Mathematical Problems

Question:

1. Recurrences[10%] Consider the recurrence T(n). [Bonus Question]
1, if n = 1
5, if n = 2
5T(n − 1) − 6T(n − 2), if n > 2 & n ∈ N.

Prove by strong induction that T(n) = 3n −2 for all n ≥ 1 and n ∈ N.2. Mathematical Induction[10%]. Prove using mathematical induction that 3 divides n 3 + 2n for every n ∈ Z +.
3. Relations [10%]. Find a relation R on the set Z that is
• Not reflexive.
• Not symmetric.
• Not transitive.

5. Relations [10%]. Let S = {{1}, {1, 2}, {1, 3}} be a set. Is there exists a totally ordered binary relation R on A. Prove your claim. Relations [10%] Define a binary relation R on Z as (x, y) ∈ R only if
| x − y |< 1.
• Is R Reflexive. Prove or disprove your claim.
• Is R Symmetric. Prove or disprove your claim.
• Is R Transitive. Prove or disprove your claim.
• Is R Antisymmetric. Prove or disprove your claim.
• Is R Comparable. Prove or disprove your claim.

6. Set Partition [10%] Let Z3 = {[0], [1], [2]} denote the set of equivalence classes modulo 3. Prove that [0] ∩ [1] = ∅, [0] ∩ [2] = ∅, and [1] ∩ [2] = φ.7. Number Theory[10%]. Prove that if n ∈ Z then n 2 ≡ 0 (mod 4) or

Number Theory[10%]. Prove that if a, b, c and m are integers such that m ≥ 2, c > 0, and a ≡ b (mod m), then ac ≡ bc (mod mc). Division Theorem [10%]. Prove that every prime number except 2 and 3 is of form 6k + 1 or 6k + 5 for some k ∈ Z. Hint note n = 6 and apply GCD [10%]. Let a, b, d ∈ Z such that d = GCD(a, b). Let d 0 ∈ Z be .

11. Number Theory[10%]. Prove that the fundamental theorem of arithmetic cannot be extended to negative integers.
12.CRT [10%] Solve the following system of congruences. [Bonus Question]

$2x \equiv 5 \pmod 7$
$4x \equiv 2 \pmod 5$
$3x \equiv 9 \pmod{11}$

13. Fermat's Little Theorem [10%]. Using Fermat's little theorem, prove that if n is a positive integer, then 42 divides n Quadratic Residusity [10%]. Let p be an odd prime and $1 \le a \le p-1$. Prove that if $a \in QR_p$ is a quadratic residue modulo p then $a^{p-1} 2 \equiv 1 \pmod p$.

Answer:

Prove by strong induction that $T(n) = 3n - 2^n$ for all $n \in N$.
Solution. : Given : $T0 = 0, T1 = 1$
Base case :
$T2 = 5T1 - 6T0 = 5 = 32 - 2^2$
$T3 = 5T2 - 6T1 = 19 = 33 - 2^3$
Assumption :
$T(n) = 3n - 2$
^{n} and $T(n-1) = 3(n-1) - 2^{(n-1)}$

Proving :
$T(n+1) = 3(n+1) - 2^{(n+1)}$ $T(n+1) = 5T(n) - 6T(n-1)$
$= 5(3n - 2^n) - 6(3(n-1) - 2^{(n-1)} = 5(3n - 2^n$
$) - 2.3^n + 3.2^n = 3n .3 - 2^n .2 = 3(n+1) - 2^{(n+1)}$

is the solution of the given recurrence
Problem 2. prove using mathematical induction that 3 divides $n^3 + 2n$ for every $n \in Z^+$.
Solution. : Given : P(n) : 3 divides $n^3 + 2n$ $1^3 + 2(1) = 3 = 3(1)$ Hence 3 divides 3 Therefore, P(n) is valid for n = 1
(ii) Assume that p(m) : $m^3 + 2m$ Now prove that it is valid for m + 1
Proving :
$(m + 1)^3 + 2(m + 1)$ is divisible by 3
$(m + 1)^3 + 2(m + 1) = m^3 + 3m^2 + 3m + 1 + 2m + 2$
$= m^3 + 2m + 3m^2 + 3m + 3$
$= m^3 + 2m + 3(m^2 + m + 1)$
$= m^3 + 2m + 3(a)$ again, let $m^2 + m + 1 = a$
$m^3 + 2m$ is divisible by three ;3(a) is also divisible by 3 (by induction hypothesis)

Hence, the sum of m3+2m, 3(a) are both divisible by three. Also, 3 divides (m+1)3+2(m+1) Thus for any integer n, 3 divides n 3 + 2n

Problem 3. A set Z from a relation R that is: not transitive, not symmetric and not reflexive.

