Math 307, Homework #2
Due Wednesday, October 16
SOLUTIONS to selected problems

1. In each of the following give a disjunction that is equivalent to the given proposition:
   (a) $P \Rightarrow Q$
   (b) $\sim P \Rightarrow Q$
   (c) $P \Rightarrow \sim Q$

   Answers: (a) $\sim P \vee Q$; (b) $P \vee Q$; (c) $\sim P \vee \sim Q$

2. Translate the following into a symbolic logic problem, then provide a proof:

   Given: If Smith wins the nomination, he will be happy, and if he is happy, he is not a good campaigner. But if he loses the nomination, he will lose the confidence of the party. He is not a good campaigner if he loses the confidence of the party. If he is not a good campaigner, then he should resign from the party. Either Smith wins the nomination or he loses it.

   Prove: Smith should resign from the party.

For questions #2 and #3, copy the whole proof onto a sheet of your homework. For all of the logic proofs from now on, you can use any of the routines on the page of "Logic Rules" from the course website.

3. Fill in the blanks to give a proof of $R \vee [P \wedge Q], \sim Q \vdash R$.

   Proof:

	Statement	Explanation
1.	$R \vee [P \wedge Q]$	hyp.
2.	$\sim R$	dischargeable hyp.
3.	$(R \vee [P \wedge Q]) \Leftrightarrow (\sim R \Rightarrow [P \wedge Q])$	taut. (see p.48)
4.	$\sim R \Rightarrow [P \wedge Q]$	MPB For 3, For 1
5.	$P \wedge Q$	MP For 4, For 2
6.	Q	RCS, For 5
7.	$\sim Q$	hyp.
8.	$Q \wedge \sim Q$	CI For 6, For 7
9.	R	II, discharge For 2, steps (2)–(8) are unusable now

4. Fill in the blanks to give a proof of $(P \wedge \sim Q) \Rightarrow (R \Rightarrow Q) \vdash P \Rightarrow [Q \vee \sim R]$. [Note: This proof uses both DT and Indirect Inference].

   Proof:

	Statement	Explanation
1.	$(P \wedge \sim Q) \Rightarrow (R \Rightarrow Q)$	hyp.
2.	P	dis. hyp.
3.	$\sim [Q \vee \sim R]$	dis. hyp.
4.	$\sim [Q \vee \sim R] \Leftrightarrow \sim Q \wedge R$	taut.
5.	$\sim Q \wedge R$	MPB For 4, For 3
6.	$\sim Q$	LCS For 5
7.	$P \wedge \sim Q$	CI For 2, For 6
8.	$R \Rightarrow Q$	MP For 1, For 7
9.	$\sim R$	MT For 8, For 6
10.	R	RCS For 5
11.	$R \wedge \sim R$	CI For 10, For 9
12.	$Q \vee \sim R$	II, discharge For 3, (3)–(11) now unusable
13.	$P \Rightarrow [Q \vee \sim R]$	DT, discharge For 2, (2)–(12) now unusable

5. Show that $[P \wedge Q] \Rightarrow R$, $\sim R$, $P \vdash \sim Q$.

Proof:

	Statement	Explanation
1.	$[P \wedge Q] \Rightarrow R$	hyp.
2.	$\sim R$	hyp.
3.	$\sim [P \wedge Q]$	MT, For 1, For 2
4.	$\sim [P \wedge Q] \Leftrightarrow [P \Rightarrow \sim Q]$	taut.
5.	$P \Rightarrow \sim Q$	MPB, For 4, For 3
6.	P	hyp.
7.	$\sim Q$	MP For 5, For 6

6. Show that $P \Rightarrow Q$, R, $R \Rightarrow [Q \Rightarrow P] \vdash P \Leftrightarrow Q$.

Proof:

	Statement	Explanation
1.	$P \Rightarrow Q$	hyp.
2.	R	hyp.
3.	$R \Rightarrow [Q \Rightarrow P]$	hyp.
4.	$Q \Rightarrow P$	MP For 3, For 2
5.	$P \Leftrightarrow Q$	CI For 1, For 4.

7. Show that $P \Rightarrow \sim Q$, $\sim R \Rightarrow Q \vdash P \Rightarrow R$.

Proof:

	Statement	Explanation
1.	$P \Rightarrow \sim Q$	hyp.
2.	$\sim R \Rightarrow Q$	hyp.
3.	P	dischargeable hyp.
4.	$\sim Q$	MP For 1, For 3
5.	R	MT For 2, For 4
6.	$P \Rightarrow R$	DT, discharge For 3, (3)–(5) now unusable.

