Universität Siegen, FB 6 – Mathematik, Prof. Dr. Hartmut Ring

Musterlösungen von Übungsaufgaben zur Vorlesung
Diskrete **Mathematik für Informatiker I**
WS 2006/2007

1. (a) Für beliebige x gilt

$$
\begin{aligned}
& x \in (A - B) \cup (A \cap B) \\
\Leftrightarrow\ & x \in (A - B) \vee x \in (A \cap B) \\
\Leftrightarrow\ & (x \in A \wedge x \notin B) \vee (x \in A \wedge x \in B) \\
\Leftrightarrow\ & x \in A \wedge (x \notin B \vee x \in B) \\
\Leftrightarrow\ & x \in A
\end{aligned}
$$

(b) <u>Von links nach rechts</u>: *Vor.* $A \subseteq B$, *Beh.* $A \cap B = A$

Beweis: Nach Vor. gilt $x \in A \Rightarrow x \in B \Rightarrow x \in (A \cap B)$

umgekehrt: $x \in (A \cap B) \Rightarrow x \in A \wedge x \in B \Rightarrow x \in A$.

<u>Von rechts nach links</u>: *Vor.* $A \cap B = A$, *Beh.* $A \subseteq B$

Beweis: Nach Vor. gilt $x \in A \Rightarrow x \in (A \cap B)$

$\Rightarrow x \in A \wedge x \in B$

$\Rightarrow x \in B$. Also gilt die Behauptung.

4. $A = \{$R, E, L, I, F, P$\}$.
$|\mathbf{P}(A)| = 2^{|A|} = 2^6 = 64$.

5. Die Gleichung $x^3 - 7x^2 + 12x = x(x^2 - 7x + 12) = 0$ hat die Nullstellen 0, 3 und 4.
Also $A = \{3, 4\}$, $B = \{2, 3, 5, 7, 11\}$.
$|A \times B| = 2 \cdot 5 = 10$
$|\mathbf{P}(A \times B)| = 2^{10} = 1024$.

7. (a) Reflexiv, symmetrisch, nicht transitiv:
A = $\{1,2,3\}$, R = $\{(1,1),(1,2),(2,1),(2,2),(2,3),(3,2),(3,3)\}$
Alle Relationen auf einer zweielementigen Menge sind transitiv!
(b) Reflexiv, nicht symmetrisch, transitiv:
A = $\{1,2\}$, R = $\{(1,1),(1,2),(2,2)\}$. Alle Relationen auf einer einelementigen Menge sind symmetrisch!
(c) Nicht reflexiv, symmetrisch, transitiv:
A = $\{1\}$, R = $\emptyset$. „Alle“ Relationen auf der leeren Menge (es gibt dort nur die leere Relation) sind reflexiv!

9. (a) *Symmetrie* von $R \cap R^{-1}$: $(x,y) \in R \cap R^{-1} \Rightarrow (x,y) \in R$ und $(x,y) \in R^{-1} \Rightarrow (y,x) \in R^{-1}$ und $(y,x) \in R$. Also $(y,x) \in R \cap R^{-1}$. Daher ist $R \cap R^{-1}$ symmetrisch.
Reflexivität von $R \cap R^{-1}$: Da R reflexiv und $R \cap R^{-1} \subseteq R$ ist auch $R \cap R^{-1}$ reflexiv.
Transitivität von $R \cap R^{-1}$: Es sei $(x,y) \in R \cap R^{-1}$ und $(y,z) \in R \cap R^{-1}$.
Dann gilt erst recht: $(x,y) \in R$ und $(y,z) \in R$. Wegen der Transitivität von R folgt $\underline{(x,z) \in R}$.
Andererseits gilt auch $(x,y) \in R^{-1}$ und $(y,z) \in R^{-1}$ und damit $(y,x) \in R$ und $(z,y) \in R$.
Wegen der Transitivität von R folgt $(z,x) \in R$. Also: $\underline{(x,z) \in R^{-1}}$.
Die beiden unterstrichenen Aussagen ergeben zusammen: $(y,z) \in R \cap R^{-1}$.
Damit ist die Transitivität von $R \cap R^{-1}$ bewiesen.
(b) Gegenbeispiel: Mit $A = \{1,2,3,4\}$, $R = \{(1,2),(2,3),(1,3)\}$, $S = \{(2,3),(3,4),(2,4)\}$ sind R und S transitiv, $R \cup S$ aber nicht.

