Proofs

- Methods of Proof
  - Divisibility
  - Floor and Ceiling
  - Contradiction & Contrapositive
  - Euclidean Algorithm

Reading (Epp's textbook)
4.3 – 4.8

Divisibility

- The notation **d** | **n** is read "*d* divides *n*." Symbolically, if *n* and *d* are integers and $d \neq 0$:

  $$d \mid n \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = dk.$$

- When "*d* divides *n*" we say that *d* is a **factor** of *n* and that *n* is a **multiple** of *d*.

- We write $d \nmid n$ when *d* does not divide *n*.

- For all integers *n* and *d*, $d \nmid n \Leftrightarrow \frac{n}{d}$ is not an integer.

Divisibility Theorems

For integers a, b, and c it is true that

- If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
  Example: 3 | 6 and 3 | 9, so 3 | 15.

- If $a \mid b$, then $a \mid bc$ for all integers c
  Example: 5 | 10, so 5 | 20, 5 | 30, 5 | 40, …

- If $a \mid b$ and $b \mid c$, then $a \mid c$ (Transitivity)
  Example: 4 | 8 and 8 | 24, so 4 | 24.

Primes and Divisibility

- A positive 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**.

- Any integer *n* > 1 is divisible by a prime number.

The fundamental theorem of arithmetic:

- Every positive integer can be written **uniquely** as a **product of primes** (*p*1*, p*2*, . . . , pk)*, and positive integers *e*1*, e*2*, . . . , ek* such that:

$$n = p1^{e1} p2^{e2} p3^{e3} \dots pk^{ek}$$

Fundamental Theorem of Arithmetic: Examples

- 75 = $3 \times 5 \times 5 = 3 \times 5^2$
- 100 = $2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$
- 15 = 3×5
- 33 = 3×11
- 12 = $2 \times 2 \times 3 = 2^2 \times 3$
- 28 = $2 \times 2 \times 7 = 2^2 \times 7$
- 512 = $2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^9$

Quotient – Remainder Theorem

- Given any integer *n* and positive integer *d*, there exist unique integers *q* and *r* such that:

$$n = dq + r \text{ and } 0 \leq r < d.$$

- In the above equation,
  - **d** is called the divisor,
  - **n** is called the dividend,
  - **q** is called the quotient, and
  - **r** is called the remainder.
- Note that the remainder cannot be negative!
- Examples where d = 5

  17 = 5 x 3 + 2. -13 = 5 x (-3) + 2.

div , mod and Parity property

- Symbolically, if n and d are integers and $d > 0$, then

$$\boldsymbol{n \text{ div } d = q \text{ and } n \bmod d = r \Leftrightarrow n = dq + r}$$

where q and r are integers and $0 \le r < d$.

- Thus $\boldsymbol{n = d \cdot (n \text{ div } d) + n \bmod d}$, and so

$$\boldsymbol{n \bmod d = n - d \cdot (n \text{ div } d).}$$

- By the quotient-remainder theorem (with $d = 2$), there exist unique integers q and r such that

$$n = 2q + r \text{ and } 0 \le r < 2.$$

$$n = 2q + 0 \textbf{ (even)} \text{ or } n = 2q + 1 \textbf{ (odd).}$$

- Any two consecutive integers have opposite parity.

Proof by Division into Cases

- To prove a statement of the form "If *A*1 or *A*2 or . . . or *An*, then *C*," prove all of the following:

  If *A*1, then *C*,

  If *A*2, then *C*,

  ...

  If *An*, then *C*.

  This process shows that *C* is true regardless of which of *A*1, *A*2, . . . , *An* happens to be the case.

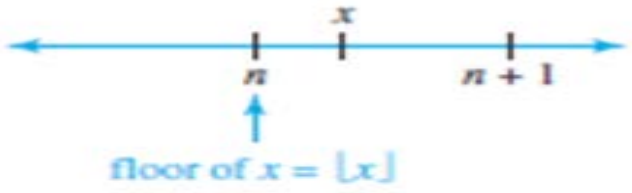
Floor and Ceiling

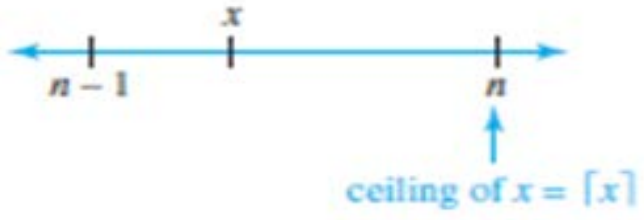
- Given any real number *x*, the **floor of *x*,** denoted $\lfloor x \rfloor$, is defined as follows:

  $\lfloor x \rfloor$ = that unique integer *n* such that $n \leq x < n + 1$.

- Given any real number *x*, the **ceiling of *x*,** denoted $\lceil x \rceil$, is defined as follows:

  $\lceil x \rceil$ = that unique integer *n* such that $n - 1 < x \leq n$.





Proving/Disproving a property of floor

Is the following statement true or false?

- $\forall\, x, y \in R,\ \lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$

Counterexample

Is the following statement true or false?

- $\forall\, x \in R\ and\ \forall\, m \in Z, \lfloor x + m \rfloor = \lfloor x \rfloor + m.$

Let n = $\lfloor x \rfloor$ and direct proof …

Proof by Contradiction

1. Suppose the statement to be proved is false.
   - ❖ That is, suppose that the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

Theorem

There is no integer that is both even and odd.

Proof by Contradiction: **1)** Suppose not. Assume that there is at least one integer *n* that is both even and odd.

