Cybersecurity Mathematics

Chapter 3

*** Euler Theorem 1 :-**

If n is positive integer and a , n are relatively prime , then

$$a^{\phi(n)} = 1 (\text{mod } n)$$

where $\phi(n)$ is Euler-phi function (totient)

EX: 1) $a^4 = 1 \text{ mod } 15$, a=1,2,4,7, 8, 11, 13,14 right

EX : 2) $a^4 = 1 \text{ mod } 15$,a= 3, 5,6 9, 10 ,12 wrong

How to solve it:-

gcd (3 | 15) , gcd (5 | 15) , ……………. !=1 (not relatively Prime)

gcd (1 , 15) , gcd (2 , 15) , gcd (4 , 15) ,………= 1 (relatively Prime)

Ex: 3) $3^{10} \text{ mod } 13 \rightarrow (3^3 . 3^3 . 3^3 . 3^1) \text{ mod } 13 = 3$

Example : Solve 3^{202} mod 13 by Euler theorem? a=3 ,n= 13 , Φ (n) = (13) = n-1 = 12

$$\begin{array}{r|l} & 16 \\ \hline 12 & 202 \\ & -192 \\ \hline & 10 \end{array}$$

check (a , n) is it prime? → yes : 202= 12*16 +10

(3,13) relatively prime? Yes

→$3^{12*16+10}$ mod 13 = 3^{12*16} * 3^{10} mod 13 = $(3)^{(12)\text{^}16}$ * 3^{10}

= 1^{16} * 3^{10} mod 13 =3^{10}

Example: Solve 4^{99} mod 35 by Euler theorem? a=4 , n=35

$\Phi(n) = \Phi(35) = (P-1)(q-1) = 4*6 = 24$

$4^{\Phi(n)} = 1 \pmod{n}$ → $4^{24} = 1$mod

35 Check:

(4 ,35) is it relatively prime? → yes

99 = 24*4+3

→$4^{24*4+3} = (4)^{24\wedge 4} * 4^{3} = 1 * 4^{3}$ mod 35 = 29

$$\begin{array}{r|l} & 4 \\ \hline 24 & 99 \\ & -96 \\ \hline & 3 \end{array}$$

- **Euler theorem :**

let p and q be distinct

primes and let $g = \gcd(p-1, q-1)$, then:- $(p-1)$

$(q-1) / g = 1 \mod pq$ for all a

Such that $\gcd(a, pq)=1$

in Particular, If p,q are odd Primes then $a(p-1)(q-1)/2 = 1 \mod pq$, for all a s.t

→$\gcd(a , pq) =1$

***Proposition: Let p be a prime and Let $e > 1$ be an integer**

Satisfying $\gcd(e, p-1) = 1$

$de = 1 \pmod{p-1}$

then $x^e = c \mod p$ *has -unique Solution:

- $X = c^d \mod p$

Example : $X^{19} = 36 \pmod{97}$

$e = 19$, $c = 36$, $p = 97$

$\gcd(19, 96) = 1$

$19 * d = 1 \bmod (96)$

$d = 91$

$X^{19} = 36^{91} \bmod 97$ → using fast powering

$X = 36 \bmod 97$

Ex: using Euler theorem to find the unit digit m

last digit

3^{100} ? $a^{\Phi(n)} = 1 (\mathrm{mod}\ n)$

$a=3$, $n=10$ n=10 , because we need the last digit

$a^{100} = 1 \ (\mathrm{mod}\ 10)$

$\Phi(n) = \Phi(10) = (5-1)(2-1) = 4$

$3^{4*25} \rightarrow 3^4 = 1 \mathrm{mod}\ 10$

$3^{(4)^{\wedge}25} = 1^{25} \mathrm{mod}\ 10 = 1$

$3^4 \mathrm{mod} 10 = 1$

X Primality Test : there is two way to check if number is prime or not

1) Fermat's Test

is p prime ?

→Fermat's theorem $a^p = a \mod p$ for integer a

Ex : is 5 prime ?

1. $5 \mid 1^5 - 1$? yes
2. $5 \mid 2^5 - 2$? yes
3. $5 \mid 3^5 - 3$? yes
4. $5 \mid 4^5 - 4$? yes

$1 \leq a < p$

$1 \leq a < 5$

$p \mid a^p - a$??

2) Miller-Robin Test:

Algo: Input : Integer n to be tested, integer a as a potential witness

1) if n is even or $1 < \gcd(a, n) < n$ return composite

2) write $n-1 = 2^k * q$ with q odd

3) Set $a = a^q \pmod{n}$

4) if $q = 1 \bmod n$, return test fails

5) Loop i : 0, 1 , 2 , … , k-1

6) If $a = -1 \pmod{n}$ return fail test.

