# Das Zahlkörpersieb

Felix Göbler

24.10.2019

## Zusammenfassung

Der Fundamentalsatz der Arithmetik besagt, dass sich jede natürliche Zahl $n$ eindeutig (bis auf Reihenfolge) in ein Produkt von Primzahlen zerlegen lässt. Diese Tatsache war auch schon Euklid bekannt. Wie man diese Zerlegung aber genau ausrechnen kann, beschäftigt die Mathematik erst seit Ende des 20. Jahrhunderts in zunehmendem Maße. Schuld daran trägt vor allem die moderne Public-Key-Kryptographie, insbesondere auf RSA basierende Verschlüsselungs- und Signaturverfahren.

Tatsächlich hat sich herausgestellt, dass dies ein sogenanntes *hartes* Problem ist (d.h. nicht in polynomieller Laufzeit berechenbar). So war es noch 1970 quasi unmöglich eine beliebige Zahl mit 20 Ziffern zu faktorisieren. Im Jahr 1977 schätzte Ron Rivest, einer der Erfinder von RSA, dass die Faktorisierung einer Zahl mit 125 Ziffern 40 Billiarden Jahre in Anspruch nehmen würde. Bereits 1994 wurde allerdings mit einer Variante des 1981 von Carl Pomerance entwickelten *Quadratischen Siebs* (kurz QS) die 129-stellige Dezimalzahl RSA-129 innerhalb von 8 Monaten faktorisiert. Darüber hinaus entwickelte John Pollard 1988 eine spezielle Version des *Zahlkörpersiebs*, welches mit Hilfe von Joe Buhler, Hendrik Lenstra und Carl Pomerance verallgemeinert wurde (englisch *general number field sieve*, kurz GNFS), sodass schließlich 1996 eine 130-stellige Dezimalzahl faktorisiert werden konnte.

Das Zahlkörpersieb war und ist immer noch der (asymptotisch) schnellste Algorithmus, um große Zahlen (mit mehr als 130 Ziffern) zu faktorisieren. Das Zahlkörpersieb faktorisiert $n$ in subexponentieller Laufzeit

$$T_{GNFS}(n) = \exp\Big(\big((\frac{64}{9})^{\frac{1}{3}} + o(1)\big)(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}\Big),$$

wobei einige heuristische, aber plausible Annahmen in der Abschätzung getroffen wurden. Das Quadratische Sieb hingegen, welches für Zahlen mit weniger als 100 Ziffern geeignet ist, hat eine (ebenfalls heuristisch geschätzte) subexponentielle Laufzeit von

$$T_{QS}(n) = \exp\big((1 + o(1))(\ln n)^{\frac{1}{2}}(\ln\ln n)^{\frac{1}{2}}\big).$$

Beide Algorithmen berechnen Kongruenzen von Quadraten mod $n$

$$a^2 \equiv b^2 \mod n,$$

aus denen jeweils mit einer Wahrscheinlichkeit von ungefähr $\frac{1}{2}$ nicht triviale Teiler von $n$ resultieren. Ist nämlich $a \not\equiv \pm b \mod n$, so sind $\mathrm{ggT}(n, a \pm b)$ echte Teiler von $n$. Das Zahlkörpersieb geht dabei wie folgt vor.

## Polynomwahl

Zuerst wird ein Polynompaar $(f, g)$ mit ganzzahligen Koeffizienten und einer gemeinsamen Nullstelle $m$ mod $n$ bestimmt. Dies kann konstruiert werden, in dem zum Beispiel $m := \lfloor \sqrt[d]{n} \rfloor$ gesetzt wird für $\deg(f) = d$ und anschließend $n$ als formale Summe über $m$ dargestellt wird: $n = \sum_{i=0}^{d} c_i m^i$, wobei $c_i \in \{0, 1, \ldots, m-1\}$ und $c_d = 1$. Dann erfüllen

$$f = \sum_{i=0}^{d} c_i X^i \quad \text{und} \quad g = X - m$$

die Bedingungen. Es wird davon ausgegangen, dass $f$ irreduzibel ist (da ansonsten die Zerlegung von $f$ eine Zerlegung von $n$ liefert). Sei $\alpha$ eine Nullstelle von $f$ in $\mathbb{C}$. Dann existiert ein surjektiver Ringhomomorphismus

$$\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z} \text{ mit } \phi(1) = 1 \mod n \text{ und } \phi(\alpha) = m \mod n.$$

## Sieben und Glattheit

Wähle eine positive Schranke $B_1$ und setze $F_{B_1}$ als die Menge der Primzahlen, die kleinergleich $B_1$ sind. $F_{B_1}$ heißt **rationale Faktorbasis**. Bezeichne ein Tupel $(a, b) \in \mathbb{Z}^2$ als $B_1$-**glatt**, falls alle Primteiler von $a - bm$ in der rationalen Faktorbasis liegen.

