Basic Concepts of Number Theory: Part 1

Assoc.Prof.Chaweewan Kaewsaiha

Founder of Modern Number Theory

Pierre De Fermat
(1601 – 1665)

Some of his contributions include Fermat numbers and Fermat primes, Fermat's principle, Fermat's Little Theorem, and Fermat's Last Theorem.

Source:
https://study.com/academy/lesson/pierre-de-fermat-contributions-to-math-accomplishments.html

Fermat Numbers and Fermat Primes

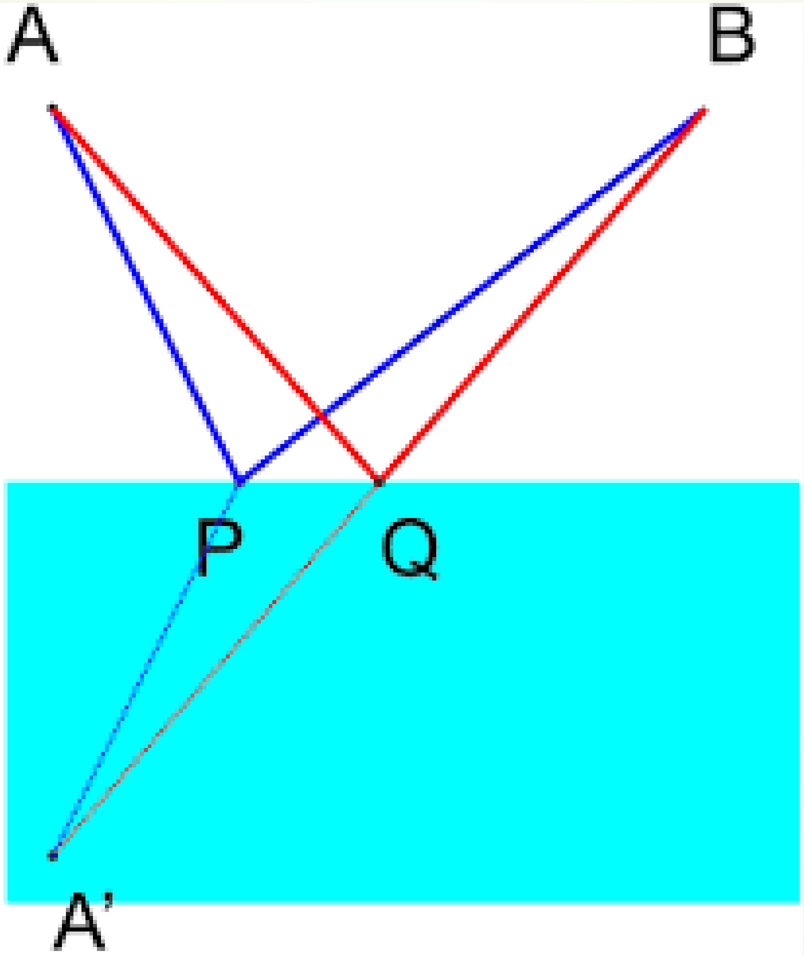
Fermat Number: $F_n = 2^{2^n} + 1$, where $n = 0,1,2,3,4, \ldots$

Fermat Primes are important to the study of prime numbers and Mersenne numbers.

Example:

$$F_0 = 2^{2^0} + 1 = 3$$
$$F_1 = 2^{2^1} + 1 = 5$$
$$F_2 = 2^{2^2} + 1 = 17$$
$$F_3 = 2^{2^3} + 1 = 257$$
$$F_4 = 2^{2^4} + 1 = 65537$$

