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*).
$\ldots$
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:

$$(a-b)-(c-d) = km - jm$$
$$a-b-c+d = (k-j)m$$
$$(a-c)-(b-d) = (k-j)m$$

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:

∀j (Even($3j + 1$) →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) →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 ≡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 ≡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