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 $\Pr(Error) \leqslant \frac{1}{2}$. [4]

Algorithm 1 Fermat's Test

```
1: procedure IsPrime(n)
2:     Select a ∈ {1, 2, ... n − 1} uniformly at random
3:     if a^{n−1} ≡ 1 (mod n) then
4:         print "Prime"
5:     else
6:         print "Composite"
7:     end if
8: 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 $i = 1, 2, \ldots t$. [4]

3. What is the order of 538 in $\mathbb{Z}^*_{1287}$? [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. [2]

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

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