TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik und Naturwissenschaften, Fachrichtung Mathematik, Institut für Algebra

Prof. Ulrike Baumann Henri Mühle Wintersemester 2017/18

7. Übungsblatt zur Vorlesung "Algebra für Informationssystemtechniker"

Multiplikative Inverse, RSA

Ü37. (a) Berechnen Sie für die folgenden Elemente $x \in \mathbb{Z}_n$ das multiplikative Inverse modulo n, falls es existiert.

$$\text{(i) } x = 18,\ n = 31, \qquad \text{(ii) } x = 60,\ n = 257,$$
$$\text{(iii) } x = 511,\ n = 1001, \quad \text{(iv) } x = 512,\ n = 1001.$$

(b) Geben Sie die Lösungsmengen der folgenden Kongruenzen an.

$$\text{(i) } 5x \equiv 1 \pmod 7, \quad \text{(ii) } 32x \equiv 14 \pmod{82}, \quad \text{(iii) } 10x \equiv 9 \pmod{25}.$$

Hinweis: Es gibt eine Regel zur Modulo-Rechnung, mit deren Hilfe die Kongruenz in (ii) geeignet umgeformt werden kann.

Ü38. Finden Sie für die folgenden natürlichen Zahlen n alle Einheiten des Restklassenrings $\mathbb{Z}_n$.

$$\text{(i) } n = 12, \quad \text{(ii) } n = 21, \quad \text{(iii) } n = 30, \quad \text{(iv) } n = 1009, \quad \text{(v) } n = 1024.$$

Ü39. (a) Zum Verschlüsseln eines Textes verwenden wir das RSA-Verfahren. Wir codieren die Buchstaben A, B, ..., Z mit den Zahlen $0, 1, \ldots, 25$. Verschlüsseln Sie den Klartext GEHEIM mit den öffentlichen Schlüsseln

$$\text{(i) } (n, e) = (33, 3), \quad \text{(ii) } (n, e) = (15, 5).$$

(b) Es wurde die mit dem RSA-Verfahren verschlüsselte Nachricht QUTCIM zum öffentlichen Schlüssel $(n, e) = (21, 5)$ abgefangen. Wie kann diese Nachricht entschlüsselt werden? Wie lautet die entschlüsselte Nachricht?

H40. (a) Geben Sie alle zu 8 teilerfremden Zahlen in $\mathbb{Z}_8$ an. Wie viele Zahlen in $\mathbb{Z}_{80}$ sind zu 80 teilerfremd?

(b) Berechnen Sie mit dem erweiterten Euklidischen Algorithmus die multiplikativen Inversen zu $a = 33$, $b = 34$ und $c = 35$ in $\mathbb{Z}_{80}$, falls diese existieren.

(c) Berechnen Sie alle Lösungen der Gleichung $33x = 15$ in $\mathbb{Z}_{80}$.

(d) Bestimmen Sie die Anzahl der Lösungen der Gleichungen $11x = 5$ und $66x = 30$ in $\mathbb{Z}_{80}$.

H41. Zeigen Sie, dass $x \in \mathbb{Z}_8$ genau dann ein multiplikatives Inverses besitzt, wenn es zu sich selbst invers ist, d.h. wenn $x^2 \equiv 1 \pmod 8$ gilt.

H42. Auf einer Insel leben r rote, g grüne und b blaue Chamäleons. Treffen sich zwei verschiedenfarbige Chamäleons, ändern sie beide ihre Farbe in die dritte Farbe. Begegnen sich zwei gleichfarbige Chamäleons, ändern sie ihre Farbe nicht.

(a) Sei $r = 1$, $g = 2$, $b = 4$. Gibt es eine Folge von (paarweisen) Begegnungen, sodass am Ende alle Chamäleons die gleiche Farbe besitzen?

(b) Sei $r = 13$, $g = 15$, $b = 17$. Gibt es eine Folge von (paarweisen) Begegnungen, sodass am Ende alle Chamäleons die gleiche Farbe besitzen?

Hinweis: Modellieren Sie die Farben als Elemente des Restklassenrings $\mathbb{Z}_3$ und überlegen Sie, was bei einer Begegnung passiert.