-Test: dieser testet, ob $a^{(N-1)/2} \equiv \pm 1 \ (N)$ gilt. Gilt dies für alle a, $(a,N)=1$, so ist N eine PZ (ohne Beweis), und dann $a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \ (N)$ nach dem Euler-Kriterium.

Allerdings gibt es zus.gesetzte Zahlen, für die diese Kriterien greifen, sich also wie Primzahlen verhalten:

7.4. **Def.:** • Eine zus.gesetzte Zahl N mit $a^{N-1} \equiv 1 \ (N)$ für ein $a \in \mathbb{Z}$, $(a,N)=1$, heißt Pseudo-Primzahl zur Basis a.

• Eine zusammengesetzte Zahl N heißt Euler-PseudoPZ zur Basis $a \in \mathbb{Z}$, $(a,N)=1$, falls $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \bmod N$ gilt, vgl. 7.3.

• Eine zus.gesetzte Zahl N heißt Carmichaelzahl, falls $a^{N-1} \equiv 1 \ (N)$ für alle $a \in \mathbb{Z}$ mit $(a,N)=1$ gilt.

7.5. **Bem.:** • Carmichael vermutete 1912, dass es ∞ viele Carmichaelzahlen gibt.

• Bewiesen [1994: Alford, Granville, Pomerance]: $\#\{N \le x;\ N \text{ Carmichaelzahl}\} \gg x^{2/7}$, wurde zu $x^{1/3}$ verbessert

• Carmichaelzahlen sind ungerade: Wäre $2 \mid N$, folgt $-1 \equiv (-1)^{N-1} \equiv 1 \ (N)$, $\lightning$ zu $N>2$.

• Carmichaelzahlen sind quadratfrei, bestehen aus mind. 3 Primfaktoren und erfüllen das Korselt-Kriterium: N Carmichael $\Leftrightarrow p-1 \mid N-1$ für alle $p \mid N$ prim. [siehe EinfZT, (ii) Blatt 12 Aufgabe 1]

• D. Larsen zeigte 2022 im Alter von 17 Jahren, dass für große $x = x(\delta)$ zwischen x und $\frac{x}{\log^{\frac{1}{2}+\delta}(x)}$ mindestens $\exp\left(\frac{\log(x)}{\log\log^{2+\delta}(x)}\right)$ viele Carmichaelzahlen liegen. → "Bertrands Postulat für Carmichael-Zahlen"

Wir zeigen nun, dass der Begriff einer Pseudo-PZ noch verfeinert werden kann angesichts des folgenden probabilistischen PZ-Tests, der bis heute (industriell) angewendet wird. Lemt 7.2 gibt es ja wenig Ansatzpunkte zu der Umkehrung des Kleinen Fermatschen Satzes – eine Idee, die zu folgendem Test ausbaufähig ist.

7.6. **Satz (Miller-Rabin-Test):** Sei $N>1$ ungerade, $N-1=2^k\cdot v$, v ungerade.
(i) Gilt für jedes $a\in\mathbb{Z}$ mit $(a,N)=1$, dass
(*) $a^v\equiv 1\ (N)$ oder ex. $l\in\{0,1,\dots,k-1\}: a^{2^l v}\equiv -1\ (N)$,
dann ist N eine Primzahl.
(ii) Ist N zus.gesetzt, gilt $\#\{a\in\{1,\dots,N-1\};\ (a,N)=1,\ (*)\}\leq\frac{\varphi(N)}{4}$.

