MATH10111 Cheat Sheet

Available at JTANG.DEV/RESOURCES

NUMBER THEORY I & II

Prime number: $\forall a \in \mathbb{N}, a|p \Rightarrow a \in \{1, p\}$

Fermat's Little Theorem
Let $p \in \mathbb{N}$ be prime and let $a \in \mathbb{N}$.
If $p \not| a$, then $a^{p-1} \equiv 1 \bmod p$.

An equivalent formulation is: $a^p \equiv a \bmod p$.

MATHEMATICAL INDUCTION

Simple Mathematical Induction
Let $p(n)$ be a statement about the $n \in \mathbb{N}$

- show $p(1)$ is true (base case),
- show for $k \in \mathbb{N}$, if $p(k)$ is true, then $p(k+1)$ is true (inductive step),
- then $p(n)$ is true for all $n \in \mathbb{N}$

For strong induction, the inductive step is $k \in \mathbb{N}$, if $p(r)$ is true for all $r \leq k$, then $p(k+1)$ is true.

SET THEORY

Let A and B be sets.
$A \subseteq B : x \in A \Rightarrow x \in B$
Empty Set: $\{\}$ or $\emptyset$
A $= \{x : x$ has property $P\}$
$A \cap B = \{x : x \in A$ and $x \in B\}$
$A \cup B = \{x : x \in A$ or $x \in B\}$
$A \setminus B = \{x : x \in A$ and $x \notin B\}$
$A \subseteq U \Rightarrow A^c = U \setminus A$
Power Set: $\mathcal{P}(A)$ is a set whose elements are all of the subsets of A.
$A \times B = \{(a, b) : a \in A, b \in B\}$
$A^n = A \times \cdots \times A$ (n times)

CARDINALITY OF SETS

Counting Subsets
Let A be a set and $k \in \mathbb{N} \cup \{0\}$. A *k-subset* of A is a subset $X \subseteq A$ with $|X| = k$.

Write $\mathcal{P}_k(A) = \{X \subseteq A : |X| = k\}$

If $|A| = n$, then

$$\mathcal{P}(A) = \bigcup_{k=0}^{n} \mathcal{P}_k(A)$$

We define $\binom{n}{k}$ to be the cardinality of $\mathcal{P}_k(\mathbb{N}_n)$

CARDINALITY OF SETS

Let $n \in \mathbb{N}$, then $n! = n(n-1)\cdots 2.1$. Define $0! = 1$.

$\mathbb{N}_n = \{1, 2, 3, \cdots n\} = \{k \in \mathbb{N} : 1 \leq k \leq n\}, n \in \mathbb{N}$
Let A be a set, A has cardinality n if there exists a bijection $f : \mathbb{N}_n \to A$, in this case, we write $|A| = n$.

Define $|\emptyset| = 0$. If $|A| = n$ for some $n \in \mathbb{N} \cup \{0\}$, then we say that A is finite, else infinite.

For $X_1, \cdots, X_n$ as pairwise disjoint finite sets:

$$|\bigcup_{i=1}^{n} X_i| = \sum_{i=1}^{n} |X_i|$$

FUNCTIONS

$f : A \to B$
f has domain A and codomain B

Let $f : A \to B$, $g : C \to D$ be functions.
$f = g \Leftarrow A = C, B = D$ and $\forall x \in A, f(x) = g(x)$

Constant function: $\exists b_0 \in B, \forall a \in A, f(a) = b_0$
Identity function: $\forall a \in A, h(a) = a$, denoted by i_A or 1_A for $h : A \to A$

Restriction of f to X: $X \subseteq A$ and $g : X \to B$ by $g(x) = f(x), \forall x \in X$, denoted by $f|_X$ or $f|X$

Injective: $\forall x, y \in A, f(x) = f(y) \Rightarrow x = y$
Surjective: $\forall y \in B, \exists x \in A$ such that $y = f(x)$
Bijective: Both injective and surjective.

Let $f : A \to B$ and $g : B \to C$ be functions.

$$g \circ f(x) = g(f(x)) \text{ for all } x \in A$$

Note that $g \circ f : A \to C$ and the codomain of f must be a subset of domain g.

Inverse: $f^{-1} : B \to A$ by $f^{-1}(y) = x$, where x is the unique $x \in A$ with $f(x) = y$

A permutation of A is a bijection from A to A.

Cycle Notation for Permutations

$(\alpha_1 \alpha_2 \cdots \alpha_r)$ denotes
$\alpha_1 \mapsto \alpha_2$, $\alpha_2 \mapsto \alpha_3 \cdots$ $\alpha_{r-1} \mapsto \alpha_r$, $\alpha_r \mapsto \alpha_1$
$\alpha \mapsto \alpha$ for all $a \in \mathbb{N}_n \setminus \{\alpha_1 \cdots \alpha_r\}$

If $c = (\alpha_1 \cdots \alpha_r)$, then $c^{-1} = (\alpha_1 \alpha_r \alpha_{r-1} \cdots \alpha_2)$
$(c_1 \circ c_2 \circ \cdots c_t)^{-1} = (c_1)^{-1} \circ (c_2)^{-1} \circ \cdots (c_t)^{-1}$

$(\alpha_1 \alpha_2 \cdots \alpha_r)$ is called a cycle with length r.

