Vorfaktorbestimmung für das Quadratische Sieb

Thorsten Reinecke

2. Februar 2000

1 Herleitung des Verfahrens

Für die effiziente Implementierung des Quadratischen Siebs zur Faktorisierung natürlicher Zahlen (und darauf aufbauender Verfahren wie des multipolynomialen Siebs) ist es erforderlich, die zu faktorisierende Zahl mit einem Vorfaktor zu multiplizieren. Je nach gewähltem Vorfaktor sind andere Primzahlen in der Faktorbasis enthalten.

Nach Abschluß des Quadratischen Siebverfahrens erhält man (grob vereinfacht ausgedrückt) eine nichttriviale quadratische Kongruenz zu 1 modulo der zu faktorisierenden Zahl, die als Produkt von Primzahlpotenzen der Faktorbasis angegeben ist.

$$(\prod_{p \in FB} p^{e_p})^2 \equiv 1 \bmod N$$

Aus Umformung der Kongruenz und Bestimmung des größten gemeinsamen Teilers erhält man schließlich einen (nicht notwendigerweise primen) Teiler der zu faktorisierenden Zahl N:

$$\gcd((\prod_{p \in FB} p^{e_p}) - 1, N)$$

Prinzipiell ist jede genügend große Faktorbasis zur Ermittlung der quadratischen Kongruenz geeignet. Da zur Ermittlung der quadratischen Relationen allerdings ein hoher Siebaufwand erforderlich ist, wäre es wünschenswert, dem Siebverfahren eine Faktorbasis zugrunde zu legen, mit der man möglichst schnell möglichst viele Relationen ermitteln kann.

Die Quadratischen Kongruenzen, aus denen die Primfaktorzerlegungen, die innerhalb der Faktorbasis aufgehen, bestimmt werden, definieren sich bei der einfachen Version des Quadratischen Siebes durch

$$Q_k(\Delta) := (\left\lfloor \sqrt{k \cdot N} \right\rfloor + \Delta)^2 - k \cdot N$$

Hierbei entsteht jedoch ein Zielkonflikt, da man lediglich über die Wahl des Vorfaktors die Faktorbasis variieren kann, ein hoher Vorfaktor jedoch ceteris paribus den Siebaufwand vergrößert.

Die erweiterte Faktorbasis bei verschiedenen Vorfaktoren k bestimmt sich für eine zu faktorisierende Zahl N wie folgt:[1]

$$FB_k^{erweitert} := \{p \mid \left(\frac{k \cdot N}{p}\right) \neq -1)\} \cup \{-1\}$$

[1] Der Faktor -1 spielt nur für die Vorzeichenbehandlung eine Rolle und braucht für die Vorfaktorermittlung nicht berücksichtigt zu werden. Die Problematik mit dem Faktorbasiselement 2 bzgl. des Legendresymbols vernachlässigen wir ebenfalls. Üblicherweise wird man in der Praxis mit der 2 und ihren Potenzen nicht sieben, da dies zu aufwendig ist. Trotzdem kann die 2 für die Vorfaktorbewertung eine Rolle spielen.

Die im Rahmen der Faktorisierung verwendeten (statischen) Faktorbasen $FB_k \subset FB_k^{erweitert}$ haben dabei eine vorher festgesetzte, von N abhängige, endliche Kardinalität und bestehen (üblicherweise) aus den den diesbezüglich kleinsten positiven Elementen von $FB_k^{erweitert}$.[2]

Man kann also davon ausgehen, daß etwa die Hälfte der in einem für die Faktorbasis relevanten Intervall vorkommenden Primzahlen quadratische Reste liefern und damit auch Elemente dieser Faktorbasis sind. – Als einzige Einflußmöglichkeit auf die Faktorbasis verbleibt dann der Vorfaktor k.

Wenn $p \in FB_k$ teilerfremd zu $k \cdot N$ ist, so erhalten wir zwei Siebtreffer in einem Siebintervall der Größe p, andernfalls lediglich einen Treffer. Nicht nur die Größe, sondern auch die Teilbarkeitsstruktur von k hat also Einfluß auf die Güte der zugehörigen Faktorbasis.

Wir gehen nun von der realistischen Grundannahme aus, daß alle Primzahlen der Faktorbasis im Siebintervall jeweils gleichverteilt mit einer Wahrscheinlichkeit von jeweils $\frac{2}{p}$ teilen, sofern p und $k \cdot N$ teilerfremd sind. Jeder Siebtreffer wird dabei mit einem Trefferbonus von $\ln p$ gewichtet.

