Problem Set 1 – Solutions
Concepts in Abstract Mathematics
MAT246 LEC0101 Winter 2020

Problem 1

The goal of this exercise is to prove the following theorem in several steps.

Theorem. *Let m and n be natural numbers. Then, there exist unique integers q and r such that $n = qm + r$ and $0 \leq r < m$.*

Recall that q is called the *quotient* and r the *remainder* of the division of n by m.

(a) Let $a, b \in \mathbb{Z}$ with $0 \leq a < b$. Prove that b divides a if and only if $a = 0$.

(b) Use part (a) to prove the uniqueness part of the theorem. That is, show that if there are two pairs $q_1, r_1 \in \mathbb{Z}$ and $q_2, r_2 \in \mathbb{Z}$ satisfying $n = q_1 m + r_1$, $0 \leq r_1 < m$, and $n = q_2 m + r_2$, $0 \leq r_2 < m$, then $q_1 = q_2$ and $r_1 = r_2$.

(c) Prove that there exist such q and r when m divides n.

(d) Prove that there exist such q and r when m does not divide n by applying the well-ordering principle to the set

$$S = \{r \in \mathbb{N} : r = n - qm \text{ for some } q \in \mathbb{Z}\}.$$

Solution

(a) If $a = 0$ then $a = kb$ with $k = 0$, so b divides a. Conversely, suppose that b divides a. Then, $a = bk$ for some $k \in \mathbb{Z}$. Note that $k \geq 0$ since $a \geq 0$ and $b > 0$. But also $bk = a < b$ and $b > 0$ so $k < 1$ and hence $k = 0$. Thus, $a = 0 \cdot b = 0$.

(b) Without loss of generality, we may assume that $r_1 \leq r_2$. We have $n = q_1 m + r_1 = q_2 m + r_2$, so $(q_1 - q_2)m = r_2 - r_1$. In particular, m divides $r_2 - r_1$. Moreover, $0 \leq r_2 - r_1 \leq r_2 < m$, so, by applying (a) with $a = r_2 - r_1$ and $b = m$, we get $r_2 - r_1 = 0$, and hence $r_1 = r_2$. Now, $(q_1 - q_2)m = r_2 - r_1 = 0$, and since $m \neq 0$, this implies that $q_1 - q_2 = 0$, so $q_1 = q_2$.

(c) By definition, $n = km$ for some $k \in \mathbb{Z}$, so we can take $q = k$ and $r = 0$.

(d) Note that $n = n - 0 \cdot m \in S$, so S is not empty. By the Well-Ordering Principle, S has a smallest element r, which is of the form $r = n - qm$ for some $q \in \mathbb{Z}$. Then, $n = qm + r$ and, since $r \in \mathbb{N}$, we have $0 \leq r$, so the only thing left to show is that $r < m$. First note that $r \neq m$ as otherwise $n = mq + m = (q+1)m$, so m divides n. If $r > m$, then $r = m + t$ for some $t > 0$. Then, $t \in \mathbb{N}$ and $t = r - m = n - (q+1)m$, so $t \in S$ and $t < r$, contradicting that r is the smallest element of S. Thus, $r < m$.

Problem 2

Prove that the Principle of Complete Mathematical Induction is equivalent to the Well-Ordering Principle.

That is, first prove the Well-Ordering Principle using the Principle of Complete Mathematical Induction, and then prove the Principle of Complete Mathematical Induction using the Well-Ordering Principle.

Solution

Proof of the Well-Ordering Principle using the Principle of Complete Mathematical Induction. We need to show that every non-empty subset of the set of natural numbers has a smallest element. Equivalently, we show that if $T \subseteq \mathbb{N}$ is a subset of the set of natural numbers with no smallest element, then T is empty.

Let S be the complement of T in $\mathbb{N}$, i.e.

$$S = \{n \in \mathbb{N} : n \notin T\}.$$

We use the Principle of Complete Mathematical Induction to show that $S = \mathbb{N}$ and hence T is empty.

