Mathematisches Institut
der Universität München
Helmut Schwichtenberg

Sommersemester 2008
Blatt 7

Übungen zur Vorlesung „Diskrete Strukturen“

Aufgabe 25. (a) Man bestimme den Rest von 3^{100} bei Division durch 8.
(b) Man bestimme den Rest von 6! bei Division durch 7 und von 7! bei Division durch 8.
(c) Sei $n \in \mathbf{N}$. Man bestimme den Rest von $n!$ bei der Division durch $n+1$, falls $n+1$ keine Primzahl ist.

Aufgabe 26. Sei $m_1 := 7$, $m_2 := 8$, $m_3 := 9$. Man löse die folgenden beiden Kongruenzensysteme
(a) $x \equiv 2 \mod 7$, $x \equiv 4 \mod 8$, $x \equiv 1 \mod 9$,
(b) $x \equiv 5 \mod 7$, $x \equiv 1 \mod 8$, $x \equiv 3 \mod 9$.

Aufgabe 27. Sei A ein Integritätsbereich und $a, b \in A$. Man zeige: $(a) = (b)$ gilt genau dann, wenn es ein $u \in A^*$ gibt mit $a = ub$.

Aufgabe 28. Es seien $p := 7$ und $q := 11$, also $N := pq = 77$.
(a) Man wähle einen privaten Schlüssel k mit $\mathrm{ggT}(\varphi(N), k) = 1$, und bestimme dazu einen passenden öffentlichen Schlüssel a (Hinweis: mit Hilfe des Euklidischen Algorithmus sind a, b zu finden mit $ak + b\varphi(N) = 1$).
(b) Man verschlüssele die Nachricht $m := 42$.
(c) Man entschlüssele die in (b) erhaltene Kodierung mit Hilfe des privaten Schlüssels k.

Abgabe. Dienstag, 17. Juni 2008, 14:15 Uhr, Briefkasten im 1. Stock