Übungen zur Angewandten Diskreten Mathematik

Prof. Dr. Helmut Maier, Dr. Hans- Peter Reck

Gesamtpunktzahl: 24 Punkte

Abgabe: Freitag, 6. Februar 2015, vor den Übungen

1. Satz 1.18.3 lässt sich nun verallgemeinern, um einer Zahl eine beliebige Wurzel modulo m zu ziehen. Es seien $m \in \mathbb{N}$ und $b, k \in \mathbb{Z}$ mit $ggT(b, m) = 1$ und $ggT(k, \varphi(m)) = 1$ sowie die Kongruenz

$$x^k \equiv b \bmod m$$

gegeben.

   (a) Zeige, dass dann $x \equiv b^u \bmod m$ eine Lösung dieser Kongruenz darstellt, wobei u über die Diophantische Gleichung $ku - \varphi(m)v = 1$ mit $u, v \in \mathbb{Z}$ gegeben ist.

   (b) Finde eine Lösung der Kongruenz $x^7 \equiv 2 \bmod 437$. (5 Punkte)

2. Claudius und Frank wollen beide einer dritten Person Lars Nachrichten versenden. Lars veröffentlicht seinen öffentlichen Schlüssel $S = (e, n)$ mit $e = 31$ und $n = 437$.

   (a) Prüfe, ob die Voraussetzungen für das RSA- Verfahren vorliegen.

   (b) Frank möchte die Botschaft $B = 21$ verschlüsselt an Lars senden. Welchen Wert C schickt er weiter?

   (c) Von Claudius erhält Lars die Botschaft $C = 410$. Was war die ursprüngliche Information?

   Hinweis:
   Nutze das Ergebnis von Aufgabe 1. (8 Punkte)

3. (a) Es sei K ein Körper und $f \in K[X]$ vom Grad 2 oder 3. Zeige, dass f in $K[X]$ genau dann irreduzibel ist, wenn f keine Nullstelle in $K[X]$ hat.

   (b) Zeige, dass $f(X) = X^2 + \overline{1}$ über $K = \mathbb{F}_3$ irreduzibel ist.

   (c) Bestimme ein irreduzibles Polynom dritten Grades über $K = \mathbb{F}_2$.

   (d) Stelle eine Additionstafel des Körpers mit neun Elementen und eine Multiplikationstafel des Körpers mit acht Elementen auf. (11 Punkte)