cse547, math547
DISCRETE MATHEMATICS

Professor Anita Wasilewska
LECTURE 12
CHAPTER 4
NUMBER THEORY

PART 1: Divisibility

PART 2: Primes
PART 1: DIVISIBILITY
Basic Definitions

Definition
Given \( m, n \in \mathbb{Z} \), we say \( m \) divides \( n \) or \( n \) is divisible by \( m \) if and only if \( m \neq 0 \) and \( n = mk \), for some \( k \in \mathbb{Z} \)

We write it symbolically

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

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. \( n = mk \)

**Clearly:** \( k \neq 0 \) is also a **divisor** of \( n \) and is uniquely determined by \( m \)

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

Definition
\( n \in \mathbb{Z} \) 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
\[n = mk, \text{ so } n = (-m)(-k) = mk\]

Definition
\((-m, -k)\) is called an associated divisor to \((m, k)\)

Fact 2
\(\pm 1\) 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 \( m \mid n \) and \( n \mid m \), then \( m, n \) are associated, i.e. \( m = \pm n \)
Proof
Assume \( m \mid n \) i.e. \( n = mk_1 \), also \( n \mid m \) 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
The Book Definition

For \( n, m, k \in \mathbb{Z} \)

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

It means the The Book considers only positive divisors \((m, k), \ m > 0, \ k \in \mathbb{Z}\).

Definition

All positive divisors, including 1, that are less than \( n \) are called proper divisors of \( n \).
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 \( m \leq \sqrt{n} = \sqrt{60} \)
\[ \text{i.e.} \quad m \leq \sqrt{60} < \sqrt{64} = 8 \]
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 $b \in \mathbb{Z}$

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

We write it:

$$a = q b + r \quad q \in \mathbb{Z} \quad r = 0, 1, 2, \ldots, |b| - 1$$

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

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

Example

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

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

In particular any $n \in \mathbb{N}$, $n=2q$ (even) or $n = 2q + 1$ (odd)
Theorem
The square of \( n \in \mathbb{Z} \) is either divisible by 4, or leaves the remainder 1 when divided by 4

Proof
Case 1: \( n = 2q \), \( n^2 = (2q)^2 = 4q^2 \)
Case 2: \( n = 2q + 1 \), \( n^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1 \)
Division and Remainders

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

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

We re-write is as

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

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

Special Notation

Old notation

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

Modern notation

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

Modern notation comes from K.E. Iverson, 1960
Division and Remainders

Book, page 67

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

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

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

Example

\[
\begin{align*}
\lfloor \frac{25}{5} \rfloor &= 5, \\
\lfloor \frac{5}{3} \rfloor &= 1, \\
\lfloor 2 \rfloor &= 2, \\
\lfloor \frac{-1}{3} \rfloor &= -1, \\
\lfloor \frac{1}{3} \rfloor &= 0
\end{align*}
\]
Division and Remainders

We **extend** notation to Real numbers

\[ x, y, q \in \mathbb{R} \quad x = [x] + y, \quad 0 \leq y < 1 \]

**Example**

\[ [\pi] = 3, \quad [e] = 2, \quad [\pi^2/2] = 4 \]

Back to the Chapter 3 - we used notation \( \{x\} \) for \( y \)
Number Systems

Given \( a, b \in N \), we represent \( a \) on base \( b \) as

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

We write it as

\[
a = (a_n, a_{n-1}, a_1, a_0)_b
\]

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!
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

\[ q_1 = b(a_n b^{n-2} + \ldots + a_2) + a_1 \]

Observation 2

\( a_1 \) is the remainder of \( q_1 \) by division by \( b \) and

\[ q_1 = bq_2 + a_1 \]

where \( q_2 = a_n b^{n-2} + \ldots + a_3 b + a_2 \)

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

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

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

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

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

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

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

$$r_{n-2} = a_{n-2} b^{n-2} + r_{n-3}$$

and etc ...
Example

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

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

\[ 1832 = 5 \cdot 7^3 + 117 \quad a_3 = 5 \]

\[ 117 = 2 \cdot 7^2 + 19 \quad a_2 = 2 \]

\[ 19 = 2 \cdot 7 + 5 \quad a_1 = 2, \quad a_0 = 5 \]

We obtained

\[ 1832 = (5, 2, 2, 5)_7 \]
Greatest Common Divisor

Definition  Common Divisor
Let  $a, b, c \in \mathbb{Z}$
If $c$ divides $a$ and $b$ simultaneously, then $c$ is called a common divisor of $a$ and $b$

Symbolically
$c$ is a common divisor of $a$ and $b$  iff  $c \mid a$ and $c \mid b$
Greatest Common Divisor

Let \( A = \{ c : \text{c} \mid a \text{ and } \text{c} \mid b \} \) be the set of all common divisors of \( a \) and \( b \).

