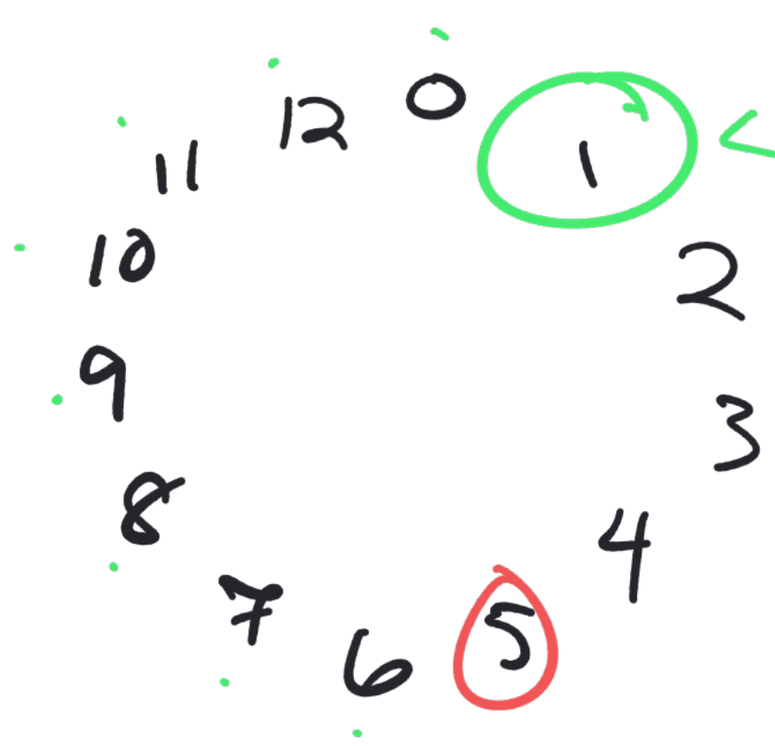
CS 338

Mon 25th Sep 2023

Modular arithmetic

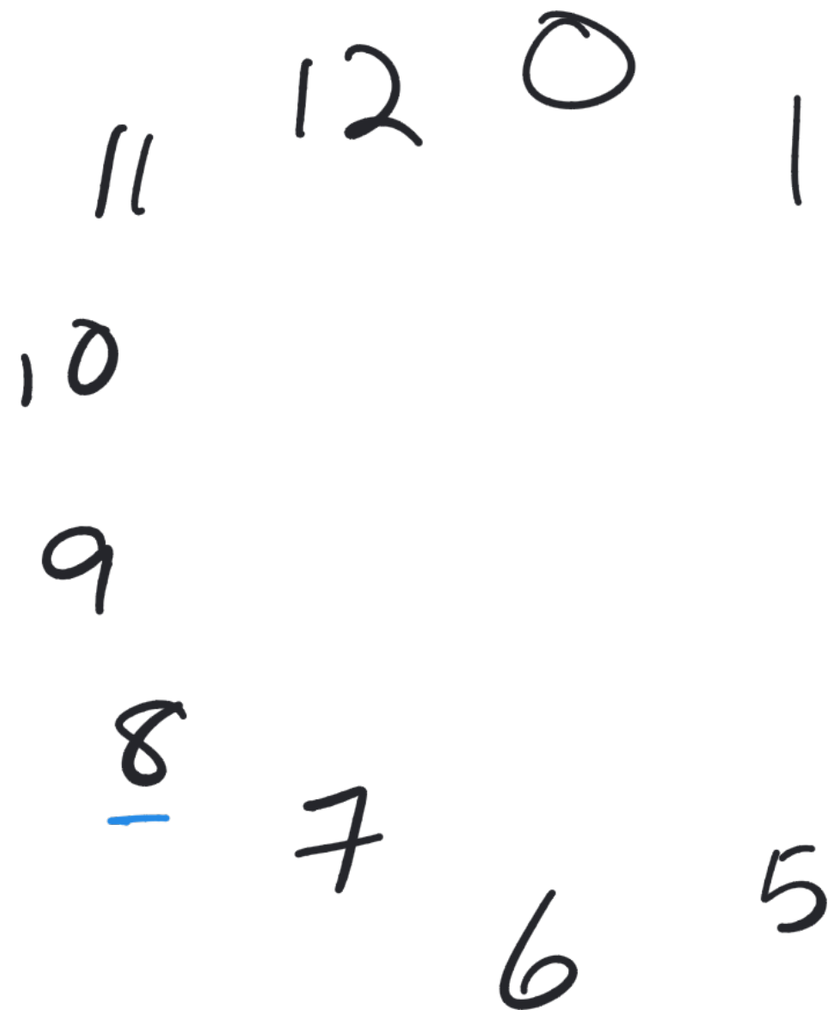
"mod 13" world

0 1 2 . . . 9 10 11 12



5+9

14
subtract highest multiple of 13 from,



10×8

$= 80 \quad 7, 13$

$= 80 - 78$

6×13

$= 2$

Multiples of 5

What is

$x = \frac{1}{5}$?

