Vorlesung/Übung *Mathematik und Logik (WIN)* im 2010

2. Prüfungstermin, am 2012-03-16, Lösung

Name: MatNr: | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

1. Wenn wir einen Beweis für die Aussage A haben, dieser aber nur korrekt ist, wennn B gilt, dann haben wir einen Beweis von
   - [ ] $A \Rightarrow B$
   - [ ] $A \vee B$
   - [ ] $A \wedge B$
   - [x] $B \Rightarrow A$

2. In einem Beweis gelangen wir zu folgender Situation:
   Annahmen: $a \in \mathbb{Z}$; $b \in \mathbb{Z}$; $c \in \mathbb{Z}$; $x \in \mathbb{Z}$; $y \in \mathbb{Z}$; $\forall_{a \in \mathbb{Z}} \exists_{c \in \mathbb{Z}} c = z \cdot a$; $\exists_{z \in \mathbb{Z}} c = z \cdot b$; $c = (x \cdot y) \cdot a$.
   Zu zeigen: $\exists_{z \in \mathbb{Z}} c = z \cdot a$.
   Welche logische Schlußregel kann hier sinnvollerweise benutzt werden?
   - [x] Allquantor-Elimination
   - [ ] Existenzquantor-Elimination
   - [x] Existenzquantor-Introduktion
   - [ ] Allquantor-Introduktion

3. Welche der folgenden Gleichungen hat eine ganzzahlige Lösung?
   - [ ] $26060 \cdot x + 10 \cdot y = 5$
   - [ ] $56515 \cdot x + 5 \cdot y = 1$
   - [ ] $25650 \cdot x + 10 \cdot y = 2$
   - [x] $56585 \cdot x + 5 \cdot y = 5$

4. Welche der folgenden Eigenschaften muß jede Äquivalenzrelation erfüllen?
   - [ ] $x \equiv z \Rightarrow x \equiv y \vee y \equiv z$
   - [ ] $(x \equiv y \Rightarrow y \equiv z) \Rightarrow x \equiv z$
   - [ ] $x \equiv y \wedge y \equiv x \Rightarrow x = y$
   - [x] $x \equiv y \wedge y \equiv z \Rightarrow x \equiv z$

5. Z bezeichne die Aussage, daß es unendlich viele Primzahlzwillinge gibt. Angenommen, jemand hat einen Beweis von $0 = 1 \Rightarrow Z$ gefunden. Was läßt sich daraus schließen?
   - [ ] Es muß ein Fehler im Beweis sein.
   - [x] Eigentlich gar nichts.
   - [ ] Es gibt nicht unendlich viele Primzahlzwillinge.
   - [ ] Es gibt unendlich viele Primzahlzwillinge

6. Welche der folgenden Formeln drückt aus, daß C die Konjunktion der Aussagen A und B ist?
   - [x] $(C \Rightarrow A) \wedge (C \Rightarrow B) \wedge \forall_{D \in \mathbb{P}} (D \Rightarrow A) \wedge (D \Rightarrow B) \Rightarrow (D \Rightarrow C)$
   - [ ] $(C \Rightarrow A) \wedge (C \Rightarrow B) \wedge \forall_{D \in \mathbb{P}} (A \Rightarrow D) \wedge (B \Rightarrow D) \Rightarrow (D \Rightarrow C)$
   - [ ] $(A \Rightarrow C) \wedge (B \Rightarrow C) \wedge \forall_{D \in \mathbb{P}} (A \Rightarrow D) \wedge (B \Rightarrow D) \Rightarrow (C \Rightarrow D)$
   - [ ] $(C \Rightarrow A) \wedge (C \Rightarrow B) \wedge \forall_{D \in \mathbb{P}} (D \Rightarrow A) \wedge (D \Rightarrow A) \Rightarrow (C \Rightarrow D)$