7) Set $a = a^2 \pmod{n}$

8) Return Composite

Ex: use Miller-Robin primality test to check if 53 is a prime number STEPS:-

1)Find $n-1 = 2^k.q$

2)Choose a : $1 < a < n-1$

3)Compute $b0 = a^q \bmod n$

-> $bi = bi^2$ –

1Note*.

If rule 4 → +-1 probably prime

-1 → prime

+1 → not prime

Miller-Robin primality test STEPS:-

1)Find n-1 = $2^k.q$

2)Choose a : 1< a<n-1

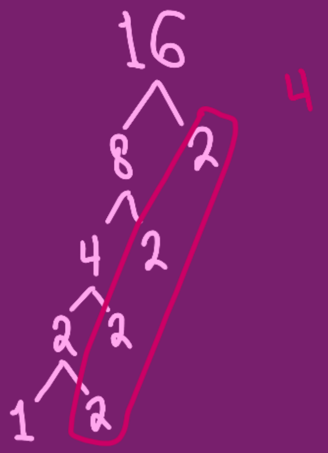
3)Compute b0 = a^q mod n

Example : using Miller – Rabin primality test check if 17 is prime ??

① **Find 17 -1 = 2^k ***

q 16 = 2^k *q

$\therefore q = 1$, $K = 4$



choose from

② $a : [2 - 15]$

$a = 2$

③ $b_0 = 2^1 \pmod{17} = \boxed{2}$

If not equal ± 1 continue

$b_1 = 2^2 \pmod{17} = 4$

$b_2 = 4^2 \pmod{17} = -1$

$\therefore$ 17 is prime

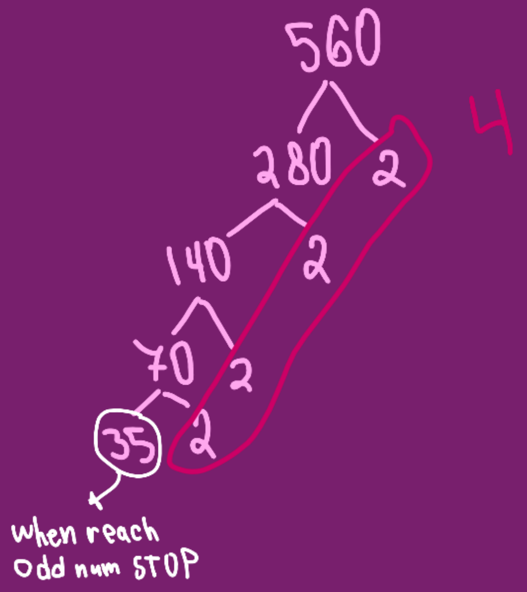
Ex: using Miller-Robin primality test to check if 561 is a prime number ??

$561 - 1 = 2^k * q$

$560 = 2^k * q$

$560 = 2^4 * 35$

∴ $k=4$, $q=35$



Choose a: [2 , 259] a=2

If b0 = ±1 , choose another a

$\boxed{b0} = a^q \bmod n$

$b0 = 2^{35} \bmod 561$

...

$= 263 \neq \pm 1$

$b1 = (263)^2 \bmod 561$

$= 166 \neq \pm 1$

$b2 = (166)^2 \bmod 561$

$= 67 \neq \pm 1$

$b3 = (67)^2 \bmod 561 = \boxed{1}$ → 561 not prime (It is composit)

3.5 : Pollards p-1 factorization Algorithm :

Suppose p , q are numbers and $N = p * q$ the Euler Fermat's theorem guarantees

$a^{p-1} = 1 \bmod p$ for all a relatively prime to p

while we do not know p we can see that happens if we work with it

suppose p - 1 is factor of L then $L = (p - 1) * k$ so $a^L = a^{P-1^k} \bmod P = 1 \bmod P$

consequently, P divides $a^L - 1$ and since p is a factor of N then $\gcd(a^L - 1, N)$ Will include P

One problem : How do we find L ??

