Korrektheit Faktorbasen-Faktorisierung

Korrektheit: Es gilt

$$x^2 \equiv \prod_{i=1}^{s+1}(x_i^2)^{f_i} \equiv \prod_{i=1}^{s+1} z_i^{f_i} = \prod_{i=1}^{s+1}\prod_{j=1}^{s} p_j^{f_i e_{i,j}}$$
$$= \prod_{j=1}^{s} p_j^{\sum_{i=1}^{s+1} f_i e_{i,j}} \equiv y^2 \bmod n.$$

Wahl der Faktorbasis:

- Wahl eines kleinen b führt zu kleiner Anzahl Iterationen von Schritt 3, allerdings auch zu einer kleinen Ws b-glatter z_i in Schritt 3.1.
- Analyse der Dichte von b-glatten Zahlen führt zur optimalen Wahl
$$b = \exp \tfrac{1}{2}\sqrt{\ln n \ln\ln n}.$$
- Wir integrieren bei der Fermat-Faktorisierung mit $z_i = x_i^2 - n$ nur solche $p \in B$ in der Faktorbasis, bei denen $(\frac{n}{p}) = 1$ gilt.
- Sei p ein Teiler von z_i. Wegen $z_i = x_i^2 - n$ folgt $x_i^2 \equiv n \bmod p$.
- D.h. n muss ein quadratischer Rest modulo p sein.

Ziel: Wähle x_i so, dass $z_i \equiv x_i^2 \bmod n$ mit großer Ws b-glatt ist. Für
$$x_i = \lceil\sqrt{n}\rceil + i \text{ gilt } z_i \approx 2i\sqrt{n}.$$

Kettenbruch Faktorisierung von Morrison-Brillhart

Idee der Kettenbruch Faktorisierung:

- Berechne den Kettenbruch von $\sqrt{n}$ mit Näherungsbrüchen $\frac{p_i}{q_i}$.
- Wähle $z_i := p_i^2 - nq_i^2$. Insbesondere gilt dann $z_i \equiv p_i^2 =: x_i^2 \bmod n$.

Lemma

Sei $n \in \mathbb{N}$ kein Quadrat und $\frac{p_i}{q_i}$ Näherungsbruch von $\sqrt{n}$. Dann gilt

$$|p_i^2 - nq_i^2| < 2\sqrt{n}.$$

Beweis: Für Näherungsbrüche gilt $|\sqrt{n} - \frac{p_i}{q_i}| \leq \frac{1}{q_i q_{i+1}}$. Es folgt

$$\begin{aligned} |p_i^2 - nq_i^2| &= q_i^2 |n - (\tfrac{p_i}{q_i})^2| = q_i^2 |\sqrt{n} - \tfrac{p_i}{q_i}| \cdot |2\sqrt{n} + \tfrac{p_i}{q_i} - \sqrt{n}| \\ &\leq \tfrac{q_i}{q_{i+1}} (2\sqrt{n} + \tfrac{1}{q_i q_{i+1}}) \end{aligned}$$

- Die Behauptung folgt mittels $q_{i+1} \geq q_i + 1$ aus

$$\begin{aligned} |p_i^2 - nq_i^2| - 2\sqrt{n} &\leq 2\sqrt{n} \left(\tfrac{q_i}{q_{i+1}} + \tfrac{1}{2\sqrt{n} q_{i+1}^2} - 1 \right) \\ &< 2\sqrt{n} \left(\tfrac{q_i}{q_{i+1}} + \tfrac{1}{q_{i+1}} - 1 \right) \leq 0. \end{aligned}$$

Wahl der Faktorbasis bei Morrison-Brillhart

Faktorbasis bei Morrison-Brillhart:

- Wir wählen wiederum nur solche $p \in B$ mit $(\frac{n}{p}) = 1$.
- Sei p ein Primteiler von $z_i = p_i^2 - nq_i^2$.
- Annahme: $q_i \notin U_p$, d.h. $p|q_i$.
- Aus $p|z_i$ und $p|q_i$ folgt $p|z_i + nq_i^2$.
- Damit gilt $p|p_i$ und $\mathrm{ggT}(p_i, q_i) \geq p$. (Widerspruch: $\mathrm{ggT}(p_i, q_i) = 1$)
- Aus $z_i = p_i^2 - nq_i^2$ folgt daher $(\frac{p_i}{q_i})^2 \equiv n \bmod p$.
- Damit ist n ein quadratischer Rest modulo p.

