Assignment (MATH 2201 for Module I and IV)

Number Theory

1. Show that $(a+b, a-b)$ is either 1 or, 2 if and only if $(a, b) = 1$.
2. Find all integers n such that $n^2 + 1$ is divisible by $n + 1$.
3. Show that for all odd integers n, $gcd(3n, 3n + 2) = 1$.
4. Prove that $n^2 + 23$ is divisible by 24 for infinitely many n.
5. If n is a positive integer such that $n^3 + 1$ is prime, then prove that $n = 1$.
6. Use Euclidean Algorithm to calculate $gcd(a, b)$ and hence express it as $au + bv$ for some $u, v \in \mathbb{Z}$ for the following a, b :

(i) $gcd(42823, 6409)$

(ii) $gcd(1819, 3587)$

7. Find integers x, y, z satisfying $gcd(198, 288, 512) = 198x + 288y + 512z$.
8. Find the general solution in integers of the equation $221x + 35y = 11$.
9. Find $\tau(360)$, $\sigma(360)$, $\tau(1482)$, $\sigma(1225)$, $\tau(1932)$, $\sigma(7007)$.
10. Show that $2903^n - 803^n - 464^n + 261^n$ is divisible by 1897 for all natural numbers n.
11. Find the least positive residues in $10^{907}(\text{ mod } 13)$.
12. Use the theory of congruences to prove that $7 | 2^{5n+3} + 5^{2n+3}$ for all $n \geq 1$.
13. Solve the linear congruence (a) $15x \equiv 9(\text{ mod } 18)$ (b) $28x \equiv 63(\text{ mod } 105)$.
14. Solve the system of linear congruences
    (a) $x \equiv 1(\text{ mod } 3)$, $x \equiv 2(\text{ mod } 5)$, $x \equiv 3(\text{ mod } 7)$
    (b) $x \equiv 2(\text{ mod } 3)$, $x \equiv 3(\text{ mod } 5)$, $x \equiv 4(\text{ mod } 7)$
    (c) $x \equiv 2(\text{ mod } 5)$, $x \equiv 3(\text{ mod } 7)$, $x \equiv 5(\text{ mod } 8)$
    (d) $x \equiv 5(\text{ mod } 6)$, $x \equiv 4(\text{ mod } 11)$, $x \equiv 3(\text{ mod } 17)$.
15. Find the number of integers less than n and prime to n, when $n = 256, 324, 900, 2048, 5040, 7200$.
16. Show that for any $n \in \mathbb{Z}^+$, $\frac{n^{19}}{19} + \frac{n^7}{7} + \frac{107n}{133}$ is an integer.
17. Find the least positive residue in $2^{41}(\text{ mod } 23)$.
18. Find the remainder when $3^{1000000}$ is divided by 16.
19. Find the integer in the unit place of $7^{7^{14}}$ using congruence.
20. Using congruence find the remainder when $2^{73} + 14^3$ is divided by 11.
21. Prove that the eighth power of any integer is of the form $17k$ or $17k \pm 1$.
22. Show that $a^{12} - b^{12}$ is divisible by 91 if a and b are both prime to 91.
23. If n is a prime > 7 prove that $n^6 - n$ is divisible by 504.
24. Show that $4(29)! + 5!$ is divisible by 31.
25. Using congruence find the remainder when 4444^{4444} is divided by 9.

26. Use Fermat's Theorem to verify that $17 | 11^{104} + 1$.

27. Prove that $641 | (2^{32} + 1)$.

28. Prove that $7 | (2222^{5555} + 5555^{2222})$.

29. If p is a prime, prove that $2(p-3)! + 1 \equiv 0(\bmod p)$.

30. Prove that $1 + 20 + 20^2 + 20^3 + ... + 20^{21} \equiv 0(\bmod 23)$.

31. If $f(x) = 14x^5 - 9x^4 + 7x^2 - 3$, find the remainder when $f(16)$ is divided by 5.

POSET and Lattice

1. Let S be the set of all lines in 3-space. A relation ρ is defined on S by "$l \rho m$ if and only if l lies on the plane of m" for $l, m \in S$. Examine if ρ is an equivalence relation.

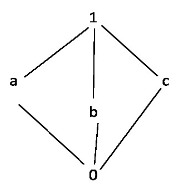
2. Define a relation R on the set $\mathbb{Z}$ of all integers by mRn if and only if $m^2 = n^2$. Is R a partial order?

