11 July. NUMBER THEORY AND CRYPTOGRAPHY

- Number theory:

1. Divisibility : a|b : when b÷a, remainder = 0.
   eg : 4|8 : 8÷4, r = 0.
   ie : a divides b.

2. Non-divisibility : a∤b : a does not divide b.
   2∤7 : 7÷2, r ≠ 0.

3. Division Algorithm:
If two integers a & b exist, where b|a, it can be represented as:

$$a = bq + r \quad ; \quad 0 \leq r < b.$$

where q: quotient ; r: remainder.

for example: a=27 ; b=7.
$27 = (7 \cdot 3) + 6$.
a = -27 ; b = 4.
$-27 = (7 \times -4) + 1$.

Note: If we write $a = bq + r$, where $0 \leq r < b$, then b|a if & only if r=0.

4. Greatest Common Divisor (GCD):

d = GCD(a,b)
for example: a=12; b=18.
Divisors of: 12: {1, 2, 3, 4, (6), 12}.
18: {1, 2, 3, 4, (6), 9, 18}.
∴ GCD(12, 18) = 6.
GCD(3, 7) = 1.

Note: If GCD(a,b)=1, we can say that a is relatively prime to b; also called 'co-prime'.

5. Euclidian Algorithm:

For 2 non-negative integers a & b, assuming b≠0, [with a>b]:

$a = q_1 b + r_1$, with $0 \le r_1 < b$.

$b = q_2 r_1 + r_2$, with $0 \le r_2 < r_1$.

$r_1 = q_3 r_2 + r_3$, with $0 \le r_3 < r_2$.

⋮

$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$, with $0 \le r_{n-1} < r_{n-2}$.

$\Rightarrow r_{n-2} = q_n r_{n-1} + 0$.

$\therefore GCD(a,b) = r_{n-1}$.

For example: Compute GCD (123, 456):

$456 = 3 \times 123 + 87$.

$123 = 1 \times 87 + 36$.

$87 = 2 \times 36 + 15$.

$36 = 2 \times 15 + 6$.

$15 = 2 \times 6 + 3$.

$6 = 2 \times 3 + 0$

$\therefore GCD(123, 456) = 3$.

Or compute GCD (654, 321):

$654 = 2 \times 321 + 12$.

$321 = 26 \times 12 + 9$.

$12 = 1 \times 9 + 3$.

$9 = 3 \times 3 + 0$

$\therefore GCD(654, 321) = 3$.

6. Extended Euclidian Algorithm:

$sa + bt = GCD(a,b)$.

Compute GCD(12,34) using extended Euclidian Algorithm; Also compute s & t.

GCD(12,34):

$34 = 2 \times 12 + 10$. $\Rightarrow 10 = 34 - 2 \times 12$ (2).

$12 = 1 \times 10 + 2$ (2) $\Rightarrow 2 = 12 - 1 \times 10$ (1).

$10 = 5 \times 2 + 0$.

GCD(12,34) = (2).

Sub (2) in (1):

$2 = 12 - 1 \times 10$.

$2 = 12 - 1(34 - 2 \times 12)$

$2 = 12 - 34 + 2(12)$.

$2 = 3(12) + 34(-1)$.

$\Rightarrow s = 3$; $t = -1$.

Qn. GCD(14,5) & find s & t.

$14 = 2 \times 5 + 4$ $\Rightarrow 4 = 14 - 2 \times 5$ (2).

$5 = 1 \times 4 + 1$ (1). $\Rightarrow 1 = 5 - 1 \times 4$ (1)

$4 = 4 \times 1 + 0$

Sub (2) in (1): $1 = 5 - 1(14 - 2(5)) = 5 - 14 + 2(5)$

$1 = 3(5) + 14(-1)$.

$\therefore GCD(14,5) = 1$; $s = -1$, $t = 3$.

To do: Textbook: 2.4.3 Computer Explorations: Exercise: Qn 3, 4.

__/__/____

18 July

4. Congruence: $a \equiv b \pmod{m}$.

2 integers a & b are congruent if $a-b$ is a multiple of m. (m is true).

Eg: $7 \equiv 1 \pmod 2$.

$\Rightarrow 7-1 = 6 \,\%\, 2 = 0$ ✓.

$14 \equiv 0 \pmod 2$.

$\Rightarrow 14-0 = 14 \,\%\, 2 = 0$ ✓.

$19 \equiv 7 \pmod 6$

$\Rightarrow 19-7 = 12 \,\%\, 6 = 0$ ✓.

$-8 \equiv 12 \pmod 5$.

$\Rightarrow -8-12 = -20 \,\%\, 5 = 0$ ✓.

$4 \equiv 4 \pmod{11}$.

$\Rightarrow 4-4 = 0 \,\%\, 11 = 0$ ✓.

$6 \equiv 16 \pmod 5$

$\Rightarrow 6-16 = -10 \,\%\, 5 = 0$ ✓.

$34 \equiv 12 \pmod{11}$

$\Rightarrow 34-12 = 22 \,\%\, 11 = 0$ ✓.

$7 \equiv -2 \pmod 3$.

$\Rightarrow 7--2 = 9 \,\%\, 3 = 0$ ✓.

$-11 \equiv 3 \pmod 7$.

$\Rightarrow -11-3 = -14 \,\%\, 7 = 0$ ✓.

n is even if $n \equiv 0 \pmod 2$. [$n \bmod 2 = 0$].

n is odd if $n \equiv 1 \pmod 2$. [$n \bmod 2 = 1$].

a & b are congruent mod 10 if their last digit are the same; a & b are congruent mod 100 if their last 2 digits are the same.

ie: $2347 \equiv 7 \pmod{10}$. ✓.

$65931 \equiv 31 \pmod{100}$. ✓.

$4 \equiv 4 \pmod 8$; $12 \equiv 4 \pmod 8$; $20 \equiv 4 \pmod 8$; $28 \equiv 4 \pmod 8$.

$a \equiv b \pmod m$ if & only if

$a = b + km$

for some integer k.

* Properties of Congruences:

1. $a \equiv b \pmod m$ if $m \mid (a-b)$.
2. $a \equiv b \pmod m$ implies $b \equiv a \pmod m$.
3. $a \equiv b \pmod m$ & $b \equiv c \pmod m$ imply $a \equiv c \pmod m$.

Congruence classes mod m:

For example: $m = 5$:

$0 \bmod 5 = \{\dots -10, -5, 0, 5, 10, 15, \dots\}$.

$1 \bmod 5 = \{\dots -9, -4, 1, 6, 11, 16, \dots\}$.

$2 \bmod 5 = \{\dots -8, -3, 2, 7, 12, 17, \dots\}$.

$3 \bmod 5 = \{\dots -7, -2, 3, 8, 13, 18, \dots\}$.

$4 \bmod 5 = \{\dots -6, -1, 4, 9, 14, 19, \dots\}$.

$\therefore m = 5$ has five congruence classes.

One set consists of all the integers that are congruent to $0 \bmod m$, another of $1 \bmod m$, then $2 \bmod m$, upto $m-1 \bmod m$.

These sets are called congruence classes mod m.

Residue classes:

A set of integers $a_1, a_2, \dots, a_m$ is called a complete system of residues modulo m, if the set contains exactly one element from each residue class modulo m.

Eg: $m = 5$: $\{-10, 11, 2, -7, 9\}$ is a complete system of residues modulo 5.

* Reduced Residue Systems:
Let $[a]_m$ be a residue class modulo m. We say that $[a]_m$ is relatively prime to m if each element in $[a]_m$ is relatively prime to m.

Ex: Find all congruence classes, 5 complete system of residue class mod 10 and all reduced residue class modulo & also least residue mod 10.

m = 10: (R_{10})
0 mod 10: {... -20, -10, 0, 10, 20, 30, ...}.
1 mod 10: {..., -19, -9, 1, 11, 21, 31, ...}. reduced
2 mod 10: {..., -18, -8, 2, 12, 22, 32, ...}.
3 mod 10: {..., -17, -7, 3, 13, 23, 33, ...}. reduced
4 mod 10: {..., -16, -6, 4, 14, 24, 34, ...}.
5 mod 10: {..., -15, -5, 5, 15, 25, 35, ...}.
6 mod 10: {..., -14, -4, 6, 16, 26, 36, ...}.
7 mod 10: {..., -13, -3, 7, 17, 27, 37, ...}. reduced
8 mod 10: {..., -12, -2, 8, 18, 28, 38, ...}.
9 mod 10: {..., -11, -1, 9, 19, 29, 39, ...}. reduced

Complete system of residue class mod 10:
1: {0, -9, 12, 33, -16, -5, 7, -2, -11, -19}.
2: {-20, 1, 22, -17, -36, -15, 26, 37, 8, 9}.
3: {20, -8, 13, 24, 15, 36, -3, -12, -1}.
4: {30, 11, 32, -7, 34, 25, 6, -13, 18, 19}.
5: {10, 21, -18, 03, 24, 35, 16, 17, 38, 39}.

Reduced Residue class modulo:

Least residue modulo m:
{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}.

* Least Residue Modulo m:
Set of all of these least (non-ve) residues.
Complete residue class with least number (non-ve).
~~The set of Zm is the set of~~ $^{m=5}$ = {0, 1, 2, 3, 4}.

22 July

Operations on Z_n.

Qn. Subtract 11 from 7 in Z_{13}.
Qn. Multiply 11 by 7 in Z_{20}.

Solutions: Sub: ~~7-11~~ 7-11 = -4 ⇒ -4 mod 13 = ~~9~~ 9.

Multi: 11 × 7 = 77 - 20 = 14.

Qn: a. Add 14 To 27 in Z_{14}.
b. Sub 43 from 12 in Z_{13}.
c. Multi 123 by -10 in Z_{19}.

Solutions: a. Add: (14+27) %. 14 = 41 mod 14 = 2.
b. Sub: (12-43) %. 13 = -31 mod 13 = 8.
c. Multi: 123 · -10 %. 19 = -1230 mod 19 = 5

* Properties:

1. (a+b) mod m = [(a mod m) + (b mod m)] mod m.
2. (a-b) mod m = [(a mod m) - (b mod m)] mod m.
3. (a×b) mod m = [(a mod m) × (b mod m)] mod m.
4. a^n (mod m) =

__/__/__

Eg: ~~##~~ $11^4 \bmod 13$:

$11^2 = 121 \equiv 4 \pmod{13}$

$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$.

$11^4 = 11 \times 11^2 \times 11^4$

$11^4 = 11 \times 1 \times 3 \equiv 132 \equiv 2 \pmod{13}$.

Qn. Compute $3^{385} \pmod{479}$. ⇒ 327.

~~3^{385} ⇒ $3^5 = 243$. mod 479 = 243.~~

$3^{385} \Rightarrow 3^3 = 27. \Rightarrow 3^5 = 243. \Rightarrow 3^6 = 729.$

~~3^6 mod 479 = 250.~~

~~$3^{385} = 3 \times 3^{384} = 3 \times (3^6)^{64}$.~~

~~3^6~~ $250^2 =$ ~~3^{12}~~ $= 62500 \bmod 479 = 230.$

$(3^6)^3 = 250^3 = 15625000 \bmod 479 = 20.$

$(3^5)^2 = 243^2 = 59049 \bmod 479 = 132.$

$3^{385} = 3^{216} + 3^{36} + 3^{36} + 3^{36} + 3^{36} + 3^{25}$.

$= (20 \times 230 \times 230) \times (230 \times 230 \times 132)$

$= 368 \cdot 417 = 146$ ✗ correct is 327.

Qn. Compute $7^{256} \bmod 13$. ⇒

$7^2 = 49 \cdot 1 \cdot 13 = 10.$

$(7^2)^5 = 7^{10} = 10^5 = 4.$

$(7^{2\cdot5})^{10} = 4^{10} = 9.$

$(((7^{2\cdot5})^{10})^2 = 9^2 = 3$ → 200

$(7^{2\cdot5})^5 = 10$ → 50

$7^6 = 12.$

$\therefore 7^{256} \cdot 1 \cdot 13 = 3 \cdot 10 \cdot 12 \cdot 1 \cdot 13$

$= 9$

__/__/____

* Identity element: e:

Additive : $e = 0$. $a + e = e + a = a$.

Multiplicative: $e = 1$. $a \times 1 = 1 \times a = a$.

Additive Modulo: $m = 5$.

+	0	1	2	3	4
0	(0)	1	2	3	4
1	1	2	3	4	(0)
2	2	3	4	(0)	1
3	3	4	(0)	1	2
4	4	(0)	1	2	3

Multiplicative Modulo: $m = 5$.

*	0	1	2	3	4
0	0	0	0	0	0
1	0	(1)	2	3	4
2	0	2	4	(1)	3
3	0	3	(1)	4	2
4	0	4	3	2	(1)

$(2 \times 3) \bmod 5 = 1$.

$2^{-1} \bmod 5 = 3$.

$3^{-1} \bmod 5 = 2$.

$2 \times 3 \equiv 1 \bmod 5$.

∴ Pairs: (2,3), (3,2) (4,4), (1,1). ← Multiplicative.

Pairs: (0,0), (1,4), (4,1), (2,3), (3,2). ← Additive.

Qn. Find all additive inverse pairs & multiplicative inverse pairs for mod 10 operation.

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

*	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Additive inverse pairs:

(0,0), (9,1), (8,2), (7,3), (6,4), (5,5), (4,6), (3,7), (2,8), (1,9).

Multiplicative inverse pairs:

(1,1), (7,3), (3,7), (9,9).

Qn. $5x \equiv 1 \bmod 14$, find x. OR $5^{-1} \bmod 14$.

$sa + bt = GCD(a,b)$

GCD(5,14) ⇒ $14 = 2 \times 5 + 4$. ⇒ $4 = 14 - 2(5)$

$5 = 1 \times 4 + 1$. ⇒ $1 = 5 - (4)1$.

$4 = 4 \times 1 + 0$.

$\therefore$ GCD = 1

$1 = 5 - (4)1 = 5 - 14 - 2(5) = 3(5) + 14(-1)$.

$\therefore s = 3$; $t = -1$.

$\Rightarrow 5^{-1} \bmod 14 = 3$.

$\Rightarrow 5 \times 3 \bmod 14 = 15 \bmod 14 = 1$.

Qn. $40x \equiv 1 \bmod 7$, find x or $40^{-1} \bmod 7$.

$sa + bt = GCD(a,b)$.

