Dis 4A: CRT, FLT,

- Join our discord; link in an email I sent!

Me: Why is there exist integer a such that a = 5 (mod 17) and a = 8 (mod 21)

My teacher:

History [edit]

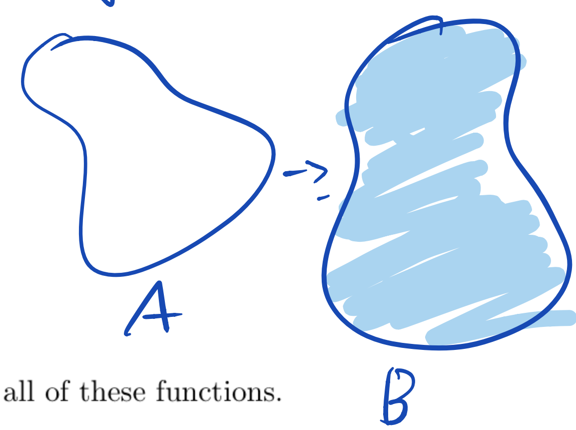
The earliest known statement of the theorem, as a problem with specific numbers, appears in the 3rd-century book *Sun-tzu Suan-ching* by the Chinese mathematician Sun-tzu:[1]

> There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?[2]

Sun-tzu's work contains neither a proof nor a full algorithm.[3] What amounts to an algorithm for solving this problem was described by Aryabhata (6th century).[4] Special cases of the Chinese remainder theorem were also known to Brahmagupta (7th century), and appear in Fibonacci's Liber Abaci (1202).[5] The result was later generalized with a complete solution called *Ta-yan-shu* (大衍術) in Ch'in Chiu-shao's 1247 *Mathematical Treatise in Nine Sections* (數書九章, *Shu-shu Chiu-chang*)[6] which was translated into English in early 19th century by British missionary Alexander Wylie.[7]

Review (Bijections)

$f: A \to B$



- f is **onto** (surjective) if $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$
  - i.e. every $b \in B$ has a pre-image.
- f is **one-to-one** (injective) if $\forall a, a' \in A, f(a) = f(a') \implies a = a'$.
  - i.e. different inputs map to different outputs,

one-to-one & onto = bijective.

Here's a helpful graphic illustrating the differences between all of these functions.

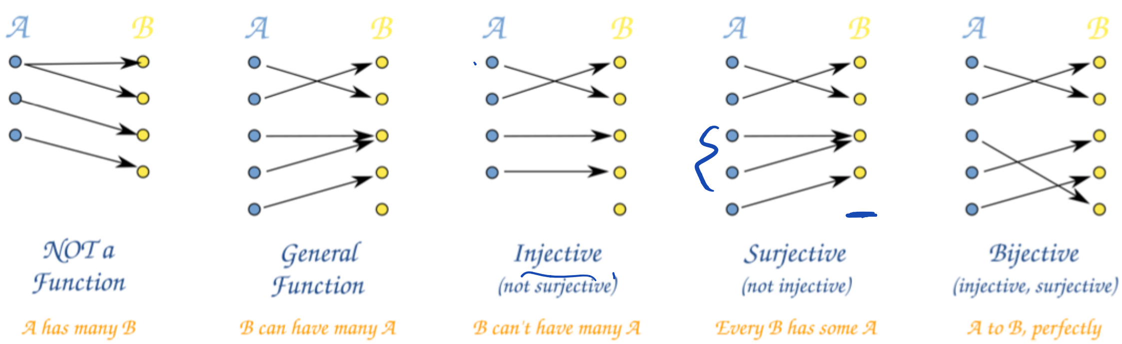


Figure 1: Examples of the four types of functions, and a non-function. Source: Math is Fun.

Review (CRT)

12, 13, 20.

Theorem 5 (Chinese Remainder Theorem). Let $m_1, \ldots, m_k$ be pairwise[a] relatively prime positive integers, and let

$$M = m_1 \ldots m_k.$$

Then for every k-tuple $(x_1, \ldots, x_k)$ of integers, there is exactly one residue class $x \pmod M$ such that

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\vdots \\ x &\equiv x_k \pmod{m_k}. \end{aligned}$$

[a] Every pair of integers is relatively prime, as opposed to being relatively prime as a whole.

