Script **generated by TTT**

Title: Meixner: ZUE_DS (18.12.2013)

Date: Wed Dec 18 17:04:30 CET 2013

Duration: 84:17 min

Pages: 39

ZÜ X

Übersicht:

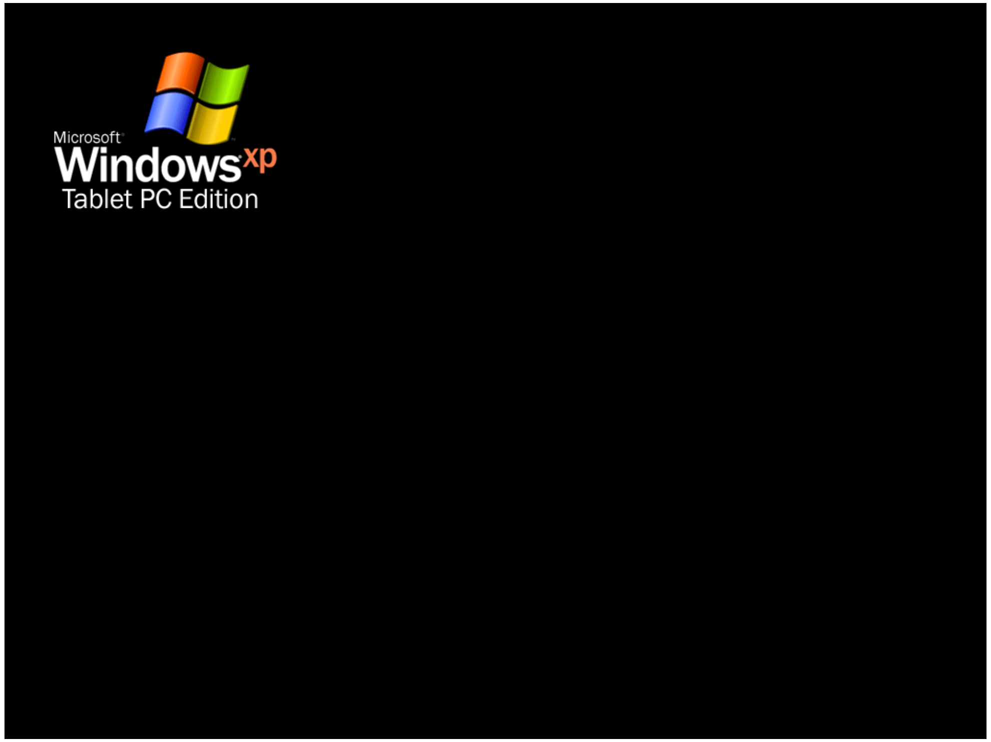
1. Übungsbetrieb: Termine, Fragen, Probleme?
2. Thema Zirkuläres Rechnen
   Rechengesetze modulo m
   Ganzzahlige Division
3. Zählen der Elemente von Mengen
   Zählen von Relationen und Mengen
   Zählen von Abbildungen
   Zählen von Wörtern

1. Termine, Fragen, Anregungen?

Termin der letzten Zentralübung im WS 13/14:

29. Januar 2014

Aktuelle Fragen, Anregungen?



1. Termine, Fragen, Anregungen?

Termin der letzten Zentralübung im WS 13/14:

29. Januar 2014

Aktuelle Fragen, Anregungen?

2. Thema: Zirkuläres Rechnen

Ganze Zahlen $a, b \in \mathbb{Z}$ nennt man

kongruent modulo m, mit $m \in \mathbb{N}$, i. Z.

$$a \equiv b \pmod{m},$$

falls sich a und b um ein ganzzahliges Vielfaches von m unterscheiden, d. h.,

falls es ein $k \in \mathbb{Z}$ gibt, so dass gilt

$$a = b + k \cdot m .$$

Man schreibt auch $a \equiv_m b$ für $a \equiv b \pmod{m}$.
$\equiv_m$ ist eine Äquivalenzrelation über $\mathbb{Z}$,
ja sogar eine „Kongruenzrelation“.

2. Thema: Zirkuläres Rechnen

Ganze Zahlen $a, b \in \mathbb{Z}$ nennt man

kongruent modulo m, mit $m \in \mathbb{N}$, i. Z.

$$a \equiv b \pmod{m},$$

falls sich a und b um ein ganzzahliges Vielfaches von m unterscheiden, d. h.,

falls es ein $k \in \mathbb{Z}$ gibt, so dass gilt

$$a = b + k \cdot m .$$

Man schreibt auch $a \equiv_m b$ für $a \equiv b \pmod{m}$.
$\equiv_m$ ist eine Äquivalenzrelation über $\mathbb{Z}$,
ja sogar eine „Kongruenzrelation“.

