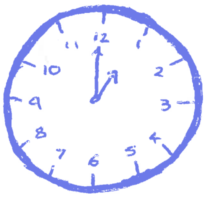
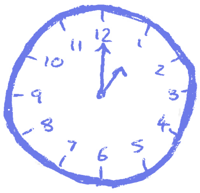
Congruences Revision

- let $m \in \mathbb{Z}$, $m > 1$ $a, b \in \mathbb{Z}$

$a \equiv b \bmod m \iff m$ divides $(a-b)$

$\iff$ a and b have the same remainder when divided by m

- Clocks use congruences modulo 12

1:00 $\leftrightarrow$  13:00 

(13:00 − 12:00 = 1:00)

- On Mercury clocks would use modulo 1,408 hours and on Neptune only 16

- We can view congruence mod m as an equiv relation

$a \sim b \iff a \equiv b \bmod m$

- This equiv rel has m equivalence classes, which we call congruence classes

$[0], [1], \ldots, [m-1]$ where

$$[r] = \{km + r \mid k \in \mathbb{Z}\}$$

eg if $m = 15$ $[7] = \{\ldots, -23, -8, 7, 22, 37, \ldots\}$

- In modulo m

$[a] + [b] = [a+b]$ $[a] \cdot [b] = [ab]$

eg $m = 17$

$$\begin{array}{ccccc} [3] & + & [5] & = & [8] \\ \parallel & & \parallel & & \parallel \\ [20] & + & [22] & = & [42] \end{array} \qquad \begin{array}{ccccccc} [2] & \cdot & [9] & = & [18] & = & [1] \\ \parallel & & \parallel & & \parallel & & \parallel \\ [19] & \cdot & [9] & = & [171] & = & [1] \end{array}$$

- $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ is a commutative ring
- Often we drop the [ ] notation

  so $\mathbb{Z}_m = \{[0], [1], \dots [m-1]\}$ and we write

  $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$
- So for $m = 17$

  $$\left.\begin{aligned} 20 + 22 &= 3 + 5 = 8 \\ 19 \cdot 9 &= 2 \cdot 9 = 1 \end{aligned}\right\}$$ as on the prev page but now without [ ]

- If p is prime $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is a field

  $\Rightarrow (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ is a group under $\times$

- if $m > 1$ is composite (not prime) $\mathbb{Z}/m\mathbb{Z}$ is a ring but <u>not</u> a field

  m comp $\Rightarrow m = ab \qquad 1 < a, b < m$

  assume for # $\quad a^{-1} \in \mathbb{Z}/m\mathbb{Z}$

  $$\begin{aligned} & m = ab \\ \Rightarrow\ & 0 = ab \quad \text{in } \mathbb{Z}/m\mathbb{Z} \quad 0 = m \\ \Rightarrow\ & a^{-1}0 = a^{-1}ab \\ \Rightarrow\ & 0 = b \\ \#\ & \text{as } \quad 1 < b < m \end{aligned}$$

- Similarly $(\mathbb{Z}/m\mathbb{Z}) \setminus \{0\}$ is not a group

  $ab = m = 0 \notin (\mathbb{Z}/m\mathbb{Z}) \setminus \{0\}$

- However;

  $U_m = \{a \in \mathbb{Z}/m\mathbb{Z} \mid (a, m) = 1\}$

  is a group

- let p be a prime and $a \neq 0$

  $ax \equiv b \bmod p$

  always has a soln.

  $a \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\} \Rightarrow a$ has an inverse a^{-1}

  $\Rightarrow a^{-1} a x \equiv a^{-1} b \bmod p$

  $\Rightarrow x \equiv a^{-1} b \bmod p$

  $\Rightarrow x = [a^{-1}b] = \{a^{-1}b + km \mid k \in \mathbb{Z}\}$ ← ∞ many solns in 1 equiv class

- let $m = ab$ be composite. Can we solve

  $cx \equiv d \bmod m$

  * if $(c,m) = 1$ there is a soln

    $c \in U_m \Rightarrow$ has an inverse c^{-1}

    $\Rightarrow c^{-1} c x \equiv c^{-1} d \bmod m$

    $\Rightarrow x \equiv c^{-1} d \bmod m$

    $\Rightarrow x = [c^{-1}d] = \{\lambda d + mk \mid k \in \mathbb{Z}\}$ ↙ ∞ many solns in 1 equiv class

  * if $(c, m) = t > 1$ there are solns $\Leftrightarrow t \mid d$

    $cx \equiv d \bmod m$ is the same as solving

    $cx - my = d$

    $\Rightarrow x = x_0 + \left(\frac{m}{t}\right)\lambda \quad y = y_0 + \left(\frac{c}{t}\right)\lambda \quad \lambda = 0, 1, \dots t-1$

    (x_0 and y_0 a particular soln)

    $\Rightarrow x = [x_0], [x_0 + (\frac{m}{t})], \dots, [x_0 + (\frac{m}{t})(t-1)]$

    ↖ ∞ many solns in t equiv classes

- $2x \equiv 5 \mod 7$

  7 prime $\Rightarrow$ must be a soln

  Find 2^{-1}

  $2\cdot 1 = 2 \quad 2\cdot 2 = 4 \quad 2\cdot 3 = 6 \quad \underbrace{2\cdot 4 = 8 = 1}_{2^{-1} = 4}$ ← test until we find the inverse

  $\Rightarrow 4\cdot 2x \equiv 4\cdot 5 \mod 7$

  $\Rightarrow x \equiv 20 \equiv 6 \mod 7$

  $\Rightarrow x = [6]$

- $3x \equiv 4 \mod 10$

  $(3, 10) = 1 \Rightarrow$ must be a soln

  Find 3^{-1} in U_m

  $3\cdot 1 = 3 \quad 3\cdot 3 = 9 \quad \underbrace{3\cdot 7 = 21 = 1}_{3^{-1} = 7}$ ← again test but now we only have to search in U_m

  $\Rightarrow 7\cdot 3x \equiv 7\cdot 4 \mod 10$

  $\Rightarrow x \equiv 28 \equiv 8 \mod 10$

  $\Rightarrow x = [8]$

- $10x \equiv 8 \mod 20$

  $(10, 20) = 10, \quad 10 \nmid 8 \Rightarrow$ no solns ← why not check this

- $6x \equiv 8 \mod 20$

  $(6, 20) = 2, \quad 2 \mid 8 \Rightarrow$ must be a soln

  find a particular soln;

  $6\cdot 1 = 6 \quad 6\cdot 2 = 12 \quad 6\cdot 3 = 18 \quad 6\cdot 4 = 24 \equiv 4 \quad 6\cdot 8 = 48 \equiv 8$

  half of 8

  $\Rightarrow x = 8 + \left(\frac{20}{2}\right)\lambda \qquad \lambda = 0, 1$

  $t - 1 = 2 - 1$

  $\Rightarrow x = [8], \left[8 + \frac{20}{2}\right] = [18]$