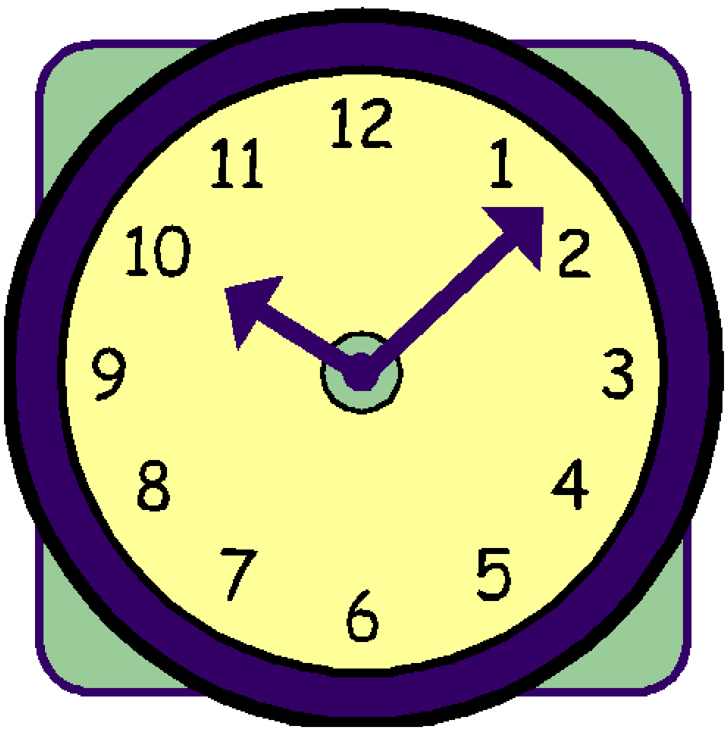
Modular Arithmetic, Chinese Remainder Theorem



Plan

In this note, we shall study some more elementary number theory.

These basics of number theory are very powerful tools in computer science.

- Modular arithmetic
  - Modular addition, multiplication
  - Applications
  - Multiplicative inverses
  - Fermat's little theorem, Wilson's theorem
- Chinese remainder theorem

12-hour clock

But this could be also 6 o'clock in the morning, when we should have breakfast.

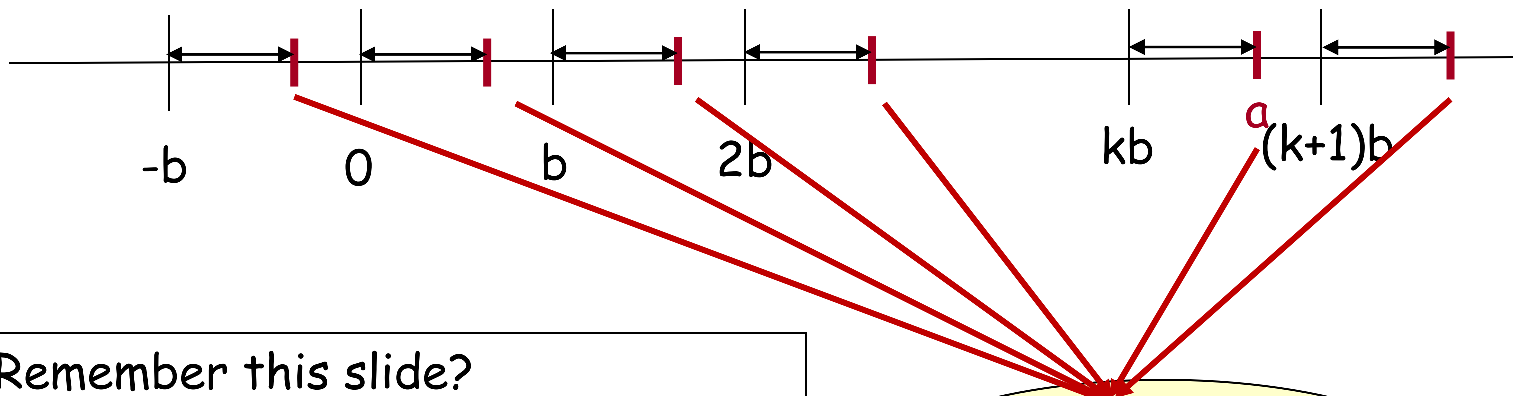
In this case, we actually view two 6 o'clocks as one single value in a clock.

This is the idea of modular arithmetic!

Partition of Integers

Given any b>0, we can partition the integers into blocks of b numbers.

For any a, there is a unique "position" for this number.



Congruence class of a modulo b:

$[a]_b = \{a+kb \mid k \in \mathbb{Z}\}$

Remember this slide?

Grouping the integers that are in the same "position" of each b-block forms a partition of integers.

E.g. $\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3.$

Denoted by $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$

Modular Arithmetic

Defintion $a \equiv b \pmod{n}$ iff $n | (a - b)$.

e.g. $12 \equiv 2 \pmod{10}$

$107 \equiv 207 \pmod{10}$

$7 \equiv 1 \pmod{2}$

$1 \equiv -1 \pmod{2}$

$13 \equiv -1 \pmod{7}$

$-15 \equiv 0 \pmod{5}$

Modular Addition

Lemma. If $a \equiv c \pmod{n}$, and $b \equiv d \pmod{n}$ then

$$a+b \equiv c+d \pmod{n}.$$

Example 1 $12 \equiv 2 \pmod{10}$, $25 \equiv 5 \pmod{10}$

=> $12 + 25 \pmod{10}$

$\equiv 2 + 5 \pmod{10} \equiv 7 \pmod{10}$

Example 2 $87 \equiv 2 \pmod{17}$, $222 \equiv 1 \pmod{17}$

=> $87 + 222 \pmod{17}$

$\equiv 2 + 1 \pmod{17}$

$\equiv 3 \pmod{17}$

Example 3 $101 \equiv 2 \pmod{11}$, $141 \equiv -2 \pmod{11}$

=> $101 + 141 \pmod{11} \equiv 0 \pmod{11}$

Modular Addition

Lemma: If $a \equiv c \pmod{n}$, and $b \equiv d \pmod{n}$ then

$a+b \equiv c+d \pmod{n}$.

Proof

$a \equiv c \pmod{n} \;\Rightarrow\; a = c + nx$ for some integer x

$b \equiv d \pmod{n} \;\Rightarrow\; b = d + ny$ for some integer y

To show $a+b \equiv c+d \pmod{n}$, it is equivalent to showing that $n \mid (a+b-c-d)$.

Consider $a+b-c-d$.

$a+b-c-d = (c+nx) + (d+ny) - c - d = nx + ny$.

It is clear that $n \mid nx + ny$.

Therefore, $n \mid a+b-c-d$.

