MATH1064 SUMMARY NOTES

Formulas and Theorems

Author
Tiana
Smarty Pants

Contents

1 Divisibility and Modular Arithmetic

1.1 Division

Principle 1.1. $a \mid b$ if there exists some $k \in \mathbb{Z}$ such that $b = a \cdot k$. We denote this by $a \mid b$.

Theorem 1.2. Let $a, b, c \in \mathbb{Z}$ and $a \neq 0$. Then:

1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
2. If $a \mid b$, then $a \mid bc$.
3. If $a \mid b$, $b \neq 0$, and $b \mid c$, then $a \mid c$.

Proposition 1.3. If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ whenever m and n are integers.

1.2 The Division Algorithm

Theorem 1.4. Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$. Here, d is called the divisor, a is called the dividend, q is called the quotient, and r is called the remainder.

1.3 Modular Arithmetic

Definition 1.5. a is congruent to b modulo m if m divides $a - b$ (where $a, b \in \mathbb{Z}$ and $m > 0$). We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m.

Theorem 1.6. Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Theorem 1.7. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$ for $m > 0$.

Theorem 1.8. Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

2 Primes and Greatest Common Divisors

2.1 Primes

Proposition 2.1. An integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

Theorem 2.2. The Fundamental Theorem of Arithmetic: Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes (primes can repeat and be counted as powers).

Theorem 2.3. If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

2.2 Greatest Common Divisors and Least Common Multiples

Definition 2.4. Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b, denoted by $\gcd(a, b)$.

Definition 2.5. The integers a and b are relatively prime if their greatest common divisor is 1.

Definition 2.6. The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. Denoted by $\operatorname{lcm}(a, b)$.

Theorem 2.7. $\gcd(a, b) = p^{\min(a_1,b_1)} \cdot p^{\min(a_2,b_2)} \cdot \ldots \cdot p^{\min(a_n,b_n)}$ - so take the smallest common prime out of the prime decomposition of a and b and take the product.

Theorem 2.8. $\operatorname{lcm}(a, b) = p^{\max(a_1,b_1)} \cdot p^{\max(a_2,b_2)} \cdot \ldots \cdot p^{\max(a_n,b_n)}$ - so take the greatest common primes out of the prime decomposition and take the product.

Theorem 2.9. Let a and b be positive integers. Then $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$.

2.3 The Euclidean Algorithm

Theorem 2.10. Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Theorem 2.11. ALGORITHM 1 The Euclidean Algorithm. to find the $\gcd(a, b)$ we can take use the euclidean algorithm. we continusly use the division algorithm until

1. Write $a = q \cdot b + r$ by the Division Algorithm.
2. If $r = 0$, then $\gcd(a, b) = b$. (i.e., if $a \mid b$)
3. If $r \neq 0$, replace (a, b) with (b, r) and repeat until you reach a remainder of 0.

the FIX THIS WITH PROPER DEFINITUON

Theorem 2.12. If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Theorem 2.13. Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

3 Counting

4 Probability

4.1 Finite Probability

Theorem 4.1. If S is a finite nonempty sample space of equally likely outcomes, and E is an event, that is, a subset of S, then the *probability* of E is $p(E) = \frac{|E|}{|S|}$.

Theorem 4.2. Let E_1 and E_2 be events in the sample space S. Then

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$$

Definition 4.3. The *probability* of the event E is the sum of the probabilities of the outcomes in E. That is,

$$p(E) = \sum_{s \in E} p(s).$$

4.2 Conditional Probability

Definition 4.4. Let E and F be events with $p(F) > 0$. The *conditional probability* of E given F, denoted by $p(E \mid F)$, is defined as

$$p(E \mid F) = \frac{p(E \cap F)}{p(F)}$$

4.3 Independence

Definition 4.5. The events E and F are independent if and only if $p(E \cap F) = p(E) \cdot p(F)$.

4.4 Random Variables

Definition 4.6. A random variable is a function from the sample space of an experiment to the set of real numbers. That is, a random variable assigns a real number to each possible outcome

Definition 4.7. The distribution of a random variable X on a sample space S is the set of pairs $(r, p(X = r))$ for all $r \in X(S)$, where $p(X = r)$ is the probability that X takes the value r. The set of pairs in this distribution is determined by the probabilities $p(X = r)$ for $r \in X(S)$.

4.5 Bayes' Theorem

Theorem 4.8. Suppose that E and F are events from a sample space S such that $p(E) \neq 0$ and $p(F) \neq 0$. Then,

$$p(F \mid E) = \frac{p(E \mid F)p(F)}{p(E \mid F)p(F) + p(E \mid \overline{F})p(\overline{F})}.$$

4.6 Expected Value and Variance

Definition 4.9. The expected value, also called the expectation or mean, of the random variable X on the sample space S is equal to

$$E(X) = \sum_{s \in S} p(s)X(s).$$

The deviation of X at $s \in S$ is $X(s) - E(X)$, the difference between the value of X and the mean of X.

Theorem 4.10. If X is a random variable and $p(X = r)$ is the probability that $X = r$, so that

$$p(X = r) = \sum_{s \in S, X(s) = r} p(s),$$

then

$$E(X) = \sum_{r \in X(S)} p(X = r)r.$$

Theorem 4.11. Linearity of Expectations
If X_i, $i = 1, 2, \ldots, n$, with n a positive integer, are random variables on S, and if a and b are real numbers, then

(i) $E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$

(ii) $E(aX + b) = aE(X) + b$

Definition 4.12. Independent Random Variables The random variables X and Y on a sample space S are independent if

$$p(X = r_1 \text{ and } Y = r_2) = p(X = r_1) \cdot p(Y = r_2),$$

or in words, if the probability that $X = r_1$ and $Y = r_2$ equals the product of the probabilities that $X = r_1$ and $Y = r_2$, for all real numbers r_1 and r_2.

Theorem 4.13. If X and Y are independent random variables on a sample space S, then $E(XY) = E(X) \cdot E(Y)$.

4.7 Variance

Definition 4.14. The variance of X, denoted by $V(X)$ is

$$V(X) = \sum_{s \in S} (X(s) - E(X))^2 p(s).$$

Theorem 4.15. If X is a random variable on a sample space S, then

$$V(X) = E(X^2) - E(X)^2.$$

5 Graphs