Math 307, Homework #3
Due Wednesday, October 23
SOLUTIONS TO SELECTED PROBLEMS

In this homework we will use many times the following definitions applicable to integers $a, b$ and a positive integer $n$: (1) $a|b \Leftrightarrow (\exists k)(k \in \mathbb{Z} \wedge b = ka)$, and (2) $a \equiv_n b \Leftrightarrow n|a - b$ ($a \equiv_n b$ in Definition (2) is the same as $a \equiv b \pmod{n}$, but it looks better typographically).

1. Show that $[U \wedge P] \Rightarrow [Q \wedge R]$, $P \Leftrightarrow [S \vee T]$, $R \wedge T \vdash U \Rightarrow Q$.

   Proof:

|  | Statement | Explanation |
|---|---|---|
| 1. | $[U \wedge P] \Rightarrow [Q \wedge R]$ | hyp. |
| 2. | $P \Leftrightarrow [S \vee T]$ | hyp. |
| 3. | $R \wedge T$ | hyp. |
| 4. | $U$ | dischargeable hyp. |
| 5. | $T$ | RCS, For 3 |
| 6. | $T \Rightarrow [S \vee T]$ | taut. |
| 7. | $S \vee T$ | MP, For 6, For 5 |
| 8. | $[S \vee T] \Leftrightarrow P$ | CPB, For 2 |
| 9. | $P$ | MPB, For 8, For 7 |
| 10. | $U \wedge P$ | CI, For 4, For 9 |
| 11. | $Q \wedge R$ | MP For 1, For 10 |
| 12. | $Q$ | LCS, For 11 |
| 13. | $U \Rightarrow Q$ | DT, discharge For 4, (4)–(12) unusable |

2. Show that $\sim P \Rightarrow Q$, $P \Rightarrow \sim Q$, $P \Leftrightarrow R \vdash \sim Q \Leftrightarrow R$. (Hint: Recall that $X \Leftrightarrow Y$ is an abbreviation for something.)

   Proof:

|  | Statement | Explanation |
|---|---|---|
| 1. | $\sim P \Rightarrow Q$ | hyp. |
| 2. | $P \Rightarrow \sim Q$ | hyp. |
| 3. | $P \Leftrightarrow R$ | hyp. |
| 4. | $R \Rightarrow P$ | RCS, For 3 |
| 5. | $R \Rightarrow \sim Q$ | SI, For 4, For 2 |
| 6. | $\sim Q$ | dischargeable hyp. |
| 7. | $P$ | MT, For 1, For 6 |
| 8. | $R$ | MPB, For 3, For 7 |
| 9. | $\sim Q \Rightarrow R$ | DT, discharge For 6, (6)–(8) unusable |
| 10. | $\sim Q \Leftrightarrow R$ | CI For 9, For 5 |

3. Show that $R \vee S$, $\sim P$, $Q \vee \sim R$, $P \Leftrightarrow Q \vdash S$.

Proof:

| | Statement | Explanation |
|---|---|---|
| 1. | $R \vee S$ | hyp. |
| 2. | $\sim P$ | hyp. |
| 3. | $Q \vee \sim R$ | hyp. |
| 4. | $P \Leftrightarrow Q$ | hyp. |
| 5. | $Q \Rightarrow P$ | RCS, For 4 |
| 6. | $\sim Q$ | MT, For 5, For 2 |
| 7. | $(Q \vee \sim R) \Leftrightarrow (\sim Q \Rightarrow \sim R)$ | taut. |
| 8. | $\sim Q \Rightarrow \sim R$ | MPB, For 7, For 3 |
| 9. | $\sim R$ | MP, For 8, For 6 |
| 10. | $(R \vee S) \Leftrightarrow (\sim R \Rightarrow S)$ | taut. |
| 11. | $\sim R \Rightarrow S$ | MPB, For 10, For 1 |
| 12. | $S$ | MP, For 11, For 9. |

4. Translate each of the following into a normal English sentence. Also, identify the statement as True or False. For example, the proposition

$$(\forall x)[(x \in \mathbb{Z} \wedge x|24) \Rightarrow x|48]$$

says that "Every divisor of 24 is a divisor of 48". It is True.

(a) $(\forall x)[(x \in \mathbb{N} \wedge x|13) \Rightarrow x \in \{1, 13\}]$

(b) $(\exists a)[a \in \mathbb{N} \wedge (a > 51 \wedge a < 52)]$

(c) $(\forall x)[(x \in \mathbb{N} \wedge x^2 = 2) \Rightarrow x = 5]$

(d) $(\forall x)[x \in \mathbb{N} \Rightarrow (\exists y)[y \in \mathbb{N} \wedge y|x]]$

(e) $(\forall n)[(n \in \mathbb{N} \wedge (4|n \wedge 6|n)) \Rightarrow 24|n]$

(a) The only natural numbers that divide 13 are 1 and 13. TRUE.