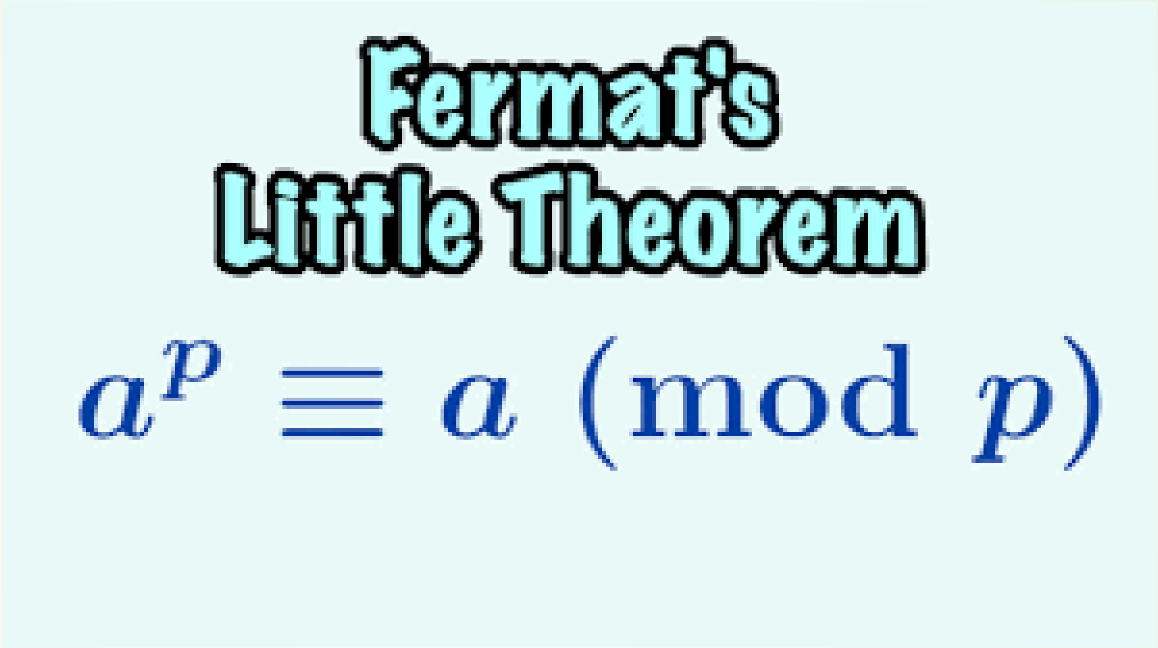
Fermat's Principle



Law of reflection

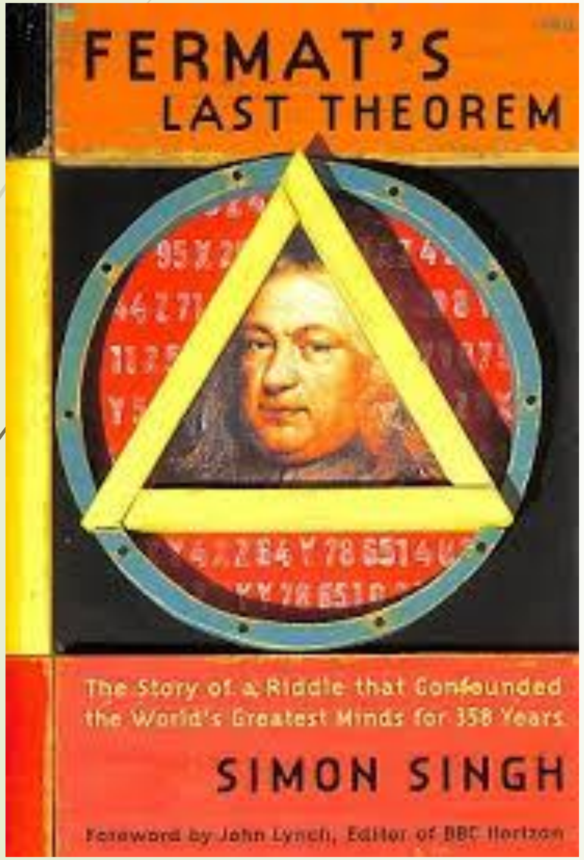
Law of refraction

Fermat’s Little Theorem



p is prime and $p|a \Rightarrow a^p \equiv a(mod\ p)$

Fermat’s Last Theorem



There are no three positive integers $x, y,$ and z for which

$$x^n + y^n = z^n$$

for any integer $n > 2$.

Prince of Mathematics

Carl Friedrich Gauss
(1777 – 1855)

Some of his contributions include number theory, binomial theorem, prime number theorem, arithmetic and geometric mean. At the age of seven, he summed the integers from 1 to 100 using 50 pairs of numbers each pair summing up to 101.

Binomial Theorem

$$(a+b)^n = \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n}a^0 b^n$$

$$\text{where } \binom{n}{r} = {}^nC_r = \frac{n!}{r!(n-r)!}$$

There are $n + 1$ terms and n is a positive integer.

							1							
						1		1						
					1		2		1					
				1		3		3		1				
			1		4		6		4		1			
		1		5		10		10		5		1		
	1		6		15		20		15		6		1	
1		7		21		35		35		21		7		1

Binomial coefficient (Pascal's Triangle)

Prime Number Theorem

Prime Number Theorem

$$\lim_{x \to \infty} \frac{\pi(x)}{x / \ln(x)} = 1$$

$\pi(x)$ is the number of primes less than or equal to x.

