1a Problem

Prove $a_1 \equiv_b a_2 \longleftrightarrow a_1 \% b = a_2 \% b$

using Theorem 0.1 & elementary Axioms

No need to prove this in both directions.

$a_1 \equiv_b a_2 \longrightarrow a_1 \% b = a_2 \% b$

Given

$a_1 \equiv_b a_2$

Prove

$a_1 \% b = a_2 \% b$

$a_1 \equiv_b a_2 \iff b \mid (a_1 - a_2) = 0$ ——— (*)

$qb = a_1 - a_2$, for some quotient q

do modular b to the both sides

$(qb) \% b = a_1 \% b - a_2 \% b$

$0 = a_1 \% b - a_2 \% b$

$\boxed{a_1 \% b = a_2 \% b}$

Now the opposite direction

$a_1 \% b = a_2 \% b \longrightarrow a_1 \equiv_b a_2$

Given

$a_1 \% b = a_2 \% b$

Prove

$a_1 \equiv_b a_2$

$a_1 \% b - a_2 \% b = 0$

$(a_1 - a_2) \% b = 0$ → Associativity

$\therefore b \mid (a_1 - a_2)$

$b \mid (a_1 - a_2) \iff \boxed{a_1 \equiv_b a_2}$ ⩛

Hence,

$a_1 \equiv_b a_2$ equivalent to

$a_1 \% b = a_2 \% b$

16)

Prove that $a \%. b \equiv_b a$

from (a) we know

$$a_2 \equiv_b a_2 \iff a_1 \%. b = a_2 \%. b$$

So our mod equation $(a \%. b) \equiv_b a$ can be written as

$$(a \%. b) \%. b = a \%. b$$

We can show $\underline{\underline{(a \%. b) \%. b = (a \%. b)}}$ to prove $a \%. b \equiv_b a$ mod equation.

We know from unique division Theorem

$$(a \%. b) = a - \left(\left\lfloor \frac{a}{b} \right\rfloor \times b \right)$$

do modulus to both side

$$(a \%. b) \%. b = a \%. b - \left(\left\lfloor \frac{a}{b} \right\rfloor * b \right) \%. b$$

$$(a \%. b) \%. b = a \%. b - 0$$

$$(a \%. b) \%. b = (a \%. b)$$

$(a \%. b) \%. b = (a \%. b)$ can be written as $a \%. b \equiv_b a$

from question 1a) ←

Hence $\boxed{a \%. b \equiv_b a}$

1c)

Prove that $(a_1 \% b) + (a_2 \% b) \equiv_b a_1 + a_2$ & $(a_1 \% b)(a_2 \% b) \equiv_b a_1 a_2$

I a) from 1b) we know,

$$a \% b \equiv a \pmod b$$

So,

$$a_1 \% b \equiv a_1 \bmod b \quad \text{—(i)}$$

$$a_2 \% b \equiv a_2 \bmod b \quad \text{—(ii)}$$

Add (i) & (ii)

$$(a_1 \% b) + (a_2 \% b) \equiv (a_1 + a_2) \bmod b$$

$$\boxed{(a_1 \% b) + (a_2 \% b) \equiv_b (a_1 + a_2)}$$

II) $(a_1 \% b)(a_2 \% b) \equiv_b a_1 a_2$

Multiplying (i) & (ii), we get

$$(a_1 \% b)(a_2 \% b) \equiv a_1 a_2 \bmod b$$

$$\boxed{(a_1 \% b)(a_2 \% b) \equiv_b a_1 a_2}$$

1d) Prove that

$$-a \equiv (b - a) \pmod b$$

$$\equiv_b b - a \equiv_b (b \% b) - (a \% b)$$

$$\equiv_b 0 - (a \% b)$$

$$\equiv_b -a$$

from $a_1 + a_2 \equiv_b (a_1 \% b) + (a_2 \% b)$

$$\boxed{\text{Hence } -a \equiv_b (b-a) \bmod b \text{ //}}$$

1e Using the above, compute $249^{16} \bmod 251$ without using numbers longer than three decimal digits.

$$
\begin{aligned}
& 249^{16} \bmod 251 \\
\equiv\ & (-2)^{16} \equiv (-2)^4 \cdot (-2)^4 \cdot (-2)^4 \cdot (-2)^4 \\
\equiv\ & 16 \cdot 16 \cdot 16 \cdot 16 \bmod 251 \\
\equiv\ & 256 \cdot 256 \bmod 251 \\
\equiv\ & 5 \cdot 5 \bmod 251 \\
\equiv\ & 5^2 \bmod 251 \\
\equiv\ & 25 \bmod 251
\end{aligned}
$$

$$\boxed{\equiv 25}$$ //

Please turn over

Problem 2

a)

