Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Hausübungen zur Vorlesung

Diskrete Mathematik II

SS 2011

Blatt 5 / 24. Mai 2011 / Abgabe **bis spätestens Dienstag 7. Juni, 09:00 Uhr**

AUFGABE 1:

Berechnen Sie die folgenden Jacobi-Symbole $(\frac{a}{b})$. Ist jeweils a quadratischer Rest modulo b? Falls ja, geben sie jeweils *alle* Quadratwurzeln von a modulo b an.

(a) $(\frac{101}{133})$ [2P]

(b) $(\frac{114}{133})$ [3P]

(c) $(\frac{84}{133})$ [3P]

(d) $(\frac{130}{133})$ [4P]

(e) $(\frac{33}{133})$ [3P]

(f) $(\frac{18}{47})$ [2P]

Bemerkungen: Ihre Lösung sollte ohne grossen Aufwand nachvollziehbar sein. (Modulo-Rechnungen mit 4-stelligen Zahlen sind OK).

$133 = 19 \cdot 7$
Für Rechnungen mit chinesichem Restsatz ist eventuell nützlich:
$-56 \bmod 7 = 0, \quad -56 \bmod 19 = 1$
$+57 \bmod 7 = 1, \quad +57 \bmod 19 = 0$

Bitte wenden!

AUFGABE 2:

Zeigen Sie:

(a) Für a, b beliebig, $n > 0$ ungerade (nicht notwendigerweise prim) gilt für die Jacbobi-Symbole: $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$. [2.5P]

(b) Für beliebiges ungerades n (nicht notwendigerweise prim) gilt: $\{a \in \mathbb{Z}_n^* \mid (\frac{a}{n}) = 1)\}$ ist eine Untergruppe von $(\mathbb{Z}_n^*, \cdot)$. [2.5P]

Hinweis zu (a): Die entsprechende Aussage wurde für Legendre-Symbole (d.h. für den Fall, dass n prim ist) in der Vorlesung gezeigt. Führen sie die Aussage auf diesen Fall zurück,

AUFGABE 3:

(a) Sei $n > 0$ ungerade, nicht notwendigerweise prim, $a, b \in \mathbb{Z}_n^*$ mit a quadratischer Rest modulo n, b quadratischer Nichtrest modulo n.
Zeigen Sie: $a \cdot b$ ist quadratischer Nichtrest modulo n. [3P]

(b) Sei $p > 0$ ungerade Primzahl und $a, b \in \mathbb{Z}_p^*$ quadratische Nichtreste modulo p.
Zeigen Sie: $a \cdot b$ ist quadratischer Rest modulo p. [2P]

(c) Zeigen Sie, dass die Aussage in Teil b) falsch wird, wenn man nicht verlangt, dass p Primzahl ist, indem Sie ein Gegenbeispiel angeben.
(d.h. finden Sie n, a, b mit n ungerade $a, b \in \mathbb{Z}_n^*$, so dass sowohl a, b als auch ab quadratische Nichtreste modulo n sind.) [2P]

Hinweise: Obwohl die Aussagen in (a) und (b) recht ähnlich klingen, sind (jedenfalls die Muster-)Lösungen recht verschieden.
Zu (a): Benutzen Sie, dass die quadratischen Reste eine Untergruppe bilden (Präsenzübung). Sie dürfen folglich verwenden, dass für ungerade n und $a, b \in \mathbb{Z}_n^*$ quadratische Reste modulo n auch $a \cdot b$ und a^{-1} quadratische Reste modulo n sind.
Zu (b): Benutzen Sie Legendre/Jacobi-Symbole.