Section 04: Formal Proofs and Number Theory

1. 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.

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

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

2. 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 _____)

3. Formal Proof (Direct Proof Rule)

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

4. 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]

(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]

5. 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]

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

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

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

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

6. A Formal Proof in Predicate Logic

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

7. 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) $1 \cdot 2 \cdot 3 \cdot 4 \mid 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

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

8. 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 $a = -b$.

(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 $a \equiv b \pmod{n}$.

9. 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).

10. Fair and Square

Prove that for all integers n, $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

11. 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

(b) Write the contrapositive of this claim

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

12. 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:

(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!