## Quadratisches Sieb - Teil 2

#### Algorithmus mit folgendem Verhalten:

- Eingabe:
  - n (zu faktorisieren)
  - F := Menge von betrachteten Primzahlen ("Faktorbasis")
- Ausgabe: Zahlen b mit der Eigenschaft:
  - $b^2 \pmod{n}$  ist zusammengesetzt aus Faktoren aus F.

# Schritte des Algorithmus – Übersicht

### **Input:** Zahl *n*, Faktorbasis *F*

- 1. Fixiere eine Menge S von "kleinen" Zahlen
- 2.  $m := |\sqrt{n}|$
- 3. **for** (jedes  $x \in S$ )
  - 3.1 Bestimme  $q(x) := (m + x)^2 n$
  - 3.2 Prüfe, ob q(x) aus Primfaktoren in F zusammengesetzt ist Falls ja  $\to$  Zahl mit gewünschter Eigenschaft gefunden

#### end

### Bsp:

**ZHAW** 

- $\bullet$   $F := \{-1, 2, 3, 5, 7\}$

### Gründe, weshalb q(x) als Kandidaten gewählt werden

- q(x) ist ein Quadrat modulo n (Wurzel: m + x)
- q(x) ist nicht "zu gross"  $(< n) \rightarrow$  Faktorzerlegung wird nicht zu lang
- q(x) ist nicht "zu klein"  $\rightarrow$  Faktorzerlegung wird nicht zu kurz

## Algorithmische Umsetzung – Grundidee

### Bsp:

- n = 1000,
- $F := \{-1, 2, 3, 5, 7\}$
- $S = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$

**Aufgabe:** Bestimme diejenigen  $x \in S$ , für die q(x) die gewünschte Bedingung erfüllt

(via Algorithmus von letzter Folie und mithilfe der Faktorisierung von PARI/GP).

## Algorithmische Umsetzung – Grundidee

Lösung der Aufgabe:

## Verbesserung – Skizze

### Analyse des bisherigen Vorgehens

• q(x) jeweils faktorisiert  $\rightarrow$  für grosse Zahlen nicht praktikabel

#### Versuch 1

- Für jeden Faktor p ∈ F: Teste, ob q(x) durch p teilbar ist. Falls ia: dividiere so oft wie möglich durch p.
- Problem: viele erfolglose Probedivisionen → ineffizient

#### Versuch 2

- Erstelle erste zwei Zeilen der vorherigen Tabelle.
- 2 Für jeden Faktor  $p \in F$ :
  - Finde einen Eintrag, der durch p teilbar ist.
  - Gehe mit Schritten der Länge p nach links und nach rechts.
  - Teile die gefunden Einträge so oft wie möglich durch p.

## Verbesserung – Skizze

**Ziel:** effiziente Umsetzung des Schrittes

"finde einen Eintrag q(x), der durch p teilbar ist"

**Erinnerung:** 
$$q(x) = (m+x)^2 - n$$
  $(m := \lfloor n \rfloor)$ 

**Bem 1:** p teilt  $q(x) \Leftrightarrow q(x) = 0 \pmod{p}$ 

Bem 2: Man kann zeigen (Details: s. später):

- Die quadratische Gleichung  $\underbrace{(m+x)^2-n}_{q(x)}=0 \pmod{p}$  hat höchstens zwei Lösungen in  $\mathbb{Z}_p^n$
- Es gibt einen effizienten Algorithmus, um diese zwei Lösungen zu bestimmen.

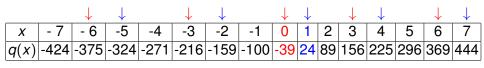
**Somit:** Der gewünschte Eintrag q(x) kann gefunden werden, indem die Gleichung  $q(x) = 0 \pmod{p}$  gelöst wird.

6/8

## Verbesserung – Skizze

#### Illustration

- Erste zwei Zeilen der Tabelle aus letztem Beispiel, leicht erweitert.
- Sieb mit *p* = 3:



- 1. Lösung für  $q(x) = 0 \pmod{3}$  in  $\mathbb{Z}_3^*$ : x = 1.
- 2. Lösung für  $q(x) = 0 \pmod{3}$  in  $\mathbb{Z}_3^*$ : x = 0.
- Weitere Lösungen resultieren, indem man mit Schrittlänge 3 nach links und rechts geht.

## Algorithmus als Ganzes

#### **Quadratisches Sieb**

- **Input:** Zahl *n*, Faktorbasis *F*
- Output: B-glatte Zahlen modulo n
  - 1. Fixiere eine Menge *S* von "kleinen" Zahlen
  - 2.  $m := \lfloor \sqrt{n} \rfloor$
  - 3. **for** (jedes  $x \in S$ ): berechne q(x) **end**
  - 4. multipliziere alle negativen Zahlen mit −1 // Sieb mit −1
  - 5. **for** (jedes  $p \in F$ ) // Sieb mit p
    - 5.1 Löse Gleichung  $q(x) = 0 \pmod{p}$   $\rightarrow$  ergibt  $x_1$  und ev. auch
  - *X*<sub>2</sub>
    - 5.2 Markiere in S die Elemente

..., 
$$x_1 - 2p$$
,  $x_1 - p$ ,  $x_1$ ,  $x_1 + p$ ,  $x_1 + 2p$ , ... und ...,  $x_2 - 2p$ ,  $x_2 - p$ ,  $x_2$ ,  $x_2 + p$ ,  $x_2 + 2p$ , ...

- 5.3 **for** (markierte x): teile q(x) so oft wie möglich durch p **end end**
- 6. Gib diejenigen q(x) aus, bei denen die fortlaufenden Divisionen zum Resultat 1 führen.