11/01/22:

(1.) Consider $\mathbb{Z}_{17}^*$:

(a.) For every element, check if it is a generator of $\mathbb{Z}_{17}^*$? Does it generate a cyclic subgroup? If so, show the subgroups - prime (or) composite?

Sol:- Given, $\mathbb{Z}_{17}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$

$|\mathbb{Z}_{17}^*| = 16$.

Now,

1 is an identity element. So, we start checking from 2.

a=2:

$2^0 \bmod 17 = 1$
$2^1 \bmod 17 = 2$
$2^2 \bmod 17 = 4$
$2^3 \bmod 17 = 8$
$2^4 \bmod 17 = 16$
$2^5 \bmod 17 = 15$
$2^6 \bmod 17 = 13$
$2^7 \bmod 17 = 9$
$2^8 \bmod 17 = 1$
$2^9 \bmod 17 = 2$
$2^{10} \bmod 17 = 4$
$2^{11} \bmod 17 = 8$
$2^{12} \bmod 17 = 16$
$2^{13} \bmod 17 = 15$
$2^{14} \bmod 17 = 13$
$2^{15} \bmod 17 = 9$.

The elements of the set are, $\{1, 2, 4, 8, 9, 13, 15, 16\}$

∴ The set do not have all the elements of the set that are present in Z_{17}^*,

Hence 2 is not a generator.

Since there are 8 elements in the subgroup and hence it is a composite order subgroup.

Now for $a = 3$:

$3^0 \bmod 17 = 1$

$3^1 \bmod 17 = 3$

$3^2 \bmod 17 = 9$

$3^3 \bmod 17 = 10$

$3^4 \bmod 17 = 13$

$3^5 \bmod 17 = 5$

$3^6 \bmod 17 = 15$

$3^7 \bmod 17 = 11$

$3^8 \bmod 17 = 16$

$3^9 \bmod 17 = 14$

$3^{10} \bmod 17 = 8$

$3^{11} \bmod 17 = 7$

$3^{12} \bmod 17 = 4$

$3^{13} \bmod 17 = 12$

$3^{14} \bmod 17 = 2$

$3^{15} \bmod 17 = 6.$

The elements of the set are, $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$.

∴ The set is a cyclic subgroup as all the elements of the set are present in Z_{17}^*.

∴ 3 is a generator.

Since there are 16 elements in the subgroup and hence it is a composite order subgroup.

11/05/22

Now for $a=4$:

$4^0 \bmod 17 = 1$
$4^1 \bmod 17 = 4$
$4^2 \bmod 17 = 16$
$4^3 \bmod 17 = 13$
$4^4 \bmod 17 = 1$
$4^5 \bmod 17 = 4$
$4^6 \bmod 17 = 16$
$4^7 \bmod 17 = 13$
$4^8 \bmod 17 = 1$
$4^9 \bmod 17 = 4$
$4^{10} \bmod 17 = 16$
$4^{11} \bmod 17 = 13$
$4^{12} \bmod 17 = 1$
$4^{13} \bmod 17 = 4$
$4^{14} \bmod 17 = 16$
$4^{15} \bmod 17 = 13$

The elements of the set are, $\{1, 4, 16, 13\}$.

∴ The set do not have all the elements of the set that are present in Z^*_{17},

Hence 4 is not a generator.

Since there are 4 elements in the subgroup and hence it is a composite order subgroup.

Now for $a=5$:

$5^0 \bmod 17 = 1$
$5^1 \bmod 17 = 5$
$5^2 \bmod 17 = 8$
$5^3 \bmod 17 = 6$
$5^4 \bmod 17 = 13$
$5^5 \bmod 17 = 14$
$5^6 \bmod 17 = 2$
$5^7 \bmod 17 = 10$
$5^8 \bmod 17 = 16$
$5^9 \bmod 17 = 12$
$5^{10} \bmod 17 = 9$

$5^{11} \bmod 17 = 11$ $5^{15} \bmod 17 = 7$.

$5^{12} \bmod 17 = 4$

$5^{13} \bmod 17 = 3$

$5^{14} \bmod 17 = 15$

∴ The elements of the set are,

$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$.

∴ The set is a cyclic subgroup, as it has all the elements of the set that are present in Z_{17}^*.

∴ 5 is a Generator.

Since there are 16 elements in the subgroup and hence it is a composite order subgroup.