「Klar: (ii) ⇒ (i)」

7.7. **Bem.:** • Erhalte so einen Test: Wähle $a\in\mathbb{Z}_N^\times$ zufällig. Gilt dann (*), entscheide "N (wahrscheinlich) prim". Die W., dass (*) gilt (für zufällig gewähltes a) und N trotzdem zus.gesetzt ist, beträgt nur $\leq\frac{1}{4}$. Bei t-facher Wdh. also $\leq(\frac{1}{4})^t$, was schnell sehr klein ist. N ist dann mit W. $\geq 1-\frac{1}{4^t}$ eine Primzahl.
• Die Miller-Rabin-Bedingung (*), wo ein l mit $a^{v\cdot 2^l}\equiv -1\ (N)$ zu ermitteln ist, kann durch sukzessives Quadrieren von a^v rechnerisch durchgeführt werden.
• Die Laufzeit dieses probabilistischen Algorithmus ist $O(\log^5(N))$ Bitoperationen. Er ist also polynomiell (in der Inputgröße $O(\log N)$) 「sofern die (ERH) wahr ist, s.u. Bem. 7.19.」

7.8. • **Bsp.:** $N=2^{400}-593$, $t=100$, ist prim mit W. $\geq 1-\frac{1}{4^{100}}$, wo $\frac{1}{4^{100}}<10^{-60}$.
(Später wurde N prim mit einem deterministischen Test bestätigt.) 「Dezimalstellenanzahl: $2^{400}=10^{400\log_{10}(2)}\overset{R}{\approx}10^{120.4}$」

7.9. **Def.:** Man nennt eine Zahl N mit (*) für ein a, $(a,N)=1$, eine **starke Pseudo-Primzahl zur Basis a.**

7.10. **Bem.:** Der Miller-Rabin-Test wurde bereits in Einf ZT E12.25 vorgestellt und nicht in allen Fällen komplett bewiesen (ii), im Fall wenn N keine Carmichaelzahl ist, wurde nicht ausgeführt). Wir zeigen hier einen vollständigen Beweis (eher selten in der Literatur zu finden). Dazu sind Vorbereitungen nötig.

7.11. **Lemma:** Sei $d := (k, m)$. Dann gibt es in der Gruppe $\{g, g^2, g^3, \dots, g^m = 1\} = \langle g \rangle$, $\operatorname{ord}(g) = m$, genau d viele Elemente x mit $x^k = 1$ (d.h. k-te EW).

Bew.: g^j erfüllt die Glg. $\Leftrightarrow g^{jk} = 1 \Leftrightarrow m \mid jk \Leftrightarrow \frac{m}{d} \mid j \cdot \frac{k}{d}$

$\underset{(\frac{m}{d}, \frac{k}{d}) = 1}{\Leftarrow}$ $\frac{m}{d} \mid j$. Nun gibt es d viele Vielfache j von $\frac{m}{d}$ so, dass $1 \le j \le m$. □

7.12. **Lemma:** Sei $p > 2$ prim, schreibe $p - 1 = 2^s t$ mit $2 \nmid t$, $s \ge 1$.

Dann: $\#\{x \in \mathbb{Z}_p^\times;\ x^{2^r v} \equiv -1\ (p),\ 2 \nmid v\} = \begin{cases} 0, & r \ge s, \\ 2^r \cdot (t, v), & r < s. \end{cases}$

Bew.: Sei g eine PW mod p, d.h. $\langle g \rangle = \mathbb{Z}_p^\times$, und schreibe $x = g^j$ mit $0 \le j < p-1$.
Da $g^{\frac{p-1}{2}} \equiv -1\ (p)$ und $p - 1 = 2^s t$, ist die Kongruenz im Lemma äquivalent zu $2^r v j \equiv 2^{s-1} t\ (2^s t)$, mit unbekanntem j. Es gibt keine Lösung, falls $r > s - 1$.
Andernfalls teile durch $2^r d$, wo $d = (t, v)$.
Die so erhaltene Kongruenz $\frac{v}{d} j \equiv 2^{s-r-1} \frac{t}{d}\ (2^{s-r} \frac{t}{d})$ hat eine einzige Lsg. mod $2^{s-r} \frac{t}{d}$, also $2^r d$ viele Lösungen mod $2^s t$. □

7.13 **Proposition:** Ist $N > 1$ ungerade zusgesetzt, dann ist N eine starke PseudoPz zu höchstens 25% aller Basen a mit $0 < a < N$. (Im Sinne von 7.6. (ii), was dann gezeigt ist.)

