Lecture 26: Congruence arithmetic

Wednesday, November 23, 2016 5:09 PM

Recall: Division algorithm For any $a, b \in \mathbb{Z}$, $b \neq 0$, there is a unique pair (q, r) of integers such that

(1) $a = bq + r$ (2) $0 \leq r < |b|$.

q is called the quotient of a divided by b, and r is called the remainder of a divided by b.

Definition. For $n \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, we say a is congruent to b modulo n and write $a \equiv b \pmod{n}$ or $a \overset{n}{\equiv} b$ if $n \mid a-b$, i.e. $a-b$ is an integer multiple of n.

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

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

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

Let's recall some of the basic properties of divisibility before we continue our study of congruence arithmetics.

Recall $\forall d, a, b \in \mathbb{Z}$, we have

① $d \mid a \Rightarrow d \mid ab$.

② $(d \mid a \wedge d \mid b) \Rightarrow d \mid a \pm b$.

Lecture 26: Congruence arithmetic

Wednesday, November 23, 2016 5:24 PM

(3) $\left.\begin{array}{l} d \mid a_1 - a_2 \\ d \mid b_1 - b_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} d \mid (a_1+b_1) - (a_2+b_2) \\ d \mid a_1 b_1 - a_2 b_2 . \end{array}\right.$

Let me just quickly recall how we showed the last assertion:

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

Since $d \mid a_1 - a_2$ and $d \mid b_1 - b_2$, there are integers k_1 and k_2 such that $a_1 - a_2 = d k_1$ and $b_1 - b_2 = d k_2$. So by ⊛ we get $a_1 b_1 - a_2 b_2 = (d k_1) b_1 + a_2 (d k_2) = d \, (\underbrace{k_1 b_1 + a_2 k_2}_{\text{is an integer}})$. Hence $d \mid a_1 b_1 - a_2 b_2$.

Lemma. For any $n \in \mathbb{Z}^+$, $a, b, c \in \mathbb{Z}$, we have

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

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

Proof. (1) $a \overset{n}{\equiv} b \Rightarrow n \mid a - b \Rightarrow n \mid (-1)(a-b) = b - a$

$\Rightarrow b \overset{n}{\equiv} a$.

(2) $\left.\begin{array}{l} a \overset{n}{\equiv} b \Rightarrow n \mid a - b \\ b \overset{n}{\equiv} c \Rightarrow n \mid b - c \end{array}\right\} \Rightarrow n \mid (a-b) + (b-c)$

$\Rightarrow n \mid a - c$

$\Rightarrow a \overset{n}{\equiv} c$. ■

(For all practical reasons it behaves like an equality.)

Corollary. For $n \in \mathbb{Z}^+$, $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, we have

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

Proof. $$\left.\begin{array}{l} a_1 \overset{n}{\equiv} a_2 \Rightarrow n \mid a_1-a_2 \\ b_1 \overset{n}{\equiv} b_2 \Rightarrow n \mid b_1-b_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} n \mid (a_1+b_1)-(a_2+b_2) \\ n \mid a_1b_1-a_2b_2 \end{array}\right\} \Rightarrow$$

$$\left\{\begin{array}{l} a_1+b_1 \overset{n}{\equiv} a_2+b_2 \\ a_1b_1 \overset{n}{\equiv} a_2b_2. \end{array}\right. \blacksquare$$

We skipped proof of this corollary in class.
How its proof goes was mentioned only verbally.

Corollary. For any $m, n \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, we have

$$a \overset{n}{\equiv} b \Rightarrow a^m \overset{n}{\equiv} b^m.$$

Proof. We prove this by induction on m.

Base of induction. $m=1$. This case is clear as

$$a^1 = a,\ b^1 = b, \text{ and } a \overset{n}{\equiv} b.$$

Induction step. For a given integer k, we have to show

$$a^k \overset{n}{\equiv} b^k \overset{?}{\Rightarrow} a^{k+1} \overset{n}{\equiv} b^{k+1}.$$

$$\left.\begin{array}{l} a^k \overset{n}{\equiv} b^k \\ a \overset{n}{\equiv} b \end{array}\right\} \Rightarrow a^k \cdot a \overset{n}{\equiv} b^k \cdot b \quad \text{(by the above lemma)}$$

$$\Rightarrow a^{k+1} \equiv b^{k+1} \pmod{n}. \blacksquare$$

Lecture 26: Division algorithm; congruence arithmetic

Wednesday, November 23, 2016 5:54 PM

__Theorem__. For any $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$, there is a unique $r \in \mathbb{Z}$ such that (1) $a \equiv r \pmod{n}$

(2) $0 \le r < n$.

__Proof__. __Existence__. By Division algorithm there are integers q and r such that ① $a = nq + r$,

② $0 \le r < n$.

So $a - r = nq$, which implies $n \mid a-r$. Hence $a \overset{n}{\equiv} r$.

Thus $a \overset{n}{\equiv} r$ and $0 \le r < n$.

__Uniqueness__ Using Division algorithm, it is enough to prove

$$\left.\begin{aligned} &a \overset{n}{\equiv} r \\ &0 \le r < n \end{aligned}\right\} \Rightarrow \begin{array}{l} r \text{ is the remainder of} \\ a \text{ divided by } n. \end{array}$$

$a \overset{n}{\equiv} r \Rightarrow n \mid a - r \Rightarrow \exists q \in \mathbb{Z},\ nq = a - r$

$$\left.\begin{aligned} &\Rightarrow a = nq + r \\ \text{and we have } &0 \le r < n \end{aligned}\right\} \Rightarrow \begin{array}{l} r \text{ is the remainder of} \\ a \text{ divided by } n. \end{array} \quad \blacksquare$$

Lecture 26: 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 any $n \in \mathbb{Z}^+$, $10^n \overset{9}{\equiv} 1^n = 1$

(by a corollary proved inductively on n.)

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

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

Solution. 109109140100103 =

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

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

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

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

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

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

Lecture 26: 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 any $n \in \mathbb{Z}^+$, $10^n \overset{11}{\equiv} (-1)^n$
(by a corollary proved inductively on 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.