Math 220 Fall 2021, Lecture 19: Number theory I

1. Number theory I

1.1. Congruence modulo n

1.1.1. Definition

Definition 1.1.1. Let $n, a, b \in \mathbb{Z}$. We say that a is **congruent to** b **modulo** n if and only if $n \mid a - b$. We shall use the notation "$a \equiv b \bmod n$" for "a is congruent to b modulo n".

We also say "$a \not\equiv b \bmod n$" for "a is not congruent to b modulo n".

Example 1.1.2. **(a)** Is $3 \equiv 7 \bmod 2$? This would mean that $2 \mid 3 - 7$, which is true since $3 - 7 = -4 = 2 \cdot (-2)$. So yes, we have $3 \equiv 7 \bmod 2$.

(b) Is $3 \equiv 6 \bmod 2$? This would mean that $2 \mid 3 - 6$, which is false since $3 - 6 = -3$ is not divisible by 2. So we have $3 \not\equiv 6 \bmod 2$.

(c) We have $a \equiv b \bmod 1$ for any $a, b \in \mathbb{Z}$, since $1 \mid a - b$ (in fact, 1 divides every integer).

(d) Two integers a and b satisfy $a \equiv b \bmod 0$ if and only if $a = b$ (since 0 divides only 0 itself).

(e) For any two integers a and b, we have $a + b \equiv a - b \bmod 2$, since $(a + b) - (a - b) = 2b$ is divisible by 2.

The word "modulo" in the phrase "a is congruent to b modulo n" originates with Gauss and means something like "with respect to". You can read "a is congruent to b modulo n" as "a equals b up to a multiple of n". Indeed, the definition can be restated as follows:

$$a \equiv b \bmod n \qquad \text{if and only if} \qquad a = b + nc \text{ for some } c \in \mathbb{Z}.$$

As we will soon see, being congruent modulo 2 means having the same parity: That is, two even numbers are congruent modulo 2, and two odd numbers are congruent modulo 2, but an even number is never congruent to an odd number modulo 2. (We will soon prove this.)

1.1.2. Basic properties

Proposition 1.1.3. Let $n, a \in \mathbb{Z}$. Then, $a \equiv 0 \bmod n$ if and only if $n \mid a$.

Proof. This is an "if and only if" statement. Thus, in order to prove it, we need to prove the two implications

$$(a \equiv 0 \bmod n) \implies (n \mid a)$$

and

$$(n \mid a) \implies (a \equiv 0 \bmod n).$$

However, both are easy:

- If $a \equiv 0 \bmod n$, then $n \mid a - 0$ (by the definition of congruence), so that $n \mid a$ (since $a - 0 = a$).
- If $n \mid a$, then $n \mid a - 0$, so that $a \equiv 0 \bmod n$ (by the definition of congruence).

So we are done. □

We note that the proofs of the above two implications are basically the same (very short) argument, written in two directions. So we can instead write up the above argument as follows:

$$\begin{aligned} (a \equiv 0 \bmod n) &\iff (n \mid a - 0) && \text{(by the definition of congruence)} \\ &\iff (n \mid a) && \text{(since } a - 0 = a\text{)}. \end{aligned}$$

This is called a "chain of equivalences": We have proved that two statements (in this case, "$a \equiv 0 \bmod n$" and "$n \mid a$") are equivalent by connecting them by a chain of statements, such that any two consecutive statements in the chain are equivalent. This works because the logical connective $\iff$ is transitive (i.e., if $P \iff Q$ and $Q \iff R$, then $P \iff R$).

Next come some staple properties of congruences:

Proposition 1.1.4. Let $n \in \mathbb{Z}$.

(a) We have $a \equiv a \bmod n$ for every $a \in \mathbb{Z}$.

(b) If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $b \equiv a \bmod n$.

(c) If $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.

(d) If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy

$$a_1 \equiv b_1 \bmod n \qquad \text{and} \qquad a_2 \equiv b_2 \bmod n,$$

then

$$\begin{aligned} a_1 + a_2 &\equiv b_1 + b_2 \bmod n; \\ a_1 - a_2 &\equiv b_1 - b_2 \bmod n; \\ a_1 a_2 &\equiv b_1 b_2 \bmod n. \end{aligned}$$

(e) Let $m \in \mathbb{Z}$ be such that $m \mid n$. If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $a \equiv b \bmod m$.