10. Eine Äquivalenzrelation zerlegt die Menge in 1, 2, 3, oder 4 Äquivalenzklassen. Für 1 und 4 Klassen ist die Zerlegung eindeutig. 2 Klassen können aus 1+3 oder 2+2 Elementen bestehen. Dafür gibt es 4 (Wahl des einen Elements) bzw. 3 (Wahl des Partners des ersten Elements, alles andere ergibt sich daraus) Möglichkeiten. Drei Klassen können nur aus 1+1+1+2 Elementen bestehen. Für die Wahl der 2 Elemente gibt es 6 Möglichkeiten. Also gibt es insgesamt 1+1+4+3+6 = 15 Äquivalenzklassen.

Universität Siegen, FB 6 – Mathematik, Prof. Dr. Hartmut Ring

Musterlösungen von Übungsaufgaben zur Vorlesung Diskrete **Mathematik für Informatiker I** WS 2006/2007

11. Äquivalenzklassen:
$\{a,b,c\}$ und $\{d,e\}$

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

14. (a) Hilfsbehauptung: Für $n \geq 3$ gilt: $n^2 > 2n+1$.
<u>Induktionsschritt</u>: Mit der Ind.**vor**. folgt:
$(n+1)^2 = \boldsymbol{n^2} + 2n + 1 > \mathbf{2n+1} + 2n+1$
$= 2(n+1)+1 + 2(n-1) > 2(n+1)+1$ (wegen $n \geq 3$)

(b) Aufgabe: Durch Nachrechnen ergibt sich, dass die Ungleichung $2^n \leq n^2$ für 2, 3 und 4 gilt. Es genügt also zu zeigen, dass $2^n > n^2$ für alle $n > 4$ ist.
<u>Induktionsschritt</u>: Vorauss.: $2^n > n^2$ Beh.: $2^{n+1} > (n+1)^2$.
Beweis: $2^{n+1} = 2 \cdot 2^n > 2\,n^2$ nach Induktionsvoraussetzung.
Die Beh. folgt mit der Hilfsbehauptung: $2\,n^2 = n^2 + \boldsymbol{n^2} > n^2 + \mathbf{2n+1} = (n+1)^2$.

15. Vollständige Induktion: $n = 1$ klar ($n = 2$: einfache Regel von de Morgan).
Induktionsschritt: $\overline{\bigcap_{i=1}^{n+1} M_i} = \overline{\bigcap_{i=1}^{n} M_i \cap M_{n+1}} = \overline{\bigcap_{i=1}^{n} M_i} \cup \overline{M_{n+1}}$
Nach Induktionsvoraussetzung ist das gleich
$\bigcup_{i=1}^{n} \overline{M_i} \cup \overline{M_{n+1}} = \bigcup_{i=1}^{n+1} \overline{M_i}$. Also gilt die Beh. auch für $n+1$.

16. Experimentieren zeigt, dass offenbar gilt $f(n) = n^2$.
Induktionsbasis: $f(1) = 1^2$ gilt.
Induktionsschritt:
(a) n sei gerade: $f(n+1) = f(n) + 2(n+1) - 1$. Nach Ind.vor. ist das $= n^2 + 2(n+1) - 1 = (n+1)^2$.
(b) n sei ungerade: $f(n+1) = 4\,f((n+1)/2)$. Nach Ind.vor. ist das $= 4\,((n+1)/2)^2 = (n+1)^2$.

