Introduction to Proof: Homework 2

Due on October 16, 2024 at 11:59 PM

Victor Ostrik 13:00

Hashem A. Damrah
UO ID: 952102243

Problem 1

In each of the following give a disjunction that is equivalent to the given proposition:

1. $P \Rightarrow Q$.
2. $\neg P \Rightarrow Q$.
3. $P \Rightarrow \neg Q$.

Solution 1

1. $\neg P \vee Q$.
2. $P \vee Q$.
3. $\neg P \vee \neg Q$.

Problem 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.

Solution 2

Let W = "Smith wins the nomination", H = "Smith is happy", G = "Smith is a good campaigner", C = "Smith has the confidence of the party", and R = "Smith should resign from the party".
Translating the given information into symbolic logic:

	Statement	Explanation
1.	$W \Rightarrow H$	Hypothesis
2.	$H \Rightarrow \neg G$	Hypothesis
3.	$\neg W \Rightarrow \neg C$	Hypothesis
4.	$\neg G \Rightarrow R$	Hypothesis
5.	$W \vee \neg W$	Hypothesis
6.	W	Dischargeable Hypothesis
7.	H	MP, for 6, for 1
8.	$\neg G$	MP, for 7, for 2
9.	R	MP, for 8, for 4
10	$W \Rightarrow R$	DT, discharge for 6 [(6) - (9) unusable]

Problem 3

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

	Statement	Explanation
1.	$R \vee [P \wedge Q]$	??
2.	$\neg R$	??
3.	??	Tautology
4.	$\neg R \Rightarrow [P \wedge Q]$	??
5.	$P \wedge Q$	??
6.	??	RCS, ??
7.	??	Hypothesis
8.	$Q \wedge \neg Q$	??
9.	R	??

Solution 3

	Statement	Explanation
1.	$R \vee [P \wedge Q]$	Hypothesis
2.	$\neg R$	Dischargeable Hypothesis
3.	$\neg R \vee R$	Tautology
4.	$\neg R \Rightarrow [P \wedge Q]$	DI, for 2, for 1
5.	$P \wedge Q$	MPD, for 2, for 4
6.	Q	RCS, for 5
7.	$\neg Q$	Hypothesis
8.	$Q \wedge \neg Q$	CI, for 6, for 7
9.	R	II, discharge for 2 [(2) - (8) unusable]

Problem 4

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

	Statement	Explanation
1.	$(P \wedge \neg Q) \Rightarrow (R \Rightarrow Q)$	??
2.	P	Dischargeable Hypothesis
3.	$\neg[Q \vee \neg R]$	Dischargeable Hypothesis
4.	??	Tautology
5.	$\neg Q \wedge R$	??
6.	$\neg Q$	??
7.	$P \wedge \neg Q$	??
8.	$R \Rightarrow Q$	??
9.	$\neg R$	??
10.	R	??
11.	$R \wedge \neg R$	??
12.	$Q \vee \neg R$	??
13.	$P \Rightarrow [Q \vee \neg R$	??

Solution 4

	Statement	Explanation
1.	$(P \wedge \neg Q) \Rightarrow (R \Rightarrow Q)$	Hypothesis
2.	P	Dischargeable Hypothesis
3.	$\neg[Q \vee \neg R]$	Dischargeable Hypothesis
4.	$\neg[Q \vee \neg R] \Leftrightarrow \neg Q \wedge R$	Tautology
5.	$\neg Q \wedge R$	MPB, for 3, for 4
6.	$\neg Q$	LCS, for 5
7.	$P \wedge \neg Q$	CI, for 2, for 6
8.	$R \Rightarrow Q$	MP, for 7, for 1
9.	$\neg R$	MT, for 6, for 8
10.	R	RCS, for 5
11.	$R \wedge \neg R$	CI, for 10, for 9
12.	$Q \vee \neg R$	II, discharge for 3 [(3) - (11) unusable]
13.	$P \Rightarrow [Q \vee \neg R]$	DT, discharge for 2 [(2) - (12) unusable]

