CS4036 : Advanced Database Management Systems

A
Course File
By

Nadiya T T

तमसो मा ज्योतिर्गमय

Department of Computer Science and Engineering

National Institute of Technology, Calicut

Winter-2017

Table of Contents

Name and Roll No.: ______________________________

Answer the questions in the spaces provided on the question paper. You can use the additional sheets for rough work.

Question No.:	1	2	3	4	5	**Total**
Marks:	3	3	4	5	5	20
Score:						

1. A binary operation $*$ on a finite set S can be represented by a square grid where rows and columns are indexed by elements of S; and the entry in the row corresponding to a and the column corresponding to b is $a * b$. For example, $(\mathbb{Z}/5\mathbb{Z}, \times)$ can be represented by the following grid: 3

$$\begin{array}{c|cccc} \times & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \hline \overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{2} & \overline{2} & \overline{4} & \overline{1} & \overline{3} \\ \overline{3} & \overline{3} & \overline{1} & \overline{4} & \overline{2} \\ \overline{4} & \overline{4} & \overline{3} & \overline{2} & \overline{1} \end{array}$$

If $(G, *)$ is a group and G is a finite set, prove that every row and every column of its grid is a permutation of the elements of G.

2. What is wrong with the following proof: [3]

   Theorem. *All horses are of the same colour.*

   Proof. We prove the theorem by induction on the number of horses.
   Base case: If there is only one horse, the theorem is trivial.
   Inductive step: Suppose the theorem is true for $n-1$ horses i.e. every horse in a group of $n-1$ horses is of the same colour. Now consider a group of n horses. By induction hypothesis, horses $1, 2, \ldots, n-1$ are of the same colour. Similarly, by induction hypothesis, horses $2, 3, \ldots, n$ are of the same colour. Therefore horses 1 and n are also of the same colour. So horses $1, 2, \ldots n$ are of the same colour. This completes the proof. $\square$

3. Suppose $(G, *)$ is a group and H is a non-empty subset of G. Suppose for all a, b in H, $a * b^{-1}$ is also in H. Prove that $(H, *)$ is a group. [4]

4. Recall $\mathbb{R}[x]$ is the set of polynomials with Real coefficients and non-negative degree. We can define congruence relation on $\mathbb{R}[x]$. We say two polynomials f and g are congruent modulo a polynomial h if h divides $f - g$. Given $h \in \mathbb{R}[x]$, we can define $\mathbb{R}[x]/h\mathbb{R}[x]$ analogous to $\mathbb{Z}/m\mathbb{Z}$.

   (a) What are the elements of the set $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$? $\boxed{1}$

   (b) How are operations $+$ and $\times$ defined on $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$? $\boxed{1}$

   (c) Is $\Big(\big(\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]\big) - \{0\}, \times\Big)$ a group? Why / Why not? $\boxed{3}$

5. Let $+$ denote the usual addition operation on integers. Let $a, b \in \mathbb{Z}$.

   (a) Is there a proper subset S of $\mathbb{Z}$ containing a and b such that $(S, +)$ is a group. If yes, give the subset; otherwise prove that such a subset doesn't exist. $\boxed{2}$

   (b) Given a group $(G, +)$. An element $g \in G$ is called a generator of the group if $G = \{ig \mid i \in \mathbb{Z}\}$. [Note: Here na is a shorthand for $\underbrace{a + a + \cdots + a}_{n \text{ times}}$]. Does $(S, +)$ (defined in the previous part of the question) have a generator? If yes, give the generator; otherwise prove it doesn't exist. $\boxed{3}$

Name and Roll No.: ______________________

Answer the questions in the spaces provided on the question paper. You can use the additional sheets for rough work.

Question No.:	1	2	3	4	5	**Total**
Marks:	3	3	4	5	5	20
Score:						

1. A binary operation $*$ on a finite set S can be represented by a square grid where rows and columns are indexed by elements of S; and the entry in the row corresponding to a and the column corresponding to b is $a * b$. For example, $(\mathbb{Z}/5\mathbb{Z}, \times)$ can be represented by the following grid: [3]

$$\begin{array}{c|cccc} \times & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \hline \overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{2} & \overline{2} & \overline{4} & \overline{1} & \overline{3} \\ \overline{3} & \overline{3} & \overline{1} & \overline{4} & \overline{2} \\ \overline{4} & \overline{4} & \overline{3} & \overline{2} & \overline{1} \end{array}$$

If $(G, *)$ is a group and G is a finite set, prove that every row and every column of its grid is a permutation of the elements of G.