3. Define a relation ρ on $\mathbb{C}$ by "$(a + ib)\rho(c + id)$ if and only if $a \leq c$ and $b \leq d$" for $a + ib, c + id \in \mathbb{C}$. Show that ρ is a partial order relation.

4. Let D_{30} be the set of all positive divisors of 30. Define a relation "$\leq$" on D_{30} by "$x \leq y$ if and only if x divides y" for $x, y \in D_{30}$. Prove that $(D_{30}, \leq)$ is a poset. Hence draw the Hasse diagram of the poset.

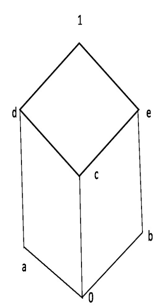
5. Let S be the set of all positive divisors of 72. Define a relation $\leq$ on S by "$x \leq y$ if and only if x is a divisor of y" for $x, y \in S$. Prove that $(S, \leq)$ is a poset. Draw the covering diagram of the poset.

6. Define distributive lattice. Give an example. Is the lattice with the following Hasse diagram distributive? Justify.



7. Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Let $x \leq y$ mean x is a divisor of y. Find the maximal element/elements in the poset $(S, \leq)$.

8. Show that the poset given in the following Hasse diagram is a lattice. Is it distributive and complemented? Justify your answer.



Morphisms, Ring and Field

1. Show that the groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic.
2. Determine whether the given map ϕ is a homomorphism.

(a) $\phi : \mathbb{R} \longrightarrow \mathbb{Z}$ under addition given by $\phi(x) =$ the greatest integer $\leq x$.

(b) $\phi : \mathbb{R}^* \longrightarrow \mathbb{R}^*$ under multiplication given by $\phi(x) = |x|$.

(c) Let $M_n(R)$ be the additive group of all $n \times n$ matrices with real entries and $\phi(A) = \det(A)$, $A \in M_n(R)$.

3. Show that $8\mathbb{Z}/72\mathbb{Z} \cong \mathbb{Z}_9$.
4. Prove that $\mathbb{Z}_8$ is not a homomorphic image of $\mathbb{Z}_{15}$.
5. Prove that the cancellation law holds in a ring R if and only if R has no divisor of zero.
6. Show that the ring of matrices $\{\begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} : a, b \in \mathbb{Z}\}$ contains divisors of zero and does not contain the unity.
7. Examine if the ring of matrices $\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{R}\}$ contains divisors of zero.
8. Prove that the ring $\mathbb{Z}[x]$, the ring of all polynomials with integer coefficients is an integral domain.
9. Prove that the ring of matrices $\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}\}$ is a field.
10. Prove that the ring of matrices $\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Q}\}$ is a field.
11. Examine if the ring of matrices $\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{R}\}$ is a field.
12. Prove that the set S of matrices $\{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in \mathbb{Z}\}$ is a subring of the ring $M_2(\mathbb{Z})$.
13. Prove that the ring $(\mathbb{Z}_n, +, \cdot)$ is an integral domain if and only if n is prime.
14. Prove that the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, the ring of Gaussian integers is an integral domain.
15. Prove that $\mathbb{Z}_{11}$, the ring of all integers modulo 11, is a field. State any theorem that you use. Find the multiplicative inverses of all the non-zero elements of $\mathbb{Z}_{11}$.
16. Let R be a ring. The centre of R is the set $\{x \in R : ax = xa\}$ for all $a \in R$. Prove that the centre of a ring is a subring.
17. In a ring $(\mathbb{Z}_n, +, \cdot)$, $[m]$ is a unit if and only if the $gcd(m, n) = 1$.
18. In a ring R with unity $(xy)^2 = x^2y^2 \ \forall x, y \in R$ then show that R is commutative.
19. Prove that in a field F, $a^2 = b^2$ implies either $a = b$ or $a = -b$ for $a, b \in F$.
20. Find all solutions of the equation $x^2 + x - 6 = 0$ in the ring $\mathbb{Z}_{14}$ by factoring the quadratic polynomial.
21. Find all solutions of the equation $x^3 - 2x^2 - 3x = 0$ in the ring $\mathbb{Z}_{12}$.
22. An element a of a ring R is idempotent if $a^2 = a$.

(a) Show that the set of all idempotent elements of a commutative ring is closed under multiplication.

(b) Find all idempotents in the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

23. Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a + b)^6$ for $a, b \in R$.
24. Prove that intersection of two subrings is a subring.