Modern Algebra

Assignment 0

Yousef A. Abood

ID: 900248250

September 2025

---

0 Parliments

Problem 2

d) The divisors of 21 are: $21, 7, 3, 1$. The divisors of 50 are: $50, 25, 10, 5, 2, 1$. So the $gcd(21, 50) = 1$.
The $lcm(21, 50) = 1050$.

Problem 4

Proof. We pick $s, t \in \mathbb{Z}$. For the sake of contradiction, assume s, t are unique. That means we can only find one value for s and one value for t such that they satisfy the equation $1 = 7s + 11t$. We choose $s = -3, t = 2$, so $7 \times -3 + 11 \times 2 = -21 + 22 = 1$, which satisfies the equation. Choose $s = 8, t = -5$, we see that $7 \times 8 + 11 \times -5 = 56 + (-55) = 1$, which satisfies the equation. We see we found two values for s, t each that satisfies the equation. Therefore, s and t are not unique. ■

Problem 7

Proof. We pick $a, b, n \in \mathbb{Z}$. For the forward direction, we assume that $a\ mod\ n = b\ mod\ n$. Since we can write $a = q_1 n + r_1$ and $b = q_2 n + r_2$ by the division algorithm, and $r_1 = r_2$ by our assumption. Then $a - b = q_1 n - q_2 n = n(q_1 - q_2)$ and $n \mid a - b$. For the backward direction, we assume that $n \mid a-b$, so there is a $k \in \mathbb{Z}$ such that $nk = a-b$. Then we use the division algorithm to divide a, b by n. So we get $a = q_1 n + r_1, b = q_2 n + r_2$, where $0 \leq r_1 < n, 0 \leq r_2 < n$. To show that $amodn = bmodn$ we need to show that $r_1 = r_2$. WLOG, we assume $r_1 \geq r_2$. By our assumption, we know that $n \mid a-b$ and

$$a - b = (q_1 n + r_1) - (q_2 n + r_2) = (q_1 n - q_2 n) + (r_1 - r_2) = nk.$$

Since $0 \leq r_1 < n, 0 \leq r_2 < n$. and $r_1 \geq r_2$, then $0 \leq r_1 - r_2 < m$. Now, we have that

$$nk = (q_1 n - q_2 n) + (r_1 - r_2) \iff (r_1 - r_2) = n(q_1 - q_2 - k)$$

, so $m \mid r_1 - r_2$. But we know that $0 \leq r_1 - r_2 < m$. Hence, $r_1 - r_2$ must be zero and $r_1 = r_2$. Therefore, that satisfies the proof. ■

Problem 10

Proof. Let $a, b \in \mathbb{Z}^+$, and $d = gcd(a, b), m = lcm(a, b)$. For the first part, We can apply prime factorization to booth a, b, t to get

$$a = p_1^{f_1} \cdot p_2^{f_2} \cdot p_3^{f_3} \cdots p_n^{f_n}$$
$$b = p_1^{g_1} \cdot p_2^{g_2} \cdot p_3^{g_3} \cdots p_n^{g_n}$$
$$t = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \cdots p_n^{r_n}$$

Where $f, g, r \in \mathbb{Z}$. By theorem 5.4.5. in the discrete math lecture notes by Dr. Daoud Siniora, we can write

$$d = p_1^{min(f_1,g_1)} \cdot p_2^{min(f_2,g_2)} \cdot p_3^{min(f_3,g_3)} \cdots p_n^{min(f_n,g_n)}$$

. Since we know that t divides a, then for every p in the prime factorization of t, the exponents must be less than or equal to the exponents of p in the prime factorization of a. So for all $i = 1, ..., k$, $r_i \leq f_i$. Since we know that t divides b, then for every p in the prime factorization of t, the exponents must be less than or equal to the exponents of p in the prime factorization of b. So for all $i = 1, ..., k$, $r_i \leq g_i$. From the previous steps, for all $r_i <= min(g_i, f_i)$. Hence, t divides d.
For the next part, We can apply prime factorization to booth a, b, s to get

$$a = p_1^{f_1} \cdot p_2^{f_2} \cdot p_3^{f_3} \cdots p_n^{f_n}$$
$$b = p_1^{g_1} \cdot p_2^{g_2} \cdot p_3^{g_3} \cdots p_n^{g_n}$$
$$s = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_n^{e_n}$$