Davon abgeleitet ist die Definition der
Operation $\bmod : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z}$:

$$b = a \bmod m \iff a \equiv b \pmod{m} \text{ und } 0 \le b < m .$$

Für jedes m ist $\bmod m$ eine unäre Operation über $\mathbb{Z}$.

$a \bmod m$ heißt Rest der natürlichen Division von a durch m.

2.1 Rechengesetze modulo m

Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$:

$$
\begin{aligned}
a &\equiv a \bmod m \pmod{m}\,, && (1)\\
(a+b) \bmod m &= [(a \bmod m) + (b \bmod m)] \bmod m\,, && (2)\\
(a \cdot b) \bmod m &= [(a \bmod m) \cdot (b \bmod m)] \bmod m\,. && (3)
\end{aligned}
$$

2. Zu beweisen ist:
$(a+b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m\,.$

Lösung:

Wir setzen linke Seite bzw. rechte Seite der Gleichung

$$
\begin{aligned}
x &:= (a+b) \bmod m\,,\\
y &:= [(a \bmod m) + (b \bmod m)] \bmod m\,.
\end{aligned}
$$

und zeigen $x = y$.

Es gilt $0 \leq x, y < m$ und

$$
\begin{aligned}
x &= a + b + k_x \cdot m\,,\\
y &= (a \bmod m) + (b \bmod m) + k_y \cdot m\,,\\
(a \bmod m) &= a + k_a \cdot m\,,\\
(b \bmod m) &= b + k_b \cdot m
\end{aligned}
$$

für gewisse $k_a, k_b, k_x, k_y \in \mathbb{Z}$ und es folgt

$$
\begin{aligned}
y &= a + k_a \cdot m + b + k_b \cdot m + k_y \cdot m\\
&= x - k_x \cdot m + k_a \cdot m + k_b \cdot m + k_y \cdot m\\
&= x + (k_a + k_b + k_y - k_x) \cdot m\\
&= x + k \cdot m\,.
\end{aligned}
$$

Wegen $0 \leq x, y < m$ folgt $x = y$.

Es gilt $0 \leq x, y < m$ und

$$
\begin{aligned}
x &= a + b + k_x \cdot m\,,\\
y &= (a \bmod m) + (b \bmod m) + k_y \cdot m\,,\\
(a \bmod m) &= a + k_a \cdot m\,,\\
(b \bmod m) &= b + k_b \cdot m
\end{aligned}
$$

für gewisse $k_a, k_b, k_x, k_y \in \mathbb{Z}$ und es folgt

$$
\begin{aligned}
y &= a + k_a \cdot m + b + k_b \cdot m + k_y \cdot m\\
&= x - k_x \cdot m + k_a \cdot m + k_b \cdot m + k_y \cdot m\\
&= x + (k_a + k_b + k_y - k_x) \cdot m\\
&= x + k \cdot m\,.
\end{aligned}
$$

Wegen $0 \leq x, y < m$ folgt $x = y$.

2.2 Ganzzahlige Division

In enger Beziehung zur mod-Operation steht die ganzzahlige Division $a \operatorname{div} m$ zweier Zahlen $a \in \mathbb{Z}, m \in \mathbb{N}$.

Es gilt

$$a = (a \operatorname{div} m) \cdot m + (a \bmod m)\,.$$

Berechnen Sie:

(i) 5 div 4, (ii) (-5) div 4, (iii) $(-x)$ div 1.

(i) 5 div 4:

Seien $a = 5$ und $m = 4$.

Dann gilt

$$(5 \operatorname{div} 4) \cdot 4 \;=\; 5 - (5 \bmod 4) \;=\; 5 - 1 \;=\; 4\,.$$

Es folgt $5 \operatorname{div} 4 = 1\,.$

(ii) (-5) div 4:

Seien $a = -5$ und $m = 4$.

Dann gilt

$$\begin{aligned}((-5) \operatorname{div} 4) \cdot 4 \;&=\; -5 - ((-5) \bmod 4)\\ &=\; (-5 - ((-5+8) \bmod 4))\\ &=\; (-5 - 3) = -8\,.\end{aligned}$$

Es folgt $(-5) \operatorname{div} 4 = -2\,.$

(iii) $(-x)$ div 1:

Seien $a = -x$ und $m = 1$.

