Faktorisierung: Probedivision

Das Finden kleiner Primfaktoren von $n \in \mathbb{Z}$ macht man mit der sogenannten Probedivision:

- Berechne Primzahlen unter fester Schranke $B \in \mathbb{R}$
- Berechne maximale Exponenten
- dann Rest prüfen auf Primalität

Beispiel: $n = 3^{21} + 1 = 10460353204$, Probedivision mit $B = 50$ ergibt Faktoren $2^2, 7^2$ und 43 mit $a = 2^2 * 7^2 * 43 = 8428$.Teilen von n durch a ergibt $m = 1241143$. Mit dem kleinen Satz von Fermat folgt aus $2^{m-1} \equiv 793958 \mod m$ dass m zusammengesetzt ist.

Die $p-1$-Methode

- n $\in \mathbb{Z}$ vorgegeben, p Primzahl mit $p|n$
- Berechne Produkt k von Primzahlpotenzen $\leq$ vorgegebener Schranke $B \in \mathbb{R}$
- Sind Primzahlpotenzen, die $p-1$ teilen, kleiner als B, so gilt $(p-1)|k$
- Damit folgt $a^k \equiv 1 \mod p$ mit kleinem Satz von Fermat
- Berechne $\mathrm{ggT}(a^k - 1, n)$ für geeignetes a
- Wird kein Teiler von n gefunden so wiederholt man das Verfahren mit neuem B

Beispiel: Sei $m = 1241143$ und $B = 13$, d.h. also $k = 2^3 * 3^2 * 5 * 7 * 11 * 13$. Damit erhält man $\mathrm{ggT}(2^k - 1, m) = 547$. Also ist $p = 547$ ein Teiler von m. Mit $\frac{m}{p} = 2269$ hat man dann die Faktorisierung von m gefunden.

Die $p-1$-Methode

Als Kandidaten für a eignen sich z.B. die von der Probedivision erhaltenen Primfaktoren.

Das $p-1$-Verfahren ist für zusammengesetzte Zahlen n geeignet, die einen Primfaktor p besitzen für den $p-1$ sich in kleine Primfaktoren zerlegt.

Eine Weiterentwicklung der $(p-1)$-Methode ist die Faktorisierungsmethode mit elliptischen Kurven (ECM). Diese funktioniert für beliebige zusammengesetzte Zahlen n.

Quadratisches Sieb

Beim Quadratischen Sieb (QS) geht man folgendermaßen vor:

- Sei $n \in \mathbb{Z}$ vorgegeben
- Bestimme $x, y \in \mathbb{Z}$ mit $x^2 \equiv y^2 \mod n$ und $x \not\equiv \pm y \mod n$
- Es gilt dann $n | x^2 - y^2 = (x-y)(x+y)$, aber $n \nmid (x-y)$ und $n \nmid (x+y)$
- Berechne $\mathrm{ggT}(x-y, n)$

Beispiel: Sei $n = 7429, x = 227, y = 210$. Dann ist $x - y = 17,\ x + y = 437$ und $x^2 - y^2 = (x-y)(x+y)$. Somit ist $\mathrm{ggT}(x-y, n) = 17$ ein echter Teiler von 7429.

Wie bestimmt man x und y?

Quadratisches Sieb

Beispiel: Sei $m = \lfloor \sqrt{n} \rfloor$ und $f(T) = (T+m)^2 - n$. Für obiges Beispiel mit $n = 7429$ ergibt sich $m = 86$, d.h. $f(T) = (T+86)^2 - 7429$. Dann gilt

- $f(-3) = 83^2 - 7429 = -540 = -1 \cdot 2^2 \cdot 3^3 \cdot 5$
- $f(1) = 87^2 - 7429 = 140 = 2^2 \cdot 5 \cdot 7$
- $f(2) = 88^2 - 7429 = 315 = 3^2 \cdot 5 \cdot 7$

also

- $83^2 \equiv -1 \cdot 2^2 \cdot 3^3 \cdot 5 \mod 7429$
- $87^2 \equiv 2^2 \cdot 5 \cdot 7 \mod 7429$
- $88^2 \equiv 3^2 \cdot 5 \cdot 7 \mod 7429$

woraus man

- $(87 \cdot 88)^2 \equiv (2 \cdot 3 \cdot 5 \cdot 7)^2 \mod n$

erhält. Damit ist z.B. $x = 87 \cdot 88 \mod n = 227$ und $y = 2 \cdot 3 \cdot 5 \cdot 7 \mod n = 210$. Wie findet man geeigneten Werte $f(s)$?