Solution: We first show that no row has duplicate elements. For the sake of contradiction, suppose there is a row (say row indexed by a) with duplicate elements. Let the columns corresponding to these elements be indexed by b and c respectively where $b \neq c$. So, $a * b = a * c$. This implies $a^{-1} * a * b = a^{-1} * a * c$. So, $b = c$. This contradicts the fact that $b \neq c$. So, our assumption that there is a row with with duplicate elements is false.

The proof for columns is similar.

Since every row and every column contains n elements and there are no duplicates, every row and every column is a permutation of the elements of the group.

2. What is wrong with the following proof: [3]

Theorem. *All horses are of the same colour.*

Proof. We prove the theorem by induction on the number of horses.
Base case: If there is only one horse, the theorem is trivial.
Inductive step: Suppose the theorem is true for $n-1$ horses i.e. every horse in a group of $n-1$ horses is of the same colour. Now consider a group of n horses. By induction hypothesis, horses $1, 2, \ldots, n-1$ are of the same colour. Similarly, by induction hypothesis, horses $2, 3, \ldots, n$ are of the same colour. Therefore horses 1 and n are also of the same colour. So horses $1, 2, \ldots n$ are of the same colour. This completes the proof. □

Solution: If $n = 2$, the sets $\{1, \ldots, n-1\}$ and $\{2, \ldots, n\}$ do not intersect; and so it cannot be inferred that horses 1 and n have the same colour. So, the *Inductive Step* fails for $n = 2$.

3. Suppose $(G, *)$ is a group and H is a non-empty subset of G. Suppose for all a, b in H, $a * b^{-1}$ is also in H. Prove that $(H, *)$ is a group. $\boxed{4}$

Solution:

- *Identity element:* Since $H \neq \varnothing$, there exists an element in H. Let this element be called a. Since $a \in H$, $a * a^{-1} = e \in H$. Therefore H contains the identity element.
- *Inverse:* Let $a \in H$. We have to show that $a^{-1} \in H$. Since $e, a \in H$, so $e * a^{-1} = a^{-1} \in H$.
- *Closure:* Let $a, b \in H$. We have to show that $a * b \in H$. Since $b \in H$, $b^{-1} \in H$. Since $a, b^{-1} \in H$, $a * (b^{-1})^{-1} = a * b \in H$.
- *Associativity:* Since $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$, and since H is a subset of G, $(a * b) * c = a * (b * c)$ for all $a, b, c \in H$.

4. Recall $\mathbb{R}[x]$ is the set of polynomials with Real coefficients and non-negative degree. We can define congruence relation on $\mathbb{R}[x]$. We say two polynomials f and g are congruent modulo a polynomial h if h divides $f - g$. Given $h \in \mathbb{R}[x]$, we can define $\mathbb{R}[x]/h\mathbb{R}[x]$ analogous to $\mathbb{Z}/m\mathbb{Z}$.

(a) What are the elements of the set $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$? $\boxed{1}$

Solution: Given $f \in \mathbb{R}[x]$, let $\overline{f} = \{g \in \mathbb{R}[x] \mid f \equiv g \pmod{x^2+1}\}$, Then $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is defined as follows: $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x] = \{\overline{f} \mid f \text{ is a polynomial of degree less than } 2\}$.

Notice that all zero degree polynomials (i.e. Real numbers) lie in different congruence classes. If $a \neq b$, polynomials $x + a$ and $x + b$ lie in different congruence classes. If a, α and β are Real numbers, then polynomials $x + a$ and $\alpha(x^2+1) + \beta(x + a)$ lie in the same congruence class.

(b) How are operations $+$ and $\times$ defined on $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$? $\boxed{1}$

Solution: $\overline{f} + \overline{g} \overset{def}{=} \overline{f+g}$ and $\overline{f} \times \overline{g} \overset{def}{=} \overline{f \times g}$

If we have to add two congruence classes $\overline{f}$ and $\overline{g}$, we add polynomials f and g and return the corresponding congruence class $\overline{f+g}$. Since the degree of $f + g$ is less than 2 if the degree of both f and g is less than 2, so $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is closed under $+$.

