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

1. Prüfungstermin, am 2012-01-20, Lösung

Name: MatNr: 0 0 0 0 0 0 0

1. Wenn wir die Aussage A bewiesen haben, nicht aber B, dann haben wir einen Beweis von
   - [ ] $A \Rightarrow B$
   - [x] $A \vee B$
   - [ ] $A \wedge \neg B$
   - [ ] $A \Rightarrow \neg B$

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

3. Welche der folgenden Gleichungen hat eine ganzzahlige Lösung?
   - [ ] $2600012 \cdot x + 14 \cdot y = 5$
   - [ ] $2600012 \cdot x + 14 \cdot y = 1$
   - [x] $2600012 \cdot x + 13 \cdot y = 2$
   - [ ] $2599987 \cdot x + 13 \cdot y = 7$

4. Welche der folgenden Eigenschaften muß eine Äquvalenzrelation NICHT erfüllen?
   - [x] $x \equiv z \Rightarrow x \equiv y \vee y \equiv z$
   - [ ] $x \equiv x$
   - [ ] $x \equiv y \Rightarrow y \equiv x$
   - [ ] $x \equiv y \wedge y \equiv z \Rightarrow x \equiv z$

5. Z bezeichne die Aussage, daß es unendlich viele Primzahlzwillinge gibt. Angenommen, jemand hat einen Beweis von $Z \Rightarrow 0 = 1$ gefunden. Was läßt sich daraus schließen?
   - [ ] Es muß ein Fehler im Beweis sein.
   - [ ] Dann ist auch $1 = 2$.
   - [x] Es gibt nicht unendlich viele Primzahlzwillinge.
   - [ ] Die Fundamente der Mathematik sind widersprüchlich.

6. Welche der folgenden Formeln drückt aus, daß d der größte gemeinsame Teiler von a und b ist?
   - [ ] $d|a \wedge d|b \wedge \forall_{z \in \mathbb{Z}} a|z \wedge b|z \Rightarrow z|d$
   - [ ] $a|d \wedge b|d \wedge \forall_{z \in \mathbb{Z}} a|z \wedge b|z \Rightarrow d|z$
   - [x] $d|a \wedge d|b \wedge \forall_{z \in \mathbb{Z}} z|a \wedge z|b \Rightarrow z|d$
   - [ ] $d|a \wedge d|b \wedge \forall_{z \in \mathbb{Z}} z|a \wedge z|a \Rightarrow d|z$

7. Im Laufe eines Beweises kommen wir zu folgender Situation:
   Annahmen: $(A \Rightarrow B) \vee (C \Rightarrow D)$, $A \vee C$.
   Zu zeigen: $B \vee D$.
   Welche logische Schlußregel ist günstig um forzufahren?
   - [x] $\vee$-Elimination
   - [ ] $\vee$-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 $x \in \mathbb{Z}$, sodaß $5 \cdot x \equiv 7 \pmod{m}$.“
   Welche logische Schlußregel wird dabei angewendet?
   - [ ] $\forall$-Elimination
   - [ ] $\exists$-Introduktion
   - [x] $\exists$-Elimination
   - [ ] $\forall$-Introduktion

9. Mitten in einem Beweis wird folgendermaßen argumentiert: „Zu zeigen: n ist eine Primzahl. Dazu zeigen wir zuerst, daß dies für gerade n gilt, und dann, daß es auch für ungerade n gilt.“ Welche logische Schlußregel wird hier verwendet?

- [ ] $\wedge$-Elimination
- [x] $\vee$-Elimination
- [ ] $\vee$-Introduktion
- [ ] $\wedge$-Introduktion

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

- [x] $B \vee \neg A$
- [ ] $\neg B \vee A$
- [ ] $\neg A \wedge B$
- [ ] $A \wedge \neg B$

11. Welche der folgenden Formeln drückt aus, daß die Multiplikation mit der Kongruenz modulo m verträglich ist?

- [ ] $a \equiv b \wedge c \equiv d \Rightarrow a \cdot b \equiv c \cdot d$
- [ ] $(a \cdot c \equiv b \cdot c \Rightarrow a \equiv b) \wedge (d \cdot a \equiv d \cdot b \Rightarrow a \equiv b)$
- [x] $a \equiv b \wedge c \equiv d \Rightarrow a \cdot c \equiv b \cdot d$
- [ ] $a \cdot b \equiv b \cdot a$

12. Für jede Zahl q möchten wir beweisen:
$\forall_{n \in \mathbb{N}} \sum_{k=0}^{n-1} q^k = \frac{q^n - 1}{q-1}$.
Was ist im Induktionsschritt zu zeigen?

