Definitions and Theorem you can use for Math 220 Homework and Exams

1 Definitions

An integer n is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

An integer n is **odd** if $n = 2a + 1$ for some $a \in \mathbb{Z}$.

Two integers have the **same parity** if they are both even or they are both odd. Otherwise they have **opposite parity**.

Suppose a and b are integers. We say that a **divides** b, written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a **divisor** of b and b is a **multiple** of a. We say a **does not divide** b if there is no integer c such that $b = ac$, and we write $a \nmid b$.

A natural number n is **prime** if it has exactly two positive divisors, 1 and n.

The **greatest common divisor** of integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b.

The **least common multiple** of non-zero integers a and b, denoted $\text{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

Given integers a and b and an $n \in \mathbb{N}$, we say that a and b are **congruent modulo** n if $n|(a - b)$. We express this as $a \equiv b \pmod{n}$. We say a and b are **not congruent modulo** n if $n \nmid (a - b)$ and we write $a \not\equiv b \pmod{n}$.

A real number x is **rational** if $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Also, if x is irrational if it is not rational, that is if $x \neq \frac{a}{b}$ for every $a, b \in \mathbb{Z}$.

The **Cartesian product** of two sets A and B is $A \times B = \{(a, b) : a \in A \text{ and } b \in b\}$.

The set A is a **subset** of B, written $A \subseteq B$, if whenever $a \in A$ then $a \in B$.

The **power set** of A is the set of all subsets of A written $\mathscr{P}(A) = \{B : B \subseteq A\}$.

The **union** of two sets A and B is $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

The **intersection** of two sets A and B is $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

The **difference** of two sets A and B is $A - B = \{x : x \in A \text{ and } x \notin B\}$.

The **complement** of sets A with universal set U is $U - A = \{x : x \in U \text{ and } x \notin A\}$.

A natural number p is called **perfect** if p is equal to the sum of all its divisors less than p.
Define n **factorial** to be $n! = n(n-1)(n-2)\dots(2)(1)$ for integers $n \geq 1$ and $0! = 1$.

Define **the binomial coefficient** $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ for integers $n \geq 0$ and $0 \leq k \leq n$ and $\binom{n}{k} = 0$ for integers $n \geq 0$ and $k < 0$ or $k > n$.

The **Fibonacci numbers** are defined recursively as $F_1 = 1$, $F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n > 2$.

A relation R on a set A is **reflexive** if for all $x \in A$ we have xRx.

A relation R on a set A is **symmetric** when for all $x, y \in A$ if xRy then yRx.

A relation R on a set A is **transitive** when for all $x, y, z \in A$ if xRy and yRz then xRz.

Suppose R is an equivalence relation on a set A. Given any element $a \in A$, the **equivalence class containing** a is the subset $\{x \in A : xRa\}$ of A consisting of all the elements of A that relate to a. This set is denoted as $[a]$. Thus the equivalence class containing a is the set $[a] = \{x \in A : xRa\}$.

A **partition** of a set A is a set of non-empty subsets of A, such that the union of all the subsets equals A, and the intersection of any two different subsets is $\emptyset$.

Let $n \in \mathbb{N}$. The equivalence classes of the equivalence relation $\equiv \pmod{n}$ are $[0], [1], [2], \ldots, [n-1]$. The **integers modulo** n is the set $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$.

A function $f : A \to B$ is **injective (one-to-one)** if when $x \neq y$ then $f(x) \neq f(y)$.

A function $f : A \to B$ is **surjective (onto)** if for all $y \in B$ there is a $x \in A$ such that $f(x) = y$.

A function $f : A \to B$ is **bijective** if if is both injective and surjective.

Suppose $f : A \to B$ is a function. If $X \subseteq A$, the **image** of X is the set $f(X) = \{f(x) : x \in X\} \subseteq B$. If $Y \subseteq B$, the **preimage** of Y is the set $f^{-1}(Y) = \{x \in A : f(x) \in Y\} \subseteq A$.

Two sets A and B **have the same cardinality**, written $|A| = |B|$, if there exists a bijective function $f : A \to B$.

2 Theorems, Propositions, and Facts

2.1 Facts you can use without justification ever

If $a, b \in \mathbb{Z}$

- $a + b \in \mathbb{Z}$
- $ab \in \mathbb{Z}$.

All your previous rules for algebra.

