Note: unrequired parts of multi-part problems are listed obfuscated as ... to recognize they are multi-parted.

1 Arithmetic

1.1 Integers

1.1.5 Fundamental Theorem of Arithmetic

Problem 1.24. *Let $a, m, n \in \mathbb{Z}$ with $(m, n) = 1$. Show $(a, mn) = (a, m)(a, n)$. Hint: Use Theorem 1.8 and recall that m and n have no common divisors.*

Proof. Suppose we have $a, m, n \in \mathbb{Z}$ such that $(m, n) = 1$, (a, m), and (a, n). We can then express using Theorem 1.8 these greatest common divisors in their prime factorizations

$$(a, m) = \prod_{i=0}^{M} p_i^{min\{a_i, m_i\}} \text{ and } (a, n) = \prod_{j=0}^{N} p_j^{min\{a_j, n_j\}}.$$

Since $(m, n) = 1$, we know that their prime factorizations are unique from one another and that they each will contribute separate primes to $m \times n$ yielding

$$(a, mn) = \prod_{i=0}^{M} p_i^{min\{a_i, m_i\}} \times \prod_{j=0}^{N} p_j^{min\{a_j, n_j\}}.$$

This cleanly becomes $(a, mn) = (a, m)(a, n)$ when the prime factorizations are re-expressed in gcd form. □

Problem 1.25. *Let p be a positive prime.*

(a) If $p \mid a^n$ for $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, then $p^n \mid a^n$. Hint: Show $p \mid a$ first.

(b) Show there are no $a, b \in \mathbb{Z}^\times$ satisfying $a^2 = pb^2$. Hint: If you could solve $a^2 = pb^2$, show you may also assume $(a, b) = 1$ by dividing. Then show $p \mid a$ and then that $p \mid b$ to get a contradiction. Alternative Hint: For (b) compare the exponents of p on the LHS and the RHS of the equation $a^2 = pb^2$.

(c) Show there is no $r \in \mathbb{Q}$ satisfying $r^2 = p$; i.e., show $\sqrt{p} \notin \mathbb{Q}$.

The problem will be broken into three separate proofs for each subproblem.

Proof. Suppose $p \mid a^n$ for some $a \in \mathbb{Z}, n \in \mathbb{Z}_{>0}$ given positive prime p. We know that the sequence of a's must contain a factor of p according to our supposition, which is only possible if $p = a$ or $p \mid a$. Because $p = a \Rightarrow p \mid a$, we can say across all valid cases that $p \mid a^n \Rightarrow p \mid a$. From this we can say

$$\begin{aligned} p|a &\Rightarrow pk = a \exists k \in \mathbb{Z} \\ &\Rightarrow (pk)^n = a^n \\ &\Rightarrow p^n k^n = a^n \\ &\Rightarrow p^n l = a^n,\ l = k^n \in \mathbb{Z} \end{aligned}$$

Therefore p^n divides a^n. □

Proof. Suppose, along with the original suppositions above, that $a^2 = pb^2$ for some $a, b \in \mathbb{Z}^\times$. We can then quickly say that $\frac{a^2}{b^2} = p$. Starting with the first requirement of p, we know that $\frac{a^2}{b^2}$ must be an integer yielding three valid possibilities:

(i) $a^2 = b^2$ would always result in the integer one;

(ii) $a^2 > b^2,\ b = 1$ will always result in the integer a^2, and;

(iii) $a^2 > b^2,\ b > 1, (a, b) > 1$, i.e. the fraction will only result in an integer when the numerator and the denominator share a common factor.

