§ 12. Einfache Faktorisierungs-Methoden

12.1. Die Fermatsche Faktorisierungs-Methode. Sei N eine ungerade, zusammengesetzte natürliche Zahl. Um N zu faktorisieren, ist die Idee von Fermat, N als Differerenz zweier Quadratzahlen darzustellen, $N = n^2 - m^2$. Dann hat man die Faktorzerlegung $N = (n+m)(n-m)$. Dass dies in der Tat möglich ist, sagt der folgende

Satz. *Jede ungerade, zusammengesetzte ganze Zahl $N \geqslant 9$ lässt sich als Differenz zweier Quadratzahlen*

$$N = n^2 - m^2 \qquad mit \;\; 0 \leqslant m < n, \; \sqrt{N} \leqslant n < N/6 + 2,$$

schreiben.

Beweis. Sei $N = ab$ mit $a \geqslant b > 1$. Da N ungerade, sind a und b ungerade, also

$$n := \frac{a+b}{2}, \quad \text{und} \quad m := \frac{a-b}{2}$$

ganze Zahlen und es gilt

$$n^2 - m^2 = \Big(\frac{a+b}{2}\Big)^2 - \Big(\frac{a-b}{2}\Big)^2 = ab = N, \qquad \text{q.e.d.}$$

Der Fermatsche Faktorisierungs-Algorithmus arbeitet nun wie folgt: Sei

$$x_0 := \Big\lceil \sqrt{N} \Big\rceil$$

die kleinste ganze Zahl $\geqslant \sqrt{N}$. Für $k = 0, 1, 2, \ldots$ berechnet man die Differenzen

$$d_k := x_k^2 - N, \quad \text{wobei } x_k := x_0 + k,$$

bis man auf eine Quadratzahl $d_k = m^2$ stößt. Dann ist $N = (x_k + m)(x_k - m)$. Bei der sukzessiven Berechnung der d_k kann man noch folgende Eigenschaft benutzen:

$$d_{k+1} - d_k = x_{k+1}^2 - x_k^2 = (x_k + 1)^2 - x_k^2 = 2x_k + 1.$$

Beispiel. Es sei $N = 10033$ zu faktorisieren. Hier ist

$$x_0 := \Big\lceil \sqrt{N} \Big\rceil = 101,$$

$$\begin{aligned} d_0 = x_0^2 - N = 10201 - 10033 &= 168 \\ 2x_0 + 1 &= 203 \\ \hline d_1 = d_0 + (2x_0 + 1) &= 371 \\ 2x_1 + 1 &= 205 \\ \hline d_2 = d_1 + (2x_1 + 1) &= 576 = 24^2 = m^2, \end{aligned}$$

also $N = (x_2 + m)(x_2 - m) = (103 + 24)(103 - 24) = 127 \cdot 79$.

Für größere Zahlen eignet sich die Fermatsche Faktorisierungs-Methode nur dann, wenn $N = a \cdot b$ mit fast gleich großen Faktoren a, b, und zwar sollte $|a - b|$ nur ein kleines Vielfaches von $N^{1/4}$ sein (siehe Übung).

Die Grundidee der Fermatschen Faktorisierungs-Methode und weiterer, daraus entwickelten Methoden, kann man so formulieren: Man sucht ganze Zahlen n, m mit

$$n^2 \equiv m^2 \bmod N, \quad n \not\equiv \pm m \bmod N.$$

Dann ist $(n + m)(n - m) \equiv 0 \bmod N$ und $\gcd(n + m, N)$ ein nicht-trivialer Teiler von N. Einer der effizientesten heute verwendeten Faktorisierungs-Algorithmen ist das sog. Quadratische Sieb, welches mit Siebmethoden arbeitet, um solche n und m zu finden. Wir werden das Quadratische Sieb in dieser Vorlesung nicht behandeln.

12.2. Das (p − 1)-Faktorisierungs-Verfahren. Sei N eine zusammengesetzte natürliche Zahl, die in Faktoren zerlegt werden soll. Das sog. $(p - 1)$-Verfahren von Pollard funktioniert dann gut, wenn es einen Primteiler $p \mid N$ gibt, so dass $p - 1$ ein Produkt von relativ kleinen Primfaktoren ist. Sei etwa

$$p - 1 = q_1^{k_1} \cdot \ldots \cdot q_r^{k_r}$$

die Primfaktor-Zerlegung von $p - 1$ und es gelte

$$q_i^{k_i} \leqslant B \quad \text{für alle } i = 1, \ldots, r$$

mit einer gewissen Schranke B. Wir kennen natürlich weder die Primfaktor-Zerlegung noch die Schranke B, machen aber gewisse Annahmen über B (z.B. $B = 128s$ mit $s = 1, 2, \ldots$). Da wir die $q_i^{k_i}$ nicht kennen, bilden wir das Produkt

$$Q(B) := \prod_{q \leqslant B} q^{\alpha(q,B)},$$

wobei das Produkt über alle Primzahlen $q \leqslant B$ gebildet wird und $\alpha(q, B)$ die größte ganze Zahl α mit $q^\alpha \leqslant B$ bezeichnet. (Mit dem Primzahlsatz kann man zeigen, dass $Q(B)$ etwa die Größenordnung e^B hat.) Unter unserer Annahme gilt dann

$$p - 1 \mid Q(B),$$

also gilt für jede ganze Zahl a mit $\gcd(a, N) = 1$, dass

$$a^{Q(B)} \equiv 1 \bmod p, \quad \text{d.h.} \quad p \mid a^{Q(B)} - 1.$$

Im Allgemeinen wird $a^{Q(B)} \not\equiv 1 \bmod N$ sein. Dann ist

$$d := \gcd(a^{Q(B)} - 1, N)$$

ein nicht-trivialer Teiler von N. Auch wenn unsere Annahmen falsch sind, ist d ein Teiler von N, es kann jedoch ein trivialer Teiler, d.h. $d = 1$ oder $d = N$ sein.

In der Praxis wählt man eine gewisse Folge

$$B_1 < B_2 < B_3 < \ldots < B_t$$

von Schranken und berechnet der Reihe nach

$$d_s := \gcd(a^{Q(B_s)} - 1, N), \quad s = 1, 2, \ldots$$

bis man auf einen nicht-trivialen Teiler von N trifft, oder das Verfahren als erfolglos abgebrochen werden muss. Dabei braucht man natürlich die Potenz $a^{Q(B_s)}$ nur modulo N berechnen. Außerdem kann man für die Berechnung von $a^{Q(B_{s+1})}$ das vorherige Ergebnis benutzen, da für $B < B'$ gilt

$$Q(B') = Q(B)Q(B, B') \quad \text{mit} \quad Q(B, B') = \prod_{B < q \leq B'} q^{\alpha(q,B') - \alpha(q,B)},$$

also

$$a^{Q(B_{s+1})} = (a^{Q(B_s)})^{Q(B_s, B_{s+1})}.$$

Wie schon gesagt, funktioniert die $(p-1)$-Faktorisierungs-Methode nur unter besonderen Umständen. Eine Weiterentwicklung davon ist die Faktorisierung mit Elliptischen Kurven, die einen größeren Anwendungsbereich hat.