Homework 1

Warren Kim

October 19, 2023

Please grade my HW carefully. Thank you.

Question 1

Prove that if $a \equiv b \ (mod\ m)$, then $\gcd(m, a) = \gcd(m, b)$.

Response

Proof. Let $a \equiv b \ (mod\ m)$. Then by definition, $b - a = mq$ **(i)** for some integer q. Let $c = \gcd(m, a)$; i.e. c is the greatest integer that divides both a and m. Then we can rewrite a and m as:

$$a = ca'$$

$$m = cm'$$

Rearranging **(i)**, we get:

$$\begin{aligned} b &= mq + a \\ &= (cm')q + ca' \\ b &= c(m'q + a') \end{aligned}$$

so $c \mid b$; i.e. $\gcd(m, a) \mid b$. But by definition, $\gcd(m, a) \mid m$ as well. So, $\gcd(m, a) \mid \gcd(m, b)$. $\gcd(m, b) \mid \gcd(m, a)$ can be shown replacing a with b and c with d. $\square$

Question 2

Prove that $(a+b)^p \equiv a^p + b^p \ (mod\ p)$ if p is prime.

Response

Proof. Let p be prime, and $a, b, p \in \mathbb{Z}$. Then, we have

$$\begin{aligned}
(a+b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^p b^{p-k} \\
&= \sum_{k=1}^{p-1} \binom{p}{k} a^p b^{p-k} + \binom{p}{0} a^p + \binom{p}{p} b^p \\
&= \sum_{k=1}^{p-1} \binom{p}{k} a^p b^{p-k} + a^p + b^p
\end{aligned}$$

For every $1 \leq k \leq p-1$, we have

$$\frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1)!}{k!(p-k)!}$$

and since p is prime, by definition $k!(p-k)$ does not have p as a factor. So, $p \mid \binom{p}{k}$ for $1 \leq k \leq p-1$; i.e. $p \mid \binom{p}{k} a^p b^{p-k}$. This implies that

$$p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^p b^{p-k}$$

or

$$\sum_{k=1}^{p-1} \binom{p}{k} a^p b^{p-k} \equiv 0 \ (mod\ p)$$

and so we have that $(a+b)^p \equiv a^p + b^p \ (mod\ p)$. $\square$

Question 3

Find all classes $X \in \mathbb{Z}/300\mathbb{Z}$ such that:

(i) $[7] \cdot X = [2]$,

(ii) $[120] \cdot X = [80]$,

(iii) $[9] \cdot X = [48]$.

Response

(i) $\gcd(7, 300) = 1$ and $1 \mid 2$, so there is one solution. Then, we get

$$7x + 300y = 1$$

$$7(43) + 300(-1) = 1$$

where $x = 43, y = -2$. Multiplying both sides by 2, we get

$$7(86) = 300(-2) = 2$$

so $X = [86]$.

(ii) $\gcd(120, 300) = 60$ and $60 \nmid 80$ so there are no solutions.

(iii) $\gcd(9, 300) = 3$ and $3 \mid 48$, so there are three solutions. Then, we get

$$9x + 300y = 3$$

$$9(-33) + 300(1) = 3$$

where $x = -33, y = 1$. Multiplying both sides by 16, we get

$$9(-528) + 300(16) = 48$$

so $X_m = [72] + \frac{300}{3}m = [72] + 100m$. Using this equation, we have

$$X = [72], X = [172], X = [272]$$

Question 4

Find all positive $m \in \mathbb{Z}$ such that $[5] \cdot [17] = [3] \cdot [4]$ in $\mathbb{Z}/m\mathbb{Z}$.

Response

We want to solve for m in

$$[85] \equiv [12] \ (mod\ n)$$

$85 - 12 = 73$ shows that any divisor of 73 will satisfy the congruence. 73 is prime, so its divisors are $1, 73$, giving us $m = 1, 73$.

Question 5

Prove that every nonzero class $[a] \in \mathbb{Z}/13\mathbb{Z}$ is equal to $[2]^i$ for some i.

Response

Proof. There are 12 cases:

$$
\begin{aligned}
2^0 &= 1 \ (mod\ 13) \\
2^1 &= 2 \ (mod\ 13) \\
2^2 &= 4 \ (mod\ 13) \\
2^3 &= 8 \ (mod\ 13) \\
2^4 &= 16 \ (mod\ 13) = 3 \ (mod\ 13) \\
2^5 &= 32 \ (mod\ 13) = 6 \ (mod\ 13) \\
2^6 &= 64 \ (mod\ 13) = 12 \ (mod\ 13) \\
2^7 &= 128 \ (mod\ 13) = 11 \ (mod\ 13) \\
2^8 &= 256 \ (mod\ 13) = 9 \ (mod\ 13) \\
2^9 &= 512 \ (mod\ 13) = 5 \ (mod\ 13) \\
2^{10} &= 1024 \ (mod\ 13) = 10 \ (mod\ 13) \\
2^{11} &= 2048 \ (mod\ 13) = 7 \ (mod\ 13)
\end{aligned}
$$

Since the sequence repeats for $i \geq 12$, we have shown that every every nonzero class $[a]$ is equal to $[2]^i$ for some i. $\square$

Question 6

Find the (multiplicative) inverse of [100] in $\mathbb{Z}/173\mathbb{Z}$.

Response

$\gcd(100, 173) = 1$ and $1 \mid 1$ so there is one solution. Then, we get

$$100x + 173y = 1$$

$$100(-64) + 173(37) = 1$$

where $x = -64, y = 37$. So $X = [109]$.

Question 7

Solve $X^2 = [5]$ in $\mathbb{Z}/11\mathbb{Z}$.

