survey hw 3

nxr8dq Sankalpa Banjade: Collaborators: Grady Hollar vhe5ak

September 2023

1 HW Due on 9/20

1.1 Exercises List: 6.4.2, 6.4.3, 8.1.5, 8.3.2, 8.3.3, 8.3.4, 8.3.5, 8.3.6(2).

Fix that $a, b, c \in Z$ with a and b being coprime and satisfying $a \mid c$ and $b|c$ Prove that $ab|c$

(1) **6.4.2** Firstly we already have that $a|c$ and $b|c$. So we have $c = ak$ and that $c = bl$ for some $k, l \in \mathbb{Z}$. Also from the given information we have $gcd(a, b) = 1$ since a and b are coprime. We fix $x, y \in \mathbb{Z}$ to satisfy the equation $a * x + b * y = 1$. From there we multiply each side of the equation by c which results in $c * a * x + b * y * c = c$. Now we substitute $c = ak$ and $c = bl$ which results in $bl * a * x + ak * y * b = c$. Then we utilise the distributive property of integers which results in $ab(lx + yk) = c$. Since we have fixed that $l, x, y, k \in \mathbb{Z}$ that means that (lx+yk) is equal to some integer w. Utilising the definition of a divisor we have completed the proof since abw = c with w being an integer means that $ab|c$.

(2) **6.4.3** Let $a = 298$ and $b = 38$. We use the Euclidean algorithim to compute gcd(a, b) and to find $u, v \in \mathbf{Z}$ such that gcd$(a, b) = au + bv$

$$gcd(298, 38)$$
$$298 = 38 \cdot (7) + 24$$
$$38 = 24 \cdot (1) + 14$$
$$24 = 14 \cdot 1 + 10$$
$$14 = 10 \cdot 1 + 4$$
$$10 = 4 \cdot 2 + 2$$
$$4 = 2 \cdot 2$$
$$gcd(298, 38) = 2.$$
$$2 = 298 \cdot u + 38 * v$$

We must iterate backwards through the euclidean algorithim

$$2 = 32 - 6 \cdot 5$$
$$2 = 32 - (38 - 32 \cdot 1) \cdot 5$$
$$2 = (32 - (38 - (298 - 38 \cdot 7) \cdot 1) \cdot 5)$$
$$2 = (298 - 38 \cdot 7) - (38 - (298 - 38 \cdot 7) \cdot 1) \cdot 5)$$
$$2 = 298 \cdot 6 + 38 \cdot (-47)$$

We have found that u = 6 and v = -47.

8.1.5

Proof. Prove that $x^2 \equiv 0$ or $1 \pmod 3$ for all $x \in \mathbf{Z}$.
Let $x \in \mathbf{Z}$ be an integer. By the division algorithim we have that $x = 3q + r$ for some $q.r \in \mathbf{Z}$ with $0 \le r < 3$. Since we have that $r \in \mathbf{Z}$ we have three choices of r, $r = 0$, $r = 1$ and $r = 2$.
Case when $r = 0$

Plug r into the equation : $x = 3q + 0$
Additive property of zero: $x = 3q$
Square both sides $x^2 = (3q)^2$
Which is also: $x^2 = 3(3q^2)$ By the definition of divisor we have $3|x^2$, or equivalently $3|x^2 - 0$. By the definition of congruence, this gives us $x^2 \equiv 0 \pmod 3$

Case when $r = 1$

Plug r into the equation : $x = 3q + 1$
Square both sides $x^2 = 9q^2 + 6q + 1$
Which is also: $x^2 - 1 = 3(3q^2 + 2q)$
By the definition of divisor we have $3|x^2 - 1$, By the definition of congruence, this gives us $x^2 \equiv 1 \pmod 3$

Case when $r = 2$

Plug r into the equation : $x = 3q + 2$
Square both sides $x^2 = 9q^2 + 12q + 4$
When we subtract one from both sides and pull out the factor of 3 on the RHS we get $x^2 - 1 = 3(3q^2 + 4q + 1)$
By the definition of divisor we have $3|x^2 - 1$, By the definition of congruence, this gives us $x^2 \equiv 1 \pmod 3$