We conclude that $a+b \equiv c+d \pmod{n}$.

Modular Multiplication

Lemma. If $a \equiv c \pmod{n}$, and $b \equiv d \pmod{n}$ then

$$ab \equiv cd \pmod{n}.$$

Example 1

$9876 \equiv 6 \pmod{10}$, $17642 \equiv 2 \pmod{10}$

=> $9876 * 17642 \pmod{10}$

$\equiv 6 * 2 \pmod{10}$

$\equiv 2 \pmod{10}$

Example 2

$10987 \equiv 1 \pmod{2}$, $28663 \equiv 1 \pmod{2}$

=> $10987 * 28663 \pmod{2} \equiv 1 \pmod{2}$

Example 3

$999 \equiv 5 \pmod{7}$, $674 \equiv 2 \pmod{7}$

=> $999 * 674 \pmod{7} \equiv 5 * 2 \pmod{7} \equiv 3 \pmod{7}$

Modular Multiplication

Lemma: If $a \equiv c \pmod{n}$, and $b \equiv d \pmod{n}$ then

$ab \equiv cd \pmod{n}$.

<u>Proof</u>

$a \equiv c \pmod{n}$ => $a = c + nx$ for some integer x

$b \equiv d \pmod{n}$ => $b = d + ny$ for some integer y

To show $ab \equiv cd \pmod{n}$, it is equivalent to showing that $n \mid (ab-cd)$.

Consider $ab-cd$.

$ab-cd = (c+nx)(d+ny) - cd$

$= cd + dnx + cny + n^2xy - cd = n(dx + cy + nxy)$.

It is clear that $n \mid n(dx + cy + nxy)$. Therefore, $n \mid ab-cd$.

We conclude that $ab \equiv cd \pmod{n}$.

Exercise

$144^4 \pmod{713}$

$= 144 * 144 * 144 * 144 \pmod{713}$

$= 20736 * 144 * 144 \pmod{713}$ ⟶ $20736 * 20736 \pmod{713}$

$= 59 * 144 * 144 \pmod{713}$

$= 8496 * 144 \pmod{713}$

$= 653 * 144 \pmod{713}$

$= 94032 \pmod{713}$

$= 629 \pmod{713}$

$20736 * 20736 \pmod{713}$

$= 59 * 59 \pmod{713}$

$= 3481 \pmod{713}$

$= 629 \pmod{713}$

Make a smart use of the modular arithmetic will significantly reduce the complexity!

Plan

- Modular arithmetic
  - Modular addition, multiplication
  - Applications
  - Multiplicative inverses
  - Fermat's little theorem, Wilson's theorem
- Chinese remainder theorem

Application

A number is divisible by 9 if and only if
the sum of its digits is divisible by 9?

Example 1. 9333234513171 is divisible by 9.

9+3+3+3+2+3+4+5+1+3+1+7+1 = 45 is divisible by 9.

Example 2. 128573649683 is not divisible by 9.

1+2+8+5+7+3+6+4+9+6+8+3 = 62 is not divisible by 9.

A coincidence? NO

This can be proved easily using modular arithmetic.

Application

Claim. A number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Hint: $10 \equiv 1 \pmod 9$.

Let the decimal representation of n be $d_k d_{k-1} d_{k-2} \ldots d_1 d_0$.

This means that $n = d_k 10^k + d_{k-1} 10^{k-1} + \ldots + d_1 10 + d_0$

Note that $d_i 10^i \bmod 9$

$$\equiv (d_i \bmod 9)\,(10^i \bmod 9) \bmod 9$$

$$\equiv (d_i \bmod 9)\,\underbrace{(10 \bmod 9)\,(10 \bmod 9) \ldots (10 \bmod 9)}_{\text{i terms}} \bmod 9$$

$$\equiv (d_i \bmod 9)\,(1 \bmod 9)\,(1 \bmod 9) \ldots (1 \bmod 9) \bmod 9$$

$$\equiv d_i \bmod 9$$

Application

Claim. A number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Hint: $10 \equiv 1 \pmod 9$.

Let the decimal representation of n be $d_k d_{k-1} d_{k-2} \ldots d_1 d_0$.

This means that $n = d_k 10^k + d_{k-1} 10^{k-1} + \ldots + d_1 10 + d_0$

Note that $d_i 10^i \bmod 9 \equiv d_i \bmod 9$.

$$
\begin{aligned}
\text{Hence } n \bmod 9 &\equiv (d_k 10^k + d_{k-1} 10^{k-1} + \ldots + d_1 10 + d_0) \bmod 9 \\
&\equiv (d_k 10^k \bmod 9 + d_{k-1} 10^{k-1} \bmod 9 + \ldots + d_1 10 \bmod 9 + d_0 \bmod 9) \bmod 9 \\
&\equiv (d_k \bmod 9 + d_{k-1} \bmod 9 + \ldots + d_1 \bmod 9 + d_0 \bmod 9) \bmod 9 \\
&\equiv (d_k + d_{k-1} + \ldots + d_1 + d_0) \bmod 9
\end{aligned}
$$

Fifteen Puzzle

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Rule: can move a numbered square to the empty one when they are adjacent.

Fifteen Puzzle

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Initial configuration

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Target configuration

Is there a sequence of moves that allows you to change the initial configuration to the target configuration?

Invariant Method

1. Find properties (the **invariants**) that are satisfied throughout the whole process.
2. Show that the target do not satisfy the properties.
3. Conclude that the target is not achievable.

What is the invariant in this game??

This is usually the hardest part of the proof.

Hint

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Initial configuration

((1,2,3,....,14,15),(4,4))

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Target configuration

((1,2,3,....,15,14),(4,4))

Hint: the two states have different parity.

Parity

Given a sequence, a pair is "disorder" if the first element is larger.

More formally, given a sequence $(a_1, a_2, \ldots, a_n)$,
a pair (i,j) is disorder if $i<j$ but $a_i > a_j$.

For example, the sequence (1,2,4,5,3) has two disorder pairs, (4,3) and (5,3).

Given a state $S = ((a_1, a_2, \ldots, a_{15}), (i,j))$

Parity of S = (number of disorder pairs + i) mod 2

row number of the empty square

Hint

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Initial configuration

((1,2,3,...,14,15),(4,4))

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Target configuration

((1,2,3,...,15,14),(4,4))

Parity of S = (number of disorder pairs + i) mod 2

Clearly, the two states have different parity.

Invariant Method

Parity is even

1. Find properties (the **invariants**) that are satisfied throughout the whole process.
2. Show that the target do not satisfy the properties.
3. Conclude that the target is not achievable.

Parity is odd

Invariant = parity of state

Claim. Any move will preserve the parity of state.

Proving the claim will finish the infeasibility proof.

