Lecture 14: Congruence relation

Wednesday, August 31, 2022 12:50 PM

Let's recall that we used the well-ordering principle and proved the division algorithm.

<u>Theorem</u> (Division algorithm) For every $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$, there exist $q, r \in \mathbb{Z}$ such that (1) $a = bq + r$, (2) $0 \le r < |b|$. Moreover, such a pair of integers q and r is unique.

(We say q is the quotient and r is the remainder of a divided by b.)

<u>Definition</u>. Suppose n is a non-zero integer. For $a, b \in \mathbb{Z}$, we say a and b are congruent modulo n if $n \mid a-b$. In this case, we write $a \equiv b \pmod{n}$, or $a \overset{n}{\equiv} b$, or simply $a \equiv b$ if n is clear from the context.

The notation was introduced in an influential book by Gauss.

<u>Ex</u>. $5 \overset{2}{\equiv} 1$ as $2 \mid 4 = 5 - 1$.

$80 \overset{3}{\equiv} -1$ as $3 \mid 81 = 80 - (-1)$.

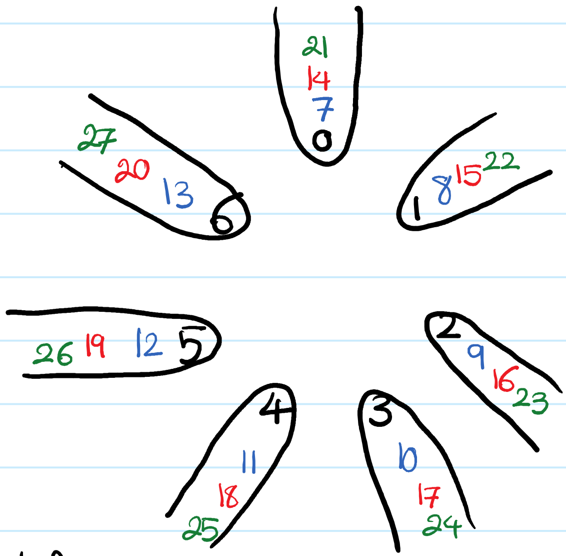
$a \overset{n}{\equiv} a$ as $n \mid 0 = a - a$.

One can visualize the congruence relation by writing integers around

Lecture 14: Congruence relation

Wednesday, November 23, 2016 5:09 PM

a circle of length n. For example for $n=7$, we are partitioning



$\mathbb{Z}$ into 7 subsets. Every subset is an arithmetic progression with increment $n=7$.

We are identifying all the numbers in the same group; similar to identifying 1pm of different days! Given an integer a, we can find out to which group a belongs by dividing a by $n=7$ and finding the remainder. This is the content of our next theorem.

Theorem. Suppose $n\in\mathbb{Z}$ and $n\geq 2$. For $a\in\mathbb{Z}$, let $r_n(a)$ be the remainder of a divided by n. Then the following statements hold.

(1) $a \overset{n}{\equiv} r_n(a)$.

(2) If $a \overset{n}{\equiv} r$ and $0\leq r<n$, then $r=r_n(a)$.

(3) For $a,b\in\mathbb{Z}$, $a\overset{n}{\equiv} b \Leftrightarrow r_n(a)=r_n(b)$.

Proof. (1) Since $r_n(a)$ is the remainder of a divided by n, there

Lecture 14: Congruence relation

Wednesday, November 23, 2016 5:24 PM

exists $q \in \mathbb{Z}$ such that $a = nq + r_n(a)$. Hence $a - r_n(a) = nq$ is an integer multiple of n. Therefore, $a \overset{n}{\equiv} r_n(a)$.

(2) Since $a \overset{n}{\equiv} r$, $n \mid a-r$. Thus, there exists $k \in \mathbb{Z}$, $a - r = nk$. Hence, $a = nk + r$ and $0 \leq r < n$. Therefore the pair of integer k and r satisfies the properties given in the statement of the division algorithm. Hence k is the quotient and r is the remainder of a divided by n. Thus, $r = r_n(a)$.

