4.4 Direct Proof and Counterexamples Part 4: Divisibility

Definitions and Notation
Let n and d be integers with $d \neq 0$. We say:

- d **divides** n, or $d|n$, if there exists an integer k such that $n = dk$.
- n is **divisible** by d.
- n is a **multiple** of d.
- d is a **divisor** of n.
- d is a **factor** of n.

Properties
Divisibility has several key properties:

- Reflexive property: $n|n$ for any integer n.
- Transitive property: If $a|b$ and $b|c$ then $a|c$.
- If $a|b$ and $b|a$ then $a = \pm b$.

Unique Factorization Theorem
Every integer $n > 1$ can be uniquely factored into primes $p_1^{a_1} \cdots p_k^{a_k}$ up to ordering of the primes. This is called the Fundamental Theorem of Arithmetic.

The standard convention is to order the primes in ascending order:

[$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$]

where $p_1 < p_2 < \cdots < p_k$. This is called the standard factored form.

Perfect Squares

If n is a perfect square, then it has a factorization into primes with all even exponents.

For example, if $n = 36 = 6^2$, then:

[$n = 2^2 \times 3^2$]

In general, if $n = k^2$, then the prime factorization of n will contain only even exponents. This property can be used to characterize and identify perfect squares.

4.5 Direct Proof and Counterexamples Part 5: Quotient-Remainder

Division and the Quotient Remainder Theorem

The quotient remainder theorem states that for integers n and d with $d > 0$, there exist unique integers q and r such that:

$[n = dq + r]$ where $0 \leq r < d$.

Here, q is the **quotient** and r is the **remainder**. This theorem formalizes division of integers into integer quotients and remainders.

Key points:

- The remainder r must satisfy $0 \leq r < d$.
- Ensures the remainder is less than the divisor d.
- Allows representing any integer as dividends, quotients, and remainders.

Computing Quotients and Remainders

Many programming languages provide integer division operators to compute quotients and remainders. For example, in Python:

- `n // d` computes the **quotient**
- `n % d` computes the **remainder**

Using the quotient remainder theorem, if $n = dq + r$, then:

$$n \div d = q$$
$$n \pmod{d} = r$$

Key points:

- Quotients and remainders can be computed.
- Be aware languages differ in handling negative remainders.
- Can compute div and mod manually using integer truncation.

The Triangle Inequality

The triangle inequality states:

$|x + y| \leq |x| + |y|$ Key points:

- Holds for absolute values of real numbers x and y.
- Called triangle inequality despite no triangles; origin of name.
- Fundamental inequality regarding absolute values.

4.6 Direct Proof and Counterexamples Part 6: Floor and Ceiling

Introduction to Floor and Ceiling Functions

The **floor** of a real number x, denoted $\lfloor x \rfloor$, is defined as the greatest integer less than or equal to x.

The **ceiling** of a real number x, denoted $\lceil x \rceil$, is defined as the least integer greater than or equal to x. Intuitively, $\lfloor x \rfloor$ rounds x down to the nearest integer, while $\lceil x \rceil$ rounds x up.

Properties of Floor and Ceiling for Integers

An important property:

If k is an integer, then $\lfloor k \rfloor = \lceil k \rceil = k$ In other words, the **floor** and **ceiling** of an integer are just the integer itself.

Relating Floor and Ceiling to the Quotient-Remainder Theorem

The floor and ceiling functions can be used to compute the quotient and remainder in the division algorithm:

Quotient-Remainder Theorem: Let n and d be integers with $d > 0$. Then there exist unique integers q and r such that: $n = dq + r$, where $0 \leq r < d$

To compute q and r:

Let $q = \lfloor \frac{n}{d} \rfloor$

Let $r = n - dq$

Then q and r satisfy the quotient-remainder theorem. This provides an efficient way to compute the quotient and remainder using just the **floor** function.