Auf diese Weise erhalten wir für eine vollständig in der Faktorbasis aufgehenden Relation folgende Äquivalenz (wobei p_j die gesiebten Primteiler, e_j deren Exponenten darstellen):

$$Q(x) = \prod_j p_j^{e_j} \Leftrightarrow \sum_j \ln p_j^{e_j} = \ln Q(x)$$

Für das Siebverfahren wird typischerweise anstelle von $\ln Q(x)$ ein einheitlicher Schwellwert für ein komplettes Siebintervall gewählt, um den Berechnungsaufwand klein zu halten. Ein geeigneter Schwellwert läßt dann das Vorkommen weiterer nichtgesiebter Primzahlpotenzen sowie einiger Primzahlen (sog. Large-Primes, Double-Large-Primes, etc.) außerhalb der Faktorbasis zu, die bei Erreichen des Schwellwertes durch Probedivision ermittelt werden. Der Schwellwert ist dabei so zu bestimmen, daß der Anteil ungeeigneter Relationen, die verworfen werden müssen, nicht ins Gewicht fällt.

Für die Bestimmung der Qualität einer zu k gehörigen Faktorbasis sollte die mittlere Summe der Trefferboni an jeder Stelle im Siebintervall unter den o.g. Annahmen maximiert werden.

Als geeignete Qualitätsfunktion setzen wir also an:

$$q(k) := \sum_{p \in FB_k} w_k(p) \cdot \ln p$$

, wobei $w_k(p)$ die Summe der Wahrscheinlichkeiten ist, mit denen die Potenzen von p an einer Stelle im Sieb treffen. (Man beachte ferner, daß $w_k(p)$ einheitlich mit $\ln p$ gewichtet werden kann, da bei höheren Potenzen die niedrigeren bereits gesiebt sind, also nur der Differenzanteil, eben $\ln p$ und nicht $\ln p^n$ für die n-te Pozenz von p als Bonus berücksichtigt werden darf.)

Als Vorfaktoren kommen ferner nur quadratfreie Zahlen in Frage, da die k teilenden Quadrate die Faktorbasis nicht positiv beeinflussen und damit den Vorfaktor unnötig erhöhen.[3]

Falls $\gcd(p, k \cdot N) = 1$, so gilt[4] $w_k(p) := \sum_{e=1}^{\infty} \frac{2}{p^e} = \frac{2}{p-1}$. Andernfalls teilen die höheren Potenzen von p nicht und $w_k(p) := \frac{1}{p}$.

Für den theoretischen Optimalwert q_{max} nehmen wir die theoretisch bestmögliche Faktorbasis FB_{opt} an, die aus direkt aufeinanderfolgenden Primzahlen besteht und setzen zusätzlich $w_k(p) := \frac{2}{p-1}$:

[2] Eine für unsere Zwecke ebenfalls zulässige Alternative wäre es, die Faktorbasis FB_k so zusammenzustellen, daß $q(k)$ minimal wird. Aber abgesehen davon, daß wir $q(k)$ momentan noch nicht definiert haben, hat diese Alternative den Nachteil, die Implementierung des Siebverfahrens für die Large-Prime-Varianten zu erschweren. Die ausgelassenen Faktorbasiselemente müßten jetzt nämlich getrennt zu den Large-Primes berücksichtigt werden.

[3] ... und außerdem die Teilbarkeitsbestimmungsregeln für Primzahlpotenzen unnötig verkomplizieren. – In der Praxis können dennoch durch nicht quadratfreie Vorfaktoren gelegentlich Laufzeitgewinne erzielt werden. Diese Laufzeitunterschiede unterliegen allerdings Schwankungen, die durch das (stochastische) Modell nicht vorhergesagt werden können.

[4] Um von der Größe N abstrahieren zu können, nehmen wir idealisierend an, daß *alle* Potenzen einer Primzahl als Teiler in Frage kommen, obwohl dies natürlich nur für diejenigen unterhalb von $Q(x)$ gelten kann.

$$q_{max} := \sum_{p \in FB_{opt}} \sum_{e=1}^{\infty} \frac{2 \cdot \ln p}{p^e} = 2 \cdot \sum_{p \in FB_{opt}} \ln p \cdot \sum_{e=1}^{\infty} p^{-e} = 2 \cdot \sum_{p \in FB_{opt}} \frac{\ln p}{p-1}$$

Mit q_{max} haben wir einen Referenzwert, an dem wir die tatsächliche Qualität der Faktorbasen messen können.

