Präsenzaufgaben

Verständnisfragen

1. Erklären Sie, wie Sie von $\phi(n)$ für $n \in \mathbb{P}$ (Primzahl) bzw. $n \in \mathbb{N}$ berechnen.
   Lösung: $\phi(n)$ gibt die Anzahl zu n teilerfremden Zahlen $< n$ an. Für Primzahlen p gilt deswegen $\phi(p) = p - 1$. Im allgemeinen berechnet man die Primfaktorzerlegung einer Zahl $n = p_1^{a_1} \cdot \ldots p_k^{a_k}$ und rechnet dann $\phi(n) = \phi(p_1^{a_1}) \cdot \ldots \phi(p_k^{a_k})$ aus. Dabei ist noch zu beachten, dass $\phi(p^k) = p^{k-1} \cdot (p-1)$ für jede Primzahl p und $k \in \mathbb{N}$ gilt. Deswegen ist
   $$\phi(n) = \phi\left(p_1^{a_1} \cdot \ldots p_k^{a_k}\right) = p_1^{a_1-1}(p_1 - 1) \cdot p_k^{a_k-1}(p_k - 1).$$

2. Berechnen Sie $\phi(5)$, $\phi(6)$, $\phi(7)$ und $\phi(97)$. *Lösung:* $\phi(5) = 4$, $\phi(6) = \phi(2)\phi(3) = 2$, $\phi(7) = 6$, $\phi(97) = 96$.

3. Die Primfaktorzerlegung von 8800 ist $2^5 \cdot 5^2 \cdot 11$. Berechnen Sie $\phi(8800)$.
   $$\phi(8800) = \phi(2^5 \cdot 5^2 \cdot 11) = \phi(2^5)\phi(5^2)\phi(11) = 2^4 \cdot (2-1) \cdot 5 \cdot (5-1) \cdot 10 = 3200$$

4. Warum kann es kein $n \in \mathbb{N}$ geben, so dass $\phi(n) = 14$?
   Antwort: Die Zahl 14 kann man entweder als $14 = 1 \cdot 14$ oder als $14 = 2 \cdot 7$ schreiben. Eine andere Zerlegung in Faktoren gibt es nicht. Da ϕ immer als Produkt der Primfaktoren berechnet wird, muss also gelten
   $$14 = 1 \cdot 14 = \phi(2) \cdot \phi(15) \quad \Rightarrow \quad \text{Widerspruch: 15 ist keine Primzahl.}$$
   Die zweite Möglichkeit ergibt:
   $$14 = 2 \cdot 7 = \phi(3) \cdot \phi(8) \quad \Rightarrow \quad \text{Widerspruch: 8 ist keine Primzahl.}$$
   Der Faktor 7 kann nur in einem Wert von ϕ auftauchen, wenn gleichzeitig der Faktor 6 auftaucht, denn $7 \cdot 6 = \phi(7^2)$.

5. Was müssen Sie berechnen, um die letzten 2 Ziffern von 89^{43} zu bestimmen? Geben Sie nur die Rechenschritte an, ohne zu rechnen. Denken Sie an den Satz von Euler.
   Antwort: Um die letzten 2 Ziffern zu bestimmen, muss man modulo 100 rechnen. Durch den Satz von Euler wissen wir, dass
   $$a^{\phi(100)} = 1 \mod 100$$
   für alle a mit $\text{ggT}(a, 100) = 1$ gilt. Da $\phi(100) = 40$ ist, können wir also rechnen
   $$89^{43} \mod 100 = 89^3 89^{40} \mod 100 = 89^3 \mod 100 \cdot 89^{40} \mod 100 = 89^3 \mod 100$$
   Den Term $89^3 \mod 100$ kann man besser berechnen, wenn man $89 \mod 100 = -11 \mod 100$ schreibt. Dann erhält man
   $$\begin{aligned} 89^3 \mod 100 &= 89^2 \mod 100 \cdot 89 \mod 100 \\ &= (-11)^2 \mod 100 \cdot (-11) \mod 100 \\ &= 21 \cdot (-11) \mod 100 \\ &= 69 \mod 100. \end{aligned}$$
   Die letzten beiden Ziffern sind also 69 von 89^{43}.