Dann gilt

$$((-x) \operatorname{div} 1) \cdot 1 \;=\; -x - ((-x) \bmod 1) \;=\; -x - 0 \;=\; -x\,.$$

Es folgt $(-x) \operatorname{div} 1 = -x\,.$

3. Zählen der Elemente von Mengen

3.1 Zählen von Relationen und Mengen

Sei $M = \{1, 2, \ldots, m\}$. Wir betrachten die Menge aller Relationen $R \subseteq M \times M$.

1. Wie viele Relationen über M gibt es?

Lösung:

Die Anzahl $\text{anz}_{Rel}(M)$ der Relationen über M ist gleich der Anzahl der Teilmengen von $M \times M$.

Wegen $|M \times M| = m^2$ gilt

$$\text{anz}_{Rel}(M) = |\mathcal{P}(M \times M)| = 2^{m^2}.$$

(ii) (-5) div 4:

Seien $a = -5$ und $m = 4$.

Dann gilt

$$\begin{aligned}((-5)\,\mathrm{div}\,4)\cdot 4 &= -5 - ((-5)\bmod 4)\\ &= (-5 - ((-5+8)\bmod 4))\\ &= (-5-3) = -8\,.\end{aligned}$$

Es folgt $(-5)\,\mathrm{div}\,4 = -2$.

(ii) (-5) div 4:

Seien $a = -5$ und $m = 4$.

Dann gilt

$$\begin{aligned}((-5)\,\mathrm{div}\,4)\cdot 4 &= -5 - ((-5)\bmod 4)\\ &= (-5 - ((-5+8)\bmod 4))\\ &= (-5-3) = -8\,.\end{aligned}$$

Es folgt $(-5)\,\mathrm{div}\,4 = -2$.

2.2 Ganzzahlige Division

In enger Beziehung zur mod-Operation steht die ganzzahlige Division $a\,\mathrm{div}\,m$ zweier Zahlen $a \in \mathbb{Z}, m \in \mathbb{N}$.

Es gilt

$$a = (a\,\mathrm{div}\,m)\cdot m + (a \bmod m)\,.$$

Berechnen Sie:

(i) 5 div 4, (ii) (-5) div 4, (iii) $(-x)$ div 1.

3. Zählen der Elemente von Mengen

3.1 Zählen von Relationen und Mengen

Sei $M = \{1, 2, \ldots, m\}$. Wir betrachten die Menge aller Relationen $R \subseteq M \times M$.

1. Wie viele Relationen über M gibt es?

Lösung:

Die Anzahl $\mathrm{anz}_{Rel}(M)$ der Relationen über M ist gleich der Anzahl der Teilmengen von $M \times M$.

Wegen $|M \times M| = m^2$ gilt

$$\mathrm{anz}_{Rel}(M) = |\mathcal{P}(M \times M)| = 2^{m^2}.$$

2. Wie viele Relationen über M mit $k \in \mathbb{N}_0$ Elementen gibt es?

Lösung:

Die Frage ist,
wie viele Teilmengen mit k Elementen besitzt $M \times M$,
d. h., welchen Wert besitzt $|\{R \in \mathcal{P}(M \times M)\,;\ |R| = k\}|$?

Nach Vorlesung besitzt jede Menge mit m Elementen genau

$$\binom{m}{k} = \frac{m!}{(m-k)!k!}$$

k-elementige Teilmengen.

Damit gilt für $k \leq m^2$ (und auch für $k > m^2$)

$$|\{R \in \mathcal{P}(M \times M)\,;\ |R| = k\}| = \binom{m^2}{k}.$$

3. Wie viele reflexive Relationen über M gibt es?

Lösung:

Zur Konstruktion einer reflexiven Relation über M entfernt man zunächst aus $M \times M$ alle m Paare (x, x) der Identität Id_M,

nimmt dann eine Teilmenge der Restmenge und

fügt anschließend alle Paare der Identität wieder hinzu.

Man beachte, dass das abschließende Hinzufügen der Identität eine injektive Operation darstellt.

Entsprechend erhält man die
Anzahl anz_{refRel} der reflexiven Relationen über M wie folgt.

$$\mathrm{anz}_{refRel}(M) = |\mathcal{P}((M \times M) \setminus \mathrm{Id}_M)| = 2^{m^2 - m}.$$

3. Wie viele reflexive Relationen über M gibt es?

Lösung:

Zur Konstruktion einer reflexiven Relation über M entfernt man zunächst aus $M \times M$ alle m Paare (x, x) der Identität Id_M,

nimmt dann eine Teilmenge der Restmenge und

fügt anschließend alle Paare der Identität wieder hinzu.

