

Splitting the Modulus (SM) ^{L32P1}

Let m, n be coprime positive integers.
Then for any integers x, a ,

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv a \pmod{n} \end{aligned} \quad (\text{simultaneously}) \iff x \equiv a \pmod{mn}$$

Pf: (\Leftarrow) $x \equiv a \pmod{mn}$

$$\Rightarrow mn \mid x - a$$

$$\Rightarrow x \equiv a \pmod{m} \quad \because m \mid mn \ \& \ mn \mid x - a$$

so by transitivity $m \mid x - a$

& $x \equiv a \pmod{n}$ similarly.

(\Rightarrow) Assume $x \equiv a \pmod{m}$ & $x \equiv a \pmod{n}$

Note $x = a$ is a solution. Since $\gcd(m, n) = 1$

by CRT $x \equiv a \pmod{mn}$ gives all solutions.

□

For what integers is $x^5 + x^3 + 2x^2 + 1$ divisible by 6?

want to solve

$$x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod{6}.$$

By (SM)

$$x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod{2}$$

$$x^5 + x^3 + 2x^2 + 1 \equiv 0 \pmod{3}$$

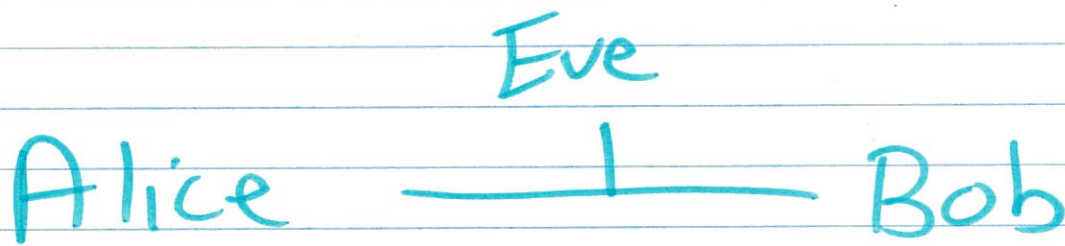
Use equation 1 and plugin $x \equiv 0 \pmod{2}$
& $x \equiv 1 \pmod{2}$. In both cases

$$x^5 + x^3 + 2x^2 + 1 \equiv 1 \pmod{2}.$$

$\therefore x^5 + x^3 + 2x^2 + 1$ is never divisible by 6.

Cryptography

- The practice/study of secure communication.



NB: A cryptosystem should not depend on the secrecy of the methods of encryption & decryption (except for possibly secret keys).

Private Key Cryptography

L32P4

- Agree before hand on a secret encryption & decryption key.

Ex! Caesar Cipher (ASCII table)

Map plaintext M to

$$C \equiv M + 3 \pmod{26} \quad (0 \leq C < 26)$$

Ex: A P P L E

00 15 15 11 04

03 18 18 14 07

D S S O H

Cons of Private Key Cryptography.

- Tough to share private key before hand.
- Too many private keys to share.
- Difficult to communicate with stranger.

Public Key Cryptography.

L32PS

Analogy: Pad lock

- Easy to lock

- Difficult to unlock without a Key

Eve

Alice

public key e

Bob

private key d

$M \mapsto C$

Decrypt C

Send C

using encryption Key

to M using d .

- Encryption & Decryption are inverses
- d & e are different
- Only d is secret.

Exponentiation Ciphers

L32P6

Alice chooses a (large) prime p and an integer e satisfying

$$1 < e < p-1 \quad \& \quad \gcd(e, p-1) = 1$$

Alice makes (e, p) public.

Alice computes d , an integer via

$$1 < d < p-1 \quad \& \quad ed \equiv 1 \pmod{p-1}$$

Note: d can be found quickly using EEA.

Note: Inverse exists $\because \gcd(e, p-1) = 1$.

To send a message $0 \leq M < p$ to Alice, Bob computes C s.t.

$$0 \leq C < p \quad \& \quad C \equiv M^e \pmod{p}$$

Bob sends C to Alice & Alice

computes $R \equiv C^d \pmod{p}$ with $0 \leq R < p$.