(b) There is a natural number that is larger than 51 and smaller than 52. FALSE.

(c) If $x$ is a natural number whose square is 2, then $x = 5$. TRUE.

(d) Every natural number has a divisor. TRUE.

(e) If 4 and 6 both divide a natural number, than 24 also divides it. FALSE.

5. The phrase "the integer $x$ is a perfect square" means $x \in \mathbb{Z} \wedge (\exists y \in \mathbb{Z})[x = y^2]$. Keeping this in mind, write out mathematical statements—using only quantifiers and other math symbols, no English words—which say the same thing as the following sentences. Do not worry about whether the statements are true or false!

(a) For every integer $a$, if $a$ is even then $a^2$ is a multiple of 5.
$(\forall a)[(a \in \mathbb{Z} \wedge 2|a) \Rightarrow 5|a^2]$

(b) 5 is smaller than every integer.
$(\forall a)[a \in \mathbb{Z} \Rightarrow 5 < a]$

(c) Every integer which is a perfect square is also a perfect cube.
$(\forall x)\big[(x \in \mathbb{Z} \wedge (\exists y)[y \in \mathbb{Z} \wedge x = y^2]) \Rightarrow (\exists z)[z \in \mathbb{Z} \wedge x = z^3]\big]$

(d) Every nonzero integer is either a multiple of six or a multiple of seven.
$(\forall x)[(x \in \mathbb{Z} \wedge x \neq 0) \Rightarrow (6|x \vee 7|x)]$

(e) There exists an integer which is larger than every other integer.

(f) There is an element of the set $A$ having the property that every element of the set $B$ divides it.

(g) Every element of the set $A$ is either even or a multiple of 13.

(h) There exists an integer which is not divisible by any divisor of 240.

(i) Every nonzero element of $\mathbb{Z}_5$ has a multiplicative inverse.

(j) For all integers $x$, if $x$ is congruent to three mod eight then there exists an integer $y$ such that $x \cdot y$ is congruent to one mod eight.

(k) There exists an integer $p$ with the following properties: $p$ is even and for every pair of integers $a$ and $b$, if $p$ divides $ab$ then it must divide either $a$ or $b$.

6. In each part, identify the given set by listing all of its elements. For example:

Given the set $\{x \in \mathbb{Z} \,|\, x \equiv_4 3 \wedge 5 \leq x \wedge x \leq 20\}$ you would answer $\{7, 11, 15, 19\}$, as these two sets are equal.

(a) $\{x \in \mathbb{Z}_4 \,|\, (\exists y)[y \in \mathbb{Z}_4 \wedge y \neq 0 \wedge xy = 0]\}$
$\{0, 2\}$

(b) $\{x^3 + 1 \,|\, x \in \mathbb{N}\} \cap \{y \,|\, y \in \mathbb{N} \wedge 1 \leq y \leq 30\}$
$\{1, 2, 9, 28\}$

(c) $\{x \in \mathbb{N} \,|\, (\exists a)(\exists b)[a \in \mathbb{N} \wedge b \in \mathbb{N} \wedge x = a^2 + b^2]\} \cap \{x \,|\, x \in \mathbb{N} \wedge x \leq 20\}$
$\{2, 5, 8, 10, 13, 17, 18, 20\}$

(d) $\{z \in \mathbb{Z}_{30} \,|\, (\exists u)[u \in \mathbb{Z}_{30} \wedge zu = 1]\}$
$\{1, 7, 11, 13, 19, 23, 29\}$

(e) $\{a \,|\, a \in \mathbb{Z} \wedge a \equiv_4 1\} \cap \{b \,|\, b \in \mathbb{Z} \wedge b \equiv_2 0\}$
$\emptyset$

(f) $\{(a, b) \,|\, a \in \mathbb{Z}_2 \wedge b \in \mathbb{Z}_2 \wedge a + b = 1\}$
$\{(0, 1), (1, 0)\}$

(g) $\{x \in \mathbb{N} \,|\, x \equiv_5 1 \wedge x \leq 40\} \cap \{x \in \mathbb{N} \,|\, x \equiv_6 4\}$
$\{16\}$

7. In each part below, use mathematical notation to write the negation of the given statement in such a way that no quantifier is immediately preceded by a negation sign, every universal quantifer is applied to a conditional, and every existential quantifier is applied to a conjunction. In each part, decide which statement is true: the given statement or its negation.