THE EUCLIDEAN ALGORITHM

Minimum and Maximum
Let A be a non-empty finite set of real numbers.

$$\exists a, b \in A, \forall x \in A, a \leq x \leq b$$

The Division Theorem
Let $a, b \in \mathbb{Z}, b > 0, then$

$$\exists! q, r \in \mathbb{Z}, a = bq + r, 0 \leq r < b.$$

The Greatest Common Divisor
If $d = \gcd(a, b)$, then $d|a$ and $d|b$, and if $c \in \mathbb{Z}$ such that $c|a$ and $c|b$ then $c \leq d$.

Reverse of the Euclidean Algorithm
Let $a, b \in \mathbb{Z}$, with $a, b > 0$.
Then $\exists s, t \in \mathbb{Z}$, $\gcd(a, b) = sa + tb$.

RELATIONS

Let A be a set with $A \neq \emptyset$. A relation R on A is a subset of $A \times A$. For $x, y \in A$, xRy if $(x, y) \in R$.

Reflexive: $\forall x \in A, xRx$.
Symmetric: $\forall x, y \in A, xRy \Rightarrow yRx$.
Transitive: $\forall x, y, z \in A, xRy$ and $yRz \Rightarrow xRz$.

An equivalence relation on a non-empty set A is a relation which is reflexive, symmetric and transitive.

Equivalence Classes
Let R be an equivalence relation on a non-empty set A. Let $a \in A$, then R_a is defined as:

$$R_a = \{x \in A : aRx\}$$

Note that $a \in R_a$ (since R is reflexive) and $R_a \subseteq A$
Also, $R_a = \{x \in A : aRx\} = \{x \in A : xRa\}$.

Partitions
Let X be a non-empty set, $\{X_i : i\ inI\}$ to be a collection of non-empty subsets of X, where I is the index set, such that:

- $\cup_{i \in I} X_i = X$ and
- $\forall i, j \in I, X_i = X_j$ or $X_i \cap X_j = \emptyset$

Then $\{X_i : i \in I\}$ is a partition of X.

Definition of $\mathbb{Q}$
Let $A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$
Define R on A by $(a, b)R(c, d) \Leftrightarrow ad = bc$
$\mathbb{Q} = \{R_{(a,b)} : (a, b) \in A\}$

Integers modulo n
Let $a, b \in \mathbb{Z}_n$, define $\oplus$ and $\odot$ on $\mathbb{Z}_n$ as follows:
Addition $\oplus$: $a \oplus b = r, r \in \mathbb{Z}_n, a + b \equiv r \bmod n$.
Mutiplication $\odot$: $a \odot b = t, t \in \mathbb{Z}_n, ab \equiv t \bmod n$.
Note that r and t are unique.

CONGRUENCE OF INTEGERS

Let $n \in \mathbb{N}$. For $a, b \in \mathbb{Z}$, we say that a and b are congruent modulo n if and only if $n|(a - b)$. We write $a \equiv b \bmod n$.
Note that $a \equiv 0 \bmod n \Leftrightarrow n|a$.

Linear Congruences
Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Suppose we want to find $x, y \in \mathbb{Z}$, such that $ax + ny = b$. This problem is the equivalent to finding $x \in \mathbb{Z}$ such that:

$$ax \equiv b \bmod n.$$

BINARY OPERATIONS

A binary operation $*$ on a set S is a function:

$$* : S \times S \to S,\ a * b = *(a, b).$$

Multiplication tables are read [row] $*$ [column].

Commutative: $\forall a, b \in S, a * b = b * a$
Associative: $\forall a, b, c \in S, a * (b * c) = (a * b) * c$
Identity element (e): $\forall a \in S, e * a = a * e = a$.

Groups
Let G be a non-empty set and $*$ be a binary operation on G. Then we call $(G, *)$ a group if:

- $*$ is associative,
- G has as identity element e with respect to $*$,
- $\forall g \in G, \exists h \in G, g * h = h * g = e$.

Commutative group: $\forall g, h \in G, g * h = h * g$

Symmetric Group
$(S_n, \circ)$ is the symmetric group, where S_n is the set of permutations $f : N_n \to N_n$ and $\circ$ be the composition of permutations. The identity map $i_{N_n} : N_n \to N_n$ is given by $i_{N_n}(a) = a$ for all a is the identity element, and write $e =_{N_n}$.

Cyclic Group
Let $(G, *)$ be a group with identity element e. Note that $\forall g \in G$ we have $g^0 = e$, we say that G is cyclic if:

$$\exists a \in G, G = \{a^k : k \in \mathbb{Z}\}.$$

Fields
Let F be a non-empty set and let $+, *$ be binary operations on F. We say $(F, +, *)$ is a field if:

- $(F, +)$ is a commutative group, let $0 = e$.
- $(F \setminus \{0\}, *)$ is a commutative group, let $1 = e$.
- $\forall a, b, c \in F, a * (b + c) = (a * b) + (a * c)$.

$-a$ is the inverse of $a \in F$ with respect to $+$.
a^{-1} is the inverse of $a \in F \setminus \{0\}$ with respect to $*$.