2-3
2-5
3-5

CRT is both constructive (HW4 #3) & can show existence. (HW 4 #4)

the big idea is that every number mod M can be broken down into its "components" mod $m_1, m_2, \ldots, m_k$. a.k.a basis vectors

key prop: coprime moduli

example: (mod 15) $\longleftrightarrow$ mod 3 & mod 5.

mod 5

mod 3 \ mod 5	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

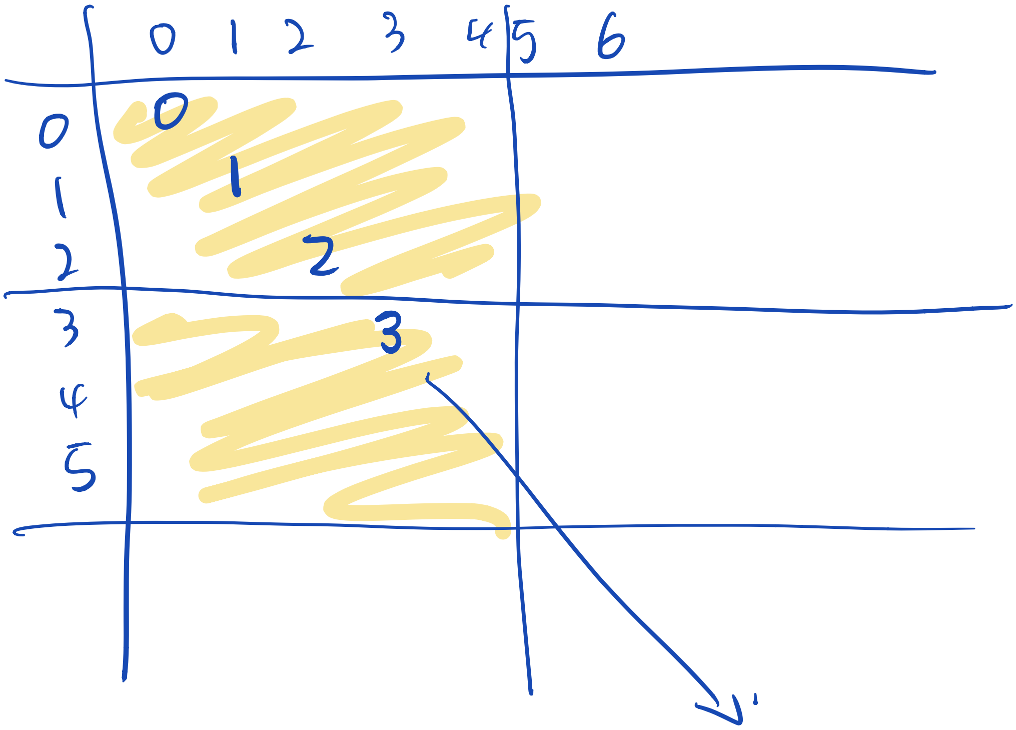
ex:

$x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$.

in general,

$$x = \sum_{i=1}^{k} C_i \left(\frac{M}{m_i}\right) \equiv \sum_{i=1}^{k} \left(\frac{M}{m_i}\right)^{-1}_{m_i} \left(\frac{M}{m_i}\right) x_i \pmod M.$$


0 1 2 3 4 5 6
0
1
2
3
4
5
0
1
2
3

1 Chinese Remainder Theorem Practice

In this question, you will solve for a natural number x such that,

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned} \tag{1}$$

(a) Suppose you find 3 natural numbers a, b, c that satisfy the following properties:

$$a \equiv 2 \pmod 3 \ ; \ a \equiv 0 \pmod 5 \ ; \ a \equiv 0 \pmod 7), \tag{2}$$

$$b \equiv 0 \pmod 3 \ ; \ b \equiv 3 \pmod 5 \ ; \ b \equiv 0 \pmod 7), \tag{3}$$

$$c \equiv 0 \pmod 3 \ ; \ c \equiv 0 \pmod 5 \ ; \ c \equiv 4 \pmod 7). \tag{4}$$

Show how you can use the knowledge of a, b and c to compute an x that satisfies (1).

$x = a + b + c.$

$x \equiv 2 + 0 + 0 \equiv 2 \pmod 3$

$x \equiv 0 + 3 + 0 \equiv 3 \pmod 5$

$x \equiv 0 + 0 + 4 \equiv 4 \pmod 7$.

