x: # of bananas

Suppose we have a basket full of bananas.
1. When we distribute the bananas to 3 monkeys, we have 2 bananas remaining.
2. When we distribute the bananas to 7 monkeys, we have 4 bananas remaining.
3. When we distribute the bananas to 11 monkeys, we have 3 bananas remaining.

① $x \equiv 2 \mod 3$

② $x \equiv 4 \mod 7$

③ $x \equiv 3 \mod 11$

pairwise relatively prime?

YES

$3 \cdot 7 \cdot 11 = 231$

Sunzi's Remainder Theorem
(Chinese Remainder Theorem)

In a series of congruences where all moduli are pairwise relatively prime, there is a unique sol'n $x \in \mathbb{Z}_{m_1 \cdot m_2 \cdots m_k}$

Recall: $x \equiv b \pmod{n} \iff x = nq + b$

Ex. Solve the system of congruences above

① $x \equiv 2 \mod 3 \rightarrow \underbrace{x = 3s + 2}$

sub. into ②

$3s + 2 \equiv 4 \pmod 7$

$3s \equiv 2 \pmod 7$ $\qquad 3 \cdot 3^{-1} \equiv 1 \pmod 7$

$\underbrace{3^{-1} \cdot 3} \cdot s \equiv 3^{-1} \cdot 2 \pmod 7$ $\qquad 5$

$s \equiv 10 \pmod 7$

$s \equiv 3 \pmod 7$

$s = 7t + 3$

(Notice: $x \equiv 11 \pmod{21}$)

$$x = 3(7t+3)+2 = 21t+11$$

③

$$21t+11 \equiv 3 \pmod{11}$$

$$21t \equiv 3 \pmod{11}$$

$$10t \equiv 3 \pmod{11}$$

$$10^{-1} \equiv 10 \pmod{11}$$

$$t \equiv 30 \pmod{11}$$

$$t \equiv 8 \pmod{11}$$

$$t = 11u + 8$$

$$x = 21(11u+8)+11$$

$$x = 231u + 179$$

$$\therefore x \equiv 179 \pmod{231}$$

$$x = 179, 410, 641, \ldots$$

In theory: There are infinitely many solutions that we can obtain by adding or subtracting multiples of 231.

In practice: There may be practical constraints that dictate the realistic range of the solution. For example, one cannot have a negative number of bananas. Or perhaps our basket is only big enough to hold up to 500 bananas. So in that case our only feasible solutions for this example might be 179 or 410.

Group theory

Def'n A binary operation $*$ on a set A takes two inputs $a, b \in A$ and outputs $a * b = c$. We say that $*$ is closed under A iff $c \in A$.

Ex. Notice, for $A = \{1, 2, 3\}$, $+$ is NOT closed on the set A.

If $A = \mathbb{R}$, then $+$ is closed on A.

Def'n A group is a set G along w/ an operation $*$ denoted as $(G, *)$ w/ the following properties:

1. G is closed under $*$
2. There exists an identity element $e \in G$
3. For every $g \in G$, there exists $g^{-1} \in G$
4. $*$ is associative on G

Def'n A group $(G, *)$ is abelian if it is commutative, i.e., when $a * b = b * a$

Note: Matrix multiplication is <u>NOT</u> commutative

<u>Ex.</u> Prove that $(\mathbb{Z}_n, \oplus)$ is a group

① Closure: Let $a, b \in \mathbb{Z}_n$

Consider $a+b \pmod{n}$

If $a+b < n$, then $a \oplus b \in \mathbb{Z}_n$

If $a+b \geq n$, then $a+b \equiv a+b-n \pmod{n}$

So, $0 \leq a+b-n < n$

then by def'n, $a+b-n \in \mathbb{Z}_n$

$\Rightarrow a \oplus b \in \mathbb{Z}_n$