Proving the Invariant

Parity of S = (number of disorder pairs + i) mod 2

Claim. Any move will preserve the parity of state.

?	?	?	?
?	a		?
?	?	?	?
?	?	?	?

$\Rightarrow$

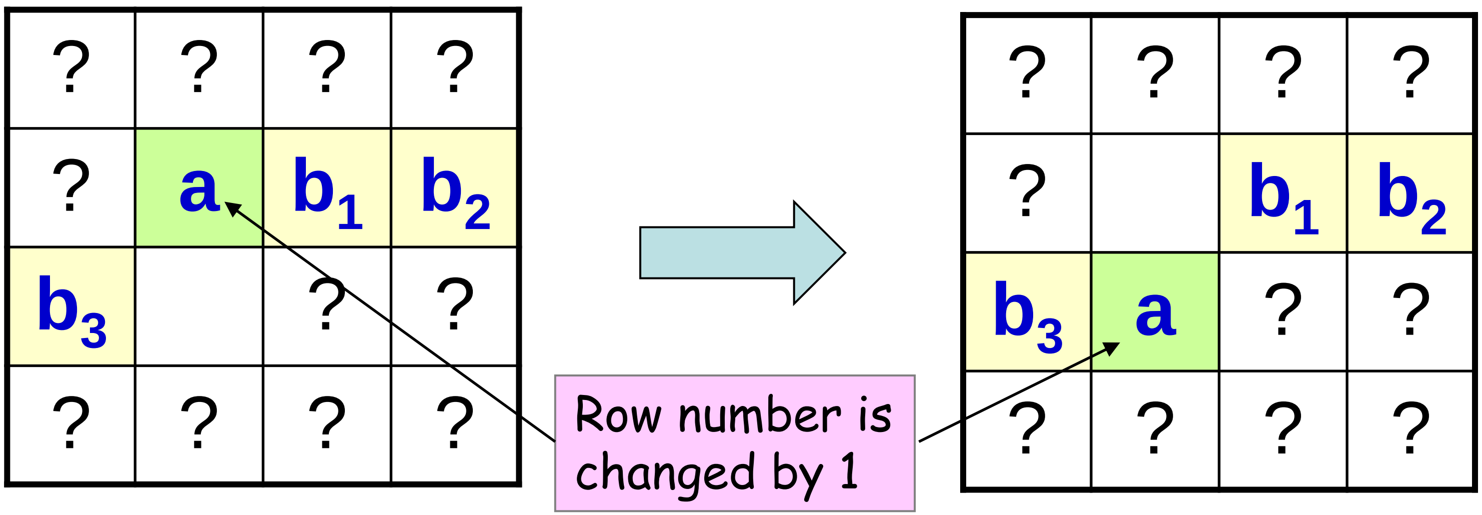
?	?	?	?
?		a	?
?	?	?	?
?	?	?	?

Horizontal movement does not change anything…

Proving the Invariant

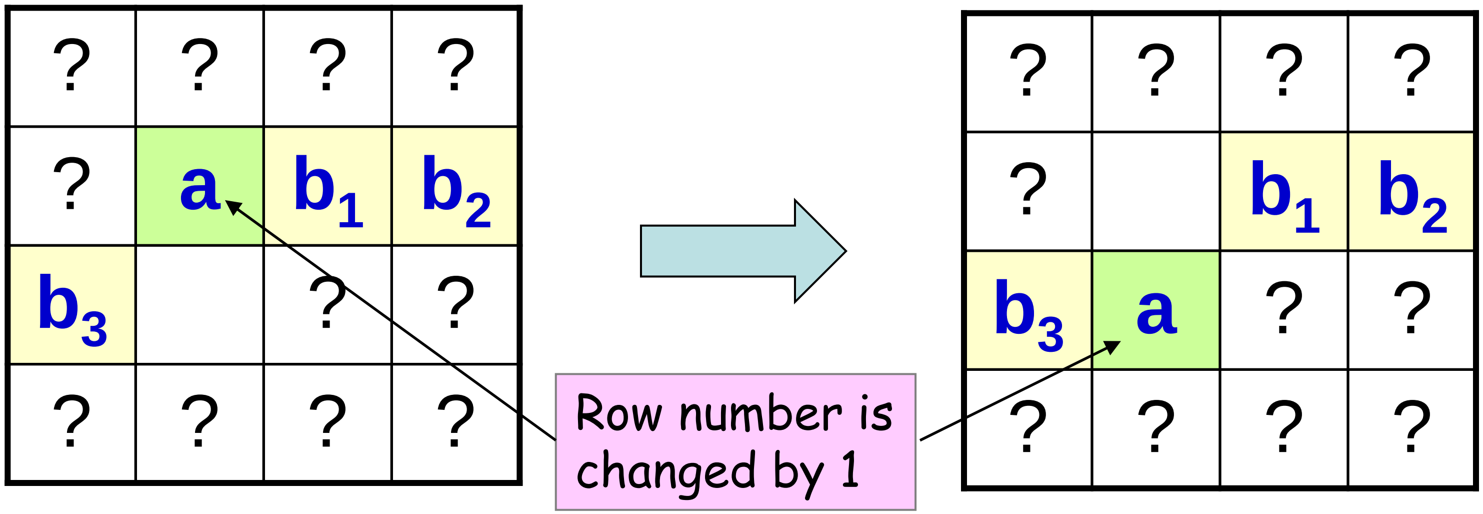
Parity of S = (number of disorder pairs + i) mod 2

Claim. Any move will preserve the parity of state.



To count the *change* on **#disorder pairs**, we need to discuss 4 cases, depending on the relative order of **a** among {a, b_1, b_2, b_3}.

Proving the Invariant



① If a is the largest, then the **#disorder pairs** will decrease by three.

② If a is the second largest, then **#disorder pairs** will decrease by one.

③ If a is the second smallest, then **#disorder pairs** will increase by one.

