

Warm-up Problem: The Keystone Kidnapper

There are 7 caskets. The caskets were counted in the following way: casket 1 was 1, casket 2 was 2, and so on until casket 7 which was 7. Then counting backwards: casket 6 was number 8, casket 5 was number 9, and so on until casket 1 which was number 13. Then the count was reversed again, and casket 2 was 14, casket 3 was 15 and so forth; this pattern continued on and on. Which of the seven caskets will be counted as 54321?

Theorem 1: (Division of Integers)

For every pair of integers a and m with $m > 0$ there exist unique integers q and r such that:

$$\begin{aligned}a &= mq + r \\0 \leq r &< m\end{aligned}$$

Example 1: Let $a = -10$ and $m = 3$, then $a = -10 = -4 \cdot 3 + 2 = mq + r$.

Definition 1: The number r in this theorem is called the *remainder* of the division of a by m .

Definition 2: $a \equiv b \pmod{m}$ means: a divided by m has the same remainder as b divided by m . In this case we say " a " is congruent to " b " in mod " m ".

Remark: $0 \equiv m \pmod{m}$, since 0 divided by m has the same remainder as m divided by m .

Remark: In mod m equations, adding, subtracting, and multiplying work the same as with real numbers. In mod m equations we can always reduce to a number r where $0 \leq r < |m|$ before or after adding, subtracting or multiplying.

Example 2: Find the number r where $0 \leq r < 7$ in each of the following:

a) $5 + 12 \equiv r \pmod{7}$

$$5 + 12 \equiv 17 \equiv \boxed{3} \pmod{7}$$

b) $50 + 73 \equiv r \pmod{7}$

$$50 + 73 \equiv 1 + 3 \equiv \boxed{4} \pmod{7}$$

c) $2 - 48 \equiv r \pmod{7}$

$$2 - 48 \equiv 2 - (-1) \equiv \boxed{3} \pmod{7}$$

d) $12 \cdot 16 \equiv r \pmod{7}$

$$12 \cdot 16 \equiv 5 \cdot 2 \equiv 10 \equiv \boxed{3} \pmod{7}$$

e) $701 \cdot 702 \cdot 703 \cdot 704 \equiv r \pmod{7}$

$$701 \cdot 702 \cdot 703 \cdot 704 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \equiv 24 \equiv \boxed{3} \pmod{7}$$

f) $222^{222} \equiv r \pmod{7}$

$$\begin{aligned} 222^{222} &\equiv 5^{222} && | \equiv 5^0 \equiv 5^6 \cdots \equiv 5^{222} \\ &\equiv 5^{222} \pmod{6} && 5 \equiv 5^1 \equiv 5^7 \cdots \equiv 5^{223} \\ &\equiv 5^0 && 4 \equiv 5^2 \equiv 5^8 \cdots \equiv 5^{224} \\ &\equiv \boxed{1} && -1 \equiv 5^3 \equiv 5^9 \cdots \equiv 5^{225} \\ &&& 2 \equiv 5^4 \equiv 5^{10} \cdots \equiv 5^{226} \\ &&& 3 \equiv 5^5 \equiv 5^{11} \cdots \equiv 5^{227} \end{aligned}$$

cycle of 6

Example 3:

If now is X, what time will it be 2500 hours from now?

$$\text{Let } d = \begin{cases} 1 & \text{Spring daylight savings} \\ 0 & \text{No daylight savings} \\ -1 & \text{Fall daylight savings} \end{cases}$$

$$\begin{aligned} X + 2500 + d &\equiv X + d + 2400 + 100 \\ &\equiv X + d + 0 + 4(24) + 4 \\ &\equiv X + d + 0 + 4 \\ &\equiv \boxed{X + d + 4} \pmod{24} \end{aligned}$$

Example 4: When assigning values in mod 7 to days of the week the table below is commonly used:

