Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Ilya Ozerov

Hausübungen zur Vorlesung

Diskrete Mathematik II

SS 2012

Blatt 4 / 22. Mai 2012

Abgabe: 12. Juni 2012, 9 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Sei $G = (V, E)$ ein Graph. Ein Pfad in G, der jeden Knoten genau einmal enthält, heißt *Hamiltonscher Pfad*. Ein Kreis in G, der jeden Knoten genau einmal enthält, heißt *Hamiltonscher Kreis*. Wir definieren

$$\text{UH-Pfad} := \{G \mid G = (V, E) \text{ ungerichtet}, G \text{ besitzt einen } \textit{Hamiltonschen Pfad.}\}$$

$$\text{UH-Kreis} := \{G \mid G = (V, E) \text{ ungerichtet}, G \text{ besitzt einen } \textit{Hamiltonschen Kreis.}\}$$

Zeigen Sie UH-Pfad $\leq_p$ UH-Kreis.

Hinweis: Benutzen Sie UH-Pfad $\leq_p$ UH-st-Pfad aus der Präsenzübung und nutzen Sie aus, dass die Relation $\leq_p$ transitiv ist.

AUFGABE 2 (5 Punkte)**:**

Sei p prim und g ein Generator von $\mathbb{Z}_p^* := \{1, 2, \ldots, p-1\}$. 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 $p = 101$ und $g = 2$. Angenommen ein DDH-Orakel liefert uns:

$$(69, 75, 39),\ (39, 42, 57) \in \text{DDH},\ (59, 94, 29) \notin \text{DDH}$$

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

$$(69, 75, 42, 22),\ (69, 75, 42, 32),\ (39, 42, 19, 73),\ (39, 42, 17, 60),\ (59, 94, 7, 1)$$

Hinweis: Benutzen Sie die Reduktionsabbildung ElGamal $\leq_p$ DDH aus der Vorlesung.

AUFGABE 3 (5 Punkte)**:**

Sei $p = 79$. 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) $a = 5$

(c) $a = 15$

(d) $a = 65$

(e) $a = 77$

AUFGABE 4 (5 Punkte)**:**

Sei $n = 65$. Entscheiden Sie für folgende $a \in \mathbb{N}$ ob a ein quadratischer Rest modulo n ist. Falls vorhanden, geben Sie alle Lösungen der Gleichung $b^2 = a \bmod n$ 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) $a = 37$

(b) $a = 39$

(c) $a = 42$

(d) $a = 51$

(e) $a = 54$

Hinweis: Es gilt $13^{-1} = 2 \bmod 5$ und $5^{-1} = 8 \bmod 13$.