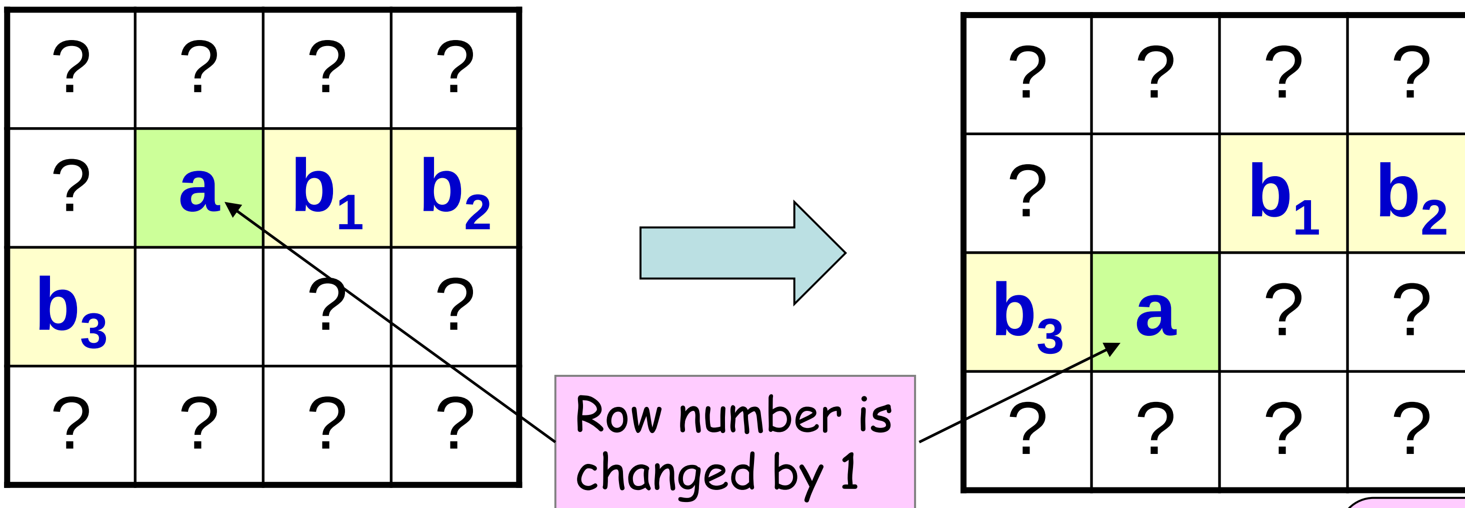
④ If a is the smallest, then **#disorder pairs** will increase by three.

In summary, the change on **#disorder pairs** is either 1 or 3.

Proving the Invariant

Parity of S = (number of disorder pairs + i) mod 2

Claim. Any move will preserve the parity of state.



If there are 3/2/1/0 disorder pairs in the current state, there will be 0/1/2/3 disorder pairs in the next state.

Difference is 1 or 3.

So the parity stays the same! We've proved the claim.

Fifteen Puzzle

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Initial configuration

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Target configuration

Is there a sequence of moves that allows you to change the initial configuration to the target configuration?

Fifteen Puzzle

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Initial configuration

15	14	13	12
11	10	9	8
7	6	5	4
3	2	1	

Target configuration

#disorder pairs = 0

Row of empty square = 4

Parity is even.

#disorder pairs
= 14 + 13 + 12 + … + 1
= (14+1)·14/2 = 105

Row of empty square = 4

Parity is odd.

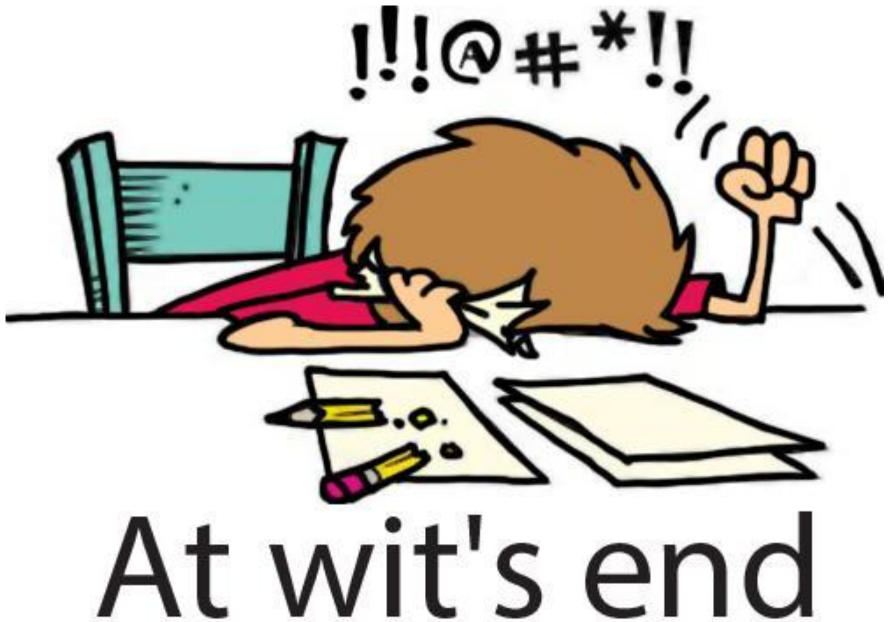
Impossible!

Fifteen Puzzle

If two configurations have the same parity, is it true that we can always move from one to the other?

YES!

The solution however requires considerably more sophisticated mathematics.



Plan

- Modular arithmetic
  - Modular addition, multiplication
  - Applications
  - Multiplicative inverses
  - Fermat's little theorem, Wilson's theorem
- Chinese remainder theorem

Multiplicative Inverse

The **multiplicative inverse** of $a \not\equiv 0 \pmod n$ is another integer a' such that:

$$a \cdot a' \equiv 1 \pmod n$$

In modular arithmetic, a special property is that there are multiplicative inverses for integers.

For example,

$$2 * 5 = 1 \ (\text{mod } 3),$$

so 5 is a multiplicative inverse of 2 modulo 3 (and vice versa).

Does every integer have a multiplicative inverse in modular arithmetic?

Multiplicative Inverse

Does every integer have a multiplicative inverse in modular arithmetic?

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

a	1	2	3	4
a'	1	3	2	4

Z_6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

a	1	2	3	4	5
a'	1	X	X	X	5

X denotes no inverse

Multiplicative Inverse

Z_5:

a	1	2	3	4
a'	1	3	2	4

Z_6:

a	1	2	3	4	5
a'	1	X	X	X	5

Z_7:

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Z_8:

a	1	2	3	4	5	6	7
a'	1	X	3	X	5	X	7

Z_9:

a	1	2	3	4	5	6	7	8
a'	1	5	X	7	2	X	4	8

What is the pattern?

Multiplicative Inverse

Why 2 does not have a multiplicative inverse under modulo 6?

Suppose it has a multiplicative inverse y.

$2y \equiv 1 \pmod 6$

=> $2y = 1 + 6x$ for some integer x

=> $2y - 6x = 1$

This is a contradiction as LHS is even while RHS is odd.

Claim. If integers k,n are not coprime (i.e. $\gcd(k,n) \geq 2$), then k does not have a multiplicative inverse modulo n.

Proof. Same as above. Leave as an exercise.

Multiplicative Inverse

What if gcd(k,n)=1?

Would k always have a multiplicative inverse under modulo n?