If we have to multiply two congruence classes $\overline{f}$ and $\overline{g}$, we multiply polynomials f and g and return the corresponding congruence class $\overline{f \times g}$. If the degree of $f \times g$ is greater than or equal to 2, then there is another polynomial h of degree less than 2 such that $\overline{f \times g} = \overline{h}$. Therefore, $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is closed under $\times$.

(c) Is $\Big(\big(\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]\big) - \{0\}, \times\Big)$ a group? Why / Why not? $\boxed{3}$

Solution: Yes, it is a group.

- *Closure:* Proved in the previous part.
- *Associativity:* Proof similar to $\mathbb{Z}/m\mathbb{Z}$.
- *Identity:* Identity element is $\overline{1}$.
- *Inverse:* Given $f \in \mathbb{R}[x]/h\mathbb{R}[x]$, it can be shown that equation $\overline{f} \times \overline{X} = \overline{1}$ has a solution in $\mathbb{R}[x]/h\mathbb{R}[x]$ if $\gcd(f, h)$ is a unit. Since $x^2 + 1$ is a irreducible, every polynomial f of degree less than $x^2 + 1$ satisfies $\gcd(f, x^2 + 1)$ is a unit. Therefore every element of $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ has an inverse.

5. Let $+$ denote the usual addition operation on integers. Let $a, b \in \mathbb{Z}$.

   (a) Is there a proper subset S of $\mathbb{Z}$ containing a and b such that $(S, +)$ is a group. If yes, give the subset; otherwise prove that such a subset doesn't exist. $\boxed{2}$

   > **Solution:** $S = \{ax + by \mid x, y \in \mathbb{Z}\}$ is the smallest subset of $\mathbb{Z}$ containing a and b which is a group. This is a proper subset of $\mathbb{Z}$ if $\gcd(a, b) \neq 1$.

   (b) Given a group $(G, +)$. An element $g \in G$ is called a generator of the group if $G = \{ig \mid i \in \mathbb{Z}\}$. [Note: Here na is a shorthand for $\underbrace{a + a + \cdots + a}_{n \text{ times}}$]. Does $(S, +)$ (defined in the previous part of the question) have a generator? If yes, give the generator; otherwise prove it doesn't exist. $\boxed{3}$

   > **Solution:** If $\gcd(a, b) \neq 1$, then $(S, +)$ is a group and $\gcd(a, b)$ is a generator.

Name and Roll No.: ____________________

Answer the questions in the spaces provided on the question paper. You can use the additional sheets for rough work.

Question No.:	1	2	3	4	5	6	**Total**
Marks:	4	4	3	2	3	4	20
Score:							

1. If the input to the following algorithm is an odd, composite, non-Carmichael number; then show that $\Pr(Error) \leqslant \frac{1}{2}$. $\boxed{4}$

Algorithm 1 Fermat's Test

```
procedure IsPrime(n)
    Select a ∈ {1, 2, ... n − 1} uniformly at random
    if a^(n−1) ≡ 1 (mod n) then
        print "Prime"
    else
        print "Composite"
    end if
end procedure
```

2. If n is an odd Carmichael number then show that $n = p_1 \cdot p_2 \cdots p_t$ for some primes $p_1, p_2, \ldots p_t$ satisfying $(p_i - 1)$ divides $(n-1)$ for $i = 1, 2, \ldots t$. $\boxed{4}$

3. What is the order of 538 in $\mathbb{Z}^*_{1287}$? $\boxed{3}$

4. For $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, we used the isomorphism between $(\mathbb{Z}_n^*, \times)$ and $(\mathbb{Z}_{p_1^{e_1}}^* \times \mathbb{Z}_{p_2^{e_2}}^* \times \cdots \times \mathbb{Z}_{p_t^{e_t}}^*, \times)$ to calculate the value of $\varphi(n)$. Can we use the same technique to calculate the value of $\varphi(p_i^{e_i})$ for $i = 1, 2, \ldots t$. Justify your answer. $\boxed{2}$

