Math 109 HW 8

Ray Tsai

11/21/2022

1. (a)

 Proposition 1. $\sim$ *is equivalent.*

 Proof. We will show that $\sim$ is reflexive, symmetric, and transitive.
 Reflexive: Let $(a, b) \in \mathbb{R}^2$. We will show that $(a, b) \sim (a, b)$. Since there exists $k = 1 \in \mathbb{R}$ such that $(a, b) = (ka, kb)$, $(a, b) \sim (a, b)$.
 Symmetric: Let $(a, b) \sim (c, d)$. We will show that $(c, d) \sim (a, b)$. Since $(a, b) \sim (c, d)$, we know that there exists $k \in \mathbb{R}$ such that $(a, b) = (kc, kd)$. Since $k \neq 0$, we can let $m = \frac{1}{k} \in \mathbb{R}$. We then get $(ma, mb) = (kmc, kmd) = (c, d)$, which shows that (c, d) (a, b).
 Transitive: Let $(a, b) \sim (c, d)$, $(c, d) \sim (e, f)$. We will show that $(a, b) \sim (e, f)$. Since $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, we have $(a, b) = (kc, kd)$ and $(c, d) = (me, mf)$, $k, m \in \mathbb{R}_{\neq 0}$. We then have $(a, b) = (kc, kd) = (kme, kmf)$. Since $km \in \mathbb{R}_{\neq 0}$, we have $(a, b) \sim (e, f)$.
 Therefore, $\sim$ is reflexive, symmetric, and transitive. $\square$

 (b)

 Proposition 2. $\sim$ *is not equivalent.*

 Proof. Consider the case $(1, 0), (0, 0) \in \mathbb{R}^2$. Since $1^2 + 0^2 = 1 \geq 0^2 + 0^2$, we have $(1, 0) \sim (0, 0)$. However, $(0, 0) \not\sim (1, 0)$ because $0^2 + 0^2 = 1 < 1^2 + 0^2$. Therefore, $\sim$ is not equivalent. $\square$

2.

 Proposition 3. $\approx$ *is an equivalent relation.*

 Proof. We will show that $\approx$ is reflexive, symmetric, and transitive.

 Reflexive: Let $a \in A$. We will show that $a \approx a$. Since $\sim$ is an equivalent relation and $f(a) = f(a)$, we know that $f(a) \sim f(a)$ by the reflexive property. Therefore, since $f(a) \sim f(a)$, we have $a \approx a$.

 Symmetric: Let $a_1 \approx a_2$. We will show that $a_2 \approx a_1$. Since $a_1 \approx a_2$, we know that $f(a_1) \sim f(a_2)$. By the symmetric property of $\sim$, we have $f(a_2) \sim f(a_1)$, which shows that $a_2 \approx a_1$.

Transitive: Let $a_1 \approx a_2$, $a_2 \approx a_3$. We will show that $a_1 \approx a_3$. Since $a_1 \approx a_2$, $a_2 \approx a_3$, we know that $f(a_1) \sim f(a_2)$ and $f(a_2) \sim f(a_3)$. By the transitive property of $\sim$, we have $f(a_1) \sim f(a_3)$, which shows that $a_1 \approx a_3$.

Therefore, $\approx$ is an equivalent relation. □

3. (a)

Proposition 4. *$S/\sim$ has 3 elements.*

Proof. We know that for all $m \in S$, $1 \leq m \leq 15$, $m \in \mathbb{Z}$. Since the 2 is the smallest integer, 1 has 0 prime factors. Since $2 \in S$, we know that $S/\sim$ contains a equivalent class for elements that have 1 prime factor. The second smallest integer is 3. Since $2 \cdot 3 = 6 \in S$, we know that $S/\sim$ contains a equivalent class for elements that have 2 prime factor. The third smallest integer is 5. The smallest integer that has 3 or more prime factors is $2 \cdot 3 \cdot 5 = 30 \notin S$, as it is greater than 15. Since all the integers that have 3 or more prime factors are greater than 15, there does not exist an equivalent class for them. Therefore, $S/\sim$ has 3 elements, namely integers that have $0, 1, 2$ prime factors respectively. □

(b) 6 has 2 prime factors, so the equivalent class containing 6 is $\{6, 10, 12, 14, 15\} \subseteq S$.

4. Let $a, b, c, d, n \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

(a)

Proposition 5. *$a + c \equiv b + d \pmod{n}$.*

Proof. Let $a = nk_1 + b$, $c = nk_2 + d$, $k_1, k_2 \in \mathbb{Z}$. We will show that $a + c \equiv b + d \pmod{n}$. We know that

$$a + c \equiv (nk_1 + b) + (nk_2 + d) \pmod{n} \quad (1)$$

$$\equiv n(k_1 + k_2) + b + d \pmod{n} \quad (2)$$

$$\equiv b + d \pmod{n}. \quad (3)$$

Therefore, $a + c \equiv b + d \pmod{n}$. □

(b)

Proposition 6. *$ac \equiv bd \pmod{n}$.*

Proof. Let $a = nk_1 + b$, $c = nk_2 + d$, $k_1, k_2 \in \mathbb{Z}$. We will show that $ac \equiv bd \pmod{n}$. We know that

$$ac \equiv (nk_1 + b)(nk_2 + d) \pmod{n} \quad (4)$$

$$\equiv n(nk_1k_2 + k_1d + k_2b) + bd \pmod{n} \quad (5)$$

$$\equiv bd \pmod{n}. \quad (6)$$

Therefore, $ac \equiv bd \pmod{n}$. □

(c)

Proposition 7. $a^m \equiv b^m \pmod{n}$ *for all* $m \in \mathbb{Z}_{>0}$.

