MA 190

→ His book should be on blackboard somewhere.

(m is an integer) On a clock with m hours, the answer to any calculation should be an integer in the range $0 \leq x \leq (m-1)$

$a \equiv b \mod m$

$\therefore$ $a-b$ is an integer multiple of m

Multiplicative inverse (cont.)

Suppose $2a \equiv 1 \mod m$ and $2b \equiv 1 \mod m$

$\rightarrow a \equiv 1a \equiv 2b.a \equiv 2a.b \equiv 1.b \equiv b$

$a \equiv b$

↳ commutativity of multiplication

TAKE → $3^{-1} \equiv ?$ mod 12

NaN, undefined. 3 has no inverse mod 12.

Which numbers do have an inverse on an m hour clock?

↳ ones whose highest common factor with 12 is 1

↳ that's why primes are used as mod for clock.

<u>How</u> do we find the inverse of K mod m?

15 mod 26 ? → allowable inverses are $0 \leq x \leq 25$, $x \in \mathbb{N}$

how do we find a number K such that $15K \equiv 1 \mod 26$?

(EUCLID'S ELEMENTS) <u>EUCLIDEAN</u> <u>ALGORITHM</u>

STEP 1: Use E.A. to find greatest common divisor (gcd)(15, 26) → 1.

STEP 2: Use the output of E.A. to find the inverse.

$26 = 1 \cdot 15 + \overset{r}{11}$

$15 = 1 \cdot 11 + \overset{r}{4}$

$11 = 2 \cdot 4 + \overset{r}{3}$

$4 = 1 \cdot 3 + \overset{r}{1}$ ← penultimate remainder is g.c.d.

$3 = 3 \cdot 1 + \overset{r}{0}$ [STOP]

use previous line to re-express 3

$1 = 4 - (1 \cdot 3)$

$= 4 - (11 - 2 \cdot 4)$

$= (3 \cdot 4) - 11$

$= 3 \cdot (15 - 11) - 11$

$1 = 3 \cdot 15 + (-4 \cdot 11)$

$= 3 \cdot 15 - 4(26 - 15)$

$1 = 7 \cdot 15 - 4 \cdot 26$

$1 = 7 \cdot 15 - 4 \cdot 0 \mod 26$

$15^{-1} \mod 26$

$\equiv 7$