GCD(40,7) = $40 = 5 \times 7 + 5$. ⇒ $5 = 40 - 7(5)$. - (3)

$7 = 1 \times 5 + 2$. ⇒ $2 = 7 - 5(1)$ - (2)

$5 = 2 \times 2 + 1$ ⇒ $1 = 5 - 2(2)$. - (1)

$2 = 1 \times 2 + 0$.

$\therefore$ GCD(40,7) = 1.

Sub (3) in (2): $2 = 7 - 40 + 7(5) = 6(7) - 40$.

Sub result in (1): $1 = 5 - 12(7) + 2(40)$.

$1 = 40 - 5(7) - 12(7) + 2(40)$.

$= 3(40) - 17(7)$.

$\therefore s = (3)$; $t = (-17)$.

$\therefore$ ~~$7^{-1} \bmod$~~ $40^{-1} \bmod 7 = 3$.

~~$40 \times 3 \bmod 7$~~ $= 120 \bmod 7 = 3$.

21 July.

__/__/____

* Fermat's Theorem:

If p is prime and 'a' is a +ve integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

$\Rightarrow$ GCD(a, p) = 1.

Qn. 7^{200} by 23; what is the remainder.

$7^{23-1} \equiv 1 \pmod{23}$.

$7^{22} \equiv 1 \pmod{23}$.

GCD(23, 7) = 1. $\quad a = 7, p = 23$.

$\rightarrow 7^{22} \pmod{23} = 1$.

$(7^{22})^2 = 1^2 = 1 \cdot \text{mod } 23 = 1$

$(7^{22})^3 = 1^3 = 1 \text{ mod } 23 = 1$.

$\therefore 7^{200} = (7^{22})^3 \times (7^{22})^3 \times (7^{22})^3 \times 7 \times 7$.

$= 1 \times 1 \times 1 \times 7 \times 7 = 49 \pmod{23} = \underline{3}$.

Qn. $2^{104} \text{ mod } 101$.

$2^{101-1} \equiv 1 \pmod{101}$.

$2^{100} \equiv 1 \pmod{101}$.

GCD(2, 100) = 1.

$\rightarrow$ ~~$2^{104} \pmod{101} = 1$.~~

$2^{104} = 2^{100} \times 2^4$.

$= 1 \times 16 = 16 \pmod{101} = \underline{16}$.

__/__/____

25 July.

* **Euler's Theorem:**

Let n be a +ve integer. The Euler-ϕ function $\phi(n)$, also called Euler's Totient function, is the number of integers j with $1 \leq j \leq n$ such that $GCD(j,n)=1$.

For example: $\phi(2)$: $n=2 \Rightarrow j=1$. $j \neq 2$ [$\because GCD(2,2) \neq 1$]
$=1$. $GCD(1,2)=1$.

$\phi(3)$: $n=3 \Rightarrow j=1,2$. $j \neq 3$ [$\because GCD(3,3) \neq 1$].
$=2$. $GCD(1,3)=1$; $GCD(2,3)=1$.

$\phi(4)$: $n=4 \Rightarrow j=1,3$.
$=2$. $GCD(1,4)=1$; $GCD(3,4)=1$.

$\phi(12)$: $n=12 \Rightarrow j=1,5,7,11$.
$=4$. $GCD(1,12)=1$; $GCD(5,12)=1$; $GCD(7,12)$; $GCD(11,12)$

Note: If p is prime, then $\phi(p) = p-1$.

Proposition: Let m,n be positive integers. If $GCD(m,n)=1$, then

$$\phi(mn) = \phi(m) \cdot \phi(n).$$

For example: $\phi(21) = \phi(3) \cdot \phi(7) = \phi(3-1) \cdot \phi(7-1) = 2 \cdot 6 = 12$.
$\phi(12) = \phi(4) \cdot \phi(3) = 2 \cdot (3-1) = 2 \cdot 2 = 4$.

Proposition: If p is a prime number and $k \geq 1$, then

$$\phi(p^k) = p^k - p^{k-1}.$$

$\phi(100) = \phi(10^2) = \phi(2^2) \cdot \phi(5^2) = (2^2-2^1) \cdot (5^2-5^1)$
$= (4-2) \cdot (25-5) = 2 \cdot 20 = 40$.

__/__/____

* Eulers Theorem:

Theorem: Let n be a +ve integer and b be an integer with GCD(b,n) = 1. Then

$$b^{\phi(n)} \equiv 1 \pmod{n}.$$

If n is prime, $b^{n-1} \equiv 1 \pmod{n}$.
[Fermat's Theorem].

Qn. Find the remainder when:

a. 3^{100} is divided by 7.

n = 7. → prime.

$3^{7-1} \equiv 1 \bmod 7.$

$3^6 \equiv 1 \bmod 7.$

$(3^6)^5 \bmod 7 = 1.$ ⇒ $3^{30}.$

$3^{100} = 3^{30} \cdot 3^{30} \cdot 3^{30} \cdot 3^6 \cdot 3^2 \cdot 3^2.$

$= 1 \cdot 1 \cdot 1 \cdot 1 \cdot 9 \cdot 9 = 81 \bmod 7$

$3^{100} = \underline{\underline{4}}.$

b. 7^{20} is divided by 21.

n = 21. ⇒ not prime.

$\phi(21) = \phi(3) \cdot \phi(7) = 2 \cdot 6 = 12.$

$7^{12} = 1 \bmod 21.$

$7^4 = 7.$

$7^{20} \pmod{21} = 7$

6 Aug.

* Wilson's Theorem:

Let p be prime, then

$$(p-1)! \equiv -1 \pmod{p}.$$

For example: $p = 7$.

$$(p-1)! = 6! = 720 \equiv -1 \pmod{7}.$$

$$\Rightarrow 6! = 6(5\cdot4)(3\cdot2)(1) \pmod{7}.$$
$$= (-1)(1)(1)(1) = -1$$

Corollary:
Let $n \geq 2$ be an integer. Then, n is prime if

$$(n-1)! \equiv -1 \pmod{n}.$$

Eg: $n = 6$.
Check if n is a prime or not:

$$5! \equiv -1 \pmod{6} \; ?$$

$$\Rightarrow 120 \equiv -1 \pmod{6} \; ?$$
$$120 \bmod 6 \equiv 0.$$
$\therefore$ No. 6 is not a prime number.

$n = 13$.

$$12! \equiv -1 \pmod{13}.$$
$$12(11\cdot10)(9\cdot8)(7\cdot6)(5\cdot4)(3\cdot2)(1)$$
$$= 12\cdot(6\cdot7)(8\cdot7)\cdot(6\cdot1) = (12\cdot8)\cdot(8\cdot6) = 10\cdot9$$
$$= 90 \bmod 13 = -1$$
. Yes, 13 is prime.

* Chinese Remainder Theorem (CRT):

Used to solve a set of congruent equations with one variable but different moduli.

$x \equiv a_1 \bmod m_1$.
$x \equiv a_2 \bmod m_2$.
:
$x \equiv a_k \bmod m_k$.

1. Find $M = m_1 \times m_2 \times m_3 \times \dots \times m_k$.
2. Compute $M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \dots, M_k = \frac{M}{m_k}$.
3. Find the multiplicative inverse of $M_1, M_2, M_3, \dots$ using corresponding moduli $m_1, m_2, \dots, m_k$ called $M_1^{-1}, M_2^{-1}, \dots, M_k^{-1}$.
4. $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \dots + a_k M_k \times M_k^{-1}) \bmod M$

Or. Find the solution:

$x \equiv 2 \bmod 3$.
$x \equiv 3 \bmod 5$.
$x \equiv 2 \bmod 7$.

3, 5, 7 are relatively prime ✓.

1. $M = 3 \times 5 \times 7 = 105$.
2. $M_1 = \frac{105}{3} = 35$. $M_2 = \frac{105}{5} = 21$. $M_3 = \frac{105}{7} = 15$.
3. $M_1^{-1} = 2$. $M_2^{-1} = 21^{-1} \bmod 5 = 1$. $M_3 = 15^{-1} \bmod 7 = 1$.
4. $x = (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1)$
   $x = (140 + 63 + 30) = 233 \bmod 105$.
   $\therefore x = 23$ //.

Qn. Find x such that

$3x \equiv 4 \pmod{10}$.

↳ connect it to : $x \equiv (1)?\ \mod 10$.

Qn. Program :

Solve the simultaneous congruences :

$n \equiv 0 \pmod 4$, $n \equiv -1 \pmod 9$,

$n \equiv -2 \pmod{25}$, $n \equiv -3 \pmod{49}$, $n \equiv -5 \pmod{121}$.

to find 6 consecutive integers that are not squarefree.

$3x \equiv 4 \pmod{10}$.

$7(3x) \equiv 7 \cdot 4 \mod 10 = 9$.

$21x \equiv \#9 \mod 10 = 9$.

$x \equiv 9 \pmod{10}$.

4 Aug.

* ~~Fi~~ Fields :

A field F, $\{F, +, *\}$, is a set of elements with two binary operations, called addition & multiplication, such that $\forall\ a, b, c$ in F, ~~the~~ closure, associative, identity, inverse and commutative are obeyed under addition; closure, associativity, distribution, commutative, ~~multi~~ identity, inverse & no zero divisor ($a \cdot b = 0$, then $a = 0$ or $b = 0$)

Qn. Check whether $(Z_3, +, *)$ is a fin. field.

Since 3 is a prime $(n-1) = 0, 1, 2$.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Addition:

Closure - $a \pmod 3 = 1$, or 2, or 0. ✓

Associative - $(a+b)+c = a+(b+c)$ ✓.

Identity - $e=0$. ✓

Inverse - $0 \to 0$, $2 \to 1$, $1 \to 2$. ✓

Commutative - $2+0, 0+2 = 2$; $2+1, 1+2 = 3 \bmod 3 = 0$, ✓

Multiplicative:

Closure - 0×2, 2×1 ✓.

Associative -

Distributive -

Commutative -

Inverse -

Identity -

Fields.

- Finite or Fields with an infinite number of elements
- Finite fields.
  - GF(p) Finite fields of order p. $\{0, 1, \dots, (p-1)\}$. $(+ \& *)$.
  - $GF(p^n)$ Finite fields with p^n elements.

GF(p):

GF(2): {0,1} (+,*)
GF(5): {0,1,2,3,4} (+, *)

GF(p^n):

GF(2^2): {00, 01, 10, 11}. {+,*}.

8 Aug.

Order (G) - Order of a group.
Number of element in a group.

Order (element) - Order of an element in a group.
For an element a, the order i is the number that satisfies:

$$a^i \bmod p = e.$$

Where a - element, i - order, p - prime number.
e - identity element.

$\langle Z_7^*, * \rangle$.

		i=1	i=2	i=3	i=4	i=5	i=6
ord(1) = 1.	a=1	$1^1 \bmod 7 = 1$	$1^2 \bmod 7 = 1$	1	1	1	1
ord(2) = 3.	a=2	$2^1 \bmod 7 = 2$	$2^2 \bmod 7 = 4$	1	2	4	1
ord(3) = 6.	a=3	3	2	6	4	5	1
ord(4) = 3.	a=4	4	2	1	4	2	1
ord(5) = 6.	a=5	5	4	6	2	3	1
ord(6) = 2.	a=6	6	1	6	1	6	1

$\phi(n) = \phi(7) = 6$. order(G) = $\phi(n)$.

__/__/___

3 is a primitive root of group Z_7.
Because all the elements in a=3 are different & non repeating.
5 is also a primitive root.
Here, the identity element will only be at i=6.

Number of primitive roots of a group: $\phi(\phi(n))$

$\phi(\phi(n)) = \phi(6) = \phi(3) \cdot \phi(2) = 2 \cdot 1 = 2$.

Each primitive root is a generator.

~~q=3 →~~ $Z_7^* = \{3^1 \bmod 7, 3^0 \bmod 7, 3^2 \bmod 7, 3^4 \bmod 7, 3^5 \bmod 7, 3^6 \bmod 7\}$.

q=5 → $Z_7^* = \{5^1 \bmod 7, 5^2 \bmod 7, 5^3 \bmod 7, 5^4 \bmod 7, 5^5 \bmod 7, 5^6 \bmod 7\}$.

The group $G = \langle Z_n^*, * \rangle$ has primitive roots only if n is $2, 4, p^t, 2p^t$.

Eg: $\langle Z_{17}^*, * \rangle$ whose 17 can be represented as $p^t = 17^1$; p is a prime number.
So $\langle Z_{17}^*, * \rangle$ has a primitive roots.

Qn. $\langle Z_{20}^*, * \rangle$. No:
$\langle Z_{38}^*, * \rangle$ Yes. $2(19)^1$. $2p^t$.
$\langle Z_{50}^*, * \rangle$. Yes. $2(5)^2$. $2p^t$.

* Cyclic Group: If a group has a primitive root, it is known as a cyclic group.

ex. For the group $\langle Z_{19}^*, * \rangle$;
a. find the order of group.
b. find the order of each element in the group.
c. find the number of primitive roots in the group.
d. find the primitive roots in the group.
e. show that the group is cyclic.

Soln: a. Order of $Z_{19}) = \phi(n) = \phi(19) = \underline{18}$.

b. Order(1) = 1. Order(2) = 18. Ord(3) = 18.
Ord(4) = 9. Ord(5) = 9. Ord(6) = 9.
Ord(7) = 3. Ord(8) = 6. Ord(9) = 9.
Ord(10) = 18. Ord(11) = 3. Ord(12) = 6.
Ord(13) = . Ord(14) = . Ord(15) = .
Ord(16) = . Ord(17) = . Ord(18) = .

c. $\phi(\phi(n)) = \phi(18) = \phi(6) \cdot \phi(3) = 2 \cdot 2 = 4$.

18 Aug.

Questions for Practice:

- Euler's Theorem:

$145^{102} \bmod 101$.

$10^{-1} \bmod 101$ using Fermat's Theorem.

- CRT:

a) $x \equiv 7 \cdot 13$. b) $x \equiv 4 \cdot 5$.
$x \equiv 11 \cdot 12$. $x \equiv 10 \cdot 11$.

23 Aug.

__/__/____

* Quadratic Residues:

In the eqn $x^2 \equiv a \pmod p$, a is QR if the eqn has 2 solutions and a is called quadratic non-residue (QNR) if the eqn has no solutions.

If a is a square mod p, we say that a is a Quadratic Residue mod p.

For example:

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

QR = $\{1, 3, 4, 9\}$ QNR = $\{2, 5, 6, 7, 8, 10\}$.