Proof. We will proceed by induction on m.
Suppose $m = 1$, we have $a \equiv b \pmod{n}$.
Suppose that $a^m \equiv b^m \pmod{n}$ for some m. We will show that $a^{m+1} \equiv b^{m+1} \pmod{n}$. Since $a \equiv b \pmod{n}$ and the induction hypothesis, we know that $a \cdot a^m \equiv b \cdot b^m \pmod{n}$ by Q4.b. Thus, $a^{m+1} \equiv b^{m+1} \pmod{n}$ if $a^m \equiv b^m \pmod{n}$.
Therefore, $a^m \equiv b^m \pmod{n}$ for all $m \in \mathbb{Z}_{>0}$. □

5.

Proposition 8. $13^{145} \equiv 13 \pmod{21}$

Proof.

$$\begin{aligned}
13^{145} &\equiv 13^{12\cdot 12+1} \pmod{21} &(7)\\
&\equiv 13 \cdot (13^{12})^{12} \pmod{21} &(8)\\
&\equiv 13 \cdot (1)^{12} \pmod{21} &(9)\\
&\equiv 13 \pmod{21} &(10)
\end{aligned}$$

□

6.

Proposition 9. $2^{101} \equiv 4 \pmod{7}$.

Proof. Since

$$\begin{aligned}
2^1 &\equiv 2 \pmod{7} &(11)\\
2^2 &\equiv 4 \pmod{7} &(12)\\
2^3 &\equiv 1 \pmod{7}, &(13)
\end{aligned}$$

we know that

$$\begin{aligned}
2^{101} &\equiv 2^{3\cdot 33+2} \pmod{7} &(14)\\
&\equiv 2^2 \cdot (2^3)^{33} \pmod{7} &(15)\\
&\equiv 4 \cdot (1)^{33} \pmod{7} &(16)\\
&\equiv 4 \pmod{7}. &(17)
\end{aligned}$$

□

7.

Proposition 10. *The possible congruence classes are* $[1], [-2]$.

Proof. Let $2x + 3 \equiv -1 \pmod 6$ for some congruence class x. We then have $2x \equiv -4 \equiv 2 \pmod 6$ by Q4.a. By Q4.b, we can cancel the 2 on all sides, which shows that $x \equiv -2 \pmod 6$ or $x \equiv 1 \pmod 6$.

Therefore, the possible congruence classes are $[1], [-2]$. $\square$

8.

Proposition 11. *There does not exist integers* x, y *such that* $x^3 + 7y^2 = 3$.

Proof. We will prove by contradiction. Let x, y be integers. Suppose for the sake of contradiction that $x^3 + 7y^2 = 3$. By taking modulo 7 of the equation, we have $x^3 + 7y^2 \equiv x^3 \equiv 3 \pmod 7$. However, there does not exist x such that $x^3 \equiv 3 \pmod 7$, since

$$
\begin{align}
0^3 &\equiv 0 \pmod 7 \tag{18}\\
(\pm 1)^3 &\equiv \pm 1 \pmod 7 \tag{19}\\
(\pm 2)^3 &\equiv \pm 8 \pmod 7 \tag{20}\\
&\equiv \pm 1 \pmod 7 \tag{21}\\
(\pm 3)^3 &\equiv \pm 27 \pmod 7 \tag{22}\\
&\equiv \pm 1 \pmod 7, \tag{23}
\end{align}
$$

none of which are congruent to 3, which contradicts our assumption.

Therefore, there does not exist integers x such that $x^3 + 7y^2 = 3$. $\square$

9.

Proposition 12. *If* $n \equiv 3 \pmod 4$, *then there does not exist integers* x, y *such that* $x^2 + y^2 = n$.

Proof. We will prove by contradiction. Let $x, y \in \mathbb{Z}$. Suppose for the sake of contradiction that $n \equiv 3 \pmod 4$. By taking modulo 4 of $x^2 + y^2 = n$, we have $x^2 + y^2 \equiv 3 \pmod 4$. Since

$$
\begin{align}
0^2 &\equiv 0 \pmod 4 \tag{24}\\
(\pm 1)^2 &\equiv 1 \pmod 4 \tag{25}\\
2^2 &\equiv 0 \pmod 4, \tag{26}
\end{align}
$$

$x^2 \pmod 4$ and $y^2 \pmod 4$ can only be congruent to 0 or 1.

If $x^2 \equiv 0 \pmod 4$, then $y^2 \pmod 4$ must be congruent to 3, which is impossible.

If $x^2 \equiv 1 \pmod 4$, then $y^2 \pmod 4$ must be congruent to 2, which is also impossible.

This contradicts our assumption and shows that there does not exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = n$. $\square$