Now, For a = 6 :-

$6^0 \bmod 17 = 1$

$6^1 \bmod 17 = 6$

$6^2 \bmod 17 = 2$

$6^3 \bmod 17 = 12$

$6^4 \bmod 17 = 4$

$6^5 \bmod 17 = 7$

$6^6 \bmod 17 = 8$

$6^7 \bmod 17 = 14$

$6^8 \bmod 17 = 16$

$6^9 \bmod 17 = 11$

$6^{10} \bmod 17 = 15$

$6^{11} \bmod 17 = 5$

$6^{12} \bmod 17 = 13$

$6^{13} \bmod 17 = 10$

$6^{14} \bmod 17 = 9$

$6^{15} \bmod 17 = 3$.

∴ The elements of the set are, $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$.

∴ The set is a cyclic subgroup, as it has all the elements of the set that are present in Z_{17}^*.

∴ 6 is a Generator.

Since there are 16 elements in the subgroup and hence it is a composite order subgroup.

Now, for $a = 7$:

$7^0 \bmod 17 = 1$
$7^1 \bmod 17 = 7$
$7^2 \bmod 17 = 15$
$7^3 \bmod 17 = 3$
$7^4 \bmod 17 = 4$
$7^5 \bmod 14 = 11$
$7^6 \bmod 17 = 9$
$7^7 \bmod 17 = 12$
$7^8 \bmod 17 = 16$
$7^9 \bmod 17 = 10$
$7^{10} \bmod 17 = 2$
$7^{11} \bmod 17 = 14$
$7^{12} \bmod 17 = 13$
$7^{13} \bmod 17 = 6.$
$7^{14} \bmod 17 = 8.$
$7^{15} \bmod 17 = 5.$

∴ The elements of the set are, {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}.

∴ The set is a cyclic subgroup, as it has all the elements of the set that are present in Z_{17}^*.

∴ 7 is a Generator.

Since there are 16 elements in the subgroup and hence it is a composite order subgroup.

Now, For $a = 8$:

$8^0 \bmod 17 = 1$
$8^1 \bmod 17 = 8$
$8^2 \bmod 17 = 13$
$8^3 \bmod 17 = 2$
$8^4 \bmod 17 = 16$
$8^5 \bmod 17 = 9$
$8^6 \bmod 17 = 4$
$8^7 \bmod 17 = 15$
$8^8 \bmod 17 = 1$
$8^9 \bmod 17 = 8$
$8^{10} \bmod 17 = 13$
$8^{11} \bmod 17 = 2$
$8^{12} \bmod 17 = 16$
$8^{13} \bmod 17 = 9$
$8^{14} \bmod 17 = 4$
$8^{15} \bmod 17 = 15.$

∴ The elements of the set are, {1, 2, 4, 8, 9, 13, 15, 16}.

∴ The set do not have all the elements of the set that are present in Z_{17}^*,

Hence 8 is not a generator.

Since there are 8 elements in the subgroup and hence it is a composite order subgroup.

Now, For a = 9:

$9^0 \bmod 17 = 1$
$9^1 \bmod 17 = 9$
$9^2 \bmod 17 = 13$
$9^3 \bmod 17 = 15$
$9^4 \bmod 17 = 16$
$9^5 \bmod 17 = 8$
$9^6 \bmod 17 = 4$
$9^7 \bmod 17 = 2$
$9^8 \bmod 17 = 1$
$9^9 \bmod 17 = 9$
$9^{10} \bmod 17 = 13$
$9^{11} \bmod 17 = 15$
$9^{12} \bmod 17 = 16$
$9^{13} \bmod 17 = 8$
$9^{14} \bmod 17 = 4$
$9^{15} \bmod 17 = 2$.

∴ The elements of the set are,

$\{1, 2, 4, 8, 9, 13, 15, 16\}$.

∴ The set do not have all the elements of the set that are present in Z_{17}^*,

Hence 9 is not a generator.

Since there are 8 elements in the subgroup and hence it is a composite order subgroup.