Quadratisches Sieb

- Vorgabe von **Faktorbasis** $F(B) := \{p \in \mathbb{P} \mid p \leq B\} \cup \{-1\}$ mit $B \in \mathbb{Z}^{>0}$
- $f(s) = (s+m)^2 - n = \prod_{i=1}^{n} p_i^{e_i}$ mit $p_i \in F(B)$ nennt man **B-glatt**
- Gesucht $S \subseteq \mathbb{Z}$ mit $\forall s \in S : f(s)$ ist B-glatt und $|S| \leq |F(B)|$
- Aufstellen und lösen eines linearen Gleichungssystems über $\mathbb{F}_2$

Haben wir S gefunden, in unserem Beispiel $S = \{-3, 1, 2\}$ und $F(7) = \{-1, 2, 3, 4, 5, 7\}$, so lösen wir das Gleichungssystem, das wir durch

$(-1 \cdot 2^2 \cdot 3^3 \cdot 5)^{\mu_1} \cdot (2^2 \cdot 5 \cdot 7)^{\mu_2} \cdot (3^2 \cdot 5 \cdot 7)^{\mu_3} =$

$(-1)^{\mu_1} \cdot 2^{2\mu_1 + 2\mu_2} \cdot 3^{3\mu_1 + 2\mu_3} \cdot 5^{\mu_1 + \mu_2 + \mu_3} \cdot 7^{\mu_2 + \mu_3} = (*)$

erhalten und bekommen $\mu_1 = 0$, $\mu_2 = \mu_3 = 1$. Daraus erhalten wir dann $(*) = (2 \cdot 3 \cdot 5 \cdot 7)^2 \mod n$. Wie bestimmt man S?

Quadratisches Sieb

Bestimmen von S:

- $l, B \in \mathbb{Z}^{>0}$ vorgegeben
- Betrachte $T := \{-l, -l+1, ..., 0, 1, ..., l-1, l\}$
- Gesucht: $S := \{t \in T \ : \ f(t)$ ist $B-$glatt$\}$
- $f(t)$ ist B-glatt, wenn aus $p | f(t)$ folgt: $p \in F(B)$
- $N_p := \{0 \leq s \leq p-1 : \ p | f(s)\}$ für $p \in F(B)$
- $\alpha \in N_p \Leftrightarrow \alpha$ ist Nullstelle von $f_p(T) \in \mathbb{F}_p[T]$
- $t \in T$ mit $p | f(t) \Rightarrow \ \exists \alpha \in N_p$ mit $t = \alpha \Rightarrow p | t - \alpha$
- $T_p := \{t \in T \mid t = \alpha \pm k \cdot p, \ \alpha \in N_p, \ k \in \mathbb{Z}$ geeignet $\}$ und $p \in F(B)$
- $S = \{t \in T \mid f(t) \cdot \left(\prod_{t \in T_p} p^{-e}\right) = \pm 1\}$

Für unser Beispiel mit $n = 7429, m = 86$ und $f(T) = (T+86)^2 - 7429$ wählen wir als Faktorbasis $F(7) = \{2, 3, 5, 7\} \cup \{-1\}$ und als Siebintervall die Menge $\{-3, -2, -1, 0, 1, 2, 3\}$.

Quadratisches Sieb

Für unser Beispiel bedeutet das also:

s	-3	-2	-1	0	1	2	3
$(s+m)^2 - n$	-540	-373	-204	-33	140	315	492
Sieb mit 2	-135		-51		35		123
Sieb mit 3	-5		-17	-11		35	41
Sieb mit 5	-1				7	7	
Sieb mit 7					1	1	

Man liest aus obiger Tabelle ab: Mit $l = 3$ und $B = 7$ ist $S = \{-3, 1, 2\}$.