There are certain things whose number is unknown.
If we count them by 3s, we have 2 left over.
If we count them by 5s, we have 3 left over.
How many things are there?

$$\{x \in \mathbb{Z} \mid x \equiv 2 \bmod 3,\ x \equiv 3 \bmod 5\}$$

$$x \equiv 2 \bmod 3 \rightsquigarrow x = 3y + 2 \quad ①$$

$$x \equiv 3 \bmod 5 \rightsquigarrow x = 5z + 3 \quad ②$$

$$\Rightarrow 3y - 5z = 1 \quad (*)$$

We know that: solutions of (*) are $\begin{cases} y = 2 + 5m \\ z = 1 + 3m \end{cases}$

Plug in ① & ②, we get

$x = 3(2+5m) + 2$
$= 5(1+3m) + 3$

$$x = 15m + 8$$

$$\Leftrightarrow \quad x \equiv 8 \bmod 15$$

That is the answer.

$$\{ x \in \mathbb{Z} \mid x \equiv 2 \bmod 3,\ x \equiv 3 \bmod 5 \}$$

$$= \{ x \in \mathbb{Z} \mid x \equiv 8 \bmod 15 \}$$

Theorem (Chinese Remainder Theorem)

Let m and n be two moduli and assume they are coprime.

Then there is a bijection

$$\left\{(a,b) \in \mathbb{Z}^2 \,\middle|\, \begin{array}{l} 0 \leq a \leq m-1 \\ 0 \leq b \leq n-1 \end{array}\right\} \xrightarrow{f} \left\{ c \in \mathbb{Z} \,\middle|\, 0 \leq c \leq m \cdot n - 1 \right\}$$

Such that :

Solutions of $\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$ are exactly

Solutions of $x \equiv c \bmod mn$ whenever $f(a,b) = c$.

Proof: suppose we have $\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$ (*)

Then there are $y, z \in \mathbb{Z}$ s.t. $\begin{cases} x = a + my \\ x = b + nz \end{cases}$

So we have $my - nz = b - a$ (*) $\rightsquigarrow a + my_0 = b + nz_0$

Since GCD$(m, n) = 1$, we can use Euclidean Algorithm to find a specific solution (y_0, z_0) of (*).

Then the general solution of (*) is

$$\begin{cases} y = y_0 + n \cdot t \\ z = z_0 + m \cdot t \end{cases}$$

$x = a + m(y_0 + n \cdot t)$
$= a + my_0 + mn \cdot t$

$x = b + n(z_0 + n \cdot t)$
$= b + nz_0 + mn \cdot t$

Hence, for x to be a solution of (☆), we must have

$$x \equiv c \mod mn, \quad (▲)$$

where c is the natural rep. of $a + my_0$ (which $= b + nz_0$) modulo mn.

One can verify that any solution of (▲) is a solution of (☆).

Hence, we have an algorithm to compute c from a, b.

In particular, we have a function f.

To see f is bijective, consider

$$g: c \longmapsto (\text{nat. rep. of } c \bmod m, \text{ nat. rep. of } c \bmod n)$$

One can verify that g is the inverse of f.

More than two congruences? (Inductive construction)

There are certain things whose number is unknown.
If we count them by 3s, we have 2 left over.
If we count them by 5s, we have 3 left over.
If we count them by 7s, we have 2 left over.
How many things are there?

$$\{x \in \mathbb{Z} \mid x \equiv 2 \bmod 3,\ x \equiv 3 \bmod 5,\ x \equiv 2 \bmod 7\}$$

$$\left.\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 3 \bmod 5 \end{aligned}\right\} \rightsquigarrow x \equiv 8 \bmod 15$$

$$\left.\begin{aligned} x &\equiv 8 \bmod 15 \\ x &\equiv 5 \bmod 7 \end{aligned}\right\} \rightsquigarrow x \equiv 23 \bmod 105$$

Another method (Direct construction)

The original answer:

count them by 3s, left over 2 ⇝ 140 ??

count them by 5s, left over 3 ⇝ 63 ??

count them by 7s, left over 2 ⇝ 30 ??

