

KRY: Wahlfach Kryptologie

Serie 9: Quadratisches Sieb, modulare Wurzeln

Aufgabe 1 (T)

Wir betrachten die zusammengesetzte Zahl $n = 91$. In dieser Aufgabe geht es darum, die Berechnungs-Schritte für das **Quadratische Sieb** durchzugehen.

Verwenden Sie folgende Werte:

- $m = \lfloor \sqrt{91} \rfloor = 9$
- $q(x) = (m + x)^2 - n$
- $F = \{-1, 2, 3, 5\}$ ($B = 5$)
- $S = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$

- (a) Bestimmen Sie mit Hilfe des Siebverfahrens diejenigen $q(x)$, die "B-glatt modulo n " sind¹.
- (b) Notieren Sie das lineare Gleichungssystem $(\bmod 2)$ zum Bestimmen eines geeigneten Produktes von B -glatten Quadraten.
- (c) Bestimmen Sie durch Lösen des Gleichungssystems aus Aufgabe b) ein geeignetes Produkt von B -glatten Quadraten, und berechnen Sie damit einen Faktor von n .

Aufgabe 2 (T)

- (a) Bestimmen Sie die quadratischen Reste modulo 11 mit Hilfe des Kriteriums von Euler.
- (b) Suchen Sie mit dem Kriterium von Euler einen quadratischen Nichtrest modulo 97.

Aufgabe 3 (T)

Bestimmen Sie mit Hilfe von Tonellis Algorithmus die Lösungen der untenstehenden Gleichungen.

- (a) $x^2 = 11 \pmod{43}$
- (b) $x^2 = 6 \pmod{97}$

¹bedeutet: diejenigen $q(x)$, deren Faktoren alle in $\{-1, 2, 3, 5\}$ liegen

$$1) n = 91 \quad ; \quad m = \lfloor \sqrt{91} \rfloor = 9$$

a)

| | A | B | C | D | E | F | G | H | I | J |
|---|-------------|-----|-----|-----|-----|-----|---|----|----|----|
| 1 | x | -4 | -3 | -2 | -1 | 0 | 1 | 2 | 3 | 4 |
| 2 | q(x) | -66 | -55 | -42 | -27 | -10 | 9 | 30 | 53 | 78 |
| 3 | Sieb mit -1 | 66 | 55 | 42 | 27 | 10 | 9 | 30 | 53 | 78 |
| 4 | Sieb mit 2 | 33 | 55 | 21 | 27 | 5 | 9 | 15 | 53 | 39 |
| 5 | Sieb mit 3 | 11 | 55 | 7 | 1 | 5 | 1 | 5 | 53 | 13 |
| 6 | Sieb mit 5 | 11 | 11 | 7 | 1 | 1 | 1 | 1 | 53 | 13 |
| 7 | B-glatt | | | | | | | | | |

$$\hookrightarrow q(-1) = -27 \quad q(0) = -10 \quad q(1) = 9 \quad q(2) = 30$$

Gl. System $(\text{mod } 2)$

b)

Faktorisierung

$$-27 = (-1) \cdot 3^3 \quad (\lambda_1)$$

$$-10 = (-1) \cdot 2 \cdot 5 \quad (\lambda_2)$$

$$9 = 3^2 \quad (\lambda_3)$$

$$30 = 2 \cdot 3 \cdot 5 \quad (\lambda_4)$$

| | λ_1 | λ_2 | λ_3 | λ_4 |
|----|-------------|-------------|-------------|-------------|
| -1 | 1 | 1 | 0 | 0 |
| 2 | 0 | 1 | 0 | 1 |
| 3 | 1 | 0 | 0 | 1 |
| 5 | 0 | 1 | 0 | 1 |



$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad (\text{mod } 2)$$

$$\lambda_1 + \lambda_2 = 0 \quad (\text{mod } 2)$$

$$\lambda_2 + \lambda_4 = 0 \quad //$$

$$\lambda_1 + \lambda_4 = 0 \quad //$$

$$\lambda_2 + \lambda_4 = 0 \quad //$$

$$c) \quad q(1) = 3^2 \rightarrow \lambda_1=0 \quad \lambda_2=0 \quad \lambda_3=1 \quad \lambda_4=0$$

$$\hookrightarrow q(x) = (g+x)^2 \pmod{u}$$

$$\text{Wenn } x=1 \rightarrow 3^2 = 10^2 \pmod{u}$$

$$\begin{array}{ccc} / & / \\ y & x & \rightarrow \text{ggT}(x-y, u) \end{array}$$

$$\text{ggT}(10-3, 91) = 7$$

$$-p=11$$

$$2) \quad a) \quad a^{\frac{p-1}{2}} = 1 \pmod{11}$$

$$\begin{array}{r|cccccccccc} a & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline a^5 \pmod{11} & 1 & 10 & 1 & 1 & 1 & 10 & 10 & 10 & 1 & 10 \end{array}$$

$$b) \quad p=97 \quad a^{\frac{p-1}{2}} = a^{48}$$

$$a^{48} = 96 \pmod{97}$$

$$1^{48} = 1 \pmod{97}$$

$$2^{48} = 1 \quad //$$

$$3^{48} = 1 \quad 4$$

$$4^{48} = 1 \quad //$$

$$\underline{5^{48} - 96} \quad 1 \quad \rightarrow a = 5$$

$$3) \quad x^2 = 11 \pmod{43}$$

Folgerung

Ist $p = 3 \pmod{4}$ so gilt für alle $a \in \mathbb{Q} \setminus \{0\}$: $a^{\frac{p+1}{4}}$ ist eine Wurzel von a .

$$a) \quad p=43 \quad 43 = 3 \pmod{4} \rightarrow \text{Fall 1}$$

$$a^{\frac{p+1}{4}} = a^{11} \rightarrow 11^{11} \pmod{43}$$

$$x_1 = 21$$

$$-11^{11} \pmod{43}$$

$$x_2 = 22$$

$$b) \quad x^2 = 6 \pmod{97} \quad 97 = 1 \pmod{4} \rightarrow \text{Fall 2}$$

$$a=6 \quad h=5 \rightarrow 5^{48} = 96 \pmod{97}$$

Aufgabe 2.b)

$$6^{48} \cdot 5^{96} = 1 \pmod{97}$$

$$6^{24} \cdot 5^{98} = -1 \quad //$$

$$6^{24} \cdot 5^{96} = 1 \quad //$$

$$6^{12} \cdot 5^{98} = -1 \quad //$$

$$6^{12} \cdot 5^{96} = 1 \quad //$$

$$6^6 \cdot 5^{98} = 1 \quad //$$

$$6^3 \cdot 5^{24} = -1 \quad //$$

$$6^3 \cdot 5^{72} = 1$$

$$x_1 = 6^2 \cdot 5^{36} \pmod{97} = 59$$

$$\hookrightarrow x_2 = -6^2 \cdot 5^{36} \pmod{97} = 43$$