Middle East Technical University Department of Computer Engineering

CENG 223

Discrete Computational Structures

Fall '2020-2021

Homework 3

Student Name and Surname: Yahya SUNGUR
Student Number: 2375723

Question 1

According to the Fermat's Little Theorem;
If p is a prime number and a is an integer not divisible by p, then:
$a^{p-1} \equiv 1(mod\ p)$ Furthermore, $a^p \equiv a(mod\ p)$
Since,

$$2^{22} = (2^{10})^2.2^2 = 1^2.2^2 \equiv 4(mod 11)$$

$$4^{44} = (4^{10})^4.4^4 = 1^4.4^4 = 256 \equiv 3(mod 11)$$

$$6^{66} = (6^{10})^6.6^6 = 1^6.6^6 = 46656 \equiv 5(mod 11)$$

$$8^{80} = (8^{10})^8 = 1^8 \equiv 1(mod 11)$$

$$10^{110} = (2^{10})^{11} = 1^{11} \equiv 1(mod 11)$$

So,

$$4 + 3 + 5 + 1 + 1 = 14 \equiv 3(mod 11)$$

Answer = 3

Question 2

- $7n + 4 = (5n + 3).1 + (2n + 1)$
- $5n + 3 = (2n + 1).2 + (n + 1)$
- $2n + 1 = (n + 1).1 + n$
- $n + 1 = n.1 + 1$
- $n = 1.n + 0$

By Euclid's Algorithm,
gcd(7n+4,5n+3) = gcd(5n+3,2n+1) = gcd(2n+1,n+1) = gcd(n+1,n) = gcd(n,1) = 1
$\implies$ gcd(5n+3,7n+4) = 1

Question 3

Since, $m^2 = n^2 + kx$
$m^2 - n^2 = kx$ So, both k and x are factors of $(m^2 - n^2)$
Therefore, both of them divide $(m^2 - n^2)$. In other words,
$k|(m^2 - n^2)$ and $x|(m^2 - n^2)$ and since $(m^2 - n^2) = (m - n) \times (m + n)$
$x|(m^2 - n^2) \implies x|(m - n).(m + n)$
So, x is a factor of (m-n) or (m+n)
Hence $x|(m - n)$ or $x|(m + n)$

Question 4

Basis:
For n = 1,

$$S_1 : 1 = \frac{1.(3-1)}{2} \textit{ is true.}$$

Inductive step:
Assume that;

$$S_k : 1 + 4 + 7 + ... + (3k - 2) = \frac{k.(3k-1)}{2} \textit{ is true.}$$

Prove that,

$$S_{k+1} : 1 + 4 + 7 + ... + (3(k + 1) - 2) = \frac{(k+1).(3(k+1)-1)}{2} \textit{ is true.}$$

Observe that,

$$1 + 4 + 7 + ... + (3(k + 1) - 2) = 1 + 4 + 7 + ... + (3k - 2) + (3k + 1)$$

due to inductive hypothesis,

$$= \frac{k.(3k-1)}{2} + (3k + 1)$$

$$= \frac{k.(3k-1) + 2.(3k+1)}{2}$$

$$= \frac{3k^2 - k + 6k + 2)}{2}$$

$$= \frac{3k^2 + 3k + 2k + 2)}{2}$$

$$= \frac{(k+1).(3k+2)}{2}$$

$$= \frac{(k+1).(3(k+1)-1)}{2}$$

Thus by the Principle of Mathematical Induction S_n is true for all n ≥ 1