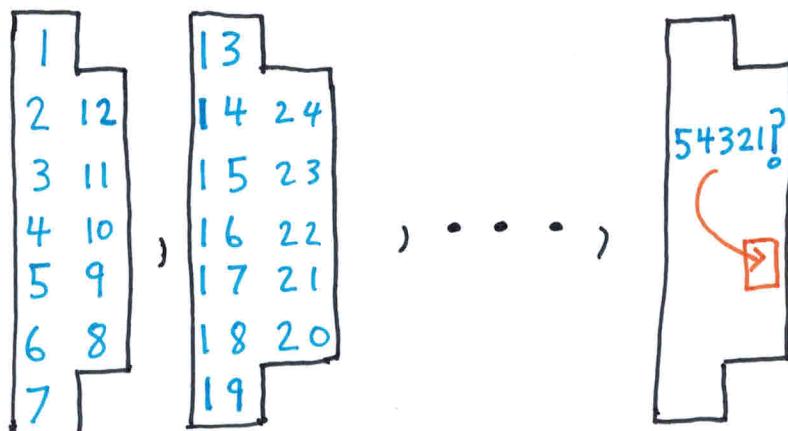
Day of the Week	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Mod 7	0	1	2	3	4	5	6

In the current year, using the conversion from the above table, Valentine's Day lands on the X^{+b} day of the week. What day will Valentine's Day be in the year 2026?

$$\begin{aligned} \text{"# of years"} &= 2026 - \text{"current year"} \\ x + (\# \text{ of years}) 365 + (\# \text{ of leap years}) \\ &\equiv [x + (\# \text{ of years}) + (\# \text{ of leap years})] \pmod{7} \end{aligned}$$

(Note: $365 \equiv 1 \pmod{7}$)

Example 5: Find a solution to the keystone kidnapper problem.

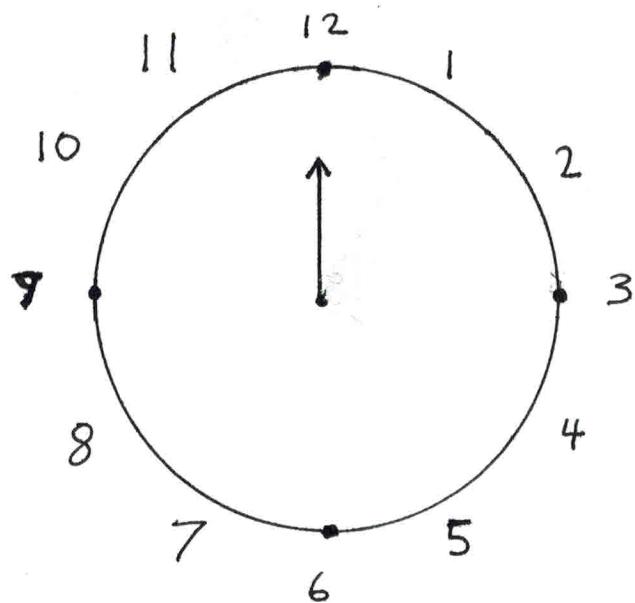


$$\begin{array}{r} 4526 \\ 12 \overline{)54321} \\ -48 \\ \hline 63 \\ -60 \\ \hline 32 \\ -24 \\ \hline 81 \\ -72 \\ \hline 9 \end{array}$$