To find some number N , choose a relatively prime to N then :

1. Evaluate $a^{k!}$, for k=1,2,3…. Up to some practical limit
2. Find the gcd $((a^{k!} - 1) \bmod N), N)$
3. Any non-trival gcd is a factor of N

Example : factor 1403 using pollards p-1 method ??

a is relatively p
gcd (2, 1403) = 1

$\boxed{a=2}$, $k=1,2,3\ldots\ldots$

$a^{k!} = 2^1 = 2$

$\gcd((a^{k!}-1) \bmod N), N)$

$\gcd((2^1-1) \bmod 1403), 1403)$

$\gcd(1, 1403) = 1$

$2^{2!} \bmod 1403 = 4 \longrightarrow \gcd(4-1, 1403) = 1$

$2^{3!} \bmod 1403 = 64 \longrightarrow \gcd(64-1, 1403) = 1$

$2^{4!} \bmod 1403 = (64)^4 \bmod 1403 = 142 \longrightarrow \gcd(142-1, 1403) = 1$

$2^{5!} \bmod 1403 = (142)^5 \bmod 1403 = 794 \longrightarrow \gcd(794-1, 1403) = 61$

Not equal 1 so
we have to
STOP
61 is a factor

$\therefore 1403 = 61 * 23$

$\boxed{\frac{1403}{61}}$

Pollards Algorithm :

Input: Enter N to be factored

1. Set a =2 (or some other convenient value)
2. Loop i=1,2,3,4…. Up to specified bound
3. Set $a = a^i \bmod N$
4. Compute d= gcd (a-1 ,N)
5. If $1<d<N$ then success , return d
6. Increment loop again at step 2.

Factorization vi difference of sequence :

$X^2 - y^2 = (x - y)(x + y)$

Example : factor 35 by using difference

sequences ? $35 + 1^2 = 36 = 6$

$35 = (6 - 1)(6 + 1)$

$35 = (5)(7)$

Index Calculus Algorithm:

1. Configure: Choose a factor base $B = \{P1, P2, P3 \ldots\ldots, PB\}$
2. Collect relations: Determine discrete logarithms (DL) of primes in B.
3. Combine: Compute DL of y based on DL of primes in B.

Task 1 and Task 2 are pre-computation. Task 3 is repeated for each query Core :

1. Any natural number can be factored into prime numbers.
2. As with the ordinary logarithm, there is a link between multiplication of natural numbers and addition of DL

$$q1 * q2 * q3 \ldots\ldots qn \pmod p$$

$$\text{Log}(q1 * q2 * q3 \ldots\ldots qn) = \log q1 + \log q2 + \log q3 \ldots. + \log qn \pmod{p-1}$$

Recall : **DL are defined only Modula P-1**

Task 2 : for random ti , try factor g^{ti} over B to get many relations

$\log_g(g^{ti} = P1^{a1\,I} * P2^{a2\,i} \dots PB^{ab\,i} \pmod p)$)

Task 3: We want to solve $y = g^x \pmod p$). Repeat until successful.

1. **Choose a random number ($1 < s < p - 1$) and compute $c = y * g$^s (mod p).**
2. **Try to factor c over the factor base B . If successful, we have:**

$y * g^s = p1^{c1} * p2^{c2} \quad pb^{cb} \pmod p$)

3. **Apply $\log_g$ on both sides to recover**

$x = \log_g y + s \log_g g = c1 \log_g p1 + c2 \log_g p2 + cb \log_g pb \bmod (p-1)$

Example : Solve $37 = 2^x \pmod{131}$ using factor base $B = \{2,3,5,7\}$

Task 2 : choose some random numbers

$g = 2$ $\quad$ $t_i = \{1, 8, 12, 14, 34\}$ factor g^{t_i} over B

$2^1 = 2^1 \pmod{131}$ $\longrightarrow$ $1 = \log_2 2 \pmod{130}$

$2^8 = 125 \pmod{131} = 5^3 \pmod{131}$ $\longrightarrow$ $8 = 3\log_2 5 \pmod{130}$

$2^{12} = 35 \pmod{131} = 5*7 \pmod{131}$ $\longrightarrow$ $12 = \log_2 5 + \log_2 7 \pmod{130}$

$2^{14} = 9 \pmod{131} = 3^2 \pmod{131}$ $\longrightarrow$ $14 = 2\log_2 3 \pmod{130}$

$2^{34} = 75 \pmod{131} = 3 * 5^2 \pmod{131}$ $\longrightarrow$ $34 = \log_2 3 + 2\log_2 5 \pmod{130}$

$\boxed{3*b = 1 \pmod{130} \quad b = 87}$

$\text{Log}_2 2 = 1$

$\text{Log}_2 5 = 8 * 3^{-1} = 8 * 87 \pmod{130} = 46$ $\quad$ $\log_2 5 = 46 \pmod{130}$