$5x = 1$

x = 8 works

10 11 12 13 5 0 1 8

2 3

3 11

9 7

8 12

7 4

6 9

5 10

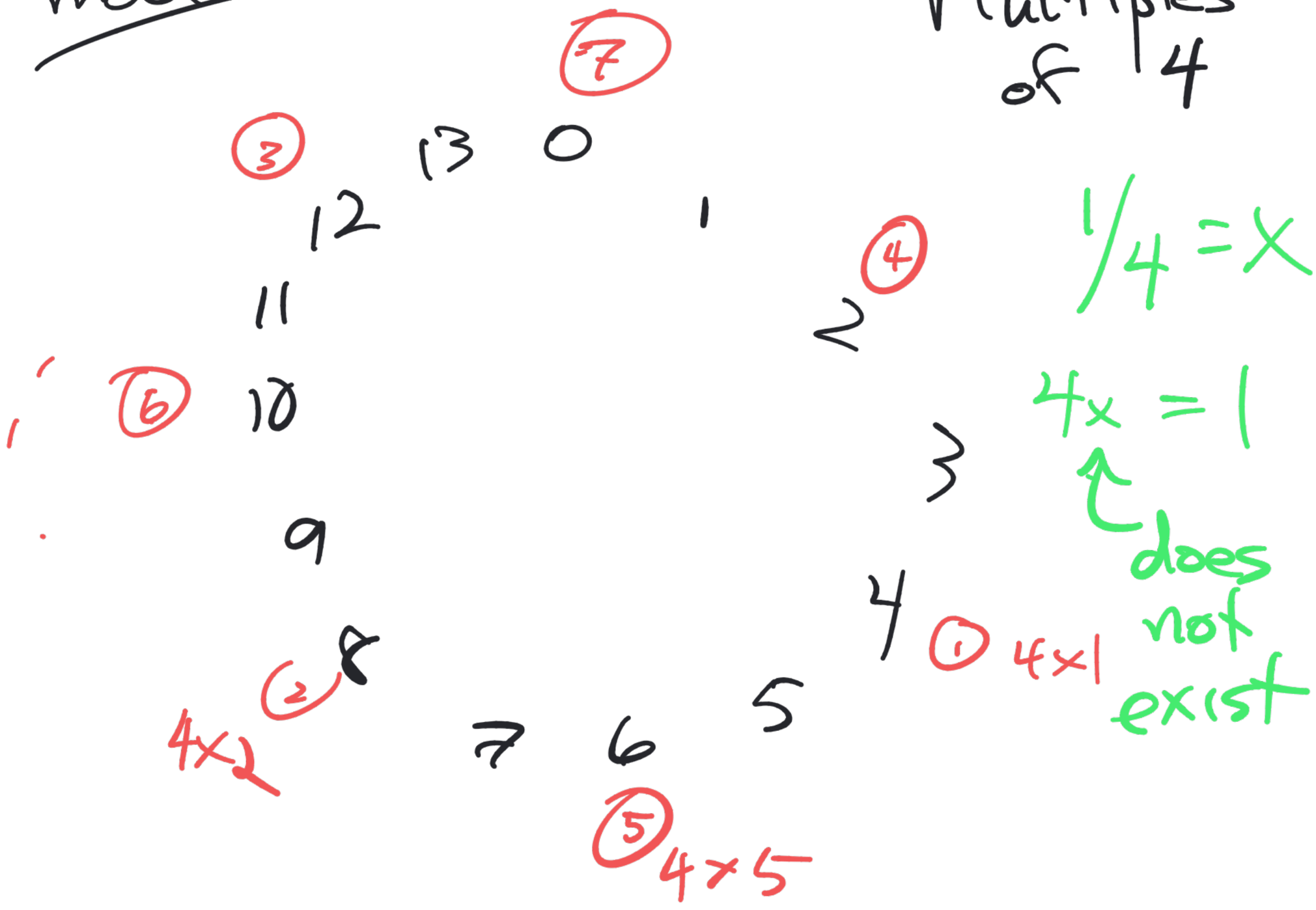
4 6

5x2

5x1

mod 14

Multiples of 4



$\frac{1}{4} = x$

$4x = 1$

does not exist

Notation

Mathematicians

$$ed = 1 \mod (p-1)(q-1)$$

Python programmers

```
