

# Bsp. Quadratisches Sieb

**Bsp:** Wir faktorisieren die Zahl  $91 = 7 \cdot 13$ .

- Als Glattheitsschranke wählen wir  $b = 5$ .
- Wir faktorisieren nur positive Zahlen  $z_i := x_i^2 - n = (10 + i)^2 - n$ .
- Daher wählen wir  $B = \{2, 3, 5\}$ . Es gilt  $\left(\frac{n}{p}\right) = 1$  für alle  $p \in B$ .
- Wir wollen die Zahlen  $z_i$  im Intervall  $0 \leq i \leq 9$  sieben.
- Damit gilt  $z_i \leq z_9 = 19^2 - n = 270$ .
- Wir berechnen alle Lösungen von  $x^2 \equiv 91 \pmod{p^r}$  mit  $p^r \leq 270$ .

$p \backslash r$	1	2	3	4	5
2	1 (11)	–	–	–	–
3	$\pm 1$ (10, 11)	$\pm 1$ (10, 17)	$\pm 19$ (19, 35)	$\pm 46$ (46, 35)	$\pm 127$ (127, 35)
5	$\pm 1$ (11, 14)	$\pm 4$ (29, 21)	$\pm 29$ (29, 96)		

## Bsp. Quadratisches Sieb

- Für eine Lösung  $\pm x_{p^r}$  steht in der Klammer das kleinste  $x_i \geq 10$  mit  $x_i \equiv x_{p^r} \pmod{p^r}$  bzw.  $x_i \equiv -x_{p^r} \pmod{p^r}$ .
- Bsp:  $z_{10}$  ist durch  $3^2$  teilbar und damit auch alle  $z_{10+3^2\mathbb{Z}}$ .
- Wir erhalten die folgenden partiellen Faktorisierungen.

$x_i$	$z_i = x_i^2 - n$	teilbar durch	Cofaktor
10	9	$3^2$	1
11	30	$2 \cdot 3 \cdot 5$	1
12	53	–	53
13	78	$2 \cdot 3$	13
14	105	$3 \cdot 5$	7
15	134	2	67
16	165	$3 \cdot 5$	11
17	198	$2 \cdot 3^2$	11
18	233	–	233
19	270	$2 \cdot 3^3 \cdot 5$	1

# Bsp. Quadratisches Sieb

- Die Zeilen 11 und 19 liefern die Kongruenz

$$(11 \cdot 19)^2 \equiv 27^2 \equiv (2 \cdot 3^2 \cdot 5)^2 = 90^2 \equiv (-1)^2 \pmod{91}.$$

- Es gilt  $27 \not\equiv \pm 1 \pmod{91}$  und  $\text{ggT}(27 \pm 1, 91) = \{7, 13\}$ .

## Anmerkungen:

- In der “Large Prime”-Variante des Siebs werden Zeilen mit demselben Co-Faktor verwendet.
- Bsp.: Für  $x_i = 16$  und  $17$  erhalten wir die zusätzliche Relation

$$(16 \cdot 17 \cdot 11^{-1})^2 \equiv 2 \cdot 3^3 \cdot 5 \pmod{91}.$$

- **Laufzeit:** Das Quadratische Sieb benötigt Zeit  $e^{\sqrt{\ln n \ln \ln n}}$ .  
(unter geeigneten Glattheitsannahmen)
- Dies ist superpolynomiell aber supexponentiell in  $\ln n$ .

# Pollards $p - 1$ Methode

## Idee:

- Sei  $n = pr$  mit  $1 < p < n$ ,  $p$  prim,  $p \nmid r$ . D.h.  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ .
- Sei  $p - 1$   $b$ -glatt, d.h.  $p - 1 = \prod_{p \in B} p^{e_B}$ .
- Sei  $k$  ein Vielfaches von  $\prod_{p \in B} p^{e_B}$ . Dann gilt
$$a^k \equiv 1 \pmod{p} \text{ für alle } a \in U_n.$$
- Falls zusätzlich  $a^k \not\equiv 1 \pmod{r}$  folgt  $p \leq \text{ggT}(a^k - 1, n) < n$ .

## Algorithmus Pollards $p - 1$ -Methode

EINGABE:  $n = pr$  zusammengesetzt,  $p$  prim, Schranke  $C$  mit  $p \leq C$ .

- 1 Wähle  $b$  geeignet, so dass  $p - 1$   $b$ -glatt ist. Sei  $B = \{p_1, \dots, p_s\}$ .
- 2 Wähle  $a \in_R \{2, \dots, n - 1\}$ . Falls  $\text{ggT}(a, n) > 1$ , Ausgabe des ggTs.
- 3 Für  $i = 1 \dots s$ 
  - 1 Wähle  $e_i$  maximal mit  $p_i^{e_i} < C$ . Berechne  $a := a^{p_i^{e_i}} \pmod{N}$ .
- 4 Falls  $\text{ggT}(a - 1, N) \notin \{1, N\}$ , Ausgabe des ggTs.