Für eine geeignete Bewertungsfunktion müssen wir den Schwellwert, den wir in etwa mit $\ln Q_k(\frac{M}{2})$ (M ist die Größe des festgelegten Siebintervalls) bzw. idealisiert mit $\ln \sqrt{k \cdot N}$ ansetzen, berücksichtigen. Die Bewertungsfunktion ergibt sich somit als

$$b(k) := \ln \sqrt{k \cdot N} - q(k) = 0.5 \ln(k \cdot N) - q(k)$$

Diese Bewertungsfunktion ist bezüglich k simulativ zu minimieren. Zunächst setzen wir dazu eine Größe $Size_{FB}$ fest, die bestimmt, wie viele Primzahlen in den zu simulierenden Faktorbasen enthalten sein sollen. Dann bestimmen wir q_{max} und anschließend für aufsteigende Vorfaktoren $b(k)$. Wir brechen die Simulation ab, wenn sichergestellt ist, daß höhere k nicht mehr zu einem minimalen $b(k)$ führen können. Hierzu ist für jeden bisher bestimmten besten Vorfaktor k_{best} die Obergrenze k_{max} zu berechnen, ab der die Simulation abgebrochen werden kann. Diese Obergrenze ist bei $b(k_{best}) = \frac{1}{2} \ln(k_{max} \cdot N) - q_{max}$ erreicht:

$$\frac{1}{2} \ln(k_{best} \cdot N) - q(k_{best}) = \frac{1}{2} \ln(k_{max} \cdot N) - q_{max}$$

$$\Leftrightarrow \frac{1}{2} \ln k_{best} + \frac{1}{2} \ln N - \frac{1}{2} \ln k_{max} - \frac{1}{2} \ln N = q(k_{best}) - q_{max}$$

$$\Leftrightarrow \ln \frac{k_{best}}{k_{max}} = 2 \cdot (q(k_{best}) - q_{max})$$

$$\Leftrightarrow k_{max} = \frac{k_{best}}{\exp(2 \cdot (q(k_{best}) - q_{max}))} = k_{best} \cdot \exp(2 \cdot (q_{max} - q(k_{best})))$$

Wie man also sieht, ist diese Obergrenze nur noch indirekt über die Faktorbasis von der zu faktorisierenden Zahl N abhängig. Anstelle der Bewertungsfunktion b kann deshalb auch eine modifizierte Bewertungsfunktion β verwendet werden:

$$\beta(k) := \ln \sqrt{k} - q(k) = \frac{1}{2} \ln k - q(k)$$

In der Praxis dürfte für größere zu simulierende Faktorbasisgrößen $Size_{FB}$ die Bedingung q_{max} unnötig hoch ausfallen. Denn es ist dann unwahrscheinlich, daß für große Faktorbasen alle Primzahlen in Folge enthalten sind. Der Wert k_{max} steigt damit sehr stark an, aber es ist nahezu ausgeschlossen, durch fortgesetzte Simulation bis zu dieser theoretischen Obergrenze noch eine Verbesserung zu erreichen. In diesem Fall empfiehlt es sich, q_{max} durch einen realistischeren Wert, z.B. $0.85 \cdot q_{max}$ zu ersetzen.

2 Praktische Ergebnisse

2.1 Messungen

Das Verfahren wurde in leicht modifizierter Form für das Faktorisierungsprogramm **qsieve** implementiert. In der folgenden Tabelle sind die Ergebnisse diverser Faktorisierungsläufe, die unter **qsieve-2.34** auf einem Pentium 166-MMX mit verschiedenen Vorfaktoren für die Zahl $N = \frac{11^{55}+20}{6196134869} = 1607911047862414358613559\ (25) \cdot 1897644264434621001343 01\ (24)$ durchgeführt wurden, zusammengefaßt. Der zehnstellige Faktor im Nenner wurde dabei durch das Pollard-Rho-Verfahren in ca. 19 Sekunden gefunden, die beiden übrigen Faktoren durch das quadratische Sieb.