Problem 5

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

Solution 5

	Statement	Explanation
1.	$[P \wedge Q] \Rightarrow R$	Hypothesis
2.	$\neg R$	Hypothesis
3.	P	Hypothesis
4.	$\neg [P \wedge Q]$	MT, for 2, for 1
5.	$\neg [P \wedge Q] \Leftrightarrow [\neg P \vee \neg Q]$	Tautology
6.	$\neg P \vee \neg Q$	MPB, for 4, for 5
7.	$\neg Q$	DI, for 3, for 6

Problem 6

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

Solution 6

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

Problem 7

Show that $P \Rightarrow \neg Q, \neg R \Rightarrow Q \vdash P \Rightarrow R$.

Solution 7

	Statement	Explanation
1.	$P \Rightarrow \neg Q$	Hypothesis
2.	$\neg R \Rightarrow Q$	Hypothesis
3.	$\neg Q \Rightarrow R$	Contrapositive, for 2
4.	$P \Rightarrow R$	SI, for 1, for 3

Problem 8

Show that $\neg P \Rightarrow Q$, $T \Rightarrow \neg P$, $\neg[Q \vee R] \vdash \neg T$

Solution 8

	Statement	Explanation
1.	$\neg P \Rightarrow Q$	Hypothesis
2.	$T \Rightarrow \neg P$	Hypothesis
3.	$\neg[Q \vee R]$	Hypothesis
4.	$\neg[Q \vee R] \Leftrightarrow [\neg Q \wedge \neg R]$	Tautology
5.	$\neg Q \wedge \neg R$	MPB, for 3, for 4
6.	$\neg Q$	RCS, for 5
7.	P	MT, for 6, for 1
8.	$\neg T$	MT, for 7, for 2

Problem 9

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

Solution 9

	Statement	Explanation
1.	$\neg P \Rightarrow Q$	Hypothesis
2.	$Q \Rightarrow [R \Rightarrow S]$	Hypothesis
3.	$\neg S$	Hypothesis
4.	$\neg P$	Dischargeable Hypothesis
5.	Q	MP, for 4, for 1
6.	$R \Rightarrow S$	MP, for 5, for 2
7.	$\neg R$	MT, for 3, for 6
8.	$\neg P \Rightarrow \neg R$	DT, discharge for 4 [(4) - (7) unusable]
9.	$R \Rightarrow P$	Contrapositive

Problem 10

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

Solution 10

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

Problem 11

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

Solution 11

	Statement	Explanation
1.	$S \Rightarrow P$	Hypothesis
2.	$Q \Rightarrow R$	Hypothesis
3.	S	Hypothesis
4.	P	MP, for 3, for 1
5.	$P \Rightarrow Q$	Dischargeable Hypothesis
6.	Q	MP, for 4, for 5
7.	R	MP, for 6, for 2
8.	$[P \Rightarrow Q] \Rightarrow R$	DT, discharge for 5 [(5) - (7) unusable]

Problem 12

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

Solution 12

	Statement	Explanation
1.	$R \Rightarrow T$	Hypothesis
2.	$\neg T \Leftrightarrow S$	Hypothesis
3.	$[R \wedge \neg S] \Rightarrow \neg Q$	Hypothesis
4.	R	Dischargeable Hypothesis
5.	T	MP, for 4, for 1
6.	$\neg S$	MT, for 5, for 2
7.	$R \wedge \neg S$	CI, for 4, for 6
8.	$\neg Q$	MP, for 7, for 3
9.	$R \Rightarrow \neg Q$	DT, discharge for 4 [(4) - (8) unusable]

Problem 13

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

Solution 13

	Statement	Explanation
1.	$\neg P \Rightarrow Q$	Hypothesis
2.	$[R \Rightarrow Q] \Rightarrow S$	Hypothesis
3.	$\neg S \vee T$	Hypothesis
4.	$R \Rightarrow \neg P$	Hypothesis
5.	R	Dischargeable Hypothesis
6.	$\neg P$	MP, for 5, for 4
7.	Q	MP, for 6, for 1
8.	$R \Rightarrow Q$	DT, discharge for 5 [(5) - (7) unusable]
9.	S	MP, for 8, for 2
10.	T	DI, for 9, for 3
11.	$T \vee V$	CI, for 10