7. Im Laufe eines Beweises kommen wir zu folgender Situation:
   Annahmen: $(A \Rightarrow B) \vee (A \Rightarrow D)$, D, $B \vee C \Rightarrow A$.
   Zu zeigen: $B \vee D$.
   Welche logische Schlußregel ist günstig um forzufahren?
   - [ ] $\vee$-Elimination
   - [x] $\vee$-Introduktion
   - [ ] $\Rightarrow$-Elimination
   - [ ] $\Rightarrow$-Introduktion

8. Im Laufe eines Beweises, in dem bisher die Variable x nicht vorgekommen ist, argumentieren wir im nächsten Schritt mit: „Sei nun $x \in \mathbb{Z}$; wir zeigen $5 \cdot x \equiv 7 \pmod{m}$." Welche logische Schlußregel wird dabei angewendet?
   - [ ] $\forall$-Elimination
   - [ ] $\exists$-Introduktion
   - [ ] $\exists$-Elimination
   - [x] $\forall$-Introduktion

9. Mitten in einem Beweis wird folgendermaßen argumentiert: „Zu zeigen: n ist eine mindestens 300-stellige Primzahl. Dazu zeigen wir zuerst, daß n mindestens 300 Stellen hat, und dann, daß n eine Primzahl ist.“ Welche logische Schlußregel wird hier verwendet?

   ☐ $\wedge$-Elimination
   ☐ $\vee$-Elimination
   ☐ $\vee$-Introduktion
   ☒ $\wedge$-Introduktion

10. Welche der folgenden Formeln ist in boolscher Logik äquivalent zu $A \vee B$?

   ☒ $\neg B \Rightarrow A$
   ☐ $A \Rightarrow \neg B$
   ☒ $\neg A \Rightarrow B$
   ☐ $B \Rightarrow \neg A$

11. Mit welcher Operation ist die Kongruenz modulo m nicht verträglich?

   ☐ Addition;
   ☐ Substraktion;
   ☐ Multiplikation;
   ☒ Division;

12. Für jede Zahl q möchten wir beweisen:
   $\forall_{n\epsilon\mathbb{N}} \sum_{k=0}^{n} \binom{n}{k} = 2^n$.
   Was ist im Induktionsschritt zu zeigen?

   ☐ $\forall_{n\epsilon\mathbb{N}}(\sum_{k=0}^{n} \binom{n}{k} = 2^n) \Rightarrow \forall_{n\epsilon\mathbb{N}} \sum_{k=0}^{n+1} \binom{n+1}{k} = 2^{n+1}$
   ☒ $\forall_{n\epsilon\mathbb{N}} \sum_{k=0}^{n} \binom{n}{k} = 2^n \Rightarrow \sum_{k=0}^{n+1} \binom{n+1}{k} = 2^{n+1}$
   ☐ $\forall_{n\epsilon\mathbb{N}} \sum_{k=0}^{n} \binom{n}{k} = 2^n \Rightarrow \sum_{k=0}^{n+1} \binom{n}{k} = 2^{n+1}$
   ☐ $\forall_{n\epsilon\mathbb{N}} \sum_{k=0}^{n} \binom{n}{k} = 2^n \Rightarrow \forall_{n\epsilon\mathbb{N}} \sum_{k=0}^{n+1})\binom{n}{k} = 2^{n+1}$

13. Wir haben $A \vee B$ bewiesen, und dann auch noch $A \Rightarrow Q$. Was fehlt uns noch, damit wir mit einer $\vee$-Elimination auf unser Beweisziel Q schließen können?

   ☐ $Q \Rightarrow B$
   ☐ $A \Rightarrow B$
   ☐ $A \wedge B \Rightarrow Q$
   ☒ $B \Rightarrow Q$

14. Von einem 29. Februar bis zu nächsten vergehen bekanntlich $4 \cdot 365 + 1$ Tage. (Das stimmt zumindest zwischen 1900 und 2100.) Im heurigen Jahr fiel er auf einen Mittwoch. Die Wochentage, Sonntag bis Samstag, codieren wir mit den den Zahlen 0 bis 6. Wie lassen sich diejenigen Schaltjahre x charakterisieren, in welchen der 29. Februar ebenfalls auf einen Mittwoch fällt?