5. If $n = 2 \cdot p^e$ for some odd prime p, then show that $\mathbb{Z}_n^*$ is cyclic. $\boxed{3}$

6. Give a subgroup of $\mathbb{Z}_{323}^*$ of size 18. $\boxed{4}$

1. If the input to the following algorithm is an odd, composite, non-Carmichael number; then show that $\Pr(Error) \leqslant \frac{1}{2}$. [4]

Algorithm 1 Fermat's Test

```
procedure IsPrime(n)
    Select a ∈ {1, 2, ... n − 1} uniformly at random
    if a^(n−1) ≡ 1 (mod n) then
        print "Prime"
    else
        print "Composite"
    end if
end procedure
```

> **Solution:** Proved in the class.

2. If n is an odd Carmichael number then show that $n = p_1 \cdot p_2 \cdots p_t$ for some primes $p_1, p_2, \ldots p_t$ satisfying $(p_i - 1)$ divides $(n - 1)$ for $i = 1, 2, \ldots t$. [4]

> **Solution:** Proved in the class.

3. What is the order of 538 in $\mathbb{Z}^*_{1287}$? [3]

> **Solution:** We know that the group $(\mathbb{Z}^*_{1287}, \times)$ is isomorphic to the group $(\mathbb{Z}^*_9 \times \mathbb{Z}^*_{11} \times \mathbb{Z}^*_{13}, \times)$. [Here $f\colon \mathbb{Z}^*_{1287} \to \mathbb{Z}^*_9 \times \mathbb{Z}^*_{11} \times \mathbb{Z}^*_{13}$, defined by $f(a) = (a \bmod 9, a \bmod 11, a \bmod 13)$, is the isomorphism function.]
>
> Since f is an isomorphism, the order of 538 in $\mathbb{Z}^*_{1287}$ is same as the order of $f(538)$ [which is equal to $(-2, -1, 5)$] in $(\mathbb{Z}^*_9 \times \mathbb{Z}^*_{11} \times \mathbb{Z}^*_{13}, \times)$.
>
> Calculating the powers of $(-2, -1, 5)$, we get $(-2, -1, 5)^1 = (-2, -1, 5)$, $(-2, -1, 5)^2 = (4, 1, -1)$, $(-2, -1, 5)^3 = (-8, -1, -5) = (1, -1, -5)$, $(-2, -1, 5)^4 = (4, 1, -1)^2 = (-2, 1, 1)$ and so on. We find that 12 is the smallest exponent e such that $(-2, -1, 5)^e = (1, 1, 1)$; and so the order is 12.

4. For $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, we used the isomorphism between $(\mathbb{Z}^*_n, \times)$ and $(\mathbb{Z}^*_{p_1^{e_1}} \times \mathbb{Z}^*_{p_2^{e_2}} \times \cdots \times \mathbb{Z}^*_{p_t^{e_t}}, \times)$ to calculate the value of $\varphi(n)$. Can we use the same technique to calculate the value of $\varphi(p_i^{e_i})$ for $i = 1, 2, \ldots t$. Justify your answer. [2]

> **Solution:** For $n = n_1 \cdot n_2 \cdots n_t$, the Chinese Remainder Theorem requires n_i to be pairwise co-prime. Therefore, we cannot say that $(\mathbb{Z}^*_{p_i^{e_i}}, \times)$ is isomorphic to $(\mathbb{Z}^*_{p_i} \times \mathbb{Z}^*_{p_i} \times \cdots \times \mathbb{Z}^*_{p_i}, \times)$

5. If $n = 2 \cdot p^e$ for some odd prime p, then show that $\mathbb{Z}^*_n$ is cyclic. [3]

Solution: We know that $\mathbb{Z}^*_{p^e}$ is cyclic for all primes p. Therefore it has a generator. Let g be a generator of $\mathbb{Z}^*_{p^e}$.

