Tutorial 1 ::: MTL2005 (Algebra)

1. For each $n = 8, 12, 20, 25$, find all positive integers less than n and relatively prime to n.
2. Find integers s, t so that $1 = 7s + 11t$. Show that s, t are not unique.
3. Show that a and b are positive integers, then $ab = \text{lcm}(a, b) \times \gcd(a, b)$.
4. Let $d = \gcd(\text{a}, \text{b})$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.
5. Show that $5n + 3$ and $7n + 4$ are relatively prime for every $n \in \mathbb{N}$.
6. Let n and a are positive integers and let $d = \gcd(a, n)$. Show that the equation $ax = 1 \bmod n$ has a solution if and only if $t = 1$.
7. Let n be a fixed integer greater than 1. For any integers i and j prove that $(i \bmod n + j \bmod \text{n}) \bmod n = (i + j) \bmod n$ and $((i \bmod n) \times (j \bmod \text{n})) \bmod n = (ij) \bmod n$.
8. Let a, b, s, t be integers. If $a = b \bmod st$, show that $a = b \bmod s$ and $a = b \bmod t$. What condition on s and t is needed to make the converse true?
9. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.
10. Use the Euclidean Algorithm to find $\gcd(34, 126)$ and write it as the linear combination of 34 and 126. (the method is to be discussed in the class.)
11. Prove that there are infinitely many primes.
12. For every positive integer n, prove by Mathematical Induction that a set with exactly n elements has exactly 2^n subsets.
13. Fibonacci numbers are $1, 1, 2, 3, 5, 8$, so on. In general, the Fibonacci numbers are defined by $f_1 = 1, f_2 = 1, f_{n+2} = f_n + f_{n+1}$ for $n \geq 1$. Prove that nth Fibonacci number f_n satisfies $f_n < 2^n$.
14. Prove that the first principle of mathematical induction is a consequence of well-ordering principle.
15. Prove by induction that for every integer n, $n^3 = n \bmod 6$.
16. Write the following bijection on $\{1, 2, 3, 4, 5, 6, 7, 8\}$ as the product of disjoint cycles.
    (i) f fixes 3 and 7, takes $1, 2, 4, 5, 6, 8$ to $6, 5, 4, 8, 1, 2$ respectively.
    (ii) $(1\ 4\ 5\ 7)(2\ 4\ 3\ 6)(7\ 1\ 3)$
    (iii) $(3\ 6\ 1\ 5)^2(4\ 1\ 6)^3$
17. Write every element of S_4 as the product of disjoint cycles.
18. Show, for any $n \in \mathbb{N}$, that the set of all nth roots of unity is a group under multiplication of complex numbers. Find for each n, all members a in it such that every member is of the form a^k for some $k \in \mathbb{N}$.
19. What are all subgroups of $\mathbb{Z}$ under addition of complex numbers?
20. Find all subgroups of S_3.
21. Find all subgroups of S_4.
22. What are all homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ (addition of complex numbers is the binary operation).
23. For a homomorphism $f: G \to H$ of groups, show that $\ker f := \{x \in G: f(x) = e\} < G$ and $f(G) < H$.
24. Consider the map $\mathbb{Z} \to C_n$, $k \mapsto e^{\frac{2\pi ik}{n}}$. Show that this is a homomorphism. Is it surjective? Find $\ker f$.
25. Consider the homomorphism $m_r: \mathbb{Z} \to \mathbb{Z}$, $k \mapsto rk$ (multiplication by r), find $\ker m_r$ and the range of m_r.
26. For every $n \in \mathbb{N}$, denote by $\mathbb{Z}_n$, the set of all the congruence classes modulo n.
    (i) Show that $|\mathbb{Z}_n| = n$.
    (ii) Show that $\mathbb{Z}_n$ is closed under multiplication modulo n.
    (iii) Show that $U_n := \{[k]_n: k \in \mathbb{N}, \gcd(k, n) = 1\}$ is a group under multiplication modulo n.
    (iv) Find $|U_n|$.