   ☒ $x \equiv 0 \pmod 4 \wedge \frac{x}{4} \cdot (4 \cdot 365 + 1) \equiv 0 \pmod 7$
   ☐ $x \equiv 0 \pmod 4 \wedge \frac{x}{4} \cdot (4 \cdot 365 + 1) \equiv 3 \pmod 7$
   ☐ $x \equiv 0 \pmod 4 \wedge \frac{x-2012}{4} \cdot (4 \cdot 365 + 1) \equiv 0 \pmod 7$
   ☐ $x \equiv 0 \pmod 4 \wedge \frac{x-2012}{4} \cdot (4 \cdot 365 + 1) \equiv 3 \pmod 7$

15. Welche der folgenden Gleichungen erfüllt die Addition natürlicher Zahlen?

   ☐ $(Sm) + (Sn) = S(m + n)$
   ☒ $(Sm) + (Sn) = S(S(n + m))$
   ☐ $(Sm) + n = S(m + Sn)$
   ☐ $(Sm) + (Sn) = S(Sm + Sn)$

16. Welchen Datentyp habe die Beweise einer Existenzaussage?

   ☐ Funktionen
   ☐ Relationen
   ☐ Paare
   ☒ Abhängige Paare

17. Für welche ganze Zahl r gilt

$$3^{1071} \equiv r \pmod{15}$$

- ☐ $r = 1$
- ☒ $r = -3$
- ☐ $r = 6$
- ☐ $r = 7$

18. Welche der folgenden Mengen ist gleichmächtig zu $\mathbb{Q} \times \mathbb{N}$?

- ☐ $\mathbb{N} \to \mathbb{Z}_3$
- ☒ $\mathbb{N} \times \mathbb{Z} \times \mathbb{Q}$
- ☐ $\mathbb{N} \to \mathbb{Z}$
- ☐ $\mathbb{Q} \to \mathbb{N}$

19. $\varphi(17) =$

- ☐ 1
- ☐ 4
- ☐ 8
- ☒ 16

20. Wozu kann der erweiterte euklidische Algorithmus direkt verwendet werden?

- ☐ Zur Berechnung hoher Potenzen modulo m.
- ☐ Zum Testen, ob eine große Zahl eine Primzahl ist.
- ☐ Zum Auffinden aller Primfaktoren.
- ☒ Zum Invertieren modulo m.

21. Welche Zahl wird mit $\varphi(m)$ bezeichnet?

- ☐ Die Anzahl der Lösungen von $x^{m-1} \equiv 1 \pmod{m}$.
- ☐ Die Anzahl der Elemente von $\mathbb{Z}_m$.
- ☒ Die Anzahl der Elemente in $\mathbb{Z}_m^*$.
- ☐ Die Anzahl der Teiler von m.

22. Warum kommt die Methode des sukzessiven Quadrierens beim RSA-Verfahren zur Anwendung?

- ☐ Es müssen viele quadratische Gleichungen gelöst werden
- ☐ Sie ist notwendig zur Berechnung der Eulerschen φ-Funktion.
- ☐ Sie hilft bei der Berechnung hoher Potenzen ganzer Zahlen.
- ☒ Von zu berechnenden Potenzen werden nur die Reste bei Division durch eine andere Zahl benötigt.

23. Mit $>$ bezeichnen wir eine Relation in einer Menge A von Personen, und $a > b$ bedeute „a liebt b". Gegeben sei die Formel:
$\forall_{a \epsilon A}(\exists_{b \epsilon A} b > a \wedge a \neq b) \wedge \forall_{b \epsilon A} \forall_{c \epsilon A} b > a \wedge c > a \Rightarrow b = c$. Was bedeutet diese?

- ☒ Jede Person wird von genau einer anderen geliebt, nicht aber von sich selbst.
- ☐ Jede Person liebt genau eine andere, nicht aber sich selbst.
- ☐ Alle lieben sich untereinander, aber nicht sich selbst.
- ☐ Alle Personen, die sich nicht selbst lieben, lieben genau eine andere.