Problem 14

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

Solution 14

	Statement	Explanation
1.	$[R \wedge \neg Q] \Rightarrow P$	Hypothesis
2.	$[T \Rightarrow S] \Leftrightarrow [R \Rightarrow Q]$	Hypothesis
3.	R	Hypothesis
4.	$\neg P \vee [T \Rightarrow S]$	Dischargeable Hypothesis
5.	$\neg P$	Dischargeable Hypothesis
6.	$R \wedge \neg Q$	Dischargeable Hypothesis
7.	P	MP, for 1, for 6
8.	$P \wedge \neg P$	CI, for 7, for 5
10.	$\neg[R \wedge \neg Q]$	II, discharge for 6 [(6) - (9) unusable]
11.	$\neg[R \wedge \neg Q] \Leftrightarrow [\neg R \vee Q]$	Tautology
12.	$\neg R \vee Q$	MP, for 10, for 11
13.	Q	DI, for 3, for 12
14.	$[\neg P \vee [T \Rightarrow S]] \Rightarrow Q$	DT, discharge for 4 [(4) - (13) unusable]

$\square$

Problem 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 15

1. $100 = 2 \cdot 37 + 26 \Rightarrow 100 - 2 \cdot 37 = 26$,
2. $37 = 1 \cdot 26 + 11 \Rightarrow 37 - 1 \cdot 26 = 11$,
3. $26 = 2 \cdot 11 + 4 \Rightarrow 26 - 2 \cdot 11 = 4$,
4. $11 = 2 \cdot 4 + 3 \Rightarrow 11 - 2 \cdot 4 = 3$,
5. $4 = 1 \cdot 3 + 1 \Rightarrow 4 - 1 \cdot 3 = 1$.

Finally, write the equation for the greatest common divisor $1 = 4 - 1 \cdot 3$. Now, we back-substitute to express 1 as a linear combination of 37 and 100.

1. Substitute $3 = 11 - 2 \cdot 4$: $1 = 4 - 1 \cdot (11 - 2 \cdot 4) = 3 \cdot 4 - 1 \cdot 11$.
2. Substitute $4 = 26 - 2 \cdot 11$: $1 = 3 \cdot (26 - 2 \cdot 11) - 1 \cdot 11 = 3 \cdot 26 - 7 \cdot 11$.
3. Substitute $11 = 37 - 1 \cdot 26$: $1 = 3 \cdot 26 - 7 \cdot (37 - 1 \cdot 26) = 10 \cdot 26 - 7 \cdot 37$.
4. Substitute $26 = 100 - 2 \cdot 37$: $1 = 10 \cdot (100 - 2 \cdot 37) - 7 \cdot 37 = 10 \cdot 100 - 27 \cdot 37$.

So, we find $a = -27, \quad b = 10$. Now we can solve the congruence.
First, subtract 42 from both sides: $37x \equiv -27 \pmod{100}$. Since $-27 \equiv 73 \pmod{100}$, we can rewrite this as $37x \equiv 73 \pmod{100}$. From Step 1, we found that $37 \cdot (-27) \equiv 1 \pmod{100}$, so the inverse of 37 modulo 100 is $-27 \equiv 73 \pmod{100}$. Now multiply both sides of the congruence by 73: $x \equiv 73 \cdot 73 \pmod{100}$ Calculate $73 \cdot 73 \pmod{100}$: $73 \cdot 73 = 5329$. Find $5329 \pmod{100}$: $5329 \pmod{100} = 29$
Thus, $x = 29$ is the solution to $37x + 42 \equiv 15 \pmod{100}$.

Problem 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 an try to make a conjecture.

