Section 04: Solutions

1. Divisibility

(a) Circle the statements below that are true. Recall for $a, b \in \mathbb{Z}$: $a \mid b$ if and only if $\exists k \in \mathbb{Z}$ such that $b = ka$.

(i) $1 \mid 3$

(ii) $3 \mid 1$

(iii) $2 \mid 2018$

(iv) $-2 \mid 12$

(v) $1 \cdot 2 \cdot 3 \cdot 4 \mid 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

Solution:

(i) True

(ii) False

(iii) True

(iv) True

(v) True

(b) Circle the statements below that are true. Recall for $a, b, m \in \mathbb{Z}$ and $m > 0$: $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$.

(i) $-3 \equiv 3 \pmod{3}$

(ii) $0 \equiv 9000 \pmod{9}$

(iii) $44 \equiv 13 \pmod{7}$

(iv) $-58 \equiv 707 \pmod{5}$

(v) $58 \equiv 707 \pmod{5}$

Solution:

(i) True

(ii) True

(iii) False

(iv) True

(v) False

2. Just The Setup

For each of these statements,

- Translate the sentence into predicate logic.
- Write the first few sentences and last few sentences of the English proof.

(a) The product of an even integer and an odd integer is even.

Solution:

$\forall x \forall y([\texttt{Even}(x) \wedge \texttt{Odd}(y)] \rightarrow \texttt{Even}(xy))$

Let x be an arbitrary even integer and let y be an arbitrary odd integer.
...
So xy is even.
Since x, y were arbitrary, we have that the product of an even integer with an odd integer is always even.

(b) There is an integer x s.t. $x^2 > 10$ and $3x$ is even.

Solution:

$\exists x[\texttt{GreaterThan10}(x^2) \wedge \texttt{Even}(3x)]$

Consider $x = 6$.
...
So $6^2 > 10$ and $3 \cdot 6$ is even.
Hence, 6 is the desired x.

(c) For every integer n, there is a prime number p greater than n.

Solution:

$\forall x \exists y[\texttt{Prime}(y) \wedge \texttt{GreaterThan}(y, x)]$

Let x be an arbitrary integer.
Consider $y = p$ (*this p is a specific prime*).
...
So p is prime and $p > x$.
Since x was arbitrary, we have that every integer has a prime number that is greater than it.

3. Modular Arithmetic

(a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers greater than 0, then $a = b$ or $a = -b$. **Solution:**

Suppose that $a \mid b$ and $b \mid a$, where a, b are arbitrary integers greater than 0. By the definition of divides, we have $a \neq 0$, $b \neq 0$ and $b = ka, a = jb$ for some integers k, j. Substituting this equation, we see that $a = j(ka)$.

Then, dividing both sides by a, we get $1 = jk$. So, $\frac{1}{j} = k$. Note that j and k are integers, which is only possible if $j, k \in \{1, -1\}$. Since a and b were arbitrary, it follows that $b = -a$ or $b = a$,

(b) Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.

Solution:

Let n and m be arbitrary integers.
Suppose $n \mid m$ with $n, m > 1$, and $a \equiv b \pmod{m}$. By definition of divides, we have $m = kn$ for some

$k \in \mathbb{Z}$. By definition of congruence, we have $m \mid a - b$, which means that $a - b = mj$ for some $j \in \mathbb{Z}$. Combining the two equations, we see that $a - b = (knj) = n(kj)$. By definition of congruence, we have $a \equiv b \pmod{n}$, as required. Since n and m were arbitrary, the claim holds.

4. Become a Mod God

Prove from definitions that for integers a, b, c, d and positive integer m, if $a \equiv b$ (mod m) and $c \equiv d$ (mod m), then $a - c \equiv b - d$ (mod m).

Solution:

Let a, b, c, d be arbitrary integers, and let m be an arbitrary positive integer. Suppose that $a \equiv b$ (mod m) and $c \equiv d$ (mod m). Then by the definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$.

