MATH10111 Questions from Lecture Notes

Available at JTANG.DEV/RESOURCES

D: Definition **P**: Proof

Number theory I

D: Prime Number
P: Let $a, b \in \mathbb{Z}$ with $a \geq 2$, then $a \not| b$ or $a \not| (b+1)$.
P: Let a and b be natural numbers and let p be a prime number. If $p|ab$, then $p|a$ or $p|b$.
P: $\sqrt{2}$ is not a rational number.
P: Every natural number greater than one has a prime divisor.
P: There are infinitely many prime numbers.

Sets

D: Subset
D: $A = B$
D: Empty Set
D: $A \cap B$
D: $A \cup B$
D: $A \setminus B$
D: A^c
D: $\mathcal{P}(A)$
D: $A \times B$

P: For any set A, we have $\emptyset \subseteq A$.
P: The empty set is unique.
P: If A has precisely n elements, then $\mathcal{P}(A)$ has 2^n elements.

Functions

D: $f = g$
D: Constant Function
D: Identity Function
D: $f|_X$
D: Injective
D: Surjective
D: Bijective
D: $g \circ f$
D: f^{-1}
D: Permutation

P: Let $f : A \to B$ and $g : B \to C$ be functions. If f and g are both 1-1, then $g \circ f$ is 1-1.
P: Let $f : A \to B$ and $g : B \to C$ be functions. If f and g are both onto, then $g \circ f$ is onto.
P: Let $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions, then $h \circ (g \circ f) = (h \circ g) \circ f$.
P: Let $f : A \to B$ be a bijection, then $f^{-1} : B \to A$ is a bijection.
P: Let $f : A \to B$ be a bijection, then $(f^{-1})^{-1} = f$.
P: Let $f : A \to B$ be a bijection, then $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.
P: Let f, g, h be permutations of set A, then $g \circ f$ is a permutation of A.
P: Let f, g, h be permutations of set A, then $h \circ (g \circ f) = (h \circ g) \circ f$.
P: Let f, g, h be permutations of set A, then f^{-1} is a permutation of A, and $f^{-1} \circ f = f \circ f^{-1} = i_A$

Cardinality

D: A has cardinality n
D: A is finite or infinite
D: A is countable
D: A k-subset of A
D: $\mathcal{P}_k(A)$
D: $\binom{n}{k}$

P: Let $m, n \in \mathbb{N}$. If there is a 1-1 function $f : \mathbb{N}_m \to \mathbb{N}_n$, then $m \leq n$.
P: Let A be a set. Suppose that $m, n \in \mathbb{N}$ and that there are bijections $f : \mathbb{N}_m \to A$ and $g : \mathbb{N}_n \to B$, then $m = n$.
P: Let A and B be finite sets and let $f : A \to B$ be a 1-1 function, then $|A| \leq |B|$. If f is a bijection, then $|A| = |B|$.
P: Let A and B be non-empty finite sets and let $f : A \to B$. If $|A| > |B|$, then $\exists x_1, x_2 \in A$, $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.
P: Let X and Y be finite sets such that $X \cap Y = \emptyset$, then $|X \cup Y| = |X| + |Y|$.
P: If $X_1, \cdots, X_n$ are pairwise disjoint finite sets, then $X_1 \cup \cdots \cup X_n = \bigcup_{i=1}^{n} X_i$ is a finite set and $|\bigcup_{i=1}^{n} X_i| = \sum_{i=1}^{n} |X_i|$.
P: Let X and Y be finite sets, then $|X \cup Y| = |X| + |Y| - |X \cap Y|$.
P: Let X and Y be finite sets, with $|X| = m$ and $|Y| = n$, then $X \times Y$ is a finite set and $|X \times Y| = mn$.
P: Let $X_1, \cdots, X_m$ be finite sets, where $|X_i| = n_i$ for each i, then $|X_1 \times \cdots \times X_m| = n_1 n_2 \cdots n_m$.
P: Let X and Y be non-empty finite sets, where $|X| = m$ and $|Y| = n$, then the number of functions $X \to Y$ is nm.
P: Let A and B be finite sets with $|A| = |B| = n$, then there are precisely $n!$ bijections $A \to B$.
P: Let $n, k \in \mathbb{N} \cup \{0\}$, then $\binom{n}{k} = 0$ if $k > n$.
P: Let $n, k \in \mathbb{N} \cup \{0\}$, $\binom{n}{0} = \binom{n}{n} = 1$ and $\binom{n}{1} = n$.
P: Let $n, k \in \mathbb{N} \cup \{0\}$, $\binom{n}{k} = \binom{n}{n-k}$.