Solution 16

To see, we'll use the equation $x^2 = p-1 \pmod{p}$. I'll use the Legendre symbol $\left(\frac{a}{p}\right)$ to determine if a is a quadratic residue module p. For $a = p-1$, we have $\left(\frac{p-1}{p}\right)$ will determine if $p-1$ is a quadratic residue of module p.

1. For $p=2$: $p-1 = 2-1 = 1$, which is a perfect square since $1^2 \pmod{2} = 1 \pmod{2}$.
2. For $p=3$: $p-1 = 3-1 = 2$. To see if 2 is a perfect square in $\mathbb{Z}_2$, we need to check all perfect squares

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 0.$$

   Therefore, 2 isn't a perfect square.
3. For $p=5$: $p-1 = 5-1 = 4$, which is clearly a perfect square since $2^2 \pmod{4} = 4 \pmod{2}$.
4. For $p=7$: $p-1 = 7-1 = 6$

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 2, \quad 4^2 = 2, \quad 5^2 = 4, \quad 6^2 = 1.$$

   Therefore, 6 isn't a perfect square.
5. For $p=11$: $p-1 = 11-1 = 10$

$$\begin{aligned}&0^1 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 5, \quad 5^2 = 3, \quad 6^2 = 3, \quad 7^2 = 5, \quad 8^2 = 9\\ &9^2 = 4, \quad 10^2 = 1.\end{aligned}$$

   Therefore, 10 isn't a perfect square.
6. For $p=13$: $p-1 = 13-1 = 12$

$$0^1 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 1, \quad 5^2 = 12.$$

   Therefore, 12 is a perfect square in $\mathbb{Z}_{12}$.
7. For $p=17$: $p-1 = 17-1 = 16$

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16.$$

   Therefore, 16 is a perfect square in $\mathbb{Z}_{17}$.
8. For $p=19$: $p-1 = 19-1 = 18$. I don't want to typeset the entire list, but 18 is not a perfect square in $\mathbb{Z}_{19}$.

   Here's a summary table of everything

Problem 16 continued on next page . . .

p	$p-1$	Quadratic Residue	$p \pmod 4$
2	1	Yes	2
3	2	No	3
5	4	Yes	1
7	6	No	3
11	10	No	3
13	12	Yes	1
17	16	Yes	1
19	18	No	3

From this, I've come to the following conjecture:

Conjecture: *Given a prime number p, $p-1$ is a perfect square in $\mathbb{Z}_p$ if and only if $p \equiv 1 \pmod 4$ (excluding the special case where $p = 2$). This is consistent with the property of the Legendre symbol*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 1 \pmod 3). \end{cases}$$

Problem 17

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

Solution 17

I'll write out all the squares of 2 in $\mathbb{Z}_7$ until we start seeing a pattern or we get $2^n = 1$.

$$2^0 = 0, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1$$

Breaking $2^{1000} = 2^{3 \cdot 333} \cdot 2^1 = 2^{999} \cdot 2 = 2$. I got my answer because I saw that $2^3 = 1$. I used this to my advantage by taking $\left\lfloor \frac{1000}{3} \right\rfloor = 999$, where $\lfloor x \rfloor$ is the biggest whole integer, z such that $z \leq x$. So, $2^{999} = 1$ and using rules of exponentiation, I got $2^{999+1} = 2^{999} \cdot 2^1 = 2$.

Now, the same process pretty much repeats for 3^{1000}

$$3^0 = 0, \quad 3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

Breaking $3^{1000} = 3^{996} \cdot 3^4 = 3^4 = 4$. Again, just like with the previous answer, I found the biggest multiple of 6, x, such that $6x \leq 1000$. That number was 166, giving us $166 \cdot 6 = 996$. And we know that any number that's divisible by 6, then $3^{6x} = 1$. Therefore, $3^{1000} = 3^{996} \cdot 3^4 = 3^4 = 4$.

$\square$

Problem 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 you 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.

