Recap: 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

- **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 $\alpha_0, \alpha_1, \ldots, \alpha_r \in \mathbb{Z}$, 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 $x := b_1 \cdots b_r, \quad y := (-1)^{\alpha_0/2} \cdot (p_1)^{\alpha_1/2} \cdots (p_k)^{\alpha_k/2}$

Schritt 2

Input: Zahl n, Faktorbasis F

1. Fixiere eine Menge S von "kleinen" Zahlen.
2. $m := \lfloor \sqrt{n} \rfloor$
3. **for** (jedes $x \in S$)
   3.1 Bestimme $q(x) := (m + x)^2 - n$
   end
4. **for** (jedes $p \in F$)
   4.1 Finde alle Einträge $q(x)$, die durch p teilbar sind.
   4.2 Teile diese so oft wie möglich durch p.
   end

return Einträge $q(x)$, bei denen 1 herauskommt.

Umsetzung von Zeile 4.1: Zwei 'Anfangs-Einträge' finden, dann in Schritten der Länge p nach links und nach rechts gehen.

Zielsetzung

verbleibende Problemstellung:
'Anfangs-Einträge' $q(x)$ finden, die durch p teilbar sind.

Beobachtungen

- 'durch p teilbar' bedeutet '$= 0 \pmod{p}$'.
- $\Rightarrow$ Anfangs-Einträge lassen sich finden durch Lösen der Gleichung $q(x) = 0 \pmod{p}$
- Erinnerung: $q(x) = (m+x)^2 - n$. Einsetzen ergibt Gleichung $(m+x)^2 = n \pmod{p}$

Lösungsverfahren für Gleichung: Wurzel ziehen!
(Inhalt der heutigen Stunde)

Modulares Wurzelziehen

Allg. Form: gesucht sind Lösungen der Gleichung $x^2 = a \pmod{p}$

Wurzeln allgemein

- **Bem:** p steht im Folgenden für eine Primzahl ≥ 3.

Beobachtung

$$\begin{aligned} 1^2 &= (p-1)^2 \\ 2^2 &= (p-2)^2 \\ 3^2 &= (p-3)^2 \\ &\vdots \\ \left(\frac{p-1}{2}\right)^2 &= \left(p - \frac{p-1}{2}\right)^2 \end{aligned}$$

Folgerungen

Satz

Die Hälfte der Elemente von $\mathbb{Z}_p^*$ hat eine Wurzel, die andere Hälfte nicht.

Satz

Jedes Element aus $\mathbb{Z}_p^*$ hat entweder 0 oder 2 Wurzeln.

Kriterium (ohne Begründung)

Satz (Euler)

Für jedes $a \in \mathbb{Z}_p^*$ gilt

$$a^{\frac{p-1}{2}} \pmod p = \begin{cases} 1, & \text{falls } a \text{ eine Wurzel hat} \\ -1, & \text{falls } a \text{ keine Wurzel hat} \end{cases}$$

Notation

- Abkürzung für 'a hat eine Wurzel in $\mathbb{Z}_p^*$': a ist QRp (quadratischer Rest modulo p)
- Abkürzung für 'a hat keine Wurzel in $\mathbb{Z}_p^*$': a ist QRNp (quadratischer Nicht-Rest modulo p)

Algorithmus von Tonelli – Fall 1

Annahme: Gegeben ist ein Element $a \in \mathbb{Z}_p^*$ mit $a \in$ QRp.
Fall 1: $p = 3 \pmod 4$

Beobachtung

Findet man ein **ungerades** u mit $a^u = 1 \pmod p$, so gilt

- $a^{u+1} = a$, und
- $a^{\frac{u+1}{2}}$ ist eine Wurzel von a.

Bestimmung einer Wurzel:

- Gemäss vorherigem Kriterium von Euler: $a^{\frac{p-1}{2}} = 1$.
- Da $p = 3 \pmod 4$, ist $\frac{p-1}{2}$ ungerade.
- Einsetzen von $u = \frac{p-1}{2}$ gibt: $a^{\frac{u+1}{2}} = a^{\frac{p+1}{4}}$ ist Wurzel

Folgerung

Ist $p = 3 \pmod 4$ so gilt für alle $a \in$ QRp: $a^{\frac{p+1}{4}}$ ist eine Wurzel von a.

Aufgabe: Löse die Gleichung: $x^2 = 13 \pmod{23}$.

Algorithmus von Tonelli – Grundidee für Fall 2

Fall 2: $p = 1 \pmod 4)$

Beobachtung

Findet man ein $h \in \mathbb{Z}_p^*$, ein **ungerades** u und ein **gerades** g mit $a^u h^g = 1 \pmod p$, so gilt

- $a^{u+1} h^g = a$, und
- $a^{\frac{u+1}{2}} \cdot h^{\frac{g}{2}}$ ist eine Wurzel von a.

