cse581
Computer Science Fundamentals: Theory

Professor Anita Wasilewska

CM - Lecture 3

Chapter 4: Number Theory

PART 1: Divisibility

PART 2: Primes

PART 1: DIVISIBILITY

Basic Definitions

Definition

Given $m, n \in Z$, we say

m **divides** n or n **is divisible by** m if and only if $m \neq 0$ and n = mk, for some $k \in Z$

We write it symbolically

$$m \mid n \quad \text{if and only if} \quad n = mk, \quad \text{for some } k \in Z$$

Definition

If $m \mid n$, then m is called a **divisor** or a **factor** of n

We call n = mk a **decomposition** or a **factorization** of n

Basic Definitions

Definition

Let m be a **divisor** of n, i.e. n = mk

Cleary: $k \neq 0$ is also a **divisor** of n and is uniquely determined by m

Definition

Divisors of of n occur in **pairs** (m,k)

Definition

$n \in Z$ is a **square number** if and only if all its divisors of n are (m, m) i.e when $n = m^2$

Basic Facts

Fact 1

If (m, k) is a divisor of n so is $(-m, -k)$

Proof

$n = mk$, so $n = (-m)(-k) = mk$

Definition

$(-m, -k)$ is called an **associated divisor** to (m, k)

Fact 2

± 1 together with $\pm n$ are **trivial divisors** of n

Proof Each number n has an obvious decomposition (1, n), (-1, -n) as $n = 1n = (-1)(-n)$

Basic Facts

Fact 3

If m|n and n|m, then m, n are **associated**, i.e $m = \pm n$

Proof

Assume m|n i.e. $n = mk_1$, also n|m i.e. $m = nk_2$, for $k_1, k_2 \in Z$

So $n = nk_1k_2$ iff $k_1 = k_2 = 1$ and $m = n$

or $k_1 = k_2 = -1$, and $m = -n$

Fact 4

If $m \mid n_1$ and $m \mid n_2$ then $m \mid (n_1 \pm n_2)$

Proof

Assume $m \mid n_1$ i.e. $n_1 = mk_1$, and $m \mid n_2$ i.e. $n_2 = mk_2$

Hence $n_1 \pm n_2 = m(k_1 \pm k_2)$ i.e. $m \mid (n_1 \pm n_2)$

Basic Facts

Fact 5

If $m \mid n$ and $n \mid k$ then $m \mid k$

Proof

$m \mid n$ iff $n = mk_1$ and $n \mid k$ iff $k = nk_2$

Hence $k = mk_1 k_2$ iff $m \mid k$

In most questions regarding **divisors** we assume that $m > 0$ and only consider **positive divisors** (m, k)

We look first at **positive factorizations** and then we work out others

Book Definition

The Book Definition

For $n, m, k \in Z$

$$m \mid n \quad \text{if and only if} \quad m > 0 \quad \text{and} \quad n = mk$$

It means the **The Book** considers only **positive divisors** $(m, k),\ m > 0,\ k \in Z$

Definition

All positive divisors, including 1 , that are less than n are called **proper divisors** of n

Basic Facts

Fact 6

If (m,k) is a divisor of n then the factors m,k can't be both $> \sqrt{n}$

Proof

Assume that for both factors $m > \sqrt{n}$ and $k > \sqrt{n}$, then $mk > \sqrt{n}\sqrt{n} = n$;

we got a **contradiction** with $n = mk$

Fact 6 Rewrite

If (m, k) is a divisor of n, then $m \leq \sqrt{n}$ or $k \leq \sqrt{n}$

Example

Problem

Find all divisors of $n = 60$

By the **Fact 6** the number of divisors of $m \leq \sqrt{n} = \sqrt{60}$ i.e.

$$m \leq \sqrt{60} < \sqrt{64} = 8$$

Hence $m < 8$, m = 1, 2, 3, 4, 5, 6, 7

and we have six pairs of divisors

$$(1, 60) \quad (3, 20) \quad (5, 12)$$

$$(2, 30) \quad (4, 15) \quad (6, 10)$$

Division and Remainders

Let $b \neq 0$ and $b \in Z$

Then any $a \in Z$ is either a multiple of b or alls between two consecutive multiples $q\,b$ and $(q+1)b$ of b

We write it:

$$a = q\,b + r \qquad q \in Z \qquad r = 0, 1, 2, ..., |b| - 1$$

r is called the least positive remainder or simply the **remainder** of a by division with b

$$0 \leq r < |b|$$

q is the incomplete quotient or simply the **quotient**

Division and Remainders

Note

Given $a, b \in Z,\ b \neq 0$ the quotient q and the remainder r are uniquely determined and each integer $a \in Z$ can be written as:

$$a = q\,b + r \qquad 0 \leq r < |b|$$

Example

$321 = 4 \cdot 74 + 25 \qquad q = 4, \quad b = 74, \quad r = 25$

$46 = (-2)(-17) + 12 \qquad q = -2, \quad b = -17, \quad r = 12$

In particular any $n \in N$, n=2q (even) or $n = 2q + 1$ (odd)

Division and Remainders

Theorem

The square of $n \in Z$ is either divisible by 4, or leaves the remainder 1 when divided by 4

