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. [2]

Solution: It is not possible.

Proof (by contradiction): Suppose there exist non-coprime integers a, n such that $a^{\varphi(n)} \equiv 1 \pmod{n}$. 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. [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. [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 $\mathbb{Z}_15[x]$? Justify your answer. [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, [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.] 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. 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.