$a = 1$: $x^2 \equiv 1 \bmod 11$.

$x^2 \bmod 11 = 1$.

When $x = 1$, $1^2 \bmod 11 = 1$.

$\mathbb{Z}_{11}^{*2} = \{1, 4, 9, 16, 25, 36, 49, 64, 81, 100\}$.

$\bmod 11 = \{1, 4, 9, 5, 3, 3, 5, 9, 4, 1\}$.

QR = $\{1, 3, 4, 5, 9\}$.

QNR = $\{2, 6, 7, 8, 10\}$.

Proposition: Let p be an odd prime & let $a \not\equiv 0 \bmod p$.
Then $a^{(p-1)/2} \equiv \pm 1 \pmod p$.
Moreover, a is a square mod p $\iff a^{(p-1)/2} \equiv 1 \pmod p$. (p if & only if)

Proof:

Let $b \equiv a^{(p-1)/2} \bmod p$

$b^2 \equiv a^{(p-1)} \bmod p$.

By Fermat's theorem:

$b^2 \equiv a^{p-1} \equiv 1 \bmod p \quad (\because a^{p-1} \equiv 1 \bmod p)$.

$b^2 \equiv 1 \bmod p$.

$b \equiv \pm 1 \bmod p$.

$\Rightarrow a^{(p-1)/2} \equiv \pm 1 \bmod p$.

If a is a square mod p, we can say:

$x^2 \equiv a \pmod p$, for some x.

So, $a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \pmod p \equiv 1 \pmod p$.

By Fermat's theorem:

$a^{p-1} \equiv 1 \pmod p$.

$\therefore a^{(p-1)/2} \equiv 1 \pmod p$.

* Legendre Symbol:

Let p be an odd prime & let a be an integer with $a \not\equiv 0 \pmod p$ define the Legendre Symbol $\left(\frac{a}{p}\right)$:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{if } x^2 \equiv a \pmod p \text{ has a solution.} \\ -1, & \text{if } x^2 \equiv a \pmod p \text{ has no solution.} \end{cases}$$

Eg:

$\left(\frac{1}{11}\right), \left(\frac{2}{11}\right), \left(\frac{3}{11}\right), \left(\frac{4}{11}\right), \left(\frac{5}{11}\right), \left(\frac{6}{11}\right), \left(\frac{7}{11}\right), \left(\frac{8}{11}\right), \left(\frac{9}{11}\right), \left(\frac{10}{11}\right)$

__/__/____

Proposition: Let p be an odd prime & let $a, b \not\equiv 0 \pmod{p}$. Then,

a) Euler's Criterion:

$$\frac{a}{p} \equiv a^{(p-1/2)} \pmod{p}.$$

b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

$a^{(p-1/2)} \bmod p \times b^{(p-1/2)} \bmod p$

$a^{(p-1/2)} \times b^{(p-1/2)} \pmod{p}$

$ab^{(p-1/2)} \bmod p$.

$\frac{ab}{p}$..

c) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

d) $\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$

$\left(\frac{a}{p}\right) = a^{(p-1/2)} \bmod p$.

$\left(\frac{-1}{p}\right) = (-1)^{p-1/2} \pmod{p}$.

Case 1: $\left(\frac{p-1}{2}\right)$ is even.

$\frac{p-1}{2} = 2k$. , k is some integer.

$p-1 = 4k$.

$p = 4k+1 \Rightarrow p \equiv 1 \pmod 4$.

Case 2: $\frac{p-1}{2}$ is odd.

$\frac{p-1}{2} = 2k+1$.

$\Rightarrow p-1 = 4k+2 \Rightarrow p = 4k+3$.

$\Rightarrow p \equiv 3 \pmod 4$.

__/__/____

* Quadratic Reciprocity:

a) Let p & q be distinct odd primes. Then

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right).$$

In other words:

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{, if atleast one of } p,q \text{ is } 1 \pmod 4. \\ -\left(\frac{p}{q}\right) & \text{, if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

c) Let p be an odd prime. Then,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \text{, if } p \equiv 1, 7 \pmod 8. \\ -1 & \text{, if } p \equiv 3, 5 \pmod 8 \end{cases}$$

Eg: $\left(\frac{8}{13}\right) = ?$

$$\frac{8}{13} = \frac{2\times2\times2}{13} = \frac{2^2\times2}{13} = \frac{2^2}{13}\cdot\frac{2}{13} = +1.$$

$\rightarrow x^2 \equiv 2^2 \pmod{13}$.

$2^2 \equiv 2^2 \pmod{13}$.

$\left(\frac{10}{13}\right) = ?$

$$\frac{10}{13} = \frac{2\times5}{13} = \frac{2}{13}\cdot\frac{5}{13}$$

$\rightarrow a^{p-1/2} \bmod p$.

$5^{13-1/2} \bmod 13$

$= 5^6 \bmod 13 = 12 \bmod 13$

$= -1.$

$$\frac{10}{13} = -1\times-1 = +1.$$

Qn. Does $x^2 \equiv 19 \pmod{101}$ have any solution?

Qn. Evaluate $\frac{1272}{43}$.

$1272 \pmod{43} \equiv 25 \pmod{43} \Rightarrow \frac{1272}{43} = \frac{25}{43}$.

$\frac{25}{43} \cdot \left(\frac{5}{43}\right)^2$ $a^{(p-1)/2} \bmod p$

$5^{43-1/2} \bmod 43$.

$5^{21} \bmod 43$.

__/__/__

Evaluate Legendre Symbol of $\frac{319}{7}$.

* Jacobi Symbol:

Let m be a positive odd integer.
Write the prime factorization of m as:

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

Let GCD $(b, m) = 1$. Define the Jacobi Symbol

$$b/m = (b/p_1)^{a_1} (b/p_2)^{a_2} \cdots (b/p_r)^{a_r}.$$

where b/p_i is the Legendre Symbol.

$\frac{2}{15}$: $p = 15$, $b = 2$.

$\frac{2}{5 \times 3}$.

$15 = 5^1 \times 3^1$.

$\frac{2}{15} = \left(\frac{2}{5}\right)^1 \times \left(\frac{2}{3}\right)^1 = -1 \times -1 = +1.$

$\frac{2}{75} = \frac{2}{3 \times 5 \times 5} = \frac{2}{3} \times \left(\frac{2}{5}\right)^2 = -1 \times (-1)^2 = -1$.

19 Aug

* Gauss's Lemma:

Let p be an odd prime and let $a \not\equiv 0 \pmod p$. Let n be the number of integers in the set $\{a, 2a, 3a, \ldots, \frac{(p-1)}{2}a\}$ that are congruent to an integer bw $p/2$ & p, then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

For example: $p = 11$ $a = 7$. $\left(\frac{p-1}{2}\right) = \left(\frac{11-1}{2}\right) = 5$.

$\{7, 2(7), 3(7), 4(7), 5(7)\} \bmod p\,(11)$.

$\Rightarrow \{7, 3, 10, 6, 2\}$.

$p/2 = 11/2 = 5$. So (5 to 11):

$\{7, 10, 6\}$. $\therefore n = 3$.

$\therefore \left(\frac{7}{11}\right) = (-1)^3 = -1$

Proof:

Assume $a \not\equiv 0 \pmod p$, $GCD(a, p) = 1$.

Let $s = \{a, 2a, 3a, \ldots, \frac{(p-1)}{2}a\}$.

None of the integers in s is congruent to 0

[$\because j \equiv 0 \bmod p$ or $a \equiv 0 \bmod p$ is not satisfied ; $1 \le j \le \left(\frac{p-1}{2}\right)$].

None of the elements in s are congruent to e/o.

[$\because$ $ra \equiv sa \pmod p$; $1 \le s$; $s \le \left(\frac{p-1}{2}\right)$.

$r \not\equiv s \pmod p$; $\because GCD(a, p) = 1$.

are not ~~possible~~ satisfied]

For example: $a = 5$. $p = 13$. $\left(\frac{p-1}{2}\right) = \left(\frac{13-1}{2}\right) = 6$.

$s = \{5, \underline{10}, 2, \underline{7}, \underline{12}, 4\}$. $\Rightarrow n = 3$ [$\because \{10, 7, 12\}$].

Let $r_1, r_2, \cdots, r_m$ be those remainders upon divisibility by p; $0 < r_i < p/2$.

$r = \{5, 2, 4\}$. $\quad s = \{10, 7, 12\}$.

& $s_1, s_2, \cdots, s_n$ be those $p/2 < s_i < p$.

So, $(m+n = \frac{p-1}{2})$.

So. $r_1, r_2, r_3, \cdots, r_m, p-s_1, p-s_2, \cdots, p-s_n$ are positive & less than $p/2$ and none of them are congruent to each other.

$r = \{5, 2, 4\}$.

$s = \{10, 7, 11\}$.

$p-s = \{3, 6, 1\}$.

Combining & of r & $p-s$, we get 1 to $\frac{p-1}{2}$.

$$\therefore \left(\frac{p-1}{2}\right)! = (r_1)(r_2)(r_3)\cdots(r_m)(p-s_1)(p-s_2)\cdots(p-s_n).$$

Since $p \equiv 0 \pmod p$: $(p-s_i) \equiv -s_i \pmod p$.

$$\left(\frac{p-1}{2}\right)! \equiv (r_1)(r_2)(r_3)\cdots(r_m)(-s_1)(-s_2)\cdots(-s_n).$$
$$\equiv (-1)^n (r_1 \cdot r_2 \cdot r_3 \cdots r_m)(s_1 \cdot s_2 \cdots s_n).$$
$$\equiv (-1)^n \{a, 2a, 3a, \cdots, \left(\tfrac{p-1}{2}\right)a\} \bmod p.$$

Taking a outside:

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a^{\left(\frac{p-1}{2}\right)} \{1, 2, 3, \cdots, \left(\tfrac{p-1}{2}\right)\} \bmod p.$$

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n \; a^{(p-1/2)} \left(\frac{p-1}{2}\right)! \bmod p.$$

$$1 \equiv (-1)^n \; a^{(p-1/2)} \bmod p.$$

$$\Rightarrow (-1)^n \equiv 1 \; a^{(p-1/2)} \bmod p. \quad [\because \text{associative prop}].$$

Since $a^{(p-1/2)} \bmod p$ is legendre symbol $(\frac{a}{p})$:

$$(-1)^n \equiv (\frac{a}{p}) \bmod p.$$

$$\therefore (\frac{a}{p}) \equiv (-1)^n \bmod p.$$

$$\therefore \boxed{(\frac{a}{p}) = (-1)^n.}$$

* Pseudo prime: A composite number that satisfies the primality test for prime, which fools the primality test.

Proposition: Let $n > 1$ be an odd integer. Choose an integer b with $1 < b < n$. If $b^{n-1} \neq 1 \pmod n$, then n is composite.
This is known as Fermat's Primality test.

Ex: Check whether 209 is prime or composite.
Choosing b as 2.

$2^{208} \bmod 209 = ? 36$

$2^{208} = (2^{100} \cdot 2^{100} \cdot 2^8) \bmod 209$. $2^{10} = 1024 \,/\, 209 = 188$.

$((2^{10})^5)^4 = ((188)^5)^4 = (177)^4 = 23 \cdot 2^8 = 23 \cdot 47 = 1081 \,/\, 209 = 36$.

$\therefore$ 209 is a composite number.

* b - pseudoprime:
A composite integer $n > 1$ is called a b-pseudoprime if $b^{n-1} \equiv 1 \pmod n$.

For example: $341 \Rightarrow 2^{340} \equiv 1 \pmod{341}$.
$\therefore$ 341 is 2-pseudoprime.

21 Aug.

* Fermat's Pseudoprime:

A composite number p is called a Fermat's pseudoprime to a base 'a' if it satisfies Fermat's Little Theorem for that base.

$$a^{p-1} \equiv 1 \pmod{p}.$$

For example: 561. 561 is not prime (∵ 3).

For base $a = 2$:

$$2^{560} \equiv 1 \pmod{561}$$

$2^{560} = (2^{10})^{56} \cdot 2^{0}$

$2^{10} = 1024 \bmod 561 = 463.$

$(463)^5 = 463. \rightarrow 2^{50}.$

$2^{50} \cdot 2^{50} \cdot 2^{50} \cdot 2^{50} \cdot 2^{50} = 2^{50^5} = 463^5 = 463.$

$\therefore 2^{250} \cdot 2^{250} \cdot 2^{30} \cdot 2^{30} = 463 \cdot 463 \cdot 166 \cdot 166$

$= 64 \cdot 64 = 4089 \bmod 561 = 1$

∴ 561 is a Fermat's Pseudoprime.

* Carmichael numbers:

A composite $n > 1$ is called a Carmichael number if

$$b^{n-1} \equiv 1 \pmod{n}$$

∀ integers b with $GCD(b, n) = 1$.

Eg: $561 = 3 \cdot 11 \cdot 17.$

Suppose $b \in \mathbb{Z}$. $GCD(b, 561) = 1$.

then $3 \nmid b$, $11 \nmid b$, $17 \nmid b$.

By Fermat's theorem:

$3 \nmid b$: $b^2 \equiv 1 \pmod 3$ - (1).

$11 \nmid b$: $b^{10} \equiv 1 \pmod{11}$ - (2).

$17 \nmid b$: $b^{16} \equiv 1 \pmod{17}$ - (3).

$b^{560} \equiv 1 \pmod{561}$.

(1) $\Rightarrow (b^2)^{280} \equiv 1 \pmod 3$ - (4)

(2) $\Rightarrow (b^{10})^{56} \equiv 1 \pmod{11}$ - (5).

(3) $\Rightarrow (b^{16})^{35} \equiv 1 \pmod{17}$ - (6)

$b^{560} \equiv 1 \pmod{(3)}$.

$b^{560} \equiv 1 \pmod{(11)}$.

$b^{560} \equiv 1 \pmod{17}$

Note: By Chinese Remainder Theorem:

$a \equiv b \pmod{m_1}$.

$a \equiv b \pmod{m_2}$.

$a \equiv b \pmod{m_3}$.

then $a \equiv b \pmod{LCM(m_1, m_2, m_3)}$.

If m_1, m_2 & m_3 are prime, $LCM = m_1 \times m_2 \times m_3$.

$\therefore b^{560} \equiv 1 \pmod{3 \times 11 \times 17}$

$b^{560} \equiv 1 \pmod{561}$.