8. Show that $\sim P \Rightarrow Q$, $T \Rightarrow \sim P$, $\sim [Q \vee R] \vdash \sim T$.

Proof:

	Statement	Explanation
1.	$\sim P \Rightarrow Q$	hyp.
2.	$T \Rightarrow \sim P$	hyp.
3.	$\sim [Q \vee R]$	hyp.
4.	T	dischargeable hyp.
5.	$\sim P$	MP For 2, For 4
6.	Q	MP For 1, For 5
7.	$\sim [Q \vee R] \Leftrightarrow [\sim Q \wedge \sim R]$	taut.
8.	$\sim Q \wedge \sim R$	MPB For 7, For 3
9.	$\sim Q$	LCS, For 8
10.	$Q \wedge \sim Q$	CI For 6, For 9
11.	$\sim T$	II, discharge For 4, (4)–(10) now unusable

9. Show that $\sim P \Rightarrow Q$, $Q \Rightarrow [R \Rightarrow S]$, $\sim S \vdash R \Rightarrow P$.

Proof:

	Statement	Explanation
1.	$\sim P \Rightarrow Q$	hyp.
2.	$Q \Rightarrow [R \Rightarrow S]$	hyp.
3.	$\sim S$	hyp.
4.	R	dischargeable hyp.
5.	$\sim P$	dischargeable hyp.
6.	Q	MP For 1, For 5
7.	$R \Rightarrow S$	MP For 2, For 6
8.	S	MP For 7, For 4
9.	$S \wedge \sim S$	CI, For 8, For 3
10.	P	II, discharge For 5, (5)–(9) now unusable
11.	$R \Rightarrow P$	DT, discharge For 4, (4)–(10) now unusable

10. Show that $P \Rightarrow T$, $Q \Rightarrow T$, $R \Leftrightarrow [P \vee Q]$, $R \vdash T$.

Proof:

	Statement	Explanation
1.	$P \Rightarrow T$	hyp.
2.	$Q \Rightarrow T$	hyp.
3.	$R \Leftrightarrow [P \vee Q]$	hyp.
4.	R	hyp.
5.	$P \vee Q$	MPB For 3, For 4
6.	$(P \vee Q) \Rightarrow T$	IC, For 1, For 2
7.	T	MP For 6, For 5.

11. Show that $S \Rightarrow P$, $Q \Rightarrow R$, $S \vdash [P \Rightarrow Q] \Rightarrow R$.

Proof:

	Statement	Explanation
1.	$S \Rightarrow P$	hyp.
2.	$Q \Rightarrow R$	hyp.
3.	S	hyp.
4.	$P \Rightarrow Q$	dischargeable hyp.
5.	$P \Rightarrow R$	SI For 4, For 2
6.	$S \Rightarrow R$	SI For 1, For 5
7.	R	MP For 6, For 3
8.	$[P \Rightarrow Q] \Rightarrow R$	DT, discharge For 4, (4)–(7) now unusable

12. Show that $R \Rightarrow T$, $\sim T \Leftrightarrow S$, $[R \wedge \sim S] \Rightarrow \sim Q \vdash R \Rightarrow \sim Q$.

Proof:

	Statement	Explanation
1.	$R \Rightarrow T$	hyp.
2.	$\sim T \Leftrightarrow S$	hyp.
3.	$[R \wedge \sim S] \Rightarrow \sim Q$	hyp.
4.	R	dischargeable hyp.
5.	T	MP For 1, For 4
6.	$S \Leftrightarrow \sim T$	CPB, For 2
7.	$\sim S$	MTB For 6, For 5
8.	$R \wedge \sim S$	CI, For 4, For 7
9.	$\sim Q$	MP For 3, For 8
10.	$R \Rightarrow \sim Q$	DT, discharge For 4, (4)–(9) now unusable.

13. Show that $\sim P \Rightarrow Q$, $[R \Rightarrow Q] \Rightarrow S$, $\sim S \vee T$, $R \Rightarrow \sim P \vdash T \vee V$.