Als Vorfaktoren kommen in der implementierten Fassung nur solche Zahlen vor, für die $k \cdot N \equiv 1 \bmod 8$ erfüllt ist. Die tatsächlich verwendete Faktorbasis hatte eine Größe von 1000 Elementen. Es wurden je ein Lauf mit einem Factor-Threshold von 1.0 (sowohl mit (B) als auch ohne (C) Berücksichtigung dynamische Faktoren[5]) und 1.5 (großer Anteil an dynamischen Faktoren (A)) durchgeführt. Die Vorfaktorbewertungen $\beta^i_{SIZE_{FB}}(k)$ wurden mit Faktorbasen der Größe von 75 und 1000 vorgenommen. Der Index i gibt dabei den Typ der Bewertungsfunktion an:

Bewertungsfunktion	Beschreibung
$\beta^1_{Size_{FB}}$	wie oben definiert, Berücksichtigung von Potenzen
$\beta^2_{Size_{FB}}$	wie oben, jedoch werden bei Siebtreffer keine Potenzen berücksichtigt
$\beta^3_{Size_{FB}}$	Berücksichtigung von Potenzen und Dirty-Sieving-Effekt
$\beta^4_{Size_{FB}}$	keine Berücksichtigung von Potenzen, Berücksichtigung des Dirty-Sieving-Effektes

In β^2 werden höhere Potenzen von Primzahlen aus der Faktorbasis vollkommen vernachlässigt. In β^3 sowie β^4 wurde gegenüber β^1 bzw. β^2 der Dirty-Sieving-Effekt[6] dadurch berücksichtigt, daß den Primzahlen aus der Faktorbasis, die $k \cdot N$ teilen, erst dann ein Bonus angerechnet wird, wenn mit ihnen auch gesiebt wird.[7]

2.2 Weitere Messungen

In der nachfolgenden Tabelle werden die Vorfaktoren für die Faktorisierung der Zahl $N = 13^{48}+22 = 5577686387918002774149382469\ (28) \cdot 52823456865058416450064747\ (26)$ bewertet.

Die Faktorbasis umfaßte 2000 Elemente, der Factor-Threshold betrug 1.8 und die ersten 5 Elemente der Faktorbasis wurden beim Siebvorgang vernachlässigt, um Zeit zu sparen. Mit Potenzen, die die Siebgröße nicht sprengten, wurde – wie auch im vorigen Beispiel – gesiebt.

[5]Die dynamischen Faktoren entsprechen in etwa den aus der Literatur hinlänglich bekannten single-large-primes, nur daß mit dynamischen Faktoren zusätzlich gesiebt wird.

[6]Als Dirty-Sieving bezeichnen wir eine Heuristik, mit der sich das Siebverfahren beschleunigen läßt: Mit kleineren Faktorbasiselementen wird nicht gesiebt.

[7]Bei teilerfremden Elementen können die Boni annäherungsweise in der kleinsten Potenz, mit der gesiebt wird, aufgeschlagen werden.

Tabelle 1: Laufzeiten und Bewertungen (Dirty-Sieving für die ersten 5 Elemente der Faktorbasis)

k	Zeit A	Zeit B	Zeit C	β^1_{75}	β^2_{75}	β^3_{75}	β^4_{75}
3	2m10.490s	3m5.500s	4m32.780s	-5.5137	-5.3374 (5)	-5.1475	-4.9712 (5)
11	1m51.390s (4)	2m11.570s (4)	3m18.690s (4)	-6.1929 (2)	-5.5863 (3)	-5.9749 (4)	-5.3683 (4)
19	1m37.970s (2)	2m5.110s (3)	3m7.720s (2)	-6.0850 (4)	-5.7305 (2)	-6.0850 (3)	-5.7305 (2)
27*	2m31.930s	3m50.310s	5m47.340s	-4.4151	-4.2388	-4.0489	-3.8726
35	2m13.260s	2m47.820s (5)	4m48.210s	-5.6097 (5)	-5.1585	-5.0098	-4.5586
43	3m5.880s	4m7.610s	7m39.600s	-3.9106	-3.8312	-3.9106	-3.8312
51	3m58.720s	7m19.100s	11m51.490s	-4.0411	-3.8417	-3.5082	-3.3088
59	1m28.870s (1)	1m33.360s (1)	2m24.800s (1)	-6.9347 (1)	-6.1698 (1)	-6.9347 (1)	-6.1698 (1)
67	4m3.660s	6m46.530s	10m40.770s	-3.4760	-3.3518	-3.4760	-3.3518
75*	2m37.650s	4m17.960s	6m24.060s	-4.2122	-4.0359	-3.5242	-3.3478
83	2m18.590s	2m59.340s	4m53.490s	-5.3405	-4.7838	-5.3405 (5)	-4.7838
91	2m48.450s	3m47.710s	6m24.770s	-4.3405	-4.1003	-3.8653	-3.6251
99*	2m9.300s (5)	3m21.500s	4m13.870s (5)	-4.3619	-4.1215	-3.7777	-3.5373
107	3m49.580s	5m31.120s	9m23.690s	-3.4666	-3.0693	-3.4666	-3.0693
131	1m41.240s (3)	1m57.120s (2)	3m15.490s (3)	-6.1114 (3)	-5.4111 (4)	-6.1114 (2)	-5.4111 (3)
851	2m31.450s	2m48.390s	5m3.050s	-4.9684		-4.9684	
923	2m37.200s	3m24.500s	5m42.870s	-4.3105		-4.1132	

