Diskrete Mathematik

8. Übungsblatt

Präsenzübungen

Aufgabe P8.1 (Lateinische Quadrate)

Ein *lateinisches Quadrat* ist ein $n \times n$-Gitter aus n verschiedenen Symbolen $s_1, \ldots, s_n$, so dass jedes Symbol in jeder Zeile und jeder Spalte genau einmal auftaucht. Ein Beispiel für ein lateinisches Quadrat ist:

L	E	Q	T	N	A	I
A	I	L	E	Q	T	N
T	N	A	I	L	E	Q
E	Q	T	N	A	I	L
I	L	E	Q	T	N	A
N	A	I	L	E	Q	T
Q	T	N	A	I	L	E

Zwei lateinische Quadrate $(a_{i,j})_{i,j}$ und $(b_{i,j})_{i,j}$ heißen *orthogonal*, wenn die Paare $(a_{i,j}, b_{i,j})$ alle verschieden sind (folglich muss unter diesen Paaren jedes Paar (s_k, s_ℓ) genau einmal auftreten). Zum Beispiel ist das folgende lateinische Quadrat orthogonal zu dem Quadrat oben:

L	I	A	N	T	Q	E
A	N	T	Q	E	L	I
T	Q	E	L	I	A	N
E	L	I	A	N	T	Q
I	A	N	T	Q	E	L
N	T	Q	E	L	I	A
Q	E	L	I	A	N	T

a) Sei $n \in \mathbb{N}$ beliebig und sei u invertierbar modulo n. Zeigen Sie, dass das Gitter $(a_{i,j})_{0 \le i,j \le n-1} \in \{0, \ldots, n-1\}^{n \times n}$ ein lateinisches Quadrat ist, wenn man $a_{i,j} \equiv u \cdot i + j \mod n$ wählt.

b) Sei n prim und $u \not\equiv u' \mod n$. Zeigen Sie, dass die beiden Quadrate, die man wie in (a) für die Paare (n, u) und (n, u') erhält zueinander orthogonal sind.

Hausübungen

Aufgabe H8.1 (Kongruenzen lösen)

a) Bestimmen Sie die Inversen von $37 + 1023\mathbb{Z}$, $49 + 2048\mathbb{Z}$.

b) Lösen Sie die Kongruenzen $8x \equiv 53 \mod 81$ und $17x \equiv 30 \mod 104$.

c) Bestimmen Sie alle Lösungen der Kongruenzen $37x \equiv 111 \mod 185$ und $37x \equiv 100 \mod 185$.

(2+2+4 Punkte)

Aufgabe H8.2 (Einheiten)

Hier bezeichnet ϕ die Eulersche ϕ-Funktion.

a) Bestimmen Sie $\phi(30)$, $\phi(31)$, $\phi(32)$. Bestimmen Sie die Elemente von $(\mathbb{Z}/30\mathbb{Z})^\times$.

b) Zeigen Sie, dass für ganze Zahlen n, k gilt: wenn n und k relativ prim sind, dann auch $n - k$ und n. Folgern Sie, dass $\phi(n)$ gerade ist für $n \geq 3$.

(2+3 Punkte)

Aufgabe H8.3 (Verschlüsselung)

Wir betrachten das folgende Verschlüsselungsverfahren: Die Buchstaben A bis Z werden mit den Zahlen 0 bis 25 identifiziert: $A = 0$, $B = 1, \ldots, Z = 25$. Ein Schlüssel ist ein Paar (u, a) mit $u \in (Z/26\mathbb{Z})^\times$ und $a \in Z26\mathbb{Z}$. Der Klartext $p_0, \ldots, p_n$ wird verschlüsselt in den Text $c_0, \ldots, c_n$ mit der Funktion

$$c_i = u \cdot p_i + a + p_{i-1}.$$

(Hierbei wird $p_{-1} = 0$ gesetzt.)

a) Bestimmen Sie die Entschlüsselungsfunktion, die die p_i aus den c_i berechnet.

b) Alice und Bob haben sich auf den Schlüssel $(7, 10)$ geeinigt. Alice schickt Bob den verschlüsselten Text „ASLTSY“. Was will sie Bob mitteilen?

(2+2 Punkte)

Abgabe bis 18.12.2015.