17. Zunächst vereinfachte Versionen: (a) Rasterpunkte auf der Zahlengeraden. Nach dem Schubfachprinzip gibt es unter drei ganzen Zahlen mindestens zwei gerade oder zwei ungerade. Die Differenz dieser beiden Zahlen ist gerade, also ist der entsprechende Verbindungsmittelpunkt ein Gitterpunkt.
(b) Ebene: Vier Schubfächer für Rasterpunkte mit (1.) x und y gerade, (2.) x gerade und y ungerade, (3.) x ugerade, y gerade, (4) x und y ungerade. Unter fünf Gitterpunkten gibt es also mindestens zwei im gleichen Schubfach. Deren Verbindungsmittelpunkt ist ein Gitterpunkt.
(c) Analog kann man die Gitterpunkte im Raum nach geraden/ungeraden Koordinaten in $2^3 = 8$ Schubfächer unterteilen. Unter neun Gitterpunkten gibt es also mindestens zwei im gleichen Schubfach. Deren Verbindungsmittelpunkt ist wieder ein Gitterpunkt.

18. Ist $|A| = 9$, so ist $|\mathbf{P}(A)| = 2^9 = 512$. Aus den 9 Lottokugeln lassen sich also 511 nicht leere Teilmengen auswählen. Die kleinstmögliche Summe ist 1+2+...+9 = 45, die größtmögliche 41+42+...+49 = 405.
Es kommen also nur 361 Zahlen als Summe in Frage. Unter den 511 Teilmengen müssen daher nach dem Schubfachprinzip mehrere die gleiche Summe haben.
Nimmt man nun zwei solche Mengen M_1 und M_2, so sind $M_1 - (M_1 \cap M_2)$ und $M_2 - (M_1 \cap M_2)$ disjunkte Mengen mit gleicher Summe. Da sie verschieden sind, ist mindestens eine nicht leer. Da beide die gleiche Summe haben, sind beide nicht leer.

19. Primfaktorenzerlegung von n. Alle Primfaktoren mit geradem Exponenten können ganz vor die Wurzel gezogen werden. Kommen keine ungeraden Exponenten vor, ist die Wurzel also eine ganze Zahl. Bein ungeraden Exponenten kann ein gerader Anteil vor die Wurzel gezogen werden. Es bleibt ein Produkt aus einer ganzen Zahl und einer Wurzel, unter der jeder Primfaktor nur einmal vorkommt. Diese Wurzel ist irrational (Beweis wie bei $\sqrt{2}$). Mit indirektem Beweis zeigt man leicht, dass das Produkt aus einer ganzen und einer irrationalen Zahl immer irrational ist.

Musterlösungen von Übungsaufgaben zur Vorlesung
Diskrete **Mathematik für Informatiker I**
WS 2006/2007

20. Fall 1: n teilbar durch m.

$$\left\lfloor \frac{n+m-1}{m} \right\rfloor = \frac{n}{m} + \left\lfloor \frac{m-1}{m} \right\rfloor = \frac{n}{m} = \left\lceil \frac{n}{m} \right\rceil$$

Fall 2: n nicht teilbar durch m.

Dann ist $\left\lfloor \frac{n-1}{m} \right\rfloor = \left\lfloor \frac{n}{m} \right\rfloor$ und $\left\lceil \frac{n}{m} \right\rceil - \left\lfloor \frac{n}{m} \right\rfloor = 1$. Damit:

$$\left\lfloor \frac{n+m-1}{m} \right\rfloor = \left\lfloor \frac{n-1}{m} \right\rfloor + 1 = \left\lfloor \frac{n}{m} \right\rfloor + 1 = \left\lfloor \frac{n}{m} \right\rfloor + \left\lceil \frac{n}{m} \right\rceil - \left\lfloor \frac{n}{m} \right\rfloor = \left\lceil \frac{n}{m} \right\rceil$$

22. Zunächst in Basis 7 umwandeln, dann durch Zusammenfassung von je 2 bzw. 3 Stellen in die Systeme zur Basis 49 bzw. 343.

30. $M = \{\{A, E, \neg B\}, \{A,B,C\}, \{\neg A, \neg D, E\}, \{A, \neg C\}\}$
Zur Ergebniskontrolle:
$\mathrm{Res}^*(M) = \{\{A,E,\neg B\}, \{A,B,C\}, \{\neg A,\neg D,E\}, \{A,\neg C\}, \{A,C,E\}, \{E,\neg B,\neg D\}, \{B,C,E,\neg D\}, \{A,B\}, \{E,\neg C,\neg D\}, \{A,C,E,\neg D\}, \{A,E\}, \{A,B,E,\neg D\}, \{C,E,\neg D\}, \{B,E,\neg D\}, \{A,E,\neg D\}, \{E,\neg D\}\}$
Die leere Klausel ist nicht dabei. Also ist M erfüllbar!