(e*d)%((p-1)*(q-1))==1
```

Encryption function E

Private key (secret): S

Public key: P

For any legal message M

$$E(\underbrace{E(M, P)}_{\text{ciphertext}}, S) == M$$ plaintext

$$E(E(M, S), P) == M$$

RSA : $P = (e, n)$ / $S = (d, n)$

$$E(M, P) = M^e \bmod n$$

$$E(E(M, P), S) = (M^e)^d \bmod n$$

$$= \ldots [\text{math}] \ldots$$

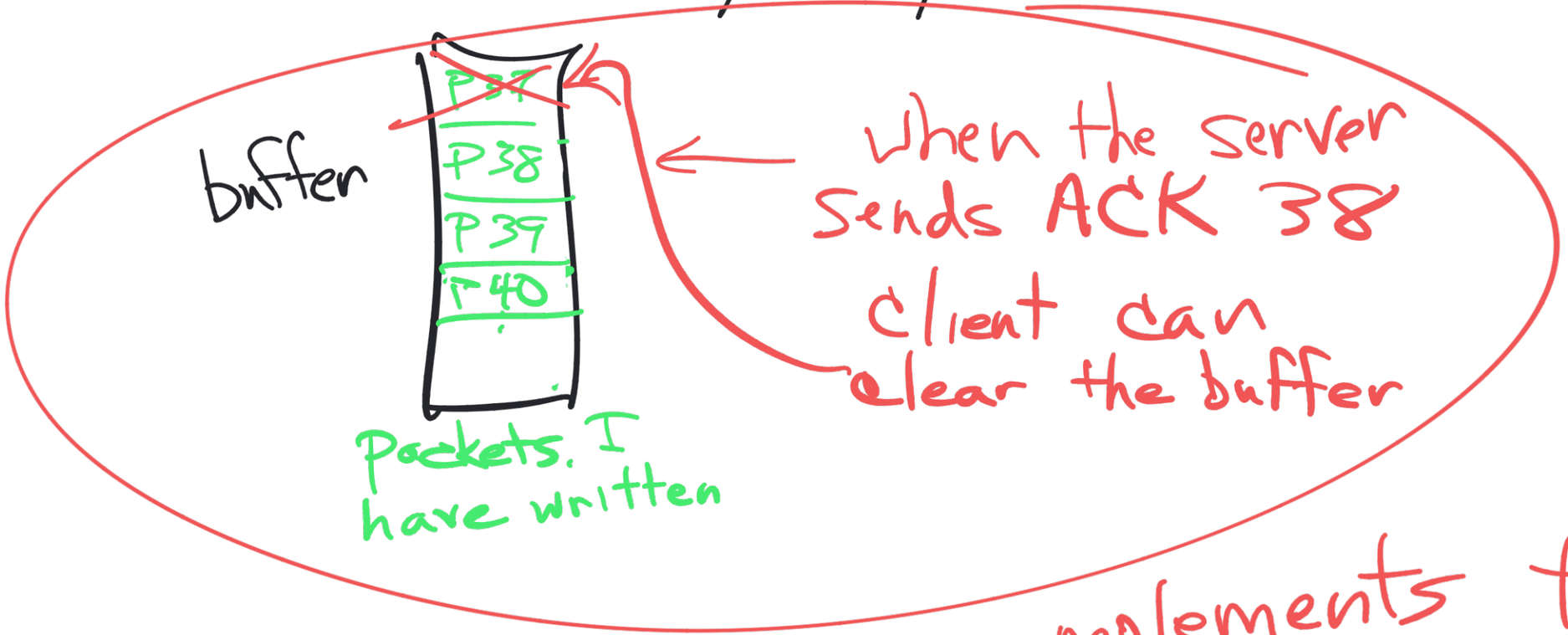
$$= M$$

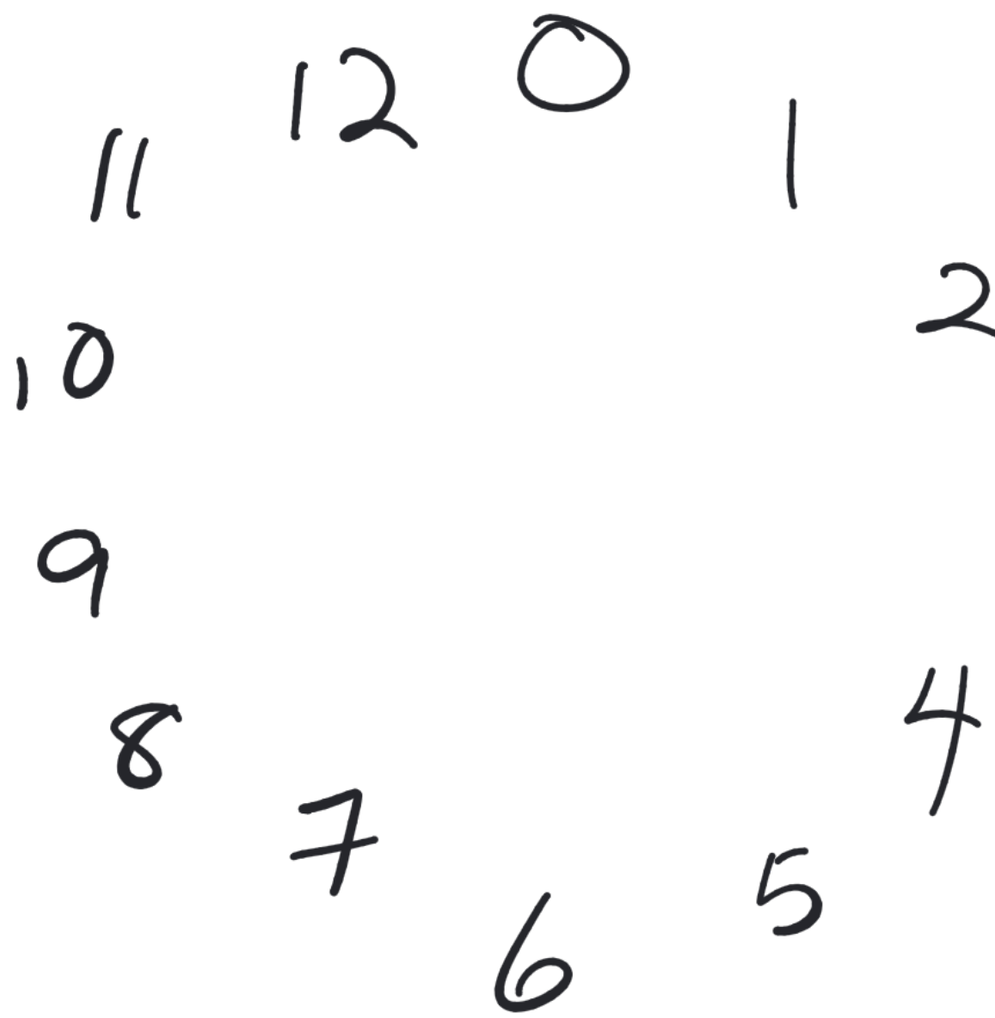
TCP connection

Client's perspective (eg. a C program)

open a "socket" ← like a file,

read/write/close




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