Proof

Case 1: $n = 2q, \ n^2 = (2q)^2 = 4q^2$

Case2: $n = 2q + 1, \ n^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$

Division and Remainders

Let $b \neq 0$; $a, b, q \in Z$

$$a = qb + r \qquad 0 \leq r < |b|$$

We re-write is as

$$\frac{a}{b} = q + \frac{r}{b} \qquad 0 \leq \frac{r}{b} < 1$$

Fact q is the greatest integer such that $q \leq \frac{a}{b}$

Division and Remainders

Special Notation

Old notation

$[q]$ = greatest integer such that it is less or equal $\frac{a}{b}$

Modern notation

$\lfloor \frac{a}{b} \rfloor$ = greatest integer such that it is less or equal $\frac{a}{b}$

Modern notation comes from K.E. Iverson, 1960

Division and Remainders

Book, page 67

FLOOR: $\lfloor x \rfloor$ = the greater integer q, $q \leq x$

CEILING: $\lceil x \rceil$ = the least integer q, $q \geq x$

$q = \lfloor \frac{a}{b} \rfloor$ = the greatest integer q, $q \leq \frac{a}{b}$ is also called the greatest integer **contained** in $\frac{a}{b}$

Example

$$\left\lfloor \frac{25}{5} \right\rfloor = 5, \quad \left\lfloor \frac{5}{3} \right\rfloor = 1, \quad \lfloor 2 \rfloor = 2, \quad \left\lfloor \frac{-1}{3} \right\rfloor = -1, \quad \left\lfloor \frac{1}{3} \right\rfloor = 0$$

Division and Remainders

We **extent** notation to Real numbers

$$x, y, q \in R \qquad x = \lfloor x \rfloor + y, \qquad 0 \leq y < 1$$

Example

$$\lfloor \pi \rfloor = 3, \quad \lfloor e \rfloor = 2, \quad \lfloor \pi^2/2 \rfloor = 4$$

Number Systems

Given $a, b \in N$, we **represent** a **on base** b as

$$a = a_n b^n + a_{n-1} b^{n-1} + \ \ldots \ + a_1 b^1 + a_0 \text{ for } a_i \in \{0, 1, \ldots, b-1\}$$

We write it as

$$\mathbf{a} = (\mathbf{a_n},\ \mathbf{a_{n-1}}, \ldots, \mathbf{a_1}, \mathbf{a_0})$$

Questions

1. How to find the representation of a on base b?
2. How to pass from one base to the other?

This we did show already in Chapter 1, CM Lecture 2

Number Systems

Consider

$$a = a_n b^n + a_{n-1} b^{n-1} + ... + a_1 b^1 + a_0$$

Observation 1

a_0 is the remainder of a by division by b as

$$a = b\,(a_n b^{n-1} + ... + a_1 b^0) + a_0$$

So we have

$$a = q_1 b + a_0 \quad \text{where} \quad q_1 = a_n b^{n-1} + ... + a_2 b + a_1$$

Number Systems

Consider now

$$q_1 = b(a_n b^{n-2} + ... + a_2) + a_1$$

Observation 2

a_1 is the remainder of q_1 by division by b and

$$q_1 = bq_2 + a_1 \quad \text{for} \quad q_2 = a_n b^{n-2} + ... + a_3 b + a_2$$

Repeat

a_i is the remainder of q_i by division by b, for $i = 1, \ldots, n-1$

to find all $a_1, a_2, \ldots, a_n$

Examples

Example

Represent 1749 in a system with base 7

$$1749 = 249 \cdot 7 + 6$$

$$249 = 35 \cdot 7 + 4$$

$$35 = 5 \cdot 7 + 0$$

$$a_0 = 6, \quad a_1 = 4, \quad a_2 = 0, \quad a_3 = 5$$

So we get

$$1749 = (5, 0, 4, 6)_7$$

Examples

Example

Represent 19151 in a system with base 12

$$19151 = 1595 \cdot 12 + 11$$

$$1595 = 132 \cdot 12 + 11$$

$$132 = 11 \cdot 12 + 0$$

$$a_0 = 11, \quad a_1 = 11, \quad a_2 = 0, \quad a_3 = 11$$

So we get

$$19151 = (11, 0, 11, 11)_{12}$$

Number Systems

We evaluated the components

$$a_0, a_1, \ldots, a_n$$

from the lowest a_0 **upward** to a_n

Now let's evaluate $a_0, \ldots, a_n$ **downward** from a_n to a_0

In this case we have to determine the **highest power** of b such that b^n is **less than** a, while the next power b^{n+1} **exceeds** a

Number Systems

We look for **division** of a by b^n and

$$a = a_n b^n + r_{n-1}$$

$$r_{n-1} = a_{n-1} b^{-1} + \ \ldots \ + a_0$$

We determine a_{n-1} from r_{n-1}

$$r_{n-1} = a_{n-1} b^{n-1} + r_{n-2}$$

$$r_{n-2} = a_{n-2} b^{n-2} + \ \ldots \ + a_0$$

We determine a_{n-2} from r_{n-2}

$$r_{n-2} = a_{n-2}\, b^{n-2} + r_{n-3} \qquad \text{and etc } \ldots$$

Example

Represent 1832 to the base 7

First calculate powers of 7

$$7^1 = 7 \quad 7^2 = 49 \quad 7^3 = 343 \quad 7^4 = 2401$$

and then calculate

$$a = a_n b^n + r_{n-1} \quad \text{for} \quad n = 3$$

$$1832 = 5 \cdot 7^3 + 117 \qquad a_3 = 5$$

$$117 = 2 \cdot 7^2 + 19 \qquad a_2 = 2$$

$$19 = 2 \cdot 7 + 5 \qquad a_1 = 2, \; a_0 = 5$$

We obtained

$$1832 = (5, 2, 2, 5)_7$$

Common and Greatest Common Divisor

Definition (Common Divisor)

Let $a, b, c \in Z$

If c divides a and b simultaneously, then c is called a common divisor a and b.