Where $f, g, e \in \mathbb{Z}$. By theorem 5.4.5. in the discrete math lecture notes by Dr. Daoud Siniora, we can write

$$m = p_1^{max(f_1,g_1)} \cdot p_2^{max(f_2,g_2)} \cdot p_3^{max(f_3,g_3)} \cdots p_n^{max(f_n,g_n)}$$

. Since we know that s is a multiple of a, then for every p in the prime factorization of s, the exponents must be greater than or equal to the exponents of p in the prime factorization of a. So for all $i = 1, ..., k$, $e_i \geq f_i$. Since we know that s is a multiple of b, then for every p in the prime factorization of s, the exponents must be greater than or equal to the exponents of p in the prime factorization of b. So for all $i = 1, ..., k$, $e_i \geq g_i$. From the previous steps, for all $e_i \geq max(g_i, f_i)$. Hence, s is a multiple of m. ■

Problem 11

Proof. Let $a, n \in \mathbb{Z}^+$ and $d = gdc(a, n)$. For the forward direction, Assume the equation $ax \ mod \ n = 1$. has a solution. Using the division algorithm, we can write the equation as $ax = qn + 1 \implies ax - qn = 1$. Since d divides a, n, it divides any linear combination of a, n. Then, we see that $d \mid ax - qn, d \mid 1$. Since $d = gcd(a, n)$, then it is a positive integer. We know that the only positive integer that divides 1 is 1. Hence, d must equal 1. For the backward direction, we assume $d = 1$. Since $d = gcd(a, n)$, we can write it as a linear combination of a, n. So $1 = ca + tn$, where $c, t \in \mathbb{Z}$. We observe that $ca + tn = ax - qn$, we can take $x = c, q = -t$. Hence, the equation has a solution. ■

Problem 13

Proof. Let $m, n, r \in \mathbb{Z}$. Suppose m, n are coprimes, so $gcd(m, n) = 1$. Since we know that the $gcd(m, n)$ is a linear combination of m, n, we can write that $1 = cm+tn$, where $c, t \in \mathbb{Z}$. We observe that by multiplying both sides by r, we get that $r = rcm+rtn = (rc)m+(rt)n$. Since, r, t, c are integers, then rt, rc are integers. Let $rt = y, rc = x$, so $r = mx + ny$. Therefore, that satisfies the proof. ■

Problem 20

Proof. Let $p_1, p_2, ..., p_n$ be primes. For the sake of contradiction, Assume that $p_1p_2 \cdots p_n+1$ is divisible by one of these primes .(1) Pick a prime p_i, we know that $p_i \mid p_1p_2 \cdots p_i \cdots p_n$.(2) By (1) and (2), $p_i \mid p_1p_2 \cdots p_n - (p_1p_2 \cdots p_n+1)$. And $(p_1p_2 \cdots p_n) - (p_1p_2 \cdots p_n) - 1 = -1$,. But -1 does not have a prime divisor, so $p_i \nmid p_1p_2 \cdots p_n - (p_1p_2 \cdots p_n + 1)$, which is a contradiction. Therefore, we proved that $p_1p_2 \cdots p_n + 1$ is not divisible by any prime. ■