Compute 5^{64} mode 19

first compute $5^2 \bmod 19$, $5^4 \bmod (19)$

i) $5^2 \bmod 19 \equiv 25 \bmod 19 \equiv 6$

ii) $5^4 \bmod 19 \equiv (5^2)^2 \bmod 19 \equiv 6^2 \bmod 19 \equiv 17$

iii) $5^8 \bmod 19 \equiv (5^2)^4 \bmod 19 \equiv (6^2)^2 \bmod 19 \equiv (17)^2 \bmod 19 \equiv -2^2 \equiv 4$

Now we can use (i), (ii), and (iii)

$$5^{64} \bmod 19 \equiv ((5^5)^5)^3 \bmod 19 \equiv ((5^4 \times 5^1)^8)^3 \equiv ((17^5 \times 5^5)^3$$

Now, we can use (i), (ii), and (iii)

$$5^{64} \bmod 19 \equiv ((5^8)^4)^2 \bmod 19$$

$$\equiv ((4)^4)^2 \bmod 19$$

$$\equiv (256)^2$$

$$\equiv 9^2$$

$$\equiv 81$$

$$\boxed{\equiv 5}$$

Hence $5^{64} \bmod 19 \equiv 5 \bmod 19$

2b)

Compute $5^{75} \mod 19$

$$5^{75} \mod 19 \equiv ((5^5)^5)^3 \mod 19$$

$$\equiv ((5^4 \times 5^1)^5)^3$$

$$\equiv ((17 \cdot 5)^5)^3$$

$$\equiv ((17^5 \cdot 5^5)^3)$$

$$\equiv ((-2^5 \cdot 5^5)^3)$$

$$\equiv [(-2^5) \cdot (5^4 \cdot 5^1)]^3$$

$$\equiv [(-32) \times 17 \times 5]^3$$

$$\equiv [-32 \times -2 \times 5]^3$$

$$\equiv [64 \times 5]^3$$

$$\equiv [7 \times 5]^3$$

$$\equiv [35]^3$$

$$\equiv 16^3 \equiv (-3)^3 \equiv (-27) \equiv 11$$

NO #2C)

Problem 3

a) for any integers $a \not\equiv_p 0$, r and s, if $ra \equiv_p sa$, then $r \equiv_p s$

Note: use the fact that

$$p \mid xy \text{ means } p \mid x \text{ or } p \mid y$$

If $ra \equiv_p sa \longrightarrow r \equiv_p s$

Given,

$ra \equiv_p sa$

$a \not\equiv_p 0 \iff p \nmid a$

To prove

$r \equiv p s$

We have,

- $ra \equiv_p sa$, which mean $p \mid (r-s)a$. $p \mid (r-s)$ or $p \mid a$??

From given $p \nmid a$, Hence $p \mid (r-s)$ — (*)

As $p \mid (r-s)$ from the (*), we can write this in terms of Congurent form.

$$p \mid (r-s) \iff r \equiv_p s$$

Hence $r \equiv_p s$

b) for any integer $a \not\equiv_p 0$, the values $a \% p$, $2a \% p$, $3a \% p$, ..., $(p-1)a \% p$ hit every element in the set $1, 2, 3, \ldots, p-1$ exactly once.

Please turn over

Given

$a \equiv_p 0$ from (1 a)

$a \% p \equiv_p a$

a can be any value from $1, \ldots, (p-1)$

Suppose we arbitarly select $a = 1$. This would still work for any a values as well.

$a = 1$

$2a \% p \equiv_p 2a \equiv_p 2 \times 1 \equiv_p 2$

$3a \% p \equiv_p 3a \equiv_p 3 \times 1 \equiv_p 3$

⋮

So on

$(p-1)\, a \% p \equiv_p (p-1)a \equiv_p (p-1) \times 1 \equiv_p (p-1)$

We have bijection between $\{a \% p, \ldots, (p-1)\, a \% p\}$ to $\{1, 2, \ldots, p-1\}$

As our a was arbitarly selected from $\{1, \ldots, p-1\}$. Any other a selected from the same set would also work.

3c) Fermat's little theorem : if $a \not\equiv_p 0$, then $a^{p-1} \equiv_p 1$

If $a \not\equiv_p 0 \longrightarrow a^{p-1} \equiv_p 1$

Using Hint given.

Multiplying all $p-1$ values.

using Part b)

$$a \times 2a \times 3a \times \cdots \times (p-1)a = 1 \times 2 \times 3 \times 4 \cdots \times p-1 \pmod p$$

Part b) said that there is bijection between $a \% p, \cdots (p-1)a \% p$

and set $1, 2, \ldots, p-1$ in some order.