Definition (Greatest Common Divisor)

Let $a, b \in Z$, not both zero, then $d \in Z$ is called the **greatest common divisor** of a and b if and only if

1. $d > 0$

2. d is a **common divisor** of a and b, and

3. each $c \in Z$ that is a common divisor of both and a and b, is a **divisor** of d

We denote the greatest common divisor (g.c.d.) of a and b by

$$gcd(a, b)$$

Proving that d = gcd(a, b)

Let $a, b \in Z$, not both zero. Since there is only question of divisibility, there is no limitation in assuming that

$a, b \in Z^+$, and $a \geq b$.

Let A be a set of **all common divisors** of a and b i.e.

$A = \{c \in Z^+ \quad c \mid a \text{ and } c \mid b\}$. We know that the divisibility $\mid$ is and order relation on Z, so we consider a poset $(A, \preceq)$, such that for for any $x, y \in A$, $x \preceq y$ if and only if $x \mid y$.

In order to **prove** that $d \in Z^+$, $d > 0$ is a the greatest common divisor of a and b, we have to **show** that

1. $d \in A$, and

2. d is the greatest element in the poset $(A, \preceq)$, i.e.

for **all** $c \in A$, $c \preceq d$.

Relatively Prime Numbers

Remark

Every number has the divisor 1, so $gcd(a, b)$ is a positive integer, i.e. $gcd(a, b) \in Z^+$

Definition

$a, b \in Z$ are **relatively prime** if and only if

$$gcd(a, b) = 1$$

Book notation

$a \perp b$ for $a, b \in Z$ **relatively prime**

Example

gcd(24, 56) = 8, $24 \not\perp 56$ and gcd(15, 21) =1, $15 \perp 22$

Euclid Algorithm

A procedure of finding the **greatest common divisor** of two positive natural numbers is known as Euclid Algorithm

The original version called Euclid Algorism comes from seventh book of Euclid's Elements (about 300 BC); however it is certainly of earlier origin

Since there is only question of **divisibility**, there is no limitation in assuming that a, b are non zero and positive and a is greater or equal b, i.e. $a, b \in N^{+}$ and $a \geq b$

Euclid Algorithm

1. We divide a by b with respect to the least positive remainder

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

2. We divide *b by* r_1 with respect to the least positive remainder

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

3. We divide r_1 *by* r_2 with respect to the least positive remainder

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

4. We divide r_2 *by* r_3 with respect to the least positive remainder

$$r_2 = q_4 r_3 + r_4 \qquad 0 \leq r_4 < r_3$$

We continue the process

Euclid Algorithm

Observe that such obtained remainders

$$r_1, \quad r_2, \quad r_3, \quad \dots r_n,$$

form a decreasing sequence of positive integers

$$r_1 > r_2 > r_3 > \dots r_n > \ \dots$$

and one must arrive on a division for which $r_{n+1} = 0$, i.e. the Euclid algorithm process:
divide a by b, divide b by r_1, ... divide r_k by r_{k+1}
must **terminate**

Euclid Algorithm

Algorithm

$$
\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
r_2 &= q_4 r_3 + r_4 \\
r_3 &= q_5 r_4 + r_5 \\
&\dots \quad \dots \quad \dots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}
$$

We have to **prove**

$$r_n = gcd(a, b)$$

Euclid Algorithm Example

Example

Find $gcd(76084\ ,\ 63,020)$

$$76,084 = 63,020 \cdot 1 + 13,064 \qquad q_1 = 1, \quad r_1 = 13,064$$

$$63,020 = 13,064 \cdot 4 + 10,764 \qquad q_2 = 4, \quad r_2 = 10,764$$

$$13,064 = 10,764 \cdot 1 + 2,300 \qquad q_3 = 1, \quad r_3 = 2,300$$

$$10,764 = 2,300 \cdot 4 + 1,564 \qquad q_4 = 5, \quad r_4 = 1,564$$

$$2,300 = 1,564 \cdot 1 + 736 \qquad q_5 = 1, \quad r_5 = 736$$

$$1,564 = 736 \cdot 2 + 92 \qquad q_6 = 2, \quad r_6 = 92$$

$$736 = 92 \cdot 8 + 0 \qquad q_7 = 8, \quad r_7 = 0 \quad \textbf{end}$$

$$gcd(76084\ ,\ 63020) = (76084\ ,\ 63020) = r_6 = 92$$

Euclid Algorithm Correctness Proof

Euclid Algorithm Correctness Theorem

For any $a, b \in N^{+}$ and $a \geq b$, and the Euclid Algorithm applied to a, b, the **last non-vanishing** remainder r_n is the **greatest common divisor** of a and b, i.e the following implication holds

$$\text{IF} \quad r_{n+1} = 0 \quad \text{THEN} \quad r_n = gcd(a, b)$$

Proof Let A be set of **all common divisors** of a and b, i.e.

$$A = \{c \in Z^{+} \quad c \mid a \ \text{ and } \ c \mid b\}$$

We know that the divisibility $\mid$ on Z is an **order relation** and we consider a **poset** $(A, \mid)$.

Euclid Algorithm Correctness Proof

In order to **prove** that $r_n > 0$ is the greatest common divisor of a and b we have to **show** that

1. $r_n \in A$, and

2. $r_n > 0$ is the **greatest element** in the poset $(A, |)$, i.e. we prove that for **all** $c \in A, \ c \mid r_n$.

