c< 338

Mon 25 Sep 2023
Modular arithmetic

"mod 13" world

0 1 2 ... 9 10 11 12

5 + 9

14 subtract higher multiple of 13 from.
10 × 8
= 80

= 80 - 78
6 × 13
= 2
Multiples of 5

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

$5x = 1$

$x = 8$ works
Notation
Mathematicians
\[ ed = 1 \mod (p-1)(q-1) \]
Python programmers
\[ (e \times d) \mod (p-1) \times (q-1) = 1 \]
Encryption function $E$

Private key: $S$
(secret)

Public key: $P$

for any legal message $M$

\[
E(E(M, P), S) = M
\]  
\[
E(E(M, S), P) = M
\]
RSA: \( P = (e, n) \) / \( S = (d, n) \)

\[
E(M, P) = M^e \mod n
\]

\[
E(E(M, P), S) = (M^e)^d \mod n
\]

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

\[
= M
\]
TCP Connection

Client's perspective (e.g., a C program)
open a "Socket" like a file
read/write/close

Buffer

Packets I have written
P38
P39
P40

When the server sends ACK 38
client can clear the buffer

etc. "sliding windows protocol"