So in all cases we have that $x^2 \equiv 0 \pmod 3$ or $x^2 \equiv 1 \pmod 3$

□

(2) Use (1) to prove that $a^2 - 3b^2 = 2$ has no integer solutions.
We proceed by contradiction,
Let $a, b \in \mathbf{Z}$ be integers and suppose that $a^2 - 3b^2 = 2$ has integer solutions.
By(1) we have that

$$a^2 \equiv 0 \pmod 3 \quad \text{or} \quad a^2 \equiv 1 \pmod 3 \quad \text{and } b^2 \equiv 0 \pmod 3 \quad \text{or} \quad b^2 \equiv 1 \pmod 3$$

By theorem 8.1.3, we can multiply both sides of the congruence by 3 giving

$$a^2 \equiv 0 \pmod 3 \quad \text{or} \quad a^2 \equiv 1 \pmod 3 \quad \text{and } 3b^2 \equiv 0 \pmod 3 \quad \text{or} \quad 3b^2 \equiv 3 \pmod 3$$

Thus we have 4 separate cases for this problem
(1) When $a \equiv 0 \pmod 3$ and $3b^2 \equiv 0 \pmod 3$ By theorem 8.1.4 we have

$$\begin{aligned} a^2 - 3b^2 &\equiv 0 - 0 \pmod 3 \\ a^2 - 3b^2 &\equiv 0 \pmod 3 \\ 2 &\equiv 0 \pmod 3 \\ 3 &\mid 2 - 0 \\ 3 &\mid 2 \end{aligned}$$

However since 3 does not divide 2 this case is false giving us a contradiction
(2) When $a \equiv 0 \pmod 3$ and $3b^2 \equiv 3 \pmod 3$ By theorem 8.1.4 we have

$$\begin{aligned} a^2 - 3b^2 &\equiv 0 - 3 \pmod 3 \\ a^2 - 3b^2 &\equiv -3 \pmod 3 \\ 2 &\equiv -3 \pmod 3 \\ 3 &\mid 2 - (-3) \\ 3 &\mid 5 \end{aligned}$$

However since 3 does not divide 5 this case is false giving us a contradiction
(3) When $a^2 \equiv 1 \pmod 3$ and $3b^2 \equiv 0 \pmod 3$.
By theorem 8.1.4

$$\begin{aligned} a^2 - 3b^2 &\equiv 1 - 0 \pmod 3 \\ 2 &\equiv 1 \pmod 3 \\ 3 &\mid 2 - 1 \\ 3 &\mid 1 \end{aligned}$$

However since 3 does not divide 1 this case is false giving us a contradiction
(4) When $a^2 \equiv 1 \pmod 3$ and $3b^2 \equiv 3 \pmod 3$.
By theorem 8.1.4

$$\begin{aligned} a^2 - 3b^2 &\equiv 1 - 3 \pmod 3 \\ 2 &\equiv -2 \pmod 3 \\ 3 &\mid 2 - (-2) \\ 3 &\mid 4 \end{aligned}$$

However since 3 does not divide 4 this case is false giving us a contradiction
Since we have shown that all four cases we considered lead to contradictions, we must conclude that there are no integer solutions to the equation $a^2 - 3b^2 = 2$ when a and b are integers. Therefore, the original statement has been proven to be true.
8.3.2 Let p be a prime and $0 < k < p$. Prove that $p \mid \binom{p}{k}$

Proof. Let p be a prime and $0 < k < p$. Prove that $p \mid \binom{p}{k}$ So using factorials we have