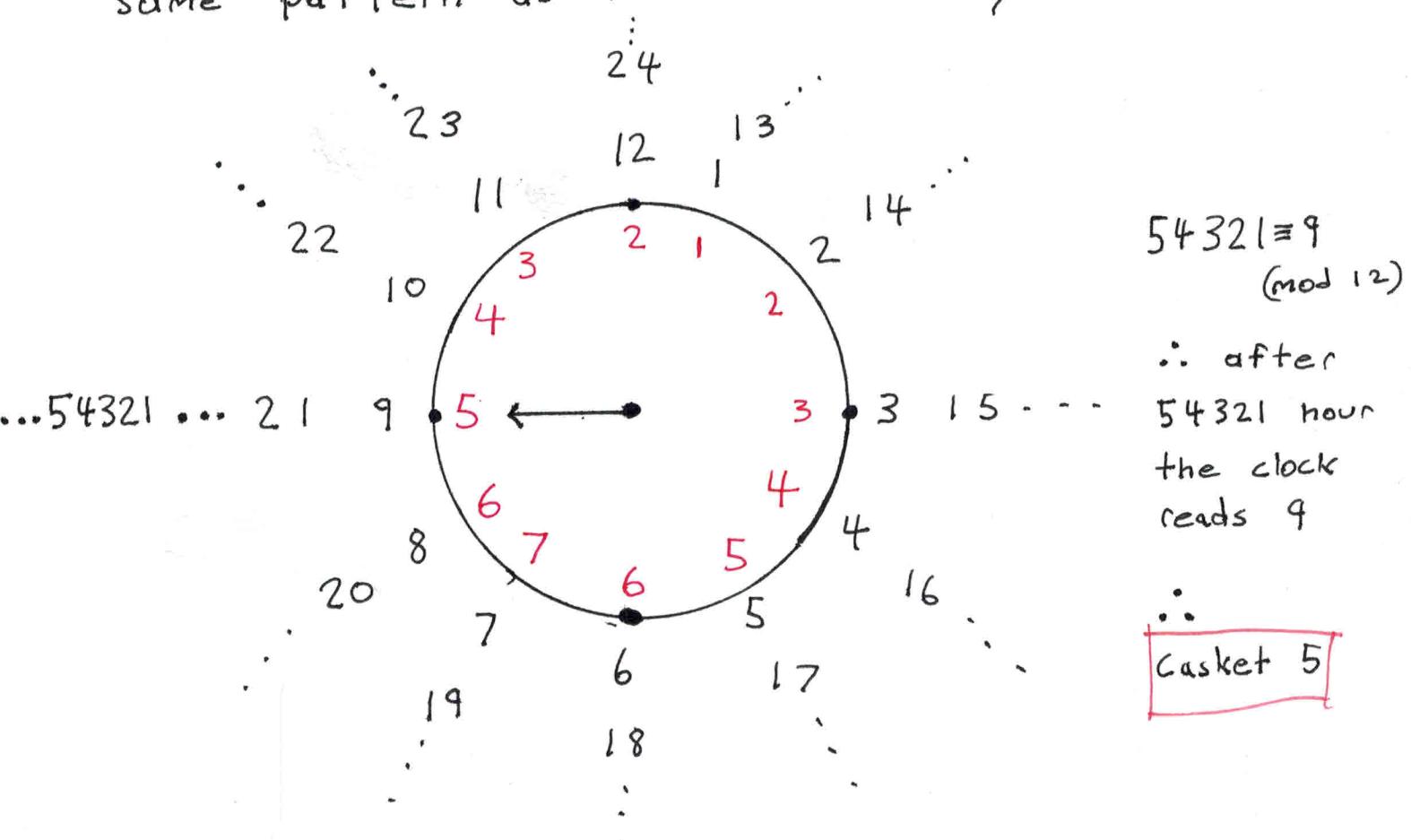
$$\begin{aligned} \therefore 54321 &\equiv 9 \pmod{12} \\ \therefore \boxed{\text{Casket 5}} \end{aligned}$$

Another explanation:

Start with a clock:



Notice the caskets are counted with the
same pattern as hours of a day:



Remark: Although division is defined on the non-zero integers it does not make sense to have a fraction in modular arithmetic congruencies. Instead of dividing; solve the following congruence:

$$3x \equiv 2 \pmod{7}$$

by multiplying both sides by an integer that isolates x . This motivates the following definition.

