

**Design & Analysis of Algorithms (IT-301)**  
**Assignment No.10**

1. Give an example of a text  $T$  of length  $n$  and a pattern  $P$  of length  $m$  such that the brute-force pattern matching algorithm will have running time  $\Omega(nm)$ .
2. Justify why the algorithm to calculate the function *failure* runs in  $O(m)$  time, where  $m$  is the length of the pattern.
3. Say that a pattern  $P$  of length  $m$  is a circular substring of a text  $T$  of length  $n$ , if  $P$  is a substring of  $T$ , or  $P$  is equal to the concatenation of a suffix of  $T$  and a prefix of  $T$ . Give an  $O(n + m)$ -time algorithm for determining whether  $P$  is a circular substring of  $T$ .
4. Suppose  $a$  and  $b$  are positive integers. Prove that if  $a$  divides  $b$ , and  $b$  divides  $a$  then it is the case that  $a = b$ .
5. Suppose that  $a$  and  $b$  are positive integers and  $c = GCD(a, b)$ . Prove that if  $d$  divides  $a$ , and  $d$  divides  $b$  then it is the case that  $d$  divides  $c$ .
6. Is it true that  $GCD(a, b) = GCD(a \bmod b, b)$ ? Give an argument in support of your answer.
7. If  $a \equiv c \bmod m$ , and  $b \equiv d \bmod m$ , then prove (1)  $a + b \equiv c + d \bmod m$ , (2)  $a.b \equiv c.d \bmod m$ .
8. Let  $x > 0$  be an element of  $Z_n$  such that  $GCD(x, n) = 1$ . Prove that  $Z_n = \{ix : i = 0, 1, 2, \dots, n - 1\}$ .
9. Write binary Euclid's Algorithm, justify its correctness, and finally analyze its running time.
10. Express  $GCD(412, 260)$  as a linear combination of the arguments.