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

$$\tag{2}$$

Which can also be represented as

$$p! = k!(p-k)!\binom{p}{k} \tag{3}$$

$$\tag{4}$$

It is is evident that $p \mid p!$ since $p! = p \cdot (p-1) \cdot (p-2) \cdot (p-3) .... \cdot 1$. From this we can conclude that $p \mid k!(p-k)!\binom{p}{k}$. From the general version of Euclid's lemma it must be true that either $p \mid k!, p \mid (p-k)!$ or $p \mid \binom{p}{k}$. If we show that the first two cases are impossible it must be the case that $p \mid \binom{p}{k}$.
Case 1: Assume that $p \mid k!$. Then $p \mid k \cdot (k-1) \cdot (k-2) \cdot (k-3) ..... \cdot 1$ Since p is a prime number, we know that the factors of p are only 1 and itself. We can assume from the general version of Euclid's lemma that p must divide one of the terms of k!. However since k < p we know that the statement $p \mid k!$ must be a contradiction as p is bigger than k so there is no factor of k! that would make $p \mid k!$ true.
Case 2: Suppose $p \mid (p-k)!$ we know that any factor of $(p-k)!$ must be less than p, Which gives us the same logic from case 1, since all the factors of $(p-k)!$ is less than p and p is a prime number with factors only being 1 and itself then $p \mid (p-k)!$ is false.
Since both cases reach a contradiction we must assume that $p \mid \binom{p}{k}$ is true.

□

8.3.3 Fix a prime p Prove the following.
(1) (Freshman's dream) Given integers, a,b $\in \mathbf{Z}$ we $(a+b)^p \equiv a^p + b^p \pmod{p}$

Proof. Let a,b $\in \mathbf{Z}$ and p be a prime from the binomial theorem we have that $(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b^1 + ...\binom{p}{p-1}a^1b^{p-1} + \binom{p}{p}b^p$
We then subtract the quantity $(a^p + b^p)$ from both sides leaving us with $(a+b)^p$ - $(a^p + b^p) = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b^1 + ...\binom{p}{p-1}a^1b^{p-1} + \binom{p}{p}b^p$ - $(a^p + b^p)$.
Due to the additive inverse property this equation becomes $(a+b)^p - (a^p + b^p) = \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + ... + \binom{p}{p-2}a^2b^{p-1} + \binom{p}{p-1}a^1b^p$ From excercise 1 we have that $p \mid \binom{p}{k}$ for as long as $0 < k < p$ so by the definition of a divisor we have.
$p \mid \binom{p}{k}a^{p-k}b^k$
$p \mid (\binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + ... + \binom{p}{p-2}a^2b^{p-1} + \binom{p}{p-1}a^1b^{p-1})$
$p|(a+b)^p - (a^p + b^p)$ (Substitution)
So by the definition of congruence we have $(a+b)^p \equiv a^p + b^p \pmod{p}$

□

(2) (Fermat's Little Theorem). For any $n \in \mathbf{N}$ we have $n^p \equiv n \pmod p$

Proof. We assume p to be prime and we proceed by induction n.
Our base case when n = 0, it is obvious that,

$$0 \equiv 0 \pmod p \tag{5}$$
$$0^p \equiv 0 \pmod p \tag{6}$$

Now for some $k \in \mathbf{N} k^p \equiv k \pmod p$We have the following
From our inductive hypothesis we have that $k^p \equiv k \pmod p$
By theorem 8.1.3 we add 1 to both sides to get $k^p + 1 \equiv k + 1$. Since 1 to any power is 1 we can raise it to the power p and the relation still holds true. $k^p + 1^p \equiv k + 1 \pmod p$ we then have from part 1 that $(k+1)^p \equiv k+1 \pmod p$ so by induction we have that $n^p \equiv n \pmod p$ For all $n \in \mathbf{N}$ □

(3) (Fermat's little theorem). For $n \in \mathbb{N}$, $n \equiv 0 \ (\text{mod}\ p)$ or $n^{p-1} \equiv 1 \ (\text{mod}\ p)$.