Solution 18

The sum of $7^2 + 8^2 + 9^2 = 194$. Finding $194 \pmod 3$, we get $194 - 3 \cdot 64 = 2$. The sum of another three consecutive squares $10^2 + 11^2 + 12^2 = 365$. Computing $365 \pmod 3$, we get $365 - 3 \cdot 121 = 2$. Another three consecutive squares $4^2 + 5^2 + 6^2 = 77$, and $77 \pmod 3 \equiv 77 - 3 \cdot 25 = 2$.

Conjecture: *The sum of the squares of three consecutive integers is congruent to* $2 \pmod 3$.

Proof: Let the three consecutive integers be $n - 1$, n, and $n + 1$. Then their squares are $(n - 1)^2$, n^2, and $(n + 1)^2$. We want to evaluate

$$(n - 1)^2 + n^2 + (n + 1)^2 \pmod 3.$$

Expanding each term, we get

$$(n - 1)^2 = n^2 - 2n + 1, \quad n^2 = n^2, \quad (n + 1)^2 = n^2 + 2n + 1.$$

Adding them together we get

$$(n^2 - 2n + 1) + (n^2) + (n^2 + 2n + 1) = 3n^2 + 2.$$

Since we are multiplying n^2 by 3, then $3n^2 \pmod 3 = 0$, leaving a remainder of 2. $\square$

Problem 19

The following proof has a mistake. Find what is wrong, and explain. $(R \lor \neg S) \Rightarrow \neg P$, $Q \Rightarrow R$, $S \Rightarrow T \vdash (P \Rightarrow \neg R) \land (Q \Rightarrow T)$.

	Statement	Explanation
1.	$(R \lor \neg S) \Rightarrow \neg P$	Hypothesis
2.	$Q \Rightarrow R$	Hypothesis
3.	P	Dischargeable Hypothesis
4.	$\neg(R \lor \neg S)$	MT, for 1, for 3
5.	$\neg(R \lor \neg S) \Leftrightarrow (\neg R \land S)$	Tautology
6.	$\neg R \land S$	MPB, for 5, for 4
7.	S	RCS, for 6
8.	$\neg R$	LCS for 6
9.	$P \Rightarrow \neg R$	DT, discharge for 3 [(3) - (8) unusable]
10.	Q	Dischargeable Hypothesis
11.	$S \Rightarrow T$	Hypothesis
12.	T	MP, for 11, for 7
13.	$Q \Rightarrow T$	DT, discharge for 10 [(10) - (12) unusable]
14.	$(P \Rightarrow \neg R) \land (Q \Rightarrow T)$	CI, for 9, for 13

Solution 19

The mistake is on line 12. The proof incorrectly uses the fact that S is true from line 7. This is not valid though, because the deduction ending on line 8 was based on assuming that P is true, which is not a given and was only a temporary assumption for a direct proof (DT). According to the rules of DT, once the assumption is discharged, all intermediate steps derived from that assumption (lines 3 to 8) become invalid outside the scope of the assumption.

Problem 20

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

Solution 20

	Statement	Explanation
1.	$(R \vee \neg S) \Rightarrow \neg P$	Hypothesis
2.	$Q \Rightarrow R$	Hypothesis
3.	$S \Rightarrow T$	Hypothesis
4.	P	Dischargeable Hypothesis
5.	$\neg(R \vee \neg S)$	MT, for 4, for 1
6.	$\neg(R \vee \neg S) \Leftrightarrow (\neg R \wedge S)$	Tautology
7.	$\neg R \wedge S$	MPB, for 5, for 6
8.	S	RCS, for 7
9.	$P \Rightarrow S$	DT, discharge for 4 [(4) - (8) unusable]
10.	Q	Dischargeable Hypothesis
11.	R	MP, for 10, for 2
12.	$\neg P$	MP, for 11, for 1
13.	$\neg P \wedge R$	CI, for 12, for 11
14.	$Q \Rightarrow (R \wedge \neg P)$	DT, discharge for 10 [(10) - (13) unusable]
15.	$(P = S) \wedge (Q \Rightarrow (\neg P \wedge R))$	CI, for 9, for 14