Abdus Salam
IT-21016
4th Year 1st Semester (Cryptography)

1) Is 1729 a Carmichael number?

Ans:

Yes, 1729 is a Carmichael number.

A Carmichael number is a composite number n such that:

$a^{n-1} \equiv 1 \mod n$ for all integers a where $\gcd(a, n) = 1$

$1729 = 7 \times 13 \times 19$, it is composite and all prime factors are distinct.

For each ~~time~~ prime divisor p, Korselt's criterion: $p-1 \mid 1729 - 1 = 1728$

→ $7-1 = 6$ and $6 \mid 1728$ is possible.

→ $13-1 = 12$ and $12 \mid 1728$ is possible

→ $19-1 = 18$ and $18 \mid 1728$ is possible.

All conditions are satisfied. So, 1728 is a Carmichael number.

Abdus Salam
IT-21016
4th Year 1st Semester

2) Primitive Root (Generator) of ~~Z_{23}~~ Z_{23}?

Ans:

→ Z^*_{23} = set of all integers from 1 to 22 under multiplication mod 23.

→ Since 23 is prime, this group is cyclic and has primitive roots.

→ The order of the group $\phi(23) = 22$

A primitive root is an integer $g \in Z^*_{23}$,

$g^k \bmod 23$, where $k = 1$ to 22

If g is a primitive root,

$g^{22/2} \not\equiv 1 \bmod 23$

$g^{22/11} \not\equiv 1 \bmod 23$

Again, $g = 5$

$5^{11} \bmod 23 = 22 \not\equiv 1$

$5^2 \bmod 23 = 2 \not\equiv 1$

So, 5 is a primitive root of mod 23.

5 is a primitive root of Z^*_{23}

and other primitive roots are,

5, 7, 10, 11, 14, 15, 17, 19, 20, 21

(Ans.)

Abdus Salam
IT-21016
4th Year 1st Semester ; (Cryptography)

3) Is $(Z_{11}, +, *)$ a Ring?

Ans: Yes, $(Z_{11}, +, *)$ is a ring.

A ring is a ~~a~~ set R with two operation $(+, \times)$.

$(R, +)$ is an abelian group,

Z_{11} under addition mod 11 is closed,

Associative, Has identity(0), Every ~~e~~ element has an additive inverse, Commutative.

$(R, \times)$ is an abelian group:

closed under multiplication mod 11,

associative, Distributive over +:

$$a \times (b + c) = a \times b + a \times c \mod 11$$

$1 \in Z_{11}$, it have a multiplicative identity.

So, $(Z_{11}, +, *)$ is a commutative ~~Rign~~ ring with identity.

Abdus Salam
IT-21016
4th Year 1st Semester (Cryptography)

4) Is $(Z_{37}, +)$, (Z_{35}, X) are abelian group?

Ans:

→ $(Z_{37}, +)$ elements are : $\{0, 1, 2, \ldots, 36\}$
operation : Addition modulo 37.

1. Closure: $a+b \bmod 37 \in Z_{37}$
2. Associativity: $(a+b)+c = a+(b+c) \bmod 37$
3. Identity: 0 is the additive identity
4. Inverse: Every $a \in Z_{37}$ has $-a \bmod 37$
5. Commutative: $a+b = b+a \bmod 37$.

So, $(Z_{37}, +)$ is an abelian group.

→ (Z^*_{35}, X), $Z^*_{35} = \{a \in Z_{35} : \gcd(a, 35) = 1\}$
that elements are all numbers from 1 to 34 coprime to 35.

1. Closure: Product of two elements coprime to 35 remains coprime to 35.
2. Associativity: Multiplication is associative.
3. Identity: 1 is the identity element.
4. Inverse: Every element in Z^*_{35} has an inverse mod 35
5. Commutative: Multiplication modulo n is commutative.

So, (Z^*_{35}, X) is an abelian group.

Abdus Salam
IT-21016
4th Year 1st Semester (Cryptography)

5) Let's take $p=2, n=3$ that makes the $GF(p^n) = GF(2^3)$. then solve this with ~~plo~~ polynomial arithmetic approach.

Solve: $p=2, n=3$, $GF(2^3)$ and elements of $GF(2) = \{0,1\}$. Elements of $GF(2^3)$ will be polynomials of degree <3 with co-efficients in $GF(2)$. So, all polynomials of the form:

$$a_2x^2 + a_1x + a_0 \quad \text{where } a_i \in \{0,1\}$$

There are $2^3 = 8$ polynomials are: $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$.

Example: $f(x) = x^3 + x + 1$, this is irreducible over $GF(2)$. We will now do arithmetic modulo.

Multiplication in $GF(2^3)$: Let's multiply $a(x) = x$ and $b(x) = x^2+1$.

$$a(x).b(x) = x(x^2+1) = x^3+x$$

Now reduce x^3+x modulo $f(x) = x^3+x+1$:

$$x^3+x \equiv (x^3+x) - (x^3+x+1) = 1 \bmod f(x)$$

So, $x(x^2+1) \equiv 1 \bmod f(x)$

Ans.