$\therefore$ 561 is a carmichael number.

* Euler Pseudoprimes:

A composite number p is called an Euler Pseudoprime to base 'a' if it satisfies (Euler's criterion):

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}.$$

Eg: 561 base 2.

LHS: $\left(\frac{a}{p}\right)\cdot\left(\frac{a}{561}\right) = \left(\frac{2}{3\times11\times17}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{11}\right)\left(\frac{2}{17}\right)$.

$= (-1)(-1)(1) = 1$.

RHS: $a^{(p-1)/2} \bmod p$.

$= 2^{560/2} \bmod 561$

$= 2^{280} \bmod 561$.

$= 2^{10^{20}} \cdot 2^{10^4} := 2^{10^{2^5}} \cdot 2^{10^{2^2}}$

$\Rightarrow 2^{10} = 1024 \,/\!.\, 561 = 463$.

$463^2 = 67$.

$67^{\cdot 5} = 67^2 = 1$.

$\therefore 2^{10^{2^5}} = 1$.

$2^{10^4} = 463^4 = 463^{2^2} = 67^2 = 1$.

$\therefore 2^{280} \equiv 1 \pmod{561}$.

OR.

$561 = 3\times11\times17$.

$2^2 \equiv 1 \pmod 3$.

$(2^2)^{140} \equiv 1 \pmod 3$.

$(2^{10})^{28} \equiv 1 \pmod{11}$.

$(2^{16})^{17}\cdot 2^8 \equiv 1 \pmod{17}$.

($2^8 = 256 \equiv 1 \pmod{17}$)

$\therefore 2^{280} = 1 \pmod{3\cdot11\cdot17}$

$2^{280} \equiv 1 \pmod{561}$.

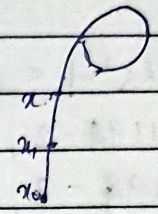
$\therefore$ LHS = RHS.

* Pollard - Rho method or Pollard ρ method:

To find small non-trivial factor of large integer n.

x_0 - random $(0, n-1)$.

x_i - $f(x_{i-1}) \pmod n$.



where x_0 is a random starting value;
n is the number to be factored.
$f \in Z(x)$ is a polynomial with integer coefficients.

Here, $f(x) = x^2 \pm a$ with $a \neq -2, 0$.
Then, $x_i \equiv x_j \pmod d$, where d is divisor of n.
ie; $x_i \not\equiv x_j \pmod n$.

$\Rightarrow d \mid (x_i - x_j)$ [d divides $(x_i - x_j)$].
ie; $d \nmid (x_i - x_j)$ [d does not divide $(x_i - x_j)$].

$\Rightarrow$ GCD $((x_i - x_j), n)$ is the non-trivial factor of n.

Ex. $n = 1387$, $f(x) = x^2 - 1$, $x_0 = 2$.

$x_0 = 2$; $x_1 = x_0^2 - 1 = 2^2 - 1 \pmod n = 3 \% 1387 = \underline{3}$.

GCD $(x_1 - x_0, n) =$ (3-2, 1387) $= \underline{1}$.
$x_2 = x_1^2 - 1 = 3^2 - 1 \% 1387 = 8$.
GCD $(x_2 - x_0, n) =$ (8-2, 1387) = (6, 1387) $= \underline{1}$.
GCD $(x_2 - x_1, n) =$ (8-3, 1387) = (5, 1387) $= \underline{1}$.

$x_2 = x_1^2 - 1 = 8^2 - 1 \pmod{1387} = 63.$

GCD (63-2, 1387) = (61, 1387) = 1.

GCD (63-3, 1387) = (60, 1387) = 1.

GCD (63-8, 1387) = (55, 1387) = 1.

$x_4 = x_3^2 - 1 = 63^2 - 1 \pmod{1387} = 3968 \pmod{1387} = 1194.$

GCD (1194-2, 1387) = (1192, 1387) = 1.

GCD (1194-3, 1387) = (1191, 1387) = 1.

GCD (1194-8, 1387) = (1186, 1387) = 1.

GCD (1194-63, 1387) = (1131, 1387) = 1.

$x_5 = x_4^2 - 1 = 1194^2 - 1 \pmod{1387} = 1186.$

GCD (1186-2, 1387) = 1.

GCD (1186-3, 1387) = 1.

GCD (1186-8, 1387) = 19.

∴ 2nd factor : 1387/19 = 73.

Qn. $n = 253$; $f(x) = x^2 + 1$; $x_0 = 2$.

$x_0 = 2$; $x_1 = x_0^2 + 1 = 4 + 1 = 5 \pmod{253} = 5$.

GCD (5-2, 253) = (3, 253) = 1.

$x_2 = x_1^2 + 1 = 25 + 1 = 26 \pmod{253} = 26.$

GCD (26-2, 253) = (24, 253) = 1.

GCD (26-5, 253) = (21, 253) = 1.

$x_3 = x_2^2 + 1 = (677 \pmod{253}) = 171.$

GCD (171-2, 253) = (169, 253) = 1.

GCD (171-5, 253) = (166, 253) = 1.

GCD (171-26, 253) = (145, 253) = 1.

$x_4 = x_3^2 + 1 = 29242 \cdot 1 \cdot 253 = 147.$

GCD $(147 - 2, 253) = (145, 253) = 1$

GCD $(147 - 5, 253) = (142, 253) = 1.$

GCD $(147 - 26, 253) = (121, 253) = 11.$

2nd factor : $253/11 = 23.$

27 Aug.

* Finite Continued fractions:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots \cdots \cfrac{1}{a_N}}}}}.$$

of the $(N+1)$, where $a_0, a_1, a_2, a_3, \cdots, a_N$ are continued fractions when there is no risk of ambiguity.

It can also be represented by as $[a_0, a_1, a_2, \cdots, a_N]$ where $a_1, a_2, \cdots, a_N$ known as partial quotients.

$$[a_0, a_1, a_2, \cdots, a_N] = a_0 + \cfrac{1}{[a_1, a_2, \cdots, a_N]}.$$

$$= [a_0, [a_1, a_2, \cdots, a_N]].$$

Simple Continued fractions:

Continued fractions where partial quotients are integers.

Qn. Express the rational numbers $\frac{17}{3}$ & $\frac{3}{17}$ into finite simple continued fractions.

$$\frac{17}{3} = 5 + \frac{2}{3} = 5 + \frac{1}{3/2}.$$

$$= 5 + \frac{1}{1 + 1/2}$$

$$\frac{17}{3} = [5, 1, 2].$$

Euclidean:

$$3 = 0 \times 17 + 3.$$
$$17 = 5 \times 3 + 2.$$
$$3 = 1 \times 2 + 1.$$
$$1 = 2 \times 1 + 0.$$

$$\frac{3}{17} = [0, 5, 1, 2].$$
$$= 0 + \frac{1}{5 + \frac{1}{3/2}}.$$
$$= 0 + \frac{1}{5 + \frac{1}{1 + \frac{1}{2}}}.$$
$$= [0, 5, 1, 2].$$

Qn. Convert the following continued fractions to rational numbers: $[-3, 2, 12]$.

$$[-3, 2, 12] = -3 + \frac{1}{2 + \frac{1}{12}}.$$

$$= -3 + \frac{1}{\frac{25}{12}}$$

$$= -3 + \frac{12}{25} = \frac{-75 + 12}{25} = -\frac{63}{25}.$$

Qn. Convert $[0, 1, 1, 100]$.

$$[0, 1, 1, 100] = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{100}}}.$$

$$= 0 + \cfrac{1}{1 + \cfrac{1}{\frac{1010}{100}}} = 0 + \cfrac{1}{1 + \frac{100}{101}}$$

$$= 0 + \cfrac{1}{\frac{201}{101}} = 0 + \frac{101}{201} = \frac{101}{201}.$$

Theorem: Every fractional number can be expressed as a finite simple continued fraction.

* Infinite Simple Continuous Fraction:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots + \infty}}}$$

is called infinite simple continuous fraction where $a_0 \in \mathbb{Z}$ and $a_1, a_2, \cdots \in \mathbb{N}$.
Also, it is denoted as $[a_0, a_1, a_2, \cdots]$.

Convergent property:

If $[a_0, a_1, a_2, \cdots]$ is infinite simple cont fraction then any finite integer $[a_0, a_1, a_2, \cdots, a_N]$ is called k^{th} convergent and it is denoted by $\frac{P_k}{q_k}$.

$\frac{P_0}{q_0} = [a_0]$.

$\frac{P_1}{q_1} = [a_0, a_1]$.

$\frac{P_2}{q_2} = [a_0, a_1, a_2]$.

__/__/___

$$\frac{p_n}{q_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}.$$

Complete Quotient:

If $[a_0, a_1, a_2, \cdots]$ is an infinite simple continued fraction then for any +ve integer k.

$[a_k, a_{k+1}, a_{k+2}, \cdots]$ is called the k^{th} complete quotient and is denoted by a_k'.

$\therefore a_0' = [a_0, a_1, a_2, \cdots]$.
$a_1' = [a_1, a_2, a_3, \cdots]$.
$a_2' = [a_2, a_3, a_4, \cdots]$.

Theorem: Every infinite simple continued fraction represents an irrational number and conversely every irrational no. can be developed as infinite simple continued fraction.

Eg: $[1, 2, 1, 2, 1, 2, \cdots] = [\overline{12}]$.

$$= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}$$

$x = [\overline{12}]$

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{x}}.$$

__/__/___

$$x = 1 + \frac{1}{\frac{2x+1}{x}} = 1 + \frac{x}{2x+1}$$

$$x = \frac{2x + 1 + x}{2x+1} = \frac{3x+1}{2x+1}$$

$$2x^2 + x = 3x + 1$$

$$2x^2 - 2x - 1 = 0.$$

$$x = \frac{2 \pm \sqrt{4+8}}{2(2)} = \frac{1 \pm \sqrt{3}}{2}.$$

Qn Find $[1,2,2,2,\ldots]$.

$[1,\bar{2}]$.

Qn. Find $\sqrt{2}$.

$$\sqrt{2} = 1 + \sqrt{2} - 1$$

$$= 1 + \frac{(\sqrt{2}-1)(\sqrt{2}+1)}{(\sqrt{2}+1)} = 1 + \frac{2-1}{\sqrt{2}+1} = 1 + \frac{1}{1+\sqrt{2}}.$$

Sub for $\sqrt{2}$:

$$\sqrt{2} = 1 + \frac{1}{1 + (1 + \frac{1}{\sqrt{2}})}$$

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \ldots}}$$

$= [1,2,2,2,\ldots]$.

$= [1,\bar{2}]$.

__/__/__

Qn ① $\sqrt{5}$.

② $\sqrt{14}$.

③ $\sqrt{8131}$. Find infinite cont. fraction: $[a_0, a_1, \cdots, a_8]$. Also find convergents p_0 to a_7.

① $\sqrt{5}$.

$a_0 = 2$.

$\sqrt{5} = 2 + \sqrt{5} - 2$.

$= 2 + \frac{(\sqrt{5}-2)(\sqrt{5}+2)}{(\sqrt{5}+2)}$

$= 2 + \frac{5-2}{\sqrt{5}+2} = 2 + \frac{3}{\sqrt{5}+2} = 2 + \frac{3}{2+\sqrt{5}} = 2 + \frac{1}{\frac{2+\sqrt{5}}{3}}$.

Sub $\sqrt{5}$: $2 + \cfrac{3}{2 + \cfrac{3}{2 + \cfrac{3}{2 + \cfrac{3}{2 + \cdots}}}}$

$\frac{2+\sqrt{5}}{3} = 1.412$.

$= 1$.

$= 2 + \cfrac{3}{4 + \cfrac{3}{4 + \cfrac{3}{4 + \cdots}}}$

$= 2 + \frac{1}{1 + \frac{2+\sqrt{5}}{3} - 1} = 2 + \frac{1}{1 + \frac{2+\sqrt{5}-3}{3}}$

$= 2 + \frac{1}{1 + \frac{\sqrt{5}-1}{3}} = 2 + \frac{1}{1 + \frac{4}{3\sqrt{5}+3}} =$

$= 2 + \cfrac{3}{4 + \cfrac{3}{4 + \cdots}}$.

② $\sqrt{14}$: $a_0 = [3]$. $+ \sqrt{14} - 3 = 3 + \frac{(\sqrt{14}-3)(\sqrt{14}+3)}{\sqrt{14}+3} = 3 + \frac{14-3}{\sqrt{14}+3}$.

$\sqrt{14} = 3 + \frac{11}{\sqrt{14}+3} = 3 + \frac{11}{3+\sqrt{14}} = 3 + \cfrac{11}{3 + 3 + \cfrac{11}{3 + 3 + \cfrac{11}{3 + \sqrt{14}}}}$.

$\sqrt{14} = 3 + \cfrac{11}{6 + \cfrac{11}{6 + \cfrac{11}{6 + 11 \cdots}}}$

$\therefore \sqrt{14} = [3, \overline{6, 11}]$.

2 Sep.

* Factorization using Continuous Fractions:
This method is based on Fermat's Algorithm & Kraitchik's improvement.

Fermat's Algorithm:
It works based on the idea to factor n by trying to find x & y such that $n = x^2 - y^2 = (x-y)(x+y)$.

If (x^2-n) is a perfect square,
$x-y$ & $x+y$ are factors.

Otherwise, add 1 to x & repeat it until (x^2-n) is a perfect square.

For example: $n = 319$.

$x = 18$.

$(x^2-n) = 18^2 - 319 = 5$. $\Rightarrow x+i$.

$(19^2-n) = 19^2 - 319 = 42$. $\Rightarrow x+1$.

$(20^2-n) = 20^2 - 319 = 81$ $\sqrt{81} = 9$.

$\therefore y = \pm 9$.

Factors $= (20+9)(20-9) = 29, 11$.

Kraitchik's Improvements:
Instead of finding x & y, to solve $(x^2-y^2) = n$ look for random x & y that solves

$x^2 \equiv y^2 \pmod n$.

ie; $x^2 - y^2 \equiv 0 \pmod n$.

ie; n will divide x^2-y^2.

ie; $x+y$ & $x-y$ are factors.

$\sqrt{5}$ =
$\sqrt{14}$ =
$\sqrt{8131}$ =

__/__/___

Qn. Compute the factors of 8131 using factorization algorithm using continuous fractions.

$n = 8131$.

① $\sqrt{n}$'s cont. fractions.

$\sqrt{8131}$ $\quad a_0 = 90$.