This means that we have to carry the proof in two steps.

Step 1 We show that the last non-vanishing remainder r_n is a **common divisor** of a and b

Step 2 We show that the r_n is the **greatest element** in the poset $(A, |)$

Euclid Algorithm Correctness Proof

We conduct the proof of the Step 1 and Step 2 by **double induction**, what is a **Mathematical Induction** with two BASIC CASES.

Step 1 We show that the last non-vanishing remainder r_n is a **common divisor** of a and b, i.e. we show that

$$r_n \mid a \quad \text{and} \quad r_n \mid b$$

Assume that r_n is the last non-vanishing remainder, i.e. $r_{n-1} = q_{n+1} r_n$ and hence

$$\textbf{1.} \quad r_n \mid r_{n-1}$$

Observe that

$$r_{n-2} = q_n r_{n-1} + r_n = q_n q_{n+1} r_n + r_n = r_n(q_n q_{n+1} + 1)$$

Hence

$$\textbf{2.} \quad r_n \mid r_{n-2}$$

Euclid Algorithm Correctness Proof

Observe that

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \quad \text{and} \quad r_n \mid r_{n-1}, \quad r_n \mid r_{n-2}$$

Hence

$$r_n \mid r_{n-3}$$

Observe that

$$r_{n-4} = q_{n-2} r_{n-3} + r_{n-2} \quad \text{and we proved that} \quad r_n \mid r_{n-3}, \quad r_n \mid r_{n-3}$$

Hence

$$r_n \mid r_{n-4}$$

We carry our **proof** by **double induction**, i.e. **Mathematical Induction** with

1. $r_n \mid r_{n-1}$, **2.** $r_n \mid r_{n-2}$ as **base cases**

Euclid Algorithm Correctness Proof

We want to prove that the continuation of this process, i.e. we want to prove that

$$r_n \mid r_{n-k} \quad \text{for all} \quad k \geq 1$$

To do so we need to develop a **general formula** for r_{n-k} of which $r_{n-1}, r_{n-2}, r_{n-3}, r_{n-4}$ are **particular cases**

This is the **key step** of the proof

The rest is just application of the **Mathematical Induction** to the general formula below

$$\mathbf{r_{n-k} = q_{n-(k-2)} r_{n-(k-1)} + r_{n-(k-2)}} \quad \text{for} \quad k \geq 1$$

Euclid Algorithm Correctness Proof

We carry our **proof** by **Mathematical Induction** on $k \geq 1$ with **1.** for $k = 1$ and **2.** for $k = 1$ as **base cases** already proved to be true

Inductive assumption

$$r_n \mid r_p \quad \text{for all} \quad p < k$$

Induction Step We **prove** from the Inductive assumption that

$$r_n \mid r_{n-k}$$

and by the Mathematical Induction Principle we get the **Induction Thesis**

$$r_n \mid r_{n-k} \quad \text{for all} \quad k \geq 1$$

In particular case when $k = n - 1$ and $k = n - 2$ we get

$$r_n \mid r_1 \quad \text{and} \quad r_n \mid r_2$$

Euclid Algorithm Correctness Proof

We have that

$$b = q_2 r_1 + r_2$$

and we just got

$$r_n \mid r_1 \quad \text{and} \quad r_n \mid r_2$$

Hence

$$r_n \mid b$$

We also have that

$$a = q_1 b + r_1$$

and we just got

$$r_n \mid r_1 \quad \text{and} \quad r_n \mid b$$

Hence

$$r_n \mid a$$

This **proves** that r_n is a **common divisor** of a and b

Euclid Algorithm Correctness Proof

In order to **complete** the proof of the **Step 1** we have to do the **Proof** of the **Induction Step**

$$r_n \mid r_{n-k}$$

Consider the general formula for r_{n-k}

$$\mathbf{r_{n-k} = q_{n-(k-2)} r_{n-(k-1)} + r_{n-(k-2)}} \quad \text{for} \quad k \geq 1$$

Observe that

$$k - 2 = p < k \quad \text{and} \quad k - 1 = p < k$$

Hence by the **Inductive assumption**

$$r_n \mid r_{n-(k-1)} \quad \text{and} \quad r_{n-(k-2)}$$

we get that

$$r_n \mid r_{n-k}$$

This **ends** the proof of the **Step 1**

Euclid Algorithm Correctness Proof

Step 2 We show that the r_n is the **greatest** common divisor of a and b. Let the set A be a set of **all** common divisors of a and b, i.e.

$$A = \{c \in Z^+ : \ c \mid a \text{ and } c \mid b\}$$

We know that | is an **order relation** on Z and we now consider a **poset** $(A, \mid)$. We have to show that r_n is the **greatest element** in it, i.e. we have to **prove** that the following

$$c \mid r_n, \text{ for all } c \in A$$

Euclid Algorithm Correctness Proof

We carry the proof, as in previous step, by the **Double Induction**. We have

$$a = q_1 b + r_1 \quad \text{and} \quad r_1 = a - q_1 b$$

so **for all** $c \in A$, $c \mid a$ and $c \mid b$, hence

1. $c \mid r_1$, for all $c \in A$

Similarly

$$b = q_2 r_1 + r_2 \quad \text{and} \quad r_2 = b - q_2 r_1$$

and $c \mid b$ and $c \mid r_1$, hence

2. $c \mid r_2$, for all $c \in A$

This is the **Base Case**

Euclid Algorithm Correctness Proof

We carry the Double Induction **inductive step** similarly to **Step 1** and we get

$$c \mid r_k, \text{ for all } c \in A, \quad \text{for all} \quad k \geq 1$$

In particular it holds for k = n and we get that

$$c \mid r_n, \text{ for all } c \in A$$

This **ends the proof** of the **correctness** of Euclid Algorithm

Faster Algorithm

Kronecker (1823 - 1891) proved that no Euclid Algorism can be shorter then one obtained by **least absolute remainders** - r_n can be negative