By the definition of divides, there exist integers k and j such that $a - b = km$ and $c - d = jm$. Subtracting the second equation from the first, we have:

$$\begin{aligned}(a - b) - (c - d) &= km - jm \\ a - b - c + d &= (k - j)m \\ (a - c) - (b - d) &= (k - j)m\end{aligned}$$

Then by the definition of divides, $m \mid (a-c)-(b-d)$. Then by the definition of congruence, $a-c \equiv b-d(modm)$, as desired.
Since a,b,c,d, and m were arbitrary the claim holds.

5. Fair and Square

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$. **Solution:**

Let n be an arbitrary integer. We will argue by cases.

Case 1: n is even. Then $n = 2k$ for some integer k. Then $n^2 = (2k)^2 = 4k^2$. Since k is an integer, k^2 is an integer. So n^2 is 4 times an integer. Then by definition of divides, $4 \mid n^2 - 0$. Then by definition of congruence, $n^2 \equiv 0 \pmod{4}$. Since $n^2 \equiv 0 \pmod{4}$, it follows that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Case 2: n is odd. Then $n = 2k+1$ for some integer k. Then $n^2 = (2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1$. So $n^2 - 1 = 4(k^2 + k)$. Since k is an integer, $k^2 + k$ is an integer. So $n^2 - 1$ is 4 times an integer. Then by definition of divides, $4 \mid n^2 - 1$. Then by definition of congruence, $n^2 \equiv 1 \pmod{4}$. Since $n^2 \equiv 1 \pmod{4}$, it follows that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Thus in all cases, $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$. Since n was arbitrary, the claim holds.

6. Even Numbers, Odd Results!

For any integer j, if $3j + 1$ is even, then j is odd

(a) Write the predicate logic of this claim

Odd(x) := x is $2k + 1$, for some integer k
Even(x) := x is $2k$, for some integer k
Solution:

$\forall$j (Even($3j+1$) $\rightarrow$Odd(j))

(b) Write the contrapositive of this claim
Solution:

For any integer j, if j is even, 3k+1 is odd
$\forall j$ (Even(j) $\rightarrow$Odd($3j+1$))

(c) Determine which claim is easier to prove, then prove it! **Solution:**

we will prove the contrapositive of this claim
Let j be an arbitrary even integer.
By the definition of even $j = 2k$ for some integer k
Then by Algebra, $3j + 1 = 3(2k) + 1 = 2(3k) + 1$
Since k is an integer, under closure of multiplication, $3k$ is an integer
Therefore 2(3k) + 1 takes the form of an odd integer so $3j + 1$ must be odd Since j was arbitrary and we have shown the contrapositive, the claim holds

7. The Trifecta

Consider the following proposition: For each integer a, if 3 divides a^2, then 3 divides a

(a) Write the contrapositive of this proposition as a sentence:
Solution:

If 3 does not divide a then 3 does not divide a^2

(b) Prove the proposition by proving its contrapositive.
Hint: Consider using cases based on the Division Algorithm using the remainder for "division by 3." There will be two cases! **Solution:**

we will prove the contrapositive of this claim
Let a be an arbitrary integer such that 3 does not divide a.
If a is not divisible by 3, it can have a remainder of either 1 or 2

Case 1: a $\equiv$1 (mod 3)
a can be expressed as an integer with remainder 1 as: a = 3k + 1, $a = 3k + 1, k \in \mathbb{Z}$
Similarly, we define a^2 as $a \cdot a = (3k+1) \cdot (3k+1) = 9k^2+6k+1 = 3(3k^2+2k)+1$ where $3k^2+2k$ is an integer under closure of addition and multiplication such that we produce an integer that is not divisible by 3.

Case 2: a $\equiv$2 (mod 3)
a can be expressed as an integer with remainder 2 as: a = 3k + 2, $a = 3k + 2, k \in \mathbb{Z}$
Similarly, we define a^2 as $a \cdot a = (3k+2) \cdot (3k+2) = 9k^2+12k+4 = 9k^2+12k+3+1 = 3(3k^2+4k+1)+1$ where $3k^2 + 4k + 1$ is an integer under closure of addition and multiplication such that we produce an integer that is not divisible by 3.

In either case for integer a, we see that 3 does not divide a^2 and results in a remainder of 1.
Since a was arbitrary, and we have demonstrated the contrapositive, the claim holds

8. Predicate Logic Formal Proof

Given $\forall x.\, T(x) \to M(x)$, we wish to prove $(\exists x.\, T(x)) \to (\exists y.\, M(y))$. The following formal proof does this, but it is missing citations for which rules are used, and which lines they are based on. Fill in the blanks with inference rules or predicate logic equivalences, as well as the line numbers.