Definition 3: Two integers a and b are said to be *multiplicative inverses* of each other in mod m if

$$a \cdot b \equiv 1 \pmod{m}.$$

Example 6: Find the multiplicative inverse for 1, 2, 3 and 6 in mod 7.

$$1 \cdot 1 \equiv 1 \quad 2 \cdot 4 \equiv 1 \quad 3 \cdot 5 \equiv 1 \quad 6 \cdot 6 \equiv 1 \pmod{7}$$

Example 7: Solve for x :

$$3 \cdot (x - 2) \equiv -4 \pmod{7}$$

$$\Rightarrow 3x - 6 \equiv -4$$

$$\Rightarrow 3x \equiv 2$$

$$\Rightarrow (5)3x \equiv (5)2$$

$$\Rightarrow x \equiv 10 \equiv 3 \pmod{7}$$

Definition 4: Two integers a and b are said to be *relatively prime* (or "r.p." for short) if they have no common positive factor other than 1.

Theorem 2: (Multiplicative Inverses in mod m)

$$a \text{ is relatively prime with } m \iff a \text{ has an inverse in mod } m.$$

Example 8: In mod 26 the only elements with multiplicative inverses are:

$$1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$$

Theorem 3: (Cancellation Law)

If $a \cdot c \equiv b \cdot c \pmod{m}$ and c is relatively prime with m $\implies a \equiv b \pmod{m}$.

Example 9: Can the common number on each of the congruence be cancelled?

- a) $1 \cdot 2 \equiv 4 \cdot 2 \pmod{2}$ No 2 is not r.p. with 2 Note: $1 \not\equiv 4 \pmod{2}$
- b) $1 \cdot 3 \equiv 7 \cdot 3 \pmod{2}$ Yes 3 is r.p. with 2 Note: $1 \equiv 7 \pmod{2}$

Example 10:

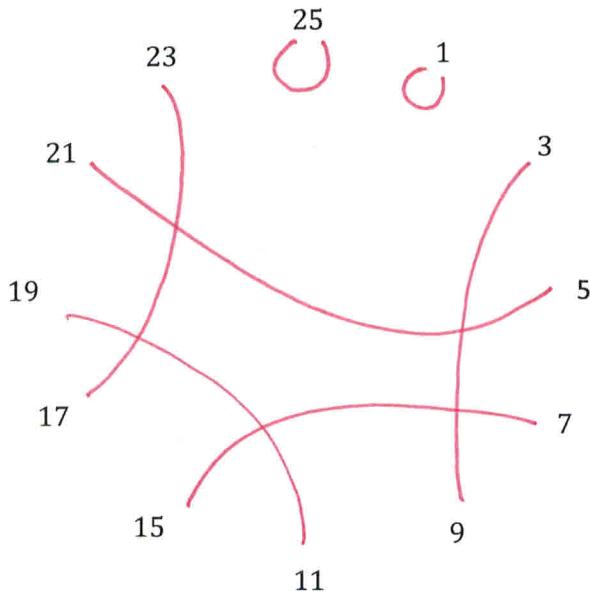
- a) Show that the pair a, b in definition 3 is unique in mod m .

$$\text{Let } ab \equiv 1 \pmod{m} \quad \& \quad ab' \equiv 1 \pmod{m}$$

$$\Rightarrow ab \equiv ab' \pmod{m}$$

$$\Rightarrow b \equiv b' \pmod{m} \quad (\text{by Thrm. 2 \& 3})$$

- b) Draw a line between each unique pair of multiplicative inverses in mod 26.



$$| \equiv 27 \equiv 3 \cdot 9 \equiv (-3)(-9) \equiv 23 \cdot 17$$

$$\equiv 53$$

$$\equiv 79$$

$$\equiv 105 \equiv 3 \cdot 5 \cdot 7 \equiv 5 \cdot 21$$

$$\equiv 7 \cdot 15$$

$$\equiv (-7)(-15)$$

$$\equiv 19 \cdot 11$$

- c) Solve for x : $y \equiv 7x + 6 \pmod{26}$.

$$\Rightarrow (15)y \equiv 15 \cdot 7x + 15 \cdot 6 \pmod{26}$$

$$\Rightarrow 15y \equiv x + 90 \equiv x + 12 \pmod{26}$$

$$\Rightarrow \boxed{x \equiv 15y - 12} \pmod{26}$$