Number Theory
1) Let $a$ and $b \in \mathbb{Z}$ with one of them is nonzero. We say that $d$ is the greatest common divisor of $a$ and $b$ which is denoted by $gcd(a, b)$ if
   i) $d \geq 0$
   ii) $d$ divides both $a$ and $b$
   iii) if $c$ divides both $a$ and $b$ then $c$ divides $d$
   a) Show that $gcd(a, b)$ exists.
   b) Show that there are integers $x$ and $y$ such that $ax + by = d$.
   c) Let $a = 23023$ and $b = 24871$. Find $d$, $x$ and $y$ as above.
   d) Given integers $a_1, \ldots, a_n$ define gcd of $a_1, \ldots, a_n$.

2) Let $a \in \mathbb{Z}$ and $p$ be a prime number which does not divide $a$. Show that $gcd(a, p) = 1$ which means they are relatively prime or coprime.

3) Let $p$ be a prime number. Show that if $p$ divides the product $ab$ then $p$ divides either $a$ or $b$.

4) We say that $a \in \mathbb{Z}/n\mathbb{Z}$ is invertible if there is a $b \in \mathbb{Z}/n\mathbb{Z}$ such that $ab = 1$.
   a) Show that $a \in \mathbb{Z}/n\mathbb{Z}$ is invertible if and only if $a$ and $n$ are relatively prime.
   b) Let $n = 35$ find the inverse of 11.
   c) Show that $n$ is prime if and only all elements except 0 in $\mathbb{Z}/n\mathbb{Z}$ are invertible.
   d) Find the invertible elements of $(\mathbb{Z}/72\mathbb{Z})$. This set of invertible elements is denoted by $(\mathbb{Z}/72\mathbb{Z})^*$.
   e) Let $p$ be a prime. Suppose that $xy = 0$ in $(\mathbb{Z}/p\mathbb{Z})$. Show that either $x = 0$ or
or \( y = 0 \).

f) \((10\mathbb{Z} + 3) \cap (6\mathbb{Z} + 1) = n\mathbb{Z} + k\). Find \( n \) and \( k \).

5) Using Fermat’s Little Theorem, find the remainder when \( 37^{126} \) and \( 29^{29} \) are divided by 13.

6) For which primes \( p \) is \( p^2 + 2 \) also prime?

7) Let \( p_n \) denote the \( n^{th} \) prime number. Show that \( p_{n+1} \leq p_1 \ldots p_n + 1 \). Deduce that \( p_n \leq 2^{2^n - 1} \).

8) Show that there are infinitely many primes \( p \) of the form \( 6k + 5 \).
(Hint: Similar proof for there are infinitely many primes of the form \( 4k + 3 \))

9) Show that there are infinitely many \( x \) and \( y \in \mathbb{N} \) such that \( x^x \) divides \( y^y \) but \( x \) does not divide \( y \).

10) Calculate the sums \( \sum_{k=0}^{n} \binom{n}{k}(-2)^k \) and \( \sum_{k=0}^{n} k \binom{n}{k} \).

Set Theory

1) Let \( U \) be any non-empty set. Let \( \phi(x) \) and \( \psi(x) \) be two properties (of elements of \( U \)). Define

\[ U_\phi = \{ x \in U : \phi(x) \} \quad \text{and} \quad U_\psi = \{ x \in U : \psi(x) \}\]

Express the following sets in terms of \( U_\phi \) and \( U_\psi \)

a) \( \{ x \in U : \phi(x) \land \psi(x) \} \)

b) \( \{ x \in U : \phi(x) \lor \psi(x) \} \)

2) Let \( A \) and \( B \) be two disjoint sets. A set \( W \) is said to be a connection of \( A \) and \( B \) if the following conditions hold:

i) if \( Z \in W \) then there are \( x \in A \) and \( y \in B \) such that \( Z = \{x, y\} \).

ii) For each \( x \in A \) there is exactly one \( y \in B \) such that \( \{x, y\} \in W \).

iii) For each \( y \in B \) there is exactly one \( x \in A \) such that \( \{x, y\} \in W \).

Show that for any two disjoint sets \( A \) and \( B \) the collection \( \Sigma(A, B) \) of all connections of \( A \) with \( B \) is a set.

3) Let \( A \) be a non-empty set, let \( \equiv \subseteq A \times A \) be relation. Prove that \( \equiv \) is
an equivalence relation if and only if there exists a set $Q$ and a surjection $\pi : A \to Q$ so that
\[ x \equiv y \iff \pi(x) = \pi(y). \]

4) Find a bijection between $\mathbb{N}$ and $\mathbb{Q}$.

5) **Definition:** A subgroup of $\mathbb{Z}$ is a subset of $\mathbb{Z}$ which is closed under subtraction.
Find all subgroups of $\mathbb{Z}$.

6) Let $K$ be a field. Show that $K$ has only two ideals namely 0 and $K$ itself.

7) Find all functions $f$ from $\mathbb{N}$ to itself which satisfies $f(x + y) = f(x) + f(y)$.

8) **Filters**
**Definition:** Let $X$ be a set. A filter on $X$ is a set $\mathcal{F}$ of subsets of $X$ that satisfies:

i) If $A \in \mathcal{F}$ and $A \subseteq B \subseteq X$, then $B \in \mathcal{F}$.
ii) If $A$ and $B$ are in $\mathcal{F}$ then $A \cap B \in \mathcal{F}$.
iii) $\emptyset \not\in \mathcal{F}$ and $X \in \mathcal{F}$.

If $A$ is a non-empty fixed subset of $X$ then the set $\mathcal{F}(A)$ of subsets of $X$ that contains $A$ is a filter on $X$. Such a filter is called a Principal Filter. If $X$ is infinite then the set of cofinite subsets of $X$ is a called a Frechet Filter. A maximal filter is called an Ultrafilter.

Fix a set $X$

a) Show that a principal filter $\mathcal{F}(A)$ on $X$ is an ultrafilter if and only if $A$ is a singleton.

b) Show that the Frechet filter (on an infinite set) cannot be contained in a principal filter.

c) Let $(\mathcal{F}_i)_{i \in I}$ be a family of filters then $\bigcap_{i \in I} \mathcal{F}_i$ is a filter.

d) Let $\mathcal{F}$ be a set of subsets of $X$ so that for any $A_1, \ldots, A_n \in \mathcal{F}$, $A_1 \cap \ldots \cap A_n \neq \emptyset$, then there is a filter that contains $\mathcal{F}$. Describe this filter in terms of $\mathcal{F}$.

e) Show that a filter $\mathcal{F}$ is an ultrafilter if and only if for any $A \subseteq X$ either $A$ or $A^c$ is in $\mathcal{F}$. Conclude that in an ultrafilter $\mathcal{F}$, if $A \cup B \in \mathcal{F}$ then either $A$ or $B$ is in $\mathcal{F}$.
f) Conclude that any ultrafilter on $X$ that contains a finite subset of $X$ is a principal filter. Deduce that every non-principal ultrafilter contains the Frechet filter.