



Präsenzübungen zur Vorlesung
Diskrete Mathematik 2
Einführung in die theoretische Informatik
Sommersemester 2014
Blatt 4 / 27./28. Mai 2014

AUFGABE 1:

Sei p prim und g ein Generator von $\mathbb{Z}_p^* := \{1, 2, \dots, p-1\}$. Wir definieren die Sprachen

$$\text{DDH} := \{(g^\alpha, g^\beta, g^y) \mid g^y = g^{\alpha\beta} \bmod p\} \subseteq (\mathbb{Z}_p^*)^3$$

$$\text{ELGAMAL} := \{(g^a, g^r, m, x) \mid x = m \cdot g^{ar} \bmod p\} \subseteq (\mathbb{Z}_p^*)^4$$

Sei nun konkret $p = 17$ und $g = 3$. Angenommen wir haben ein ElGamal-Orakel, das uns folgende Informationen liefert:

$$(11, 14, 3, 1), (5, 7, 13, 7) \in \text{ELGAMAL}, (15, 8, 11, 1) \notin \text{ELGAMAL}$$

Entscheiden Sie für folgende Tupel, ob sie in der Sprache DDH liegen:

$$(11, 14, 6), (11, 14, 9), (5, 7, 13), (5, 7, 11), (15, 8, 14)$$

Verwenden Sie folgende Reduktionsabbildung $f : (\mathbb{Z}_p^*)^3 \rightarrow (\mathbb{Z}_p^*)^4$ aus der Vorlesung:

Algorithm 1 Funktion f für $\text{DDH} \leq_p \text{ELGAMAL}$

- 1: **Eingabe** : $(g^\alpha, g^\beta, g^y) \in (\mathbb{Z}_p^*)^3$, Gruppe: $[g, p, q = p-1]$
- 2: **Ausgabe** : $(g^a, g^r, m, x) \in (\mathbb{Z}_p^*)^4$
- 3:
- 4: $g^a \leftarrow g^\alpha$
- 5: $g^r \leftarrow g^\beta$
- 6: $m \in_R \mathbb{Z}_p^*$
- 7: $x \leftarrow m \cdot g^y \bmod p$
- 8: **return** (g^a, g^r, m, x)

AUFGABE 2:

Sei $p = 31$. Berechnen Sie das Legendre-Symbol $\left(\frac{a}{p}\right)$ für die angegebenen $a \in \mathbb{N}$. Sie sollten die Rechenregeln auf Folie 98 und das Quadratische Reziprozitätsgesetz (Folie 99) verwenden. Entscheiden Sie jeweils, ob a ein quadratischer Rest modulo p ist. Führen Sie alle Berechnungen ohne Taschenrechner durch und geben Sie alle Zwischenschritte an.

(a) $a = 2$

(b) $a = 21$

AUFGABE 3:

Sei $n = 55$. Entscheiden Sie für folgende $a \in \mathbb{N}$ ob a ein quadratischer Rest modulo n ist. Falls vorhanden, geben Sie alle Lösungen der Gleichung $b^2 = a \pmod{n}$ an (Quadratwurzeln von a).

Berechnen Sie dazu einer Liste aller Quadrate modulo jedem Teiler von n und lesen Sie daraus die Wurzeln modulo den Teilern ab. Setzen Sie diese dann mit dem Chinesischen Restsatz zu einer Wurzel modulo n zusammen.

Bestimmen Sie zudem jeweils das Jacobi-Symbol $\left(\frac{a}{n}\right)$. Führen Sie alle Berechnungen ohne Taschenrechner durch und geben Sie alle Zwischenschritte an.

(a) $a = 14$

(b) $a = 43$

Hinweis: Es gilt $11^{-1} = 1 \pmod{5}$ und $5^{-1} = -2 \pmod{11}$.

AUFGABE 4:

Wir betrachten das Blum-Goldwasser-Kryptosystem: Sei $pk = 77$ und $sk = (7, 11)$:

(a) Verschlüsseln Sie für $r = 5$ die Nachricht $m = (0, 1, 0)$.

(b) Entschlüsseln Sie den Ciphertext $c = (1, 0, 0, 9)$

Hinweis: Es gilt $25^2 = 9 \pmod{77}$ und $16^2 = 25 \pmod{77}$.