Diskrete Mathematik

9. Übungsblatt

Präsenzübungen

Aufgabe P9.1 (Chinesischer Restsatz) Bestimmen Sie das Inverse von 7 modulo $288 = 32 \cdot 9$. Gehen Sie dazu wie folgt vor:

a) „Erraten“ Sie die Inversen von 7 modulo 9 und modulo 32.

b) Setzen Sie die beiden Werte mit dem chinesischen Restsatz zusammen.

Hinweis: In (a) suchen Sie ein Vielfaches von 7, dass sich um 1 unterscheiden von einem Vielfachen von 9 bzw. 32. Der Faktor von 7 ist bis auf Vorzeichen das gewünschte Inverse. Auch die Koeffizienten für (b) können Sie (bzw. haben Sie bereits) erraten.

Aufgabe P9.2 (Multiplikative Funktionen)

Wir definieren die Funktion

$$f\colon \mathbb{N}_{>0} \to \mathbb{N}_{>0}$$
$$f(n) = \begin{cases} 0 & 5 \mid n \\ \mu(n) & \text{sonst} \end{cases}$$

(wobei μ die Möbius-Funktion ist). Zeigen Sie, dass

$$\sum_{d|n} f(d) = \begin{cases} 1 & n \text{ ist eine Potenz von 5} \\ 0 & \text{sonst.} \end{cases}$$

Hinweis: Verwenden Sie Möbius-Inversion.

Hausübungen

Aufgabe H9.1 (Simultane Kongruenzen)

Benutzen Sie den chinesischen Restsatz um die simultanen Kongruenzen

$$3x \equiv 9 \mod 11 \qquad 4x \equiv 8 \mod 12 \qquad 5x \equiv 7 \mod 13$$

zu lösen. Das heißt, finden Sie eine Restklasse $x+1716\mathbb{Z}$, so dass x alle Kongruenzen gleichzeitig löst.

(3 Punkte)

Aufgabe H9.2 (RSA)

Alice hat sich die beiden Primzahlen 17 und 19 ausgesucht und als öffentlichen Schlüssel $(323, 7)$ gewählt.

a) Was ist Alices privater Schlüssel?

b) Bob möchte Alice die Nachricht „20“ übermitteln. Wie lautet die verschlüsselte Botschaft?

c) Von Carol hat Alice die verschlüsselte Nachricht „35“ erhalten. Wie lautet der Klartext?

(2+2+2 Punkte)

Aufgabe H9.3 (Projektive Ebenen) Eine *projektive Ebene* besteht aus einer Menge P von *Punkten* und einer Menge $L \subseteq \mathfrak{P}(P)$ von *Linien* so dass folgende Axiome gelten:

- Für je zwei Punkte p, q gibt es genau eine Linie $\ell \in L$ mit $p, q \in \ell$.
- Für je zwei Linien $\ell, m \in L$ gibt es genau einen Punkt $p \in P$ mit $p \in \ell \cap m$.
- Es gibt vier Punkte, so dass keine Linie mehr als zwei davon enthält.

Eine Menge $D \subseteq \mathbb{Z}/n\mathbb{Z}$ ist eine Differenzmenge wenn für jedes $a \in \mathbb{Z}/n\mathbb{Z} \setminus \{0 + n\mathbb{Z}\}$ genau ein Paar $(d, e) \in D \times D$ existiert mit $a = d - e$.

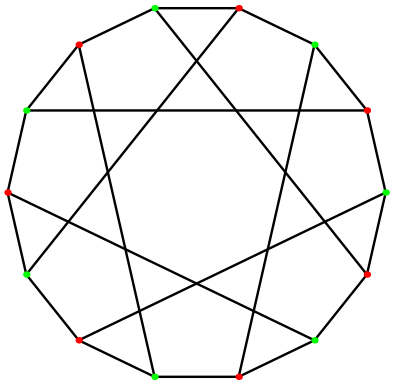
a) Sei $D \subseteq \mathbb{Z}/n\mathbb{Z}$ eine Differenzmenge. Wir setzen $P = \mathbb{Z}/n\mathbb{Z}$ und

$$L = \{\{b + d \mid d \in D\} \mid b \in \mathbb{Z}/n\mathbb{Z}\}.$$

Zeigen Sie, dass P und L eine projektive Ebene bilden.

b) Finden Sie eine Differenzmenge in $\mathbb{Z}/7\mathbb{Z}$.

(2+2 Punkte)



Aufgabe H9.4 (RSA vervollständigt)

In der Vorlesung haben wir gezeigt, dass für das RSA-Verfahren gilt

$$m^{ed} \equiv m \mod n$$

wenn $m \perp n$. Zeigen Sie, dass diese Kongruenz auch sonst gilt.

Hinweis: Wenn m nicht relativ prim zu n ist wird m entweder von p oder von q geteilt. Schließen Sie nun am einfachsten mit dem chinesischen Restsatz. **(3 Punkte)**

Abgabe bis 15.1.2016.