Proof. **(a)** For every $a \in \mathbb{Z}$, we have $a \equiv a \bmod n$, since $n \mid a - a$ is true (because $a - a = 0 = n \cdot 0$).

(b) Let $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$. Thus, $n \mid a - b$. However, $a - b \mid b - a$ (since $b - a = (a - b)(-1)$). Combining these two divisibilities, we obtain $n \mid b - a$. In other words, $b \equiv a \bmod n$.

(c) Let $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$ and $b \equiv c \bmod n$. Thus, $n \mid a-b$ and $n \mid b-c$. We must prove that $a \equiv c \bmod n$; in other words, we must prove that $n \mid a-c$. However, $a-c = (a-b)+(b-c)$. From $n \mid a-b$ and $n \mid b-c$, we obtain $n \mid (a-b)+(b-c)$ (because $d \mid x$ and $d \mid y$ entail $d \mid x+y$, as we have shown last time). In other words, $n \mid a-c$ (since $a-c = (a-b)+(b-c)$). So $n \mid a-c$ is proved, and part **(c)** follows.

(d) Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy

$$a_1 \equiv b_1 \bmod n \qquad \text{and} \qquad a_2 \equiv b_2 \bmod n.$$

Thus, $n \mid a_1 - b_1$, so that $a_1 - b_1 = nc_1$ for some integer c_1. Similarly, $a_2 - b_2 = nc_2$ for some integer c_2. Consider these c_1 and c_2.

From $a_1 - b_1 = nc_1$, we obtain $a_1 = b_1 + nc_1$. Similarly, $a_2 = b_2 + nc_2$.

Now, let us prove that $a_1 + a_2 \equiv b_1 + b_2 \bmod n$. Indeed,

$$\left(\underbrace{a_1}_{=b_1+nc_1} + \underbrace{a_2}_{=b_2+nc_2} \right) - (b_1+b_2) = (b_1+nc_1+b_2+nc_2) - (b_1+b_2)$$
$$= nc_1 + nc_2 = n(c_1+c_2)$$

is clearly divisible by n. So $a_1 + a_2 \equiv b_1 + b_2 \bmod n$ is proved.

Next, let us prove that $a_1 - a_2 \equiv b_1 - b_2 \bmod n$. Indeed,

$$\left(\underbrace{a_1}_{=b_1+nc_1} - \underbrace{a_2}_{=b_2+nc_2} \right) - (b_1-b_2) = (b_1+nc_1-b_2-nc_2) - (b_1-b_2)$$
$$= nc_1 - nc_2 = n(c_1-c_2)$$

is clearly divisible by n. So $a_1 - a_2 \equiv b_1 - b_2 \bmod n$ is proved.

Finally, let us prove that $a_1 a_2 \equiv b_1 b_2 \bmod n$. Indeed,

$$\underbrace{a_1}_{=b_1+nc_1}\ \underbrace{a_2}_{=b_2+nc_2} - b_1b_2 = (b_1+nc_1)(b_2+nc_2) - b_1b_2$$
$$= b_1b_2 + nc_1b_2 + b_1nc_2 + nc_1nc_2 - b_1b_2$$
$$= nc_1b_2 + b_1nc_2 + nc_1nc_2$$
$$= n(c_1b_2 + b_1c_2 + nc_1c_2)$$

is clearly divisible by n. So $a_1a_2 \equiv b_1b_2 \bmod n$ is proved. Part **(d)** has been proved.

(e) is left to the reader. □

Proposition 1.1.4 **(d)** is saying that congruences modulo n (for a fixed integer n) can be added, subtracted and multiplied together. This does not mean that you can do anything with them that you can do with equalities. In fact,

- you cannot divide them: $2 \equiv 0 \bmod 2$ and $2 \equiv 2 \bmod 2$ but $2/2 \not\equiv 0/2 \bmod 2$.