$$
\begin{aligned}
140 &= \boxed{2 \cdot} \; 2 \cdot 5 \cdot 7 \\
63 &= \boxed{1 \cdot} \; 3 \cdot 3 \cdot 7 \\
30 &= \boxed{1 \cdot} \; 2 \cdot 3 \cdot 5
\end{aligned}
$$

remainder

other moduli

$$
\begin{aligned}
\boxed{2 \cdot} \; 5 \cdot 7 - 23 \cdot 3 &= 1 \\
\boxed{1 \cdot} \; 3 \cdot 7 - 4 \cdot 5 &= 1 \\
\boxed{1 \cdot} \; 3 \cdot 5 - 2 \cdot 7 &= 1
\end{aligned}
$$

Bézout Identity

Theorem (Chinese Remainder Theorem) general version

Let m_i $(i \in I)$ be some moduli and assume they are coprime.

Then there is a bijection

$$M = \prod_{i \in I} m_i$$

$$\left\{ (a_i)_{i \in I} \in \mathbb{Z}^I \;\middle|\; \underset{\forall i \in I}{0 \le a_i \le m_i - 1} \right\} \xrightarrow{f} \left\{ A \in \mathbb{Z} \;\middle|\; 0 \le A \le M - 1 \right\}$$

such that

Solutions of $x \equiv a_i \bmod m_i$ $(i \in I)$

are exactly

Solutions of $x \equiv A \bmod M$ whenever $f((a_i)_I) = A$.

Construction of f: $M = \prod_{i \in I} m_i$ $\quad M_i$ = prod of m_j other than m_i

Let M_i be M/m_i. Then M_i & m_i are coprime.

By Bézout's Identity, there exist integers N_i & n_i, s.t.

$$M_i N_i + m_i n_i = 1.$$

Let A be the natural rep. of $\sum_{i \in I} a_i M_i N_i$ modulo M.

Then for any $x \equiv A \bmod M$, we have

$$x \equiv a_i M_i N_i \equiv a_i (1 - m_i n_i) \equiv a_i \bmod m_i$$

- $x \equiv a_i M_i N_i$: if $j \neq i$, then $m_i \mid M_j$ $\Rightarrow m_i \mid a_j M_j N_j$
- $a_i M_i N_i \equiv a_i (1 - m_i n_i)$: $M_i N_i + m_i n_i = 1$
- $a_i (1 - m_i n_i) \equiv a_i$: $m_i \mid \cdots$

for all $i \in I$.

One can thus verify $f((a_i)_I) = A$ works.

17

Theorem (Chinese Remainder Theorem) Abstract Version.

Let m_i $(i \in I)$ be some moduli and assume they are coprime.

Then there is an "isomorphism" (bijection + preserving operations) $M = \prod_{i \in I} m_i$

$$\mathbb{Z}/M \xrightarrow{P.} \prod_{i \in I} \mathbb{Z}/m_i = \left\{ (a_i)_{i \in I} \;\middle|\; a_i \in \mathbb{Z}/m_i \right\}$$

Proof: In fact, $P.$ is

$$[a]_M \longmapsto ([a]_{m_i})_{i \in I}$$

operations are defined componentwise

$$(a_i)_{i \in I} + (\beta_i)_{i \in I} := (a_i + \beta_i)_{i \in I}$$

$$(a_i)_{i \in I} \cdot (\beta_i)_{i \in I} := (a_i \beta_i)_{i \in I}$$

$0 := (0)_{i \in I}$ neutral

$1 := (1)_{i \in I}$ identity

Need to show:

i) $P.$ preserves operations.

ii) $P.$ is injective.

iii) $P.$ is bijective.

i) P. preserves operations.

Lemma. If $n \mid m$, then the natural map

$$\mathbb{Z}/m \longrightarrow \mathbb{Z}/n \quad : \quad [a]_m \longmapsto [a]_n$$

preserves operations.

