TECHNISCHE UNIVERSITÄT DRESDEN

Bereich Mathematik und Naturwissenschaften, Fakultät Mathematik, Institut für Algebra

Jun.-Prof. Friedrich Martin Schneider, Dr. Henri Mühle. Wintersemester 2018/19

10. Übungsblatt zur Vorlesung "Diskrete Strukturen für Informatiker"

Gruppen

V. Vervollständigen Sie die nachstehende Verknüpfungstafel, sodass die Menge $\{a, b, c, d\}$ mit der durch die Tafel gegebenen Operation eine Gruppe bildet. Wie viele Möglichkeiten gibt es?

$\circ$	a	b	c	d
a	a	b	c	d
b	b			
c	c		a	
d	d			

Ü55. (a) Berechnen Sie $(24 \cdot 12)^{2018} \pmod{101}$.

(b) Berechnen Sie $13^{469} \pmod{11}$ und $7^{967} \pmod{18}$ ohne Square-and-Multiply.

(c) Zeigen Sie, dass für zwei beliebige Primzahlen p, q, mit $p \neq q$, und für jede Zahl $a \in \mathbb{Z}$, die nicht durch p oder q teilbar ist, gilt:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p \cdot q}.$$

Ü56. (a) Es sei $(\mathbb{Z}_{14}^*, \cdot)$ die Gruppe der Einheiten des Restklassenrings $(\mathbb{Z}_{14}, +, \cdot)$.

(i) Stellen Sie die Verknüpfungstafel für $(\mathbb{Z}_{14}^*, \cdot)$ auf.

(ii) Für welche $k \in \mathbb{N}$ kann $(\mathbb{Z}_{14}^*, \cdot)$ Untergruppen der Ordnung k besitzen?

(iii) Finden Sie alle Untergruppen von $(\mathbb{Z}_{14}^*, \cdot)$ und geben Sie deren Ordnung an.

(iv) Bestimmen Sie die Menge der Linksnebenklassen $\{k \cdot U \mid k \in \mathbb{Z}_{14}^*\}$ für eine nichttriviale Untergruppe U von $(\mathbb{Z}_{14}^*, \cdot)$.

(b) Es sei $(G, \circ)$ eine Gruppe. Zeigen Sie, dass für jedes $g \in G$ und jede Teilmenge $U \subseteq G$ die zugeordnete Abbildung $f\colon U \to g \circ U$ mit $f(u) = g \circ u$ bijektiv ist.

Ü57. Für $n > 2$ bezeichne $\mathfrak{D}_n$ die *Diedergruppe* der Ordnung $2n$. Dies ist die Symmetriegruppe eines regulären n-Ecks in der Ebene bzgl. der Hintereinanderausführung. Sie besteht also aus allen Spiegelungen und Drehungen, die das n-Eck auf sich selbst abbilden.

55) Satz von Fermat: falls $ggT(a,n)=1$ dann gilt $a^{\varphi(n)} \equiv 1 \pmod n$

$(24\cdot 12)^{1018} \pmod{101}$

$24\cdot 12 \equiv 288 \equiv 86 \pmod{101}$

$\varphi(101) = 100$

$ggT(86,101)=1 \Rightarrow (86)^{18} \pmod{101}$ $\quad 18=[10010]_2$

$18 = 1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 0\cdot 2^0$

$86^{(2\cdot 2\cdot 2+1)\cdot 2} \pmod{101}$

10
100
1000
10001
100010

Setze $c_5 = 1$

$b_4=1$	$d_4 \equiv c_5^2 \equiv 1$	$c_4 \equiv d_4 \cdot a^{b_4} \equiv 86$
$b_3=0$	$d_3 \equiv c_4^2 \equiv 23$	$c_3 \equiv d_3 a^{b_3} \equiv 23$
$b_2=0$	$d_2 \equiv c_3^2 \equiv 24$	c_2 24
$b_1=1$	$d_1 \equiv c_2^2 \equiv 71$	c_1 46
$b_0=0$	$d_0 \equiv c_1^2 \equiv 96$	$c_0 \equiv d_0 a^{b_0} \equiv 96$

b) $13^{469} \quad 13 \equiv 2 \pmod{11} \quad ggT(2,11)=1 \quad \varphi(11)=10 \quad 469 \equiv 9 \pmod{10}$