Problem 28

Proof. We proceed by mathematical induction. Let $P(n) =: 2^n 3^{2n} - 1$ is divisible by 17.
Base case: We show the statement $P(n)$ is true for $P(0)$. When $n = 0$, $2^0 3^0 - 1 = 1 - 1 = 0$, clearly divisible by 17.
Induction step: We need to show that $P(n) \to P(n+1)$ for all $n \geq 1$, where $n \in \mathbb{Z}^+$ Suppose $P(n)$ is true, we need to show that $P(n+1)$ is true as well. We observe that

$$2^{n+1} 3^{2n+2} - 1 = 2 \cdot 9 \cdot (2^n \cdot 3^{2n}) - 1$$

. By our assumption, $2^n 3^{2n} - 1 = 17k \implies 2^n 3^{2n} = 17k + 1$, where $k \in \mathbb{Z}$. We subistitue back in

$$\begin{aligned} 2 \cdot 9 \cdot (2^n \cdot 3^{2n}) - 1 &\overset{IH}{=} 2 \cdot 9 \cdot (17k + 1) - 1 \\ &= 18(17k + 1) - 1 = 18 \cdot 17k + 18 - 1 \\ &= 17 \cdot 18k - 17 = 17(18k - 1). \end{aligned}$$

Hence, we proved that $2^{n+1} 3^{2n+2} - 1$ is divisible by 17 and $P(n+1)$ is true. Therefore, We proved that $2^n 3^{2n} - 1$ is divisible by 17 for all $n \in \mathbb{Z}^+$ ■

Problem 33

Proof. By definition, we can write the mathematical induction with predicate logic as:

$$(P(0) \land \forall n(P(n) \to P(n+1))) \leftrightarrow \forall n P(n)$$

To proof the forward direction, we assume that $(P(0) \land \forall n(P(n) \to P(n+1)))$ is true. We need to show that $\forall n P(n)$ is true. For the sake of the contradiction, suppose that $\forall n P(n)$ is not true. That mean we have some $k \in \mathbb{N}$ such that $P(k)$ does not hold. We construct the set $S = \{n \in \mathbb{N} \mid \neg P(n)\}$, which contains all the elements that does not satisfy $P(n)$. By our assumption, the set S is not empty. By the **The well-ordering principle**, we deduce that S has a least element, which we call t. Since t is the first element that does not satisfy $P(n)$, then $P(t-1)$ holds. Moreover, $t \neq 0$, as t does not have the property P. So, $t \geq 1$ and $t - 1 \geq 0$, such that $t - 1$ is a natural number such that $P(t-1)$ holds. But, by our assumption, we have $P(t-1) \to P(t)$. Since we have that $P(t-1) \to P(t)$ and $P(t-1)$ are true, then $P(t)$ is true, which contradicts that $P(t)$ is false. Therefore, $\forall n P(n)$ is true, where $n \in \mathbb{N}$.
For the backward direction, we assume that $\forall n P(n)$ is true, which implies $P(0)$ is true, and $P(n) \to P(n+1)$ is true. ■

Problem 35

Proof. We proceed by mathematical induction. Let $P(n) =: n^3 + (n+1)^3 + (n+2)^3$ is a multiple of 9. for all $n \in \mathbb{Z}^+$.

Base case: We need to show that $P(1)$ is true. $P(1) = 1 + 8 + 27 = 36$, which is clearly a multiple of 9.

Induction step: We need to show that $P(n) \to P(n+1)$ for all $n \geq 1$. Suppose $P(n)$ is correct, we need to show that $P(n+1)$ is true as well. We observe by $P(n)$, then $n^3 + (n+1)^3 + (n+2)^3 = 9k$, where $k \in \mathbb{Z}$. Then,

$$\begin{aligned}
(n+1)^3 + (n+2)^3 + (n+3)^3 &= (n+1)^3 + (n+2)^3 + n^3 + 9n^2 + 27n + 27 \\
&= n^3 + (n+1)^3 + (n+2)^3 + 9n^2 + 27n + 27 \\
&\overset{IH}{=} 9k + 9n^2 + 27n + 27 \\
&= 9(k + n^2 + 3n + 3).
\end{aligned}$$

Which is a multiple of 9. Therefore, we proved that for all positive integers $n^3 + (n+1)^3 + (n+2)^3$ is a multiple of 9. ■

Problem 57

Problem 58

Problem 59

Problem 63