The set \( A \) is finite, so the poset \((A, \leq)\) is a finite, with a total (linear) order and hence always has the greatest element.

This greatest element is called a greatest common divisor (g.c.d.) of \( a \) and \( b \) and denoted by \( \gcd(a, b) \).

Remark: The greatest element in the poset \((A, \leq)\) is its unique maximal element so it justifies the BOOK definition:

\[
\gcd(a, b) = \max\{ c : \text{c} \mid a \cap \text{c} \mid b \}
\]
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

$$a \perp b \text{ for } a, b \in Z \text{ relatively prime}$$

Example
$gcd(24, 56) = 8$, $24 \nmid 56$ and $gcd(15, 21) = 1$, $15 \perp 22$
Euclid Algorithm

Theorem
Any common divisor of two numbers divides their greatest common divisor

Proof By procedure known as Euclid Algorism (Algorithm)
Euclid Algorism is known from seventh book of Euclid’s Elements (about 300 BC); however it is certainly of earlier origin

Here it is
Let \( a, b \in \mathbb{Z} \) be two integers whose \( \gcd(a,b) \) we want to be studied

Since there is only question of divisibility, there is no limitation in assuming that \( a, b \) are positive and \( a \) is greater or equal \( b \), i.e. \( a, b \in \mathbb{Z}^+ \) and \( a \geq b \)
Euclid Algorithm

1. We divide $a$ by $b$ with respect to the least positive remainder
   \[ a = q_1 b + r_1 \quad 0 \leq r_1 < b \]

2. We divide $b$ by $r_1$ with respect to the least positive remainder
   \[ b = q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1 \]

3. We divide $r_1$ by $r_2$ with respect to the least positive remainder
   \[ r_1 = q_2 r_2 + r_3 \quad 0 \leq r_3 < r_1 \]

We continue the process
Euclid Algorithm

Observe that such obtained remainders

\[ r_1, \ r_2, \ r_3, \ldots r_n, \]

form a decreasing sequence of positive integers

\[ r_1 > r_2 > r_3 > \ldots r_n > \ldots \]

and one must arrive on a division for which \( r_{n+1} = 0 \), i.e. the Euclid Algorism process:
divide a by b, divide b by \( r_1 \), \ldots divide \( r_k \) by \( r_{k+1} \)
must terminate
Euclid Algorithm

Euclid Algorism

\[ a = q_1 b + r_1 \]
\[ b = q_2 r_1 + r_2 \]
\[ r_1 = q_2 r_2 + r_3 \]
\[ \ldots \]
\[ r_{n-2} = q_n r_{n-1} + r_n \]
\[ r_{n-1} = q_{n+1} r_n + 0 \]

Theorem

\[ r_n = (a, b) = gcd(a, b) \]
Euclid Algorithm Example

Example
Find $gcd(76084, 63020)$

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

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

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

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

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

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

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

$gcd(76084, 63020) = (76084, 63020) = r_6 = 92$
Euclid Algorithm Correctness Proof

Theorem
For any $a, b \in \mathbb{Z}^+$ and $a \geq b$, and the Euclid Algorithm applied to $a, b$ the following holds

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

Proof
We conduct 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 common divisor of $a$ and $b$
Euclid Algorithm Correctness Proof

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

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

Observe that

$$ r_{n-2} = q_nr_{n-1} + r_n = q_nq_{n+1}r_n + r_n = r_n(q_nq_{n+1} + 1) $$

Hence

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

\[ r_n \mid r_{n-3} \]

We carry our proof by double induction with 1. and 2. as base cases proved already to be true.

Inductive Assumption

\[ r_n \mid r_{n-k} \quad \text{and} \quad r_n \mid r_{n-(k+1)} \quad \text{for} \quad k \geq 1 \]

Inductive Thesis

\[ r_n \mid r_{n-(k+2)} \]
Euclid Algorithm Correctness Proof

Observe that

\[ r_{n-(k+2)} = q_{n-(k+1)}r_{n-(k+1)} + r_{n-k} \]

and by inductive assumption

\[ r_n \mid r_{n-(k+1)}, \quad r_n \mid r_{n-k} \]

Hence

\[ r_n \mid r_{n-(k+2)} \]

By **Double Induction** Principle

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

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 \( r_n \mid r_1 \) and \( r_n \mid r_2 \)