- you cannot take them to each other's power: $2 \equiv 2 \bmod 2$ and $2 \equiv 0 \bmod 2$ but $2^2 \not\equiv 2^0 \bmod 2$.

However, we can take a congruence to the k-th power when $k \in \mathbb{N}$:

Exercise 1.1.1. Let $n, a, b \in \mathbb{Z}$ be such that $a \equiv b \bmod n$. Prove that $a^k \equiv b^k \bmod n$ for each $k \in \mathbb{N}$.

Now, let us use the above to prove the rule for divisibility by 9 (stated in the previous lecture):

Proposition 1.1.5. Let m be a positive integer. Let s be the sum of the digits of m written in decimal. (For instance, if $m = 302$, then $s = 3 + 0 + 2 = 5$.) Then, $9 \mid m$ if and only if $9 \mid s$.

Proof. Let m have the decimal representation $m_d m_{d-1} \cdots m_0$ (where m_d is the leading digit). Thus,

$$m = m_d \cdot 10^d + m_{d-1} \cdot 10^{d-1} + \cdots + m_0 \cdot 10^0.$$

However, $10 \equiv 1 \bmod 9$, since $9 \mid 10 - 1$. Hence, by Exercise 1.1.1, we have $10^k \equiv 1^k \bmod 9$ for every $k \in \mathbb{N}$. In other words, $10^k \equiv 1 \bmod 9$ for every $k \in \mathbb{N}$. Hence, we obtain the congruence

$$m_k \cdot 10^k \equiv m_k \bmod 9 \qquad \text{for every } k \in \{0, 1, \ldots, d\}$$

(by multiplying the congruences $m_k \equiv m_k \bmod 9$ and $10^k \equiv 1 \bmod 9$). Now, sum these congruences over all $k \in \{0, 1, \ldots, d\}$. This results in

$$m_d \cdot 10^d + m_{d-1} \cdot 10^{d-1} + \cdots + m_0 \cdot 10^0 \equiv m_d + m_{d-1} + \cdots + m_0 \bmod 9.$$

This rewrites as

$$m \equiv s \bmod 9$$

(since $m_d \cdot 10^d + m_{d-1} \cdot 10^{d-1} + \cdots + m_0 \cdot 10^0 = m$ and $m_d + m_{d-1} + \cdots + m_0 = s$). Hence, $s \equiv m \bmod 9$.

However, if $9 \mid m$, then $m \equiv 0 \bmod 9$, so that $s \equiv 0 \bmod 9$ because $s \equiv m \bmod 9$, and therefore $9 \mid s$. A similar argument can be done in reverse, showing that $9 \mid s$ implies $9 \mid m$. Hence, we conclude that $9 \mid m$ if and only if $9 \mid s$. □

A similar argument works if 9 is replaced by 3. In fact, $s \equiv m \bmod 9$ entails $s \equiv m \bmod 3$ because $3 \mid 9$.

1.1.3. Chains of congruences

Equalities can be chained together: e.g., if $a = b$ and $b = c$ and $c = d$, then $a = d$. You just write $a = b = c = d$ in this case.

The same works for congruences: e.g., if $a \equiv b \bmod n$ and $b \equiv c \bmod n$ and $c \equiv d \bmod n$, then $a \equiv d \bmod n$. You just write

$$a \equiv b \equiv c \equiv d \bmod n$$

in this case. The reason why this works is the following proposition:

Proposition 1.1.6. Let n and $a_1, a_2, \ldots, a_k$ be integers. Assume that $a_i \equiv a_{i+1} \bmod n$ for each $i \in \{1, 2, \ldots, k-1\}$. Then, $a_i \equiv a_j \bmod n$ for all i and j, and in particular $a_1 \equiv a_k \bmod n$.

Proof. Boring induction on k, using Proposition 1.1.4 **(c)**. □

We will write $a_1 \equiv a_2 \equiv \cdots \equiv a_k \bmod n$ in the situation of Proposition 1.1.6. Note that if you chain together multiple congruences, the moduli (i.e., the n's) of these congruences must be equal! For example, you cannot chain together

$$a \equiv b \bmod 2 \qquad \text{and} \qquad b \equiv c \bmod 3.$$