2) By definition: $n = 2b + 1$ and $n = 2a$, for some integers *a* and *b*.

Then $2b + 1 = 2a \Leftrightarrow 1 = 2a - 2b \Leftrightarrow (a - b) = 1/2$. *(Contradiction?)*

3) The supposition is false and, hence, the theorem is true.

Proof by Contraposition

- Express the statement to be proved in the form

  $\forall x$ in D, if $P(x)$ then $Q(x)$.

- Rewrite this statement in the contrapositive form

  $\forall x$ in D, if $Q(x)$ is false then $P(x)$ is false.

- Prove the contrapositive by a direct proof.
  a. Suppose x is a (particular but arbitrarily chosen) element of D such that $Q(x)$ is false.
  b. Show that $P(x)$ is false.

Relation between Contradiction & Contraposition

- Express the statement to be proved in the form

  $\forall x$ in D, if $P(x)$ then $Q(x)$.

Suppose x is arbitrary element of D such that $\sim Q(x)$. → Sequence of steps → $\sim P(x)$

Proof by Contraposition

Suppose $\exists x$ in D such that $P(x)$ and $\sim Q(x)$. → Same sequence of steps → *Contradiction:* $P(x)$ and $\sim P(x)$

Proof by Contradiction

Example

- For all integers *n*, if n^2 is even then *n* is even.

Proof by Contraposition: Suppose *n* is any odd integer. By definition of odd

$n = 2k + 1$ for some integer k.

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

- But $2k^2 + 2k$ is an integer because products and sums of integers are integers.
- So n^2 = 2·(an integer) + 1, and thus, by definition of odd, n^2 is odd.

Proof by Contradiction: Suppose not. That is, suppose there is an integer *n* such that n^2 is even and *n* is not even. Hence, *n* is odd, and thus, by definition

$n = 2k + 1$ for some integer k. (Same sequence of steps)

Greatest Common Divisors

Let a and b be integers, not both zero.

- The largest integer d such that d | a and d | b is called the **greatest common divisor** of a and b.
- The greatest common divisor of a and b is denoted by gcd(a, b).

Example 1: What is gcd(48, 72) ?

- The positive common divisors of 48 and 72 are 1, 2, 3, 4, 6, 8, 12, 16, and 24, so gcd(48, 72) = 24.

Example 2: What is gcd(19, 72) ?

- The only positive common divisor of 19 and 72 is 1, so gcd(19, 72) = 1.

Greatest Common Divisors

Theorem of arithmetic:

$x = p_1^{a1} p_2^{a2} \ldots p_n^{an}$, $y = p_1^{b1} p_2^{b2} \ldots p_n^{bn}$,
where $p_1 < p_2 < \ldots < p_n$ are primes and $a_i, b_i \in \mathbf{N}$ for $1 \leq i \leq n$

- $\gcd(x, y) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)}$

Example:

$a = 60 = 2^2 3^1 5^1$

$b = 54 = 2^1 3^3 5^0$

$\gcd(a, b) = 2^1 3^1 5^0 = 6$

Least Common Multiples

The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b.

- We denote the least common multiple of a and b by lcm(a, b).

Examples:

lcm(3, 7) = 21

lcm(4, 6) = 12

lcm(5, 10) = 10

Least Common Multiples

Theorem of arithmetic:

$a = p_1^{a1} \; p_2^{a2} \ldots p_n^{an}$, $b = p_1^{b1} \; p_2^{b2} \ldots p_n^{bn}$,

where $p_1 < p_2 < \ldots < p_n$ are primes and $a_i, b_i \in \mathbf{N}$ for $1 \leq i \leq n$

- $\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} \; p_2^{\max(a_2, b_2)} \ldots p_n^{\max(a_n, b_n)}$

Example:

$a = 60 = 2^2 \; 3^1 \; 5^1$

$b = 54 = 2^1 \; 3^3 \; 5^0$

$\text{lcm}(a, b) = 2^2 \; 3^3 \; 5^1 = 4 \times 27 \times 5 = 540$

GCD and LCM

a = 60 = $2^2 3^1 5^1$

b = 54 = $2^1 3^3 5^0$

gcd(a, b) = $2^1 3^1 5^0 = 6$

lcm(a, b) = $2^2 3^3 5^1 = 540$

Theorem: a×b = gcd(a,b)×lcm(a,b)

The Euclidean Algorithm

Lemma:

If a and b are any integers not both zero, and if q and r are any integers such that $a = bq + r$, then

$$\gcd(a, b) = \gcd(b, r).$$

The **Euclidean Algorithm** finds the **greatest common divisor** of two integers a and b.

1. Let A and B be integers with $A > B \geq 0$.
2. Repeatedly apply the Lemma since the pair (B, r) is smaller than (A, B) until ***r = 0.***

The Euclidean Algorithm

For example, if we want to find gcd(287, 91), we **divide** 287 by 91:

- 287 = 91·3 + 14
- Apply the Lemma , gcd(287, 91) = gcd(91, 14).
- In the next step, we divide 91 by 14:
- 91 = 14·6 + 7
- This means that gcd(91,14) = gcd(14, 7).
- So we divide 14 by 7:
- 14 = 7·2 + 0
- We find that 7 | 14, and thus gcd(14, 7) = 7.

Therefore, gcd(287, 91) = 7.

The Euclidean Algorithm

In **pseu-docode**, the algorithm can be implemented as follows:

```
procedure gcd(a, b: positive integers)
  x := a
  y := b
  while y ≠ 0
  begin
        r := x mod y
        x := y
        y := r
  end {x is gcd(a, b)}
```