Division algorithm and primes.

Wednesday, November 25, 2015 11:09 AM

In the previous lecture we stated the division theorem and defined the integer part of a real number. We proved:

$$\forall x \in \mathbb{R},\ \exists!\ n \in \mathbb{Z},\quad n \le x < n+1$$

and called it the integer part $\lfloor x \rfloor$ of x.

So $$\lfloor x \rfloor \le x < \lfloor x \rfloor + 1.$$

Theorem (Division theorem)

$$\forall\ (a,b) \in \mathbb{Z} \times \mathbb{Z}^{+},\ \exists!\ (q,r) \in \mathbb{Z} \times \mathbb{Z},$$

(1) $\quad a = bq + r$

(2) $\quad 0 \le r < b.$

Proof **Existeness.** Let $q = \lfloor a/b \rfloor$, and $r = a - b\lfloor a/b \rfloor$.

Then clearly (1) holds.

$$\left.\begin{array}{r} a/b - 1 < \lfloor a/b \rfloor \le a/b \\ 0 < b \end{array}\right\} \Rightarrow \begin{array}{l} a - b < b\lfloor a/b \rfloor \le a \\ \Rightarrow -a \le -b\lfloor a/b \rfloor < b - a \end{array}$$

$$\Rightarrow 0 \le a - b\lfloor a/b \rfloor < b$$

$$\Rightarrow 0 \le r < b.$$

Uniqueness. Suppose (q_1, r_1) and (q_2, r_2) satisfy (1) and (2).

Then $a = bq_1 + r_1 = bq_2 + r_2$

$0 \le r_1, r_2 < b.$

By symmetry we can and will assume $r_1 \le r_2$.

So $0 \le r_2 - r_1 < b$ and $r_2 - r_1 = b(q_1 - q_2)$ $\Rightarrow r_1 = r_2$

$$\Rightarrow \left.\begin{array}{r} 0 \le q_1 - q_2 < 1 \\ q_1, q_2 \in \mathbb{Z} \end{array}\right\} \Rightarrow q_1 = q_2$$

$\blacksquare$

Corollary. For any $n \in \mathbb{Z}^{+}$, any integer can be written in

Corollary. For any $n \in \mathbb{Z}'$, any integer can be written in one and only one of the forms:

$$nk \;, \quad nk+1, \quad nk+2, \quad \dots, \quad nk+(n-1).$$

Corollary. $n \mid m \iff$ the remainder of the division of m by n is 0.

Proof $(\Rightarrow)$ $n \mid m \Rightarrow m = nq$

$\Rightarrow$ by uniqueness q is the quotient and $r=0$ is the remainder.

$(\Leftarrow)$ $\left.\begin{array}{l} m = nq+r \\ r=0 \end{array}\right\} \Rightarrow m = nq \Rightarrow n \mid m.$

Corollary. $n \mid a_2 - a_1 \iff$ the remainder of a_1 divided by n is equal to the remainder of a_2 divided by n.

Proof. $(\Rightarrow)$ $\left.\begin{array}{l} a_1 = n q_1 + r_1 \\ n \mid a_2 - a_1 \Rightarrow a_2 - a_1 = n q \end{array}\right\} \Rightarrow \begin{array}{l} a_2 = (a_2 - a_1) + a_1 \\ \quad = n(q+q_1) + r_1 \end{array}$

$\Rightarrow$ by uniqueness $q_2 = q + q_1$ is the quotient and r_1 is the remainder.

(Notice that $0 \le r_1 < n$.)

$(\Leftarrow)$ $\left.\begin{array}{l} a_1 = n q_1 + r_1 \\ a_2 = n q_2 + r_2 \\ r_1 = r_2 \end{array}\right\} \Rightarrow \left.\begin{array}{l} a_2 - a_1 = n(q_2 - q_1) \\ q_2 - q_1 \in \mathbb{Z} \end{array}\right\} \Rightarrow n \mid a_2 - a_1.$ ■

Theorem (Euclid) There are infinitely many primes.

Proof. Suppose to the contrary that there are only finitely many primes: $p_1, p_2, \dots, p_n$.

Let $m = p_1 p_2 \cdots p_n + 1$. Long time ago we used strong induction to prove that any positive integer can be written as a

l f

product of primes. Suppose p is a prime and

$p \mid m$.

Since $p_1, \dots, p_n$ are the only primes, $p = p_i$ for some i.

So the remainder of m divided by $p = p_i$ is 1

, but it should be zero which is a contradiction. ■

Ex. Prove that for any $n \in \mathbb{Z}^+$ there is $m \in \mathbb{Z}^+$ such that

ⓐ the digits of m in base 10 are either 1 or 0.

ⓑ $n \mid m$.

Proof. Consider the remainders of $1, 11, 111, \dots, \underbrace{11\cdots1}_{n+1 \text{ many}}$

divided by n. So we get $n+1$ integers

$$0 \le r_1, \dots, r_{n+1} < n.$$

By pigeonhole principle, for some $i<j$, $r_i = r_j$.

Hence $n \mid \underbrace{1\cdots1}_{j} - \underbrace{1\cdots1}_{i} = \underbrace{1\cdots1}_{j-i}\underbrace{0\cdots0}_{i}$. ■

Definition. $a_1 \overset{n}{\equiv} a_2$ if $n \mid a_1 - a_2$. (we also write $a_1 \equiv a_2 \pmod{n}$.)

We say either a_1 is congruent to a_2 modulo n or

a_1 is a_2 mod n.

