Quadratisches Sieb

- **Ziel:** Faktorisierung einer gegebenen Zahl n
- Grundidee: x, y finden, so dass

  $x^2 = y^2 \pmod{n}$, und

  $x \neq y, \quad x \neq -y \pmod{n}$

  $\rightarrow \mathrm{ggT}(x - y, n)$ liefert einen Faktor von n.

- **Aufgabe:** Es gilt $106^2 = 17^2 \pmod{3649}$.
  Bestimme ausgehend von dieser Gleichung einen Faktor von 3649.

- **Vorgehen** (Skizze)

1. Bestimme eine Menge F von **kleinen** Primzahlen.
2. Finde Werte b_i, so dass $b_i^2 \pmod{n}$ nur aus Primfaktoren aus F besteht.
   $M :=$ Menge dieser b_i.
3. Finde $b_1, \ldots, b_r \in M$,
   gerade Zahlen $\alpha_0, \alpha_1, \ldots, \alpha_r \in \mathbb{N}$, und
   Primfaktoren $p_1, \ldots, p_k \in F$ so dass
   $$b_1^2 \cdot b_2^2 \cdots b_r^2 = (-1)^{\alpha_0} \cdot (p_1)^{\alpha_1} \cdots (p_k)^{\alpha_k}$$
   setze $x := b_1 \cdots b_r$, $y := (-1)^{\alpha_0/2} \cdot (p_1)^{\alpha_1/2} \cdots (p_k)^{\alpha_k/2}$

Teil 1: Schritt Nr. 3
Teil 2: Schritt Nr. 2

- $\alpha_0, \alpha_1, \alpha_2, \ldots$ werden mithilfe eines Gleichungs-Systems bestimmt.

Veranschaulichung anhand eines Beispiels

- $n = 117$
- $F = \{-1, 2, 3, 5, 7\}$ (**Bem:** -1 gehört als 'Nicht-Primzahl' dazu.)
- $M := \{15, 25, 37, 47\}$.
- Beleg, dass Quadrate aus M nur aus Primfaktoren aus F bestehen:
  - $b_1 = 15$: $15^2 = (-1) \cdot 3^2 \pmod{n}$
  - $b_2 = 25$: $25^2 = 2^3 \cdot 5 \pmod{n}$
  - $b_3 = 37$: $37^2 = (-1) \cdot 5 \cdot 7 \pmod{n}$
  - $b_4 = 47$: $47^2 = (-1) \cdot 2 \cdot 7 \pmod{n}$

Gesucht: $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ so dass bei $\left(15^2\right)^{\lambda_1} \cdot \left(25^2\right)^{\lambda_2} \cdot \left(37^2\right)^{\lambda_3} \cdot \left(47^2\right)^{\lambda_4}$ alle Elemente von F gerade Exponenten haben. Respektive:

(1) $\lambda_1 + \lambda_3 + \lambda_4 = 0 \pmod{2}$ [(-1) hat geraden Exponent]

(2) $\lambda_2 + \lambda_4 = 0 \pmod{2}$ [2 hat geraden Exponent]

(3) $\lambda_2 + \lambda_3 = 0 \pmod{2}$ [5 hat geraden Exponent]

(4) $\lambda_3 + \lambda_4 = 0 \pmod{2}$ [7 hat geraden Exponent]

Schritt 3

- **Eine Lösung des Gleichungs-Systems:** $\lambda_1 = 0$, $\lambda_2 = \lambda_3 = \lambda_4 = 1$.
- Für das gesuchte Produkt: Wähle b_2, b_3, b_4.
- Somit (mithilfe der linken und rechten Einträge vom Beleg auf der vorherigen Folie):

$$x = b_2 \cdot b_3 \cdot b_4 = 25 \cdot 37 \cdot 47 = 68 \pmod{n},$$

$$y = (2^3 \cdot 5)^{\frac{1}{2}} \cdot ((-1) \cdot 5 \cdot 7)^{\frac{1}{2}} \cdot ((-1) \cdot 2 \cdot 7)^{\frac{1}{2}} = (-1) \cdot 2^2 \cdot 5 \cdot 7 = 94 \pmod{n}$$

- $\mathrm{ggT}(x - y, n) = \mathrm{ggT}(68 - 94, 117) = 13 \Rightarrow$ gesuchter Faktor = 13

Terminologie

- Menge F heisst **Faktorbasis**
  (enthält Primzahlen bis zu einer gewissen Schranke B und -1).
- Eine Zahl t heisst B**-glatt mod** n, wenn $t \pmod{n}$ nur aus Primfaktoren von F besteht.
  (Das Vorzeichen wird so gewählt, dass der Betrag der Zahl möglichst klein wird.)
- Die Menge M besteht aus allen Zahlen aus einer Grundmenge $\{-S, \ldots, +S\}$, deren Quadrate B**-glatt mod** n sind.

Aufgabe: Wir betrachten wieder $n = 117$ und $F = \{-1, 2, 3, 5, 7\}$.

Welche der Zahlen aus $\{11, 23, 35, 70\}$ gehören zu M?