Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann

Hausübungen zur Vorlesung

Diskrete Mathematik 2
Einführung in die theoretische Informatik

Sommersemester 2014

Blatt 5 / 24./25. Juni 2014

Abgabe: 24. Juni 2014, 09:15 Uhr (vor der Vorlesung), Kasten NA 02

AUFGABE 1 (5 Punkte)**:**

Sei $n = 35$. Berechnen Sie das Jacobi-Symbol $\left(\frac{a}{n}\right)$ für die angegebenen $a \in \mathbb{N}$. Benutzen Sie ausschließlich die Rechenregeln auf Folie 101 und den Algorithmus auf Folie 102, d.h. führen Sie die Berechnung nicht auf die Berechnung des Legendre-Symbols zurück. Führen Sie alle Berechnungen ohne Taschenrechner durch und geben Sie alle Zwischenschritte an.

(a) $a = 16$

(b) $a = 8$

(c) $a = 54$

(d) $a = 10$

(e) $a = 34$

Hinweis: $(35^2 - 1)/8 = 153$

AUFGABE 2 (5 Punkte)**:**

Bestimmen Sie einen Huffman-Code zu einer erinnerungslosen Quelle Q über dem Alphabet $A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ mit jeweiligen Wahrscheinlichkeiten p_i für a_i, wobei

$$p_1 = \frac{43}{100}, p_2 = \frac{1}{10}, p_3 = \frac{4}{25}, p_4 = \frac{1}{25}, p_5 = \frac{19}{100}, p_6 = \frac{2}{25}$$

Ist dieser eindeutig? Was ist die erwartete Codewortlänge für Ihren Code?

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Gegeben seien die folgenden Zeichenmengen:

$$C_1 = \{11, 001, 101, 110, 0010, 1010, 1100, 1001, 00100, 01000, 10001, 11000, 10100\}$$
$$C_2 = \{11, 001, 101, 110, 0010, 1010, 1100, 0001, 00100, 01000, 10001, 11000, 10100\}$$

Handelt es sich jeweils um einen eindeutig entschlüsselbaren Code? Weisen Sie die Korrektheit Ihrer Antwort anhand von Definitionen oder Sätzen aus der Vorlesung nach.

AUFGABE 4 (5 Punkte)**:**

Gegeben folgendes Polynom $f(x) = x^3 + 5x + 3 \in \mathbb{Z}_{23}$. Berechnen Sie für die elliptische Kurve impliziert durch $f(x)$ und die Punkte $P_1 = (11, 3)$, $P_2 = (7, 17)$, $P_3 = (11, 20)$ folgendes:

(a) Alle Punkte auf der Kurve für $x = 15$.

(b) $P_1 + P_2$

(c) $P_1 - P_3$

Geben Sie dabei alle Rechenschritte an.