- [ ] $\forall_{n \in \mathbb{N}} (\sum_{k=0}^{n-1} q^k = \frac{q^n-1}{q-1}) \Rightarrow \forall_{n \in \mathbb{N}} \sum_{k=0}^{n} q^k = \frac{q^{n+1}-1}{q-1}$
- [x] $\forall_{n \in \mathbb{N}} \sum_{k=0}^{n-1} q^k = \frac{q^n-1}{q-1} \Rightarrow \sum_{k=0}^{n} q^k = \frac{q^{n+1}-1}{q-1}$
- [ ] $\forall_{n \in \mathbb{N}} \sum_{k=0}^{n-1} q^k = \frac{q^n-1}{q-1} \Rightarrow \sum_{k=0}^{n+1} q^k = \frac{q^{n+1}-1}{q-1}$
- [ ] $\forall_{n \in \mathbb{N}} \sum_{k=0}^{n-1} q^k = \frac{q^n-1}{q-1} \Rightarrow \forall_{n \in \mathbb{N}} \sum_{k=0}^{n+1} q^k = \frac{q^{n+1}-1}{q-1})$

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

- [ ] $A \wedge B$
- [x] $A \vee B$
- [ ] $A \Rightarrow B$
- [ ] $B \Rightarrow A$

14. Eine Firma produziert ein Produkt A und ein Produkt B. Pro produzierter Einheit des Produktes A fallen 17 Einheiten Abfall an; bei Produkt B sind es 28 Einheiten. Der Abfall kann verkauft werden, allerdings nur in Paketen zu 100 Einheiten. 34 Einheiten Abfall aus einer früheren Produktion stehen noch herum. Die nächste Produktion sollte so geplant werden, daß am Ende kein Abfall mehr vorhanden ist. Durch welche Gleichung kann diese Einschränkung beschrieben werden?

- [ ] $28 \cdot x + 17 \cdot y + 34 = 100$
- [ ] $28 \cdot x \equiv -34 \pmod{100} \wedge 17 \cdot y \equiv -34 \pmod{100}$
- [x] $28 \cdot x + 17 \cdot y + 34 \equiv 0 \pmod{100}$
- [ ] $28 \cdot x + 17 \cdot y + 34 \cdot z = 100$

15. Welche der folgenden Gleichungen erfüllt die Multiplikation?

- [x] $(Sm) \cdot n = m \cdot n + n$
- [ ] $(Sm) \cdot (Sn) = m \cdot n + n + m$
- [ ] $(Sm) \cdot n = S(m \cdot n)$
- [ ] $(Sm) \cdot (Sn) = S(m \cdot n)$

16. Welchen Datentyp habe die Beweise einer Konjunktion?

- [ ] Funktionen
- [ ] Relationen
- [x] Paare
- [ ] Abhängige Paare

17. Bestimmen Sie eine ganze Zahl r zwischen -10 und $+10$, sodaß

$$2^{1025} \equiv r \pmod{20}.$$

- [ ] $r = 4$
- [ ] $r = -4$
- [ ] $r = 8$
- [x] $r = -8$

18. Welche der folgenden Mengen ist nicht gleichmächtig zu den anderen?

- [ ] $\mathbb{Z}_3 \to \mathbb{N}$
- [ ] $\mathbb{N} \times \mathbb{Z} \times \mathbb{Q}$
- [x] $\mathbb{N} \to \mathbb{Z}$
- [ ] $\mathbb{Q}$

19. $\varphi(10) =$

- [ ] 1
- [x] 4
- [ ] 5
- [ ] 9

20. Wozu dient der erweiterte euklidische Algorithmus NICHT?

- [x] Zum Potenzieren modulo m.
- [ ] Zum Auffinden von ganzzahligen Lösungen einer Gleichung.
- [ ] Zum Lösen von Kongruenzen.
- [ ] Zum Invertieren modulo m.