24. Welche der folgenden aussagenlogischen Formeln ist unerfüllbar?

- ☐ $A \Rightarrow \neg A$
- ☒ $(A \Rightarrow \neg A) \wedge A$
- ☐ $(B \Rightarrow A) \wedge A \wedge \neg B$
- ☐ $(A \vee B) \wedge (\neg A \vee \neg B)$

25. A und B seien Aussagen. Dann ist $A \vee B$ die

- [ ] schwächste Aussage P, sodaß $P \Rightarrow A$ und $P \Rightarrow B$
- [x] stärkste Aussage P, sodaß $A \Rightarrow P$ und $B \Rightarrow P$
- [ ] stärkste Aussage P, sodaß $P \Rightarrow A$ und $P \Rightarrow B$
- [ ] schwächste Aussage P, sodaß $A \Rightarrow P$ und $B \Rightarrow P$

26. X sei ein Datentyp, und $P(x)$ fur jedes $x \epsilon X$ eine Aussage. Dann ist $\forall_{x \epsilon X} P(x)$ die

- [ ] schwächste Aussage Q, sodaß $\forall_{x \epsilon X} P(x) \implies Q$
- [x] schwächste Aussage Q, sodaß $\forall_{x \epsilon X} Q \implies P(x)$
- [ ] stärkste Aussage Q, sodaß $\forall_{x \epsilon X} Q \implies P(x)$
- [ ] stärkste Aussage Q, sodaß $\forall_{x \epsilon X} P(x) \implies Q$

27. Die Zahl a sei durch ihre Oktalentwicklung gegeben: $a = 60512613562562323473230000003$.
Bestimmen Sie den Rest von a bei Division durch 3.

- [ ] 0
- [x] 1
- [ ] 2
- [ ] 3

28. Welche der folgenden logischen Äquivalenzen ist auch dann allgemeingültig, wenn es mehr als 2 Wahrheitswerte gibt?

- [ ] $(A \wedge B) \Rightarrow C \Leftrightarrow (A \Rightarrow C) \vee (B \Rightarrow C)$
- [x] $(A \vee B) \wedge C \Leftrightarrow (A \wedge C) \vee (B \wedge C)$
- [ ] $(A \vee B) \Rightarrow C \Leftrightarrow (A \Rightarrow C) \vee (B \Rightarrow C)$
- [ ] $(A \vee B) \wedge C \Leftrightarrow (A \vee C) \wedge (B \vee C)$

29. Bestimmen Sie zu $(A \wedge B) \vee (C \wedge D)$ eine möglichst einfache disjunktive Normalform. Aus wieviel Klauseln besteht sie?

- [ ] 1
- [x] 2
- [ ] 3
- [ ] 4

30. Welche Eigenschaft muß eine wohlfundierte Relation erfüllen?

- [ ] ist symmetrisch;
- [ ] ist antisymmetrisch;
- [ ] enthält ein kleinstes Element;
- [x] ist für Induktionsbeweise geeignet;

31. Durch Rechnung stellen wir fest, daß $7^{23456788999} \equiv 6208169143 \pmod{23456789000}$. Was können wir daraus schließen?

- [ ] 23456789000 ist eine Primzahl.
- [ ] 23456789000 könnte eine Primzahl sein.
- [x] 23456789000 ist eine zusammengesetzte Zahl.
- [ ] Dies ist ein Hinweis darauf, daß 23456789000 eine zusammengesetzte Zahl ist.

32. Welche der folgenden Formeln ist keine Hornklaus bzw. nicht als Konjunktion von Hornklausen darstellbar?

- [x] $\neg S \Rightarrow P \vee T$;
- [ ] $K \vee T \Rightarrow \neg S$;
- [ ] $\neg K \wedge P \Rightarrow T$;
- [ ] $B \wedge W \Rightarrow T \wedge D$;