Theorem. If gcd(k,n)=1, then have k' such that

$$k \cdot k' \equiv 1 \pmod{n},$$

where k' is an *inverse* of k (mod n).

gcd(k,n)=spc(k,n)

Proof: Since gcd(k,n)=1, there exist s and t so that $sk + tn = 1$.

So $tn = 1 - sk$

This means $n \mid 1 - sk$.

This means $1 - sk \equiv 0 \pmod{n}$.

This means $1 \equiv sk \pmod{n}$.

So $k' = s$ is a multiplicative inverse of k (mod n).

Cancellation

Note that $\equiv$ (mod n) behaves similarly to $=$.

If $a \equiv b \pmod{n}$, then $a+c \equiv b+c \pmod{n}$.

If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$

However, if $ac \equiv bc \pmod{n}$ and $c \not\equiv 0 \pmod{n}$,
it is not necessarily true that $a \equiv b \pmod{n}$.

For example, $4 \cdot 2 \equiv 1 \cdot 2 \pmod{6}$, but $4 \not\equiv 1 \pmod{6}$

There is no general cancellation in modular arithmetic.

Cancellation

What makes $a \cdot k \equiv b \cdot k \pmod{n}$ possible when $a \neq b$?

Without loss of generality, assume $0 \leq a, b, k < n$. This is because if $a \cdot k \equiv b \cdot k \pmod{n}$, then $(a \bmod n) \cdot (k \bmod n) \equiv (b \bmod n) \cdot (k \bmod n) \pmod{n}$.

smaller than n.

This means $(a-b)k = ak - bk \equiv 0 \pmod{n}$.

So $(a-b)k$ is divisible by n.

Since $0 \leq a, b < n$ and $a \neq b$, it implies that $0 < |a-b| < n$.

This is possible only when n and k share a common divisor, that is,

$$\gcd(n,k) \geq 2 \;\; !$$

Okay, so, can we say something when $\gcd(n,k)=1$?

Cancellation

Claim. If $i \cdot k \equiv j \cdot k \pmod{n}$ *and* $\gcd(k,n) = 1$,

then $i \equiv j \pmod{n}$.

For example, multiplicative inverse always exists if n is a prime!

Proof. Since $\gcd(k,n) = 1$, there exists k' such that $kk' \equiv 1 \pmod{n}$.

$$i \cdot k \equiv j \cdot k \pmod{n}$$

$$\Rightarrow i \cdot k \cdot k' \equiv j \cdot k \cdot k' \pmod{n}$$

$$\Rightarrow i \equiv j \pmod{n}$$

This makes arithmetic modulo prime a field,

a structure that "behaves like" real numbers.

Arithmetic modulo prime is very powerful in coding theory.

Plan

- Modular arithmetic
  - Modular addition, multiplication
  - Applications
  - Multiplicative inverses
  - Fermat's little theorem, Wilson's theorem
- Chinese remainder theorem

Fermat's Little Theorem

If p is a prime and $\gcd(k,p) = 1$, then we can cancel k. So

$$k \pmod p,\ 2k \pmod p,\ \ldots,\ (p-1)k \pmod p$$

are all different.

This yields that

$k \pmod p$, $2k \pmod p$, …, $(p-1)k \pmod p$

must be a *permutation* of

$$1, 2, \cdots, (p-1)$$

(each number appears exactly once.)

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Fermat's Little Theorem

Theorem. Let p be a prime and $\gcd(k,p) = 1$. Then

$$k^{p-1} \equiv 1 \pmod{p}.$$

Proof.

A permutation

$$1 \cdot 2 \cdots (p-1) \equiv (k \bmod p) \cdot (2k \bmod p) \cdot \cdots \cdot ((p-1)k \bmod p) \pmod{p}$$

$$\equiv (k \cdot 2k \cdot \cdots \cdot (p-1)k) \pmod{p}$$

$$\equiv (k^{p-1}) \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod{p}$$

Since $1, 2, \cdots, (p-1)$ are coprime with p, they can be cancelled on both sides, we have

$$1 \equiv k^{p-1} \pmod{p}$$

Wilson's Theorem

Theorem. p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

We first consider the "if" side.

Wlog, suppose p is not a prime and $p \geq 6$. (Why?)

Then $p=qr$ for some $2 \leq q, r < p$.

If $q \neq r$, then both q and r appear in $(p-1)!$,

and so $(p-1)! \equiv 0 \pmod{p}$.

If $q = r$, then $p = q^2 > 2q$ (since $p \geq 6$).

then both q and $2q$ are in $(p-1)!$,

and so again $(p-1)! \equiv 0 \pmod{p}$.

Wilson's Theorem

Theorem. p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

To prove the "only if" direction, we will need a lemma.

Lemma. Let p be a prime number. Then

$x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

Proof. $x^2 \equiv 1 \pmod{p}$

$\Leftrightarrow p \mid x^2 - 1 = (x - 1)(x + 1)$

$\Leftrightarrow p \mid (x - 1)$ or $p \mid (x+1)$

Recall p prime and $p|ab$ implies $p|a$ or $p|b$.

$\Leftrightarrow x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$

Wilson's Theorem

Theorem. p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

Let's get the proof idea by considering a concrete example.

$$
\begin{aligned}
& 10! \\
\equiv\ & 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10 \pmod{11} \\
\equiv\ & 1\cdot 10\cdot (2\cdot 6)\cdot (3\cdot 4)\cdot (5\cdot 9)\cdot (7\cdot 8) \pmod{11} \\
\equiv\ & 1\cdot (-1)\cdot (1)\cdot (1)\cdot (1)\cdot (1) \pmod{11} \\
\equiv\ & -1 \pmod{11}
\end{aligned}
$$

Except for 1 and 10, the remaining are paired up into multiplicative inverses!

Wilson's Theorem

Theorem. p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Consider an odd prime p. Each k from 1 to $p-1$ has a multiplicative inverse.

In particular, each k between 2 and $p-2$ has an inverse $k' \neq k$ by the lemma.

Since p is odd, the numbers from 2 to $p-2$ can be grouped into pairs $\{a_1,b_1\},\{a_2,b_2\},\ldots,\{a_{(p-3)/2},b_{(p-3)/2}\}$ so that $a_ib_i \equiv 1 \pmod{p}$.