Proof:

	Statement	Explanation
1.	$\sim P \Rightarrow Q$	hyp.
2.	$[R \Rightarrow Q] \Rightarrow S$	hyp.
3.	$\sim S \vee T$	hyp.
4.	$R \Rightarrow \sim P$	hyp.
5.	$\sim (T \vee V)$	dischargeable hyp.
6.	$\sim (T \vee V) \Leftrightarrow (\sim T \wedge \sim V)$	taut.
7.	$\sim T \wedge \sim V$	MPB For 6, For 5
8.	$\sim T$	LCS, For 7
9.	$(\sim S \vee T) \Leftrightarrow (S \Rightarrow T)$	taut.
10.	$S \Rightarrow T$	MPB For 9, For 3
11.	$\sim S$	MT For 10, For 8
12	$R \Rightarrow Q$	SI, For 4, For 1
13.	S	MP For 2, For 12
14.	$S \wedge \sim S$	CI For 13, For 11
15.	$T \vee V$	II, discharge For 5, (5)–(14) now unusable.

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

Proof:

	Statement	Explanation
1.	$[R \wedge \sim Q] \Rightarrow P$	hyp.
2.	$[T \Rightarrow S] \Leftrightarrow [R \Rightarrow Q]$	hyp.
3.	R	hyp.
4.	$\sim P \vee [T \Rightarrow S]$	dischargeable hyp.
5.	$\sim Q$	dischargeable hyp.
6.	$R \wedge \sim Q$	CI For 3, For 5
7.	P	MP For 1, For 6
8.	$\big(\sim P \vee [T \Rightarrow S]\big) \Leftrightarrow (P \Rightarrow [T \Rightarrow S])$	taut.
9.	$P \Rightarrow [T \Rightarrow S]$	MPB For 8, For 4
10.	$T \Rightarrow S$	MP For 9, For 7
11.	$R \Rightarrow Q$	MPB, For 2, For 10
12.	Q	MP For 11, For 3
13.	$Q \wedge \sim Q$	CI For 12, For 5
14.	Q	II, discharge For 5, (5)–(13) now unusable
15.	$[\sim P \vee [T \Rightarrow S]] \Rightarrow Q$	DT, discharge For 4, (4)–(14) now unusable.

15. Use the Euclidean Algorithm to find integers a and b such that $37a + 100b = 1$. Use this information to solve $37x + 42 = 15$ in $\mathbb{Z}_{100}$.

Solution:

The additive inverse of $42 \in \mathbb{Z}_{100}$ is 58. Thus if $37x + 42 = 15$, then $(37x + 42) + 58 = 15 + 58$, that is $37x = 73$ in $\mathbb{Z}_{100}$. We know that $\gcd(100, 37) = 1$ (since 37 is prime), so 37 has a multiplicative inverse 37^{-1} in $\mathbb{Z}_{100}$. Multiply both sides of the equation by 37^{-1} to get $x = 37^{-1} \cdot 73$.

It remains to find the explicit value of 37^{-1}, as we can then use this to find x. We use the Euclidean algorithm:

$$\begin{aligned}
100 &= 2 \cdot 37 + 26\\
37 &= 1 \cdot 26 + 11\\
26 &= 2 \cdot 11 + 4\\
11 &= 2 \cdot 4 + 3\\
4 &= 1 \cdot 3 + 1
\end{aligned}$$

Now turn these equations around:

$$\begin{aligned}
1 &= 4 - 1 \cdot 3\\
&= 4 - 1(11 - 2 \cdot 4)\\
&= 3 \cdot 4 - 1 \cdot 11\\
&= 3(26 - 2 \cdot 11) - 1 \cdot 11\\
&= 3 \cdot 26 - 7 \cdot 11\\
&= 3 \cdot 26 - 7(37 - 26)\\
&= 10 \cdot 26 - 7 \cdot 37\\
&= 10(100 - 2 \cdot 37) - 7 \cdot 37\\
&= 10(100) - 27 \cdot 37.
\end{aligned}$$

So we have $1 \equiv (-27) \cdot 37 \pmod{100}$. Since $-27 \equiv 73 \pmod{100}$ we get that $37^{-1} = 73$ in $\mathbb{Z}_{100}$.

Finally, we have $x = 37^{-1} \cdot 73 = 73 \cdot 73 = 29$ (since $73 \cdot 73 = 5329$ in $\mathbb{Z}$).