(A) We need to show that $1 \in S$, i.e. that $1 \notin T$. But if $1 \in T$, then 1 would be a smallest element of T since every element $t \in T$ is in $\mathbb{N}$ so $t \geq 1$. Hence, $1 \notin T$, so $1 \in S$.

(B) Suppose that $k \in \mathbb{N}$ is such that $\{1, 2, 3, \ldots, k\} \subseteq S$. We need to show that $k + 1 \in S$. By assumption, all the numbers $1, 2, 3, \ldots, k$ are not in T. Hence, if $k+1 \in T$, then $k+1$ would be a smallest element of T since every element $t \in T$ is a natural number other than $1, 2, 3, \ldots, k$, so $t \geq k+1$. Thus, $k+1 \notin T$ so $k+1 \in S$.

By the Principle of Mathematical Induction, $S = \mathbb{N}$, so T is empty.

Proof of the Principle of Complete Mathematical Induction using the Well-Ordering Principle. Let $S \subseteq \mathbb{N}$ be such that

(A) $1 \in S$

(B) If $k \in \mathbb{N}$ is such that $\{1, 2, 3, \ldots, k\} \subseteq S$ then $k+1 \in S$.

We need to show that $S = \mathbb{N}$. Let T be the complement of S in $\mathbb{N}$, i.e.

$$T = \{n \in \mathbb{N} : n \notin S\}.$$

We need to show that T is empty. By the Well-Ordering Principle, it suffices to show that T has no smallest element. Suppose, by contradiction, that T has a smallest element $t \in T$. By (A) we have $1 \in S$, so $1 \notin T$, and hence $t > 1$. Thus, $t = k+1$ for some $k \in \mathbb{N}$. Moreover, since t is the smallest element of T, all natural numbers smaller than t are not in T and hence they are elements of S, i.e. $\{1, 2, 3, \ldots, k\} \subseteq S$. By (B), this implies that $k+1 \in S$. But $k+1 = t \in T$ so $k+1 \notin S$ and we get a contradiction. Therefore, T has no smallest element, so T is empty by the Well-Ordering Principle, and hence $S = \mathbb{N}$.

Problem 3

Prove that $17^{2n} + 42^n + 93^{2n+1}$ is divisible by 19 for every natural number n.

Solution

We have $17 \equiv -2 \pmod{19}$, $42 \equiv 4 \pmod{19}$, and $93 \equiv -2 \pmod{19}$, so

$$17^{2n} + 42^n + 93^{2n+1} \equiv (-2)^{2n} + 4^n + (-2)^{2n+1} \pmod{19}.$$

But

$$(-2)^{2n} + 4^n + (-2)^{2n+1} = 4^n + 4^n - 2 \cdot 4^n = 0$$

so $17^{2n} + 42^n + 93^{2n+1} \equiv 0 \pmod{19}$ for every $n \in \mathbb{N}$.

Problem 4

Prove that there are no solutions to the equation $x^3 + y^3 = 7777781$ such that both x and y are integers.

Solution

Note that $7777781 = 7 \cdot 1111111 + 4$, so

$$7777781 \equiv 4 \pmod 7$$

Hence, it suffices to show that if $x, y \in \mathbb{Z}$, then $x^3 + y^3 \not\equiv 4 \pmod 7$. We have

$$\begin{aligned} 0^3 &\equiv 0 \pmod 7 \\ 1^3 &\equiv 1 \pmod 7 \\ 2^3 &\equiv 1 \pmod 7 \\ 3^3 &\equiv -1 \pmod 7 \\ 4^3 &\equiv 1 \pmod 7 \\ 5^3 &\equiv -1 \pmod 7 \\ 6^3 &\equiv -1 \pmod 7, \end{aligned}$$

so $x^3 + y^3 \equiv r + s \pmod 7$ for some $r, s \in \{-1, 0, 1\}$. Thus, $x^3 + y^3 \equiv t \pmod 7$, for some $t \in \{-2, -1, 0, 1, 2\}$. Since $-2 \equiv 5 \pmod 7$ and $-1 \equiv 6 \pmod 7$, we showed that $x^3 + y^3 \equiv t \pmod 7$ for some $t \in \{0, 1, 2, 5, 6\}$. In particular, $x^3 + y^3 \not\equiv 4 \pmod 7$, so $x^3 + y^3 \neq 7777781$.