(a) $(\forall y)[y \in \mathbb{Z} \Rightarrow y > 0]$
$(\exists y)[y \in \mathbb{Z} \wedge y \leq 0]$
The second statement is true.

(b) $(\forall x)[(x \in \mathbb{Z} \wedge 2|x) \Rightarrow 4|x]$
$(\exists x)[(x \in \mathbb{Z} \wedge 2|x) \wedge 4 \not| x]$
The second statement is true.

(c) $(\forall x)[x \in \mathbb{Z}_6 \Rightarrow (\exists y)[y \in \mathbb{Z}_6 \wedge x +_6 y = 0]]$
$(\exists x)[x \in \mathbb{Z}_6 \wedge (\forall y)[y \in \mathbb{Z}_6 \Rightarrow x +_6 y \neq 0]]$
The first statement is true.

(d) $(\exists x)[x \in \mathbb{Z}_6 \wedge (\forall y)[y \in \mathbb{Z}_6 \Rightarrow x +_6 y = 0]]$
$(\forall x)[x \in \mathbb{Z}_6 \Rightarrow (\exists y)[y \in \mathbb{Z}_6 \wedge x +_6 y \neq 0]]$
The second statement is true.

(e) $(\forall x)[x \in \mathbb{Z} \Rightarrow (\exists y)[y \in \mathbb{Z} \wedge x = y^2]]$
$(\exists x)[x \in \mathbb{Z} \wedge (\forall y)[y \in \mathbb{Z} \Rightarrow x \neq y^2]]$
The second statement is true.

(f) $(\exists a)[a \in \mathbb{N} \wedge (\forall b)[[b \in \mathbb{N} \wedge a \neq b] \Rightarrow b > a]]$
$(\forall a)[a \in \mathbb{N} \Rightarrow (\exists b)[b \in \mathbb{N} \wedge a \neq b \wedge b \leq a]$
The first statement is true.

(g) $(\exists m)(\exists n)[m, n \in \mathbb{N} \wedge m > n]$

(h) $(\forall m)(\forall n)[m, n \in \mathbb{N} \Rightarrow m > n]$

(i) $(\exists m)[m \in \mathbb{N} \wedge (\forall n)[n \in \mathbb{N} \Rightarrow m > n]$

(j) $(\forall m)[m \in \mathbb{N} \Rightarrow (\exists n)[n \in \mathbb{N} \wedge m > n]$

(k) $(\forall a)(\forall b)[(a, b \in \mathbb{R} \wedge a < b) \Rightarrow (\exists c)[c \in \mathbb{R} \wedge [a < c \wedge c < b]]]$

8. Fill in the blanks in the outline below to prove that $(\forall a, b, k)[[a, b, k \in \mathbb{Z} \wedge (k \geq 1 \wedge a|b)] \Rightarrow a^k|b^k]$.

Proof:

1. Assume $a, b, k \in \mathbb{Z}$ and $k \geq 1$ and $a|b$.
2. $(\exists y)(y \in \mathbb{Z} \wedge b = y \cdot a)$
3. $b = y \cdot a$ for some $y \in \mathbb{Z}$ IE
4. $b^k = y^k a^k$
5. $(\exists u)(u \in \mathbb{Z} \wedge\ b^k = ua^k\ )$ EI
6. $a^k|b^k$
7. $[a, b, k \in \mathbb{Z} \wedge (k \geq 1 \wedge a|b)] \Rightarrow a^k|b^k$ DT, discharge For 1
8. $(\forall a, b, k)[[a, b, k \in \mathbb{Z} \wedge (k \geq 1 \wedge a|b)] \Rightarrow a^k|b^k]$ IU

Answer the following questions:

(i) The above proof used one IE step, one EI step, and one IU step. Label them in column 2 of your proof (the same column with DT in it).

(ii) The definition of $a|b$ used $k$ for the variable in the existential statement. In step 2, why did we change and use $y$ instead?

The variable $k$ was already introduced in step 1, and so to avoid confusion it is best not to use it inside the existential appearing in (2).

(iii) In step 5 we introduced the variable $u$ in the existential statement. Could we have used $k$ here instead? What about $y$?

The variable $k$ could not be used here, as $k$ already plays a different role in this statement (it is the exponent on $a$ and $b$). The variable $y$ *could* technically have been used, but because $y$ already plays a different role in the proof it is best to avoid using it here.

9. Fill in the blanks in the outline below to prove that $(\forall a, b, c)[[a, b, c \in \mathbb{Z} \wedge (a|b \wedge b|c)] \Rightarrow a|c]$. [Hint: Notice that $P$ and $Q$, from step 6, will have to appear in steps 1–5 somewhere.]

