Middle East Technical University Department of Computer Engineering

CENG 223

Discrete Computational Structures

Fall '2020-2021

Homework 3 ANSWER SHEET

Question 1

Use Fermat's Little Theorem the find $(2^{22} + 4^{44} + 6^{66} + 8^{80} + 10^{110})\ mod\ 11 \equiv$?

Fermat's Little Theorem (Section 4.4, Theorem 3) states that; if p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1\ mod\ p$.

Using this information, 11 is prime and 2, 4 ,6, and 10 are all non-divisible by 11. Hence, $2^{10} \equiv 4^{10} \equiv 6^{10} \equiv 8^{10} \equiv 10^{10} \equiv 1\ mod\ 11$.

Provided by the above information $2^{20} * 2^2 \equiv 1 * 2^2\ mod\ 11$. We can do similar calculations for the others too, so:

$2^2 + 4^4 + 6^6 + 8^0 + 10^0$ is actually asked in the question, which is:

$4 + 256 + 46656 + 1 + 1 = 461918$. Which is $461918\ mod\ 11 \equiv 3$.

Question 2

- $7n + 4 = 1(5n + 3) + 2n + 1$
- $5n + 3 = 2(2n + 1) + 1$
- $2n + 1 = 1(n + 1) + n$
- $n + 1 = 1 \cdot n + 1$
- $n = n$

Hence, $gcd(7n + 4, 5n + 3) = 1$, because 1 is the last nonzero remainder.
If $a = bq + r$, $gcd(a, b) = gcd(b, r)$ you can check section 4.3 - the Euclidean algorithm.

Question 3

Given $m^2 – n^2 = kx$;

We can infer that $(m - n)(m + n) = kx$;

Since we know that x does not equal zero because it is a prime number, we can write $((m-n)(m+n))/x = k$
.
Euclid's Lemma states that, if p is prime and $p|a * b$, then $p|a$ or $p|b$
x is prime and $x|(m + n)(m - n)$, therefore $x|(m + n)$ or $x|(m - n)$ (using Euclid's Lemma, Lemma 3 from the Section 4.3 in Rosen's book)

We know that k is an integer therefore we can say that $x|(m + n)$ or $x|(m - n)$ is true.

Question 4

For any integer n ≥ 1, let P_n be the statement that $1 + 4 + 7 + \cdots + (3n - 2) = \frac{n(3n-1)}{2}$

Basis: The statement P_1 says that

$1 = \frac{1(3-1)}{2}$, which is true.

Inductive Step: Fix $k \geq 1$, and suppose thatP_k holds, that is,

$1 + 4 + 7 + \cdots + (3k - 2) = \frac{k(3k-1)}{2}$

It remains to show that P_{k+1} holds, that is,

$1 + 4 + 7 + \cdots + (3(k + 1) - 2) = \frac{(k+1)(3(k+1)-1)}{2}$

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

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

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

$1 + 4 + 7 + \cdots + (3(k + 1) - 2) = \frac{k(3k-1)}{2} + (3k + 1)$

$1 + 4 + 7 + \cdots + (3(k + 1) - 2) = \frac{k(3k-1)+2(3k+1)}{2}$

$1 + 4 + 7 + \cdots + (3(k + 1) - 2) = \frac{3k^2-k+6k+2}{2}$

$1 + 4 + 7 + \cdots + (3(k + 1) - 2) = \frac{3k^2+5k+2}{2}$

$1 + 4 + 7 + \cdots + (3(k + 1) - 2) = \frac{(k+1)(3k+2)}{2}$

$1 + 4 + 7 + \cdots + (3(k + 1) - 2) = \frac{(k+1)(3(k+1)-1)}{2}$

As we are able to show that when P_n is assumed P_{n+1} is also true, by the principle of mathematical induction, for all n ≥ 1,P_n holds.