Hence if we mod p in

$$a \times 2a \times 3a \times \cdots \times (p-1)a$$

we get,

$$1 \times 2 \times 3 \times \cdots \times p-1 \pmod p$$

or, $a \times 2a \times 3a \times \cdots \times (p-1)a = 1 \times 2 \times 3 \times \cdots \times p-1 \pmod p$

or, $a^{p-1} \times \prod_{i=1}^{p-1} i = (p-1)! \bmod p$

$a^{p-1} \times (p-1)! = (p-1)! \bmod p$

dividing both side by $(p-1)!$ using $ra \equiv_p sa \longrightarrow r \equiv_p s$

we get

$$a^{p-1} = 1 \bmod p$$

or, $a^{p-1} \equiv 1 \bmod p$

3(d) fer-ma or fur-ma

3e) Show that every non-zero element modulo p has an inverse

$a \in \{1, \ldots, p-1\}$

$\exists b \; ; \; ab \equiv_p 1$

$b = ?$

Using fermat's little Theorem

$$a^{p-1} = 1$$

or $a^{p-2} a = 1$ $\quad \therefore \; b = a^{p-2}$

or $a^{p-1} a^{-1} a = 1$

or $1 \; a^{-1} a = 1$ $\quad \therefore b = a^{-1} = a^{p-2}$

$$a^{-1} a \equiv_p 1$$

Hence there will always will be b which will be the inverse of element modulo p

(4)

Design a crypto scheme

- message length of S message space = $\{m_1, \ldots, m_S\}$

Suppose you have a message m_1

$m_1 =$ 1 3 5

1 → S length

for the Key $K \in \{1, \ldots, S\}$

Note
∴ Key length = message length
$= S$

any Key from our key space will have s length as message. So to encrypt our message (m_1) roll a dice with S faces S times

$m_1 =$ 1 3 5

K 3 4 ... 6

→ S length

Key was obtained by rolling a dice with S faces S times.

Now to <u>encrypt</u>

$$\text{Encrypt}(K, m_1) = (m_1 + K) \bmod S = C$$

To Decrypt

$$\text{Decrypt}(K, C) = (m_1 + K - K) \bmod S = m$$

This is litterally like OTP but instead of mod 2, we have mod S.

Perfectly secure

Encrypt (m)

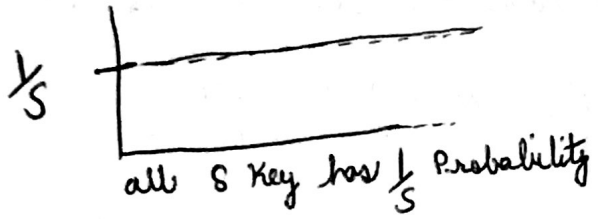
- Chooses K uniformly at random from

$K = \{1, \ldots, S\}$

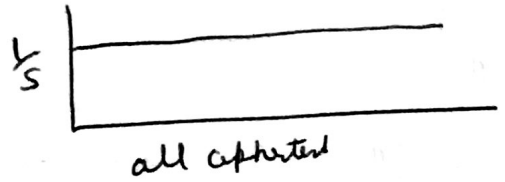
one key selected has length S

- output $(m + K) \bmod S$

Probability distribution of Key



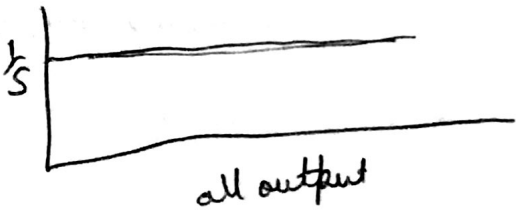
Probabilty dist of Ciphertx



random_ctxt

- output uniformly random S length of Cipher text

Probability distr of the output = 1/S



We cannot differentiate a given ciphertext is from encrypt(m) or random_ctxt. Thus, this scheme is perfectly secure.

5)

a) Are the orders securely encrypted - that is, can an eavesdropper Eve obtain any information about what is being traded from observing the messages from Bob to Alice? Why or Why not?

⇒ This is not secured as they are using key of one time pad several time. Eventually Eve would be able to figure out the message

Suppose

$$m_1 \oplus K = C_1$$

$$m_2 \oplus K = C_2$$

$$C_1 \oplus C_2 = m_1 \oplus m_2$$

He could Xor the ciphertext and easily obtain xored messages and slowly figure out the message as Alice & Bob keep on using that same key.

(b)

firstly, Moe won't know what the message contained. So, Eventhough Moe can change the cipher text, he won't be able to ~~change the Cipher text~~ change the message as he likes. If it is a buy order, Moe can't change it to a sell order. No, Moe can't change the order if he doesn't know whether it is buy or sell as he won't know what is there ciphertext encode. He won't even know these are for "buying & selling Stores" messages. OTP if used once is perfectly secure. Given any particular ciphertext, it can be encoded from any message from the message space.