(3) ($\Rightarrow$) $a \overset{n}{\equiv} b \Rightarrow n \mid a-b \Rightarrow a - b = nk$ for some $k \in \mathbb{Z}$. Let q be the quotient of a divided by n. Hence $a = nq + r_n(a)$. Then

$b = a - nk = nq + r_n(a) - nk = n(q-k) + r_n(a)$, and so

$b - r_n(a) = n\underbrace{(q-k)}_{\text{in } \mathbb{Z}}$, which implies that $b \overset{n}{\equiv} r_n(a)$.

Since $b \overset{n}{\equiv} r_n(a)$ and $0 \leq r_n(a) < n$, by part (2), $r_n(b) = r_n(a)$.

($\Leftarrow$) Let q_1 and q_2 be the quotients of a and b divided by n, resp. Hence $a = q_1 n + r_n(a)$ and $b = q_2 n + r_n(b)$. Since $r_n(a) = r_n(b)$, $a - b = n(q_1 - q_2)$. Therefore, $n \mid a-b$, which implies $a \overset{n}{\equiv} b$. ∎

Lecture 14: Congruence relation

Wednesday, November 23, 2016 5:54 PM

We want to treat the congruence relation as a type of "equality".

For that reason, we check the three properties: reflexive, symmetric, and transitive. A relation is call equivalent if it has these three properties.

Lemma. Suppose $n \in \mathbb{Z}$ and $n \geq 2$. For every $a, b, c \in \mathbb{Z}$,

- (Reflexive) $a \overset{n}{\equiv} a$.
- (Symmetric) $a \overset{n}{\equiv} b \Rightarrow b \overset{n}{\equiv} a$.
- (Transitive) $\left.\begin{array}{l} a \overset{n}{\equiv} b \\ b \overset{n}{\equiv} c \end{array}\right\} \Rightarrow a \overset{n}{\equiv} c$.

Proof. • Since $r_n(a) = r_n(a)$, $a \overset{n}{\equiv} a$.

- $a \overset{n}{\equiv} b \Rightarrow r_n(a) = r_n(b) \Rightarrow r_n(b) = r_n(a) \Rightarrow b \overset{n}{\equiv} a$.
- $\left.\begin{array}{l} a \overset{n}{\equiv} b \Rightarrow r_n(a) = r_n(b) \\ b \overset{n}{\equiv} c \Rightarrow r_n(b) = r_n(c) \end{array}\right\} \Rightarrow r_n(a) = r_n(c) \Rightarrow a \overset{n}{\equiv} c$. ■

The main point of the congruence relation is the fact that it behaves well with the arithmetic operations $+, -,$ and $\cdot$. You have already seen this in your 1st homework assignment.

Lemma. Suppose $n \in \mathbb{Z}$, $n \geq 2$, $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Then

Lecture 14: Congruence arithmetic

Wednesday, November 23, 2016 5:39 PM

$$\left.\begin{array}{l} a_1 \overset{n}{\equiv} a_2 \\ b_1 \overset{n}{\equiv} b_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} a_1 \pm b_1 \overset{n}{\equiv} a_2 \pm b_2 . \\ a_1 b_1 \overset{n}{\equiv} a_2 b_2 . \end{array}\right.$$

Proof. $\left.\begin{array}{l} a_1 \overset{n}{\equiv} a_2 \Rightarrow n \mid a_1 - a_2 \Rightarrow \exists k \in \mathbb{Z},\ a_1 - a_2 = nk \\ b_1 \overset{n}{\equiv} b_2 \Rightarrow n \mid b_1 - b_2 \Rightarrow \exists \ell \in \mathbb{Z},\ b_1 - b_2 = n\ell . \end{array}\right\}$ hypothesis

$$(a_1-b_1)-(a_2-b_2) = (a_1-a_2)-(b_1-b_2) = nk - n\ell = n\underbrace{(k-\ell)}_{\text{in } \mathbb{Z}} \Rightarrow$$

$$n \mid (a_1-b_1)-(a_2-b_2) \Rightarrow a_1 - b_1 \overset{n}{\equiv} a_2 - b_2 .$$

