MA301 HW#5

Raymond Hu

-[U36258213]-

April 10, 2023

Problem 1

a_5^9

Prove that congruence mod n is an equivalence relation on $\mathbb{Z}$.

Proof. To show that congruence mod n is an equivalence relation on $\mathbb{Z}$, we will show the following properties hold for congruence mod n given any $x, y, z \in \mathbb{Z}$:

(1) reflexive: $x \equiv x \pmod{n}$,

(2) symmetric: $x \equiv y \pmod{n}$ implies $y \equiv x \pmod{n}$,

(3) transitive: $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$ implies $x \equiv z \pmod{n}$.

To show (1), note that $n \mid (x - x)$ holds for any $x \in \mathbb{Z}$ because $0n = x - x = 0$ holds for any x. Thus $x \equiv x \pmod{n}$ for any $x \in \mathbb{Z}$, so congruence mod n is **reflexive**.

To show (2), note that if $x \equiv y \pmod{n}$, then $n \mid (x - y)$. In other words, there exists $c \in \mathbb{Z}$ such that $cn = x - y$. But this implies $-cn = y - x$, meaning $y \equiv x \pmod{n}$. Thus congruence mod n is **symmetric**.

Finally, to show (3), note that $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$ implies $n \mid (x - y)$ and $n \mid (y - z)$. In other words, there exists $c, c' \in \mathbb{Z}$ such that $cn = x - y$ and $c'n = y - z$. Then $cn + c'n = (c + c')n = x - y + y - z = x - z$. Since $(c + c')n = x - z$ implies $x \equiv z \pmod{n}$, we conclude that congruence mod n is **transitive**.

Thus congruence mod n is an equivalence relation on $\mathbb{Z}$. ■

Problem 2

Prove that two integers are in the same congruence class mod n if and only if they have the same remainder when divided by n.

Proof. First, we will prove that if $a, b \in \mathbb{Z}$ are in the same congruence class, they must have the same remainder when divided by n.

If a and b are in the same congruence class, then $a \equiv b \pmod{n}$. In other words, $n \mid (a - b)$, so $cn = a - b$ for some $c \in \mathbb{Z}$.

Now let $r, r' \in \mathbb{Z}$ be the remainders of a and b respectively when divided by n. Then $a = kn + r$ and $b = k'n + r'$ for $k, k' \in \mathbb{Z}$ such that $0 \leq r \leq n - 1$ and $0 \leq r' \leq n - 1$. Returning to $cn = a - b$, this means $cn = kn + r - k'n - r' = (k - k')n + (r - r')$, so $r - r' = (c - k + k')n = jn$ where $j = c - k + k'$ is any integer. We can then infer that $r - r' = jn$ can only hold for $r = r'$:

From the inequalities defining r, we know $0 \leq r \leq n - 1$ and $1 - n \leq -r' \leq 0$, so $1 - n \leq r - r' \leq n - 1$. This means $|r - r'| \leq |n - 1|$. Thus $|r - r'| = |jn| \leq |n - 1|$. This can only hold for $j = 0$, which implies $r - r' = 0$. Thus we must have $r = r'$, so $a \equiv b \mod n$ implies the remainders of a and b are equal when divided by n.

Now assume a and b have the same remainder $r \in \mathbb{Z}$. Then there exists $k, k' \in \mathbb{Z}$ such that $a = kn + r$ and $b = k'n + r$. This implies $a - b = kn + r - k'n - r = (k + k')n$, which means $n \mid (a - b)$. Thus $a \equiv b \mod n$, so a and b are in the same congruence class mod n.

Thus a and b are in the same congruence class mod n if and only if they have the same remainder when divided by n. ■

Problem 3

(a) Let $a \equiv r \pmod{n}$ and $b \equiv s \pmod{n}$. Prove that $ab \equiv rs \pmod{n}$.

Proof. We can show that if $a \equiv r \pmod{n}$ and $b \equiv s \pmod{n}$, then we must have $n \mid (ab - rs)$.

From $a \equiv r \pmod{n}$ and $b \equiv s \pmod{n}$, we know that $n \mid (a - r)$ and $n \mid (b - s)$. Then there exists $c, c' \in \mathbb{Z}$ such that $cn = a - r$ and $c'n = b - s$. Next, we can write $a = cn + r$ and $b = c'n + s$, so $ab = cc'n^2 + csn + c'rn + rs$. Subtracting rs from both sides, we obtain $ab - sr = n(cc'n + cs + c'r)$, so $n \mid (ab - rs)$. Thus $ab \equiv rs \pmod{n}$. ■

(b) Show that if n is not prime, then it is possible that $a \not\equiv 0 \pmod{n}$ and $b \not\equiv 0 \pmod{n}$ but $ab \equiv 0 \pmod{n}$.

Proof. If n is not prime, then there exist smaller $a, b \in \mathbb{N}$ such that $ab = n$. Then $a \not\equiv 0 \pmod{n}$ because $1 < a - 0 < n$, which implies there does not exist $c \in \mathbb{Z}$ such that $cn = a - 0$. By the same logic, $b \not\equiv 0 \pmod{n}$. However, $ab - 0 = 1n$, so $n \mid (ab - 0)$. Thus $ab \equiv 0 \pmod{n}$. ■

Problem 4

The sum of two even integers is even, the sum of an even and an odd integer is odd, and the sum of two odd integers is even. What is the generalization of this statement to congruence classes mod 3?