$= 90 + \sqrt{8131} - 90$

$= 90 + \frac{8131 - 90^2}{\sqrt{8131} + 90} = 90 + \frac{31}{90 + \sqrt{8131}} = 90 + \frac{1}{\frac{90 + \sqrt{8131}}{31}}$.

$\frac{90 + \sqrt{8131}}{31} = 5.812$.

≈ 5.

$\therefore a_1 = 5$.

$= 90 + \frac{1}{5 + \frac{90 + \sqrt{8131} - 5}{31}}$.

$5 + \left(\frac{90 + \sqrt{8131}}{31}\right) 5 = 5 + \frac{90 + \sqrt{8131} - 155}{31} = 5 + \frac{8131 - 65^2}{31(\sqrt{8131} + 65)}$

$= 5 + \frac{3906}{31\sqrt{8131} + 65}$.

① Compute convergents with 5 iterations of k.

k	0	1	2	3	4
$[a_0, a_1, a_2 \ldots]$ a_k	90	5	81	4	3
$P_k \pmod n$	90	451	541	2615	255
~~$P_k^2 \pmod n$~~	~~8100~~	126	~~8046~~	54	~~2108~~
		-31		-35	-23.

$\frac{P_0}{q_0} = \frac{a_0}{1}$.

$P_0 = a_0$. $P_1 = 1 + a_0 a_1$.

$P_n = a_n P_{n-1} + P_{n-2}$. $P_k = a_k P_{k-1} + P_{k-2}$

② Consider the last row of the table & find prime factorization for each value of k.

k	$P_k^2 \pmod{8131}$	Prime factorization	
0	-31	(-1)(31)	~~X~~
1	126	(2)(3)(3)(7).	✓
2	-35	(-1)(7)(5).	X
3	54	(2)(3)(3)(3).	✓
4	-23	(-1)(23).	X

④ Identify the B-set, prime factors ~~app~~ that appears more than once.

B-set : $\{(-1), (2), (3), (7)\}$.

⑤ Ignore the k = 0, 2 & 4 because there exist primes in these prime factorization that do not appear in B.

⑥ Find the vector form for remaining k.

ie, k = 1 & 3.

~~k=1~~ → Vector is formed by number of times each element in B is present.

$k=1$: $[0, 1, 2, 1]$.
$k=3$: $[0, 1, 3, 0]$.

(1) Add these 2 vectors mod 2.
$[0\ 1\ 2\ 1] + [0\ 1\ 3\ 0]$.
$= [0\ 2\ 5\ 1] \bmod 2$.
$= [0\ 0\ 1\ 1]$.

Since it is not a zero vector, we need to consider more iterations of k.

k	0	1	2	3	4	5	6	7	8
a_k	90	5	1	4	3	7	1	1	8
P_k mod 91	90	451	541	2615	255	4100	4655	924	3916
P_k^2 mod n	-31	126	-35	54	-23	89	-90	21	-10.

k	P_k^2 (mod 8131)	Prim fact.	
0	-31	(-1)(31).	X
1	126	(2)(3)(3)(7).	✓
2	-35	(-1)(5)(7)	✓
3	54	(2)(3)(3)(3).	✓
4	-23	(-1)(23)	X
5	89	(89)	X
6	-90	(-1)(2)(3)(3)(5)	✓

~~Ignore~~ B set = $\{(-1), 2, 3, 5, 7\}$.
Ignore $k = 0, 4, 5$.
vectors: $k=1$: $[0\ 1\ 2\ 0\ 1]_{v_1}$
$k=2$: $[1\ 0\ 0\ 1\ 1]_{v_2}$
$k=3$: $[0\ 1\ 3\ 0\ 0]_{v_3}$
$k=6$: $[1\ 1\ 2\ 1\ 0]_{v_6}$
Combined mod 2: $[2\ 3\ 4\ 2\ 2] \cdot v = [0\ 0\ 0\ 0]$.
$(v_1+v_2+v_6)$

(8) If $x^2 \equiv y^2 \pmod{n}$ & $x \not\equiv y \pmod{n}$, then the factors are $GCD(x \pm y, n)$

$x \equiv (451)(541)(465\overline{5}) \pmod{8131}$.

$x = 7501$. ~~or -630.~~ ?

$y^2 \equiv [[(2)(3)^2(7)], [(-1)(5)(7)][(-1)(2)(3)(3\times5)]]$

$= [(-1)^2 (2)^2 (3)^4 (\overline{5})^2 (7)^2]$.

$= [(2)(3)^2(5)(7)]^2$.

$= [630]^2$.

$\therefore y = \pm 630$.

Is $x \equiv y \pmod{n}$.

$7501 \equiv -630 \pmod{8131}$.

Consider upto $k=8$.

Finally $x = 7409$; $y = [(2)(3)(5)\overline{(5)}]^2$. $\Rightarrow y = \pm 30$.

$7409 \not\equiv \pm 30 \pmod{8131}$.

$\therefore$ Factors : $GCD(7409 \pm 30, 8131)$.

$= 47, \overline{8}173$.

$\therefore 8131 = 47 \times 173$.

Q. Factorize the following numbers using ~~co~~ factorization using continuous fractions:
(1) 33 (2) 55 (3) 21 (4) 63.

* ~~Crypto~~

Knapsack Cryptosystem (9m):

b = [7 11 19 39 79 157 313]. x_i = [1100111].
n = 900 r = 37. perm = [1 2 5 3 1 7 6].

$t_i = b_i \cdot r \bmod n$.
t_i = [259 407 703 543 223 409 481].
a = [543 407 223 703 259 481 409].
x_i = [1 1 0 0 1 1 1].
$S = a_i x_i = 543 + 407 + 223 + 259 + 781 + 409 = 2399$

Decryption: $S' = r^{-1} \cdot S \pmod n$. $r^{-1} \bmod n = 43$.
$S' = 43 \cdot 2399 \pmod{900}$
$S' = 527$.

i	b_i	S'	$S' \geq b_i$	x_i	$S' = S' - b_i$.
7	313	527	T	1	214
6	157	214	T	1	57.
5	79	57	F	0	57.
4	39	57	T	1	18.
3	19	18	F	0	18.
2	11	18	T	1	7.
1	7	7	T	1	0.

$\therefore x' = [1\ 1\ 0\ 0\ 1\ 1\ 1]$. after perm: [1 2 5 3 1 7 6]
$\Rightarrow x = [1100111] \Rightarrow q$.
[x' taken bottom to top from the table].

Factorization:

$\sqrt{2} = 1 + \sqrt{2} - 1$

$= 1 + \frac{(\sqrt{2}-1)(\sqrt{2}+1)}{\sqrt{2}+1} = 1 + \frac{2-1}{\sqrt{2}+1} = 1 + \frac{1}{\sqrt{2}+1}$

$= 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{1+\sqrt{2}}$

$\sqrt{2}+1 = 2.414$

$= 1 + \cfrac{1}{1 + \left[1 + \cfrac{1}{1 + \left[1 + \cfrac{1}{1+\sqrt{2}}\right]}\right]}$ ...

$= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}} = \langle 1; \overline{2} \rangle$

$\frac{\sqrt{3}+1}{2} = 1.366$

$\sqrt{3} = 1 + (\sqrt{3}-1) = 1 + \frac{\sqrt{3}-1}{\sqrt{3}+1} = 1 + \frac{2}{\sqrt{3}+1} = 1 + \frac{1}{\frac{\sqrt{3}+1}{2}}$

$= 1 + \frac{1}{1 + (\frac{\sqrt{3}+1}{2} - 1)} = 1 + \frac{1}{1 + \frac{1}{2/\sqrt{3}+1}}$

$\frac{\sqrt{3}+1}{2} - 2 \quad \frac{\sqrt{3}-1}{2} = 0.366$

$2/\sqrt{3}+1 = 2.73$

$= 1 + \cfrac{1}{1 + \cfrac{1}{2 + (\frac{2}{\sqrt{3}+1} - 2)}} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{4-2\sqrt{3}}{\sqrt{3}+1}}}$

$\frac{2}{\sqrt{3}-1} - 2 = \frac{2 - 2\sqrt{3} + 2}{\sqrt{3}-1} = \frac{4-2\sqrt{3}}{\sqrt{3}+1} = 0.73$

$\frac{\sqrt{3}+1}{\text{reci}} = 1.366$

$= 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{(\sqrt{3}-1)/(4-2\sqrt{3})}}} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{\sqrt{3}-1}{4-2\sqrt{3}} - 1}}}$

$\frac{\sqrt{3}-1-4+2\sqrt{3}}{4-2\sqrt{3}} = \frac{3\sqrt{3}-5}{4-2\sqrt{3}} = 2.73$

$= 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + 1/2 + \cdots}}} = \langle 1; \overline{1,2} \rangle$

__/__/____

Q. $\langle 1; \overline{2} \rangle = [1; 2, 2, 2 \ldots]$.

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}} = 1 + \cfrac{1}{1 + x}$$

$$x = \frac{1}{1 + x} + 1 = \frac{1 + x + 1}{1 + x} = \frac{2 + x}{1 + x}$$

$x + x^2 = 2 + x \Rightarrow x^2 - 2 = 0$.

~~$x^2 + x - 2 - x = 0$~~

~~$b^2 - 4ac = -4(1)(-2) = 8$~~

~~$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{2 \pm 8}{2} = 1 \pm 4$~~

$x^2 - 2 = 0$.

$x^2 = 2 \Rightarrow x = \sqrt{2}$.

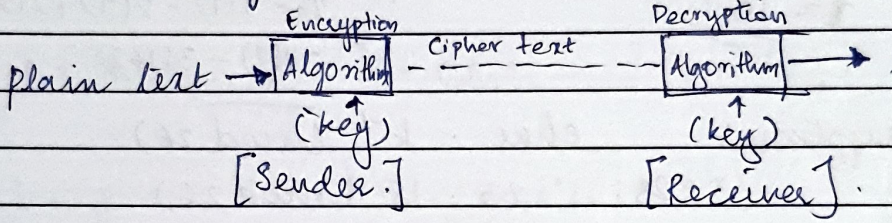
__/__/____

3 Sep.

* Cryptograph:

Encryption:
A method to securely communicate.

Confidentiality → Only receiver understands sender's msg.
Integrity → Message should not be altered in btw.
Authenticity → Keepin' it real.



Cryptanalysis:
Finding out the key, encryption/decryption algorithm & breaking the cipher text.

① Substitution Cipher:
- Mono alphabetic: Shift cipher or Ceasar cipher:
Shifting number, one to one change.

For example: Additive:

$$[P+k \cdot 1.26] \longrightarrow [C-k \cdot 1.26]$$

5 Sep.

Q. With multiplicative substitution method: Hello, encrypt the message with key 7.

Ans: XCZZU.

$7 \times 7 \cdot 1.26 = 49 \cdot 1.26 = 23$. $11 \times 7 \cdot 1.26 = 77 \cdot 1.26 = 25$.
$4 \times 7 \cdot 1.26 = 28 \cdot 1.26 = 2$. $14 \times 7 \cdot 1.26 = 98 \cdot 1.26 = 20$.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$1 = (26 - 3(7)) - 2(7 - (26 - 3(7))$

$1 = (26 - 3(7)) - 2(7) + 2(26) - 6(7)$

$= 26 - 3(7) - 2(7) + 2(26) - 6(7)$

$= 3(26) -$

k^{-1}. $\quad y^{-1} \mod 26$.

$7x \equiv 1 \mod 26$.

$GCD(7, 26) = 1$

$26 = 3 \times 7 + 5$	$5 = 26 - 3(7)$.
$7 = 1 \times 5 + 2$.	$2 = 7 - 5$.
$5 = 2 \times 2 + 1$	$\Rightarrow 1 = 5 - 2(2)$.
$2 = 2 \times 1 + 0$.	

$1 = 5 - 2(7 - 26 + 3(7))$

$1 = 26 - 3(7) - 2(7) + 2(26) - 6(7)$

$1 = (-11)(7) - 3(26)$

$x = 15$.

Decryption: $\quad$ chars $\cdot k^{-1} \pmod{26}$.

$x = 23$: $= 23 \cdot 15 \pmod{26}$

$= 345 \pmod{26}$

$= 7$.

$a = 2$: $= 2 \cdot 15 \pmod{26}$.

$= 30 \pmod{26}$.

$= 4$.

$z = 25$: $= 25 \cdot 15 \pmod{26}$.

$= 375 \pmod{26} = 11$.

$u = 20$: $= 20 \cdot 15 \pmod{26}$

$= 300 \pmod{26} = 14$.

Affine Ciphers:

2 layers:

First: multiplication, then addition.

Decryption: first ~~of~~ subtraction, then mult-inverse.

__/__/____

23 Sep

- Monoalphabetic Substitution: an alpha is substituted by a single alpha, always.

- Polyalphabetic substitution: an alpha is ~~sbs~~ subsitituted by more than 1 alpha.
  Different keys used for letters.

① Autokey Ciphers:

$P = P_1P_2P_3\cdots \quad C = C_1C_2C_3\cdots \quad k = (k_1, P_1, P_2 \cdots)$.

Encryption: $C_i = (P_i + k_i) \bmod 26$.
Decryption: $P_i = (C_i - k_i) \bmod 26$.

② Playfair Cipher:

Key is a 5x5 matrix.
I/J are considered same.

Eg: hello. Since L 2 times, helxlo.

h	e	l	x	o
a	b	c	d	f
g	i/j	k	m	n
p	q	r	s	t
u	v	w	x	y

he: Same row: EL.
lx: RL
lo: LH.
helxlo: ELRLLH?

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

he: Same row: EC.
lx: Same col: QZ.
lo: Same diag: L → B, X ← O. BX.

⇒ hello = ECQZBX.

Name 7 - prathvi.

__/__/____

Brute force is very difficult. Size of key domain = 25!.

Qn. Plaintext : Computer. Co mp ut er

Password : Python.

Find ciphes text:

P	Y	T	H	O
N	A	B	C	D
E	F	G	I/J	K
L	M	Q	R	S
U	V	W	X	Z

Ciphes: DHLYWPI/JL.

→ DHLYWPIL.

(3) Vigenere ciphes:

$P = p_1 p_2 p_3 \cdots$ $C_1 = C_1 C_2 C_3 \cdots$ $K = [(k_1, k_2 \cdots k_m), (k_1, k_2, \cdots k_m), \cdots]$

Encryption : $C_i = p_i + k_i$.