Hence

\[ r_n \mid b \]

We also have that

\[ a = q_1 b + r_1 \]

and we just got \( r_n \mid r_1 \) and \( r_n \mid b \)

Hence

\[ r_n \mid a \]

It proves that \( r_n \) is a **common divisor** of \( a \) and \( b \) and it **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 $A$ be a set of all common divisors of $a$ and $b$, i.e.

$$A = \{ c : \quad c \mid a \cap c \mid b \}$$

We have to show that for any $c \in A$

$$c \mid r_n$$

i.e. that $r_n$ is the greatest element in the poset $(A, \mid)$

Exercise: Show that $\mid$ is an order (partial order) relation in $\mathbb{Z}$
Euclid Algorithm Correctness Proof

We have

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

so for any \( c \in A \), \( c \mid a \) and \( c \mid b \), hence

\[ c \mid r_1 \]

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

\[ c \mid r_2 \]

By Mathematical Induction

\[ c \mid r_k \quad \text{for all} \quad k \geq 1 \]

and in particular

\[ c \mid r_n \]

what ends the proof of the correctness of the Euclid Algorithm
Faster Algorithm

Kronecker (1823 - 1891) proved that no Euclid Algorithm can be shorter than 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 $\text{mod} \subseteq R \times R$ as

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

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 $a, b \in \mathbb{Z}, b \neq 0$ we get

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

and

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

Fact

$a \mod b$ 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 \( m, n \in \mathbb{Z}, \ 0 \leq m < n \) 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 \( a, b \in \mathbb{Z}, \ 0 \leq a < b \)
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

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

\[ f(12, 18) = f(6, 12) = f(0, 6) = 6 \quad gcd(12, 18) = f(0, 6) = 6 \]

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

\( m, n \in \mathbb{N} - \{0, 1\} \) 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

If \( b \mid ac \) and \( a \perp b \) then \( b \mid c \)

**Proof**

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

\[
a = q_1 b + r_1 \\
b = q_2 r_1 + r_2 \\
\vdots \\
r_{n-2} = q_n r_{n-1} + 1
\]
Some Consequences of Euclid Algorithm

Multiply by $c$

$$ac = q_1 bc + r_1 c$$

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

... ...

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

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

If \( a \perp b_i \), for \( i = 1, 2, \ldots k \), then \( a \perp b_1 b_2 \ldots b_k \)

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

$$a \perp b, \quad \text{and} \quad d \mid a, \quad \text{hence we get} \quad d \perp b$$

We also have

$$a \perp c, \quad \text{and} \quad d \mid a, \quad \text{hence we get} \quad d \perp c$$

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

\[ a = q_1 b + r_1 \]

\[ \ldots \ldots \]

\[ r_{n-2} = q_n r_{n-1} + r_n \]

\[ r_{n-1} = q_{n+1} r_n + 0 \]

We multiply each step by \( k \)
Some Consequences of Euclid Algorithm

We multiply each step by $k$

$$ka = kq_1 b + kr_1$$

$$\ldots \ldots$$

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

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

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 $a = a_1d, \ b = b_1d$

$$\frac{a}{b} = \frac{a_1d}{b_1d} = \frac{a_1}{b_1}$$

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 \( a, b, m \in \mathbb{Z} \)

\( m = \text{cm}(a, b) \) is a common multiple of \( a \) and \( b \) iff \( a | m \) and \( b | m \) and \( m > 0 \)
Least Common Multiple

Let \( A = \{ m : a \mid m \text{ and } b \mid m \} \) 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 \( \text{lcm}(a, b) \).

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

\[
\text{lcm}(a, b) = \min\{m : m > 0 \text{ and } a \mid m \text{ and } b \mid m\}
\]
Least Common Multiple

Theorem 4
Any common multiple of $a$ and $b$ is divisible by $\text{lcm}(a,b)$

Proof
Let $m = \text{cm}(a,b)$
We divide $m$ by $\text{lcm}(a,b)$, i.e.

$$m = qlcm(a, b) + r \quad 0 \leq r < \text{lcm}(a, b)$$

But $a \mid \text{lcm}(a, b)$ and $b \mid \text{lcm}(a, b)$ 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 $0 \leq r < \text{lcm}(a, b)$, so $r=0$ what proves that $m = q \cdot \text{lcm}(a, b)$, i.e. $m$ is divisible by $\text{lcm}(a,b)$
Least Common Multiple

**Theorem 5**
For any $a, b \in Z^+$ such that \( \text{lcm}(a,b) \) and \( \text{gcd}(a, b) \) exist

\[
\text{lcm}(a, b) \cdot \text{gcd}(a, b) = ab
\]

**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

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

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

\[
\text{if} \quad k \mid p \quad \text{then} \quad k = 1 \quad \text{or} \quad k = p
\]

Some primes

\[
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots
\]
Primes

Observe 2 is the only even prime!