$\Rightarrow 13^{469} \equiv 2^9 \equiv 512 \equiv 6 \pmod{11}$

$7^{967} \pmod{18}$

$ggT(7,18)=1 \quad \varphi(18)=6 \quad 967 \equiv 1 \pmod 6$

$7^{967} \equiv 7 \pmod{18}$

c) p,q bel. Primzahl $p \neq q$

z.z.! $\forall a \in \mathbb{Z} \quad p \nmid a \quad q \nmid a: \quad a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

$\varphi(p\cdot q) = p\cdot q\,(1-\frac{1}{p})(1-\frac{1}{q}) = (p-1)(q-1)$

$p \nmid a \wedge q \nmid a \Rightarrow ggT(a,pq)=1 \overset{\text{Fermat}}{\Rightarrow} a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

56) $\mathbb{Z}_{14}^* := \{1,3,5,9,11,13\}$

·	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	10
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	10	9	5	3	1

ii) Satz von Lagrange $(\mathbb{Z}_{14}^*, \cdot)$ hat Untergruppe der Ordnung k
$\Leftrightarrow$ k Teiler von $|\mathbb{Z}_{14}^*|$

$|\mathbb{Z}_{14}^*| = 6 \Rightarrow$ Es ex. Untergruppen der Ordnung 1, 2, 3 und 6

iii) Ordnung

1. triviale UG $M_1 = \{1\}$
2. UG von Ord 2. enthalten neutrales und 1 Element. dass zu sich selbst inverse ist
   $M_2 = \{1, 13\}$
3. UG besitzen NE und 2 Element. die zueinander inverse sind.
   (Quadrat der einer Zahl ergibt jeweils das andere EL)
   $M_3 = \{1, 9, 11\}$
4. gesamte Gruppe $M_4 = \mathbb{Z}_{14}^*$

iv) $\{k \cdot u \mid k \in \mathbb{Z}_{14}^*\}$ für nicht triviale UG. U von $(\mathbb{Z}_{14}^*, \cdot)$

$U = M_2$: $1 \cdot M_2 = \{1, 13\} = 13 \cdot M_2$

$3 \cdot M_2 = \{3, 11\} = 11 \cdot M_2$

$5 \cdot M_2 = \{5, 9\} = 9 \cdot M_2$

$U = M_3$: $1 \cdot M_3 = \{1, 9, 11\} = 9 \cdot M_3 = 11 \cdot M_3$

$3 \cdot M_3 = \{3, 5, 13\} = 13 \cdot M_3 = 5 \cdot M_3$

b) $(G, \circ)$ Gruppe, $g \in G$, $U \leq G$

$f: U \to g \circ U$ mit $f(u) = g \circ u$ soll bijektiv sein

Beweis: Seien $U \leq G$, $g \in G$

Sei $h \in g \circ U$, also gibt es ein $u \in U$ mit $h = g \circ u$

also auch $f(u) = h \Rightarrow f$ surjektiv.