$12 - 46 = \log_2 7 \pmod{130}$ $\quad$ $\log_2 7 \pmod{130} = 96$

$34 = \log_2 3 + 2(46)$ $\longrightarrow$ $\log_2 3 = 34 - 2(46) = 72 \pmod{130}$

Try random S. Compute $y * g^s \pmod{p}$ and hope it factor over B

$S=2 \longrightarrow 37 * 2^2 = 17 \pmod{131}$

$S=3 \longrightarrow 37 * 2^3 = 34 \pmod{131}$

$S=4 \longrightarrow 37 * 2^4 = 68 \pmod{131}$

$S=5 \longrightarrow 37 * 2^5 = 5 \pmod{131}$

$S=6 \longrightarrow 37 * 2^6 = 10 \pmod{131} = 2 * 5 \pmod{131}$

Note : Stop when the result is from group B, or if we can multiply two numbers from B group and get the same result. So in this example we can stop when S= 5 or when S=6

$\log_2 37 + 6 \log_2 2 = \log_2 2 + \overbrace{\boxed{\log_2 5}}^{46} \pmod{130}$

$\therefore \log_2 37 = (-6 + 1 * 1 + 1 * 46) \pmod{130}$

$\log_2 37 = 41 \pmod{130} \longrightarrow 37 = 2^{41} \pmod{131}$ $\boxed{x = 41}$

3.9 : Quadratic Residues and Quadratic Reciprocity:

Def : Let $a, n \in \mathbb{Z}$ with $n>0$ and $\gcd(a, n) = 1$ then a is said to be a quadratic residue Modula (n) if $x^2 \equiv a \pmod{n}$ is Solvable Otherwise, its quadratic nonresidue

Example : n=7 find QR and NR ?! $a \in \{1, 2, 3, 4, 5, 6\}$

$1^2 = 1 \bmod 7 = 1$
$2^2 = 1 \bmod 7 = 4$
$3^2 = 1 \bmod 7 = 2$
$4^2 = 1 \bmod 7 = 2$
$5^2 = 1 \bmod 7 = 4$
$6^2 = 1 \bmod 7 = 1$

$\therefore QR = \{1, 2, 4\}$

$\therefore NR = \{3, 5, 6\}$

Example : n=8 gcd (a,8) =1 {1,3,5,7}

$1^2 \bmod 8 = 1$
$3^2 \bmod 8 = 1$
$5^2 \bmod 8 = 1$
$7^2 \bmod 8 = 1$

$\therefore QR = \{1\}$

$\therefore NR = \{3, 5, 7\}$

Properties : QR *

$\boxed{QR = QR}$

$\boxed{QR * NR = NR}$

$\boxed{NR * NR = QR}$

Proposition :

Let p be odd prime $p \nmid a$ (p doesn't divide a) solving $ax^2 + bx + c = 0 \pmod p$)

$$\underbrace{(2ax + b)^2}_{x} = \underbrace{b^2 - 4ac}_{a} \pmod p$$

$b^2 - 4ac$ is QR modulo p

$P \mid b^2 - 4ac$ true if $b^2 - 4ac \pmod p = 0$

Example : using QR proposition / properties find the solution of $x^2 + 3x - 5 = 0 \pmod 7$)

Solution :

as we see the value of a= 1, b =3 , c =-5

$(2x + 3)^2 = 9 - 4(-5) \pmod 7) \longrightarrow (2x + 3)^2 = 1 \bmod 7$

The legende Symbo :

Def : $(q / p) = \begin{cases} 1 & \text{if } a \text{ is QR mod } p \\ -1 & \text{if } a \text{ is QNR mod } p \\ 0 & \text{if } p \mid a \end{cases}$

Example : n=7

$1^2 = 1 \bmod 7$

$2^2 = 4 \bmod 7$

$3^2 = 2 \bmod 7$

$4^2 = 2 \bmod 7$

$5^2 = 4 \bmod 7$

$6^2 = 1 \bmod 7$

$a \in (1 - (n-1)) \longrightarrow (1 - 6)$

* QR $\{1,2,4\}$, $\left(\frac{1}{7}\right) = 1$, $\left(\frac{2}{7}\right) = 1$, $\left(\frac{4}{7}\right) = 1$

* QNR $\{3,5,6\}$, $\left(\frac{3}{7}\right) = -1$, $\left(\frac{5}{7}\right) = -1$, $\left(\frac{6}{7}\right) = -1$

Theorem : (Euler criterian)