Example Find $gcd(76084\ ,\ 63020)$ by the least absolute remainders

$$76,084 = 63,020 \cdot 1 + 13,064$$

$$63,020 = 13,064 \cdot 5 - 2,300$$

$$13,064 = 2,300 \cdot 6 - 736$$

$$2,300 = 736 \cdot 2 + 92$$

$$736 = 92 \cdot 8$$

$$gcd(76084\ ,\ 63020) = 92$$

We did it in 5 steps instead of 7 steps

"mod" Binary Operation

Definition

For any $x, y \in R$ we define a binary relation $mod \subseteq R \times R$ as

$$x \ mod \ y = x - y \left\lfloor \frac{x}{y} \right\rfloor \quad \text{for} \quad y \neq 0$$

and

$$x \ mod \ 0 = x$$

Example

$$5 \ mod \ 3 = 5 - 3 \left\lfloor \frac{5}{3} \right\rfloor = 5 - 3 \cdot 1 = 2$$

$$5 \ mod \ (-3) = 5 - (-3) \left\lfloor \frac{5}{-3} \right\rfloor = 5 - (-3) \cdot (-1) = -1$$

”mod” Binary Operation

Observe that when $a, b \in Z,\ b \neq 0$ we get

$$a = b \left\lfloor \frac{a}{b} \right\rfloor + a\ mod\ b$$

and

$$a = b\ q + r \quad \text{for} \quad q = \left\lfloor \frac{a}{b} \right\rfloor, \quad r = a\ mod\ b$$

Fact

For any $a, b \in Z,\ b \neq 0$,
$a\ mod\ b$ is a **remainder** in the division of a by b

Example

We evaluated $r_1 = 5\ mod\ 3 = 2$, $r_2 = 5 mod\ (-3) = -1$
and we have

$$5 = 3 \cdot 1 + 2 \quad \text{and} \quad 5 = (-3)(-1) - 1$$

"mod" Euclid Algorithm

We use the the mod relation to formulate a more modern version of Euclid Algorithm

We define a recursive function f for any $m, n \in Z, \ \ 0 \leq m < n$ we put

$$f(m,n) = f(n \ mod \ m, \ \ m) \quad \text{for} \quad m > 0$$

$$f(0,n) = n \quad \text{for} \quad m = 0$$

Theorem

For any $a, b \in Z, \ \ 0 \leq a < b$

If the function $f = f(m,n)$ applied recursively to a, b as the initial values terminates at $f(0,k)$, **then**

$$gcd(a,b) = f(0,k)$$

Proof Book pages 103, 103 - but this is just a translation of our proven theorem!

Examples

Example 6

$$f(m,n) = f(n \; mod \; m, \; m) \text{ for } m > 0, \qquad f(0,n) = n$$

$$f(12,18) = f(6,12) = f(0,6) = 6 \qquad gcd(12,18) = f(0,6) = 6$$

Example 2

$$f(63020\ ,\ 76084) = f(13064\ ,\ 63020) = f(10764\ ,\ 13064)$$

$$= f(2300\ ,\ 107640) = f(1564\ ,\ 2300) = f(736\ ,\ 1564)$$

$$f(92\ ,\ 736) = f(0\ ,\ 92)$$

$$gcd(63020\ ,\ 76084) = f(0\ ,\ 92) = 92$$

Some Consequences of Euclid Algorithm

Definition

$m, n \in N - \{0, 1\}$ are **relatively prime** if and only if $gcd(m, n) = 1$

Notation $n \perp m$ for m, n **relatively prime**

We now use Euclid Algorithm to derive other properties of the gcd. The most important one is the following

Division Lemma

When a product ac of two natural numbers is divisible by a number b that is **relatively prime** to a, the factor c must be divisible by b

Some Consequences of Euclid Algorithm

Division Lemma written symbolically

$$\text{If } b \mid ac \text{ and } a \perp b \text{ then } b \mid c$$

Proof

Since $a \perp b$, i.e. $gcd(m, n) = 1$, hence the last non zero remainder r_n in the Euclid Algorithm must be 1, so E A has a form

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$\dots \quad \dots$$

$$r_{n-2} = q_n r_{n-1} + 1$$

$$r_{n-1} = q_{n+1} r_n + 0$$

Some Consequences of Euclid Algorithm

Multiply by c

$$ac = q_1 bc + r_1 c$$

$$bc = q_2 r_1 c + r_2 c$$

$$\cdots \quad \cdots$$

$$r_{n-2}c = q_n r_{n-1} c + c$$

$$r_{n-1} = q_{n+1} r_n + 0$$

and $b \mid ac$, so $b \mid r_1 c$, and hence $b \mid r_2 c$

By Mathematical Induction we get

$$\forall i \geq 1(b \mid r_i)$$

In particular $b \mid r_{n-2}c$, and hence $b \mid c$

It **ends the proof**

Some Consequences of Euclid Algorithm

Theorem 1

When a number is relatively prime to each of several numbers, it is relatively prime to their product