Grundidee:

- h := irgendein Element **ohne** Wurzel ('quadratischer Nichtrest')
- gemäss dem Euler-Kriterium ist $a^{\frac{p-1}{2}} \cdot h^{p-1} = 1$.
- Halbiere die Exponenten der obigen Gleichung so lange, bis der Exponent von a ungerade wird.
  (Sollte das Produkt -1 werden, erhöhe Exponenten von h um $\frac{p-1}{2}$.
  Dies entspricht einer Multiplikation mit -1.)

Algorithmus von Tonelli – Grundidee für Fall 2

Fall 2: $p = 1 \pmod 4$ (Forts.)
Beispiele:

- Gleichung: $x^2 = 6 \pmod{73}$.
  Algorithmus von Tonelli:
  - Setze $a := 6$.
  - Wähle (zum Beispiel) $h = 5$.
    (Da $5^{36} = -1 \pmod{73}$, ist 5 ein quadratischer Nichtrest.)
  - Einsetzen ergibt: $a^{\frac{p-1}{2}} \cdot h^{p-1} = 6^{36} \cdot 5^{72} = 1 \pmod{73}$.
  - Halbierung der Exponenten: $6^{18} \cdot 5^{36} = 1 \pmod{73}$.
  - Halbierung der Exponenten: $6^{9} \cdot 5^{18} = 1 \pmod{73}$.
  - Einsetzen von $u := 9$ und $g := 18$ in der Beobachtung auf der vorherigen Folie ergibt:
    $a^{\frac{u+1}{2}} \cdot h^{\frac{g}{2}} = 6^{\frac{9+1}{2}} \cdot 5^{\frac{18}{2}} = 6^5 \cdot 5^9 = 15 \pmod{73}$ ist eine Lösung.

Fall 2: $p = 1 \pmod 4$ (Forts.)
Beispiele:

- Gleichung: $x^2 = 2 \pmod{73}$.
  Algorithmus von Tonelli:
  - Setze $a := 2$.
  - Wähle (zum Beispiel) $h = 10$.
    (10 ist quadratischer Nichtrest, da $10^{36} = -1 \pmod{73}$)
  - Einsetzen ergibt: $a^{\frac{p-1}{2}} \cdot h^{p-1} = 2^{36} \cdot 10^{72} = 1 \pmod{73}$.
  - Halbierung der Exponenten: $2^{18} \cdot 10^{36} = -1 \pmod{73}$.
  - Korrektur: $\frac{p-1}{2} = 36$. Addition im Exponenten ergibt:
    $2^{18} \cdot 10^{36+36} = 2^{18} \cdot 10^{72} = 1 \pmod{73}$
  - Halbierung der Exponenten: $2^9 \cdot 10^{36} = -1 \pmod{73}$
  - Korrektur: $2^9 \cdot 10^{36+36} = 2^9 \cdot 10^{72} = 1 \pmod{73}$
  - Einsetzen von $u := 9$ und $g := 72$ in der Beobachtung auf einer vorherigen Folie ergibt:
    $a^{\frac{u+1}{2}} \cdot h^{\frac{g}{2}} = 2^{\frac{9+1}{2}} \cdot 10^{\frac{72}{2}} = 2^5 \cdot 10^{36} = 41 \pmod{73}$ ist eine Lösung.

Algorithmus von Tonelli – Fall 2

FINDEWURZEL(a, p) // a QRp; löse $x^2 = a \pmod{p}$ in $\mathbb{Z}_p^*$

1. Setze h auf einen beliebigen QNRp.
   $e_1 := \frac{p-1}{2}$
   $e_2 := p - 1.$
   $c := a^{e_1} \cdot h^{e_2} \pmod{p}.$
2. **while** $(2|e_1)$ // $c == a^{e_1} \cdot h^{e_2} == 1 \pmod{p}$
   $e_1 := \frac{e_1}{2}; \qquad e_2 := \frac{e_2}{2}$
   if $(a^{e_1} \cdot h^{e_2} == -1 \pmod{p})$
   $e_2 := e_2 + \frac{p-1}{2}$ // Mult. mit $h^{\frac{p-1}{2}} = -1 \pmod{p}$
   end
   // $a^{e_1} \cdot h^{e_2} == 1 \pmod{p}$ mit e_1 ungerade und e_2 gerade $\Rightarrow$ $a^{e_1+1} \cdot h^{e_2} == a \pmod{p}$
3. **return** $x_{1,2} = \pm a^{\frac{e_1+1}{2}} \cdot h^{\frac{e_2}{2}} \pmod{p}$

end

Aufgabe

- Löse die Gleichung $x^2 = 18 \pmod{41}$