P: Let $n, k \in \mathbb{N} \cup \{0\}$, if $0 < k \leq n$, then $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.
P: Let $n, k \in \mathbb{N} \cup \{0\}$ with $k \leq n$, then $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Euclidean Algorithm

D: $\gcd(a, b)$

P: Let A be a non-empty finite set of real numbers, then A has a minimum and a maximum element.
P: Let $a, b \in \mathbb{Z}$ with $b > 0$, then there are unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.
P: Let $a, b \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$. Suppose $q, r \in \mathbb{Z}$ with $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.
P: Let $a, b \in \mathbb{Z}$ with $a, b > 0$, then $\exists s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$.
P: Let p be a prime, then $\forall a, b \in \mathbb{N}, p|ab \Rightarrow p|a$ or $p|b$.

Congruence of integers

D: $a \equiv b \bmod n$

D: Linear congruence

P: Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, then $a \equiv b \bmod n \Leftrightarrow a$ and b have the same remainder after division by n.
P: Let $a, b, c, d, \lambda \in \mathbb{Z}$ and $n, k \in \mathbb{N}$. Suppose that $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $a + c \equiv b + d \bmod n$.
P: Let $a, b, c, d, \lambda \in \mathbb{Z}$ and $n, k \in \mathbb{N}$. Suppose that $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $ac \equiv bd \bmod n$.
P: Let $a, b, c, d, \lambda \in \mathbb{Z}$ and $n, k \in \mathbb{N}$. Suppose that $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $\lambda a \equiv \lambda b \bmod n$.
P: Let $a, b, c, d, \lambda \in \mathbb{Z}$ and $n, k \in \mathbb{N}$. Suppose that $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $a^k \equiv b^k \bmod n$.
P: Let $c \in \mathbb{Z}$ and $n \in \mathbb{N}$. Suppose $\gcd(c, n) = 1$, then $\exists s \in \mathbb{Z}$ such that $sc \equiv 1 \bmod n$.
P: Let $d, n \in \mathbb{N}$ with $d|n$ and let $b_1, b_2 \in \mathbb{Z}$, then $db_1 \equiv db_2 \bmod n \Leftrightarrow b_1 \equiv b_2 \bmod \frac{n}{d}$.
P: Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. $ax \equiv b \bmod n$ has a solution $\Leftrightarrow d|b$, where $d = \gcd(a, n)$.
P: Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Write d = gcd(a,n). Suppose $d|b$. Let $x \in \mathbb{Z}$ be a solution to $ax \equiv b \bmod n$, then $\forall k \in \mathbb{Z}$,$x+kn$ is also a solution. Instead suppose that $d = 1$. Then $ax \equiv b \bmod n$ has a unique solution in $\{0, 1, ..., n-1\}$.

Relations

D: Relation R on A
D: Reflexive relation
D: Symmetric relation
D: Transitive relation
D: Equivalence relation
D: Equivalence class
D: Partition
D: The set $\mathbb{Q}$
D: Addition $\oplus$
D: Multiplication $\odot$

P: Let R be an equivalence relation on a set non-empty A. Let $a, b \in \mathbb{A}$. If aRb, then $R_a = R_b$.
P: Let R be an equivalence relation on a set non-empty A. If $a \not R\, b$, then $R_a \cap R_b = \emptyset$.
P: Let R be an equivalence relation on a non-empty set A. Then $\{R_a : a \in A\}$ is a partition of A.
P: Let A be a non-empty set and let $\{A_i : i \in I\}$ be a partition of A. Define a relation R on A by $aRb \Leftrightarrow \{a, b\} \subseteq A_i$ for some $i \in I$. Then R is an equivalence relation, with equivalence classes A_i for $i \in I$.

Number theory II

D: Fermat's little theorem

P: Let p be a prime, and let $a_1, \cdots, a_n \in \mathbb{Z}$. If $p|a_1 \cdots a_n$, then p divides at least one of $a_1, \cdots, a_n$.
P: Let $n \in \mathbb{N}$ with $n \geq 2$, then $n = p_1 \cdots p_r$, where each p_i is prime and any two such expressions for n differ only in the order of writing.
P: Let $p \in \mathbb{N}$ be prime, and let $a \in \mathbb{N}$. If $p \not| a$, then $a^{p-1} \equiv 1 \bmod p$.
P: Let $p \in \mathbb{N}$ be prime and $a \in Z_p \setminus \{0\}$, then the map $f : Z_p \setminus \{0\} \to Z_p \setminus \{0\}$ defined by $f(x) = a \odot x$ is a permutation.

Binary Operations

D: $*$ on a set S
D: $*$ is commutative
D: $*$ on associative
D: Identity element w.r.t S
D: Group
D: Commutative group
D: Symmetric group
D: Cyclic group
D: Field

P: Let $*$ be a binary operation on a set S. Let $e, f \in \mathbb{S}$ be identity elements for S with respect to $*$, then $e = f$.