UNIT-II

NUMBER THEORY

- An integer n is **even** if, and only if, n equals twice some integer.

  i.e. if n is an integer, then n is even $\Leftrightarrow \exists$ an integer k such that $\underline{n = 2k}$

- An integer n is **odd** if, and only if, n equals twice some integer plus 1.

  i.e. N is odd $\Leftrightarrow \exists$ an integer k such that $\underline{n = 2k+1}$.

a. Is 0 even?

b. Is -301 odd?

c. If a and b are integers, is $6a^2b$ even?

d. If a and b are integers, is $10a+8b+1$ odd? e. Is every integer either even or odd?

- An integer n is **prime** if and only if, $n > 1$ and for all positive integers r and s,

  if $n = rs$, then either r or s equals n.

  i.e. n is prime $\Leftrightarrow \forall$ positive integers r and s, if $n = rs$ then

  either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.

- An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

  n is composite $\Leftrightarrow \exists$ positive integers r and s such that $n = rs$

  and $1 < r < n$ and $1 < s < n$.

- Is 1 prime?
- b. Is every integer greater than 1 either prime or composite?
- c. Write the first six prime numbers.
- d. Write the first six composite numbers.

- No. A prime number is required to be greater than 1.
- Yes. Let n be any integer that is greater than 1. Consider all pairs of positive integers r and s such that n =rs. There exist at least two such pairs, namely r =n and s =1 and r =1 and s =n.

Moreover, since n =rs, all such pairs satisfy the inequalities $1 \le r \le n$ and $1 \le s \le n$. If n is prime, then the two displayed pairs are the only ways to write n as rs.

Otherwise, there exists a pair of positive integers r and s such that n =rs and neither r nor s equals either 1 or n. Therefore, in this case $1 < r < n$ and $1 < s < n$, and hence n is composite.

- 2, 3, 5, 7, 11, 13
- 4, 6, 8, 9, 10, 12

- $\exists x \in D$ such that $Q(x)$ is true if and only if,

  $Q(x)$ is true for at least one x in D.

Prove the following:

1. $\exists$ an even integer n that can be written in two ways as a sum of two prime numbers.

1. Suppose that r and s are integers. Prove the following: $\exists$ an integer k such that $22r + 18s = 2k$.

- Let $n = 10$. Then $10 = 5+5 = 3+7$ and 3, 5, and 7 are all prime numbers.
- Let $k = 11r + 9s$. Then k is an integer because it is a sum of products of integers; and by substitution, $2k = 2(11r + 9s)$, which equals $22r + 18s$ by the distributive law of algebra.
- Disprove the following statement by finding a counterexample:
  - ✓ $\forall$ real numbers a and b, if $a^2 = b^2$ then $a = b$

Generalizing from the particular:

Step	Visual Result	Algebraic Result
Pick a number.	□	x
Add 5.	□ |||||	$x + 5$
Multiply by 4.	□ ||||| □ ||||| □ ||||| □ |||||	$(x + 5) \cdot 4 = 4x + 20$
Subtract 6.	□ || □ || □ ||||| □ |||||	$(4x + 20) - 6 = 4x + 14$
Divide by 2.	□ || □ |||||	$\frac{4x + 14}{2} = 2x + 7$
Subtract twice the original number.	|| |||||	$(2x + 7) - 2x = 7$

The sum of any two even integers is even.

- Suppose m and n are [particular but arbitrarily chosen] even integers,vthen show that m+n is even.

  By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s.

  Then $m+n = 2r + 2s$ by substitution

  $m+n = 2(r + s)$ by factoring out

- Note that r and s are integers therefore r + s is also is an integer (because it is a sum of integers.) m+n is some integer multiple of 2
- Hence m + n is an integer.

Show that " there is a positive integer n such that n^2+3n+2 is prime" is false.

- Suppose n is any arbitrarily chosen positive integer.
- Since $n^2+3n+2 = (n+1)(n+2)$
- n+1 and n+2 both are integer as they are sum of integer also
- $n+1 > 1$ & $n+2 > 1$ (since $n> 1$)
- n^2+3n+2 is product of two integers both are greater than 1.
- Therefore n^2+3n+2 not prime.

- A real number r is **rational** if and only if, it can be expressed as a quotient of two integers with a non zero denominator.
- A real number that is not rational is **irrational**.

More formally,

if r is a real number, then r is rational ⇔ ∃ integers a and b such that r = a b and b =0.

- Is 10/3 a rational number?
- b. Is− 5 39 a rational number?
- c. Is 0.281 a rational number?
- d. Is 7 a rational number?
- e. Is 0 a rational number?

- If neither of two real numbers is zero, then their product is also not zero
- Every integer is a rational number
- $\forall$real numbers r and s, if r and s are rational then r +s is rational.
- The double of a rational number is rational

• Definition

If n and d are integers and $d \neq 0$ then

n is **divisible by** d if, and only if, n equals d times some integer.

Instead of "n is divisible by d," we can say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation $\mathbf{d \mid n}$ is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

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

- Is 21 divisible by 3?
- b. Does 5 divide 40?
- c. Does $7|42$?
- d. Is 32 a multiple of -16?
- e. Is 6 a factor of 54?
- f. Is 7 a factor of -7?

- The only divisor of 1 are 1 or -1.
- If a and b are integers, is 3a+3b divisible by 3?
- If k and m are integers, is 10km divisible by 5?
- For all integers n and d, $d \nmid n \Leftrightarrow n/d$ is not an integer.
- Prove that for all integers a, b, and c, if $a|b$ and $b|c$, then $a|c$.
- For all integers a and b, if $a|b$ and $b|a$ then $a = b$.