32. In 1000! kommen als Faktoren die ersten 200 Vielfachen von 5 vor: 5, 10, 15, ... 1000. Weiter kommen die ersten 40 Vielfachen von 25, die ersten 8 Vielfachen von 125 und der Faktor 725 vor. Damit enthält 1000! den Primfaktor 5 also 200+40+8+1 = 249 mal. Ebenso zeigt man, dass der Primfaktor 2 über 500 mal vorkommt. Also ist 1000! durch 10^{249} teilbar.

38. Erweiterter Euklid liefert $-15\cdot\mathbf{97} + 14\cdot\mathbf{104} = \mathbf{1}$. Damit:

		mod 97	mod 104	
(1)	$-15\cdot\mathbf{97}$	0	1	
(2)	$14\cdot\mathbf{104}$	1	0	
(3)	$3\cdot 14\cdot\mathbf{104}$	3	0	(2) mit 3 multipliziert
(4)	$-2\cdot 15\cdot\mathbf{97}$	0	2	(1) mit 2 multipliziert
(5)	$3\cdot 14\cdot\mathbf{104}-2\cdot 15\cdot\mathbf{97}$	3	2	Summe aus (3) und (4) = 1458

$3\cdot 14\cdot 104-2\cdot 15\cdot 97 = 1458$ ist eine Lösung. Da 97 und 104 teilerfremd sind, haben die Lösungen nach dem Chinesischen Restsatz den Abstand $97\cdot 104 = 10088$. Also gibt es keine weitere vierstellige Lösung.

40. $3^0 \bmod 4 = 1$, $3^1 \bmod 4 = 3$, $3^2 \bmod 4 = 1$, $3^4 \bmod 4 = 3$ usw. Allgemein: $3^{2k+1} \bmod 4 = 3 \Rightarrow (3^{2k+1}-1)/2$ ungerade. Mit $k = 38$ folgt die erste Behauptung.

$3^{77}-1 = (3^7)^{11}-1$. $\quad \dfrac{(3^7)^{11}-1}{3^7-1} = \sum_{i=0}^{10} (3^7)^i$ (geometr. Summe).

$\Rightarrow 3^{77}-1 = (3^7-1)(1+3^7+3^{14}+ \ldots +3^{70})$

Musterlösungen von Übungsaufgaben zur Vorlesung
Diskrete **Mathematik für Informatiker I**
WS 2006/2007

41. Annahme: $p \mid n^2 + 1. \Rightarrow n^2 \equiv -1 \pmod{p}$.
Da $(p-1)/2$ ist ungerade ist $\Rightarrow (n^2)^{(p-1)/2} \equiv -1 \pmod{p}$
$\Rightarrow n^{p-1} \equiv -1 \pmod{p}$. Nach dem kleinen Satz von Fermat ist aber $n^{p-1} \equiv 1 \pmod{p}$. Widerspruch!

42. $1111^{2^{1111}} \bmod 100 = 11^{2^{1111}} \bmod 100$

$1111^{2^{1111}} \equiv 11^{2^{1111}} \pmod{100}$

$11^{2^1} \equiv \mathbf{21} \pmod{100}$,

$11^{2^2} \equiv 11^4 \equiv (11^2)^2 \equiv 21^2 \equiv 41 \pmod{100}$,

$11^{2^3} \equiv 11^8 \equiv (11^4)^2 \equiv 41^2 \equiv 81 \pmod{100}$,

$11^{2^4} \equiv (11^{2^3})^2 \equiv 81^2 \equiv 61 \pmod{100}$,

$11^{2^5} \equiv (11^{2^4})^2 \equiv 61^2 \equiv \mathbf{21} \pmod{100}$, usw.

$11^{2^{1111}} \equiv 11^{2^{4\cdot 277+3}} \equiv 11^{2^3} \equiv 81 \pmod{100}$.