Then, summarize in English what is going on here.

1. $\forall x.\, T(x) \to M(x)$ (_____)
   - 2.1. $\exists x.\, T(x)$ (_____)

   Let r be the object that satisfies $T(r)$
   - 2.2. $T(r)$ (_____, from _____)
   - 2.3. $T(r) \to M(r)$ (_____, from _____)
   - 2.4. $M(r)$ (_____, from _____)
   - 2.5. $\exists y.\, M(y)$ (_____, from _____)
2. $(\exists x.\, T(x)) \to (\exists y.\, M(y))$ (_____, from _____)

Solution:

1. $\forall x.\, T(x) \to M(x)$ (Given)
   - 2.1. $\exists x.\, T(x)$ (Assumption)

   Let r be the object that satisfies $T(r)$
   - 2.2. $T(r)$ ($\exists$ elimination, from 2.1)
   - 2.3. $T(r) \to M(r)$ ($\forall$ elimination, from 1)
   - 2.4. $M(r)$ (Modus Ponens, from 2.2 and 2.3)
   - 2.5. $\exists y.\, M(y)$ ($\exists$ introduction, from 2.4)
2. $(\exists x.\, T(x)) \to (\exists y.\, M(y))$ (Direct Proof Rule, from 2.1-2.5)

Following the premise of the implication, we suppose there is an object that satisfies $T(\cdot)$. Then it must satisfy $M(\cdot)$ also, by the given, which gives us the conclusion of the implication.

9. Formal Proof (Direct Proof Rule)

Show that $\neg t \to s$ follows from $t \vee q$, $q \to r$ and $r \to s$. **Solution:**

1.	$t \vee q$		[Given]
2.	$q \to r$		[Given]
3.	$r \to s$		[Given]
	4.1.	$\neg t$	[Assumption]
	4.2.	q	[Elim of $\vee$: 1, 4.1]
	4.3.	r	[MP of 4.2, 2]
	4.4.	s	[MP 4.3, 3]
4.	$\neg t \to s$		[Direct Proof Rule]

10. Formal Spoofs

For each of the following proofs, determine why the proof is incorrect. Then, consider whether the conclusion of the proof is true or not. If it is true, state how the proof could be fixed. If it is false, give a counterexample.

(a) Show that $\exists z\ \forall x\ P(x, z)$ follows from $\forall x\ \exists y\ P(x, y)$.

1.	$\forall x\ \exists y\ P(x, y)$	[Given]
2.	$\forall x\ P(x, c)$	[$\exists$ Elim: 1, c special]
3.	$\exists z\ \forall x P(x, z)$	[$\exists$ Intro: 2]

Solution:

The mistake is on line 2 where an inference rule is used on a subexpression. When we apply something like the $\exists$ Elim rule, the $\exists$ must be at the start of the expression and outside all other parts of the statement.

The conclusion is false, it's basically saying we can interchange the order of $\forall$ and $\exists$ quantifiers. Let the domain of discourse be integers and define $P(x, y)$ to be $x < y$. Then the hypothesis is true: for every integer, there is a larger integer. However, the conclusion is false: there is no integer that is larger than every other integer. Hence, there can be no correct proof that the conclusion follows from the hypothesis.

(b) Show that $\exists z\ (P(z) \wedge Q(z))$ follows from $\forall x\ P(x)$ and $\exists y\ Q(y)$.

1.	$\forall x\ P(x)$	[Given]
2.	$\exists y\ Q(y)$	[Given]
3.	Let z be arbitrary	
4.	$P(z)$	[$\forall$ Elim: 1]
5.	$Q(z)$	[$\exists$ Elim: 2, let z be the object that satisfies $Q(z)$]
6.	$P(z) \wedge Q(z)$	[$\wedge$ Intro: 4, 5]
7.	$\exists z\ P(z) \wedge Q(z)$	[$\exists$ Intro: 6]

Solution:

The mistake is on line 5. The $\exists$ Elim rule must create a new variable rather than applying some property to an existing variable.