16. For what primes p is the element $p - 1$ a perfect square in $\mathbb{Z}_p$? Investigate this question by working out the cases $p = 2$, $p = 3$, $p = 5$, $p = 7$, $p = 11$, $p = 13$, $p = 17$, and $p = 19$. See if you notice any patterns, and try to make a conjecture.

17. Find 2^{1000} in $\mathbb{Z}_7$. Then find 3^{1000} in $\mathbb{Z}_7$. Explain how you got your answers.

    Solution:

    We have $2^3 = 8 \equiv 1 \pmod 7$. Thus $2^{999} = (2^3)^{333} \equiv 1^{333} = 1 \pmod 7$, and

    $$2^{1000} = 2 \cdot 2^{999} \equiv 2 \cdot 1 = 2 \pmod 7.$$

    Similarly, $3^3 = 27 \equiv -1 \pmod 7$ (since $27 - (-1) = 27 + 1 = 28$ is divisible by 7).

    Thus $3^{999} = (3^3)^{333} \equiv (-1)^{333} = -1 \pmod 7$, and

    $$3^{1000} = 3 \cdot 3^{999} \equiv 3 \cdot (-1) = -3 \equiv 4 \pmod 7.$$

    Answer: $2^{1000} = 2$ and $3^{1000} = 4$ as elements of $\mathbb{Z}_7$.

18. Consider a sum of three consecutive squares (like $7^2 + 8^2 + 9^2$). What do you get when you reduce this mod 3 (that is, when you compute the remainder when divided by 3)? Pick another sum of three consecutive squares and try it again. Try it one more time. State a conjecture, and see if you can prove it.

19. The following proof has a mistake. Find what is wrong, and explain.

    $(R \vee \sim S) \Rightarrow \sim P,\ Q \Rightarrow R,\ S \Rightarrow T \vdash (P \Rightarrow \sim R) \wedge (Q \Rightarrow T).$

	Statement	Explanation
1.	$(R\vee \sim S) \Rightarrow \sim P$	hyp.
2.	$Q \Rightarrow R$	hyp.
3.	P	dis. hyp.
4.	$\sim (R\vee \sim S)$	MT, For 1, For 3
5.	$\sim (R\vee \sim S) \Leftrightarrow (\sim R \wedge S)$	taut.
6.	$\sim R \wedge S$	MPB, For 5, For 4
7.	S	RCS, For 6
8.	$\sim R$	LCS, For 6
9.	$P \Rightarrow \sim R$	DT, discharge For 3
10.	Q	dis. hyp.
11.	$S \Rightarrow T$	hyp.
12.	T	MP, For 11, For 7
13.	$Q \Rightarrow T$	DT, discharge For 10
14	$(P \Rightarrow \sim R) \wedge (Q \Rightarrow T)$	CI, For 9, For 13.

The mistake is in step 12. At this point in the proof Formula (7) is unusable, because it was part of the Deduction Theorem routine from (3)–(8). These steps became unusable after we discharged hypothesis (3) in step 9.

20. Show that $(R\vee \sim S) \Rightarrow \sim P$, $Q \Rightarrow R$, $S \Rightarrow T \vdash (P \Rightarrow S) \wedge (Q \Rightarrow (\sim P \wedge R))$.

Proof:

	Statement	Explanation
1.	$(R\vee \sim S) \Rightarrow \sim P$	hyp.
2.	$Q \Rightarrow R$	hyp.
3.	$S \Rightarrow T$	hyp.
4.	P	dis. hyp.
5.	$\sim (R\vee \sim S)$	MT, For 1, For 4
6.	$\sim (R\vee \sim S) \Leftrightarrow (\sim R \wedge S)$	taut.
7.	$\sim R \wedge S$	MPB, For 6, For 5
8.	S	RCS, For 7
9.	$P \Rightarrow S$	DT, discharge For 4, (4)–(8) now unusable
10.	Q	dis. hyp.
11.	R	MP, For 2, For 10
12.	$R \Rightarrow (R\vee \sim S)$	taut.
13.	$R \Rightarrow \sim P$	SI, For 12, For 1
14	$\sim P$	MP, For 13, For 11
15.	$\sim P \wedge R$	CI, For 14, For 11
16.	$Q \Rightarrow (\sim P \wedge R)$	DT, discharge For 10, (10)–(15) now unusable
17.	$(P \Rightarrow S) \wedge (Q \Rightarrow (\sim P \wedge R))$	CI For 9, For 16