Solution. : Given : u, v, w for R = (u,v),(v,w)

Not transitive :

$(u, w) \notin R$

Not symmetric :

$(v, u) \notin R$

Not reflexive :

$(u, u) \notin R$

Note that u is related to v and v is related to w. A totally ordered binary relation R in A for a set S = (1, 1),(1, 2),(1, 3).

Solution. : Total order relation must fulfill 4 aspects:

1)Transitivity

2)Anti-symmetric

3)Reflexive

4)Comparability

S = (1, 1),(1, 2),(1, 3)

Absence of (2, 2),(3, 3) $\Longrightarrow$ non-reflexive

Absence of (2, 1) $\Longrightarrow$ anti-symmetry

Presence of (1, 1),(1, 2) $\Longrightarrow$ transitive

since the set is non reflexive, then there is no totally ordered binary relation R in A

Problem 5. Defining a binary relation R on Z for (x, y) and when $| x - y | < 1$

Solution. : R is reflexive :

$| x - x | < 1$

Thus xRx

R is symmetric :

For R x and y, when xRy, $| x - y | < 1$ and $| y - x | < 1$

yRx = xRy

R is transitive :

If xRy = yRz, then $| x - y | < 1$ and $| y - z | < 1$

$| x - y | + | y - z | = | x - z | < 1$

Thus xRz

Hence, Transitive R is anti-symmetric :For R x and y, when xRy, $| x - y | < 1$ and $| y - x | < 1$

y 6= x
Hence R is not anti-symmetric R is comparable :
Neither y ≥ x nor x ≥ y for R
Thus, R is incomparable

Prove for a set of equivalence classes of modulo 3 .
Solution. : Let : x ∈ [0] ∩ [1], then x ∈ [0] and x ∈ [1]
so, 3 | x and 3 | x − 1
so, 3 | x − (x − 1)
so, 3 | 1, contradicting
Thus, [0] ∩ [1] = ∅
Let : y ∈ [1] ∩ [2], then y ∈ [1] and x ∈ [2]
so, 3 | y − 1 and 3 | y − 2
so, 3 | (y − 1) − (y − 2)
so, 3 | 1, contradicting
Thus, [0] ∩ [2] = ∅
Let : z ∈ [1] ∩ [2]
so, 3 | z and 3 | z − 2
so, 3 | z − (z − 2)
so, 3 | 2, contradicting
Thus, [1] ∩ [2] = ∅
Problem 7. Prove that n ∈ Z , n
2 ≡ 1 (mod 4) or n
2 ≡ 0 (mod 4)
Solution. : Proof : Then, n is either even or odd
Case (i) : Assume n is odd
m ∈ Z such that n = 2m + 1
Thus, n
2 = 4m2 + 4m + 1
Hence : n
2 − 1 = 4(m2 + m)
So n
2 ≡ 1 (mod 4)
Case (ii) : Assume n is even
m ∈ Z such that n = 2m
Thus, n
2 = 4m2
Hence : 4 | m2
So n

$2 \equiv 0 \pmod 4$
Proved!
Problem 8. Solution. : It means that : $a \equiv b \pmod m \implies m \mid a - b$
Let $c > 0$ then $mc \mid c(a - b)$
Note that when ($a \mid b$ also $ac \mid bc$)
$\implies mc \mid c(a - b)$
$\implies mc \mid ca - cb)$
$\implies ca \equiv cb \pmod{mc}$
Proved!
Problem 9. Prove for prime number exist as $6k + 5$ or $6k + 1$ apart from 2 and 3 for $k \in Z$

Solution. : Let : $n > 3$ and n be a prime
Division algorithm yields $n = 6k = 2.3.k$; even
$n = 6k + 1$;prime
$n = 6k + 2 = 2(3k + 1)$; even
$n = 6k + 3 = 3(2k + 1)$
$n = 6k + 4 = 2(3k + 2)$; even
$n = 6k + 5$;prime

Conclusion : None of these will represent a prime greater than 2 and 3 Proving : Thus p must be either $6k + 1$ or $6k + 5$. . Prove that d 0
| d when d = GCD (a, b) and when d
$0 \in Z$
Solution. : Given : Bezout's identity
Proof :
$\exists\, x, y \in Z$ such that $d = ax + by$
Let d
0 be a C.D for a, b