Proof. Given that n $\in$ **N** and p is a prime Since p is also $\in$ **N** we have two cases which are when n = p and when n $\neq$ p.
Case 1: since n = p it is trivially true that n $\equiv 0 \pmod p$
Case 2: since n $\neq$ p that n and p are coprime.
Utilise Question 2, For any $n \in \mathbf{N}$ we have $n^p \equiv n \pmod p$
We can rewrite the LHS as $n \cdot n^{p-1}$ and the RHS as $n \cdot 1 \pmod p$
We then utilise the cancellation law on a = n to get $n^{p-1} \equiv 1 \pmod p$
Thus For $n \in \mathbb{N}$, $n \equiv 0 \ (\text{mod}\ p)$ or $n^{p-1} \equiv 1 \ (\text{mod}\ p)$. □

Hint You will use the previous exercises and the binomial theorem. For (2) you'll want to induct on n.

8.3.4
Find all solutions to each of the following congruence's
(1) $5x \equiv 2 \ (\text{mod}\ 107)$
$5x \equiv 2 + 428 \pmod{107}$
$5x \equiv 430 \pmod{107}$
Applying cancellation law when a = 5 we have
$ax = a * 86 \pmod{107}$
Then cancel a from both sides $x \equiv 86 \pmod{107}$ so $x = 107k + 86$
(2) $3x \equiv 6 \pmod{12}$
We can rewrite this as $3x - 6 \equiv 12k$
We then add 6 to both sides to get $3x \equiv 12k + 6$
Apply cancellation law when a = 3 to get $x \equiv 4k + 2$
(3) $3x \equiv 1 \ (\text{mod}\ 12)$
This relation has no solutions, to prove this we proceed by contradiction so lets assume that $3x \equiv 1 \ (\text{mod}\ 12)$ has an integer solution x. By the definition

of congruence this equation turns into $3x-1 \equiv 12k$ For some k $\in \mathbf{Z}$ Then when we divide both sides by 3 we get $x-\frac{1}{3}=4k$ which makes our contradiction false as $x-\frac{1}{3}$ is not an integer and the term $4k$ can only be an integer.

8.3.5 Fix $a, b \in \mathbb{Z}$ and $n, m \in \mathbb{Z}_{+}$. Prove that $am \equiv bm \pmod{nm}$ if and only if $a \equiv b \pmod{n}$. **Proof** Suppose a $\equiv b \pmod{n}$ By definition then for some $k \in Z$ the equation $a \equiv b+nk$ is satisfied **Part 1** We multiply both sides by m which results in $am \equiv bm+nkm$. By definition of congruence we have $am \equiv bm \pmod{nm}$. Which must mean that $am-bm=knm$. Pulling out the m we have $m(a-b) \equiv knm$. Utilising the cancellation law we can eliminate the m to get $(a-b) \equiv kn$. Which by definition of congruence is $a \equiv b \pmod{n}$ **Part 2** Now to prove the other side of the if and only if statement, $a \equiv b$ (mod n) if and only if $am \equiv bm \pmod{nm}$. Assuming that $a \equiv b \pmod{n}$ we can rewrite this using Definition 8.1.1, that $a-b=nk$ for some $k \in \mathbf{Z}$. We now multiply and distribute m on both sides to get the equation $ma-mb=mnk$. By definition this means that nm divides $ma-mb$. Which by definition 8.1.1 $am \equiv bm \pmod{nm}$

8.3.6(2) Fix $n \in \mathbb{Z}_{+}$ and $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{n}$. Suppose that a, b are nonnegative. Is $k^{a} \equiv k^{b} \pmod{n}$ for all $k \in \mathbb{Z}$? Prove or disprove. We will disprove this with a counterexample, let $n=3, a=5$, and $b=2$, This satisfies the condition that $a \equiv b \pmod{n}$ as $5=2+3 \cdot 1$ We will consider k $=2$ for our k, since we only have to show for one k that k^{a} does not divide k^{b} (mod n) or by definition 8.1.3 that n does not divide $k^{a}-k^{b}$ for the k we pick.
$k^{5}-k^{2} \equiv 2^{5}-2^{2}$
$k^{5}-k^{2} \equiv 28$
However since 3 does not divide 28 we have that it is not the case that $k^{a} \equiv k^{b}$ (mod n) for all $k \in \mathbb{Z}$