Übungsblatt 15

Aufgabe 74 ***mündlich***

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

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

Aufgabe 75 ***mündlich***

Betrachten Sie für $a_1, \ldots, a_n \in \mathbb{Z}$ und $m_1, \ldots, m_n \in \mathbb{N}$ folgendes System von linearen Kongruenzen:

$$x \equiv_{m_i} a_i, \quad i = 1, \ldots, n \quad (*)$$

(a) Zeigen Sie, dass das Kongruenzgleichungssystem $(*)$ höchstens eine Lösung modulo $\text{kgV}(m_1, \ldots, m_n)$ hat.

(b) Zeigen Sie, dass das System $(*)$ genau dann lösbar ist, wenn für alle $1 \leq i < j \leq n$ die Zahl $\text{ggT}(m_i, m_j)$ ein Teiler von $(a_i - a_j)$ ist.

Hinweis: Führen Sie einen Induktionsbeweis und verwenden Sie Aufgabe 74.

Aufgabe 76 ***mündlich***

Wir betrachten das ElGamal-System über der Gruppe $\mathbb{F}_{27}^*$, wobei wir zur Konstruktion des Körpers $\mathbb{F}_{27}$ das irreduzible Polynom $m(x) = x^3 + 2x^2 + 1$ benutzen. Angenommen, wir wählen als Erzeuger das Element $\alpha = x$ und als privaten Schlüssel $a = 11$. Wie lässt sich damit der Kryptotext

$$y = (K, H)(P, X)(N, K)(H, R)(T, F)(V, Y)(E, H)(F, A)(T, W)(J, D)(U, J)$$

entschlüsseln, wenn wir die 25 Zeichen $A, \ldots, Z$ der Reihe nach mit den Körperelementen $1, 2, x, x + 1, x + 2, 2x, \ldots, 2x^2 + 2x + 2$ kodieren?