MAT115A HW1

Tao Wang

September 29, 2024

Exercise 1(a)

Proposition: $0 \mid 10$

True or False? False

Disproof:

$$\begin{aligned}
&0 \mid 10 \\
&\iff (\exists m \in \mathbb{Z})(10 = 0 \cdot m) && \text{(Definition of Divisibility (2.1.1))} \\
&\iff (\exists m \in \mathbb{Z})(10 = 0) && \text{(Proposition 1.0.1)} \\
&\iff \text{False} && \text{(Contradicts Reflexivity of Equality)}
\end{aligned}$$

Since $0 \mid 10 \iff$ False, we know that $0 \mid 10$ must be false. □

Exercise 1 (b)

Proposition: $14 \mid 2024$

True or False? False

Disproof:

$$\begin{aligned}
&14 \mid 2024 \\
&\iff (\exists m \in \mathbb{Z})(2024 = 14 \cdot m) && \text{(Definition of Divisibility (2.1.1))} \\
&\iff (\exists m \in \mathbb{Z})\left(\frac{2024}{14} = m\right) && \text{(Division on both sides of equality)} \\
&\iff \text{False} && \text{(m cannot be an integer and not an integer)}
\end{aligned}$$

Since $14 \mid 2024 \iff$ False, we know $14 \mid 2024$ must be False. □

Exercise 1 (c)

Proposition: $17 \mid 998189$

True or False? True.

Proof:

$$\begin{aligned}
&17 \mid 998189 \\
&\iff (\exists m \in \mathbb{Z})(998189 = 17 \cdot m) && \text{(Definition of Divisibility (2.1.1))} \\
&\iff \text{True} && \text{(Choose } m \text{ to be 58717)}
\end{aligned}$$

Therefore, we've shown that $17 \mid 998189$ is equivalent to true. □

Exercise 2 (a)

Proposition: $(a, b, c, \in \mathbb{Z})\,((a \mid b) \wedge (c \mid d)) \implies a + c \mid b + d$.

True or False? False.

Counter-example: $a = 3, b = 6, c = 1, d = 3$
$3 \mid 6$ and $1 \mid 3$, but $4 \nmid 9$. □

Exercise 2 (b)

Proposition: $(a, b, c, \in \mathbb{Z})\,((a \mid b) \wedge (c \mid d)) \implies ac \mid bd$.

True or False? True.

Proof:

Assume $(a, b, c, \in \mathbb{Z})$, $a \mid b$ and $c \mid d$. Then, for some $m, n \in \mathbb{Z}$, $b = a \cdot m$ and $d = c \cdot n$. If we multiply the two equations, we get,

$$b \cdot d = a \cdot m \cdot c \cdot n$$

Since multiplication is associative, we have,

$$bd = ac(mn)$$

This implies $ac \mid bd$.

□

Exercise 2 (c)

Proposition: $(a, b, c, \in \mathbb{Z})\,((a \nmid b) \wedge (b \nmid c)) \implies a \nmid c$

True or False? False.

Counter-example: $a = 3, b = 5, c = 6$
$3 \nmid 5$ and $5 \nmid 6$, but $3 \mid 6$.

$\square$

Exercise 3

Proposition: $(\forall n)(5 \mid n^5 - n)$

True or False? True

Proof:

We'll prove this proposition through the induction principle. For the base case, assume $n = 0$. We have $5 \mid 0$, which is true because we can choose the other divisor to be zero. Therefore, we can assume that $5 \mid k^5 - k$ as the inductive hypothesis.

We have two inductive cases, n = k + 1 for the positive integers and n = k - 1 for the negative integers, where $k \in \mathbb{Z}$.

For the $n = k + 1$ case, we have

$$5 \mid (k + 1)^5 - (k + 1)$$

If we expand the power, we get

$$5 \mid k^5 + 5k^4 + 10k^3 + 10k^2 + 4k$$

We can add k and subtract k to the polynomial

$$5 \mid k^5 - k + 5k^4 + 10k^3 + 10k^2 + 5k$$

$$= 5 \mid k^5 - k + 5(k^4 + 2k^3 + 2k^2 + k)$$

We see that 5 divides $5(k^4+2k^3+2k^2+k)$ because $(k^4+2k^3+2k^2+k)$ is an integer. Also, $5 \mid k^5 - k$ from the base case.