Seien $h_1, h_2 \in g \circ U$ mit $h_1 = h_2$ also gibt es $u_1, u_2 \in U$

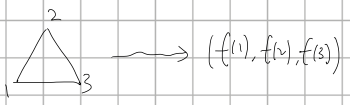
mit $f(u_1) = g \circ u_1 = h_1 = h_2 = g \circ u_2 = f(u_2)$

Es folgt

$$\underbrace{g^{-1}(g \circ u_1)}_{id} = \underbrace{g^{-1}(g \circ u_2)}_{id}$$

$\Rightarrow u_1 = u_2 \Rightarrow f$ injektiv

Diedergruppe:



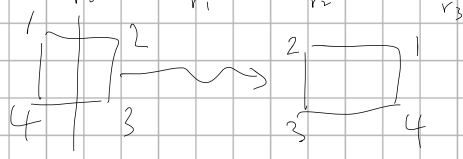
$\longrightarrow (f(1), f(2), f(3))$

$n = 3$

$D_3 = \{\underbrace{(1,2,3)}_{id}, (2,3,1), (2,1,3), (1,3,2), (3,1,2), (3,2,1)\}$

r: Drehung s: Spiegelung — Drehung — Spiegelung

$D_4 = \{\underbrace{(1,2,3,4)}_{r_0}, \underbrace{(2,3,4,1)}_{r_1}, \underbrace{(3,4,1,2)}_{r_2}, \underbrace{(4,1,2,3)}_{r_3}, \underbrace{(2,1,4,3)}_{s_0}, \underbrace{(4,3,2,1)}_{s_1}, \underbrace{(3,2,1,4)}_{s_2}, \underbrace{(1,4,3,2)}_{s_3}\}$



(a) Schreiben Sie die Gruppen $\mathfrak{D}_n$ für $n \in \{3,4,5\}$ elementweise auf.

(b) Stellen Sie die Verknüpfungstafel für $\mathfrak{D}_4$ auf.

(c) Bestimmen Sie alle Untergruppen von $\mathfrak{D}_4$.

(d) Es sei p eine Primzahl, und sei $n \in \mathbb{N}$ mit $n > 0$. Für welche $k \in \mathbb{N}$ kann $\mathfrak{D}_{p^n}$ Untergruppen der Ordnung k besitzen?

Hinweis: Zeichnen Sie zunächst ein reguläres n-Eck, und beschriften Sie die Eckpunkte von 1 bis n im Uhrzeigersinn. Spiegelungen und Drehungen sind dann (spezielle) bijektive Abbildungen der Form $f\colon \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$, und lassen sich einfach mit Hilfe des Tupels $\big(f(1), f(2), \ldots, f(n)\big)$ der Bildwerte darstellen.

A58. **Hausaufgabe, bitte vor Beginn der 11. Übung (oder im Lernraum) unter Angabe von Name, Matrikelnummer, Übungsgruppe und Übungsleiter abgeben.**
Es sei $(\mathbb{Z}_{20}^*, \cdot)$ die Gruppe der Einheiten des Restklassenrings $(\mathbb{Z}_{20}, +, \cdot)$.

(a) Geben Sie alle Elemente von $\mathbb{Z}_{20}^*$ an, und stellen Sie die Verknüpfungstafel von $(\mathbb{Z}_{20}^*, \cdot)$ auf.

(b) Bestimmen Sie alle Untergruppen der Ordnung 2 von $(\mathbb{Z}_{20}^*, \cdot)$.

(c) Bestimmen Sie die Menge der Linksnebenklassen $\big\{k \cdot U \mid k \in \mathbb{Z}_{20}^*\big\}$ für $U = \{1,3,7,9\}$.

(d) Berechnen Sie alle $x \in \mathbb{Z}_{20}$, die die Kongruenz $9887^{8899}x \equiv 11 \pmod{20}$ erfüllen.

H59. 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 $(\mathbb{Z}_3, +, \cdot)$ und überlegen Sie, was bei einer Begegnung passiert.

H60. Sei $(G, \circ)$ eine Gruppe mit neutralem Element e, und sei $A \subseteq G$. Zeigen Sie, dass $\langle A \rangle$ die bzgl. Inklusion kleinste Untergruppe von G ist, die A enthält, und dass gilt

$$\langle A \rangle = \big\{a_1 \circ a_2 \circ \cdots \circ a_k \mid k \in \mathbb{N},\ a_i \in A \cup A^{-1} \cup \{e\}\big\}.$$