- $a_1 b_1 - a_2 b_2 = a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2 = (a_1-a_2) b_1 + a_2 (b_1 - b_2)$

$$= nkb_1 + a_2 n \ell = n\underbrace{(kb_1 + a_2\ell)}_{\text{in } \mathbb{Z}}$$

$$\Rightarrow n \mid a_1 b_1 - a_2 b_2 \Rightarrow a_1 b_1 \overset{n}{\equiv} a_2 b_2 . \qquad \blacksquare$$

The above result implies that in every algebraic expresion involving integers and operations $+, -,$ and $\cdot$, we can replace every integer with another integer as long as they are congruent modulo n, and the final answers are congruent modulo n. In particular, if $a \overset{n}{\equiv} b$, then $a^m \overset{n}{\equiv} b^m$ for every $m \in \mathbb{Z}^+$.

Lecture 14: Remainder of division by 9

Wednesday, November 23, 2016 6:03 PM

Ex. What is the remainder of 10^n divided by 9 (for $n \in \mathbb{Z}^+$)?

Solution. $10 \overset{9}{\equiv} 1 \Rightarrow$ for every $n \in \mathbb{Z}^+$, $10^n \overset{9}{\equiv} 1^n = 1$

$\Rightarrow$ the remainder of 10^n divided by 9 is 1.

Ex. What is the remainder of 109109140100103 divided by 9?

Solution. $109109140100103 =$

$3 + 10 \times 0 + 10^2 \times 1 + 10^3 \times 0 + 10^4 \times 0 + 10^5 \times 1 + 10^6 \times 0 + 10^7 \times 4 +$

$10^8 \times 1 + 10^9 \times 9 + 10^{10} \times 0 + 10^{11} \times 1 + 10^{12} \times 9 + 10^{13} \times 0 + 10^{14} \times 1$

$\overset{9}{\equiv} 3+0+1+0+0+1+0+4+1+\cancel{9}^{0}+0+1+\cancel{9}^{0}+0+1$

$\boxed{10^n \equiv 1 \pmod 9) \Rightarrow \text{powers of 10 can be replaced with 1}}$

$\boxed{\text{which means we are adding the digits of this number}}$

$\overset{9}{\equiv} 12 \overset{9}{\equiv} 3$. So the remainder of this division is 3. ∎

Since $10 \overset{3}{\equiv} 1$, you can use the same technique to find the remainder of an integer divided by 3. Next we discuss how we can find the remainder of an integer divided by 11.

Lecture 14: Remainder of a division by 11

Wednesday, November 23, 2016 6:18 PM

Ex. What is the remainder of 10^n divided by 11 (for $n \in \mathbb{Z}^+$)?

Solution. $10 \overset{11}{\equiv} -1 \implies$ for every $n \in \mathbb{Z}^+$, $10^n \overset{11}{\equiv} (-1)^n$

So, if n is even, remainder is 1.

And, if n is odd, remainder is 10.

(warning: Remainder is always non-negative.)

Ex. What is the remainder of 109109140100103 divided by 11?

Solution. 109109140100103 =

$$3 + 10 \times 0 + 10^2 \times 1 + 10^3 \times 0 + 10^4 \times 0 + 10^5 \times 1 + 10^6 \times 0 + 10^7 \times 4 +$$

$$10^8 \times 1 + 10^9 \times 9 + 10^{10} \times 0 + 10^{11} \times 1 + 10^{12} \times 9 + 10^{13} \times 0 + 10^{14} \times 1$$

$$\overset{11}{\equiv} 3 - 0 + 1 - 0 + 0 \cancel{- 1} + 0 - 4 \cancel{+ 1} - \cancel{9} + 0 - \cancel{1} + \cancel{9} - 0 + \cancel{1}$$

$$\boxed{\begin{array}{l} 10^n \equiv (-1)^n \ (\text{mod } 10) \implies \text{powers of 10 should be replaced with } 1 \text{ or } -1 \\ \implies \text{we should alternate between adding and subtracting digits.} \end{array}}$$

$\overset{11}{\equiv} 0$. So this number is divisible by 11 and the remainder is 0.

