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 \( \text{gcd}(a, b) \), 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 \( \mathcal{P}(A) = \{B : B \subseteq A\} \).

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 \( A \setminus B = \{x : x \in A \text{ and } x \not\in B\} \).

The **complement** of sets \( A \) with universal set \( U \) is \( U \setminus A = \{x : x \in U \text{ and } x \not\in A\} \).

A natural number \( p \) is called **perfect** if \( p \) is equal to the sum of all its divisors less than \( p \).
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

BIG 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 \( a + b \) is even.

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

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 \( a, b \), \( \text{gcd}(a, b) \leq a \) and \( \text{gcd}(a, b) \leq b \).

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. 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 12. 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 13. If \( a, b \in \mathbb{N} \), then there exist integers \( k \) and \( \ell \) for which \( \text{gcd}(a, b) = ak + b\ell \).

Proposition 14. For \( a, b \in \mathbb{N} \) and \( k, \ell \in \mathbb{Z} \), if \( D = ak + b\ell \) then \( \text{gcd}(a, b) | D \).