6. Welche der folgenden Strukturen besitzen ein neutrales Element? Bestimmen Sie es:
   Lösung: Sei $(G, \circ)$ eine Gruppe. Dann heißt $e \in G$ ein neutrales Element, falls für alle $g \in G$ gilt: $g \circ e = g$.
   (a) $(\mathbb{N}, +)$. Da wir $\mathbb{N} = \{1, 2, \dots\}$ definiert haben, gibt es kein neutrales Element.
   (b) $(\mathbb{N}, \cdot)$. Ja, 1 ist das neutrale Element, denn $n \cdot 1 = n$ für alle $n \in \mathbb{N}$.
   (c) $(\mathbb{N}, *)$ mit $a * b := 2a + b$ für $a, b \in \mathbb{N}$. Es muss gelten $a * e = 2a + e = a$ für alle $a \in \mathbb{N}$, also muss $e = -a$ sein. Aber $-a \notin \mathbb{N}$. Damit gibt es kein neutrales Element.
   (d) $(\mathbb{Z}, *)$ mit $a * b := |a + b|$ für $a, b \in \mathbb{Z}$. Es muss gelten $a * e = |a + e| = a$ für alle $a \in \mathbb{Z}$. Wir machen eine Fallunterscheidung:
   Fall 1: $a + e \geq 0$, dann ist $|a + e| = a + e = a$, also $e = 0$. Für $a \geq 0$ ist e ein neutrales Element.
   Fall 2: $a + e < 0$, dann ist $|a + e| = -(a + e) = a$, also $-a - e = a \Leftrightarrow -2a = e$. Das ist kein neutrales Element, da dieses nicht von a abhängen darf. Das neutrale Element ist immer eindeutig bestimmt in einer Gruppe, es gibt also immer nur genau eins.
   $(\mathbb{Z}, *)$ besitzt also kein neutrales Element.

7. Zeigt die folgende Verknüpfungstabelle auf der Menge $\{e, a, b, c, d\}$ eine Gruppe?

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

   Lösung: Man muss zum einen überprüfen, ob es ein neutrales Element gibt. Man sieht, dass e das neutrale Element. Weiter muss man überprüfen, ob in jeder Zeile und Spalte einmal das neutrale Element vorkommt. Denn nur dann besitzt jedes Element ein inverses Element. Die Verknüpfungstabelle zeigt also eine Gruppe.

Standardaufgaben

1. Berechnen Sie
   (a) $\phi(101) = 100$
   (b) $\phi(142) = \phi(2 \cdot 71) = 70$
   (c) $\phi(169) = \phi(13^2) = 13 \cdot 12 = 156$
   (d) $\phi(1024) = \phi(2^{10}) = 2^9 \cdot 1 = 512$

2. Für welche n gilt $n = 2\phi(n)$?
   Lösung: Sei $n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$ die Primfaktorzerlegung mit $p_1 < p_2 < \dots < p_k$, dann

ist $\phi(n) = p_1^{a_1-1}(p_1-1)\cdot\dots\cdot p_k^{a_k-1}(p_k-1)$. Es muss gelten

$$p_1^{a_1}\cdot\dots\cdot p_k^{a_k} = 2\cdot p_1^{a_1-1}(p_1-1)\cdot\dots\cdot p_k^{a_k-1}(p_k-1), \quad \big|\text{teilen durch } p_1^{a_1-1},\dots,p_k^{a_k-1}$$
$$p_1\cdot p_2\cdot\dots\cdot p_k = 2\cdot(p_1-1)\cdot(p_2-1)\cdot\dots\cdot(p_k-1)$$

Also muss gelten $p_1 = 2$ und $p_1 - 1 = 1$. Wir teilen also die Gleichung durch 2 und erhalten:

$$p_2\cdot\dots\cdot p_k = (p_2-1)\cdot\dots\cdot(p_k-1).$$

Damit die Gleichung erfüllt ist, muss es einen Index i geben, so dass $p_2 - 1 = p_i$ ist. Dies ist aber nicht möglich, da die Primzahlen der Größe nach geordnet sind und somit $p_i \geq p_2$ ist und damit $p_i > p_2 - 1$. Also kann n keine anderen Primfaktoren außer $p_1^{k_1} = 2^{k_1}$ enthalten. Die Zahl n muss damit eine Zweierpotenz sein $n = 2^k$:
Es ist $n = 2\phi(n) = 2\phi(2^k) = 2\cdot 2^{k-1}$.

3. Berechnen Sie die letzten beiden Ziffern von 89^{43}. Verwenden Sie den Satz von Euler.
Lösung: s. Lösung oben bei den Verständnisfragen.

4. Welche der folgenden Strukturen sind Gruppen? Falls ein Beispiel keine Gruppe ist, geben Sie kurz an, welches Gruppengesetz verletzt wird.