k	Zeit A	β^1_{75}	β^2_{75}	β^3_{75}	β^4_{75}	β^3_{2000}	β^4_{2000}
7	9m44.410s	-5.5967 (5)	-5.3671 (3)	-5.3187	-5.0891 (3)	-8.9514	-8.7207 (4)
15	7m56.410s (3)	-6.0596 (2)	-5.8555 (2)	-5.3715 (5)	-5.1674 (2)	-9.1485 (5)	-8.9431 (3)
23	5m59.990s (2)	-7.6912 (1)	-6.9243 (1)	-7.6912 (1)	-6.9243 (1)	-11.6272 (1)	-10.8590 (1)
31	11m44.180s	-4.2522	-4.1384	-4.1414	-4.0276	-7.9966	-7.8817
39	13m47.480s	-3.8850	-3.7487	-3.3215	-3.1852	-7.1155	-6.9780
47	12m43.800s	-4.7923	-4.2008	-4.7923	-4.2008	-8.4529	-7.8603
55	13m36.590s	-3.8666	-3.7983	-3.3267	-3.2585	-7.0727	-7.0034
63*	10m14.920s	-4.8482	-4.6187 (5)	-4.2040	-3.9745	-7.8522	-7.6216
71	9m17.650s (5)	-5.4048	-4.8346 (4)	-5.4048 (3)	-4.8346 (4)	-9.2310 (3)	-8.6595 (5)
79	9m56.530s	-4.5392	-4.3286	-4.5392	-4.3286 (5)	-8.4649	-8.2531
87	14m2.430s	-4.1611		-3.6787		-7.3236	-7.0967
95	10m1.320s	-5.2110		-4.8891		-8.7181	-8.1780
143	8m47.380s (4)	-5.8008 (4)		-5.3855 (4)		-9.2240 (4)	-8.6058
183	9m42.700s	-5.1475				-8.6128	-8.2565
207*	5m55.710s (1)	-5.8602 (3)		-5.4939 (2)		-9.4300 (2)	-9.0280 (2)

2.3 Bewertung und Folgerungen

Nicht aus den Tabellen ersichtlich sind die mit steigender zu simulierender Faktorbasis ansteigenden Simulationslaufzeiten. Das implementierte Verfahren (mit β_{75}) liefert in allen vier Varianten für die Praxis brauchbare Ergebnisse. Die Entscheidung, welches Verfahren in einer konkreten Implementierung des Quadratischen Siebs eingesetzt werden sollte, bedarf genauer Analysen. Das Entscheidungsverfahren sollte nach Möglichkeit die implementierten Heuristiken berücksichtigen. Falls "Dirty-Sieving" zum Einsatz kommt und nicht vollständig mit Potenzen gesiebt wird, sollte eine Variante der Bewertungsfunktion β^4vorgezogen werden.

Eine Verbesserung der Resultate bezüglich der Simulationslaufzeit läßt sich dabei mit folgender Heuristik erreichen:

Zunächst werden mit einer relativ kleinen Faktorbasis die fünf besten Vorfaktoren ermittelt. Nur für diese fünf Werte wiederholt man die Vorfaktorbewertung mit einer größeren Faktorbasis.