All of these possibilities, however, do not result in a positive prime p. The first option is invalid as all primes are greater than 1. The second option is invalid as $\frac{a^2}{b^2} = (a, b)^2$ guarantees the fraction will yield a composite number (the square of their greatest common divisor). Finally, the third option is invalid for the same reason as two, albeit more obviously: a^2 can never be prime. Therefore $a^2 \neq pb^2\ \forall a, b \in \mathbb{Z}^\times$. $\square$

Proof. Suppose $\exists r \in \mathbb{Q}$ such that $r^2 = p \Leftrightarrow \sqrt{p} \in \mathbb{Q}$. Because $r \in \mathbb{Q}$, we can say $\exists a, b \in \mathbb{Z}^\times$ such that $\frac{a}{b} = r \Rightarrow \frac{a^2}{b^2} = r^2 = p$. However, we know from the previous proof that this latter equation can never be true. Therefore $\sqrt{p} \notin \mathbb{Q}$. $\square$

1.2 Modular Arithmetic

1.2.1 Congruence

Problem 1.29. *Which of the following statements are true?*

(a) $6 \stackrel{?}{\equiv} 42 \pmod 2$ *(c)* $7 \stackrel{?}{\equiv} 108 \pmod{10}$ *(e)* $2 \stackrel{?}{\equiv} 54 \pmod 3$

(b) $6 \stackrel{?}{\equiv} 43 \pmod 2$ *(d)* $7 \stackrel{?}{\equiv} 117 \pmod{10}$ *(f)* $2 \stackrel{?}{\equiv} 56 \pmod 3$

Statement (a) is true as $2 \mid (42 - 6) \Rightarrow 2 \mid 36$ thus both are congruent to $[0] \pmod 2$. Statement (b) is false as $[6] \equiv [0] \not\equiv [1] \equiv [43] \pmod 2$. Statement (c) is also false as $[7] \not\equiv [8] \equiv [108] \pmod{10}$. Statement (d) however is true as $10 \mid (117 - 7) \Rightarrow 10 \mid 110$ thus both are congruent to $[7] \pmod{10}$. Statement (e) is false as $[2] \not\equiv [0] \equiv [54] \pmod 3$. Finally, Statement (f) is true as $3 \mid (56 - 2) \Rightarrow 3 \mid 54$ thus both are congruent to $[2] \pmod 3$.

To summarize:

(a) $6 \equiv 42 \pmod 2$ (c) $7 \not\equiv 108 \pmod{10}$ (e) $2 \not\equiv 54 \pmod 3$

(b) $6 \not\equiv 43 \pmod 2$ (d) $7 \equiv 117 \pmod{10}$ (f) $2 \equiv 56 \pmod 3$

Problem 1.32. *Complete the following:*

(a) If $x \equiv 2 \pmod 5$, *what is* $3x^4 + x^3 + 2x - 6$ *congruent to modulo 5?*

(b) If $x \equiv 3 \pmod 6$, *what is* $2x^{47891} + 5x^3 + 2x + 1$ *congruent to modulo 6?*

Please refer to the answers of Problem 43, as they are the same problem phrased differently.

Problem 1.34. *Find an example of the following:*

(a) $ab \equiv 0 \pmod{n}$ *but* $a, b \not\equiv 0$.

(b) $ab \equiv ac \pmod{n}$ *with* $a \not\equiv 0$ *and* $b \not\equiv c$.

(c) $a^2 \equiv b^2 \pmod{n}$ *but* $a \not\equiv \pm b$. *Hint: Look in a nonprime modulus.*

Problem 1.36. *Recall that our decimal system is a base 10 system. For example, this means that 5672 is the decimal representation of* $5 \cdot 10^3 + 6 \cdot 10^2 + 7 \cdot 10^1 + 2 \cdot 10^0$. *The numbers 5, 6, 7, 2 are called the* digits *of the number. In general, let* $n \in \mathbb{Z}_{\geq 0}$ *and write its decimal representation as* $a_N \ldots a_2 a_1 a_0$ *so that* $n = \sum_{k=0}^{N} a_k 10^k$. *Use modular arithmetic to verify the following rules.*

(a) *For* $k \in \mathbb{N}$, *show* $k \mid n \Leftrightarrow n \equiv 0 \pmod{k}$.

(b) *Show* $2 \mid n \Leftrightarrow 2$ *divides the last digit of* n, *i.e., if and only* a_0 *is even.*

(c) *Show* $3 \mid n \Leftrightarrow 3$ *divides the sum of the digits of* n, *i.e., if and only if* $3 \mid \sum_{k=0}^{N} a_k$. *Hint: Notice* $10 \equiv 1 \pmod{3}$.