Now, For $a = 10$:-

$10^0 \bmod 17 = 1$
$10^1 \bmod 17 = 10$
$10^2 \bmod 17 = 15$
$10^3 \bmod 17 = 14$
$10^4 \bmod 17 = 4$
$10^5 \bmod 17 = 6$
$10^6 \bmod 17 = 9$
$10^7 \bmod 17 = 5$
$10^8 \bmod 17 = 16$
$10^9 \bmod 17 = 7$
$10^{10} \bmod 17 = 2$.
$10^{11} \bmod 17 = 3$
$10^{12} \bmod 17 = 13$
$10^{13} \bmod 17 = 11$.
$10^{14} \bmod 17 = 8$
$10^{15} \bmod 17 = 12$.

∴ The elements of the set are,
$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$

∴ The set is a cyclic subgroup, as it has all the elements of the set that are present in Z_{17}^*.
∴ 10 is a Generator.

Since there are 16 elements in the subgroup and hence it is a composite order subgroup.

Now, For $a = 11$:-

$11^0 \bmod 17 = 1$
$11^1 \bmod 17 = 11$
$11^2 \bmod 17 = 2$
$11^3 \bmod 17 = 5$
$11^4 \bmod 17 = 4$
$11^5 \bmod 17 = 10$
$11^6 \bmod 17 = 8$
$11^7 \bmod 17 = 3$
$11^8 \bmod 17 = 16$
$11^9 \bmod 17 = 6$
$11^{10} \bmod 17 = 15$
$11^{11} \bmod 17 = 12$
$11^{12} \bmod 17 = 13$
$11^{13} \bmod 17 = 7$
$11^{14} \bmod 17 = 9$
$11^{15} \bmod 17 = 14$.

∴ The elements of the set are, {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}.

∴ The set is a cyclic subgroup, as it has all the elements of the set that are present in Z_{17}^*.

∴ 11 is a Generator.

Since there are 16 elements in the subgroup and hence it is a composite order subgroup.

Now, For a = 12 :-

$12^0 \bmod 17 = 1$ $\quad$ $12^8 \bmod 17 = 16$

$12^1 \bmod 17 = 12$ $\quad$ $12^9 \bmod 17 = 5$

$12^2 \bmod 17 = 8$ $\quad$ $12^{10} \bmod 17 = 9$

$12^3 \bmod 17 = 11$ $\quad$ $12^{11} \bmod 17 = 6$

$12^4 \bmod 17 = 13$ $\quad$ $12^{12} \bmod 17 = 4$

$12^5 \bmod 17 = 3$ $\quad$ $12^{13} \bmod 17 = 14$.

$12^6 \bmod 17 = 2$ $\quad$ $12^{14} \bmod 17 = 15$.

$12^7 \bmod 17 = 7$ $\quad$ $12^{15} \bmod 17 = 10$.

∴ The elements of the set are, {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}.

∴ The set is a cyclic subgroup, as it has all the elements of the set that are present in Z_{17}^*.

∴ 12 is a Generator.

Since there are 16 elements in the subgroup and hence it is a composite order subgroup.

Now, For $a = 13$:-

$13^0 \bmod 17 = 1$
$13^1 \bmod 17 = 13$
$13^2 \bmod 17 = 16$
$13^3 \bmod 17 = 4$
$13^4 \bmod 17 = 1$
$13^5 \bmod 17 = 13$
$13^6 \bmod 17 = 16$
$13^7 \bmod 17 = 4$
$13^8 \bmod 17 = 1$
$13^9 \bmod 17 = 13$
$13^{10} \bmod 17 = 16$
$13^{11} \bmod 17 = 4$
$13^{12} \bmod 17 = 1$
$13^{13} \bmod 17 = 13$
$13^{14} \bmod 17 = 16$
$13^{15} \bmod 17 = 4$.

∴ The elements of the set are, $\{1, 4, 13, 16\}$

∴ The set do not have all the elements of the set that are present in $\mathbb{Z}_{17}^*$,

Hence 13 is not a generator.

Since there are 4 elements in the subgroup and hence it is a composite order subgroup.

Now, For $a = 14$:-

$14^0 \bmod 17 = 1$
$14^1 \bmod 17 = 14$
$14^2 \bmod 17 = 9$.
$14^3 \bmod 17 = 7$
$14^4 \bmod 17 = 13$
$14^5 \bmod 17 = 12$
$14^6 \bmod 17 = 15$
$4^7 \bmod 17 = 6$.
$4^8 \bmod 17 = 16$.
$4^9 \bmod 17 = 3$
$4^{10} \bmod 17 = 8$.
$4^{11} \bmod 17 = 10$
$4^{12} \bmod 17 = 4$
$4^{13} \bmod 17 = 5$.
$4^{14} \bmod 17 = 2$.
$4^{15} \bmod 17 = 11$.

