Lesson 19

Congruence classes mod m

Def: If $a, b \in \mathbb{Z}$ a, b are called coprime if $(a, b) = 1$

Th If a divides bc and $(a, b) = 1$ then a divides c.

$bc = ak$ for some $k \in \mathbb{Z}$

Proof: We can write $1 = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$. So $c = cax_0 + bcy_0$ so $c = cax_0 + aky_0$ for some k so a divides c

Corollary: if p is prime and p div ab then p divides a or p divides b

Corollary: if p is prime and p div $a_1 \cdots a_n$ then p divides a_i for some i.

Corollary: prime factorization is unique:

by contradiction assume there is $n \in \mathbb{Z}^+$ which has 2 distinct prime factorizations that is $n = p_1^{k_1} \cdots p_n^{k_n} = q_1^{h_1} \cdots q_m^{h_m}$, with p_i is and q_j $1 < j < m$ all prime and $i \leq n$ either no p is equal to q_1, which is impossible because q_1 must divide p_i for some i so $q_1 = p_i$ or $p_1 = q_1$ but $h_1 > k_1$ which after dividing both sides by $q_1^{k_1}$ becomes the previous case.

Congruence classes mod m

EVEN

$x = 2q + 0$

ODD

$x = 2q + 1$

$[0]_3$

$x = 3q + 0$

$[1]_3$

$x = 3q + 1$

$[2]_3$

$x = 3q + 2$

$[0]_m$

$x = mq + 0$

$[1]_m$

$x = mq + 1$

. . .

$[m-1]_m$

$x = mq + m - 1$

Def given $m > 0$ $m \in \mathbb{Z}$ $0 \leq r < m$

$$[r]_m = \{ x \in \mathbb{Z} \mid x = qm + r \text{ for some } q \in \mathbb{Z} \}$$

Ex $[2]_5 = \{2, 7, 12, 17, \ldots -3, -8, \ldots\}$

$-3 = 5 \cdot (-1) + 2$

Def Given $a, b, m \in \mathbb{Z}$ $m > 0$ we say a is congruous to b modulus m $a \equiv_m b$ or $a \equiv b \mod m$ if a and b have the same reminder when divided by m i.e if there is r s.t $a, b \in [r]_m$

Ex $126 \equiv 11 \mod 5$

$126 = 5 \cdot 25 + 1$

$11 = 5 \cdot 2 + 1$

Th $a \equiv b \bmod m \iff m \text{ div } (a-b)$

Proof Suppose $a \equiv b \bmod m$ then

$a = mq_1 + r$ and $b = mq_2 + r$

so $a - b = m(q_1 - q_2)$ so m div $a-b$.

Now suppose $a - b = mq$ and

$a = mq_1 + r_1$, $b = mq_2 + r_2$ then

$a - b = m(q_1 - q_2) + r_1 - r_2 = mq$

so $r_1 - r_2 = m(q - q_1 + q_2) = mk$

where $k \in \mathbb{Z}$. but $0 \le r_1, r_2 < m$

so $-m < r_1 - r_2 < m$ so

k must be 0, therefore $r_1 = r_2$

Ex $126 - 11 = 115$ which is divisible by 5, so $126 \equiv 11 \bmod 5$

Th Given $m \in \mathbb{Z}$ $m > 0$

1) $\forall a \in \mathbb{Z}$ $a \equiv_m a$ Reflexive

2) $\forall a, b \in \mathbb{Z}$ $a \equiv_m b \Rightarrow b \equiv_m a$ Symmetric

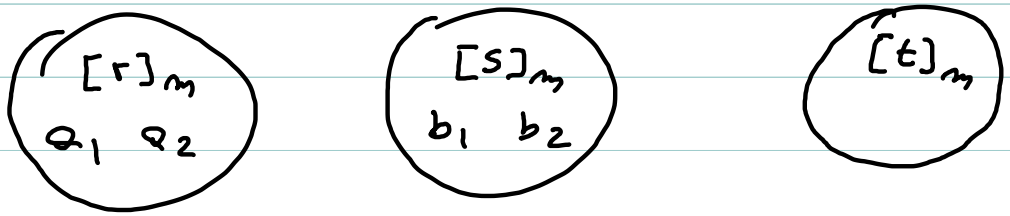
3) $\forall a, b, c \in \mathbb{Z}$ $a \equiv_m b \wedge b \equiv_m c \Rightarrow a \equiv_m c$ Transitive

Th Given $m \in \mathbb{Z}$ $m > 0$

a) $a_1 \equiv_m a_2 \wedge b_1 \equiv_m b_2 \Rightarrow a_1 + b_1 \equiv_m a_2 + b_2$

b) $a_1 \equiv_m a_2 \wedge b_1 \equiv_m b_2 \Rightarrow a_1 - b_1 \equiv_m a_2 - b_2$

c) $a_1 \equiv_m a_2 \wedge b_1 \equiv_m b_2 \Rightarrow a_1 b_1 \equiv_m a_2 b_2$



Proof:

Suppose $a_1 = mq_1 + r$ $a_2 = mq_2 + r$

$b_1 = mt_1 + s$ $b_2 = mt_2 + s$

a) $a_1 + b_1 = m(q_1 + t_1) + r + s = m(q_1 + t_1 + q) + r'$

$a_2 + b_2 = m(q_2 + t_2) + r + s = m(q_2 + t_2 + q) + r'$

if $r + s = mq + r'$

b) hw

c) $a_2 b_2 - a_1 b_1 = (mq_2 + r)(mt_2 + s) - (mq_1 + r)(mt_1 + s) = mk$

where k is an integer so m div $a_2 b_2 - a_1 b_1$ therefore $a_1 b_1 \equiv_m a_2 b_2$

The previous theorem tells us we can define operations $+, -, \cdot$ on congruence classes.

$$[r_1]_m + [r_2]_m = [s]_m$$

where $r_1 + r_2 = mq + s$

$$[r_1]_m - [r_2]_m = [t]_m$$

where $r_1 - r_2 = ml + t$

$$[r_1]_m \cdot [r_2]_m = [u]_m$$

where $r_1 \cdot r_2 = mw + u$

Binary arithmetic

$$[1]_2 + [1]_2 = [0]_2$$

$$[3]_5 + [3]_5 = [1]_5$$

Computation mod m

i.e compute

$$7 \times 2 + 3 \mod 5$$

what do we mean?

$$[2]_5 \cdot [2]_5 + [3]_5 = [2]_5$$

$$7 \times 2 + 3 = 17 \equiv 2 \mod 5$$

Note: When we compute mod m we are allowed to replace a number (NOT an exponent) with some other number congruent to it mod m

Ex: Compute

$8^{10} + 3^{10} + 3 \cdot 4 + 79 \mod 7 =$

$1^{10} + 3^{10} + 12 + 2 \mod 7 =$

$1 + 3^{10} + 14 \mod 7 =$

$1 + (3^2)^5 + 0 \mod 7 =$

$1 + 2^5 \mod 7 =$

$1 + 32 \mod 7 =$

$5 \mod 7$

Clock computation

Rome is 9 hours ahead of Seattle. Flying from Seattle to Rome takes 10 hours.
If a flight leaves Seattle at 2 pm local time, what time is it in Rome when the flight lands?

$$14 + 9 + 10 \mod 24$$

9 am