Symbolically

$$\text{If} \quad a \perp b_i, \quad \text{for} \quad i = 1, 2, \ldots k, \quad \text{then} \quad a \perp b_1 b_2 \ldots b_k$$

Proof By contradiction; we show case $i = 2$ and the rest is carried by Mathematical Induction

Assume $a \perp b$ and $a \perp c$, and $a \not\perp bc$

By definition we have hence that $gcd(a, bc) \neq 1$, i.e. a has a common divisor d with bc, i.e. there is d such that

$$d \mid a \quad \text{and} \quad d \mid bc$$

Some Consequences of Euclid Algorithm

We have that there is d such that

$$d \mid a \quad \text{and} \quad d \mid bc$$

and

$a \perp b$, and $d \mid a$, hence we get $d \perp b$

We also have

$a \perp c$, and $d \mid a$, hence we get $d \perp c$

So from $d \mid bc$ and $d \perp b$ we get by the **Division Lemma** that $d \mid c$ what is **contrary** to $d \perp c$

Exercise Write the full proof by Mathematical Induction

Some Consequences of Euclid Algorithm

Theorem 2

$$gcd(ka, kb) = k \cdot gcd(a, b)$$

Proof

$gcd(a, b) = r_n$ in the Euclid Algorithm

$$a = q_1 b + r_1$$

$$\dots \qquad \dots$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} r_n + 0$$

We multiply each step by k

Some Consequences of Euclid Algorithm

We multiply each step by k

$$ka = kq_1 b + kr_1$$

$$\dots \qquad \dots$$

$$kr_{n-2} = kq_n r_{n-1} + kr_n$$

$$kr_{n-1} = q_{n+1} kr_n + 0$$

This is the Euclid Algorithm for $ka, \; kb$ and

$$gcd(ka, kb) = k \cdot r_n = k \cdot gcd(a, b)$$

Some Consequences of Euclid Algorithm

Theorem 3

Let $d = gcd(a, b)$ be such that

$$a = a_1 d \quad \text{and} \quad b = b_1 d$$

Then

$$a_1 \perp b_1$$

Proof

Evaluate using **Theorem 2**

$$gcd(a\ ,\ b) = gcd(a_1 d\ ,\ b_1 d)$$

$$= d \cdot gcd(a_1\ ,\ b_1) = gcd(a, b) gcd(a_1\ ,\ b_1)$$

So we get $gcd(a_1\ ,\ b_1) = 1$, as nk=k iff k=1

This means

$$a_1 \perp b_1$$

Some Consequences of Euclid Algorithm

The **Theorem 3** applies in elementary arithmetic in the reduction of fractions

Take any fraction and $a = a_1 d, \;\; b = b_1 d$

$$\frac{a}{b} = \frac{a_1 d}{b_1 d} = \frac{a_1}{b_1}$$

for

$$a_1 \perp b_1$$

I.e any fraction can be represented in **reduced form** with numerator and denominator that are relatively prime

Least Common Multiple

A number m is said to be a common multiple of the numbers a and b when it is divisible by both of them

For example, the product ab is a common multiple of a and b

Since, as before there is only question of divisibility, there is no limitation in considering only positive multiples

Definition Common Multiple

Let $a, b, m \in Z$

m= cm(a , b) is a common multiple of a and b iff

$a \mid m$ and $b \mid m$ and $m > 0$

Least Common Multiple

Let $A = \{m : \quad a \mid m \text{ and } b \mid m\}$ be the set of **all common multiples** of a and b

This **least** element is called a **least common multiple** (l.c.m.) of a and b and denoted by $lcm(a, b)$

Remark The **least** element in the poset $(A, \leq)$ is its unique minimal element so it justifies the BOOK definition

$$lcm(a, b) = min\{m : \quad m > 0 \text{ and } a \mid m \text{ and } b \mid m\}$$

Least Common Multiple

Theorem 4

Any common multiple of a and b is **divisible** by lcm(a,b)

Proof

Let m = cm(a,b)

We divide m by lcm(a,b), i.e

$$m = q lcm(a, b) + r \qquad 0 \leq r < lcm(a, b)$$

But $a \mid lcm(a, b)$ and $b \mid lcm(a, b)$ and $a \mid m$ and $b \mid m$

Hence $a \mid r$ and $b \mid r$ and r is a common multiple of a, b

But $0 \leq r < lcm(a, b)$, so r=0 what proves that
$m = q \cdot lcm(a, b)$, i.e. m is **divisible** by lcm(a,b)

Least Common Multiple

Theorem 5

For any $a, b \in Z^+$ such that lcm(a,b) and gcd(a, b) exist

$$lcm(a, b) \cdot gcd(a, b) = ab$$

Theorem 6

$$lcm(a, b) = ab \quad \text{if and only if} \quad a \perp b$$

Exercise Prove both Theorems

PART 2: PRIME NUMBERS

Definition

Definition

A positive integer is called **prime** if it has only two divisors 1 and itself

We assume **convention** that 1 is not prime

We denote by P the **set of all primes**

Symbolically

$$p \in P \subseteq N \quad \text{if and only if} \quad p > 1 \text{ and for any } k \in Z$$

$$\text{if } \; k|p \; \text{ then } \; k = 1 \; \text{ or } \; k = p$$

Some primes

$$2,\ 3,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19, 23,\ 29,\ 31,\ 37,\ \ldots$$

Primes

Observe 2 is the only even prime!