The order of $(1, g)$ in $(\mathbb{Z}^*_2 \times \mathbb{Z}^*_{p^e}, \times)$ is same as the order of g in $(\mathbb{Z}^*_{p^e}, \times)$, which is equal to $p^{e-1}(p-1)$. Since $(\mathbb{Z}^*_2 \times \mathbb{Z}^*_{p^e}, \times)$ is isomorphic to $(\mathbb{Z}^*_{2p^e}, \times)$, the order of $(1, g)$ in $(\mathbb{Z}^*_2 \times \mathbb{Z}^*_{p^e}, \times)$ is same as the order of $f^{-1}(1, g)$ in $(\mathbb{Z}^*_{2p^e}, \times)$. [Here $f \colon \mathbb{Z}^*_{2p^e} \to \mathbb{Z}^*_2 \times \mathbb{Z}^*_{p^e}$ is the isomorphism function]. Therefore, the order of $f^{-1}(1, g)$ in $(\mathbb{Z}^*_{2p^e}, \times)$ is $p^{e-1}(p-1)$.

Since the size of $(\mathbb{Z}^*_{2p^e}, \times)$ is $\varphi(2p^e) = 2p^e(1 - \frac{1}{2})(1 - \frac{1}{p}) = p^{e-1}(p-1)$, therefore $f^{-1}(1, g)$ is the generator of $(\mathbb{Z}^*_{2p^e}, \times)$. Hence $(\mathbb{Z}^*_{2p^e}, \times)$ is a cyclic group.

6. Give a subgroup of $\mathbb{Z}^*_{323}$ of size 18. $\boxed{4}$

Solution: We know that the group $(\mathbb{Z}^*_{323}, \times)$ is isomorphic to the group $(\mathbb{Z}^*_{17} \times \mathbb{Z}^*_{19}, \times)$. [Here $f \colon \mathbb{Z}^*_{323} \to \mathbb{Z}^*_{17} \times \mathbb{Z}^*_{19}$ is the isomorphism function.]

It is easy to see that $(\{1\} \times \mathbb{Z}^*_{19}, \times)$ is a subgroup of $(\mathbb{Z}^*_{17} \times \mathbb{Z}^*_{19}, \times)$ of size 18. Since the group $(\mathbb{Z}^*_{323}, \times)$ is isomorphic to the group $(\mathbb{Z}^*_{17} \times \mathbb{Z}^*_{19}, \times)$, therefore $\left(f^{-1}(\{1\} \times \mathbb{Z}^*_{19}), \times\right)$ is a subgroup of $(\mathbb{Z}^*_{323}, \times)$ of size 18. [Here $f^{-1}(\{1\} \times \mathbb{Z}^*_{19})$ denotes the set $\{x \in \mathbb{Z}^*_{323} \mid f(x) \in \{1\} \times \mathbb{Z}^*_{19}\}$].

By Chinese Remainder Theorem, we get $f^{-1}(\{1\} \times \mathbb{Z}^*_{19}) = \{17x + 1 \mid 0 \leqslant x < 18\}$.

Name and Roll No.: ______________________________

Answer the questions in the spaces provided on the question paper. You can use the additional sheets for rough work.

Question No.:	1	2	3	4	5	6	**Total**
Marks:	2	2	3	4	4	5	20
Score:							

Useful formula: If $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, then Euler's totient function
$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right)$

1. Is it possible that $a^{\varphi(n)} \equiv 1 \pmod{n}$ if a is not co-prime to n? Justify your answer. $\boxed{2}$

2. Let G be a group and let H be a subgroup of G. Which cosets of G wrt. H are subgroups of G? Justify your answer. $\boxed{2}$

3. Does $\overline{x+5}$ have an inverse in $\big(\mathbb{R}[x]/(x^2+1)\mathbb{R}[x], \times\big)$? If yes give the inverse, otherwise prove that it doesn't exist. $\boxed{3}$

4. Let $\mathbb{Z}_n[x]$ denote the set of all polynomials with non-negative degree and coefficients in $\mathbb{Z}_n$, with addition and multiplication modulo n. For example, $(x+4)\times(x+7) = x^2+(11\times x)+13$ in $\mathbb{Z}_{15}[x]$. Does Unique Factorization Theorem hold for $\mathbb{Z}_n[x]$? Justify your answer. $\boxed{4}$

   [Hint: If n is composite, then an equation of degree d may have more than d solutions in $\mathbb{Z}_n$.]

