Faktorisierungsalgorithmen

Handout zum Vortrag im Seminar „Elementare Zahlentheorie und Algebra“
von Dr. Stephan Ehlen

Referent: Julian Sander 04. Juni 2019

Was ist ein Faktorisierungsalgorithmus?

Sei $n \in \mathbb{N}$ zusammengesetzt. Ziel ist es, die Zahl n in ihre Primfaktoren zu zerlegen. Dazu reicht es aus, Algorithmen zu finden, die n nicht-trivial in ein Produkt zweier natürlicher Zahlen zerfallen lassen. Die rekursive Anwendung eines solchen Algorithmus auf die Faktoren liefert die vollständige Primfaktorzerlegung von n.

Probedivision

Der einfachste Algorithmus ist die Probedivision. Hier teilt man alle Zahlen $x \leq \lfloor \sqrt{n} \rfloor$ durch n, bis man einen Teiler findet.

Das Lemma von Fermat

Sei n eine natürliche Zahl.

1. Ist n ungerade und zusammengesetzt, dann ist n die Differenz zweier Quadrate, d.h. $n = x^2 - y^2$ mit $x, y \in \mathbb{Z}$, wobei $x \not\equiv \pm y \mod n$ gilt.
2. Sei $x^2 - y^2 = cn$ mit $x, y, c \in \mathbb{Z}$ und $x \not\equiv \pm y \mod n$, dann sind $a := \mathrm{ggT}(x - y, n)$ und $b := \mathrm{ggT}(x + y, n)$ echte Teiler von n.

Einfacher Fermat-Algorithmus

Sei $n \in \mathbb{N}$ ungerade. Man kann n wie folgt faktorisieren:

1. Berechne $x := \lceil \sqrt{n} \rceil$ und $z := x^2 - n$.
2. Falls $z = y^2$ ein Quadrat ist, bestimme $ggT(x \pm y, n)$ und finde so Teiler von n. Sind echte Teiler dabei, ist man fertig.
3. Andernfalls erhöhe x um eins, $x \to x+1$, und setze $z \to z+2x+1$, sodass weiter $z = x^2 - n$ gilt. Fahre mit 2. fort.

Definition: Faktorbasis

Die Faktorbasis B zu $b \in \mathbb{N}$ ist definiert als

$$B = \{-1\} \cup \{p \in \mathbb{P} \mid p \leq b\}.$$

Eine Zahl $n \in \mathbb{Z}$ heißt *B-glatt*, falls sie ein Produkt von Elementen aud B ist. Sie heißt *b-glatt*, falls sie B-glatt ist, wobei B die Faktorbasis zu b ist.

Im Folgenden sei n immer ungerade.

Fermat-Algorithmus

1. Für alle i aus einem Intervall $I = [0, c]$ berechne $x_i = \lceil \sqrt{n} \rceil + i$ und $z_i = x_i^2 - n$.
2. Wähle ein passendes $b \in \mathbb{N}$ und bilde die Faktorbasis B zu b. Falls kein $p \in B$ ein Teiler von n ist, braucht man nur diese p aufzunehmen, für die $\left(\frac{n}{p}\right) = 1$ gilt.
3. Faktorisiere die z_i per Probedivision durch die Elemente aus B und streiche die z_i (und die zugehörigen x_i), die nicht b-glatt sind.
4. Suche eine Teilmenge J der verbliebenen i, sodass $\prod_{i \in J} z_i = y^2$ ein Quadrat ist. Ist $x = \prod_{i \in J} x_i$, gilt $x^2 \equiv y^2 \mod n$ und falls $x \not\equiv \pm y \mod n$, findet man echte Teiler von n mit dem Lemma von Fermat. Findet man kein Quadrat/keine echten Teiler, produziere weitere x_i und z_i, wende 3. auf sie an und wiederhole 4.

Kettenbruchalgorithmus von Brillhart-Morrison

Seien $\frac{p_i}{q_i}$ die Näherungsbrüche in der Kettenbruchentwicklung von $\sqrt{n}$. Dann setze $x_i = p_i$ und $z_i = p_i^2 - nq_i^2$. Führe nun mit diesen x_i und z_i den Fermat-Algorithmus durch.
Ist die Periode der Kettenbruchentwicklung von $\sqrt{n}$ zu klein, um ein passendes Quadrat zu erhalten, kann man zusätzlich Näherungsbrüche der Kettenbruchentwicklung von $\sqrt{kn}$ mit $k \in \mathbb{N}$ betrachten (dann muss man aber die komplette Faktorbasis benutzen).

Das quadratische Sieb

Man kann den dritten Schritt des Fermat-Algorithmus wie folgt verbessern: Damit eine Primzahl(-potenz) ein z_i teilen kann, muss das zugehörige x_i kongruent zu einer quadratischen Wurzel modulo dieser Primzahl(-potenz) sein. Berechne dementsprechend alle Quadratwurzeln x_{p_r} modulo p^r mit $p \in B$ und $p^r < z_c$. Finde dann das kleinste x_i mit $x_i \equiv x_{p_r} \mod p^r$. Für dieses x_i und alle $x_i + kp^r$ mit $k \in \mathbb{N}$ sind dann die zugehörigen z_i durch p^r teilbar.

Shor-Algorithmus

Der Algorithmus von Shor ist der modernste Faktorisierungsalgorithmus, der auf dem Lemma von Fermat beruht. Hier wählt man fest $y = 1$, man sucht also $x \in \mathbb{Z}$ mit $x^2 \equiv 1 \mod n$. Dazu berechnet man die Ordnung d eines zufälligen Elementes $a \in U_n$. Ist diese gerade, setzt man $x := a^{d/2}$ und erhält so $x^2 \equiv 1 \mod n$. Die Ordnung von a zu berechnen, ist auf „normalen“ Computern sehr aufwendig, lässt sich aber auf Quantencomputern in polynomialer Zeit durchführen.