Quadratisches Sieb

Aufgabenstellung

Sei $N > 1$ eine zerlegbare positive ganze Zahl. Wir wollen ein Verfahren entwickeln, mit dem N in Primfaktoren zerlegt werden kann.

Ist N von der Form $N = p^e$ mit einer Primzahl p, so können wir dies in Laufzeit $\text{poly}(\log(N))$ (mit großer Wahrscheinlichkeit) wie folgt feststellen. Zunächst können wir durch Wurzelziehen in Laufzeit $\text{poly}(\log(M))$ den maximalen Exponenten $e \geq 1$ bestimmen, so daß $N = N_0^e$ für eine ganze Zahl $N_0 > 1$ gilt. Mit Hilfe eines Primzahltests (eines Zerlegbarkeitstests) können wir dann in Laufzeit $\text{poly}(\log(N_0))$ feststellen, ob N_0 (mit großer Wahrscheinlichkeit) eine Primzahl ist.

Zum Faktorisieren eines beliebigen zerlegbaren N genügt ein Verfahren, welches einen nicht-trivialen Faktor M von N berechnet. Denn wendet man dieses Verfahren rekursiv auf M und N/M an, so erhalten wir schließlich nicht notwendigerweise verschiedende Primzahlen p_i mit $N = \prod_{i=1}^{n} p_i$. Die Anzahl der Aufrufe dieses Verfahrens ist durch $\log_2(N)$ beschränkt, wie man induktiv leicht sieht. Unter Verwendung des Tests auf $N = p^e$ kann für ein solches Verfahren sogar angenommen werden, daß N mindestens zwei verschiedene Primfaktoren enthält.

Als Beispiel betrachten wir die Probedivision. Hier testen wir, ob N durch M mit $1 < M \leq N^{1/2}$ teilbar ist. Die Laufzeit dieses Verfahrens ist $N^{1/2}\text{poly}(\log(N)) = \exp((1/2 + o(1))\log(N))$, also exponentiell in $\log(N)$. An der Laufzeit dieses Verfahrens ändert sich aufgrund des Primzahlsatzes 12 auch nichts, wenn man sich nur auf Primzahlen M beschränkt. Das quadratische Sieb, was im folgenden besprochen wird, hat dagegen eine Laufzeit von grob gesprochen $\exp(c\log(N)^{1/2})$, also subexponentiell vom Exponenten $1/2$ in $\log(N)$. Dies stellt eine enorme Verbesserung gegenüber der Probedivision dar.

Das quadratische Sieb (genauer das multiple quadratische Sieb) ist in der Tat das asymptotisch zweiteffizienteste Verfahren zur Faktorisierung, welches gegenwärtig bekannt ist. Das asymptotisch schnellste Verfahren ist das

Zahlkörpersieb, welches eine Laufzeit von grob gesprochen $\exp(c\log(N)^{1/3})$ besitzt. Dies ist also subexponentiell vom Exponenten $1/3$ in $\log(N)$.

Idee des Verfahrens

Das quadratische Sieb berechnet nicht-triviale Faktoren von N mit Hilfe des folgenden Lemmas.

1 Lemma. *Sei N zerlegbar mit mindestens zwei verschiedenen Primfaktoren. Werden $a, b \in \mathbb{Z}$ mit $1 \leq a, b \leq N-1$, $\gcd(a,N) = \gcd(b,N) = 1$ und $a^2 \equiv b^2 \bmod N$ gewählt, so ist $\gcd(a-b,N)$ mit Wahrscheinlichkeit $\geq 1/2$ ein nicht-trivialer Faktor von N.*

Beweis. Folgt leicht unter Verwendung des chinesischen Restsatzes. $\square$

Die Aufgabe besteht daher darin, zufällige Kongruenzen $a^2 \equiv b^2 \bmod N$ zu bestimmen. Dies geschieht wie folgt. Seien $\varepsilon > 0$ und

$$\begin{aligned} f(X) &= (\lfloor N^{1/2} \rfloor + X)^2 - N, \\ I_\varepsilon &= \{x \in \mathbb{Z} \,|\, 1 \leq x \leq N^\varepsilon\}. \end{aligned}$$

