4.6

Chinese Remainder Theorem ([[2, 3], [3, 5], [2, 7]])

23

$x \equiv 2 \mod 3$

$x \equiv 3 \mod 5$

$x \equiv 2 \mod 7$

4.6 - Classical cryptography

- Caesar cipher:
  - Replace each letter by an element of Z_{26} (an integer from 0 to 25)
  - can be represented by the function f that assigns the non-negative integer p, $p \leq 25$, the integer $f(p)$ in the set $\{0, 1, \ldots, 25\}$ with

$f(p) = (p+3) \mod 26$

(p: original message's letter (integer); $f(p)$: encrypted letter (integer))

Shift cipher

Encryption:

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10

L	M	N	O	P	Q	R	S	T	U	V
11	12	13	14	15	16	17	18	19	20	21

W	X	Y	Z
22	23	24	25

ex: What is the secret message from the message "MEET YOU EN THE PARK" using the Caesar cipher?
12, 4, 4, 19, 24, 14, 20, 0, 13, 19, 7, 9, 15, 0, 17, 10

solution:

- Because it's a caesar cipher, shift key is 3.
- Step 1: convert letters to numbers.
- Step 2: shift by 3 and mod by 26.
- Step 3: convert back to letters

15, 7, 7, 22, 1, 17, 23, 11, 16, 22, 10, 7, 18, 3, 20, 13

PHHW BRX LQ WKH SDUN

shift cipher decryption:

$f^{-1}(p) = (p-k) \bmod 26$

ex: Encrypt the plaintext message "STOP" using shift cipher with shift key K=11

Solution:

Step 1: STOP

18, 19, 14, 15

↓ (p+11) mod 26

Step 2: 2, 4, 25, 0

Step 3: DEZA ← final answer