Therefore, $(p-1)! \equiv 1\cdot(p-1)\cdot 2\cdot 3\cdots(p-3)\cdot(p-2) \pmod{p}$

$$\equiv 1\cdot(p-1)\cdot(a_1b_1)\cdot(a_2b_2)\cdots(a_{(p-3)/2}b_{(p-3)/2}) \pmod{p}$$

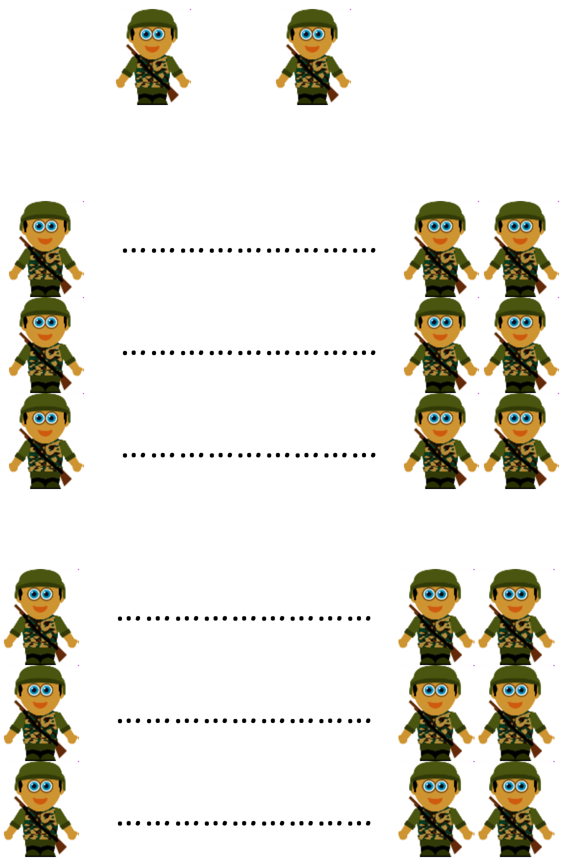
$$\equiv 1\cdot(-1)\cdot(1)\cdot(1)\cdots(1) \pmod{p}$$

$$\equiv -1 \pmod{p}.$$

Plan

- Modular arithmetic
  - Modular addition, multiplication
  - Applications
  - Multiplicative inverses
  - Fermat's little theorem, Wilson's theorem
- Chinese remainder theorem

Chinese Remainder Theorem



Picture from
http://img5.epochtimes.com/i6/801180520191974.jpg

One Equation

How to solve the following equation?

$$\boxed{ax \equiv b \pmod{n}}$$

$2x \equiv 3 \pmod{7}$	$x = 5 + 7v$ for any integer v
$5x \equiv 6 \pmod{9}$	$x = 3 + 9v$ for any integer v
$4x \equiv -1 \pmod{5}$	$x = 1 + 5v$ for any integer v
$4x \equiv 2 \pmod{6}$	$x = 2 + 3v$ for any integer v
$10x \equiv 2 \pmod{7}$	$x = 3 + 7v$ for any integer v
$3x \equiv 1 \pmod{6}$	no solutions

One Equation

$$\boxed{ax \equiv b \pmod{n}}$$

Case 1: $\gcd(a,n) = 1$.

Note that a can be replaced by $a \bmod n$, so we may assume $0 < a < n$.

e.g. $103x \equiv 6 \pmod{9} \Leftrightarrow 4x \equiv 6 \pmod{9}$.

Since $\gcd(a,n) = 1$, there exists a multiplicative inverse a' for a.
Hence we can multiply a' on both sides of the equation to obtain

$$\boxed{x \equiv a'b \pmod{n}}$$

Therefore, a solution always exists when a and n are coprime.

One Equation

$$ax \equiv b \pmod{n}$$

Case 2: $\gcd(a,n) = c > 1$.

Case 2a: c divides b.

$ax \equiv b \pmod{n}$

$\Leftrightarrow$ $ax = b + nk$ for some integer k

$\Leftrightarrow$ $a_1cx = b_1c + n_1ck$

$\Leftrightarrow$ $a_1x = b_1 + n_1k$

$\Leftrightarrow$ $a_1x \equiv b_1 \pmod{n_1}$

Therefore, we can reduce to **Case 1**.

One Equation

$$\boxed{ax \equiv b \pmod{n}}$$

Case 2: $\gcd(a,n) = c > 1$.

Case 2b: c does not divide b.

$ax \equiv b \pmod{n}$

$\Leftrightarrow ax = b + nk$ for some integer k

$\Leftrightarrow a_1cx = b + n_1ck$

$\Leftrightarrow b = (a_1x - n_1k)c$

This is a contradiction as RHS is divisible by c while LHS is not.

So there is no solutions in this case.

One Equation

$$\boxed{ax \equiv b \pmod{n}}$$

Theorem. Given integers a, b, n,
the above equation has a solution if and only if $\gcd(a,n) \mid b$.

Moreover, the solutions are all of the form $y \pmod{n/\gcd(a,n)}$.

Proof. First, divide b by $\gcd(a,n)$.

If not divisible, then there is no solutions by **Case (2b)**.

If divisible, then we can simplify the equation as **Case (2a)**.

Then we proceed as **Case 1** to compute the solution.

Ancient Application of Number Theory

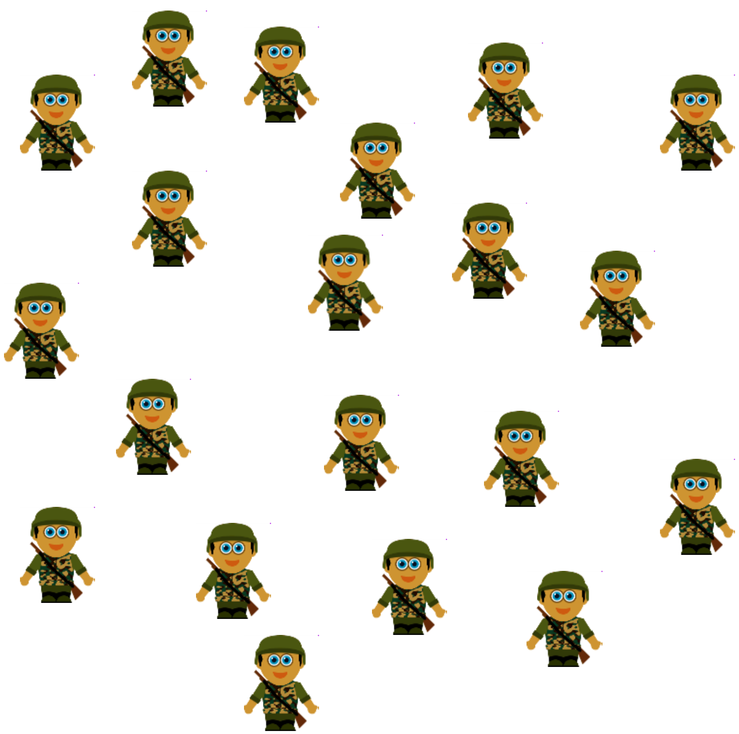
In Ancient China, there was a General named Han Xin, who led an army of 1500 soldiers in a battle. An estimated 400-500 soldiers died in the battle. **When the soldiers stood 3 in a row, there were 2 soldiers left over. When they lined up 5 in a row, there were 4 soldiers left over. When they lined up 7 in a row, there were 6 soldiers left over. Han Xin immediately said, "There are 1049 soldiers."**

(from https://chinesetuition88.com/2015/04/25/chinese-remainder-theorem-history-韩信点兵/)

Ancient Application of Number Theory

Starting from 1500 soldiers, about 400-500 soldiers died at a battle.