Proof:

1. Assume $a, b, c \in \mathbb{Z} \wedge (a|b \wedge b|c)$
2. $(\exists k)[k \in \mathbb{Z} \wedge b = k \cdot a]$
3. $b = P \cdot a$ for some $P \in \mathbb{Z}$ IE
4. $(\exists k)[k \in \mathbb{Z} \wedge c = k \cdot b]$
5. $c = Q \cdot b$ for some $Q \in \mathbb{Z}$ IE
6. $c = Q \cdot b = P \cdot (Qa) = PQ \cdot a$
7. $(\exists r)[r \in \mathbb{Z} \wedge\ c = ra\ ]$ EI
8. $a|c$
9. $[a, b, c \in \mathbb{Z} \wedge (a|b \wedge b|c)] \Rightarrow a|c$ DT, discharge For 1
10. $(\forall a, b, c)[a, b, c \in \mathbb{Z} \wedge (a|b \wedge b|c)] \Rightarrow a|c$ IU

Answer the following questions:

(i) The above proof used two IE steps, one EI step, and one IU step. Label them in column 2 of your proof (the same column with DT in it). You do not have to give reasons for any of the other steps.

(ii) It is okay that we used $k$ in both step 2 and step 4. Why? (This might be hard to explain in words, but at least try to come to some kind of understanding for yourself).

It is okay that we used the same letter $k$ in both places. When a variable is quantified by $\exists$, that variable only has meaning in the scope of that particular quantifier. So the "k" that appears in line 2 only exists on that particular line, and similarly for the "k" that appears in line 4. So there is no chance to get the two entities confused.

10. Fill in the blanks in the outline below to prove that $(\forall n)[(n \in \mathbb{N} \wedge 3 \nmid n) \Rightarrow n^2 \equiv_3 1]$. Also:

(i) There are three uses of the Deduction Theorem in this proof. Label the appropriate DT steps.

(ii) There are two steps at the end of the proof with the phrase "Logical rule?" in bold. For these, label the appropriate rule from symbolic logic that is being used.

| | | |
|---|---|---|
| 1. | Assume $n \in \mathbb{N}$ and $3 \nmid n$ | dys. hyp. |
| 2. | $n \not\equiv_3 0$ | |
| 3. | So either $n \equiv_3 1$ or $n \equiv_3 2$ | |
| 4. | Assume $n \equiv_3 1$. | dys. hyp. |
| 5. | Then $3 \mid n - 1$ | |
| 6. | So $n - 1 = 3 \cdot P$ for some $P \in \mathbb{Z}$ | IE |
| 7. | $n = 3P + 1$ | |
| 8. | $n^2 = 9P^2 + 6P + 1 = 3 \cdot (3P^2 + 2P) + 1$ | |
| 9. | $n^2 - 1 = 3 \cdot (3P^2 + 2P)$ | |
| 10. | $(\exists y)[y \in \mathbb{Z} \wedge n^2 - 1 = 3y]$ | EI |
| 11. | $3 \mid n^2 - 1$ | |
| 12. | $n^2 \equiv_3 1$ | |
| 13. | So $n \equiv_3 1 \Rightarrow n^2 \equiv_3 1$. | DT, discharge for 4 |
| 14. | Now assume $n \equiv_3 2$. | dys. hyp. |
| 15. | Then $3 \mid n - 2$ | |
| 16. | So $n - 2 = 3 \cdot Q$ for some $Q \in \mathbb{Z}$ | IE |
| 17. | $n = 3Q + 2$ | |
| 18. | $n^2 = 9Q^2 + 12Q + 4 = 3 \cdot (3Q^2 + 4Q + 1) + 1$ | |
| 19. | $n^2 - 1 = 3 \cdot (3Q^2 + 4Q + 1)$ | |
| 20. | $(\exists y)[y \in \mathbb{Z} \wedge n^2 - 1 = 3y]$ | EI |
| 21. | $3 \mid n^2 - 1$ | |
| 22. | $n^2 \equiv_3 1$ | |
| 23. | So $n \equiv_3 2 \Rightarrow n^2 \equiv_3 1$. | DT, discharge for 14 |
| 24. | We therefore have $(n \equiv_3 1 \vee n \equiv_3 2) \Rightarrow n^2 \equiv_3 1$ | IC for 13 and 23 |
| 25. | So $n^2 \equiv_3 1$ | MP for 24,3 |
| 26. | $(n \in \mathbb{N} \wedge 3 \nmid n) \Rightarrow n^2 \equiv_3 1$ | DT, discharge for 1 |
| 27. | $(\forall n)[(n \in \mathbb{N} \wedge 3 \nmid n) \Rightarrow n^2 \equiv_3 1]$. | IU |