In $\mathbb{Z}_3$, we have

$$[0] = \{x \in \mathbb{Z} \mid x = 3k\}$$
$$[1] = \{x \in \mathbb{Z} \mid x = 3k + 1\}$$
$$[2] = \{x \in \mathbb{Z} \mid x = 3k + 2\}$$

where $k \in \mathbb{Z}$. Thus

$$\cdots = [-6] = [-3] = [0] = [3] = [6] = \cdots$$
$$\cdots = [-5] = [-2] = [1] = [4] = [7] = \cdots$$
$$\cdots = [-4] = [-1] = [2] = [5] = [8] = \cdots$$

and we have that

$$[0] + [0] = [0]$$
$$[0] + [1] = [1]$$
$$[0] + [2] = [2]$$
$$[1] + [1] = [2]$$
$$[1] + [2] = [3] = [0]$$
$$[2] + [2] = [4] = [1].$$

Thus the sum of

- two numbers from [0] is in [0]
- a number from [1] and a number from [2] is in [0]
- a number from [0] and a number from [1] is in [1]
- two numbers from [2] is in [1]

- a number from [0] and a number from [2] is in [2]
- two numbers from [1] is in [2].

Problem 5

Show that a number's equivalence class mod 3 is the same as the sum of its digits.

Proof. Let $i \in \mathbb{Z}$ be any integer with digits a_j, $0 \leq j \leq k$ where i is a $(k+1)$-digit number. Then $i = \sum_{j=0}^{k} a_j 10^j$. Let $s = \sum_{j=0}^{k} a_j$ be the sum of the digits of i. Then $i - s = \sum_{j=0}^{k} a_j 10^j - \sum_{j=0}^{k} a_j = \sum_{j=0}^{k} (10^j - 1)a_j = 0 + \sum_{j=1}^{k} (10^j - 1)a_j$. From the polynomial property $(x^j - 1) = (x-1)\sum_{n=0}^{j-1} x^n$, we factorize $10^j - 1 = (10-1)\sum_{n=0}^{j-1} 10^n = 9\sum_{n=0}^{j-1} 10^n$. Then

$$i - s = \sum_{j=1}^{k} (10^j - 1)a_j = \sum_{j=1}^{k} 9 \sum_{n=0}^{j-1} 10^n a_j = 9 \sum_{j=1}^{k} \sum_{n=0}^{j-1} 10^n a_j = 3c$$

where $c = 3\sum_{j=1}^{k} \sum_{n=0}^{j-1} 10^n a_j$, so $c \in \mathbb{Z}$. Thus $3 \mid (i - s)$, which means $i \equiv s \pmod 3$. Therefore any number has the same equivalence class as the sum of its digits equivalence mod 3. ■

Problem 6

Prove that there are an infinite number of natural numbers that cannot be written as the sum of three squares.

Proof. We will show that the sum of three perfect squares can never take the form $8k + 7$, $k \in \mathbb{Z}$.

From the property proved in Problem 3a, if $a \equiv r \pmod n$, then $a^2 \equiv r^2 \pmod n$.

In mod 8, any natural number is in some congruence class $[j]$, $0 \leq j \leq 7$. Therefore let $a_j \in \mathbb{N}$ be any number in the congruence class $[j]$. Then $a_j \equiv j \pmod 8$, so $a_j^2 \equiv j^2$

(mod 8). In other words, $[a_j^2] = [j^2]$, which means

$$[a_0^2] = [0]$$

$$[a_1^2] = [1]$$

$$[a_2^2] = [4]$$

$$[a_3^2] = [9] = [1]$$

$$[a_4^2] = [16] = [0]$$

$$[a_5^2] = [25] = [1]$$

$$[a_6^2] = [36] = [4]$$

$$[a_7^2] = [49] = [1]$$

Thus the square of any natural number is either in the congruence class [0], [1], or [4]. This means the sum of three squares $x^2 + y^2 + z^2$, $x, y, z \in \mathbb{N}$, is in some congruence class $[0j_1 + 1j_2 + 4j_3]$ where $j_1, j_2, j_3 \in \mathbb{N}$ such that $j_1 + j_2 + j_3 = 3$. By computing all the possibilities, it can be shown that we never have $0j_1 + 1j_2 + 4j_3 = 7c$ for any $c \in \mathbb{Z}$, so $[x^2 + y^2 + z^2] \neq [7]$ always. Thus we always have $x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$. In other words, $8 \nmid (x^2 + y^2 + z^2 - 7)$, so there does not exist any $k \in \mathbb{Z}$ such that $8k = x^2 + y^2 + z^2 - 7$. Hence $x^2 + y^2 + z^2 \neq 8k + 7$, so the set $\{x \in \mathbb{N} \mid x = 8k + 7\}$ defines an infinite set of natural numbers that cannot be written as the sum of three squares. ■