(b) Find a natural number a that satisfies (2). In particular, an a such that $a \equiv 2 \pmod 3$ and is a multiple of 5 and 7. It may help to approach the following problem first:

(b.i) Find a^*, the multiplicative inverse of 5×7 modulo 3. What do you see when you compute $(5 \times 7) \times a^*$ modulo 3, 5 and 7? What can you then say about $(5 \times 7) \times (2 \times a^*)$?

$a \equiv 0 \pmod{35}$ $\boxed{a = 35}$

$\equiv 35$

$35 \equiv 2 \pmod 3$

$a^* \equiv (5 \times 7)^{-1} \pmod 3$

$a^* \equiv 2.$

$140 \equiv 35.$

(c) Find a natural number b that satisfies (3). In other words: $b \equiv 3 \pmod 5$ and is a multiple of 3 and 7.

$b^* \equiv (3 \times 7)^{-1}$ (modulo 5)

$\equiv 21^{-1} \equiv 1^{-1} \equiv 1$

$b = b^* \times 3 \times 3 \times 7 = 63$

(d) Find a natural number c that satisfies (4). That is, c is a multiple of 3 and 5 and $\equiv 4 \pmod 7$.

$c^* \equiv (3 \times 5)^{-1} \pmod 7$

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

$c = c^* \times 4 \times 3 \times 5 = 60.$

(e) Putting together your answers for Part (a), (b), (c) and (d), report an x that indeed satisfies (1).

$x = 35 + 63 + 60 \equiv 158 \equiv 53 \pmod{105}.$

2 CRT Decomposition

In this problem we will find $3^{302} \mod 385$.

(a) Write 385 as a product of prime numbers in the form $385 = p_1 \times p_2 \times p_3$.

(b) Use Fermat's Little Theorem to find $3^{302} \mod p_1$, $3^{302} \mod p_2$, and $3^{302} \mod p_3$.

(c) Let $x = 3^{302}$. Use part (b) to express the problem as a system of congruences (modular equations mod 385). Solve the system using the Chinese Remainder Theorem. What is 3^{302} mod 385?

Fermat's Little Theorem

For prime p,

$a^p \equiv a \pmod p$.

Equiv., if $\gcd(a,p)=1$,

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

(a) $35 \times 11 = 5 \times 7 \times 11$.

(b) $3^{302} \equiv (3^4)^k \cdot 3^2 \pmod 5$

$\equiv 1^k \cdot 3^2 \equiv 3^2$.

$\boxed{a^{5-1} = a^4 \equiv 1 \pmod 5}$

$(302 \equiv 2 \pmod 4)$

$3^{302} \equiv 3^2 \equiv 2 \pmod 7$

$3^{302} \equiv (3^4)^{75} \cdot 3^2 \equiv 1^{75} \cdot 3^2$

$\equiv 3^{4 \cdot 75 + 2}$. $\equiv 3^2$

$302 = 4 \cdot 75 + 2$

$(302 \equiv 2 \pmod 6)$

$3^{302} \equiv 3^2 \equiv 9 \pmod{11}$.

$(302 \equiv 2 \pmod{10})$

(c).

$x \equiv 4 \pmod 5$

$x \equiv 2 \pmod 7$

$x \equiv 9 \pmod{11}$.

4, 9, 14

2, 9, 16

$x \equiv 9 \pmod{35}$.

$\boxed{x \equiv 9 \pmod{385}}$

$(a)^{-1}_m$

$\Rightarrow a^{-1} \pmod m$.

$\boxed{3^{302} \equiv 9 \pmod{385}}$

$a = (7 \times 11)^{-1}_5 \cdot 7 \times 11 \times 4 \equiv 3 \cdot 7 \cdot 11 \cdot 4 \equiv 154$

$b = (5 \times 11)^{-1}_7 \cdot 5 \times 11 \times 2 \equiv -1 \cdot 5 \cdot 11 \cdot 2 = -110. \equiv 6 \cdot 5 \cdot 11 \cdot 2$

$c = (5 \times 7)^{-1}_{11} \cdot 5 \cdot 7 \cdot 9 \equiv 6 \times 5 \times 7 \cdot 9 \equiv -35$

$\boxed{9}$