Bew.: **1. Fall:** Sei N quadratfaktorfrei, d.h. $\exists p > 2$ prim: $p^2 \mid N$. Es gelte $p^\alpha \| N$, $\alpha \ge 2$.

Z.z.: Dann ist N keine Pseudo-Pz für mehr als $\frac{N-1}{4}$ viele Basen a mit $0 < a < N$.

Sei dazu a derart mit $a^{N-1} \equiv 1\ (N)$, also $a^{\frac{N-1}{2}} \equiv 1\ (p^2)$.
Nun ist $(\mathbb{Z}_{p^2})^\times$ zyklisch laut Einf ZT EZG, d.h. ex. $g \in \mathbb{Z}$ mit $(\mathbb{Z}_{p^2})^\times = \{g, g^2, g^3, \dots, g^{p(p-1)}\}$,
beachte: $\varphi(p^2) = p^2 - p = p(p-1)$.
Laut Lemma 7.11 ist $\#\{b\ (p^2);\ b^{N-1} \equiv 1\ (p^2)\} = d = (p(p-1), N-1)$. Da $p \mid N$ folgt $p \nmid N - 1$, also $p \nmid d$. Das größtmögliche d ist also $d = p - 1$. Daher ist

$$\frac{\#\{b\ (p^2);\ 0 < b < N,\ p^2 \nmid b,\ b^{N-1} \equiv 1\ (p^2)\}}{\#\{b\ (p^2);\ 0 < b < N;\ p^2 \nmid b\}} \le \frac{p-1}{p^2-1} = \frac{1}{p+1} \le \frac{1}{4}.$$

2. Fall: Sei $N = pq$ mit $p, q > 2$ prim, $p \neq q$. Schreibe $p-1 = 2^s t$ mit $2 \nmid t$, $s \geq 1$,
$q-1 = 2^{s'} t'$ mit $2 \nmid t'$, $s' \geq 1$.
(Sei $N-1 = 2^k v$, $2 \nmid v$.)

Sei o.E. $s \leq s'$. Um z.z., dass ein $a \in \mathbb{Z}_N^\times$ eine Basis ist, zu der N eine starke PseudoPZ ist, muss folgendes eintreten: (1) $a^v \equiv 1 \ (p)$ und $a^v \equiv 1 \ (q)$,
oder (2) $a^{2^r v} \equiv -1 \ (p)$ und $a^{2^r v} \equiv -1 \ (q)$ für ein r, $0 \leq r < s$. [CRS]

Laut Lemma 7.11 ist die # der a mit (1) das Produkt $(v,t) \cdot (v,t') \leq tt'$.
Laut Lemma 7.12 ist für jedes $r < \min(s,s') = s$ die # der a mit $a^{2^r v} \equiv -1 \ (N)$
gleich $2^r (v,t) \cdot 2^r (v,t') < 4^r tt'$.

Wegen $N-1 > \varphi(N) = 2^{s+s'} tt'$ folgt, dass der Anteil der $b \bmod N$, $0 < b < N$, für die N eine starke PseudoPZ ist, höchstens $\dfrac{\overbrace{tt'}^{(1)} + \overbrace{tt'}^{r=0} + \overbrace{4tt'}^{r=1} + \overbrace{4^2 tt'}^{r=2} + \dots + \overbrace{4^{s-1} tt'}^{r=s-1}}{2^{s+s'} tt'} = 2^{-s-s'} \left(1 + \dfrac{4^s - 1}{4-1}\right)$
beträgt.