Decryption : $p_i = c_i - k_i$.

(4) Hill Ciphes :

Key in matrix form.

P = "code is ready" + z. ← Bogus.

$$C = P \cdot \begin{bmatrix} 02 & 14 & 03 & 09 \\ 08 & 18 & 14 & 07 \\ 00 & 03 & 21 & 25 \end{bmatrix}_{3\times4} \cdot \times K \begin{bmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}_{4\times4}$$

(Encrypt).

Decrypt : $P = C \cdot K^{-1}$.

(5) Rotor Ciphes : BEE → rotation. → BLL.

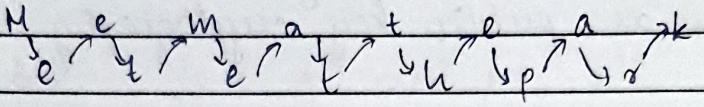
↓ initial → 1st rotation → 2nd rotation.

Mono-but changes mapping after every sub of letter.

* Transposition Ciphers:
Not substitution, but changing positions of the letters:

① Rail Fence Cipher:

Meet me at the park:



Cipher: Memateakeetethpr.

② Keyed Transposition Cipher:

"Enemy Attacks Tonight".
Encryption key: 3 1 4 5 2.
1 2 3 4 5.

Enemy attac kstonb ightz.
↓
eemyn taact tkons hitzg.

Decryption key: 1 2 3 4 5. ⇒ 2 5 1 3 4.
3 1 4 5 2

__/__/____

24 Sep

* Symmetric Cryptography:

Same key for encryption & decryption.
Secret key must be exchanged securely.

* Assymmetric Cryptography:
One private & one public key.
Also known as public key cryptography.

Encrypt using someones public key & they can decrypt with their private key.

① Diffie-Hellman key exchange:

Primitive root of q: when $(q^1, q^2, q^3 \cdots q^{p-1}) \bmod p$ are distinct.

Global elements:
$q < p$ (prime)
q is primitive root of p.

Alice	Bob
- Private key. $X_A < p$	- Private key. $X_B < p$
- Calculate public key: $Y_A = q^{X_A} \bmod p$	- Calculate public key: $Y_B = q^{X_B} \bmod p$
- Shared Secret key: $k = Y_B^{X_A} \bmod p$	- Shared secret key: $k = Y_A^{X_B} \bmod p$

Qn. Alice & Bob agree to use the prime $p = 17$ & the primitive root $q = 3$.
Alice's secret key $X_a = 54$, Bob's $X_b = 24$.
Compute public keys for both & shared secret keys.

Alice: $Y_A = q^{X_A} \bmod p = 3^{54} \cdot /. 17$

$3^{16} \cdot /. 17 = 1. \Rightarrow 16^3 = 48.$

$3^6 \cdot /. 17 = \underline{15}$

Bob: $Y_B = q^{X_B} \bmod p = 3^{24} \cdot /. 17$

$3^{16} \cdot /. 17 = 1.$

$3^8 \cdot /. 17 = \underline{16}$

Alice: $K = Y_B^{X_A} \bmod p = 16^{54} \bmod 17.$

$16^{16} \cdot /. 17 = 1.$

$16^6 \cdot /. 17 = \underline{1}.$

Bob: $K = Y_A^{X_B} \bmod p = 15^{24} \bmod 17$

$15^{16} \cdot /. 17 = 1.$

$15^8 \cdot /. 17 = \underline{1}.$

$\therefore$ Shared key $= \underline{1}$.

Qn. Alice: $a = 347.$ $p = 941.$
Bob: $b = 781.$ $g = 627.$

[Public: 380, 691.
Shared: 470]

Alice: $Y_A = g^{X_A} \bmod p = 627^{347} \cdot /. 941.$

~~Euler's theorem~~

__/__/____

25 sep

* Discrete Logarithm Problem:

$g^x \bmod p$

If $2^x \bmod 7 = 1$; x can be 2, 5, etc.

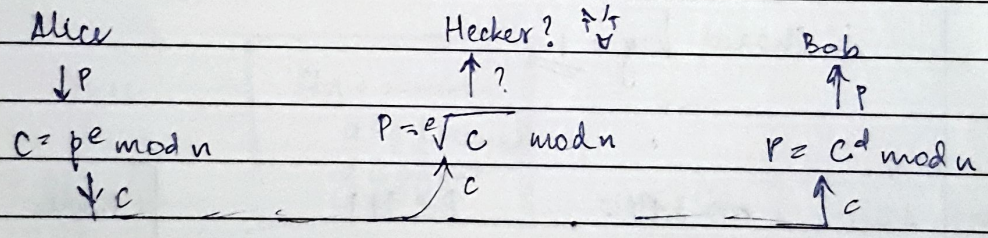
Here can say $2^x \bmod 7 = 1$, but finding x is hard.

One way function: Easy one way, hard backwards.
f is easy to compute, but not f^{-1}.

Trapdoor one way function: Given y & a teapdoor, x can be easily computed.

* RSA Cryptosystem:

Asymmetric cryptosystem.



Key generation:

1. p & q - prime numbers.
2. $n = p \times q$ - calc.
3. $\phi(n) = (p-1)(q-1)$ - Calc.
4. Choose e: GCD$(\phi(n), e) = 1$; $1 < e < \phi(n)$.
5. Calc d. $d = e^{-1} \bmod \phi(n)$.
6. Public key: $KU = \{e, n\}$.
7. Private key: $KR = \{d, n\}$.

60/13 = 4
52
8

6 mod 13

d x e = 1 mod ϕ(n).

10 x 13

60

130/60 = 1.

Eg: p = 3, q = 11. n = 33.

ϕ(n) = 2 · 10 = 20.

If public key is 7, then compute the private keys; public keys & encrypt the message M = 31 using RSA cryptosystem. Also do the decryption process. [e = 7].

Public key: KU = {e, n} = {7, 33}.

Private key: KR = {d, n}.

$d = e^{-1} \bmod \phi(n)$.

$7^{-1} \bmod 20 := 7x \bmod 20 = 1$.

x = 3

$\therefore d = 3 \bmod 20 = 3$.

KR = {3, 33}.

M = 31.

$C = P^e \bmod n$.

$C = 31^7 \bmod 33 = 25 \cdot 31 \bmod 33 =$ 1.

$P = C^d \bmod n$.

$P = 1^3 \bmod 33 = 31$.

$e = 13$.

$\frac{130}{60} = 1$ x 13 + 60.

130 · 1 · 60.

26 Sep

Qn. p = 7 q = 11. n = 77. ϕ(n) = 60. e = 13. d = 37.

Compute public & private keys, encrypt M = 5 & decrypt it.

KU = {e, n} = {13, 77}.

$d = e^{-1} \bmod \phi(n) = 37 \bmod 60 = 37$.

KR = {d, n} = {37, 77}.

M = 5: $C = P^e \bmod n = 5^{13} \cdot 1 \cdot 77 = 5^{10} \cdot 5^3 \cdot 1 \cdot 77 = (25^2 \cdot 18) \cdot 77$.

C = 26.

$26^5 = 15^6 = 1$.

$P = C^d \bmod n = 26^{37} \cdot 1 \cdot 77 = 5$

__/__/____

* Digital Signature:
Document verification can be done using this.

* Attacks on RSA:

1. Factorization: finding p & q from n; calc d with e; hack!

2. Chosen-Ciphertext attack: Because e & d are mult inverse.
Prevention: Padding - add extra digits to throw off.
Hybrid encryption.

3. Attacks on the Modulus: If hacker(?) ~~has~~ is a part of the community, they can factor n since they too have {e, d, n} like the other 2.
- Common n.

4. Timing Attack:
$c = 3$ $d = 13$ $n = 17$. $d_3 d_2 d_1 d_0$ $1101 \rightarrow 13$.

$p = 1$: $d_2 = 1$:

$p = p^2 = 1^2 = 1$; $p = p \times c = 1 \times 3 = 3$.

$d_2 = 1$:

$p = p^2 = 3^2 = 9$; $p = 9 \times 3 = 27 \% 17 = 10$.

$d_3 = 0$:

$p = 10^2 = 100 \% 17 = 15$.

$d_4 = 1$:

$p = 15^2 = 225 \% 17 = 4$; $p = 4 \times 3 = 12$.

$\Rightarrow 3^{13} \% 17 = 12$.

Finding d: if calculation takes a lot of time, $\Rightarrow 1$; if it takes less time, $\Rightarrow 0$.
Make binary out of it.

__/__/____

Initially $d_0 = 1$ because d is an odd number.

Solutions:
1. Add random delays to ~~not~~ the exponentiations so that both of them takes same amount of time.

* ElGamal Cryptosystem:

Ex. $p = 11$. $e_1 = 2$. $d = 3$. $e_2 = e_1^d = 8$. } Bobs.
Public keys $(2, 8, 11)$. Private key $= 3$. }

Alice: $r = 7$. Plain text $= 7$.
Calculate C_1 & C_2.

$C_1 = e_1^r \bmod n = 2^7 \cdot 1 \cdot 11 = 16 \cdot 1 \cdot 11 = 5/11$.
$\therefore C_2 = (P \times e_2^r) \bmod n = (7 \cdot 8^7) \cdot 1 \cdot 11 = 6/11$.
$(C_1, C_2) = (5, 6)$.

$P \leftarrow [C_2((C_1)^d)^{-1}] \bmod p$.

Oct

* Knapsack Cryptosystem:

$s = \text{knapsack\_sum}(a, x) = x_1 a_1 + x_2 a_2 + \cdots + x_k a_k$.

Given a & x, its easy to find s.
But given s & a, its ~~not~~ difficult to find x.

Knapsack is a one-way function.
Trapdoor: Sort set of numbers $a = [a_1, a_2, \cdots, a_k]$.
$\rightarrow a_i \geq a_1 + a_2 + \cdots + a_{i-1}$.

Eg: $a = [14, 25, 46, 94, 201, 400]$.

0 1 1 0 1 0

0 → X considered in sum, 1 → ✓ considered for sum.

$S = 25 + 46 + 201 = 272$

Given (s, a), desiring $x \rightarrow$ inverse process.

i	a_i	s	$s \geq a_i$	x_i	$s \leftarrow s - a_i x_i$
6	400	272	False	0	$s = 272$
5	201	272	True	1	$s = 71$.
4	94	71	False	0	$s = 71$.
3	46	71	True	1	$s = 25$.
2	25	25	True	1	$s = 0$.
1	14	0	False	0	$s = 0$.

∴ Chosen $i = 5, 3, 2$. $x' = [0\,1\,0\,1\,1\,0]$

$\Rightarrow a_i = 201, 46, 25$. $\Rightarrow x = [0\,1\,1\,0\,1\,0] = ✓$.

Key generation process:

1. Create a superincreasing k-tuple $b = [b_1, b_2, \cdots, b_k]$.
2. Choose a modulus n, such that $n > b_1 + b_2 + \cdots + b_k$.
3. Select a random int s that is relatively prime with n and $1 \leq s \leq n-1$.
4. Create a temporary k-tuple $t = [t_1, t_2, \cdots, t_k]$ in which $t_i = s \times b_i \bmod n$.
5. Select a permutation of k objects, find a new tuple $a = \text{permute}(t)$.
6. Public key is the k-tuple a. Private key is n, s, and the k-tuple b.

__/__/__

Q. $b = [7, 11, 19, 39, 79, 157, 313]$.
$n = 900$, $x = 37$. [4 2 5 3 1 7 6] permutation.

$t = [259, 407, 703, 543, 223, 409, 781]$.
$a = [543, 407, 223, 703, 259, 781, 409]$.
Public key.
Private key: $(900, 37, [7, 11, 19, 39, 79, 157, 313])$

Encryption: plain-text: q: 1100111. (103).
$x = [1\ 1\ 0\ 0\ 1\ 1\ 1]$.
$s = (a, x) = 543 + 407 + 259 + 781 + 409 = 2399$. $\Rightarrow c$.

Decryption: Private key $(900, 37, b)$.

$s' = x^{-1} \times s \bmod n$.
$s' = 37^{-1} s \bmod 900 = 73$.
$s' = 73 \cdot 2399 \bmod 900 = 527$.

inv_knapsack (b, s'): ↓ then permute.

i	b_i	s'	$s' \geq b_i$	x_i	$s' - b_i x_i$
7	313	527	True	1	214.
6	157	214	True	1	57.
5	79	57	False	0	57.
4	39	57	True	1	18
3	19	18	False	0	18.
2	11	18	True	1	7.
1	7	7	True	1	0.

$\therefore x = [1\ 1\ 0\ 1\ 0\ 1\ 1]$. $\Rightarrow$ ~~7+11+39+157+313 = 527~~
Permute x: $[1\ 1\ 0\ 0\ 1\ 1\ 1]$. $\Rightarrow q$ //
~~$s' = 527$ $b = [7, 11, \ldots]$~~
[x_i taken bottom to top from the table]

__/__/____

3 Oct.

* Strong Prime (Gordon method):

A strong prime number (p) is when r, s & t satisfy the following:

- (p-1) has a large prime factor s.
- (p+1) has a large prime factor s.
- (r-1) has a large prime factor t.

A prime number that is greater than the arithmatic mean of the nearest prime above & below.

$$p_n > \frac{p_{n-1} + p_{n+1}}{2}$$

Eg: 2 3 5 7 11 13 17 19 23.

$$2 > \frac{2+5}{2} = 3.5 \times.$$

$$5 > \frac{3+7}{2} = 5 \times$$

$$7 > \frac{5+11}{2} = 8 \times.$$

$$11 > \frac{7+13}{2} = 10 \checkmark.$$

* Safe Prime Number:

A Safe prime is a prime number of the form: $2p+1$ where p is also a prime.

For example:

__/__/__

5 7 11 23 47 59 83.

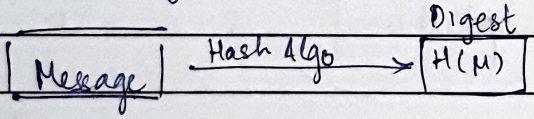
5 = 2(2)+1 ✓
7 = 2(3)+1 ✓
11 = 2(5)+1 ✓
14 = 2(8)+1 ✗ Since 8 is not a prime.

* Forgery Types:
(for digital signatures).