$(a / p) = a^{(p-1)/2} \mod p$, p is prime , $p \nmid a$

Ex : p = 7

$(1/7) = 1^3 \pmod 7 = 1$

$(2/7) = 2^3 \pmod 7 = 1$

$(3/7) = 3^3 \pmod 7 = -1$

$(4/7) = 4^3 \pmod 7 = 1$

$(5/7) = 5^3 \pmod 7 = -1$

$(6/7) = 6^3 \pmod 7 = -1$

Lemma :

let p be an odd prime , $p \nmid a$, let n= * least positive residues
Of a , 2a , 3a .....((p-1) /2) a that are greater than p/2 , then $(a/p) = (-1)^2$

Example :p = 13 , a=5

1*5 = 5 (mod 13)

2*5 = 10 (mod 13)

$> \frac{p}{2} = \frac{13}{2} = 6$

3*5 = 2 (mod13)

4*5 = 7 (mod13)

5*5 = 12 (mod13) = -1

6*5 = 4 (mod13)

to get the value n
we have to see how many
numbers gives result greater
than 6

as we see we have 3 num (7 ,10 ,12)

so $\boxed{n = 3}$, $(5 / 13) = 5^6 \pmod{13} = -1$

Properties : Let p be odd prime such that $p \nmid a$, $p \nmid b$ then

1- $(a^2 / p) = 1$

2- $(a / p) = (b / p)$ if $a \equiv b \pmod p$

3- $(a b / p) = (a / p) (b / p)$

Example : is -13 Quadratic Residue module 11?

$(-13 / 11) = (-1 / 11) (13 / 11) = (-1 / 11) (2 / 11)$

$(-1) (-1) = 1$ $\quad$ $-1 / 11 = (-1)^5 \bmod 11 = -1$

$\therefore$ TRUE $\quad$ $2 / 11 = 2^5 \bmod 11 = -1$

Lemma : p = odd prime , $p \nmid a$, a = odd

$$N = \sum_{j=1}^{p-1/2} \left\lfloor \frac{j*a}{p} \right\rfloor \quad \text{then } \left(\frac{a}{p}\right) = (-1)^{N}$$

Example : p = 13 , a = 9

$$\sum_{j=1}^{6} \left\lfloor \frac{9*j}{13} \right\rfloor = \left\lfloor \frac{9}{13} \right\rfloor + \left\lfloor \frac{18}{13} \right\rfloor + \left\lfloor \frac{27}{13} \right\rfloor + \left\lfloor \frac{36}{13} \right\rfloor + \left\lfloor \frac{45}{13} \right\rfloor + \left\lfloor \frac{54}{13} \right\rfloor$$

$$0 + 1 + 2 + 2 + 3 + 4 = 12$$

$$\therefore \left(\frac{9}{13}\right) = (-1)^{12} = 1 \longrightarrow \therefore 9 \text{ QR } 13$$

Quadratic Reciprocity :

Let p and q are odd numbers , then :

1) (-1 / p) = $\begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$

2) (2 / p) = $\begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8} \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8} \end{cases}$

3) (p / q) = $\begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \end{cases}$

Ex : Is 31 QR modulo 103

Find $(31/103) = (-1)(103/31)$ 103 mod 31

$= (-1)(10/31)$ use 2.1 $\left(\frac{2}{31}\right) = 1$

$= (-1)\boxed{(2/31)}(5/31)$

$= (-1)(1)(5/31)$ 31 mod 5 = 1

$= (-1)(1)\ (31/5)$

$= (-1/5) = 1$

Example : Find (139 / 433)

$(139 / 433) = (1)(433 / 139)$ → **use 3.1 433 = 1 (mod4)**

433 mod 139

$(16 / 139)$ → **QR since $16 = 4^2$ because its perfect square**

Find (523 / 1103)

$(523 / 1103) = (-1)\ (1103 / 523)$
$(-1)(57 / 523)$
$(-1)(1)(523 / 57)$
$(-1)(10 / 57)$
$(-1)(2/57)(5/57)$
$(-1)(1)(57/5)$
$(-1)(2/5)$ → $(-1)(-1) = 1$

Is there a solution for $x^2 = 1247 \pmod{1481}$

Find $(1247/1481) = (1)(1481/1247)$ use 3.1

$1247 = 29 * 43$

$=(1481/29)(1481/43)$

$=(2/29)(19/43)$

$=(-1)(43/19)(-1)$ use 2.2 and 3.2

$=(5/19) = (1)(19/5)$ use 3.1

$=(4/5)$ $4 = 2^2$

It's perfect square

$\therefore$ QR