- Falls $s' > s$, ist dies $\leq 2^{-2s-1} \left(\frac{2}{3} + \frac{4^s}{3}\right) \overset{s \geq 1}{\leq} 2^{-3} \cdot \frac{2}{3} + \frac{1}{6} = \frac{1}{4}$. ✓
- Falls $s' = s$, muss eine der Ungleichungen $(v,t) \leq t$, $(v,t') \leq t'$ strikt sein
  [Sonst $t \mid v$, $t' \mid v$. Aus $N-1 = 2^k v = pq - 1 = q - 1 \ (t)$
  folgt dann $t \mid q-1 = 2^{s'} t'$, also $t \mid t'$, und analog $t' \mid t$, $p = q$ ↯.]

Einer der beiden ggT's (v,t) und (v,t') ist daher strikt kleiner als t oder t', muss also um mindestens einen Faktor 3 kleiner sein (arbeiten mit ungeraden Zahlen).
In diesem Fall ersetze tt' durch $\frac{1}{3} tt'$ in obigen Abschätzungen für b, für das N eine starke PseudoPZ (zu b) ist.

Dies zeigt $\dfrac{\#\{b;\ 0 < b < N,\ N \text{ starke PseudoPZ zu } b\}}{\#\{b;\ 0 < b < N\}}$

$$\leq \frac{1}{3} \cdot 2^{-2s} \left(\frac{2}{3} + \frac{4^s}{3}\right) \overset{s \geq 1}{\leq} \frac{1}{18} + \frac{1}{9} = \frac{1}{6} < \frac{1}{4}.$$

3. Fall: Sei $N = p_1 \cdots p_i$ das Produkt von $i \geq 3$ vielen verschiedenen Pzen. Schreibe $p_j - 1 = 2^{s_j} t_j$ mit ungeraden t_j, gehe so vor wie im 2. Fall. OE sei $s_1 = \min\{s_1, \dots, s_i\}$. Erhalten folgende o.S. für die # der b, für die N starke Pseudo-Pz (zu b) ist:

$$2^{-s_1-s_2-\dots-s_i} \cdot \left(1 + \frac{2^{i \cdot s_1} - 1}{2^i - 1}\right) \leq 2^{-i s_1} \left(\frac{2^i - 2}{2^i - 1} + \frac{2^{i s_1}}{2^i - 1}\right)$$

$$= 2^{-i s_1} \cdot \frac{2^i - 2}{2^i - 1} + \frac{1}{2^i - 1} \underset{s_1 \geq 1}{\leq} 2^{-i} \cdot \frac{2^i - 2}{2^i - 1} + \frac{1}{2^i - 1} = 2^{1-i} \leq \frac{1}{4} \text{ da } i \geq 3.$$

□

7.14. **Bem.:** Kann Satz 7.6 / der Miller-Rabin-PZtest demnach zur Erzeugung großer Pzen (mit bestimmter Stellenanzahl) herangezogen werden?
Betr. etwa 100-stellige Zahlen, davon gibt es $10^{100} - 10^{99} = 9 \cdot 10^{99}$ viele.
Laut einer Tschebyschev-Version gilt für so große N, dass $0.9212 \cdot \frac{N}{\log(N)} < \pi(N) < 1.1056 \frac{N}{\log(N)}$,
dies zeigt $3.59696 \cdot 10^{97} < \pi(10^{100}) - \pi(10^{99}) < 4.07695 \cdot 10^{97}$,
also $> 0.4 \cdot 10^{97}$ viele Pzen im Intervall $[10^{99}, 10^{100}[$, ihr Anteil ist $> \frac{0.4 \cdot 10^{97}}{9 \cdot 10^{99}} > \frac{1}{2250}$
Wählt man also zufällig eine Zahl im IV und testet auf Primalität, muss der Rechner im Schnitt höchstens 2250 mal testen, bis er so auf eine Primzahl stößt.