Wir nennen $f(X)$ das Siebpolynom und I_ε das Siebintervall. Für $x \in I_\varepsilon$ gilt

$$f(x) = O(N^{1/2+\varepsilon}), \tag{2}$$

da sich der Hauptterm N in $(\lfloor N^{1/2} \rfloor + x)^2$ wegen Subtraktion von N weghebt. Für $x_1, \ldots, x_{r'} \in I_\varepsilon$ und mit $a_j = (\lfloor N^{1/2} \rfloor + x_j)$ erhalten wir Kongruenzen

$$a_j^2 \equiv f(x_j) \bmod N. \tag{3}$$

Ziel ist es jetzt, solche Kongruenzen geeignet zu multiplizieren, so daß neben der linken Seite auch die rechte Seite ein Quadrat wird, also die linke Seite gleich a^2 und die rechte Seite gleich b^2 für $a, b \in \mathbb{Z}$ wird. Dann gilt $a^2 \equiv b^2 \bmod N$ und wir wenden Lemma 1 an. Zum Beispiel sind $f(x_1) = 3 \cdot 7$, $f(x_2) = 5 \cdot 7$ und $f(x_3) = 3 \cdot 5$ keine Quadrate, aber ihr Produkt $f(x_1)f(x_2)f(x_3)$ ist ein Quadrat.

Um systematisch solche Produkte zu finden, wird lineare Algebra modulo 2 in den den Exponenten der Primfaktorisierungen der $f(x_j)$ betrieben. Sei $B > 0$ und

$$\begin{aligned} S &= \{p \,|\, p \text{ Primzahl mit } p \leq B\} \\ &= \{p_1, \ldots, p_s\}. \end{aligned}$$

Wir nennen S eine Faktorbasis. Mit $v_i = v_{p_i}$ gilt dann

$$f(x_j) = \prod_{i=1}^{s} p_i^{v_i(f(x_j))}, \tag{4}$$

sofern $f(x_j)$ über der Faktorbasis S vollständig zerfällt. Durch Anwendung von log auf beide Seiten von (4) kann dann $f(x_j)$ als Linearkombination der $\log(p_i)$ mit den Koeffizienten $v_i(f(x_j))$ aufgefaßt werden. Genauer gilt dann

$$\begin{aligned}\big(\log(f(x_1)), \ldots, \log(f(x_r))\big) &= \qquad\qquad (5)\\ \big(\log(p_1), \ldots, \log(p_s)\big) &\begin{pmatrix} v_1(f(x_1)) & \cdots & v_1(f(x_r)) \\ \vdots & & \vdots \\ v_s(f(x_1)) & \cdots & v_s(f(x_r)) \end{pmatrix}.\end{aligned}$$

Sei M die Matrix in $\mathbb{F}_2^{s\times r}$, die durch Reduktion der Koeffizienten der obigen Matrix $(v_i(f(x_j)))_{i,j}$ entsteht. Für $r > s$ besitzt M einen nicht-trivialen Spaltenkern $\ker(M)$. Sei $w = (w_i)_i \in \ker(M)\backslash\{0\}$. Wir fassen w im folgenden als Vektor in $\{0,1\}^s \subseteq \mathbb{Z}^r$ auf. Multiplikation von (5) mit w von rechts liefert

$$\sum_{j=1}^{r} w_j \log(f(x_j)) = \big(\log(p_1), \ldots, \log(p_s)\big) \begin{pmatrix} \sum_{j=1}^{r} w_j v_1(f(x_j)) \\ \vdots \\ \sum_{j=1}^{r} w_j v_s(f(x_j)) \end{pmatrix}. \tag{6}$$

In multiplikativer Schreibweise liefert (6) zusammen mit (3)

$$\prod_{j=1}^{r} a_j^{2w_j} \equiv \prod_{j=1}^{r} f(x_j)^{w_j} = \prod_{i=1}^{s} p_i^{\sum_{j=1}^{r} w_j v_i(f(x_j))} \bmod N. \tag{7}$$

Der Spaltenvektor auf der rechten Seite von (6) besitzt nach Wahl von w gerade Koeffizienten $\sum_{j=1}^{r} w_j v_i(f(x_j))$. Daher ist die rechte Seite der Kongruenz in (7) ein Quadrat. Wir definieren

$$a = \prod_{j=1}^{r} a_j^{w_j} \bmod N, \quad b = \prod_{i=1}^{s} p_i^{(1/2)\sum_{j=1}^{r} w_j v_i(f(x_j))} \bmod N$$

und erhalten schließlich wie gewünscht

$$a^2 \equiv b^2 \bmod N.$$

Optimierung und Verfeinerung des Verfahrens

Die beiden Hauptschritte des Verfahrens sind der Siebschritt und der Matrixschritt. Im Siebschritt werden r' Kongruenzen (3) und r Faktorisierungen (4) bestimmt, bis $r > s$ ist (zum Beispiel $r > s + 10$). Im Matrixschritt werden solange w und a, b berechnet, bis N mittels Lemma 1 zerlegt werden kann.

Siebschritt. Die Berechnung von S kann in Laufzeit $O(B\log(B))$ erfolgen (Übungsaufgabe, es ist sogar $O(B/\log(\log(B)))$ möglich).