Bsp. Morrison-Brillhart Faktorisierung

Bsp: Wir faktorisieren $n = 133 = 7 \cdot 19$.

- Wir wählen $b = 5$ als Glattheitsschranke. Es gilt
$$(\tfrac{133}{2}) = (\tfrac{1}{2}) = 1, (\tfrac{133}{3}) = (\tfrac{1}{3}) = 1 \text{ und } (\tfrac{133}{5}) = (\tfrac{3}{5}) = (-1).$$
- D.h. wir wählen die Faktorbasis $B = \{-1, 2, 3\}$.
- Der Kettenbruchalgorithmus liefert
$$\sqrt{133} = [11, 1, 1, 7, 5, 1, 1, 1, 2, 1, 1].$$
- Die ersten Näherungsbrüche sind damit $11, 12, \frac{23}{2}, \frac{173}{15}, \frac{888}{77}, \frac{1061}{92}$.
- Unser Algorithmus FAKTORBASIS liefert uns folgende Relationen.

$x_i \equiv p_i \bmod n$	$z_i = p_i^2 - nq_i^2$	e_i	$e_i \bmod 2$
11	$-12 = (-1) \cdot 2^2 \cdot 3$	$(1, 2, 1)$	$(1, 0, 1)$
12	11		
23	$-3 = (-1) \cdot 3$	$(1, 0, 1)$	$(1, 0, 1)$
40	$4 = 2^2$	$(0, 2, 0)$	$(0, 0, 0)$
90	-13		
130	$9 = 3^2$	$(0, 0, 2)$	$(0, 0, 0)$

Bsp. Morrison-Brillhart Faktorisierung

- Die letzte Relation liefert
$$130^2 \equiv 3^2 \bmod 133.$$
- Allerdings gilt $130 \equiv -3 \bmod 133$. D.h. die Relation ist nutzlos.
- Die ersten beiden Relationen sind linear abhängig und liefern
$$(11 \cdot 23)^2 \equiv 120^2 \equiv ((-1)^1 2^1 3^1)^2 = (-6)^2 \bmod 133.$$
- Es gilt $120 \not\equiv \pm 6 \bmod 133$ und damit
$$\mathrm{ggT}(120 \pm 6, 133) = \mathrm{ggT}(-13 \pm 6, 133) = \{7, 19\}.$$
- Ebenso erhält man die Faktorisierung aus der 3. Relation
$$40^2 \equiv 2^2 \bmod 133.$$

Anmerkung:

- Oft liefern die Näherungsbrüche nicht genügend viele Relationen.
- Hier betrachtet man zusätzlich die Kettenbrüche von
$$\sqrt{kn} \text{ für kleine } k \in \mathbb{N}.$$
- *Vorsicht:* In diesem Fall kann man nur Primzahlen p mit $(\frac{kn}{p}) = (-1)$ für alle k in der Fakorbasis ausschließen.

Quadratisches Sieb

Idee: Statt Teilbarkeit für die z_i sukzessive zu testen, berechne für viele z_i gleichzeitig die Teilbarkeit durch $p_i^{e_i}$ mit $p_i \in B$.

Prinzip des Siebens:

- Im Fermat Algorithmus ist $z_i := x_i^2 - n$ durch p teilbar gdw
$$x^2 \equiv n \bmod p.$$
- D.h. wir berechnen die Lösungen $\pm x_p$ dieser Kongruenz.
- Diese Lösungen existieren, da $(\frac{n}{p}) = 1$ für alle $p \in B$.
- Damit sind genau diejenigen z_i mit $x_i \equiv \pm x_p \bmod p$ durch p teilbar.
- Diese z_i werden durch p dividiert.
- Analog verfährt man für die Primpotenzen. D.h. wir berechnen Lösungen von $x^2 \equiv n \bmod p^r$ für hinreichend großes r.
(Einen Algorithmus dafür werden wir später kennenlernen.)
- Durch sukzessives Dividieren werden die b-glatten z_i zu 1.