7.15. **Bem.:** • Unter Ann. der erweiterten Riemannschen Vermutung (ERH) wurde von E. Bach gezeigt: $1 \neq G \leq \mathbb{Z}_N^\times$ mit $a \in G$ für alle $0 < a < x, (a,N) = 1 \Rightarrow x < 3 \log^2(N)$.
Somit: N zus. gesetzt $\Rightarrow \exists a \leq 3 \log^2(N)$ mit $a \notin P$,
wo P die UG der Basen in $\mathbb{Z}_N^\times$ ist, zu denen N starke Pseudo-PZ ist.
Siehe [E. Bach: Explicit bounds for primality testing and related problems, 1990; Thm. 3.].
• Sucht man also die a gezielt ab bzw. testet $a = 2, 3, \dots$ stößt man sehr bald auf ein $a \notin P$, es sei denn, die erweiterte Riemannsche Vermutung ist falsch.
(Die ERH bedeutet Nullstellenfreiheit aller Hecke-L-Funktionen in $\frac{1}{2} < \sigma < 1$.)
• Die Arbeit von Bach beruht auf einer Vorarbeit von Ankeny zur Größe des kleinsten quadratischen Nichtrests, nämlich folgendes Resultat.

7.16. **Satz (Ankeny, 1952):** Sei p prim. Dann ist in $\mathbb{Z}_p^\times$ der kleinste quadratische Nichtrest $q = n_p \bmod p$ (d.h. mit $\left(\frac{q}{p}\right) = -1$) von der Größe $n_p \ll \log^2(p)$, falls die verallg. Riemannsche Vermutung (GRH) wahr ist.

7.17. **Bem.:** Ohne Ann. der (GRH), d.h. unkonditionell, kann nur $n_p \ll \sqrt{p}$ gezeigt werden. Vgl. a17 in ZT II, in (ü) Blatt 8 Aufgabe 1 von ZT II wurde $n_p \ll \sqrt{p}\log(p)$ gezeigt.

7.18. **Beweis des Satzes 7.12 von Ankeny:** (sogar, wenn der Modul q nicht prim.)
Sei $\chi \neq \chi_0 \bmod q$ und $n(\chi) := \min\{n \in \mathbb{N};\ \chi(n) \neq 1,\ \chi(n) \neq 0\}$.
Wir nehmen an, dass $L(s,\chi) \neq 0$ für $\sigma > \frac{1}{2}$ gelte (die (GRH) für $L(s,\chi)$).
Z.z.: $n(\chi) \ll \log^2(q)$. Dazu betrachte

① $$\sum_{n \le x} \chi(n)\Lambda(n)\cdot(x-n) = \frac{-1}{2\pi i}\int_{\sigma_0 - i\infty}^{\sigma_0 + i\infty} \frac{L'}{L}(s,\chi)\,\frac{x^{s+1}}{s\cdot(s+1)}\,ds,$$ wo $\sigma_0 > 1$ (Perron-Formel a3.12)

Durch Verschiebung des Integralwegs auf die Gerade $\sigma = \frac{1}{4}$ ist dies (laut Residuensatz)

$$= -\sum_s \frac{x^{s+1}}{s(s+1)} - \frac{x^{5/4}}{2\pi}\int_{-\infty}^{\infty} \frac{L'}{L}\left(\tfrac{1}{4}+it,\chi\right)\frac{x^{it}}{(\frac{1}{4}+it)(\frac{5}{4}+it)}\,dt.$$

Laut [Lemma a10.7, ZT II] ist die s-Summe $\ll x^{\frac{3}{2}}\log(q)$ aufgrund der (GRH).
Weiter ist $\frac{L'}{L}(\frac{1}{4}+it,\chi) \ll \log(q(|t|+2))$, so dass der $\int$-Term $\ll x^{\frac{5}{4}}\log(q)$ ist.
"Hatten in ZT II, a10, " $\ll \log^2(q(|t|+2))$ gezeigt für σ nahe 1;
dies läßt sich bei $\sigma = \frac{1}{4}$ verbessern mit Lemma a10.7 aus ZT II, und aufgrund der (GRH).]
Für $x \ge C'\log(q)\log\log(q)$ ist andererseits