Man beachte, dass das abschließende Hinzufügen der Identität eine injektive Operation darstellt.

Entsprechend erhält man die
Anzahl anz_{refRel} der reflexiven Relationen über M wie folgt.

$$\mathrm{anz}_{refRel}(M) = |\mathcal{P}((M \times M) \setminus \mathrm{Id}_M)| = 2^{m^2 - m}.$$

3. Wie viele reflexive Relationen über M gibt es?

Lösung:

Zur Konstruktion einer reflexiven Relation über M entfernt man zunächst aus $M \times M$ alle m Paare (x, x) der Identität Id_M,

nimmt dann eine Teilmenge der Restmenge und

fügt anschließend alle Paare der Identität wieder hinzu.

Man beachte, dass das abschließende Hinzufügen der Identität eine injektive Operation darstellt.

Entsprechend erhält man die
Anzahl anz_{refRel} der reflexiven Relationen über M wie folgt.

$$\mathrm{anz}_{refRel}(M) = |\mathcal{P}\left((M \times M) \setminus \mathrm{Id}_M\right)| = 2^{m^2 - m}\,.$$

3. Wie viele reflexive Relationen über M gibt es?

Lösung:

Zur Konstruktion einer reflexiven Relation über M entfernt man zunächst aus $M \times M$ alle m Paare (x, x) der Identität Id_M,

nimmt dann eine Teilmenge der Restmenge und

fügt anschließend alle Paare der Identität wieder hinzu.

Man beachte, dass das abschließende Hinzufügen der Identität eine injektive Operation darstellt.

Entsprechend erhält man die
Anzahl anz_{refRel} der reflexiven Relationen über M wie folgt.

$$\mathrm{anz}_{refRel}(M) = |\mathcal{P}\left((M \times M) \setminus \mathrm{Id}_M\right)| = 2^{m^2 - m}\,.$$

ZÜ DS
©Dr. Werner Meixner
3.1 Zählen von Relationen und Mengen
16/33

4. Sei A eine n-elementige Menge und es sei B eine m-elementige Teilmenge von A.

   Wie viele Teilmengen C von A gibt es, die B enthalten, für den Fall $n = 5$ und $m = 2$?

   Geben Sie eine Formel für den allgemeinen Fall $n, m \in \mathbb{N}_0$ an und begründen Sie diese Formel.

Lösung:

Sei $B \subseteq A$.
Seien $A' := A \setminus B$ und $[B, A] := \{C \subseteq A\,;\ B \subseteq C \subseteq A\}$.

Dann ist $f : [B, A] \to \mathcal{P}(A')$ mit $f(C) = C \setminus B$
eine bijektive Abbildung von $[B, A]$ auf $\mathcal{P}(A')$.

Es gilt wegen $|A'| = n - m$

$$|\mathcal{P}(A')| = 2^{n-m}\,.$$

Für $n = 5$ und $m = 2$ ergibt sich $|\mathcal{P}(A')| = 2^3 = 8$.

3.2 Zählen von Abbildungen

Sei $M = \{0, 1, 2\}$.

1. Listen Sie alle Äquivalenzrelationen über M auf!

Lösung:

Äquivalenzrelationen sind durch
die Menge ihrer zugeordneten Äquivalenzklassen bestimmt.

Über der Grundmenge M mit 3 Elementen gibt es

Äquivalenzrelationen mit 3 Klassen,

mit 2 Klassen und

mit einer einzigen Klasse.

Die Menge der zugeordneten Klassen bildet eine Partition P der Grundmenge M.

Äquivalenzrelationen mit
1 Klasse: $P_{1,1} = \{\{0, 1, 2\}\}$.

Äquivalenzrelationen mit
2 Klassen:

$$P_{2,1} = \{\{0\}, \{1, 2\}\}.$$
$$P_{2,2} = \{\{1\}, \{0, 2\}\}.$$
$$P_{2,3} = \{\{2\}, \{1, 0\}\}.$$

Äquivalenzrelationen mit
3 Klassen: $P_{3,1} = \{\{1\}, \{2\}, \{0\}\}$.

2. Wie viele Partitionen gibt es über M?

Lösung:

Die Partitionen entsprechen eineindeutig den Äquivalenzrelationen.

Also gibt es 5 Partitionen über M.

3. Gibt es eine Äquivalenzrelation über der leeren Menge?

Lösung:

Falls $M = \emptyset$,
dann ist $R = \emptyset$ eine Äquivalenzrelation über M.

