The Division Algorithm

If $a, b \in Z$, with $b > 0$, then there exist unique $q, r \in Z$ with $a = qb + r$, $0 \le r < b$.

- q is referred to as the quotient
- r the remainder
- b is the divisor
- a is the dividend

Examples

(a) When $a = 170$ and $b = 11$:

(b) When a = 98 and b = 7:

(c) When a = -45 and b = 8:

Section 4.4: The Greatest Common Divisor

Definition: For $a, b \in Z$, a position integer c is said to be a *common divisor* of a and b if $c|a$ and $c|b$.
E.g.

Definition: Let $a, b \in Z$, where either $a \neq 0$ or $b \neq 0$. Then $c \in Z^+$ is called a *greatest common divisor* of a, b if

(a) $c|a$ and $c|b$ (that is, c is a common divisor of a, b), and
(b) For any common divisor d of a and b, we have $d|c$

E.g.

Theorem

For all $a, b \in Z^+$, there exists a unique $c \in Z^+$ that is the greatest common divisor of a, b.

Proof:

Theorem Proof - cont'd…

Theorem Proof - cont'd…

Relatively Prime Numbers

Definition: Two integers a and b are *relatively prime* if gcd(a, b) = 1.

E.g.
Are 15 and 28 relatively prime?

Are 55 and 28 relatively prime?

Are 35 and 28 relatively prime?

Least Common Multiple

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).

E.g.

Section 4.5: The Fundamental Theorem of Arithmetic

Lemma 4.2: If $a, b \in Z^+$ and p is prime, then $p|ab \Rightarrow p|a$ or $p|b$.

Proof:

Another Lemma

Lemma 4.3: Let $a_i \in Z^+$ for all $1 \le i \le n$. If p is prime and $p|a_1 a_2 \cdots a_n$, then $p|a_i$ for some $1 \le i \le n$.

Proof:

Lemma Proof cont'd…

Example

Show that $\sqrt{2}$ is irrational.

Example - cont'd…

The Fundamental Theorem of Arithmetic

The *fundamental theorem of arithmetic*: Every positive integer can be written **uniquely** as the **product of primes**, where the prime factors are written in order of increasing size.

E.g.

Partial Proof of Fundamental Theorem of Arithmetic

Let's prove the existence of a prime factorization, and leave the uniqueness of it as a separate proof.

Partial Proof - cont'd…

Example

Suppose that n Z+ and that

$10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot n = 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14$

Show that $17|n$

Aside: Pi Notation

We've already seen sigma notation for summations, Pi-notation is the same type of notation for multiplications.

E.g.

$$\prod_{i=1}^{6} x_i =$$

$$\prod_{i=3}^{6} i =$$

$$\prod_{i=m}^{n} i =$$