Lecture 14: Pigeonhole and divisibility

Monday, November 28, 2016 6:08 PM

Problem. For every $k_1, \dots, k_{n+1} \in \mathbb{Z}$, there are $i \neq j$ such that

$$n \mid k_i - k_j .$$

Solution. Let's recall that $n \mid k_i - k_j \Leftrightarrow k_i \overset{n}{\equiv} k_j \Leftrightarrow r_n(k_i) = r_n(k_j)$.

This points us towards considering the remainder function.

Let $f: \{1, 2, \dots, n+1\} \to \{0, 1, \dots, n-1\}$, $f(i) = r_n(k_i)$.

(Notice that $r_n(a)$ is an integer in $\{0, 1, \dots, n-1\}$, so f is well-defined.)

So there are $n+1$ pigeons and n pigeonholes. Therefore, by the pigeonhole principle, there exist $i \neq j$ such that $f(i) = f(j)$; this means $r_n(k_i) = r_n(k_j)$ for some $i \neq j$. Hence $k_i \overset{n}{\equiv} k_j$ which implies

$$n \mid k_i - k_j . \qquad \blacksquare$$

For $n = 2$, we obtain the following result which was the bonus problem in your first exam. For every $a, b, c \in \mathbb{Z}$, $2 \mid a-b$ or $2 \mid b-c$ or $2 \mid c-a$. Hence, $2 \mid (a-b)(b-c)(c-a)$.

(This problem has the following alternative solution which was the intended solution for your exam. Suppose to the contrary that $(a-b)(b-c)(c-a)$ is odd. Then $a-b$, $b-c$, and $c-a$ are odd. Notice that when we add three odd numbers, we get an odd number. Hence,

$$(a-b)+(b-c)+(c-a) \text{ is odd.}$$

But $(a-b)+(b-c)+(c-a)=0$ is even, which is a contradiction.

Definition. Let a and b be two integers such that at least one of them is non-zero. The greatest common divisor of a and b is denoted by $\gcd(a,b)$. So, if $d=\gcd(a,b)$, then

- $d \mid a$ and $d \mid b$ (d is a common divisor of a and b)
- $\left.\begin{array}{l} d' \mid a \\ d' \mid b \end{array}\right\} \Rightarrow d' \leq d$ (every common divisor of a and b is at most d.)

Recall. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

Lemma. For every non-zero integers a and b we have

$$1 \leq \gcd(a,b) \leq \min\{|a|,|b|\}$$

Proof. • $1 \mid a$ and $1 \mid b \Rightarrow 1 \leq \gcd(a,b)$.

• Let $d=\gcd(a,b)$. So $1 \leq d$, and hence $|d|=d$.

Lecture 14: gcd of two integers

Monday, November 28, 2016 6:19 PM

$$\left.\begin{array}{l} \left.\begin{array}{l} d \mid a \\ a \neq 0 \end{array}\right\} \Rightarrow |d| \leq |a| \\ \left.\begin{array}{l} d \mid b \\ b \neq 0 \end{array}\right\} \Rightarrow |d| \leq |b| \end{array}\right\} \Rightarrow d = |d| \leq \min\{|a|, |b|\}.$$

$\blacksquare$

The following is one of the most important properties of the gcd of two integers.

<u>Theorem</u>. Let a and b be positive integers. Then there are integers r and s such that $\gcd(a,b) = ra + sb$.

We will use the well-ordering principle and prove this theorem in the next lecture. For now, we mention the following corollary.

<u>Corollary</u>. Suppose $a, b \in \mathbb{Z}^+$. If $d \mid a$ and $d \mid b$, then

$$d \mid \gcd(a,b).$$

<u>Proof.</u> By the previous theorem, there exist $r, s \in \mathbb{Z}$ such that $\gcd(a,b) = ra + sb$. Since $d \mid a$ and $d \mid b$, $a \overset{d}{\equiv} 0$ and $b \overset{d}{\equiv} 0$. Therefore $ra + sb \overset{d}{\equiv} (r)(0) + (s)(0) \overset{d}{\equiv} 0$. Hence $d \mid ra+sb$, which implies $d \mid \gcd(a,b)$. $\blacksquare$