1. Existential Forgery:
Forge any and every message (difficult).

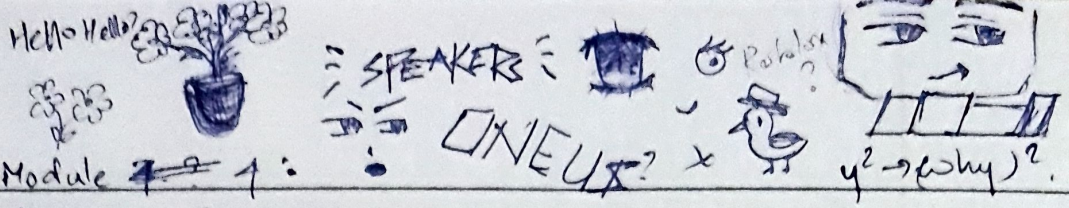
2. Selective Forgery:
Selectively chosen messages can be forged.

* Hash Algorithm:



One way function.

The digest of hash algo sign instead of the normal (message?).



7 Oct

Module ~~1~~ 1 :

Elliptic Curves:

** Cubic Curve:

Refers to any curve defined by a cubic polynomial equation in 2 variables.

Eg: $y = ax^3 + bx^2 + cx + d$.

* Singular point:

Point where the curve exhibits some form of 'bad behaviour'.

A point where the curve fails to be smooth.

Mathematically:

$$\frac{\partial F}{\partial x}(x_0, y_0) = 0 \quad \& \quad \frac{\partial F}{\partial y}(x_0, y_0) = 0.$$

For a curve defined by $F(x,y) = 0$, a point (x_0, y_0) is a singular point if both partial derivs vanish at that point.

Eg: $y^2 = x^3 - 4x$.

$$\frac{\partial F(x,y)}{\partial x} = 0 \quad \& \quad \frac{\partial F(x,y)}{\partial y} = 0.$$

$y^2 - x^3 + 4x = 0$.

$\frac{\partial F}{\partial x} = -3x^2 + 4 = 0$.

$-3x^2 = -4$.

$x^2 = \frac{4}{3} \Rightarrow x = \pm 2/\sqrt{3}$.

$2y - 0 = 0$.

$2y = 0 \Rightarrow y = 0$.

$\therefore$ Points = $(-2/\sqrt{3}, 0)$ & $(2/\sqrt{3}, 0)$.

* Discriminant:
A scalar value derived from the coeffs a, b, c & d. Provides info about the nature of the roots & singular points of a polynomial.

$$D = 18abcd - 4b^3d + b^2c^2 - 4ac^2 - 27a^2d^2.$$

If:

$D > 0$: 3 distinct real roots.
→ Smooth curve, no singular point.

$D = 0$: Multiple roots.
→ Curve may have singular points.

$D < 0$: One real & 2 complex conjugate roots.
→ Maybe smooth curve,
does not intersect the x-axis 3 times.

Qn. $x^3 - 3x + 2$. Find discriminant for this polynomial.

$F(x) = x^3 - 3x + 2$.
$a = 1, b = 0, c = -3, d = 2$.

$D = 18abcd - 4b^3d + b^2c^2 - 4ac^2 - 27a^2d^2$.
Since $b = 0$:
$D = -4ac^2 - 27a^2d^2 = -4(1)(-3)^2 - 27(1)^2(2)^2$
$D = -36 - 108 = \underline{-144}$.

$\Rightarrow D < 0$, one real root, 2 complex roots.

0000 Ooooh! Chem ~~Geometry~~ ::
_/_/_

- Elliptic Curves:

$$Y^2 = X^3 + AX + B.$$

one form of cubic curve.
Also called Weierstrass equations.

If there are no repeated roots, there will be no intersection in the curve, thus no singular point.

When $D>0$, [when $4a^3 + 27b^2 \neq 0$], there will be distinct roots.

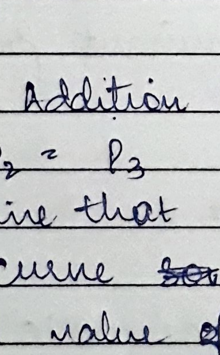
- Point at Infinity ($\mathcal{O}$)

Points after which the curve goes to infinity ??? Does not meet anymore and just walks away like they are divorced ??? Huh???

The ~~dd~~ Addition Law:

$P_1 + P_2 = P_3$ (You don't say??).

The line that connects P_1 & P_2 will intersect the curve ~~so~~ at point P_3', which is the reflection/added value of P_1 & P_2.



If $P_1 = P_2$, draw the tangent, find point of intersection, reflection of it is $2P = P_1 + P_2$.

* The Line: [ominous!]

$P_1 = (x_1, y_1)$; $P_2 = (x_2, y_2)$.

Slope = $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

→ eqtn at P_1.

$y - y_1 = \lambda (x - x_1)$.

Slope-intercept ⇒ $y = \lambda x - \lambda x_1 + y_1$.

$\beta = y_1 - \lambda x_1$.

$y = \lambda x + \beta$.

=.

Finding x_3, y_3:

$y^2 = (\lambda x + \beta)^2$.

Elliptic curve: $y^2 = x^3 + ax + b$.

→ $(\lambda x + \beta)^2 = x^3 + ax + b$.

$0 = x^3 - \lambda^2 x^2 - 2\lambda x \beta - \beta^2 + ax + b$.

x_1, x_2 & x_3 are the roots. [Coeffs of x^2 is the opposite sum of the roots].

$(x_1 + x_2 + x_3) = \lambda^2$.

$x_3 = \lambda^2 - x_1 - x_2$.

$y_3 = \lambda(x_1 - x_3) - y_1$. [$\because y_3 - y_1 = \lambda(x_3 - x_1)$ line bhw P_1 & P_3].

When $P_1 = P_2$, slope = 0, $\Rightarrow \lambda = 0$. So we consider a tangent: $\lambda = \frac{dy}{dx}$.

For $y^2 = x^3 + ax + b$.

$2y \frac{dy}{dx} = 3x^2 + A$.

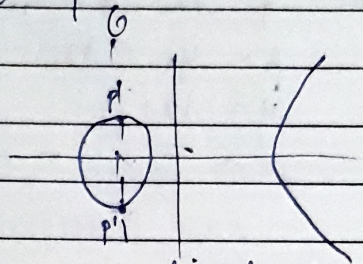
$\frac{dy}{dx} = \frac{3x^2 + A}{2y}$.

If $P_1 = P_2$: $\lambda = \frac{3x^2 + A}{2y}$.

$P_1 \neq P_2$: $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

In elliptic curve, the identity element is addition is ∞ ($\mathcal{O}$).

$\because P + \mathcal{O} = P$.



$P + \mathcal{O}$ draws a vertical line through P. It gives P', which is the point where the vertical line intersects other that at P in the curve.

If $P_1 + P_2 = \mathcal{O}$, then $P_1 + P_1' = \mathcal{O}$ since P_1' & P_2' are reflections. ???

$P_1 + -P_1 = \mathcal{O}$.

Then $-P_1$ is the inverse of P_1.

Elliptic Curve Addition Algorithm:

$E = y^2 = x^3 + Ax + B$.

- If $P_1 = \mathcal{O}$, then $P_1 + P_2 = P_2$.
- ~~If $P_1 = \mathcal{O}$~~ $P_1 = (x_1, y_1)$ & $P_2 = (x_2, y_2)$;
  If $x_1 = x_2$, $y_1 = -y_2$; then $P_1 + P_2 = \mathcal{O}$.
- $\lambda = \begin{cases} y_2 - y_1 / x_2 - x_1 & : P_1 \neq P_2 \\ 3x^2 + A / 2y & : P_1 = P_2 \end{cases}$
- $x_3 = \lambda^2 - x_1 - x_2$. $\quad y_3 = \lambda(x_1 - x_3) - y_1$.

Qn On an elliptic curve, $y^2 = x^3 - 43x + 166$. Calculate the addition of 2 points P_1 & P_2, $P_1 = (-5, -16)$; $P_2 = (11, 32)$.

$P_1 \neq P_2$ $\therefore \lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{32+16}{11+5} = \frac{48}{16} = \frac{6}{2} = 3$

$x_3 = \lambda^2 - x_1 - x_2 = 9 + 5 - 11 = 3$.

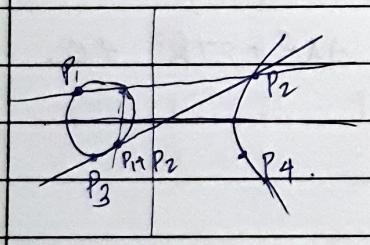
$y_3 = \lambda(x_1 - x_3) - y_1 = 3(-5-3) + 16 = -24 + 16 = -8$.

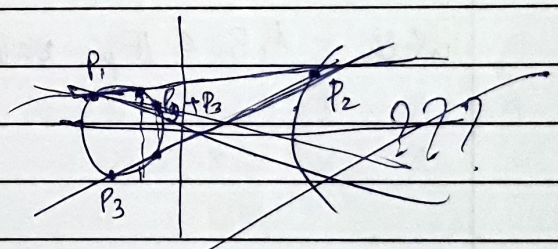
$\therefore P_1 + P_2 = (3, -8)$.

10 Oct

Associativity:

Check if $(P_1 + P_2) + P_3 = P_4 == P_1 + (P_2 + P_3) = P_4$.





But apparently, they're the same. :D.

Group structure:

Addition:

Identity, Inverse, Associative, Closed, Commutative.

* Bezout's Theorem:

If the degree of 2 curves are different, then the number of intersection points = no(deg(curve 1)) * no(deg(curve 2)).

__/__/___

* Points of finite order:

$E[n] = \{P \in E : nP = O\}$.

$\underbrace{P+P+P+\cdots\cdots+P}_{n \text{ times}} = O$.

Let $n \geq 1$ be an integer. A point $P \in E$ satisfying $nP = O$ is called a point of order n.

* Elliptic Curve over Finite Fields:

Let $p \geq 3$ be a prime. An elliptic curve over $\mathbb{F}_p$ is an eqn of the form:

$E : y^2 = x^3 + Ax + B$.

with $A, B \in \mathbb{F}_p$ satisfying $4A^3 + 27B^2 \neq 0$.

Ex: Consider an elliptic curve $Y^2 = X^3 + 3X + 8$ over the field $\mathbb{F}_{13}$.

0 - 0.	9 - 3.		
1 - 1	10 - 9.		
2 - 4	11 - 4.		
3 - 9	12 - 1.		
4 - 3			
5 - 12			
6 - 10			
7 - 10			
8 - 12.			

Put X values in Y^2 eqn.

For value of X, if Y^2 satisfies $Z^2 \equiv Y^2_{val} \pmod{13}$.

Check square root (mod 13).

$0 = 8 \Rightarrow X$.

$1 = 12 \Rightarrow \checkmark (5, 8)$.

$2 = 22 = 9 \Rightarrow \checkmark (3, 10)$.

$3 =$

14 Oct.

~~(9,6) (9,7) (12,~~

$\Rightarrow \{ 0, (1,5) (1,8) (2,3) (2,10), (9,6), (9,7), (12,2), (12,11) \}$.

$(1,5) + (1,8) = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-5}{1-1} = \underline{\underline{\infty}}$.

$(1,8) + (1,5) = \infty \Rightarrow$ Inverse.

$(2,3) + (2,10) = \frac{y_2 - y_1}{x_2 - x_1} = \frac{10-3}{2-2} = \underline{\underline{\infty}}$.

Qn. Find # all points over elliptic curve $Y^2 = X^3 + 1$ over finite field F_{11}.

$4A^3 + 27B^2 \Rightarrow 4(0)^3 + 27(1)^2 = 27 \neq 0$ ✓.

$F_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$.

$x^2 = \{ 0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1 \}$.

$\rightarrow \{ 0, 1, 3, 4, 5, 9 \}$.

$x =$	0	1	2	3	4	5	6	7	8	9	10.
$y^2 =$	1	2	9	6	10	5	8	3	7	4	0
	✓	x	✓	x	x	✓	x	✓	x	✓	✓

Points = $\{ (0,1), (0,10), (2,3), (2,8), (5,4), (5,7), (7,5), (7,6), (9,2), (9,9), (10,0), \infty \}$.

↑ Elliptic curve on finite field M's points.




1013?

for exam: 2nd test + 3rd module.

15 Oct

* Elliptic Curve Discrete Logarithm problem (ECDLP):

Discrete Logarithm Problem:

$a^x \bmod p = b$

Easy to find b but difficult to find x.

n is considered private key if

$nP = Q$ [i.e. $P+P+P+P\cdots+P$, n times].

$nP = Q$.

$n = P/Q$. $\log n = \log_Q P$.

One way function.

Elliptic Diffie-Hellman Key exchange.

Alice: $Q_A = n_A P$.

Bob: $Q_B = n_B P$.

$n_A Q_B = n_A (n_B P) = n_B (n_A P)$
$= n_B Q_A$.

Qn. Alice and Bob decide to use elliptic Diffie-Hellman with the following prime, elliptic curve and point.

$p = 23$; $E = y^2 = x^3 - 2x + 5$; Point $= (4,5) \in E(F_{23})$.

Alice and Bob chooses respective secret values $n_A = 3$ & $n_B = 7$. Compute public keys for both & symmetric shared secret key.

$Q_A = n_A P = 3 \cdot (4,5)$ $3x^2+A / 2y$.

$= 2P + P = (4,5) + (4,5) + P = \frac{3(16)+2}{2(5)} = 46/10$.

$= 46 \pmod{23} / 10 \pmod{23} = 0$.

$x_3 = \lambda^2 - 2x_1 = 0^2 - 9 = -9 \pmod{23} = 15$.

$y_2 = \lambda(x_1 - x_3) - y_1 = 0 - y_1 = -5 \bmod 23 = 18$.

$\Rightarrow 2P = (15, 18)$.

$3P = (15,18) + (4,5) = \frac{y_2 - y_1}{x_2 - x_1}$

$= \frac{5-18}{4-15} = \frac{+13}{+11}$

$Q_B = n_B P = 7P = 2P + 2P + 3P$.

$(15,18) + (15,18) = \frac{3(15^2) + -2}{2(18)}$

$= \frac{673}{36} = \frac{6}{13}$.

$x_3 = \lambda^2 - 2x_1 = (\frac{6}{13})^2 - 2(15) = \frac{36}{169} - 30$

$= \frac{13}{8} - 37 = \frac{43}{8} = \frac{20}{8} = 2.5$???