∴ The elements of the set are, {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}.

∴ The set is a cyclic subgroup, as it has all the elements of the set that are present in Z_{17}^*.

∴ 14 is a Generator.

Since there are 16 elements in the subgroup and hence it is a composite order subgroup.

Now, <u>For a = 15 :-</u>

$15^0 \bmod 17 = 1$
$15^1 \bmod 17 = 15$
$15^2 \bmod 17 = 4$
$15^3 \bmod 17 = 9$
$15^4 \bmod 17 = 16$
$15^5 \bmod 17 = 2$
$15^6 \bmod 17 = 13$
$15^7 \bmod 17 = 8$
$15^8 \bmod 17 = 1$
$15^9 \bmod 17 = 15$
$15^{10} \bmod 17 = 4$
$15^{11} \bmod 17 = 9$
$15^{12} \bmod 17 = 16$
$15^{13} \bmod 17 = 2$
$15^{14} \bmod 17 = 13$
$15^{15} \bmod 17 = 8$.

∴ The elements of the set are, {1, 2, 4, 8, 9, 13, 15, 16}.

∴ The set do not have all the elements of the set that are present in Z_{17}^*,

Hence 15 is not a generator.

Since there are 8 elements in the subgroup and hence it is a composite order subgroup.

Now, For $a = 16$:-

$16^0 \bmod 17 = 1$
$16^1 \bmod 17 = 16$
$16^2 \bmod 17 = 1$
$16^3 \bmod 17 = 16$
$16^4 \bmod 17 = 1$
$16^5 \bmod 17 = 16$
$16^6 \bmod 17 = 1$
$16^7 \bmod 17 = 16$
$16^8 \bmod 17 = 1$
$16^9 \bmod 17 = 16$
$16^{10} \bmod 17 = 1$
$16^{11} \bmod 17 = 16$
$16^{12} \bmod 17 = 1$
$16^{13} \bmod 17 = 16$
$16^{14} \bmod 17 = 1$
$16^{15} \bmod 17 = 16.$

∴ The elements of the set are, $\{1, 16\}$

∴ The set do not have all the elements of the set that are present in Z^*_{17},

Hence 16 is not a generator.

Since, There are only 2 elements in the subgroup and hence, it is a Prime order subgroup.

(b.) Verify that the Prime-order cyclic subgroups tally with the residues modulo p formula.

Sol:- we know that the residue modulo p,

$p = (r * q) + 1$ where $p = 17$ & $q = 2$

(From prime order cyclic subgroup, where set $\{1, 16\}$)

$17 = (r * 2) + 1$

$17 - 1 = 2 * r$

$2 * r = 16 \Rightarrow r = \frac{16}{2} = 8.$

Since $n \geq 1$, then the subgroup of n^{th} residues modulo p is defined as:

$$G = \{(h^n \bmod p) \mid h \in Z_p^*\}$$

$G = \{1^8 \bmod 17, 2^8 \bmod 17, 3^8 \bmod 17, 4^8 \bmod 17, 5^8 \bmod 17, 6^8 \bmod 17, 7^8 \bmod 17, 8^8 \bmod 17, 9^8 \bmod 17, 10^8 \bmod 17, 11^8 \bmod 17, 12^8 \bmod 17, 13^8 \bmod 17, 14^8 \bmod 17, 15^8 \bmod 17, 16^8 \bmod 17\}$.

$G = \{1, 16, 1, 16, 1, 16, 1, 16, 1, 16, 1, 16, 1, 16, 1, 16\}$

$\therefore G = \{1, 16\}$

∴ The subgroup of n^{th} residue modulo p tallies with the prime order subgroup.

(c-) Verify that every element of a prime-order sub-group is a generator.

Sol:

$16^0 \bmod 17 = 1$

$16^1 \bmod 17 = 16$

Since 16 can generate the subgroup or its own of 1 is by default a generator and Hence $\{1, 16\}$ are generators.

(2.) Consider $\mathbb{Z}_n^*$ for $n = 15$. Using Fermat's little theorem, how many witnesses can you find? which ones? Are there any strong liars? which ones?

