Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

Sommersemester 2000
21. Juni 2000

Übungen zur Kryptologie

10. Übung

Abgabe am 12. Juli 2000

Aufgabe 35

a) Zeigen Sie, dass für jedes $a \in \mathbb{Z}_m^*$ ein $k > 0$ existiert mit $a^k \equiv 1 \pmod{m}$.

b) Sei nun $\mathrm{ord}_m(a) = k$. Zeigen Sie, dass die Menge

$$\{a^0 \bmod m, a^1 \bmod m, a^2 \bmod m, \ldots\}$$

eine Untergruppe von $\mathbb{Z}_m^*$ mit genau k Elementen bildet. Folgern Sie $k|\varphi(m)$.

c) Zeigen Sie $a^i \equiv 1 \pmod{m}$ genau dann, wenn $i|\mathrm{ord}_m(a)$.

Aufgabe 36

Lösen Sie die folgenden Systeme von linearen Kongruenzen.

a) $\begin{aligned} x &\equiv 4 \pmod{11} \\ x &\equiv 3 \pmod{17} \end{aligned}$ b) $\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned}$ c) $\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 6 \pmod{7} \end{aligned}$

Aufgabe 37

Berechnen Sie $\varphi(75\,600)$, $\varphi(14\,948)$, $\log_{7,3} 4$, $\log_{37,2} 3$, $\mathrm{ord}_7(2)$ und $\mathrm{ord}_{31}(2)$.

Aufgabe 38

Seien $m_1, \ldots, m_{n+1} \in I\!N$. Sei $g_i = \mathrm{ggT}(m_i, m_{n+1})$, $i = 1, \ldots, n$. Zeigen Sie

$$\mathrm{kgV}(g_1, \ldots, g_n) = \mathrm{ggT}(\mathrm{kgV}(m_1, \ldots, m_n), m_{n+1}).$$

Aufgabe 39

a) Welche der folgenden Systeme von linearen Kongruenzen sind lösbar? Bestimmen Sie gegebenenfalls die Lösung.

1) $\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{6} \end{aligned}$ 2) $\begin{aligned} x &\equiv 4 \pmod{6} \\ x &\equiv 13 \pmod{15} \end{aligned}$ 3) $\begin{aligned} x &\equiv 5 \pmod{6} \\ x &\equiv 3 \pmod{10} \\ x &\equiv 8 \pmod{15} \end{aligned}$

b) Zeigen Sie, dass das System von linearen Kongruenzen

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

genau dann lösbar ist, wenn $\mathrm{ggT}(m_1, m_2)|(a_1 - a_2)$. Zeigen Sie: wenn eine Lösung existiert, dann ist sie eindeutig modulo $\mathrm{kgV}(m_1, m_2)$.

c) Zeigen Sie, dass das System von linearen Kongruenzen

$$x \equiv a_i \pmod{m_i} \quad i = 1, \ldots n$$

genau dann lösbar ist, wenn $\mathrm{ggT}(m_i, m_j) | (a_i - a_j)$ für alle Paare (i, j) mit $1 \leq i < j \leq n$. Zeigen Sie: wenn eine Lösung existiert, dann ist sie eindeutig modulo $\mathrm{kgV}(m_1, m_2, \ldots, m_n)$.

Hinweis: Führen Sie einen Induktionsbeweis und verwenden Sie Aufgabe 39.