Proof. $[0]_m \longmapsto [0]_n$ neutral to neutral

$[1]_m \longmapsto [1]_n$ identity to identity

$$\begin{array}{ccc} [a]_m + [b]_m & & [a]_n + [b]_n \\ \| & & \| \\ [a+b]_m & \longmapsto & [a+b]_n \end{array}$$

sum to sum

$$\begin{array}{ccc} [a]_m \cdot [b]_m & & [a]_n \cdot [b]_n \\ \| & & \| \\ [a \cdot b]_m & \longmapsto & [a \cdot b]_n \end{array}$$

product to product

By the lemma,

$P_i : \mathbb{Z}/M \longrightarrow \mathbb{Z}/m_i : [a]_M \longmapsto [a]_{m_i}$ preserves operations.

The map $P_\bullet$ is $a \longmapsto (P_i(a))_{i\in I}$.

Lemma. If we have $g_i : R \longrightarrow R_i$ $(i\in I)$, each preserves operations

then so is the map $g_\bullet : R \longrightarrow \prod_{i\in I} R_i$ given by

$$a \longmapsto (g_i(a))_{i\in I}$$

Proof. $g_\bullet(0) = (g_i(0))_{i\in I} = (0)_{i\in I} =: 0$ in $\prod_{i\in I} R_i$

$g_\bullet(1) = (g_i(1))_{i\in I} = (1)_{i\in I} =: 1$ in $\prod_{i\in I} R_i$ $\quad g_\bullet(\alpha) + g_\bullet(\beta)$

$g_\bullet(\alpha+\beta) = (g_i(\alpha+\beta))_{i\in I} = (g_i(\alpha) + g_i(\beta))_{i\in I} =: (g_i(\alpha))_{i\in I} + (g_i(\beta))_{i\in I}$

$g_\bullet(\alpha\cdot\beta) = (g_i(\alpha\cdot\beta))_{i\in I} = (g_i(\alpha)\cdot g_i(\beta))_{i\in I} =: (g_i(\alpha))_{i\in I} \cdot (g_i(\beta))_{i\in I}$

$g_\bullet(\alpha)$ $\quad g_\bullet(\beta)$

ii) $P_\cdot$ is injective.

Lemma: $P_\cdot^{-1}(0) = [0]_M$ (0 is the neutral in $\prod_{i\in I} \mathbb{Z}/m_i$, namely, $([0]_{m_i})_{i\in I}$)

Namely, $x \equiv 0 \bmod m_i$ for all $i\in I$ $\Leftrightarrow$ $x \equiv 0 \bmod M$.

Proof: LHS means $m_i \mid x$ for all $i\in I$

We know this is eq to $\underset{i\in I}{\mathrm{LCM}}(m_i) \mid x$ (Recall: def prop of LCM)

But since m_i are coprime, $\underset{i\in I}{\mathrm{LCM}}(m_i) = \prod_{i\in I} m_i = M$. ∎

Take $a, b \in \mathbb{Z}$, if $P_\cdot([a]_M) = P_\cdot([b]_M)$, then

$$0 = P_\cdot([a]_M) - P_\cdot([b]_M) = P_\cdot([a]_M - [b]_M) = P_\cdot([a-b]_M)$$

By the lemma, $[a-b]_M = [0]_M$ namely $[a]_M = [b]_M$. ∎

iii) bijective: Since both side have the same size: $\#(\cdots) = M$.

Coro. φ is multiplicative

Proof: The isomorphism $\mathbb{Z}/_{mn} \xrightarrow{\text{P.}} \mathbb{Z}/_{m} \times \mathbb{Z}/_{n}$ (where m, n are coprime)

induces an isomorphism $\mathbb{Z}_{mn}^{*} \longrightarrow \mathbb{Z}_{m}^{*} \times \mathbb{Z}_{n}^{*}$.

Why? Only need to verify:

For any $a \in \mathbb{Z}_{mn}^{*}$, the natural rep of a modulo m (resp. modulo n) is multiplicatively invertible, i.e. $\in \mathbb{Z}_{m}^{*}$ (resp. $\mathbb{Z}_{n}^{*}$)

Proof. take $b \in \mathbb{Z}_{mn}^{*}$ s.t. $ab \equiv 1 \bmod mn$.

Then $ab \equiv 1 \bmod m$ (and $\bmod n$)

Hence a, as well as its nat. rep. is invertible mod m (and mod n)