(d) *If* n *has a decimal representation of* $a_4 a_3 a_2 a_1 a_0$, *show* $7 \mid n \Leftrightarrow 7 \mid (-3a_4 - a_3 + 2a_2 + 3a_1 + a_0)$. *Describe the general pattern.*

1.2.2 Congruence Classes

Problem 1.39. *Complete the following:*

(a) *In* $\mathbb{Z}_5$, *which sets are the same as* $[2]$*:*

(i) $\{12 + 5k \mid k \in \mathbb{Z}\}$

(ii) $\{14 + 5k \mid k \in \mathbb{Z}\}$

(iii) $\{27 - 5k \mid k \in \mathbb{Z}\}$

The first and third sets are congruent to $[2]$ as $5|(12-2) \Rightarrow 5 \mid 10$ and $5|(27-2) \Rightarrow 5 \mid 25$. The second set is not congruent to $[2]$ as $5 \nmid (14-2) \Rightarrow 5 \nmid 12$.

Problem 1.41. *Let* $m, n \in \mathbb{N}$. *Attempt to define a map* $f : \mathbb{Z}_m \mapsto \mathbb{Z}_n$ *by setting* $f([a]_m) = [a]_n$ *for* $[a]_m \in \mathbb{Z}_m$.

1. *Show this supposed function may not be well defined by finding an example in which* $[a]_n \neq [a+m]_n$.

2. *Show* f *is a well defined function if and only if* $n \mid m$. *Hint: Show* f *is well defined if and only if, for each* $k \in \mathbb{Z}$ *(especially* $k = 1$*),* $a + km = a + jn$ *for some* $j \in \mathbb{Z}$.

1.2.3 Arithmetic

Problem 1.42. *Write out the entire addition and multiplication tables for:*

(a) $\mathbb{Z}_4$,

(b) ...

The following are the addition and multiplication tables $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_4, \cdot)$, respectively.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Problem 1.43. *Complete the following:*

(a) If $x = [2] \in \mathbb{Z}_5$*, simplify* $[3]x^4 + x^3 + [2]x - [6]$.

(b) If $x = [3] \in \mathbb{Z}_6$*, simplify* $[2]x^{47,891} + [5]x^3 + [2]x + [1]$.

For subproblem (a), we can calculate the expression as

$$\begin{aligned} [3]x^4 + x^3 + [2]x - [6] &= [3][2]^4 + [2]^3 + [2][2] - [6] \\ &= [3 \cdot 2^4] + [2^3] + [2 \cdot 2] - [6] \\ &= [48 + 8 + 4 - 6] \\ &= \boxed{[58] = [3] \pmod 5}. \end{aligned}$$

The expression from subproblem (b) can be calculated similarly, but it's important to note that $[3]^n = [3]\ \forall n \in \mathbb{Z}_{>0}$. Thus we calculate the expression as

$$\begin{aligned} [2]x^{47,891} + [5]x^3 + [2]x + [1] &= [2][3]^{47,891} + [5][3]^3 + [2][3] + [1] \\ &= [2 \cdot 3] + [5 \cdot 3] + [2 \cdot 3] + [1] \\ &= [6 + 15 + 6 + 1] \\ &= \boxed{[28] = [4] \pmod 6} \end{aligned}$$

Problem 1.44. *Since* $\mathbb{Z}_n$ *has only* n *elements, it is possible to solve an explicit equation simply by substituting in all possible values of* $\mathbb{Z}_n$ *and checking for success. Use this method to find all solutions to the following equations.*

(a) $x^3 + x^2 + x = [0]$ *in* $\mathbb{Z}_4$.

(b) ...

There are only four possible values for x:

- $x = 0$: $[0]^3 + [0]^2 + [0] = [0]$
- $x = 1$: $[1]^3 + [1]^2 + [1] = [3] \not\equiv [0]$
- $x = 2$: $[2]^3 + [2]^2 + [2] = [8 + 4 + 2] = [14] \equiv [2] \not\equiv [0]$
- $x = 3$: $[3]^3 + [3]^2 + [3] = [27 + 9 + 3] = [39] \equiv [3] \not\equiv [0]$

Therefore $[0]^3 + [0]^2 + [0] = [0] \Rightarrow x = [0]$.