Soln

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

$$|\mathbb{Z}_{15}^*| = 8.$$

Left to see

If 15 is a prime for $a \in \mathbb{Z}_{15}^*$,

we know that in FLT, $\boxed{a^{n-1} \bmod n = 1}$

i) $a = 2$,

$$2^{14} \bmod 15 = 4$$

$\therefore$ 2 is a witness of 15 being composite.

ii) $a = 4$,

$$4^{14} \bmod 15 = 1$$

$\therefore$ 4 is a strong liar

iii) $a = 7$,

$$7^{14} \bmod 15 = 4$$

$\therefore$ 7 is a witness of 15 being composite.

iv) $a = 8$,

$$8^{14} \bmod 15 = 4$$

$\therefore$ 8 is a witness of 15 being composite.

v) $a = 11$,

$$11^{14} \bmod 15 = 1$$

∴ 11 is a strong liar.

vi.) $a = 13$,

$13^{14} \bmod 15 = 4$

∴ 13 is a witness of 15 being composite.

vii.) $a = 14$,

$14^{14} \bmod 15 = 1$

∴ 14 is a strong liar.

∴ witness of compositness $= \{2, 7, 8, 13\}$.

∴ strong liars $= \{4, 11, 14\}$

11/06/22

(3.) Let's say, instead of using a composite $N = pq$ in the RSA cryptosystem, we just use prime modulo p.

Sol:

We know that in RSA,

$$\phi(n) = (p-1)(q-1)$$

→ Since we use prime modulo p, then the equation will be $N = p$ and $\phi(n) = (p-1)$.

And Hence, the modified RSA is not secure because the adversary knows the parameters p, e, C, and would be able to get the d through the equation $e \cdot d \bmod \phi(n) = 1$.

→ If $C = m^e \bmod p$, now since the adversary has all the values to substitute in the equation $y = c^d \bmod p$ and get the value of y. Thus, it is not secure to just use a prime modulo p instead of composite $n = p \cdot q$.

(4.) Consider an RSA system with the following parameters; $p = 17$, $q = 23$; $n = 391$; $e = 3$.

Find d. Encrypt $m = 55$; Show the resulting ciphertext C. Now, decrypt C (using d after computation), and verify we get back m.

Sol: We know that RSA Decryption to find d is,

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

where $\phi(n) = (p-1)(q-1)$

$$3 \cdot d \bmod (17-1)(23-1) = 1$$

$$3 \cdot d \bmod (16)(22) = 1$$

$$3d \bmod 352 = 1$$

$\therefore d = 235$. (From modulo multiplicative inverse)

Now encrypting $m = 55$ to Show the ciphertext 'C'.

We know that in RSA Decryption,

$$C = m^e \pmod n$$

$c = 55^3 \pmod{391}$

$c = (55^2 * 55 \bmod 391) \bmod 391.$

$c = (3025 * 55 \bmod 391) \bmod 391.$

$c = (288 * 55 \bmod 391) \bmod 391$

$c = 200 \bmod 391 = \underline{200}.$

Now, Decrypting c' to verify the m.

we know that RSA Decryption to get m,

$$c^d \pmod{N} = m$$

$$200^{235} \pmod{391} = m$$

$\therefore \underline{55}$. Hence verified.

(5.) Consider an Encryption scheme defined:

Sol:- The following step is as we know $PK = \{g_1, g_2, g_3\}$ and $SK = \{a, b\}$ such that $g_1^a = g_2^b = g_3$

then $C = (g_1^x, g_2^y, m \cdot g_3^{x+y})$

Now we have to find m; such that.

$c_1 = g_1^x g_2^y$ & $c_2 = m \cdot g_3^{x+y}$ (since we already know, $g_1^a = g_2^b = g_3$)

$$m = \frac{c_2}{g_3^{x+y}}$$

$$m = \frac{c_2}{(g_3)^x \cdot (g_3)^y} = \frac{c_2}{(g_1 a)^x \cdot (g_2 b)^y}$$

Now substitute c_2 in the above to get m,

$$\frac{m \cdot g_3^{x+y}}{(g_1 a)^x \cdot (g_2 b)^y}$$

$$\frac{m \cdot (g_1 a)^x \cdot (g_2 b)^y}{(g_1 a)^x (g_2 b)^y} = m.$$