Theorem 4.3.5 Unique Factorization of Integers Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

• Definition

Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \cdots < p_k$.

The Quotient Reminder Theorem

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

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

• Definition

Given an integer n and a positive integer d,

$$\begin{aligned} \boldsymbol{n \ div \ d} &= \text{the integer quotient obtained} \\ &\quad\ \text{when } n \text{ is divided by } d \text{, and} \\ \boldsymbol{n \ mod \ d} &= \text{the nonnegative integer remainder obtained} \\ &\quad\ \text{when } n \text{ is divided by } d. \end{aligned}$$

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

$$n \ div \ d = q \quad \text{and} \quad n \ \ mod \ \ d = r \quad \Leftrightarrow \quad n = dq + r$$

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

• Definition

For any real number x, the **absolute value of x**, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}.$$

For all real numbers r, $-|r| \leq r \leq |r|$.

Proof:

Suppose r is any real number. We divide into cases according to whether $r \geq 0$ or $r < 0$.

Case 1 ($r \geq 0$): In this case, by definition of absolute value, $|r| = r$. Also, since r is positive and $-|r|$ is negative, $-|r| < r$. Thus it is true that

$$-|r| \leq r \leq |r|.$$

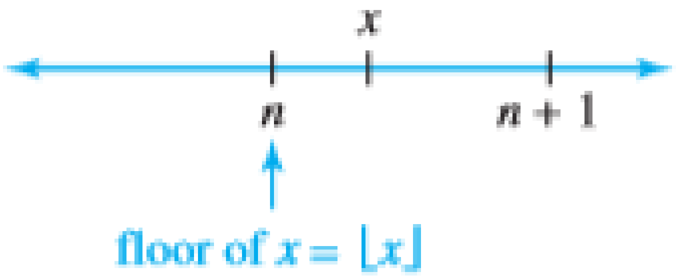
• Definition

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

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

Symbolically, if x is a real number and n is an integer, then

$$\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \leq x < n + 1.$$



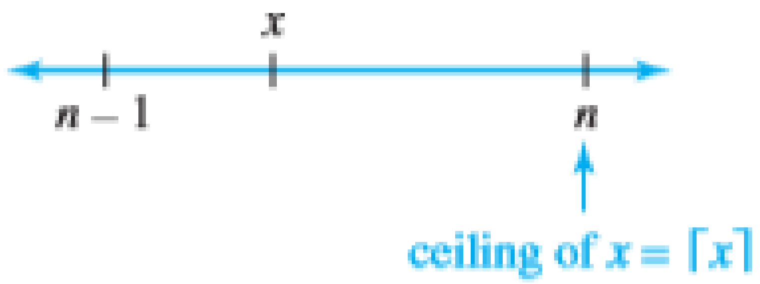
• Definition

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

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

Symbolically, if x is a real number and n is an integer, then

$$\lceil x \rceil = n \quad \Leftrightarrow \quad n - 1 < x \leq n.$$



The square of any odd integer has the form $8m + 1$ for some integer m.

Proof:

Suppose n is a *[particular but arbitrarily chosen]* odd integer. By the quotient-remainder theorem, n can be written in one of the forms

$$4q \quad \text{or} \quad 4q+1 \quad \text{or} \quad 4q+2 \quad \text{or} \quad 4q+3$$

for some integer q. In fact, since n is odd and $4q$ and $4q + 2$ are even, n must have one of the forms

$$4q+1 \quad \text{or} \quad 4q+3.$$

Case 1 ($n = 4q + 1$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 1$,

$$\begin{aligned} n^2 &= (4q+1)^2 && \text{by substitution} \\ &= (4q+1)(4q+1) && \text{by definition of square} \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 && \text{by the laws of algebra.} \end{aligned}$$

Let $m = 2q^2 + q$. Then m is an integer since 2 and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Case 2 ($n = 4q + 3$ for some integer q): *[We must find an integer m such that $n^2 = 8m + 1$.]* Since $n = 4q + 3$,

$$\begin{aligned} n^2 &= (4q+3)^2 && \text{by substitution} \\ &= (4q+3)(4q+3) && \text{by definition of square} \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + (8+1) \\ &= 8(2q^2 + 3q + 1) + 1 && \text{by the laws of algebra.} \end{aligned}$$

[The motivation for the choice of algebra steps was the desire to write the expression in the form $8 \cdot$ (some integer) $+ 1$.]

Let $m = 2q^2 + 3q + 1$. Then m is an integer since 1, 2, 3, and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Cases 1 and 2 show that given any odd integer, whether of the form $4q + 1$ or $4q + 3$, $n^2 = 8m + 1$ for some integer m. *[This is what we needed to show.]*

Greatest Common Divisor

- Let a and b be integers that are not both zero.
- The greatest common divisor of a and b, denoted gcd(a,b), is that integer d with the following properties:

1. d is a common divisor of both a and b.

    In other words, $d|a$ and $d|b$.

2. For all integers c, if c is a common divisor of both a and b, then c is less than or equal to d.

In other words, for all integers c,if $c|a$ and $c|b$,then $c \leq d$.

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

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

- $\gcd(a,b) = \gcd(b,r)$
- if a,b,q, and r are integers with $a = b \cdot q + r$ and $0 \leq r < b$. 2. $\gcd(a,0) = a$.]