$y_3 = \lambda(x_1 - x_3) - y_1 = \frac{6}{13}(15 - 2.5) - 18$

$= \frac{75}{13} - 18 = \frac{6}{13} - 18 = \frac{228}{13} = \frac{21}{13} = 1.62$??

??? HUH?

Nevermind.

$7P = 3P + 3P + 1P$.

$= \frac{13}{11} + \frac{13}{11} + ($

$3P = (15,18) + (4,5) = \frac{y_2 - y_1}{x_2 - x_1}$

$= \frac{5-18}{4-15} = \frac{13}{11} \bmod 23 =$ since it's in decimal,

$= 13 \cdot 11^{-1} \pmod{23}$.

$4 \cdot 11^{-1} \bmod 23)$

$11^{-1} \bmod 23 = 21$:

$3P = \frac{20}{1} = 20$.

$x_3 = \lambda^2 - x_1 - x_2 = 20^2 - 15 - 4 = 381 \cdot 1 \cdot 23 = 13$

$y_3 = \lambda(x_1 - x_3) - y_1 = 20(15 - 13) - 18 = 22$

$Q_A = (13, 22)$ $(3x^2 + A / 2y)$.

$Q_B = 3P + 3P + P = 7P = 2P + 2P + 3P$.

$3P + 3P = (13,22) + (13,22) = \frac{3(13)^2 + 2}{2(22)} = \frac{508}{44}$? $2P$

__/__/___

$7P + 3P = (15,18) + (15,18)$ $\quad 3x^2 + A / 2y$.

$= \frac{3(15)^2 - 2}{2(18)} = \frac{673}{36} = \frac{6}{13}$.

$\lambda = \frac{6 \cdot 13^{-1}}{13 \cdot 13^{-1}} \bmod 23 = \frac{6 \cdot 16}{13 \cdot 16} \bmod 23 = 4$.

$x_3 = \lambda^2 - x_1 - x_2 = 16 - 15 - 15 = -14 \bmod 23 = 9$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 4(15 - 9) - 18 = -6 \bmod 23 = 17$.

$\therefore 4P = (9,6)$.

$\Rightarrow 7P = 4P + 3P = (9,6) + (13,22)$. $\quad \frac{y_2 - y_1}{x_2 - x_1}$.

$= \frac{22-6}{13-9} = \frac{16}{4} = 4$.

~~$\lambda = 16 \cdot 4 \bmod 23$~~

~~$4 \cdot 4^{-1}$~~

$x_3 = \lambda^2 - x_1 - x_2 = 16 - 9 - 13 = -6 \bmod 23 = 17$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 4(9 - 17) - 6 = -38 \bmod 23 = 8$.

$\therefore 7P = (17,8)$.

Shared key $= n_A Q_B = n_B Q_A$.

$3(17,8) = (17,8) + (17,8) + (17,8)$.

$2Q_B = (17,8) + (17-8)$ $\quad 3x^2 + A / 2y$.

$= \frac{3(17)^2 + -2 / 2(8)}{16} = \frac{865}{16} = \frac{14}{16} = \frac{7}{8}$.

$\lambda = \frac{7 \cdot 8^{-1}}{8 \cdot 8^{-1}} \bmod 23 = 7 \cdot 3 \bmod 23 = 21$.

$x_3 = \lambda^2 - x_1 - x_2 = 441 - 17 - 17 = 407 \bmod 23 = 16$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 21(17 - 16) - 8 = 13$.

$\frac{y_2 - y_1}{x_2 - x_1}$.

$3Q_B = (16,13) + (17,8) = \frac{8-13}{17-16} = \frac{-5}{1} = 18$.

$x_3 = \lambda^2 - x_1 - x_2 = 18^2 - 16 - 17 = 291 = 15$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 18(16 - 15) - 13 = 5$.

$\therefore$ shared key $= (15,5)$.

__/__/__

Shared key = $n_B Q_A = 7(13,22)$ = ~~3+3+1~~ 2,2,3

$3(13,22) = 2(13,22) + 1(13,22)$.

$2(13,22) = (13,22) + (13,22)$ $\quad 3x^2+A/2y$.

$= 3(13^2) - 2/2(22) = 505/44 = 22/21$.

$\lambda = \frac{22 \cdot 21^{-1}}{21 \cdot 21^{-1}} \bmod 23 = 22 \cdot 11 \cdot \bmod 23 = 12$//

$x_3 = \lambda^2 - x_1 - x_2 = 12^2 - 13 - 13 = 118 - 1 \cdot 23 = 3$//

$y_3 = \lambda(x_1 - x_3) - y_1 = 12(13-3) - 22 = 98 - 1 \cdot 23 = 6$//

$2(13,22) = (3,6)$.

$3(13,22) = (3,6) + (13,22)$. $\quad y_2 - y_1 / x_2 - x_1$.

$= 22-6/13-3 = 16/10 = 8/5$.

$\lambda = 8 \cdot 5^{-1} \bmod 23 = 8 \cdot 14 - 1 \cdot 23 = 20$//

$\uparrow_{14}$

$x_3 = \lambda^2 - x_1 - x_2 = 20^2 - 3 - 13 = 384 = 16$//

$y_3 = \lambda(x_1 - x_3) - y_1 = 20(3-16) - 6 = 10$//

$3(13,22) = (16,10)$//

∴ 2+2 = 4 $\quad 3x^2+A/2y$.

$4(13,22) = (3,6) + (3,6) = 3(9) - 2/2(6) = 25/12$.

$\lambda = 25 \cdot 12^{-1} \bmod 23 = 25 \cdot 2 \bmod 23 = 4$

$\uparrow_2$

$x_3 = \lambda^2 - x_1 - x_2 = 4^2 - 3 - 3 = 10$//

$y_3 = \lambda(x_1 - x_3) - y_1 = 4(3-10) - 6 = 12$//

4+3=7: $(10,12) + (16,10) = 10-12/16-10 = -2/6$ ~~y_2-y_1/x_2-x_1~~.

$= -1/3 = 22/3$.

$\lambda = 22 \cdot 3^{-1} \bmod 23 = 22 \cdot 8 \bmod 23 = 15$//

$\uparrow_8$

$x_3 = \lambda^2 - x_1 - x_2 = 15^2 - 10 - 16 = 199 - 1 \cdot 23 = 15$//

$y_3 = \lambda(x_1 - x_3) - y_1 = 15(10-15) - 12 = 5$//

∴ $n_B Q_A = (15,5) = n_A Q_B$//

WATER.

__/__/__

\$ 14 Oct.

* Factorization using Elliptic Curve :- Lenstra's Algo:

$kP = 0$

$(k-1)P + P = 0.$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod N.$

If $(x_2 - x_1) \bmod N = 0$, $(y_2 - y_1) * (x_2 - x_1)^{-1} \bmod N.$

↓ ~~get~~ $GCD(x_2 - x_1, N) = 1$,

$GCD(x_2 - x_1, N) \neq 1$, So there exists no inverse, also, N has a factor.

Qu Factor 493 using Elliptic curve $y^2 = x^3 + x + 1$, and point on curve $(0,1)$.

→ $j = 2! = 2.$ $(3x^2+A)/2y.$

$2P = (0,1) + (0,1) = [3(0)^2 + 1]/2(1) = 1/2.$

$\lambda = \frac{1}{2} \cdot \frac{2^{-1} \bmod 493}{2^{-1} \bmod 493} = 247 \cdot 1 \cdot 493 = \underline{247}.$ (247)

$x_3 = \lambda^2 - x_1 - x_2 = 247^2 - 0 - 0 = \underline{370}.$

$y_3 = \lambda(x_1 - x_3) - y_1 = 247(0 - 370) - 1 = \underline{307}.$

→ $2P = (370, 307).$

$j = 3! = 6.$

$6P = 2P + 2P + 2P.$

$4P = (370, 307) + (370, 307) = 3(370)^2 + 1 / 2(307) = 32/121.$

$\lambda = \frac{32 \cdot 121^{-1} \bmod 493}{121 \cdot 121^{-1}} = 32 \cdot 383 \bmod 493 = \underline{424}.$ (383)

$x_3 = \lambda^2 - x_1 - x_2 = 424^2 - 370 - 370 = 71.$

$y_3 = \lambda(x_1 - x_3) - y_1 = 424(370 - 71) - 307 = \underline{182}.$

$4P = (71, 182).$

$293^{-1} \bmod 493$.

$493 = (1)293 + 200$.
$293 = (1)200 + 93$.
$200 = (2)93 + 14$.
$93 = (6)14 + 9$.
$14 = (1)9 + 5$.
$9 = (1)5 + 4$.

__/__/__

$6P = 4P + 2P = (77, 182) + (370, 307)$

$\frac{y_2 - y_1}{x_2 - x_1}$.

$\lambda = 304 - 182 / 370 - 77 = 125/293$.

~~GCD (493, 293) = 3 ≠ 1.~~

~~Since GCD (493, 293) ≠ 1, inverse does not exist.~~
~~293^{-1} mod 493 does not exist.~~

$\therefore$

$\lambda = 125 \cdot 293^{-1} \bmod 493 = 125 \cdot 387 \cdot 1 \cdot 493 = 61$.
($293^{-1} = 387$)

$x_3 = \lambda^2 - x_1 - x_2 = 61^2 - 77 - 370 = 316$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 61(77 - 316) - 182 = 29$.

$\Rightarrow 6P = (316, 29)$.

$A! = 4(6P)$.

$2(6P) = (316, 29) + (316, 29) = 3(316)^2 + 1 / 2(29) = 318/58 = 159/29$.

GCD (29, 493) = 17

Since GCD (29, 493) ≠ 1, inverse does not exist.
29^{-1} mod 493 does not exist.
When inverse doesn't exist, we get the factors, Yoo!!

Factor 1 = 17, factor 2 = 493 / 17 = 29.

21 Oct.

A ElGamal Cryptosystem is Elliptic curve:

Alice: $Q_A = n_A P$. ⟶ Q_A - Public key.
Bob: M - plaintext. k - random element.
Use Q_A to compute:
$C_1 = kP \in E(F_p)$.
$C_2 = M + kQ_A \in E(F_p)$.
Send ciphertext (C_1, C_2).
Alice: $C_2 - n_A C_1 \in E(F_p) = M$.

Qn: Point $P = (5,1)$, $y^2 = x^3 + 2x + 2$ F_{17}.
$n_A = 6$; $M = (3,10) \in E(F_p)$. $k = 3$.
Compute publickey (Alice), Ciphertext to be sent by Bob.
Decrypt the ciphertext at Alice.

→ $Q_A = n_A P = 6(5,1)$.

$3x^2 + A / 2y$.

$2(5,1) = 3(5)^2 + 2 / 2(1) = 77/2$.

$\lambda = 77 \cdot 2^{-1} \bmod 17 = 77 \cdot 9 \bmod 17 = 13$.
(2 → 9)

$x_3 = \lambda^2 - x_1 - x_2 = 13^2 - 5 - 5 = 6$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 13(5-6) - 1 = 3$.

$2(5,1) = (6,3)$.

~~$3P = (5,1) + (6,3) = \frac{y_2 - y_1}{x_2 - x_1}$~~

$3P = (6,3) + (5,1)$ $(5,1) + (6,3) = \frac{y_2 - y_1}{x_2 - x_1} = 3-1 / 6-5 = 2$.

$x_3 = 2^2 - 5 - 6 = 10$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 2(5-10) - 1 = 6$.

$3P = (10,6)$.

$3x^2 + A / 2y$.

$6P = (10,6) + (10,6) = 3(10^2) + 2 / 2(6) = 151/6$.

$\lambda = 151 \cdot 6^{-1} \bmod 17 = 151 \cdot 3 \bmod 17 = 11$.
(6 → 3)

$x_3 = \lambda^2 - x_1 - x_2 = 11^2 - 10 - 10 = 101 \bmod 17 = 16$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 11(10 - 16) - 6 = 13$.

$6P = (16,13)$.

$C_1 = kP = 3P = (10,6)$.

$C_2 = M + kQ_A = (3,10) + 3(16,13)$.

$2(16,13) = 3(16)^2 + 2 / 2(13) = 385/13$.

$\lambda = 385 \cdot 13^{-1} \bmod 17 = 385 \cdot 4 \bmod 17 = 10$.
(13 → 4)

$x_3 = \lambda^2 - x_1 - x_2 = 10^2 - 16 - 16 = 68 \bmod 17 = 0$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 10(16 - 0) - 13 = 11$.

$2(16,13) = (0,11)$.

$3(16,13) = (16,13) + (0,11) = \frac{y_2-y_1}{x_2-x_1} = \frac{11-13}{0-16} = \frac{-2}{-16} = \frac{1}{8}$.

$\lambda = 1 \cdot 8^{-1} \bmod 17 = 15 \cdot 1 \cdot 17 = 15$.

$x_3 = \lambda^2 - x_1 - x_2 = 15^2 - 16 - 5 = 5$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 15(16-5) - 13 = 16$.

$3P = (5,16)$.

$\therefore C_2 = (3,10) + 3(16,13)$

$= (3,10) + (6,1) = \frac{y_2-y_1}{x_2-x_1} = \frac{1-10}{6-3} = \frac{-9}{3} = -3$

$x_3 = \lambda^2 - x_1 - x_2 = (-3)^2 - 3 - 6 = 0$.

$\therefore C_2 = (3,10) + (5,16) = \frac{y_2-y_1}{x_2-x_1} = \frac{16-10}{5-3} = \frac{6}{2} = 3$.

$x_3 = \lambda^2 - x_1 - x_2 = 9 - 3 - 5 = 1$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 3(3-1) - 10 = 13$.

$\therefore C_2 = (1,13)$.

$(C_1, C_2) = ((10,6), (1,13))$.

Decryption: $M' = C_2 - n_A C_1$.

$n_A C_1 = 6(10,6)$.

$2(10,6) = (16,13)$.

$3(10,6) = (7,6)$.

$6(10,6) = (5,16)$.

$M' = (1,13) - (5,16)$. $-(5,16)$ = reflection on x axis.

$= (1,13) + (5,-16) = (1,13) + (5,1)$ $[\because -16 \% 17 = 1]$.

$M' = \frac{y_2-y_1}{x_2-x_1} = \frac{1-13}{5-1} = \frac{-12}{4} = -3 = 14$.

$x_3 = \lambda^2 - x_1 - x_2 = 14^2 - 1 - 5 = 3$.

$y_3 = \lambda(x_1 - x_3) - y_1 = 14(1-3) - 13 = 10$.

verified !!

$M' = (3,10)$.