Now try it yourself. Give line proofs for the following statements:

11. $(\forall n)[(n \in \mathbb{N} \wedge n \equiv_6 3) \Rightarrow n^2 + 2n + 10 \equiv_{12} 1]$

| | | |
|---|---|---|
| 1. | Assume $n \in \mathbb{N}$ and $n \equiv_6 3$ | dis. hyp. |
| 2. | $6 \| n - 3$ | |
| 3. | $(\exists k)[k \in \mathbb{Z} \wedge n - 3 = 6k]$ | |
| 4. | $n - 3 = 6k$ for some $k$ in $\mathbb{Z}$ | IE |
| 5. | $n = 6k + 3$ | |
| 6. | So $n^2 + 2n + 10 = (6k+3)^2 + 2(6k+3) + 10$<br>$= 36k^2 + 36k + 9 + 12k + 6 + 10 = 36k^2 + 48k + 25$ | |
| 7. | So $n^2 + 2n + 10 = 36k^2 + 48k + 24 + 1 = 12(3k^2 + 4k + 2) + 1$ | |
| 8. | $(n^2 + 2n + 10) - 1 = 12(3k^2 + 4k + 2)$ | |
| 9. | $(\exists r)[r \in \mathbb{Z} \wedge (n^2 + 2n + 10) - 1 = 12r]$ | EI |
| 10. | $12 \| (n^2 + 2n + 10) - 1$ | |
| 11. | $n^2 + 2n + 10 \equiv_{12} 1$ | |
| 12. | $(n \in \mathbb{N} \wedge n \equiv_6 3) \Rightarrow n^2 + 2n + 10 \equiv_{12} 1$ | DT for 1; 1-11 unusable |
| 13. | $(\forall n)\big[(n \in \mathbb{N} \wedge n \equiv_6 3) \Rightarrow n^2 + 2n + 10 \equiv_{12} 1\big]$ | IU |

12. $(\forall n)[(n \in \mathbb{N} \wedge n \equiv_5 2) \Rightarrow (2 \nmid n \vee n^2 \equiv_{20} 4)]$

[Hint: Remember that $(X \vee Y) \Leftrightarrow (\sim X \Rightarrow Y)$. Use DT twice in this proof.]

| | | |
|---|---|---|
| 1. | Assume $n \in \mathbb{N}$ and $n \equiv_5 2$ | dis. hyp. |
| 2. | $5 \| n - 2$ | |
| 3. | $(\exists k)[k \in \mathbb{Z} \wedge n - 2 = 5k]$ | |
| 4. | $n - 2 = 5r$ for some $r$ in $\mathbb{Z}$ | IE |
| 5. | $n = 5r + 2$ | |
| 6. | Assume $2 \| n$ | dis. hyp. |
| 7. | $(\exists k)[k \in \mathbb{Z} \wedge n = 2k]$ | |
| 8. | $n = 2s$ for some $s$ in $\mathbb{Z}$ | IE |
| 9. | $5r + 2 = n = 2s$ | |
| 10. | $r = 2s - 4r - 2 = 2(s - 2r - 1)$ | |
| 11. | $(\exists t)[t \in \mathbb{Z} \wedge r = 2t]$ | EI |
| 12. | $r = 2t$ for some $t \in \mathbb{Z}$ | IE |
| 13. | $n = 5r + 2 = 10t + 2$ | |
| 14. | So $n^2 = (10t + 2)^2 = 100t^2 + 40t + 4$ | |
| 15. | $n^2 - 4 = 100t^2 + 40t = 20(5t^2 + 2t)$ | |
| 16. | $(\exists u)[u \in \mathbb{Z} \wedge n^2 - 4 = 20u]$ | EI |
| 17. | $20 \| n^2 - 4$ | |
| 18. | $n^2 \equiv_{20} 4$ | |
| 19. | $2 \| n \Rightarrow n^2 \equiv_{20} 4$ | DT for 6; 6-19 unusable |
| 20. | $(2 \nmid n \vee n^2 \equiv_{20} 4)$ | taut. $(X \vee Y) \Leftrightarrow (\sim X \Rightarrow Y)$ |
| 21. | $(n \in \mathbb{N} \wedge n \equiv_5 2) \Rightarrow (2 \nmid n \vee n^2 \equiv_{20} 4)$ | DT for 1; 1-20 unusable |
| 22. | $(\forall n)[(n \in \mathbb{N} \wedge n \equiv_5 2) \Rightarrow (2 \nmid n \vee n^2 \equiv_{20} 4)]$ | IU |