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. [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. [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. [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. [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, [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.] [5]