The conclusion is true in this case. Instead of declaring z to be arbitrary and then applying $\exists$ Elim to make it specific, we can instead just apply the $\exists$ Elim rule directly to create z. To do this, we would remove lines 3 and 5 and define z by applying $\exists$ Elim to line 2. Note, it's important that we define z before applying line 4.

11. Find the Bug

Each of these inference proofs is incorrect. Identify the line (or lines) which incorrectly apply a law, and explain the error. Then, if the claim is false, give concrete examples of propositions to show it is false. If it is true, write a correct proof.

(a) This proof claims to show that given $a \to (b \vee c)$, we can conclude $a \to c$.

1. $a \to (b \vee c)$ [Given]
   - 2.1. a [Assumption]
   - 2.2. $\neg b$ [Assumption]
   - 2.3. $b \vee c$ [Modus Ponens, from 1 and 2.1]
   - 2.4. c [$\vee$ elimination, from 2.2 and 2.3]
2. $a \to c$ [Direct Proof Rule, from 2.1-2.4]

Solution:

The error here is in lines 2.2 and 2. When beginning a subproof for the direct proof rule, only one assumption may be introduced. If the author of this proof wanted to assume both a and $\neg b$, they should have used the assumption $a \wedge \neg b$, which would make line 3 be $(a \wedge \neg b) \rightarrow c$ instead.

And the claim is false in general. Consider:
a: "I am outside"
b: "I am walking my dog"
c: "I am swimming"
If we assert "If I am outside, I am walking my dog or swimming," we cannot reasonably conclude that "If I am outside, I am swimming" $(a \rightarrow c)$.

(b) This proof claims to show that given $p \rightarrow q$ and r, we can conclude $p \rightarrow (q \vee r)$.

$1. p \rightarrow q$	[Given]
$2. r$	[Given]
$3. p \rightarrow (q \vee r)$	[Intro $\vee$ (1,2)]

Solution:

Bug is in step 3, we're applying the rule to only a subexpression.

The statement is true though. A correct proof introduces p as an assumption, uses MP to get q, introduces $\vee$ to get $q \vee r$, and the direct proof rule to complete the argument.

(c) This proof claims to show that given $p \rightarrow q$ and q that we can conclude p

$1. p \rightarrow q$	[Given]
$2. q$	[Given]
$3. \neg p \vee q$	[Law of Implication (1)]
$4. p$	[Eliminate $\vee$ (2,3)

Solution:

The bug is in step 4. Eliminate $\vee$ from 3 would let us conclude $\neg p$ if we had $\neg q$ or q if we had p. It doesn't tell us anything with knowing q.

Indeed, the claim is false. We could have p: "it is raining"
q: "I have my umbrella"

And be a person who always carries their umbella with them (even on sunny days). The information is not sufficient to conclude p.

12. A Formal Proof in Predicate Logic

Prove $\exists x\ (P(x) \vee R(x))$ from $\forall x\ (P(x) \vee Q(x))$ and $\forall y\ (\neg Q(y) \vee R(y))$. **Solution:**

1.	$\forall x\ (P(x) \lor Q(x))$	[Given]
2.	$\forall y\ (\neg Q(y) \lor R(y))$	[Given]
3.	$P(a) \lor Q(a)$	[Elim $\forall$: 1]
4.	$\neg Q(a) \lor R(a)$	[Elim $\forall$: 2]
5.	$Q(a) \to R(a)$	[Law of Implication: 4]
6.	$\neg\neg P(a) \lor Q(a)$	[Double Negation: 3]
7.	$\neg P(a) \to Q(a)$	[Law of Implication: 5]
	8.1. $\neg P(a)$ [Assumption]	
	8.2. $Q(a)$ [Modus Ponens: 8.1, 7]	
	8.3. $R(a)$ [Modus Ponens: 8.2, 5]	
8.	$\neg P(a) \to R(a)$	[Direct Proof]
9.	$\neg\neg P(a) \lor R(a)$	[Law of Implication: 8]
10.	$P(a) \lor R(a)$	[Double Negation: 9]
11.	$\exists x\ (P(x) \lor R(x))$	[Intro $\exists$: 10]