Die Faktorisierung der r' Werte $f(x_j)$ über S mittels Division durch jeweils alle p_i erfordert eine Laufzeit von $(r's)\mathrm{poly}(\log(N))$. Dies kann durch die Verwendung eines Siebs erheblich verbessert, woher auch der Name des gesamten Verfahrens rührt. Dies wird im folgenden beschrieben.

Das Problem bei der Probedivision ist, daß $f(x_j)$ zwar auf der einen Seite potentiell durch jedes $p \in S$ teilbar sein kann, aber die Anzahl der verschiedenen Primfaktoren von $f(x_j)$ wesentlich geringer als die Kardinalität von S ist. Damit geht die überwiegende Mehrheit der Divisionen durch $p \in S$ nicht auf und ist somit „verschwendete Zeit“. Die Idee des Siebens ist, vorherzusehen, welche $f(x_j)$ durch ein $p \in S$ teilbar sind. Hierzu berechnen wir für jedes $p \in S$ Nullstellen $x_{1,p}$ und $x_{2,p}$ von $f(X) \equiv 0 \bmod p$ in $\{1,\ldots,p\}$. Da $f(X)$ quadratisch ist, gibt es höchstens zwei Nullstellen. Für $x \in I_\varepsilon$ gilt dann $f(x) \equiv 0 \bmod p$ genau dann, wenn $x = x_{1,p} + \lambda p$ oder $x = x_{2,p} + \mu p$ für $\lambda, \mu \in \mathbb{Z}^{\geq 1}$ ist. Gibt es keine Nullstellen $x_{1,p}, x_{2,p}$, so ist auch kein $f(x) \equiv 0 \bmod p$.

Das Sieben wird dann folgendermaßen durchgeführt. Wir wählen $x_j = j$ und erstellen eine Liste $f(x_1), f(x_2), \ldots, f(x_{r'})$. Für jedes $p \in S$ betrachten wir nur x_j von der Form $x_j = x_{1,p} + \lambda p$ oder $x_j = x_{2,p} + \mu p$ mit $\lambda, \mu \in \mathbb{Z}^{\geq 1}$. Für diese x_j ersetzen wir $f(x_j)$ durch $f(x_j)/p^{v_p(f(x_j))}$. Sind alle p abgearbeitet, so sind genau die $f(x_j)$ über der Faktorbasis zerlegbar, für welche der entsprechende Eintrag in der Liste gleich 1 ist.

Die Berechnung der $x_{1,p}, x_{2,p}$ kann mit Verfahren zur Faktorisierung von Polynomen über endlichen Körpern erfolgen. Die Laufzeit hierfür für ein p ist $\mathrm{poly}(\log(p))$, also insgesamt für alle p höchstens $s\mathrm{poly}(\log(N))$. Die Laufzeit für das Sieben ist dann $\sum_{p\in S}(r'/p)\mathrm{poly}(\log(N))$. Wegen $\sum_{p\in S}(1/p) \leq \sum_{x\leq B} 1/x = O(\log(B))$ (Summe als Treppenfunktion schreiben, mit $1/x$-Funktion nach oben abgrenzen und integrieren) und $B \leq N$ ergibt sich $r'\mathrm{poly}(\log(N))$ für das Sieben. Wegen $r' \geq s$ ergibt sich als Gesamtlaufzeit für den Siebschritt

$$r'\mathrm{poly}(\log(N)). \tag{8}$$

Matrixschritt Mit dem Gaußalgorithmus kann w in Laufzeit $O(s^2r)$ berechnet werden. Dies läßt sich mit dem Verfahren von Wiedemann erheblich beschleunigen. Dieses Verfahren berechnet gleichverteilt zufällige Elemente w des Kerns in einer erwarteten Laufzeit $O(sr)$ mit Wahrscheinlichkeit $> 1/2$. Die Berechnung von a, b, $\gcd(a,N)$, $\gcd(b,N)$ und $\gcd(a-b,N)$ erfordert dann eine Laufzeit $r\mathrm{poly}(\log(N))$. Zusammen erhalten wir für den Matrixschritt

$$O(sr + r\mathrm{poly}(\log(N))). \tag{9}$$

Wahl der Parameter und Komplexität

Wir werden B deutlich kleiner als $N^{1/2}$ wählen, da sonst allein die Berechnung von S exponentiell in $\log(N)$ wäre. Dann stellt sich allerdings die Frage nach dem Verhältnis von r' und r, da nicht jedes $f(x_j)$ über S faktorisiert. Wir benötigen daher eine Aussage, wieviele $f(x_j)$ über S faktorisieren.