Problem 5

Let m be a natural number greater than 1. Suppose that m has the property that whenever m divides the product ab of two natural numbers a, b, then either m divides a or m divides b. Prove that m is a prime number.

Solution

Equivalently, we need to show that if m is not prime, then there exist natural numbers a, b such that m divides ab but m does not divide a nor b. Since m is not prime, there exists $a, b \in \mathbb{N}$ such that $m = ab$ and $1 < a < m$, $1 < b < m$. Then, m divides ab, but m does not divide a nor b.

Problem 6

Let a and b be natural numbers whose prime factorizations have no primes in common. Use the Fundamental Theorem of Arithmetic to show that if a and b divide a natural number m, then ab divides m.

Solution

By assumption, we can write $a = p_1 \cdots p_u$ and $b = q_1 \cdots q_v$, where p_i, q_i are primes such that $p_i \neq q_j$ for all i, j. Suppose that a and b divide m. Then, $m = ka$ and $m = lb$ for some $k, l \in \mathbb{N}$. Write $m = r_1 \cdots r_w$ for some primes r_i. Then,

$$m = r_1 \cdots r_w = p_1 \cdots p_u k = q_1 \cdots q_v l$$

and, after expanding k and l as products of primes, this gives three prime factorizations of m. By the Fundamental Theorem of Arithmetic, those prime factorizations are the same after reordering. Hence, since $p_i \neq q_j$ for all i, j, we can reorder $r_1, \ldots, r_w$ such that

$$\begin{aligned} r_1 &= p_1, & r_2 &= p_2, & \ldots, && r_u &= p_u, \\ r_{u+1} &= q_1, & r_{u+2} &= q_2, & \ldots, && r_{u+v} &= q_v. \end{aligned}$$

Then, $m = p_1 \cdots p_u \cdot q_1 \cdots q_v \cdot r_{u+v+1} \cdots r_w = ab \cdot r_{u+v+1} \cdots r_w$, so $ab \mid m$.

Problem 7

Find all primes $p \geq 5$ such that $6^p \cdot (p-4)! + 10^{3p}$ is divisible by p.

Hint: Use Fermat's Little Theorem and Wilson's Theorem.

Solution

Let $p \geq 5$ be prime. By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Since

$$(p-1)! = (p-1) \cdot (p-2) \cdot (p-3) \cdot (p-4)!$$

and $p \equiv 0 \pmod{p}$, we get

$$-1 \equiv (-1) \cdot (-2) \cdot (-3) \cdot (p-4)! \pmod{p}$$

so

$$6 \cdot (p-4)! \equiv 1 \pmod{p}.$$

Now, by Fermat's Little Theorem, $6^p \equiv 6 \pmod{p}$ and $10^{3p} = 1000^p \equiv 1000 \pmod{p}$, so

$$\begin{aligned} 6^p \cdot (p-4)! + 10^{3p} &\equiv 6 \cdot (p-4)! + 1000 \pmod{p} \\ &\equiv 1001 \pmod{p}. \end{aligned}$$

Then, $p \mid 6^p \cdot (p-4)! + 10^{3p}$ if and only if $6^p \cdot (p-4)! + 10^{3p} \equiv 0 \pmod{p}$ if and only if $1001 \equiv 0 \pmod{p}$ if and only if $p \mid 1001$. The prime factorization of 1001 is $7 \cdot 11 \cdot 13$, so $p \mid 1001$ if and only if $p \in \{7, 11, 13\}$.

Thus, if $p \geq 5$ is prime, then $6^p \cdot (p-4)! + 10^{3p}$ is divisible by p if and only if $p = 7$, $p = 11$, or $p = 13$.