Aus $\emptyset \times \emptyset = \emptyset$ folgt,
dass $\emptyset$ die einzige Relation über $\emptyset$ ist.

Die Menge der Klassen dieser Relation R ist leer.
Damit entspricht die leere Menge von Klassen in diesem Fall einer (einzigen) Partition von M.

4. Wie viele surjektive Abbildungen f von M auf $M' = \{1, 2\}$ gibt es?

Lösung:

Damit f surjektiv ist, muss $\{k_1, k_2\}$ mit $k_1 := f^{-1}(1)$ und $k_2 := f^{-1}(2)$ eine 2-elementige Partition über M bilden.

Also kommen nur
die Partitionen $P_{2,1}$, $P_{2,2}$ und $P_{2,3}$ für $\{k_1, k_2\}$ in Frage.

Für die Zuordnung der Urbildklassen k_1, k_2 zu den Klassen der Partitionen $P_{i,j}$ gibt es nun stets 2 Möglichkeiten.

Deshalb erhalten wir insgesamt 6 surjektive Abbildungen.

3. Gibt es eine Äquivalenzrelation über der leeren Menge?

Lösung:

Falls $M = \emptyset$,
dann ist $R = \emptyset$ eine Äquivalenzrelation über M.

Aus $\emptyset \times \emptyset = \emptyset$ folgt,
dass $\emptyset$ die einzige Relation über $\emptyset$ ist.

Die Menge der Klassen dieser Relation R ist leer.
Damit entspricht die leere Menge von Klassen in diesem Fall einer (einzigen) Partition von M.

4. Wie viele surjektive Abbildungen f von M auf $M' = \{1, 2\}$ gibt es?

Lösung:

Damit f surjektiv ist, muss $\{k_1, k_2\}$ mit $k_1 := f^{-1}(1)$ und $k_2 := f^{-1}(2)$ eine 2-elementige Partition über M bilden.

Also kommen nur
die Partitionen $P_{2,1}$, $P_{2,2}$ und $P_{2,3}$ für $\{k_1, k_2\}$ in Frage.

Für die Zuordnung der Urbildklassen k_1, k_2 zu den Klassen der Partitionen $P_{i,j}$ gibt es nun stets 2 Möglichkeiten.

Deshalb erhalten wir insgesamt 6 surjektive Abbildungen.

5. Wie viele injektive Operationen $f : M \to M$ gibt es?

Lösung:

Eine injektive Operation über einer endlichen Menge M ist gleichzeitig surjektiv und damit bijektiv.

Für die Abbildung von 0 gibt es 3 Möglichkeiten.

Für jede dieser Möglichkeiten gibt es dann 2 Möglichkeiten der Abbildung des Elementes 1.

Damit erhalten wir $2 \cdot 3 = 6$ injektive Operationen über M.

6. Geben Sie alle Variationen von M an!

Die Begriffe k-Variation und k-Permutation sind synonym.

Lösung:

Eine k-Variation (k-Permutation) einer Menge A wurde als Sequenz $q_1, q_2, \ldots, q_k$ der Länge k von paarweise verschiedenen Elementen q_i aus A definiert.

Eine k-Variation mit $k = |A|$ wird Permutation von A genannt.

Wir ordnen jeder Variation $q_1, q_2, \ldots, q_k$ über einer endlichen Menge A in eineindeutiger Weise eine bijektive Abbildung $f : [1, k] \to A$ wie folgt zu

$$f(i) = q_i \,.$$

6. Geben Sie alle Variationen von M an!

Die Begriffe k-Variation und k-Permutation sind synonym.

Lösung:

Eine k-Variation (k-Permutation) einer Menge A wurde als Sequenz $q_1, q_2, \ldots, q_k$ der Länge k von paarweise verschiedenen Elementen q_i aus A definiert.

Eine k-Variation mit $k = |A|$ wird Permutation von A genannt.

Wir ordnen jeder Variation $q_1, q_2, \ldots, q_k$ über einer endlichen Menge A in eineindeutiger Weise eine bijektive Abbildung $f : [1, k] \to A$ wie folgt zu

$$f(i) = q_i \,.$$

Fall $k = 3$ (Permutationen):

Wir erhalten die folgenden 6 Abbildungen $f_1, f_2, \ldots, f_6$.

	1	2	3
f_1	0	1	2
f_2	0	2	1
f_3	1	0	2
f_4	1	2	0
f_5	2	0	1
f_6	2	1	0