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

Definition

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

Symbolically

$n \in CN$ if and only if $n \leq 1 \cup \exists k \in Z (k | n \cap k \neq 1 \cap k \neq n)$

Directly from the definition we have that

Fact 1

$$\forall m \in N \setminus \{0, 1\} ( m \in P \cup m \in CN) \text{ and } P \cap CN = \emptyset$$
Primes

Definition

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

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

Fact 2

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

Fact 3

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

Symbolically

$$\forall p \in \mathbb{P} \ \forall m, n \in \mathbb{Z} \ (p | mn \Rightarrow (p | m \cup p | n))$$
Primes

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

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

$p \nmid m$ so by Fact 2 $p \perp m$

Now when $p \mid mn$ and $p \perp m$ we get $p \mid n$ and we get a contradiction with $p \nmid n$

Fact 4
A product $q_1q_2\ldots q_n$ of prime numbers (factors) $q_i$ is divisible by a prime $p$ only when $p = q_i$ for some $q_i$
Primes

Fact 4

\[ \forall p, q_1, q_2, \ldots, q_n \in P \ (p \mid \prod_{k=1}^{n} q_k \Rightarrow \exists 1 \leq i \leq n (p = q_i)) \]

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 \( p = q_i \)

Fact 5

Every natural number \( n, \ n > 1 \) is divisible by some prime
Primes

Fact 5

\[ \forall n \in \mathbb{N}, n > 1 \exists p \in \mathbb{P} \ (p \mid n) \]

Proof

When \( n \in \mathbb{P} \), 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

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

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 than 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 $n \in \mathbb{N}$, $n > 1$, there are $\alpha_i \in \mathbb{N}$, $\alpha_i \geq 1$, 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 $n$

$\alpha_i$ 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

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

and this representation is unique

This is an infinite product, but 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

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

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

$$p_1 < p_2 < \ldots p_n < \ldots$$

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

and we write

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

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

$$n = < n_1, n_2, n_3, \ldots n_k, \ldots >$$
Example

Here are few representations

\[ 7 = 7 \text{ so } 7 = \langle 0, 0, 0, 1, 0, \ldots \rangle = \langle 0, 0, 0, 1 \rangle \]
\[ 12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3 \text{ so } 12 = \langle 2, 1, 0, 0, \ldots \rangle = \langle 2, 1 \rangle \]
\[ 18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2 \text{ so } 18 = \langle 1, 2, 0, 0, \ldots \rangle = \langle 1, 2 \rangle \]
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

\[ k = n \cdot m = \prod_p p^{n_p} \cdot \prod_p p^{m_p} = \prod_p p^{n_p + m_p} \]

We have hence proved

Fact 6

\[ k = n \cdot m \quad \text{if and only if} \quad k_p = n_p + m_p, \quad \text{for all} \quad p \in P \]
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
\[ m \mid n \quad \text{iff} \quad \text{there is} \quad k, \quad \text{such that} \quad n = mk \quad \text{and} \quad k = \prod_p p^{k_p} \]
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 we definitions we get the following

Fact 8

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

\[ k = \text{lcm}(m, n) \quad \text{if and only if} \quad k_p = \max\{m_p, n_p\} \]
Example

Example 1
Let

\[ 12 = 2^2 \cdot 3^1 \quad 18 = 2^1 \cdot 3^2 \]

\[ \text{gcd}(12, 18) = 2^{\min\{2,1\}} \cdot 3^{\min\{2,1\}} = 2^1 \cdot 3^1 = 6 \]
\[ \text{lcm}(12, 18) = 2^{\max\{2,1\}} \cdot 3^{\max\{2,1\}} = 2^2 \cdot 3^2 = 36 \]

Example 2
Let

\[ m = 2^6 \cdot 3^2 \cdot 5^1 \cdot 7^0 \quad n = 2^5 \cdot 3^3 \cdot 5^0 \cdot 7^0 \]

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

\[ \text{lcm}(m, n) = 2^6 \cdot 3^3 \cdot 5 \cdot 7 \]
Exercises

1. Use Facts 6-8 to prove Theorem 5
   For any $a, b \in \mathbb{Z}^+$ 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 $lcm(n \text{ mod } m, m)$ when $n \text{ mod } m \neq 0$
   This is Ch4 Problem 2