Response

We want to solve $X^2 \equiv [5]$ $(mod\ 11)$. There are 11 possible solutions:

$$
\begin{aligned}
0^2 \ (mod\ 11) &\equiv 0 \\
1^2 \ (mod\ 11) &\equiv 1 \\
2^2 \ (mod\ 11) &\equiv 4 \\
3^2 \ (mod\ 11) &\equiv 9 \\
4^2 \ (mod\ 11) &\equiv 5 \\
5^2 \ (mod\ 11) &\equiv 3 \\
6^2 \ (mod\ 11) &\equiv 3 \\
7^2 \ (mod\ 11) &\equiv 5 \\
8^2 \ (mod\ 11) &\equiv 9 \\
9^2 \ (mod\ 11) &\equiv 7 \\
10^2 \ (mod\ 11) &\equiv 1
\end{aligned}
$$

So the solutions are $X = [4], [7]$.

Question 8

Find all $k \in \mathbb{N}$ such that $[2]^k = [1]$ in $\mathbb{Z}/17\mathbb{Z}$.

Response

We want to solve $[2]^k \equiv [1]\ (mod\ 17)$. The smallest value of k that satisfies the congruence is $k = 8$. Then, we have

$$2^8 \equiv 1\ (mod\ 17)$$

Raising both sides to the power of n, we get

$$(2^8)^n \equiv 1^n\ (mod\ 17)$$

$$2^{8n} \equiv 1\ (mod\ 17)$$

So $k = 8n$ where $n \in \mathbb{N}$ are all the solutions to $[2]^k \equiv [1]\ (mod\ 17)$.

Question 9

Let X be the set of all pairs $(a, b), a, b \in \mathbb{R}$ such that $a^2 + b^2 > 0$. We write $(a, b) \sim (c, d)$ if $ad = bc$. Show that $\sim$ is an equivalence relation and determine all equivalence classes.

Response

To show that $\sim$ is an equivalence relation, we need to show that it is

(i) Reflexive $a \sim a$

(ii) Symmetric $a \sim b \implies b \sim a$

(iii) Transitive $a \sim b, b \sim c \implies a \sim c$

(i) For any $(a, b) \in X$, we have that $ab = ba = ab$ so $\sim$ is reflexive.

(ii) Assume $(a, b) \sim (c, d)$. Then, $ad = bc \iff bc = ad$ or $(c, d) \sim (a, b)$ so $\sim$ is symmetric.

(iii) Assume $(a, b) \sim (c, d), (c, d) \sim (e, f)$. Then, $ad = bc$ and $cf = de$. There are two cases:

(i) a, b, c, d are not zero.

$$\begin{aligned} ad(cf) &= bc(de) \\ a(dc)f &= b(cd)e \\ af &= be \end{aligned}$$

(ii) $cd = 0$. Then either $c = 0$ or $d = 0$ since $c^2 + d^2 > 0$, so

$$(a, b) \sim (0, d) \implies a = 0$$

$$(0, d) \sim (e, f) \implies e = 0$$

or

$$(a, b) \sim (c, 0) \implies b = 0$$

$$(c, 0) \sim (e, f) \implies f = 0$$

so $af = 0 = be$

So $\sim$ is transitive.

Since we've shown *(i), (ii), (iii)* for $\sim$, it is an equivalence relation.

All equivalence classes are $[(a, b)] := \{(c, d) \in X : ad = bc\}$.

Proof.

(i) Take any pair $(a, b) \in X$. Then $(a, b) \in [(a, b)]$. Since this pair was arbitrary, this holds for all $(a, b) \in X$.

(ii) Assume we have two distinct equivalence classes $[(a_1, b_1)], [(a_2, b_2)]$ and assume they are not disjoint. Then, there is some $(x, y) \in X$ such that $(x, y) \in [(a_1, b_1)]$ and $(x, y) \in [(a_2, b_2)]$. Then, we have $(x, y) \sim (a_1, b_1)$ and $(x, y) \sim (a_2, b_2)$. By symmetry we get $(a_1, b_1) \sim (x, y) \sim (a_2, b_2)$ and by transitivity we get $(a_1, b_1) \sim (a_2, b_2)$. So, it must be true that $[(a_1, b_1)] = [(a_2, b_2)]$

□

Question 10

Prove that $a^{2^{n-2}} \equiv 1 \ (mod\ 2^n)$ for every odd integer a and every $n \geq 3$.

Response

Proof. Let a be an odd integer. Then we can write $a = 2k + 1$ for some integer k. We will induct on $n \geq 3$.

(i) $(n = 3)$

$$\begin{aligned} a^{2^{3-2}} &= a^2 \\ &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

and $4k^2 + 4k + 1 \equiv 1 \ (mod\ 8)$ for all $k \in \mathbb{Z}$, which is true.

(ii) $(n = n + 1)$

$$\begin{aligned} a^{2^{(n+1)-2}} &= a^{2^{n-2+1}} \\ &= a^{2^{n-2} \cdot 2} \\ &= \left(a^{2^{n-2}}\right)^2 \\ &= (1 + 2^n m)^2 && \text{by Inductive Hypothesis} \\ &= 1 + 2(2^n)m + 2^{2n}m^2 \\ &= 1 + 2^{n+1}m + 2^{2n}m^2 \end{aligned}$$

Since $n + 1 \leq 2n$ for $n \geq 3$, we have that

$$2^{n+1} \mid 2^{2n}$$

so we get

$$a^{2^{(n+1)-2}} = 1 + 2^{n+1}m$$

or

$$a^{2^{(n+1)-2}} \equiv 1 \ (mod\ 2^{n+1})$$

This completes the induction.

$\square$