5. Suppose Bob wants to securely receive messages from Alice. To do this, $\boxed{4}$

   - **Key generation:** Bob first generates an encryption and a decryption key in the following way:
     1. He chooses large distinct primes p and q, and computes $n = pq$.
     2. He chooses e co-prime to $\varphi(n)$. The pair (n, e) is given to Alice who will use it as the encryption key. Bob keeps d and $\varphi(n)$ secret. [Recall $\varphi(n)$ denotes the Euler's totient function.]
     3. He then computes d satisfying $de \equiv 1 \pmod{\varphi(n)}$.
   - **Encryption:** Now suppose Alice wants to send a message m (where $\gcd(m, n) = 1$) to Bob. She computes $c = m^e \mod n$. She sends c to Bob.
   - **Decryption:** Bob receives c and computes $m' = c^d \mod n$.

   Prove that $m' = m$.

6. Is 2 a generator of the group $(\mathbb{Z}_{83}^*, \times)$? Why / Why not? [Note: No marks for brute force or nearly brute force solutions.] $\boxed{5}$

Name and Roll No.: ______________________________

Answer the questions in the spaces provided on the question paper. You can use the additional sheets for rough work.

Useful formula: If $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, then Euler's totient function $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_t}\right)$

1. Is it possible that $a^{\varphi(n)} \equiv 1 \pmod n$ if a is not co-prime to n? Justify your answer. $\boxed{2}$

Solution: It is not possible.

Proof (by contradiction): Suppose there exist non-coprime integers a, n such that $a^{\varphi(n)} \equiv 1$ (mod n). Then $a \cdot a^{\varphi(n)-1} \equiv 1 \pmod n$. So, $a^{\varphi(n)-1}$ is the inverse of a in $\mathbb{Z}_n$. But we know that a cannot have an inverse in $\mathbb{Z}_n$ if it is not co-prime to n. This gives us a contradiction, and so our assumption that "there exist non-coprime integers a, n such that $a^{\varphi(n)} \equiv 1 \pmod n$" is false.

2. Let G be a group and let H be a subgroup of G. Which cosets of G wrt. H are subgroups of G? Justify your answer. $\boxed{2}$

Solution: H is the only coset of G wrt. H which is a subgroup of G.

Proof: Since cosets of G wrt. H are disjoint, only one coset can contain the identity element. Since we know that H (which is same as $e + H$ and $h + H$ for all $h \in H$) contains identity, so other cosets cannot contain identity, and hence are not subgroups of G. This completes the proof.

3. Does $\overline{x+5}$ have an inverse in $\left(\mathbb{R}[x]/(x^2+1)\mathbb{R}[x], \times\right)$? If yes give the inverse, otherwise prove that it doesn't exist. $\boxed{3}$

Solution: Yes, $\overline{\frac{-1}{26}x + \frac{5}{26}}$ is the inverse of $\overline{x+5}$.

Proof: $\overline{(x+5)} \times \overline{\left(\frac{-1}{26}x + \frac{5}{26}\right)} = \overline{\frac{-1}{26}x^2 + \frac{25}{26}}$. It can be seen that $\frac{-1}{26}x^2 + \frac{25}{26} = \frac{-1}{26}(x^2+1) + 1$. Therefore $\frac{-1}{26}x^2 + \frac{25}{26} \equiv 1 \pmod{x^2+1}$, and hence $\overline{(x+5)} \times \overline{\left(\frac{-1}{26}x + \frac{5}{26}\right)} = \overline{\frac{-1}{26}x^2 + \frac{25}{26}} = \overline{1}$.

4. Let $\mathbb{Z}_n[x]$ denote the set of all polynomials with non-negative degree and coefficients in $\mathbb{Z}_n$, with addition and multiplication modulo n. For example, $(x+4) \times (x+7) = x^2 + (11 \times x) + 13$ in $\mathbb{Z}_{15}[x]$. Does Unique Factorization Theorem hold for $\mathbb{Z}_1 5[x]$? Justify your answer. $\boxed{4}$

[Hint: If n is composite, then an equation of degree d may have more than d solutions in $\mathbb{Z}_n$.]

