Q: It's 12:30 pm now, what time will it be in 53 hours?

$$12{:}30 +_{24} 53 = 12{:}30 + 5 = 5{:}30 \text{ pm}$$
(or 17:30)

Functions w/ a, b given integers, m integer ≥ 2

$$f: \mathbb{Z} \to \mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\} \text{ given by } f(x) = ax+b \bmod m.$$

Opening application vignette:

Modular arithmetic and <u>check</u> digits

1. UPC code: 12 digits $x_1, x_2, x_3, \ldots, x_{12} \in \mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$.

   Valid UPC code satisfies

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + \cdots + 3x_{11} + x_{12} \equiv 0 \pmod{10}$$

Ex.) See if

2 3 7 1 4 5 5 0 1 3 2 7

is valid as a UPC code.

$$3(2)+3+3(7)+1+3(4)+5+3(5)+0+3(1)+3+3(2)+7 \stackrel{?}{\equiv} 0 \pmod{10}$$

$$\underbrace{\cancel{6}+\cancel{3}+\cancel{21}}_{=30\equiv 0}+\underline{1}+\underline{12}+\cancel{5}+\cancel{15}+3+3+\underbrace{6+7}_{\equiv 3}$$

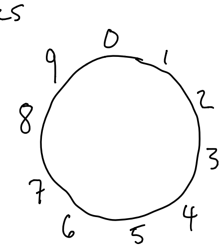
$$\equiv 1+2+3+3+3 = 12 \equiv 2 \pmod{10}$$

A: It isn't valid - we didn't get 0.

Ex.) What final digit x_{12}, instead of 7, makes

$$2\,3\,7\,1\,4\,5\,5\,0\,1\,3\,2\,\underline{x_{12}}$$

a valid UPC code?



We saw already that when $x_{12} = 7$, our sum

$$3x_1 + x_2 + \cdots + 3x_{11} + x_{12} \equiv \underline{2} \pmod{10}$$

wanted 0

Replace $x_{12} = 7$ by $x_{12} = \underline{5}$ it makes the code valid

2. ISBN-10 : 10 digits $x_1, x_2, x_3, \ldots, x_{10} \in \{0, 1, 2, \ldots, 9, X\}$

(newer ISBN-13)

Valid ISBN 10's satisfy:

$$\sum_{i=1}^{10} i x_i = x_1 + 2x_2 + 3x_3 + \cdots + 10x_{10} \equiv \underline{0} \pmod{11}$$

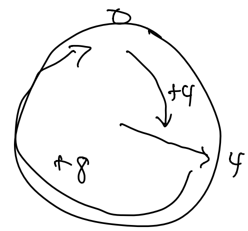
Subject of Friday: Solving linear congruence eqns. $ax + b \equiv c \pmod{m}$

Theorem: Let a, m be integers w/ $m \geq 2$ and $\gcd(a, m) = 1$.

i) There exist integers s, t such that $as + mt = 1$.
(Find s, t using Extended E.A.)

ii) $s \bmod m$ is the number in $\mathbb{Z}_m$ which is a's multiplicative inverse (i.e. $a \cdot_m s = 1$).

In fact: 'a' has a multiplicative inverse ($\cdot_m$) iff $\gcd(a, m) = 1$.

Ex.) Solve $7x + 4 \equiv 9 \pmod{12}$ 

Can undo $\underline{+4}$ by adding $\underline{8}$ more

$$7x + 4 + 8 \equiv 9 + 8 \pmod{12}$$

$$7x \equiv 5 \pmod{12}$$

Now want to multiply both sides by a mult. inv. to 7

Only 12 candidates: $0, 1, 2, 3, \ldots, 11$

Can find it (I know it exists since $\gcd(7,12) = 1$)

using trial-and-error

$$7 \cdot_{12} 0 = 0$$

$$7 \cdot_{12} 1 = 7 \quad (\text{not } 1)$$

$$7 \cdot_{12} 2 = 2 \quad (\text{not } 1)$$

somewhere in between we would find $7 \cdot_{12} \_\_ = 1$

$$\vdots$$

$$7 \cdot_{12} 11 = 5 \quad (\text{not } 1)$$

E.A. w/ $r_0 = 12$, $r_1 = 7$

$$\begin{cases} 12 = \underline{1}\,(7) + \underline{5}^{\,r_2} \\ 7 = \underline{1}\,(5) + \underline{2}^{\,r_3} \end{cases}$$

$$5 = \underline{2}\,(2) + \underline{1}^{\,r_4} \leftarrow \text{gcd}$$

$$2 = \underline{2}\,(1) + \underline{0}^{\,\text{0 remainder}}$$

Apply steps of extended E.A.: goal write gcd ($= r_4$) in terms of $\underline{r_0, r_1}$

$$1 = 5 - 2(2) = r_2 - 2(r_3)$$

$$2 = 7 - 5 \qquad (\text{or } r_3 = r_1 - r_2)$$

$$5 = 12 - 7 \qquad (\text{or } r_2 = \underline{r_0} - \underline{r_1})$$

$$1 = 5 - 2(2) \qquad \text{now insert formula for 2}$$

$$= 5 - 2(7 - 5)$$

$$= 5 - 2(7) + 2(5)$$

$$= 3(\underline{5}) - 2(7)$$

(so r_4 written in terms of $\underset{=5}{r_2}$ and $\underset{=7}{r_1}$)

$$= 3(12 - 7) - 2(7)$$

$$= 3(12) - 3(7) - 2(7)$$

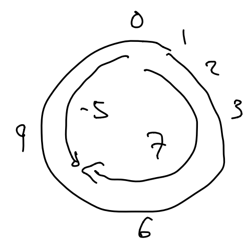
$$= 3(12) - 5(7)$$

$$= t r_0 + s r_1 \qquad \text{w/ } s = -5$$

(ii) of theorem says

$$-5 \bmod 12 = 7$$

is multiplicative inverse of 7 in mod 12 arithmetic.



$$7 \cdot_{12} 7 = 49 \bmod 12 = 1$$

Returning to our congruence eqn.

$$7x \equiv 5 \pmod{12}$$

Now multiply both sides by 7's mult. inv. (which is 7)

$$\underbrace{7 \cdot 7}_{\equiv 1} x \equiv 7 \cdot 5 \pmod{12}$$

$$\underline{x} \equiv \underline{11} \pmod{12}$$

So, there are inf. many solns. to $7x + 4 \equiv 9 \pmod{12}$.

$$\ldots, -13, -1, 11, 23, 35, \ldots$$

all can be characterized as

$$12 \mid (x-11)$$

or $$12k = x - 11$$

$$x = 11 + 12k$$
some $k \in \mathbb{Z}$.

Ex.) Solve $$5x \equiv 19 \pmod{26}$$

Q: Does 5 have a mult. inv. mod 26?

A: Yes, since $\gcd(26,5) = 1$.

$$26 = \underline{5}(5) + \underline{1} \leftarrow \text{gcd}$$

$$5 = \underline{5}(1) + \underline{0}$$

Rewrite this as $1 = 1(26) - 5(5)$

$$\underset{\uparrow}{}$$
$s = -5$

$\underline{-5} \bmod 26 = \underline{21}$ is 5's mult. inv.

Solve $$5x \equiv 19 \pmod{26}$$

by multiplying both sides by 21:

$$\underline{21}(5x) \equiv (21)(19) \pmod{26}$$

$$x \equiv 399 \equiv 9 \pmod{26}$$

Ex.)

$311x \equiv 3518 \pmod{6215}$

$-1239 \bmod 6215$ is 311's mult. inv.

$= \underline{4976}$