



Einführung in die Mathematik für Informatiker WS 2009/10
Vorlesung Diskrete Strukturen

6. Übungsblatt für die Woche 23.11. - 27.11.2009

Gruppen, Euler-Fermat

DS-Ü31 (a) Finden Sie in $\text{GF}(13)$ alle primitiven Elemente. Geben Sie zu allen Elementen das multiplikativ Inverse an.

(b) Zeigen Sie, dass allgemein in \mathbb{Z}_n gilt: $n - 1$ ist zu sich selbst multiplikativ invers.

DS-Ü32 (a) Ermitteln Sie:

(i) $7^{469} \pmod{11}$ (ii) $11^{965} \pmod{13}$ (iii) $5^{643} \pmod{1122}$

(b) Zeigen Sie, dass für alle $m \in \mathbb{N}$

- m^{13} und m im Dezimalsystem die gleiche Endziffer haben.
- $\frac{1}{5}m^5 + \frac{1}{3}m^3 + \frac{7}{15}m$ eine natürliche Zahl ist.

DS-Ü33 Untersuchen Sie die Gruppe $G = \{s_1, s_2, s_3, s_4, s_5, s_6\}$ mit der folgenden Verknüpfungstafel.

\circ	s_1	s_2	s_3	s_4	s_5	s_6
s_1	s_1	s_2	s_3	s_4	s_5	s_6
s_2	s_2	s_3	s_1	s_6	s_4	s_5
s_3	s_3	s_1	s_2	s_5	s_6	s_4
s_4	s_4	s_5	s_6	s_1	s_2	s_3
s_5	s_5	s_6	s_4	s_3	s_1	s_2
s_6	s_6	s_4	s_5	s_2	s_3	s_1

(a) Geben Sie alle Untergruppen von G an.

(b) Ermitteln für eine nichttriviale Untergruppe alle Nebenklassen.

DS-H34 (a) Ermitteln Sie:

(i) $2^{3610} \pmod{1001}$ (ii) $19^{255} \pmod{51}$ (iii) $46^{5637} \pmod{47}$

(b) Für welche $a \in \{0, 1, 2, \dots, 16\}$ gilt $a^{1025} \equiv a \pmod{17}$?

DS-H35 Wir betrachten die Gruppe $D = \{a, b, c, d, e, f, g, h\}$ mit der folgenden Verknüpfungstafel.

\circ	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	f	g	h	d
b	b	c	e	a	g	h	d	f
c	c	e	a	b	h	d	f	g
d	d	h	g	f	e	c	b	a
f	f	d	h	g	a	e	c	b
g	g	f	d	h	b	a	e	c
h	h	g	f	d	c	b	a	e

- (a) Geben Sie alle Untergruppen von D an.
 (b) Ermitteln für eine nichttriviale Untergruppe alle Nebenklassen.

DS-H36 Anne und Ben möchten abhörsicher miteinander kommunizieren und wollen sich dafür auf einen gemeinsamen Schlüssel einigen. Sie haben sich (öffentlich) darauf geeinigt, modulo $n = 1031$ zu rechnen.

Anne wählt für sich $a = 76$ und Ben $b = 34$.

Anne sendet an Ben $A = 2^a \bmod n$, Ben sendet an Anne $B = 2^b \bmod n$.

Ermitteln Sie mittels Square and Multiply die Zahlen A , B und den gemeinsamen Schlüssel.