Universität Bielefeld

Peter Zeiner
Fakultät für Mathematik

Bielefeld, 16.1.2015

Wintersemester 2014/15

Diskrete Mathematik

Übungszettel 12

Aufgabe 61: Lösen Sie das folgende System von Kongruenzen:

$$x \equiv 3 \pmod 4$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 5 \pmod 7$$

(4 Punkte)

Aufgabe 62: Sei k die Ordnung von a modulo m. Zeigen Sie:

(a) $a^h \equiv 1 \pmod m$ genau dann, wenn $k|h$.

(b) $a^i \equiv a^j \pmod m$ genau dann, wenn $i \equiv j \pmod k$.

(c) Die Restklassen $[a]_m, [a^2]_m, \dots, [a^k]_m$ sind paarweise verschieden.

(d) $\mathrm{ord}_m(a^h) = \frac{k}{\mathrm{ggT}(h,k)}$.

(e) $\mathrm{ord}_m(a^h) = k$ genau dann, wenn $\mathrm{ggT}(h,k) = 1$. **(1+1+1+2+1 Punkte)**

Aufgabe 63: Zeigen Sie:

(a) Für beliebiges n gilt: $2730 \mid (n^{13} - n)$.
Hinweis: Bestimmen Sie die Primfaktorzerlegung von 2730 und beweisen Sie die Teilbareit für jeden Primfaktor separat.

(b) $6^{30} - 6^{18} - 6^{12} + 1$ ist durch 247 teilbar.
Hinweis: analog zu oben. **(2+2 Punkte)**

Aufgabe 64: Seien p, q zwei Primzahlen. Ist es schwierig, die Primzahlen p, q zu bestimmen, wenn man nur $n = pq$ und $\varphi(n)$ kennt? **(2 Punkte)**

Aufgabe 65*: Dieselbe Botschaft m werde zweimal mit dem RSA-Verfahren verschlüsselt, einmal mit (n, s_1) und einmal mit (n, s_2) – die RSA-Moduln sind also beide Male gleich. Zeigen Sie, dass man die Botschaft leicht entschlüsseln kann, wenn man die verschlüsselten Botschaften c_1, c_2 kennt und s_1 und s_2 teilerfremd sind. **(3 Bonuspunkte)**

Abgabe bis zum 23.1.2015!