   - ☐ $(\mathbb{Z}, +)$: Gruppe
   - ☐ $(\mathbb{N}, +)$: keine Gruppe, da kein neutrales Element und keine inversen Elemente
   - ☐ $(2\mathbb{Z}, +)$: Gruppe
   - ☐ $(\mathbb{Z}\setminus\{0\}, +)$, keine Gruppe, neutrales Element fehlt
   - ☐ $(\mathbb{Z}, \cdot)$, keine Gruppe, da keine inversen Elemente
   - ☐ $(\mathbb{Q}\setminus\{0\}, \cdot)$: Gruppe
   - ☐ $(\mathbb{Z}_8, +)$: Gruppe
   - ☐ $(\mathbb{Z}_8, \cdot)$: keine Gruppe, denn nicht alle Elemente haben ein inverses Element: z.B. hat 4 kein inverses Element.
   - ☐ $(\mathbb{Z}_8\setminus\{0\}, \cdot)$: keine Gruppe, s.o.
   - ☐ $(\mathbb{Z}_8^*, \cdot)$: Gruppe

5. Bestimmen Sie die inversen Elemente von 3 in den folgenden Gruppen:
   (a) $(\mathbb{Z}_5, +)$: $x = 2$, denn $3 + 2 = 0 \mod 5$.
   (b) $(\mathbb{Z}_5^*, \cdot)$: $x = 2$, denn $3\cdot 2 = 1 \mod 5$
   (c) $(\mathbb{Z}_8^*, \cdot)$: $x = 3$, denn $3\cdot 3 = 1 \mod 8$.

6. Zeigen Sie, dass es in jeder Gruppe ein Element der Ordnung 1 gibt.
Lösung: In jeder Gruppe gibt es ein neutrales Element e, also $e^1 = e$, und damit ein Element der Ordnung 1.

7. Zeigen Sie, dass es in jeder Gruppe genau ein Element der Ordnung 1 gibt.
Lösung: Sei $g \neq e$ ein zweites Element der Ordnung 1, dann ist $g^1 = e$, also muss $g = e$ gelten. Damit gibt es genau ein Element der Ordnung 1, das neutrale Element.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

8. Stellen Sie die Additions- und Multiplikationstabelle für $\mathbb{Z}_6$ auf. Zeigen Sie, dass $\mathbb{Z}_6 \setminus \{0\}$ keine Gruppe bezüglich der Multiplikation ist.
   Wir sehen in der Tabelle, dass die Elemente 2,3 und 4 keine inversen Elemente besitzen. Somit ist $\mathbb{Z}_6 \setminus \{0\}$ keine Gruppe.

9. Bestimmen Sie die Ordnung aller Elemente in
   (a) $(S_3, \circ)$. Wir bezeichnen die Elemente wie in der Vorlesung mit $id = (1,2,3)$, $s_1 = (1,3,2)$, $s_2 = (2,1,3)$, $s_3 = (2,3,1)$, $s_4 = (3,1,2)$, $s_5 = (3,2,1)$. Das Element id hat als neutrales Element Ordnung 1. Alle Elemente, durch die nur zwei Zahlen vertauscht werden, haben Ordnung 2: s_1, denn $s_1 \circ s_1 = id$, und s_2 und s_5. Die anderen Elemente „verschieben“ alle Zahlen jeweils nach rechts bzw. links. Man benötigt also 3 Anwendungen, um wieder die Identität zu erhalten: s_3 und s_4 haben also Ordnung 3.
   (b) $(\mathbb{Z}_6, +)$. Es ist $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$. Es ist ord(0) = 1 (neutrales Element), ord(1) = 6, denn $(1+1+1+1+1+1) \mod 6 = 0 \mod 6$. ord(2) = 3, denn $(2+2+2) \mod 6 = 0 \mod 6$, ord(3) = 2, ord(4) = 3, denn $(4+4+4) \mod 6 = 0 \mod 6$, ord(5) = 6, denn $(5+5+5+5+5+5) \mod 6 = 0 \mod 6$.
   (c) $(\mathbb{Z}_6^*, \cdot)$. Es ist $\mathbb{Z}_6^* = \{1,5\}$, also ord(1) = 1 als neutrales Element und ord(5) = 2, denn $5^2 \mod 6 = 1 \mod 6$.

10. Welche Kardinalität können die Untergruppen folgender Gruppen haben: *Kardinalität* ist gleichbedeutend zu Mächtigkeit einer Menge bzw Ordnung einer Gruppe. Es bezeichnet in allen Fällen die Anzahl von Elementen in der Gruppe bzw. Untergruppe. Die Ordnung einer Untergruppe einer endlichen Gruppe teilt immer die Ordnung der Gruppe.
    (a) $(\mathbb{Z}_7, +)$, da $|\mathbb{Z}_7| = 7$, kann es nur Untergruppen mit Ordnung 1 oder 7 geben, wobei natürlich eine Untergruppe der Ordnung 7 mit $\mathbb{Z}_7$ übereinstimmen muss.
    (b) $(\mathbb{Z}_6, +)$, da $|\mathbb{Z}_6| = 6$, kann es Untergruppen der Ordnung 1,2,3 oder 6 geben.
    (c) $(\mathbb{Z}_8, +)$, da $|\mathbb{Z}_8| = 8$, kann es Untergruppen der Ordnung 1,2,4 oder 8 geben.