10 Definition. Seien $x, y, z \geq 1$ ganze Zahlen. Dann heißt z y-glatt, wenn alle Primfaktoren von z kleiner gleich y sind. Wir definieren

$$\psi(x, y) = \#\{z \mid z \leq x \text{ und } z \text{ ist } y\text{-glatt.}\}.$$

11 Satz. *Sei $\delta > 0$, $x \geq y > 1$ und $u = \log(x)/\log(y)$. Für $\log(x)^\delta \leq y \leq \log(x)^{1-\delta}$ gilt*

$$\psi(x, y) = x \cdot u^{-u(1+f(x,y))}$$

mit $f(x, y) \to 0$ gleichmäßig in y für $x \to \infty$.

Wir wenden Satz 11 im Hinblick auf (2) für $x = O(N^{1/2+\varepsilon})$ und $y = B$ an. Unter der heuristischen Annahme, daß sich $f(x)$ für $x \in I_\varepsilon$ wie eine zufällig gewählte Zahl $\leq O(N^{1/2+\varepsilon})$ verhält, ist $f(x)$ nach Satz 11 mit Wahrscheinlichkeit $u^{-u(1+o(1))}$ B-glatt, läßt sich also über S faktorisieren. Wir gehen also davon aus, daß $r = r'u^{-u(1+o(1))}$ gilt.

Da wir nun noch r geringfügig größer als s wählen wollen, benötigen wir zur Bestimmung von r' noch den Wert von s.

12 Satz. *Für die Anzahl $\pi(x)$ der Primzahlen $\leq x$ gilt*

$$\pi(x) \sim x/\log(x).$$

Wir wenden Satz 12 mit $x = B$ an und erhalten also $s = B/\log(B)$. Zur Vereinheitlichung der Notation definieren wir $n = \log(N)$ und $b = \log(B)$. Da wir die Voraussetzungen von Satz 11 für ein $\delta > 0$ einhalten wollen, gilt $b \to \infty$ und $u \to \infty$ für $n \to \infty$. Außerdem nehmen wir an, daß $\varepsilon = o(1)$ ist. Es gilt $u = (1/2 + \varepsilon)(n/b)$. Weiter erhalten wir

$$\begin{aligned}
s &= \exp\bigl((1 + o(1))b\bigr), \\
r &= \exp\bigl((1 + o(1))b\bigr), \\
u^{-u(1+o(1))} &= \exp\bigl((1/2 + o(1))(n/b)\log(n/b)\bigr), \\
r' &= \exp\bigl((1 + o(1))b + (1/2 + o(1))(n/b)\log(n/b)\bigr).
\end{aligned}$$

Aus (8) und (9) ergibt sich für die Komplexität von Siebschritt und Matrixschritt, also für das gesamte Verfahren,

$$\begin{aligned} &r'\mathrm{poly}(\log(N)) + O(sr + r\mathrm{poly}(\log(N))) = \\ &\qquad \exp\big((1+o(1))b + (1/2+o(1))(n/b)\log(n/b)\big) + \exp\big((1+o(1))(2b)\big), \end{aligned} \tag{13}$$

da poly(log(N)) in die $o(1)$-Terme der Exponenten aufgenommen werden kann. Um (13) asymptotisch für $n \to \infty$ zu minimieren, müssen wir b so wählen, daß

$$b + n/(2b)\log(n/b) = 2b \tag{14}$$

gilt. Eine kurze Rechung zeigt, daß dies für

$$b = (1/2)(n\log(n))^{1/2} \tag{15}$$

der Fall ist. Dieser Wert minimiert auch die Laufzeit des Siebschritts unabhängig vom Matrixschritt. Als Gesamtlaufzeit ergibt sich damit durch Einsetzen von (15) in (13)

$$\exp\big((1+o(1))(n\log(n))^{1/2}\big). \tag{16}$$

Wir sehen jetzt auch, daß wir ε zum Beispiel mit $(1/n)^{1/3} \leq \varepsilon \leq 1/\log(n)$ wählen können. Denn dann gilt $\#I_\varepsilon \geq r'$, was für den Siebschritt als Nebenbedingung erforderlich ist.

Die komplexitätstheoretische Funktion $L_N(c,d)$ ist definiert als

$$L_N(c,d) = \exp\big((d+o(1))(\log(N)^c \log(\log(N))^{1-c}\big).$$

Wir erhalten zusammenfassend:

17 Satz. *Mit dem quadratischen Sieb kann eine ganze Zahl N in heuristischer Laufzeit*

$$L_N(1/2,1)$$

faktorisiert werden.

Das Ergebnis ist insbesondere deswegen heuristisch, da die Aussage über die Glattheitswahrscheinlichkeit $u^{-u(1+o(1))}$ der $f(x_j)$ nur heuristischer Natur ist.