21. Welche der folgenden Beschreibungen entspricht NICHT $\varphi(m)$?

- [x] Die Anzahl der Lösungen von $x^{m-1} \equiv 1 \pmod{m}$.
- [ ] Die Anzahl der invertierbaren Elemente von $\mathbb{Z}_m$.
- [ ] Die Anzahl der Elemente in $\mathbb{Z}_m^*$.
- [ ] Die Anzahl der natürlichen Zahlen bis m, die zu m teilerfremd sind.

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 ist notwendig für die Primfaktorzerlegung.
- [x] Es müssen hohe Potenzen berechnent werden.

23. Mit $>$ bezeichnen wir eine Relation in der Menge A, und $a > b$ bedeute, daß a besser ist als b. Gegeben sei die Formel:
$\forall_{a \epsilon A}(\exists_{b \epsilon A} b > a \wedge P(b)) \wedge \forall_{b \epsilon A} \forall_{c \epsilon A} b > a \wedge c > a \wedge P(b) \wedge P(c) \Rightarrow b = c$. Was bedeutet diese?

- [ ] Wenn es zu einem Element von A ein besseres mit der Eigenschaft P gibt, so ist dieses eindeutig bestimmt.
- [x] Zu jedem Element von A gibt es genau ein besseres, das die Eigenschaft P hat.
- [ ] Alle Elemente von A, welche die Eigenschaft P haben, sind besser als jene, die diese Eigenschaft nicht haben.
- [ ] Je zwei Elemente, die die Eigenschaft P haben und von denen eines besser ist als das andere, sind gleich.

24. Welche der folgenden aussagenlogischen Formeln ist erfüllbar?

- [ ] $A \iff \neg A$
- [x] $(A \Rightarrow \neg A) \wedge \neg A$
- [ ] $(A \Rightarrow B) \wedge A \wedge \neg B$
- [ ] $(A \vee B) \wedge \neg A \wedge \neg B$

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

- [ ] schwächste Aussage P, sodaß $A \implies P \wedge B$
- [ ] stärkste Aussage P, sodaß $A \implies P \wedge B$
- [ ] stärkste Aussage P, sodaß $P \wedge A \implies B$
- [x] schwächste Aussage P, sodaß $P \wedge A \implies B$

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

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

27. Die Zahl a sei durch ihre Hexadezimalentwicklung gegeben:
$a = A0512A10A56B0000A0A0A05A232357800000023$.
Bestimmen Sie den Rest von a bei Division durch 5.

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

28. Von welcher der folgenden Formeln bedeutet ihre Allgemeingültigkeit NICHT, daß es genau 2 Wahrheitswerte gibt?

- [ ] $\neg(\neg A) \Rightarrow A$
- [ ] $A \vee \neg A$
- [x] $A \Rightarrow \neg(\neg A)$
- [ ] $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$

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

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

30. Die Beweise welcher Aussagen sind Funktionen, bei denen der Datentyp des Funktionsergebnisses vom Input abhängt?

- [ ] Implikationen
- [ ] Disjunktionen
- [x] Allaussagen
- [ ] Existenzaussagen

31. Durch Rechnung stellen wir fest, daß $7^{23456788} \equiv 1 \pmod{23456789}$. Was können wir daraus schließen?

- [ ] 23456789 ist eine Primzahl.
- [x] 23456789 könnte eine Primzahlsein.
- [ ] 23456789 ist eine zusammengesetzte Zahl.
- [ ] Dies ist ein Hinweis darauf, daß 23456789 eine zusammengesetzte Zahl ist.

32. Welche der folgenden Auskünfte ist nicht so gut als Hornklause darstellbar?

- [x] Wenn sich das Auto nicht starten läßt, so gibt es ein Problem mit dem Starter oder der Tank ist leer.
- [ ] Wenn der Starter kaputt ist oder der Tank leer ist, dann läßt sich das Auto nicht starten.
- [ ] Wenn der Starter in Ordnung ist und es Startprobleme gibt, dann ist der Tank leer.
- [ ] Wenn nur noch wenig Benzin im Tank ist, sollte man dringend tanken.