Therefore, it follows from Proposition 2.1.5 that $5 \mid k^5 - k + 5(k^4 + 2k^3 + 2k^2 + k)$ is true.

For the $n = k - 1$ case, we can follow the same procedure and get

$$5 \mid k^5 - k + 5(k - k^4 + 2k^3 - 2k^2)$$

Proposition 2.1.5 again shows that $5 \mid k^5 - k + 5(k - k^4 + 2k^3 - 2k^2)$ is true.

As a result, we've shown that $(\forall n)(5 \mid n^5 - n)$ is true in the base case and the two inductive cases that cover the positive and negative integers. Therefore, it is true for all n.

$\square$

Exercise 4 (a)

Proposition: 201

Prime or Not Prime? Not Prime
$201 = 3(67)$.

Exercise 4 (b)

Proposition: 211

Prime or Not Prime? Prime

Exercise 4 (c)

Proposition: 213

Prime or Not Prime? Not Prime
$213 = 3(71)$.

Exercise 4 (d)

Proposition: 221

Prime or Not Prime? Not Prime
$221 = 17(13)$.

Exercise 5

Proposition: if a prime is in the arithmetic progression $3n + 1, n = 1, 2, 3, \ldots$ then it is also in the arithmetic progression $6k + 1, k = 1, 2, 3, \ldots$

Proof:

> Assume a prime, p, is in $3n + 1$, where $n \in \mathbb{Z}^+$. Then, $p = 3n + 1$.
>
> Since p is a prime number, we know that n must not be an odd positive integer. That's because If $(\exists m \in \mathbb{Z}_{\geq 0})(n = 2m + 1)$, then we have $p = 6m + 3 + 1$, which means p is divisible by 2. However, p is a prime that cannot equal 2, so it should not be divisible by 2 by the definition of prime numbers, so there's a contradiction.
>
> Therefore, n must be an even positive integer. If $(\exists k \in \mathbb{Z}^+)(n = 2k)$, then $p = 3(2k)+1 = 6k+1$. We conclude that $(\exists k \in \mathbb{Z}^+)(p = 6k+1)$, so p is in the arithmetic progression, $6k + 1$, for $k = 1, 2, 3, \ldots$

$\square$

Exercise 6(a)

Proposition: If p is a prime, then $2^p - 1$ is a prime.

True or False? False.

Counter-example:$p = 11$.

$p = 11$ is prime, but $2^1 1 - 1 = 2047$, which is not a prime number because $2047 = 89(23)$.

$\square$

Exercise 6(b)

Proposition: If $2^p - 1$ is a prime, then p is a prime.

True or False? True.

Proof:

We will show the proposition is true by showing that its contrapositive is true. Therefore, if p is not a prime, then $2^p - 1$ is not a prime.

We will assume that p is a composite, so $p = a \cdot b$, where $1 < a, b < p$. Now we have $2^p - 1 = 2^{ab} - 1$, where $1 < a, b < p$.

Recall that the sum of a finite geometric series is

$$1 + r^2 + r^3 + \cdots + r^{n-1} = \frac{r^n - 1}{r - 1}, \quad \text{where } r \neq 1$$

If $r = 2^a$ and $n = b$, we have

$$1 + 2^{2a} + 2^{3a} + \cdots + 2^{a(b-1)} = \frac{2^{ab} - 1}{2^a - 1}, \quad \text{where } 2^a \neq 1$$

Multiply $2^a - 1$ to both sides, we get

$$2^{ab} - 1 = (2^a - 1)(1 + 2^{2a} + 2^{3a} + \cdots + 2^{a(b-1)}), \quad \text{where } 2^a \neq 1$$

The divisor, a, is greater than 1, so $2^a \neq 1$. Therefore, we have

$$2^{ab} - 1 = (2^a - 1)(1 + 2^{2a} + 2^{3a} + \cdots + 2^{a(b-1)}), \quad \text{where } 1 < a, b < p$$

We've shown that 2^{ab} consists of two divisors that are greater than 1. Therefore, $2^{ab} - 1$ is not a prime.

This is equivalent showing that if $2^p - 1$ is prime, then p is prime.

$\square$