Question Is 91 prime? No, it isn't as $91 = 7 \cdot 13$

Definition

$n \in N,\ n > 1$ is called **composite** and denoted by CN, if it is **not prime**

Symbolically

$$n \in CN \quad \text{if and only if} \quad n \leq 1 \cup \exists_{k \in Z}(k|n \ \cap\ k \neq 1 \cap k \neq n)$$

Directly from the definition we have that

Fact 1

$$\forall_{m \in N-\{0,1\}}(\ m \in P\ \cup\ m \in CN) \quad \text{and} \quad P \cap CN = \emptyset$$

Primes

Definition

$m, n \in N$ are **relatively prime** if and only if $gcd(m, n) = 1$

Notation $n \perp m$ for $m, n \in N$ relatively prime

Fact 2

$$\forall_{p \in P} \forall_{n \in N} (p \perp n \cup p | n)$$

Fact 3

A product of two numbers is divisible by a prime p only when p **divides** at least one of the factors

Symbolically

$$\forall_{p \in P} \forall_{m,n \in Z} (p \mid mn \Rightarrow (p \mid m \cup p \mid n))$$

Proof

Assume that **Fact 3** is not true, i.e.

$$\exists_{p \in P} \exists_{m,n \in Z} \ (p \mid mn \ \cap \ p \nmid m \ \cap p \ \nmid n \ )$$

$p \nmid m$ so by **Fact 2** $p \perp m$. Now when $p \mid mn$ and $p \perp m$ we get by **Fact 2** that $p \mid n$. We get a contradiction with $p \nmid n$

Observation

For any $p \in P, \ m, n \in Z$,

if p divides m or p divides m, then p divides mn

Proof Assume $p \mid m$, i.e. $m = kp$ for $k \in Z$. Hence $mn = kmp$ and $p \mid mn$. The case $p \mid m$ is similar

Primes

Because of the obvious character of the **Observation** we usually formulate and prove the **Fact 3** in the following more general form

Fact 3a

A product of two numbers is divisible by a prime p if and only if p **divides** at least one of the factors

Symbolically

$$\forall_{p \in P} \forall_{m,n \in Z} \ (p \mid mn \ \Leftrightarrow \ (p \mid m \cup p \mid n))$$

Fact 4

A product $q_1 q_2 \dots q_n$ of prime numbers (factors) q_i is **divisible** by a prime p only when $p = q_i$ for some q_i

Symbolically

$$\forall_{p, q_1 q_2 \dots q_n \in P} \left(p \mid \prod_{k=1}^{n} q_k \Rightarrow \exists_{1 \leq i \leq n} (p = q_i)\right)$$

Proof

Let $p \mid \prod_{k=1}^{n} q_k$. By the **Fact 3** $p \mid q_i$ for some g_i where $q_i \in P$; but $p > 1$ as $1 \notin P$ hence $p = q_i$

Primes

Fact 5

Every natural number n, $n > 1$ is **divisible** by some prime

Symbolically

$$\forall_{n \in N, n>1} \exists_{p \in P} \, (p \mid n)$$

Proof

When $n \in P$, this is evident as $n \mid n$

When n is composite it can be factored $n = n_1 n_2$

where $n_1 > 1$

The smallest possible one of these divisors of n_1 must be prime

Main Factorization Theorem

We are now ready to prove the main theorem about factorization. The idea of this theorem, as well as all **Facts 1-5** we will use in proving it, can be found in **Euclid's** Elements in **Book VII** and **Book IX**

Main Factorization Theorem

Every composite number can be **factored uniquely** into prime factors

Main Factorization Theorem

We present here an ”old” and pretty straightforward proof

You have another proof in the Book pages 105-105 and all this without saying that it is a Theorem, and a quite important one

Proof We conduct it in two steps

Step 1 We show that every composite number $n > 1$ is product of prime numbers

Step 2 We show the uniqueness

Main Factorization Theorem

Step 1 We show that every composite number $n > 1$ is product of prime numbers

By **Fact 5** there is $p_1 \in P$ such that $n = p_1 n_1$

If n_1 is composite, then by **Fact 5** again, $n_1 = p_2 n_2$

We continue this process with a decreasing sequence

$$n_1 > n_2 > n_3 > \ \ldots$$

of numbers together with a corresponding sequence of prime numbers

$$p_1, \ p_2, \ p_3, \ \ldots$$

until some n_k becomes a prime, i.e. $n_k = p_k$ and we get

$$n = p_1 p_2 p_3 \ \ldots p_k$$

Main Factorization Theorem

Step 2 We show the **uniqueness**

Assume that we have two different prime factorizations

$$n = p_1 p_2 p_3 \dots p_k = q_1 q_2 q_3 \dots q_m$$

Each $p_i \mid n$, so for each p_i

$$p_i \mid \prod_{k=1}^{m} q_k$$

By the **Fact 4** $p_i = q_j$ for some j and $1 \leq j \leq m$

Conversely, we also have that each $q_i \mid n$, so for each q_i

$$q_i \mid \prod_{n=1}^{k} p_n$$

By the **Fact 4** $q_i = p_n$ for some n and $1 \leq n \leq k$

Main Factorization Theorem

This proves that both sides of

$$n = p_1 p_2 p_3 \ \ldots p_k = q_1 q_2 q_3 \ \ldots q_m$$

contain the same primes

The only difference might be that a prime p could occur a greater number of times on one side then on the other

In this case we cancel p on both sides sufficient number of times and get equation with p on one side, not the other