Proposition. Let $n \in \mathbb{Z}^{\ge 2}$. Then

$$\forall a \in \mathbb{Z},\ \exists!\, r \in \{0, 1, \dots, n-1\},\ a \overset{n}{\equiv} r.$$

Moreover r is the remainder of a divided by n.

Proof. Existence. Let q and r be the quotient and remainder

of a divided by n. So $a = nq + r$ and $r \in \{0, 1, \dots, n-1\}$.

$\Rightarrow n \mid nq = a - r \Rightarrow a \overset{n}{\equiv} r$.

Uniqueness. Suppose $a \overset{n}{\equiv} r$ and $r \in \{0, 1, \dots, n-1\}$.

Then $n \mid a-r \Rightarrow \exists q \in \mathbb{Z}$ s.t. $a-r = nq$

$$\Rightarrow \left\{ \begin{array}{l} a = nq + r \\ 0 \leq r < n \end{array} \right\} \Rightarrow$$ by the algorithm theorem r is the remainder of a divided by n. In particular, it is unique. ■

<u>Corollary</u> $\forall m_1, m_2 \in \mathbb{Z}, \forall n \in \mathbb{Z}^{\geq 2}$, $m_1 \overset{n}{\equiv} m_2 \Leftrightarrow$ the remainder of m_1 divided by n is equal to the remainder of m_2 divided by n.

<u>Proof</u>. By the above <u>Proposition</u>

$m_1 \overset{n}{\equiv} r_1$, where r_1 is the remainder of m_1 divided by n

$m_2 \overset{n}{\equiv} r_2$, where r_2 is the remainder of m_2 divided by n

$(\Rightarrow)$ $$\left. \begin{array}{l} m_1 \overset{n}{\equiv} m_2 \Rightarrow r_1 \overset{n}{\equiv} r_2 \\ r_1, r_2 \in \{0, 1, \dots, n-1\} \end{array} \right\} \Rightarrow$$ by the uniqueness in the above proposition, $r_1 = r_2$.

$(\Leftarrow)$ $m_1 \overset{n}{\equiv} r_1 = r_2 \overset{n}{\equiv} m_2 \Rightarrow m_1 \overset{n}{\equiv} m_2$. ■

<u>Corollary</u> $\forall n \in \mathbb{Z}^{\geq 2}$, any integer is of <u>one</u> and <u>only</u> <u>one</u> of the following forms: nk, $nk+1$, $\dots$, $nk+(n-1)$ for some integer k.

<u>Ex</u>. Any integer is of <u>one and only one</u> of the forms

$2k$, $2k+1$ for some integer k

Hence $2 \nmid m \Leftrightarrow m = 2k+1$ for some integer k.

<u>Ex</u>. Any integer is of <u>one and only one</u> of the forms

$3k$, $3k+1$, $3k+2$ for some integer k.

Hence $3 \nmid m \Leftrightarrow m = 3l \pm 1$ for some integer l.

(that

(Notice that $3k+2=3(k+1)-1$.)

Long time ago you have proved in your HW assignment that

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

Lemma.

$$\left.\begin{array}{l} a_1 \overset{n}{\equiv} b_1 \\ a_2 \overset{n}{\equiv} b_2 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} a_1+a_2 \overset{n}{\equiv} b_1+b_2 \\ a_1a_2 \overset{n}{\equiv} b_1b_2 . \end{array}\right.$$

Ex. $10 \overset{9}{\equiv} 1 \longrightarrow 10^k = \underbrace{10\times\cdots\times 10}_{k \text{ times}} \overset{9}{\equiv} \underbrace{1\times\cdots\times 1}_{k \text{ times}} = 1.$

Ex. Suppose $\overline{a_k a_{k-1} \cdots a_0}$ is the representation of a positive integer in base 10, e.g. for 12075 we have $a_0=5$, $a_1=7$, $a_2=0$, $a_3=2$, and $a_4=1$. Hence $\overline{a_k a_{k-1} \cdots a_0} = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$.

Using the previous example we have

$$\overline{a_k a_{k-1} \cdots a_1 a_0} = a_k 10^k + \cdots + a_1 10 + a_0 \overset{9}{\equiv} a_k + \cdots + a_1 + a_0$$

So to find the remainder of <u>m divided by 9</u>, it is enough to add its digits again and again.

Ex. Find the remainder of 1207530458 divided by 9.

Solution.
$$\begin{aligned} 1207530458 &\overset{9}{\equiv} 1+2+0+7+5+3+0+4+5+8 \\ &= 35 \\ &\overset{9}{\equiv} 3+5 = 8 \end{aligned}$$

and $0 \le 8 < 9$. So the remainder is 8 by the above proposition.

Ex. Any perfect square is of the form $3k$ or $3k+1$ for some integer k.

Proof. $\forall n \in \mathbb{Z}$, $n \overset{3}{\equiv} 0$ or $n \overset{3}{\equiv} 1$ or $n \overset{3}{\equiv} 2$

3 3 (

$$n \overset{3}{\equiv} 0 \implies n^2 = (n)(n) \overset{3}{\equiv} (0)(0) = 0 \implies \exists k \in \mathbb{Z},\ n^2 = 3k,$$

$$n \overset{3}{\equiv} 1 \implies n^2 = (n)(n) \overset{3}{\equiv} (1)(1) = 1 \implies \exists k \in \mathbb{Z},\ n^2 = 3k+1,$$

$$n \overset{3}{\equiv} 2 \implies n^2 = (n)(n) \overset{3}{\equiv} (2)(2) = 4 \overset{3}{\equiv} 1 \implies \exists k \in \mathbb{Z},\ n^2 = 3k+1.$$

$\blacksquare$