Tabelle 2: Laufzeiten und Bewertungen (Dirty-Sieving für die ersten 5 Elemente der Faktorbasis)

k	Zeit A	Zeit B	Zeit C	β^1_{1000}	β^2_{1000}	β^3_{1000}	β^4_{1000}
3	2m10.490s	3m5.500s	4m32.780s	-8.5511 (5)	-8.3737 (5)	-8.1849	-8.0075 (5)
11	1m51.390s (4)	2m11.570s (4)	3m18.690s (4)	-9.2709 (2)	-8.6631 (3)	-9.0529 (4)	-8.4451 (4)
19	1m37.970s (2)	2m5.110s (3)	3m7.720s (2)	-9.2395 (3)	-8.8837 (2)	-9.2395 (2)	-8.8837 (2)
27*	2m31.930s	3m50.310s	5m47.340s	-7.4525	-7.2751	-7.0863	-6.9089
35	2m13.260s	2m47.820s (5)	4m48.210s	-8.5417	-8.0895	-7.9419	-7.4896
43	3m5.880s	4m7.610s	7m39.600s	-6.9102	-6.8297	-6.9102	-6.8297
51	3m58.720s	7m19.100s	11m51.490s	-6.7411	-6.5409	-6.2083	-6.0081
59	1m28.870s (1)	1m33.360s (1)	2m24.800s (1)	-10.0599 (1)	-9.2936 (1)	-10.0599 (1)	-9.2936 (1)
67	4m3.660s	6m46.530s	10m40.770s	-6.4128	-6.2875	-6.4128	-6.2875
75*	2m37.650s	4m17.960s	6m24.060s	-7.2624	-7.0850	-6.5743	-6.3969
83	2m18.590s	2m59.340s	4m53.490s	-8.2826	-7.7247	-8.2826 (5)	-7.7247
91	2m48.450s	3m47.710s	6m24.770s	-7.3926	-7.1513	-6.9173	-6.6760
99*	2m9.300s (5)	3m21.500s	4m13.870s (5)	-7.4399	-7.1983	-6.8557	-6.6141
107	3m49.580s	5m31.120s	9m23.690s	-6.5389	-6.1403	-6.5389	-6.1403
131	1m41.240s (3)	1m57.120s (2)	3m15.490s (3)	-9.2242 (4)	-8.5226 (4)	-9.2242 (3)	-8.5226 (3)
851	2m31.450s	2m48.390s	5m3.050s	-8.0211	-7.3517	-8.0211	-7.3517
923	2m37.200s	3m24.500s	5m42.870s	-7.4409	-6.9114	-7.2436	-6.7141

Der damit ermittelte Vorfaktor wird schließlich übernommen. Zusätzlich kann man die Größe der Simulations-Faktorbasen von der Größe der zu faktorisierenden Zahl bzw. von der Größe der später tatsächlich verwendeten Faktorbasis abhängig machen, um damit die Simulationslaufzeit an die Größe der zu faktorisierenden Zahl zu koppeln.

3 Fazit

Die vorgestellten Bestimmungsmethoden optimieren zwar den Vorfaktor, aber für die Optimierung wird die Laufzeit des Quadratischen Siebs weitgehend vernachlässigt. Möglicherweise kann also ein mit diesem Verfahren ermittelter optimaler Vorfaktor bezüglich der tatsächlichen Laufzeit des Quadratischen Siebs suboptimal sein. Für genauere Analysen benötigt man allerdings die Laufzeit verschiedener Siebalgorithmen auch in Abhängigkeit von der Qualität der Faktorbasen. Ob man hier durch theoretische Analysen zu sinnvollen Ergebnissen kommt, darf bezweifelt werden. Auch dürfte ein simulativer Ansatz diesbezüglich erfolgversprechender sein.

Für die in der Praxis häufig auftretenden Fälle dürften die hier vorstellten Verfahren brauchbare Vorfaktoren liefern, zumal sich durch Variation eines Vorfaktors leicht Laufzeitunterschiede um den Faktor zwei und mehr erreichen lassen. Laufzeitunterschiede um den Faktor zwei entsprechen andererseits Schwankungen um drei Dezimalstellen in der zu faktorisierenden Zahl, so daß auch die in seltenen Fällen auftretenden dreistelligen Vorfaktoren nicht zu substantiellen Laufzeitunterschieden führen dürften, selbst wenn kleinere Vorfaktoren bessere Laufzeitresultate aufweisen könnten.

In jedem Fall erweisen sich die vorgestellten Vorfaktorbestimmungsmethoden gegenüber Selektionsverfahren aus konstant vorgegebenen Vorfaktormengen überlegen.

Literatur

[1] Robert D. Silverman: The Multiple Polynomial Quadratic Sieve, Mathematics Of Computation, Vol. 48, January 1987, p. 329-339

[2] Riesel, Hans: "Prime Numbers and computer methods for factorization", Boston; Basel; Stuttgart: Birkhäuser, 1985