This **contradicts** just proven the fact that both sides of the equation contain the same primes

Main Factorization Theorem

We re-write our Theorem in a more formal way as follows

Main Factorization Theorem

For any $n \in N$, $n > 1$, there are $\alpha_i \in N$, $\alpha_i \geq 1$, and prime numbers $p_1 \neq p_2 \neq \ \ldots \ \neq p_r$ $r \geq 1$, $1 \leq i \leq r$, such that

$$n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \ \cdot \ {p_r}^{\alpha_r} = \prod_{k=1}^{r} {p_k}^{\alpha_k}$$

and this representation is unique

p_i' s are different prime factors of n

α_i is the multiplicity , i.e. the number of times p_i occurs in the prime factorization

Main Factorization Theorem; General Form

We write our Theorem shortly in a more general form, as in the Book (page 107)

Main Factorization Theorem General Form

$$n = \prod_{p} p^{\alpha_p} \quad \text{for} \quad p \in P, \ \ \alpha_p \geq 0$$

and this representation is unique

This is an infinite product, bur for any particular n all but few exponents $\alpha_p = 0$, and $p^0 = 1$

Hence for a given n it is a finite product

Some Consequences of Main Factorization Theorem

We know, by the **Main Factorization Theorem** that any $n > 1$ has a unique representation

$$n = \prod_{p} p^{n_p} \quad \text{for} \quad p \in P, \quad n_p \geq 0$$

Consider now the poset $(P, \leq)$, i.e. we have that all prime numbers in P are in the sequence

$$p_1 < p_2 < \ \dots \ p_n < \ \dots$$

$$2 < 3 < 5 < 7 < 11 < 13 < \ \dots$$

and we write

$$n = \prod_{i \geq 1} {p_i}^{n_i} \quad \text{for} \ \ n_i \geq 0$$

Because of the uniqueness of the representation we can represent n as

$$n = < n_1, \ n_2, n_3, \ \dots \ n_k, \dots \ >$$

Example

Reminder

$$2 < 3 < 5 < 7 < 11 < 13 < \ \ \dots$$

Here are few representations

$$7 = 7 \quad \text{so} \ \ 7 =< 0, 0, 0, 1, \ 0, \dots \ \ = < 0, 0, 0, 1 >$$

$$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3 \quad \text{so} \ \ 12 =< 2, 1, 0, 0, \dots \ \ >= < 2, 1 >$$

$$18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2 \quad \text{so} \ \ 18 =< 1, 2, 0, 0, \dots \ \ >= < 1, 2 >$$

Some Consequences of Factorization Theorem

Observe that when we have the general representations

$$k = \prod_{p} p^{k_p}, \quad n = \prod_{p} p^{n_p} \quad \text{and} \quad m = \prod_{p} p^{m_p}$$

then we evaluate

$$k = n \cdot m = \prod_{p} p^{n_p} \cdot \prod_{p} p^{m_p} = \prod_{p} p^{n_p + m_p} = \prod_{p} p^{k_p}$$

We have hence **proved** the following

Fact 6

$$k = n \cdot m \quad \text{if and only if} \quad k_p = n_p + m_p, \quad \text{for all } p \in P$$

Some Consequences of Factorization Theorem

Fact 7

Let

$$m = \prod_p p^{m_p} \quad \text{and} \quad n = \prod_p p^{n_p}$$

Then

$$m \mid n \quad \text{if and only if} \quad m_p \leq n_p \quad \text{for all} \quad p \in P$$

Proof

$m \mid n$ iff there is k, such that $n = mk$ and $k = \prod_p p^{k_p}$

By **Fact 6** we get that $n = mk$ iff $n_p = k_p + m_p$ iff $m_p \leq n_p$ and it **ends** the proof

Some Consequences of Factorization Theorem

Directly from **Fact 7** and definitions we get the following

Fact 8

$$k = gcd(m, n) \quad \text{if and only if} \quad k_p = min\{m_p, n_p\}$$

$$k = lcd(m, n) \quad \text{if and only if} \quad k_p = max\{m_p, n_p\}$$

Example

Example 1

Let

$$12 = 2^2 \cdot 3^1 \qquad 18 = 2^1 \cdot 3^2$$

$$gcd(12,\ 18) = 2^{min\{2,1\}} \cdot 3^{min\{2,1\}} = 2^1 \cdot 3^1 = 6$$

$$lcm(12,\ 18) = 2^{max\{2,1\}} \cdot 3^{max\{2,1\}} = 2^2 \cdot 3^2 = 36$$

Example 2

Let

$$m = 2^6 \cdot 3^2 \cdot 5^1 \cdot 7^0 \qquad n = 2^5 \cdot 3^3 \cdot 5^0 \cdot 7^0$$

$$gcd(m,\ n) = 2^{min\{6,5\}} \cdot 3^{min\{2,3\}} \cdot 5^{min\{1,0\}} \cdot 7^{min\{0,0\}} = 2^5 \cdot 3^2$$

$$lcm(m,\ n) = 2^6 \cdot 3^3 \cdot 5 \cdot 7$$

Exercises

1. Use **Facts 6-8** to prove

Theorem 5

For any $a, b \in Z^+$ such that lcm(a,b) and gcd(a, b) exist

$$lcm(a, b) \cdot gcd(a, b) = ab$$

2. Use **Theorem 5** and the BOOK version of Euclid Algorithm to express lcm(n mod m, m) when $nmodm \neq 0$

This is Ch4 Problem 2