② $$\sum_{n \le x} \chi_0(n)\Lambda(n)(x-n) = \sum_{n \le x}\Lambda(n)(x-n) + O\left(x\log(x)\log(q)\right) \gg x^2.$$

Falls $\chi(n) = \chi_0(n)$ für alle Primpotenzen $n \le x$ gilt,
sind die l.S. von ① und ② gleich. Die r.S. sind aber inkonsistent,
falls man $x = C'\log^2(q)$ nimmt, denn $\log^{\frac{5}{2}}(q)\log(q) \gg \log^4(q)$ ist ein $\lightning$.
Es folgt die Beh., dass ein $n \le x$ mit $\chi(n) \neq \chi_0(n)$ ex.

□

7.19 **Bem.:** • Dies beleuchtet die Rolle der Riemannschen Vermutung für die Algor. ZT: Führt man den Miller-Rabin-Test für alle $a \in \mathbb{N}$ mit $(a, N) = 1$ und $1 < a \leq 3\log^2(N)$ aus, so dass jeweils (*) gilt, so ist N prim oder die (ERH) ist falsch. Also kann man sich getrost in der Praxis auf so wenige a verlassen! Unter Ann. der (ERH) ist die Laufzeit (= # Bitop.) $O(\log^5(N))$, vgl. [Yan, Thm. 2.2.13].

• Ist $g(p) \in \mathbb{N}$ die kleinste Primitivwurzel mod p, d.h. Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$, so gilt $n_p \leq g(p)$. Jede obere Schranke für $g(p)$ liefert also auch eine für n_p.
Die bislang beste o.B. ist $g(p) \ll \omega(p-1)^4 (\log(\omega(p-1)+1)^4 \log^2 p$ [Shoup 1992] unter Ann. der (GRH). Unkonditionell: $g(p) \ll p^{1/4+\varepsilon}$ [Burgess 1962]

• Ist $g \in \mathbb{N}$ gegeben, können auch die Pzen p mit $g(p) = g$ betrachtet werden. Dies führt zur:

7.20 **Artinsche Primitivwurzelvermutung:** Ist $g \in \mathbb{N}$ keine □-Zahl, gibt es unendl. viele p mit $\mathrm{ord}(g) = p-1$, d.h. für die g eine PW mod p ist.
Über die Zä/Hfunktion dieser $p \leq x$ vermutet man eine sehr genaue Asymptotik:
Sei (etwas allgemeiner) $g \in \mathbb{Q} \setminus \{-1, 0, 1\}$.
Ist $\mathcal{P}(g) := \{p \in \mathbb{P};\ \mathrm{ord}_p(g) = p-1\}$, und $\mathcal{P}(g)(x) = \#\{p \in \mathcal{P}(g);\ p \leq x\}$, ist $h \in \mathbb{Z}$ maximal mit $g = g_0^h$ für ein $g_0 \in \mathbb{Q}$, so sollte die Asymptotik

$$\mathcal{P}(g)(x) = \underbrace{\prod_{\substack{q \nmid h \\ q \text{ prim}}} \left(1 - \frac{1}{q(q-1)}\right) \prod_{\substack{q \mid h \\ q \text{ prim}}} \left(1 - \frac{1}{q-1}\right)}_{=: A(g)} \cdot \frac{x}{\log(x)} + o\left(\frac{x}{\log(x)}\right)$$

gelten.

$\rightsquigarrow$ beachte $A(h) = 0$ für $2 \mid h$ $\rightsquigarrow$ die Asymptotik zeigt $\#\mathcal{P}(g) = \infty$ genau wenn g kein □

Dabei ist $A(1) = \prod_q \left(1 - \frac{1}{q(q-1)}\right) = 0.37395581\ldots$ die Artinsche Konstante, vgl. [P. Moree, Artin's Primitive Root Conjecture – A Survey, 2012].