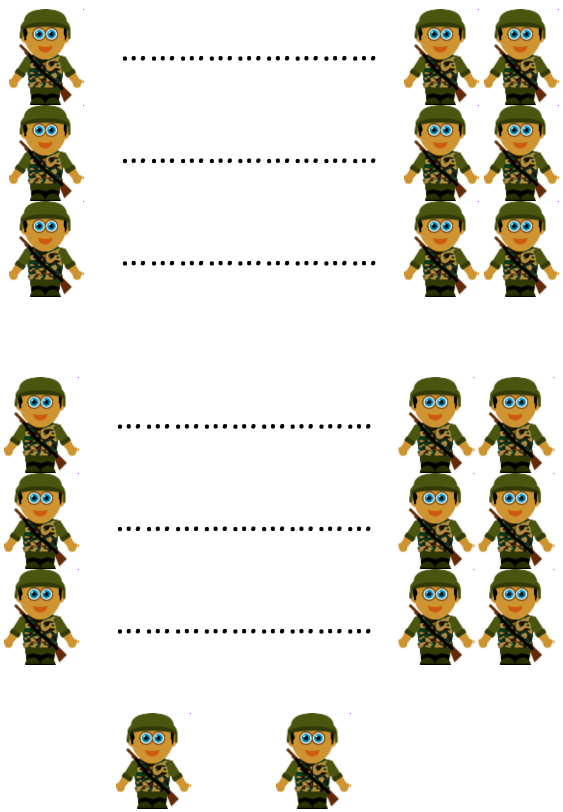
Now we want to know how many soldiers are left.



Form groups of 3 soldiers

Han Xin (韓信)

Ancient Application of Number Theory

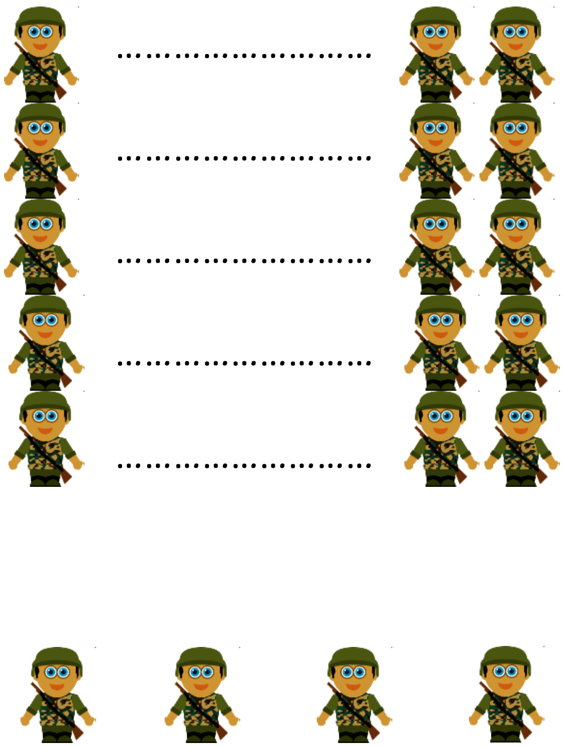


There are 2 soldiers left.

Form groups of 5 soldiers

Han Xin (韓信)

Ancient Application of Number Theory

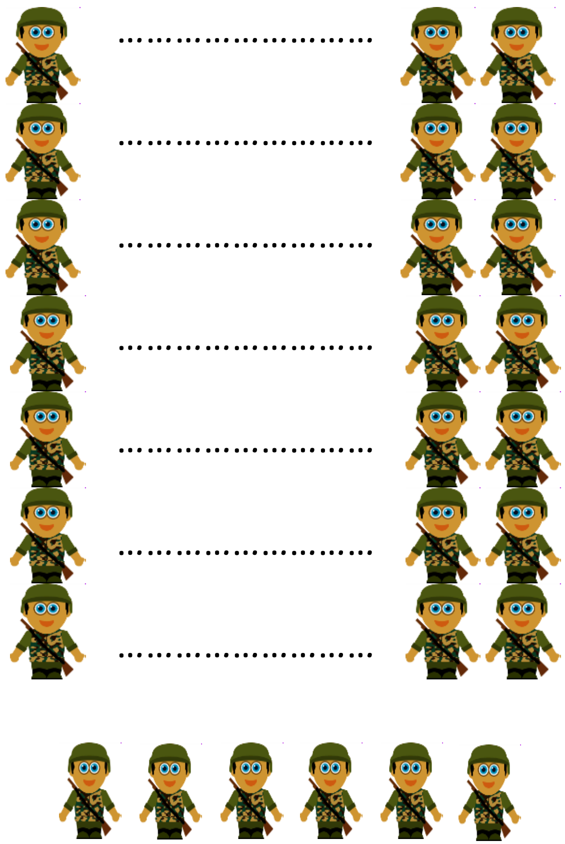


There are 4 soldiers left.

Form groups of 7 soldiers

Han Xin (韓信)

Ancient Application of Number Theory



There are 6 soldiers left.

We have 1049 soldiers.

Han Xin (韓信)

How did he figure this out?!

The Question

$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 6 \pmod 7$$

$+$

$$1000 \le x \le 1100$$

$\Rightarrow$

$$x = 1049$$

How to solve this system of modular equations?

Two Equations

Find a solution to satisfy both equations simultaneously.

$$\boxed{\begin{aligned} c_1 x &\equiv d_1 \pmod{m_1} \\ c_2 x &\equiv d_2 \pmod{m_2} \end{aligned}}$$

First we can reduce each equation to its simple form when possible.

$$\boxed{\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned}}$$

Of course, there may be no solutions sometimes.

For example, consider $x \equiv 1 \pmod 3$ and $x \equiv 2 \pmod 3$.

$x \equiv 1 \pmod 6$ and $x \equiv 2 \pmod 4$.

Two Equations

Case 1: n_1 and n_2 are coprime.

$$x \equiv 2 \pmod{3}$$
$$x \equiv 4 \pmod{7}$$

Then $x = 2+3u$ and $x = 4+7v$ for some integers u, v.

$2+3u = 4+7v \quad \Rightarrow \quad 3u = 2+7v$

$\Rightarrow \quad 3u \equiv 2 \pmod{7}$

Note that 5 is a multiplicative inverse for 3 modulo 7.