Proved!
Solving a system of linear congruence : If you are supposed to solve one by one
1: $2x \equiv 5 \pmod 7$ We begin by finding the inverse of 5 modulo 7
$5.3 \equiv 15 \equiv 1 \pmod 7$
So, $5(-1) \equiv 3 \pmod 7$
$3.2x \equiv 6x \equiv 1 \pmod 7$
also find the inverse of 6 modulo 7
$6.6 \equiv 36 \equiv 1 \pmod 7$
Hence 6 is its own inverse and we have:

6.6x ≡ x ≡ 6 (mod 7)
So the reduced form is x ≡ 6 (mod 7)
2: 4x ≡ 2 (mod 5)
We have 3.2 ≡ 6 ≡ 1 (mod 5)
So, 2(−1) ≡ 3 (mod 5)
3.4x ≡ 12x ≡ 2x ≡ 1 (mod 5)
and;
3.2x ≡ x ≡ 3 (mod 5)
So the reduced form is x ≡ 3 (mod 5)
3: 3x ≡ 9 (mod 11)

We have 9.5 ≡ 45 ≡ 1 (mod 11)
So, 9(−1) ≡ 5 (mod 11)
5.3x ≡ 15x ≡ 4x ≡ 1 (mod 11)
and;
4.3 ≡ 12 ≡ 1 (mod 11)
So, 4(−1) ≡ 3 (mod 11)
3.4x ≡ x ≡ 3 (mod 11)
So the reduced form is x ≡ 3 (mod 11)
Combined:

If they are to be solved simultaneously, we will use the Chinese remainder theorem.
x ≡ 6 (mod 7)
x ≡ 3 (mod 5)
x ≡ 3 (mod 11)
Let’s start with
x = 5.11 + 7.11 + 7.5
These two terms should vanish when a remainder of x modulo 7, 5, 11 are to be considered.
Taking modulo 7, we have:
x ≡ 5.11 ≡ 55 ≡ 6 (mod 7)
Taking modulo 5, we have:
x ≡ 7.11 ≡ 77 ≡ 2 (mod 5)
We want to end with 3, thus we multiply the second term with 2 modulo 3 and then 3.
But, 2.3 ≡ 1 (mod 5)
Hence, our new choice of x is:
x = 5.11 + 7.11.3.3 + 7.5
Taking modulo 5, we end up with a remainder 3 as we desired
Taking modulo 11, we have:

x ≡ 35 ≡ 2 (mod 11)
We wanted to remain with 3, thus we multiply the third term with the inverse of 2 modulo
11 and by 3.
But, 2.6 ≡ 1 (mod 11)
Hence, our new choice of x is:
x = 5.11 + 7.11.3.3 + 7.5.6.3 = 1378
Hence, from CRT, our least positive solution is:
x ≡ 1378 (mod 7.5.11) reduced to
x ≡ 1378 (mod 385)
=⇒ x ≡ 223 (mod 385)
Thus the general solution to this system is:
x = 223 + 385n for n ∈Z
Problem 11. Prove that fundamental theorem cannot be satisfied with negative integers
.
Solution. : Proof : Every positive integer n is a product of primes
From induction, n = 1 and n > 1
Example:
15 = 3 * 5

The same cannot be expounded to negative integers Proving :
15 6= (−3) ∗ (−5)
The integer is divided into a prime, composite and unit Suppose n = 2, 3, ..., k, consider k + 1. It is either a prime
If k + 1 is not prime, then, k + 1= ab
with definitions as 1 ¡ a k and 1 ¡ b k
a and b are finite product of primes
ab is a finite product (−3) ∗ (−5) = −15 6= 15 (finite product)
Solution. Since 42 has prime multiples of 2, 3, 7 we need to show that n
can be divided by 2, 3 and 7.
From FLT:
if m = 2, 3, 7 then m | n
n
(m−1) ≡ 1(mod m)equation1
(m − 1) | 6 for m = 2, 3, 7
Thus, (6 m−1) is an integer
Raise both sides of equation 1 to (6 m−1
) th power 6
n(m−1)(m−1) ≡

6 1 (m−1) (mod m)
n 6 ≡ 1 (mod m)
multiply both sides by n
n 7 ≡ n (mod m)
This means:
m | (n 7 − n) for m = 2, 3, 7
Since 2, 3, 7 are all prime (n 7 − n) is divided by 42.