Solution: Unique Factorization Theorem does not hold for $\mathbb{Z}_{15}[x]$ since $x^2 - 1$ has two factorizations $(x-1)(x-14)$ and $(x-4)(x-11)$

5. Suppose Bob wants to securely receive messages from Alice. To do this, $\boxed{4}$

- **Key generation:** Bob first generates an encryption and a decryption key in the following way:

1. He chooses large distinct primes p and q, and computes $n = pq$.
2. He chooses e co-prime to $\varphi(n)$. The pair (n, e) is given to Alice who will use it as the encryption key. Bob keeps d and $\varphi(n)$ secret. [Recall $\varphi(n)$ denotes the Euler's totient function.]
3. He then computes d satisfying $de \equiv 1 \pmod{\varphi(n)}$.

- **Encryption:** Now suppose Alice wants to send a message m (where $\gcd(m, n) = 1$) to Bob. She computes $c = m^e \mod n$. She sends c to Bob.
- **Decryption:** Bob receives c and computes $m' = c^d \mod n$.

Prove that $m' = m$.

Solution: $c^d \equiv (m^e)^d \equiv m^{de} \pmod{n}$.

Since $de \equiv 1 \pmod{\varphi(n)}$, so $\varphi(n)$ divides $de - 1$. Therefore $de - 1 = k \cdot \varphi(n)$ for some integer k. So, $de = 1 + k \cdot \varphi(n)$.

Therefore $c^d \equiv m^{de} \equiv m^{1+k\cdot\varphi(n)} \equiv m^1 \cdot m^{k\cdot\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \equiv m \pmod{\varphi(n)}$ [by Euler's Theorem].

6. Is 2 a generator of the group $(\mathbb{Z}_{83}^*, \times)$? Why / Why not? [Note: No marks for brute force or nearly brute force solutions.] $\boxed{5}$

Solution: Yes, 2 is a generator.

Proof: Since 83 is prime, size of $\mathbb{Z}_{83}^*$ is 82. We have to show that $order(2) = 82$.

By Lagrange's Theorem, $order(2)$ divides 82. So, the only possibilities for $order(2)$ are 1, 2, 41 and 82. If we can show that $2^1 \neq 1$, $2^2 \neq 1$ and $2^{41} \neq 1$ in $\mathbb{Z}_{83}^*$, then By Fermat's Little Theorem $order(2) = 82$.

It is obvious that $2^1 \neq 1$ and $2^2 \neq 1$ in $\mathbb{Z}_{83}^*$. To compute 2^{41} we use the fact that $2^{41} = 2^{32} \cdot 2^8 \cdot 2^1$.

In $\mathbb{Z}_{83}^*$, $2^1 = 2$, $2^2 = 4$, $2^4 = (2^2)^2 = 4^2 = 16$, $2^8 = (2^4)^2 = (16)^2 = 256 = 7$, $2^{16} = (2^8)^2 = 7^2 = 49$, and $2^{32} = (2^{16})^2 = 49^2 = 7^3 \cdot 7 = 343 \cdot 7 = 11 \cdot 7 = 77$.

Therefore, in $\mathbb{Z}_{83}^*$, $2^{41} = 2^{32} \cdot 2^8 \cdot 2^1 = 77 \cdot 7 \cdot 2 = (77 \cdot 2) \cdot 7 = 154 \cdot 2 = (-12) \cdot 2 = -84 = -1$.

7. [Substitute question] If G is a group of size p where p is a prime, then prove that G has a generator. $\boxed{2}$

Solution: By Lagrange's Theorem for all $a \in G$, $order(a)$ divides p. Since p is a prime, $order(a)$ can either be 1 or p. Since identity is the only element of order 1, every other element has order p, and hence is a generator.

Course Outcome Attainment Scores

CO1(Amortized Analysis)	: 1.08
CO2(Classical paradigms)	: 1.3
CO3(Complexity assessment)	: 2.68
CO4(Randomized Algorithms)	: 3

Weighted Average CO Attainment	: 1.94
Cumulative Percentage Attainment of COs	: 64.61

PO1	: 2.09
PO2	: 2.32
PO3	: 2.32
PO4	: 2.13
PO5	: 2.25
PO6	: 0
PO7	: 0
PO8	: 0
PO9	: 0
PO10	: 0
PO11	: 2.25
PO12	: 2.04

Weighted Average PO Attainment	: 1.28
Cumulative Percentage Attainment of POs	: 42.79