We multiply 5 on both sides to get:

$u \equiv 5 \cdot 2 \equiv 3 \pmod{7}$

$\Rightarrow \quad u = 3 + 7w$

Therefore, $x = 2+3u = 2+3(3+7w) = 11+21w$.

So any $x \equiv 11 \pmod{21}$ is a solution.

Where did we use the assumption that n_1 and n_2 are coprime?

Two Equations

Case 1: n_1 and n_2 are coprime.

$$\boxed{\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 4 \pmod{7} \end{aligned}}$$

In fact, we can construct such an x directly.

Set $x = 3 \cdot a + 7 \cdot b$

When x is divided by 3, the remainder is determined by the second term.

And when x is divided by 7, the remainder is determined by the first term.

How do we choose a so that $3a$ has remainder 4 when divided by 7?

This is just asking $3a \equiv 4 \pmod{7}$ => $a \equiv 5 \cdot 4 \equiv 6 \pmod{7}$.

Similarly, we have $7b \equiv 2 \pmod{3}$ => $b \equiv 2 \pmod{3}$.

So the answer is $x = 3a+7b \equiv 3 \cdot 6 + 7 \cdot 2 \pmod{21} \equiv 32 \pmod{21} \equiv 11 \pmod{21}$.

Three Equations

$$\boxed{\begin{aligned} x &\equiv 2 \pmod 3) \\ x &\equiv 4 \pmod 5) \\ x &\equiv 6 \pmod 7) \end{aligned}}$$

Set $x = 5\cdot 7\cdot a + 3\cdot 7\cdot b + 3\cdot 5\cdot c$

Then the first (second, third) term is determined by the first (second, third) equation.

Now we just need to solve the following equations separately.

$$35a \equiv 2 \pmod 3, \quad 21b \equiv 4 \pmod 5, \quad 15c \equiv 6 \pmod 7.$$

$$\Rightarrow \quad 2a \equiv 2 \pmod 3, \quad b \equiv 4 \pmod 5, \quad c \equiv 6 \pmod 7.$$

$$\Rightarrow \quad a \equiv 1 \pmod 3, \quad b \equiv 4 \pmod 5, \quad c \equiv 6 \pmod 7.$$

Then $x = 35a + 21b + 15c \equiv 35\cdot 1 + 21\cdot 4 + 15\cdot 6 \pmod{3\cdot 5\cdot 7} \equiv 209 \pmod{105}$.

Since Han Xin knew that $1000 \le x \le 1100$, he concluded that $x = 1049$.

Wait, but how did he know that there was no other solutions?

Chinese Remainder Theorem

Theorem. Let $n_1, n_2, \ldots, n_k$ be **mutually** coprime. Then

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a **unique** solution modulo n, where $n = n_1 n_2 \ldots n_k$.

We will give a proof when k=3, but it can be extended easily to any k.

Proof of Chinese Remainder Theorem

Let $\mathbf{N}_1 = n_2 n_3$ $\mathbf{N}_2 = n_1 n_3$ $\mathbf{N}_3 = n_1 n_2$

Since N_i and n_i are coprime, there exist x_1, x_2, x_3 such that

$$N_1 x_1 \equiv 1 \pmod{n_1} \qquad N_2 x_2 \equiv 1 \pmod{n_2} \qquad N_3 x_3 \equiv 1 \pmod{n_3}$$

$$\Rightarrow N_1 x_1 a_1 \equiv a_1 \pmod{n_1}, N_2 x_2 a_2 \equiv a_2 \pmod{n_2}, N_3 x_3 a_3 \equiv a_3 \pmod{n_3}$$

$$\boxed{\text{Let } x = N_1(x_1 a_1) + N_2(x_2 a_2) + N_3(x_3 a_3)}$$

Note that n_1 divides both $\mathbf{N}_2$ and $\mathbf{N}_3$, so

$$x \equiv N_1(x_1 a_1) \equiv a_1 \pmod{n_1}$$

Similarly, $\boxed{x \equiv a_2 \pmod{n_2}}$ $\boxed{x \equiv a_3 \pmod{n_3}}$

Uniqueness

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

$$x \equiv a_k \pmod{n_k}$$

- Let x, y be solutions to the above system.
- Then $x - y \equiv 0 \pmod{n_i}$ for each i.
- Hence $n_i \mid x - y$ for each i.
- Since $n_1, n_2, \ldots, n_k$ are mutually coprime,
- it follows that $n_1 n_2 \ldots n_k \mid x - y$. (Why?)
- Therefore, $x \equiv y \pmod{n_1 n_2 \ldots n_k}$.

General Systems

What if $n_1, n_2, \ldots, n_k$ are **not** mutually coprime?

$x \equiv 3 \pmod{10}$

- $\cancel{x \equiv 3 \pmod 2 \equiv \mathbf{1} \pmod{\mathbf{2}}}$ (a)
- $x \equiv \mathbf{3} \pmod{\mathbf{5}}$ (b)

$x \equiv 8 \pmod{15}$

- $x \equiv 8 \pmod 3 \equiv \mathbf{2} \pmod{\mathbf{3}}$ (c)
- $\cancel{x \equiv 8 \pmod 5 \equiv \mathbf{3} \pmod{\mathbf{5}}}$ (d)

$x \equiv 5 \pmod{84}$

- $x \equiv 5 \pmod 4 \equiv \mathbf{1} \pmod{\mathbf{4}}$ (e)
- $\cancel{x \equiv 5 \pmod 3 \equiv \mathbf{2} \pmod{\mathbf{3}}}$ (f)
- $x \equiv \mathbf{5} \pmod{\mathbf{7}}$ (g)

So we reduce the problem to the mutually-coprime case.

The answer is **173 (mod 420)**.

(e) is stronger than (a).

(b) and (d) are the same.

(c) and (f) are the same.

A Faster Method

There is an alternative way to solve the system of modular equations.

$$x \equiv 3 \pmod{10}$$
$$x \equiv 8 \pmod{15}$$
$$x \equiv 5 \pmod{84}$$

From the third equation we have $x = 5+84u$.

Plug it into the second equation gives $5+84u \equiv 8 \pmod{15}$ => $9u \equiv 3 \pmod{15}$.

Solving this gives $u \equiv 2 \pmod{5}$ => $u = 2 + 5v$.

Hence, $x = 5+84u = 5+84(2+5v) = 173 + 420v$.

Plug it into the first gives $173+420v \equiv 3 \pmod{10}$ => $420v = -170 \pmod{10}$.

This equation is always true.

So we conclude that $x = 173+420v$, or equivalently $x \equiv 173 \pmod{420}$.

This method can also be used to prove the Chinese remainder theorem.

It is much faster (no need to find factorization), solving only k-1 modular equations.