Universität Bielefeld **Wintersemester 2013/14**
C. Huck

Übungen zur Vorlesung
Diskrete Mathematik
Blatt 13 (Letztes Übungsblatt)

Aufgabe 1 (Satz von Wilson)
Sei p eine Primzahl. Zeigen Sie die Gültigkeit der Kongruenz

$$(p-1)! \equiv -1 \pmod{p}.$$

Hinweis. Anders gesagt ist also die Gültigkeit der Gleichung $\prod_{x \in \mathbb{Z}_p^*} x = -1$ in $\mathbb{Z}_p$ zu zeigen. Dazu überlege man sich, welche Elemente in $\mathbb{Z}_p^*$ zu sich selbst invers sind.

(4 Punkte)

Aufgabe 2
Verschlüsseln Sie die Nachricht "X" mit dem RSA-System unter Verwendung des öffentlichen Schlüssels $n = 65$, $k = 5$. Berechnen Sie dann den geheimen Schlüssel m und entschlüsseln Sie die verschlüsselte Nachricht.

Hinweis. Vermeiden Sie bei der Ver- und Entschlüsselung das Rechnen mit großen Zahlen.

(4 Punkte)

Aufgabe 3
Folgende Botschaft ist mit dem RSA-Verfahren verschlüsselt: 13715 178394. Der öffentliche Schlüssel ist $n = pq = 262699$, $k = 211$. Übernehmen Sie die Rolle eines Aggressors und entschlüsseln Sie die Botschaft.

Hinweis. Jeder Block steht für drei Buchstaben. Wie üblich bedeutet 01: A, 02: B, ..., 26: Z, 00: Leerzeichen. Computereinsatz (z.B. Maple) ist ausdrücklich erlaubt. Geben Sie keinen Programmcode ab, aber beschreiben Sie, wie Sie vorgehen (Screenshots etc.).

(3 Punkte)

Aufgabe 4
Sei $n > 1$ keine Primzahl. Zeigen Sie, dass $\mathbb{Z}_n$ kein Körper ist.

Hinweis. Beweis durch Widerspruch. Nehmen Sie also an, dass sämtliche Elemente von $\mathbb{Z}_n^*$ ein multiplikatives Inverses haben.

(3 Punkte)

Aufgabe 5
Sei p eine Primzahl. Zeigen Sie, dass Zahlen der Form $(x+y)^p - x^p - y^p$, wobei $x, y \in \mathbb{Z}$, stets durch p teilbar sind. Modulo p gilt also

$$(x+y)^p \equiv x^p + y^p.$$

Hinweis. Satz von Fermat.

(2 Punkte)

Abgabe bis Freitag, 31.01.2014, 10.00 Uhr, in den Postfächern der Tutoren im Kopierraum V3-128