# Analyse von Pollards $p - 1$ -Methode

## Korrektheit:

- In Schritt 3.1 wird  $a^k \bmod N$  berechnet mit  $k = \prod_{i=1}^s p_i^{e_i}$ .
- Falls  $p - 1$   $b$ -glatt ist, gilt  $p - 1 | k$ .
- Damit ist  $\text{ggT}(a^k - 1, n) \geq p$ .
- D.h. wir finden einen nicht-trivialen Teiler, falls  $\text{ggT}(a^k - 1, n) < n$ .
- Sei  $q$  ein Primteiler von  $r$ , so dass  $q - 1$  nicht  $b$ -glatt ist.
- Damit existiert ein  $q' | q - 1$ ,  $q' \in \mathbb{P}$  mit  $q' > b$ .
- Ferner gelte  $q' | \text{ord}(a)$  in  $U_q$ . Dann gilt

$$a^k \not\equiv 1 \pmod{q} \text{ und damit } \text{ggT}(a^k - 1, n) < n.$$

- Wir berechnen die Ws, dass  $q' | \text{ord}(a)$  in  $U_q$ .
- Sei  $U_q$  zyklisch mit Generator  $g$ . Wir schreiben  $a \equiv g^i \pmod{q}$ .
- Es folgt  $\text{ord}(a) = \frac{q-1}{\text{ggT}(i, q-1)}$  in  $U_q$ . Falls  $q' \nmid i$ , gilt  $q' | \text{ord}(a)$ .
- Da  $a$  zufällig gewählt ist, geschieht dies mit Ws  $1 - \frac{1}{q'}$ .

# Analyse von Pollards $p - 1$ -Methode

## **Laufzeit:**

- Schritt 3 benötigt Zeit  $\mathcal{O}(s \log C \log N^2) = \mathcal{O}(s \log^3 N)$ .

## **Problem** der $p - 1$ -Methode:

- Die Laufzeit ist abhängig von der Ordnung von  $U_p$ .
- Sei  $\frac{p-1}{2} \in \mathbb{P}$  mit  $\frac{p-1}{2} \approx \sqrt{n}$ .
- Dann benötigen wir  $p_s \approx \sqrt{n}$  und damit

$$s = |\{x \in \mathbb{P} \mid x \leq p_s\}| \approx \frac{\sqrt{n}}{\log n}.$$

- In diesem Fall ist die Laufzeit nicht besser als bei Probedivision.

# Quadratische Erweiterung

## Ziel:

- $\mathbb{F}_p^2$  besitzt Ordnung  $|\mathbb{F}_p^2| = p^2 - 1 = (p + 1)(p - 1)$ .
- Wir konstruieren eine Untergruppe von  $\mathbb{F}_p^2$  mit Ordnung  $p + 1$ .
- Unsere Hoffnung ist, dass  $p + 1$  in kleine Primfaktoren zerfällt.

## Definition

Sei  $R$  ein kommutativer Ring,  $D \in R$  kein Quadrat.  $R[\sqrt{D}] = R \oplus R\sqrt{D}$  heißt *quadratische Erweiterung* von  $R$ . Sei  $\omega = x + y\sqrt{D} \in R[\sqrt{D}]$ .

- 1 Das zu  $\omega$  *konjugierte* Element ist definiert als  $\bar{\omega} = x - y\sqrt{D}$ .
- 2 Die *Spur* ist definiert als  $\text{Tr} : R[\sqrt{D}] \rightarrow R, \omega \mapsto \omega + \bar{\omega}$  mit
$$\text{Tr}(x + y\sqrt{D}) = 2x.$$
- 3 Die *Norm* ist definiert als  $N : R[\sqrt{D}] \rightarrow R, \omega \mapsto \omega\bar{\omega}$  mit
$$N(x + y\sqrt{D}) = x^2 - Dy^2.$$

**Anmerkung:** Die Spur ist additiv, die Norm multiplikativ.

# Eigenschaften von Norm und Spur

## Lemma Eigenschaften von Norm und Spur

Sei  $\omega \in R[\sqrt{D}]$  beliebig. Es gilt

- 1  $\omega \in R[\sqrt{D}]^*$  gdw  $N(\omega) \in R^*$ .
- 2  $\omega, \bar{\omega}$  sind Nullstellen des Polynoms  $X^2 - \text{Tr}(\omega)X + N(\omega)$ .

**Beweis:**

(1)  $\Rightarrow$ : Sei  $\omega \in (R[\sqrt{D}])^*$ . Dann gilt

$$1 = N(1) = N(\omega\omega^{-1}) = N(\omega)N(\omega^{-1}).$$

- D.h.  $N(\omega) \mid 1$  und damit  $N(\omega) \in R^*$ .
- $\Leftarrow$ : Sei  $N(\omega) \in R^*$ . Für  $\omega^{-1} := \bar{\omega}N(\omega)^{-1}$  gilt

$$\omega\omega^{-1} = \omega\bar{\omega}N(\omega)^{-1} = N(\omega)N(\omega)^{-1} = 1.$$

(2) Offenbar sind  $\omega$  und  $\bar{\omega}$  Nullstellen des Polynoms

$$(X - \omega)(X - \bar{\omega}) = X^2 - (\omega + \bar{\omega})X + \omega\bar{\omega} = X^2 - \text{Tr}(\omega)X + N(\omega).$$