(d) $(\mathbb{Z}_n, +)$, $n \in \mathbb{Z}$, da $|\mathbb{Z}_n| = n$, kann es Untergruppen der Ordnung d mit $d \mid n$ geben.

Übungsaufgaben: Abgabe

1. Zeigen Sie die folgende Aussage:

$$\forall n \in \mathbb{N}, n \text{ ungerade} : \phi(2n) = \phi(n)$$

Lösung: Sei n ungerade, dann ist ggT(n, 2) = 1. Also gilt: $\phi(2n) = \phi(2) \cdot \phi(n)$. Da $\phi(2) = 1$, folgt die Aussage. **(10 Punkte: je nach Schlüssigkeit des Arguments.)**

2. Bestimmen Sie den Rest von 11^{1213} bei Division durch 26, indem Sie die Eulersche ϕ-Funktion und den Satz von Euler verwenden.
Lösung: Es ist $\phi(26) = 12$ und $1213 = 101 \cdot 12 + 1$. Also können wir schreiben:

$$11^{1213} = \left(11^{12}\right)^{101} \cdot 11$$

Aus dem Satz von Euler folgt $11^{\phi(26)} \mod 26 = 1 \mod 26$, also $11^{12} = 1 \mod 26$. Damit folgt

$$11^{1213} \mod 26 = (1 \mod 26)^{101} \cdot 11 \mod 26 = 11 \mod 26.$$

(10 Punkte: 2 Punkte $\phi(26)$ berechnen, 2 Punkte Zerlegung von 1213, restliche Punkte für Rechnung (-1 Punkt bei Rechenfehler.)

3. Stellen Sie die Multiplikationstabelle für $\mathbb{Z}_7$ und $\mathbb{Z}_8$ auf. Überprüfen Sie, ob es sich bei $(\mathbb{Z}_7, \cdot)$ bzw. $(\mathbb{Z}_8, \cdot)$ um eine Gruppe handelt.
Lösung:

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

$\mathbb{Z}_8$ ist keine multiplikative Gruppe, da die Elemente 2,4,6 keine inversen Elemente besitzen. $\mathbb{Z}_7$ ist eine multiplikative Gruppe, wenn man die 0 herausnimmt. **(15 Punkte: jeweils 5 Punkte pro Tabelle, und 5 Punkte für Begründung, ob Gruppe.**

4. Bestimmen Sie die Ordnung aller Elemente in S_4 (der Gruppe aller bijektiven Abbildungen $\{1,2,3,4\} \to \{1,2,3,4\}$). Bitte geben Sie die jeweilige Rechnung an.
Die Gruppe S_4 enthält $4! = 24$ Elemente. Somit können die Elemente Ordnung $1, 2, 3, 4, 6, 8$ oder 12 besitzen. Jedes Element entspricht einer Permutation der Menge $\{1,2,3,4\}$. Man kann sich überlegen, wie man die verschiedenen Permutationen erzeugen kann: Werden nur zwei Zahlen miteinander vertauscht, ist die Ordnung der Permutation 2. Wir können z.B. 1 mit 2 vertauschen (oder 3,oder 4), die 2 kann man mit der 3 oder 4 vertauschen usw. Von diesen einfachen Vertauschen gibt es also genau 6 Stück. Wenn man zweimal zwei solcher Vertauschungen ausführt, kann entweder wieder Ordnung 2 entstehen, wenn die vertauschten Zahlen unterschiedlich sind, oder Ordnung 3, wenn man eine Zahl zweimal hintereinander vertauscht.
Führen wir drei „echte“ Vertauschungen hintereinander aus, erhält man Elemente der Ordnung 4.

   - Das neutrale Element (1234) hat Ordnung 1.
   - Alle Elemente, die nur zwei Zahlen vertauschen, haben Ordnung 2: (2134), (3214), (4231), (1324), (1432), (1243).
   - Alle Elemente, die zweimal je zwei verschiedene Zahlen vertauschen, haben Ordnung 2:(3412), (2143), (4321).
   - Alle Elemente, die durch das zweimalige Vertauschen entstehen, so dass eine Zahl fest bleibt, haben Ordnung 3:(1423), (4213),(3124), (1342), (3241), (2431), (2314),(4132).
   - Alle Elemente mit Ordnung 4, die aus drei Vertauschungen entstanden sind: (2341), (2413), (3142), (3421), (4123), (4312).

   (15 Punkte: Punkte anteilig für richtig bestimmte Ordnung. Rechnung oder Argumentation für Ordnung sollte vorhanden sein.)