Wähle eine positive Schranke $B_2$ und setze $F_{B_2}$ als die Menge der Primideale von $\mathbb{Z}[\alpha]$, die Ordnung eins haben und deren Norm durch $B_2$ beschränkt ist. Diese Menge heißt **algebraische Faktorbasis**. Jedes dieser Primideale korrespondiert bijektiv zu einem Paar $(p, r \mod p)$, wobei $p$ eine Primzahl ist und $f(r) \equiv 0 \mod p$ gilt. Schließlich kann die Norm von $a - b\alpha \in \mathbb{Z}[\alpha]$ durch $f$ ausgedrückt werden: $N(a - b\alpha) = b^d f(\frac{a}{b})$. Die Primteiler $p$ von $b^d f(\frac{a}{b})$ entsprechen nun genau den Primidealen erster Ordnung mit Norm $p$. Daher wird ein Tupel $(a, b) \in \mathbb{Z}^2$ als $B_2$-**glatt** bezeichnet, wenn jeder Primteiler von $N(a - b\alpha)$ zu einem Primideal innerhalb der algebraischen Faktorbasis korrespondiert.

Wähle für einen positiven Parameter $u$ die Menge $U = \{(a, b) \in \mathbb{Z}^2 \mid |a| \leq u,\ 0 < b \leq u,\ \mathrm{ggT}(a, b) = 1\}$. Dann wird nach all den Paaren $(a, b) \in U$ gesucht, die sowohl über der rationalen als auch über der algebraischen Faktorbasis glatt sind.

## Lineare Abhängigkeiten finden

Als nächstes wird versucht, ein Produkt der zuvor gefundenen glatten Paare $(a, b)$ zu bilden, sodass jeder Primteiler (bzw. jedes Primideal) mit einer geraden Anzahl vorkommt. Dafür werden die Exponenten der Primfaktorzerlegung von $(a - bm)$ und $N(a - b\alpha)$ jeweils in einen gemeinsamen Vektor geschrieben und jeder Eintrag $\mod 2$ gerechnet. Dann wird eine nicht triviale Linearkombination dieser Vektoren über dem endlichen Körper $\mathbb{F}_2 \coloneqq \mathbb{Z}/2\mathbb{Z}$ berechnet. Am effizientesten kann dies mit dem Lanczos- oder mit dem Block-Wiedemann-Algorithmus erledigt werden. Schließlich wird eine Teilmenge $S \subset U$ gefunden, sodass

$$\prod_{(a,b)\in S} (a + bm) = z^2 \text{ und } \prod_{(a,b)\in S} (a + b\alpha) = y$$

gilt.

## Wurzeln ziehen

In obiger Gleichung ist $z^2$ sicher ein Quadrat in $\mathbb{Z}$, wohingegen $y$ nur sehr wahrscheinlich ein Quadrat in $\mathbb{Z}[\alpha]$ ist. Dieses Probleme wird mit quadratischen Charakteren gelöst. Es existiere also $\gamma \in \mathbb{Z}[\alpha]$ mit $\gamma^2 = y$. Während $z$ direkt mit Hilfe der Primfaktorzerlegung von $z^2$ berechnet werden kann, wird $\gamma$ meist mit dem Algorithmus von Montgomery bestimmt.

## Finale Berechnung

Eine Kongruenz von Quadraten folgt nach Anwendung des Homomorphismus

$$\varphi : \mathbb{Z} \times \mathbb{Z}[\alpha] \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\ (x, y) \mapsto (x \mod n, \phi(y))$$

auf $(z, \gamma)$. Nach Konstruktion von $\phi$ folgt nämlich $z^2 \equiv \phi(\gamma)^2$. Gilt $z \not\equiv \pm\phi(\gamma) \mod n$, so erhält man schließlich zwei echte Teiler $\mathrm{ggT}(n, z \pm \phi(\gamma))$.