MATH1064 SUMMARY NOTES

Formulas and Theorems

Author
Tiana
Smarty Pants

Contents

1 Examples

Theorem 1.1. This is a theorem.

Proposition 1.2. This is a proposition.

Principle 1.3. This is a principle.

2 Divisibility and Modular Arithmetic

2.1 Division

Principle 2.1. $a \mid b$ if there exists some $k \in \mathbb{Z}$ such that $b = a \cdot k$. We denote this by $a \mid b$.

Theorem 2.2. 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 2.3. 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.

2.2 The Division Algorithm

Theorem 2.4. 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.

2.3 Modular Arithmetic

Definition 2.5. 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 2.6. 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 2.7. 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 2.8. 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 $ac \equiv bd \pmod{m}$.

3 Primes and Greatest Common Divisors

3.1 Primes

Proposition 3.1. 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 3.2. 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 3.3. If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

3.2 Greatest Common Divisors and Least Common Multiples

Definition 3.4. 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 3.5. The integers a and b are relatively prime if their greatest common divisor is 1.

Definition 3.6. 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 $\text{lcm}(a, b)$.

Theorem 3.7. $\gcd(a, b) = p^{\min(a_1,b_1)} \cdot p^{\min(a_2,b_2)} \cdot \ldots \cdot p^{\min(a_n,b_n)}$ - so take the smallest common prime out of the prime decomposition of a and b and take the product.

Theorem 3.8. $\text{lcm}(a, b) = p^{\max(a_1,b_1)} \cdot p^{\max(a_2,b_2)} \cdot \ldots \cdot p^{\max(a_n,b_n)}$ - so take the greatest common primes out of the prime decomposition and take the product.