2.2 Theorems and propositions we can start to use without justification

Note: If a problem asks you to prove one of the following (or even something equivalent to one of the following) you will need to prove it using more basic facts and propositions. You should know how to prove any of the following if asked.

Proposition 1. An integer n is even if and only if n^2 is even.

Proposition 2. An integer n is odd if and only if n^2 is odd.

Proposition 3. If $a, b \in \mathbb{Z}$ are of the same parity if and only if is $a + b$ is even.

Proposition 4. If $a, b \in \mathbb{Z}$ are of opposite parity if and only if is $a + b$ is odd.

Proposition 5. Let $a, b \in \mathbb{Z}$. The product ab is odd if and only if both a and b are odd.

Proposition 6. Let $a, b \in \mathbb{Z}$. The product ab is even if and only if a or b is even.

Proposition 7. For two non-zero integers a, b, $\text{lcm}(a, b) \geq a$ and $\text{lcm}(a, b) \geq b$.

Proposition 8. For two positive integers a, b, $\gcd(a, b) \leq a$ and $\gcd(a, b) \leq b$.

Proposition 9. For the integers a, b, c and $n \in \mathbb{N}$, if $a \equiv b \pmod{n}$ then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$.

Proposition 10. (Division Algorithm) If $a, b \in \mathbb{N}$, then there exist unique integers q and r such that $a = qb + r$ where $0 \leq r < b$. The r is called the **remainder**.

Proposition 11. (Division Algorithm Generalized) If $a, b \in \mathbb{Z}$ and $b \neq 0$, then there exist unique integers q and r such that $a = qb + r$ where $0 \leq r < |b|$.

Proposition 12. For the integer a and $n \in \mathbb{N}$, there is a unique r such that $0 \leq r < n$ and $a \equiv r \pmod{n}$.

Proposition 13. For the integers a, b and $n \in \mathbb{N}$, $a \equiv b \pmod{n}$ if and only if the remainders of a and b when divided by n are equal.

Proposition 14. (Proposition 7.1 from the book) If $a, b \in \mathbb{N}$, then there exist integers k and ℓ such that $\gcd(a, b) = ak + b\ell$.

Proposition 15. (Generalized Proposition 7.1 from the book) If $a, b \in \mathbb{Z}$ where at least a or b is nonzero, then there exist integers k and ℓ where $\gcd(a, b) = ak + b\ell$.

Proposition 16. For $a, b \in \mathbb{N}$ and $k, \ell \in \mathbb{Z}$, if $D = ak + b\ell$ then $\gcd(a, b)|D$.

Proposition 17. For integers n and k we have

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Proposition 18. Suppose a and b are integers. If p is prime and $p|ab$, then $p|a$ or $p|b$.

Proposition 19. Suppose $a_1, a_2, \ldots, a_n$ are n integers, where $n \geq 2$. If p is prime and $p|(a_1 \cdot a_2 \cdot a_3 \cdots a_n)$, then $p|a_i$ for at least one of the a_i.

Theorem 1 (Fundamental Theorem of Arithmetic). Any integer $n > 1$ has a unique prime factorization. That is, if $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ and $n = a_1 \cdot a_2 \cdot a_3 \cdot a_\ell$ are two prime factorizations of n, then $k = \ell$, and the primes p_i and a_i are the same, except that they may be in a different order.

Theorem 2. Suppose R is an equivalence relation on a set A. Suppose also that $a, b \in A$. Then $[a] = [b]$ if and only if aRb.

Theorem 3. Suppose R is an equivalence relation on a set A. Then the set $\{[a] : a \in A\}$ of equivalence classes of R forms a partition of A.

Theorem 4. Suppose $f : A \to B$ and $g : B \to C$. If both f and g are injective, then $g \circ f$ is injective. If both f and g are surjective, then $g \circ f$ is surjective.

Theorem 5. Let $f : A \to B$ be a function. Then f is bijective if and only if the inverse relation f^{-1} is a function from B to A.

Theorem 12.4 from your book.

Proposition 20. The sets $\mathbb{N}$, $\mathbb{Q}$, and $\mathbb{Z}$ are countably infinite. The sets $(0, 1)$, $[0, 1]$, and $\mathbb{R}$ are uncountable. Also $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$.

Proposition 21. If A and B are countably infinite then $A \times B$ and $A \cup B$ are countably infinite.