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

\begin{align*}
(1) \quad a &= bq + r \\
(2) \quad 0 \leq r < |b|.
\end{align*}

$q$ 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 $a \equiv b \pmod{n}$ if $n \mid a-b$, i.e. $a-b$ is an integer multiple of $n$.

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

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

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

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

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

\begin{align*}
(1) \quad d \mid a &\Rightarrow d \mid ab. \\
(2) \quad (d \mid a \land d \mid b) &\Rightarrow d \mid a \pm b.
\end{align*}
Lecture 26: Congruence arithmetic

Wednesday, November 23, 2016  5:24 PM

\( \text{(3) } d \mid a_1-a_2 \iff d \mid (a_1+b_1)-(a_2+b_2) \)
\( d \mid b_1-b_2 \iff d \mid a_1b_1-a_2b_2. \)

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

\( a_1b_1-a_2b_2 = a_1b_1-a_2b_1 + a_2b_1-a_2b_2 = (a_1-a_2)b_1 + a_2(b_2-b_1) \) \( \odot \)

Since \( d \mid a_1-a_2 \) and \( d \mid b_1-b_2 \), there are integers \( h_1 \) and \( h_2 \) such that \( a_1-a_2 = dh_1 \) and \( b_1-b_2 = dh_2 \). So by \( \odot \)

we get \( a_1b_1-a_2b_2 = (h_1b_1 + h_2a_2)(b_2-b_1) = d h_1 b_2 - d h_2 b_1 \).

Hence \( d \mid a_1b_2-a_2b_1. \)

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

(1) \( a \equiv b \rightarrow b \equiv a. \)

(2) \( a \equiv b \iff a \equiv c. \)

Proof. (1) \( a \equiv b \rightarrow n \mid a-b \rightarrow n \mid (-1)(a-b) = b-a \)

\( \rightarrow b \equiv a. \)

(2) \( a \equiv b \rightarrow n \mid a-b \rightarrow n \mid (a-b) + (b-c) \)

\( b \equiv c \rightarrow n \mid b-c \rightarrow n \mid a-c \)

\( \rightarrow a \equiv c. \) \( \blacksquare \)

(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
\[
\begin{align*}
  a_1 \equiv a_2 \quad &\Rightarrow \quad a_1 + b_1 \equiv a_2 + b_2, \\
  b_1 \equiv b_2 \quad &\Rightarrow \quad a_1 b_1 \equiv a_2 b_2.
\end{align*}
\]

Proof. \( a_1 \equiv a_2 \Rightarrow n \mid (a_1 - a_2) \Rightarrow n \mid (a_1 + b_1) - (a_2 + b_2) \Rightarrow b_1 \equiv b_2 \Rightarrow n \mid b_1 - b_2 \Rightarrow n \mid a_1 b_1 - a_2 b_2 \]
\[
\begin{align*}
  a_1 + b_1 &\equiv a_2 + b_2, \\
  a_1 b_1 &\equiv a_2 b_2.
\end{align*}
\]

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

Corollary. For any \( m, n \in \mathbb{Z}^+ \), \( a, b \in \mathbb{Z} \), we have
\[
  a \equiv b \Rightarrow a^n \equiv b^m.
\]

Proof. We prove this by induction on \( m \).

Base of induction, \( m=1 \). This case is clear as
\[
  a^1 = a, \quad b^1 = b, \quad \text{and} \quad a^n \equiv b.
\]

Induction step. For a given integer \( k \), we have to show
\[
  a^k \equiv b^k \Rightarrow a^{k+1} \equiv b^{k+1}.
\]
\[
\begin{align*}
  a^k &\equiv b^k \Rightarrow a^k \cdot a^n \equiv b^k \cdot b^n \quad \text{(by the above lemma)} \\
  a^n &\equiv b^n \Rightarrow a^{k+1} \equiv b^{k+1} \pmod{n}.
\end{align*}
\]
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. \( 0 \leq r < n \).

Proof. Existence. By Division algorithm there are integers \( q \) and \( r \) such that

1. \( a = nq + r \),
2. \( 0 \leq r < n \).

So \( a - r = nq \), which implies \( n \mid a - r \). Hence \( a \equiv r \pmod{n} \).

Thus \( a \equiv r \) and \( 0 \leq r < n \).

Uniqueness Using Division algorithm, it is enough to prove \( a \equiv r \Rightarrow r \) is the remainder of \( a \) divided by \( n \).

\[
\begin{align*}
\quad & a \equiv r \Rightarrow n \mid a - r \Rightarrow \exists q \in \mathbb{Z}, \quad nq = a - r \\
\quad & \Rightarrow a = nq + r \Rightarrow r \text{ is the remainder of } a \text{ divided by } n.
\end{align*}
\]
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. $10 \equiv 1 \implies$ for any $n \in \mathbb{Z}^+$, $10^n \equiv 1^n = 1$

(by a corollary proved inductively on $n$.)

$\implies$ 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

\equiv 3 + 0 + 1 + 0 + 0 + 1 + 0 + 4 + 1 + 9 + 0 + 1 + 9 + 0 + 1

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

which means we are adding the digits of this number

$9 \equiv 12 \equiv 3$. 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. $10 \equiv -1 \mod 11$ for any $n \in \mathbb{Z}^+$, $10^n \equiv (-1)^n$ (by a corollary proved inductively on $n$.)

So, if $n$ is even, remainder is 1. (Warning: Remainder is always non-negative.)

And, if $n$ is odd, remainder is 10.

Ex. What is the remainder of 109109140 100 103 divided by 11?

Solution. $109109140 100 103 = $

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

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

$11 \equiv 3 - 0 + 1 - 0 + 0 - 1 + 0 - 4 + 1 - 9 + 0 - 1 + 9 - 0 + 1$

$10^n \equiv (1)^n \mod 10$ $\Rightarrow$ powers of 10 should be replaced with 1 or -1

$\Rightarrow$ we should alternate between adding and subtracting digits.

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