Arithmetic – Geometric Mean

Formula

$$A = \frac{1}{n}\sum_{i=1}^{n} a_i$$

A = arithmetic mean

n = number of values

a_i = data set values

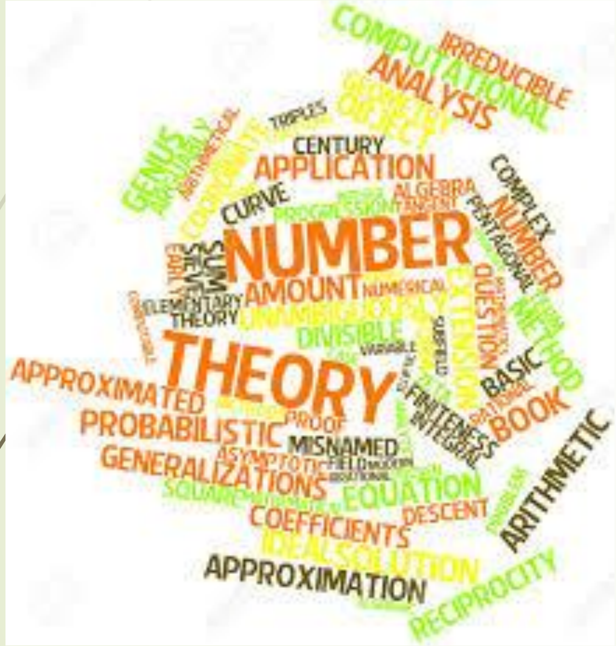
$$\left(\prod_{i=1}^{n} x_i\right)^{\frac{1}{n}} = \sqrt[n]{x_1 x_2 \cdots x_n}$$

$\prod$ = geometric mean

n = number of values

x_i = values to average

Number Theory



Number theory is the branch of mathematics that deals with the properties and relationships of numbers, especially the positive integers.

Natural Numbers – Whole Numbers – Integers

Definition 1: The set of *natural numbers* is $N = \{1, 2, 3, 4, 5, \dots\}$. N is also called the set of ***positive integers***.

Definition 2: The set of *whole numbers* is $W = \{0, 1, 2, 3, 4, 5, \dots\}$. W is also referred to the set of ***non-negative integers***.

Definition 3: The set of ***integers*** is $I = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

I is also denoted by Z.

$$N \subset W \subset I$$

Properties of Integers

Properties of Addition

Property 1 Closure under Addition:

$$a + b \text{ is in } I \text{ for all } a \text{ and } b \text{ in } I.$$

Property 2 Associative Law of Addition

$$a + (b + c) = (a + b) + c \text{ for all } a, b \text{ and } c \text{ in } I.$$

Properties of Integers (cont.)

Properties of Addition (cont.)

Property 3 Commutative Law of Addition:

$a + b = b + a$ for all a and b in I.

Property 4 Additive Identity

There is an element 0 in I such that $a + 0 = 0 + a = a$ for all a in I.

Properties of Integers (cont.)

Properties of Addition (cont.)

Property 5 Additive Inverse:

For each element a in I, there is an element $-a$ in I such that $a + (-a) = (-a) + a = 0$.

Properties of Integers (cont.)

Properties of Multiplication

Property 6 Closure under Multiplication:

ab is in I for all a and b in I.

Property 7 Associative Law of Multiplication

$a(bc) = (ab)c$ for all a, b and c in I.

Properties of Integers (cont.)

Properties of Multiplication (cont.)

Property 8 Commutative Law of Multiplication:

$ab = ba$ for all a and b in I.

Property 9 Multiplicative Identity

There is an element 1 in I such that $a(1) = (1)a = a$ for all a in I.

Remark: The inverse property is not satisfied for every element a in I. Because the identity element is equal to 1, but no two integers multiply to give 1 except 1 itself.

Properties of Integers (cont.)

Property Relating Addition and Multiplication

Property 10 Distributive Laws:

i. $c \cdot (a + b) = c \cdot a + c \cdot b$ for all a, b and c in I. (left distributive law)
ii. $(a + b) \cdot c = a \cdot c + b \cdot c$ for all a, b and c in I. (right distributive law)

Even Numbers and Odd Numbers

Definition 4: A number is ***even*** if it can be written in the form $2n$, where n is an integer; a number is ***odd*** if it can be written in the form $2n + 1$.

The set of even numbers is $E = \{\dots, -4, -2, 0, 2, 4, 6, \dots\}$.

The set of odd numbers is $O = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$.

Even and Odd Number Theorems

Theorem 1: The sum of two odd numbers is even.

Proof: Let a and b be odd numbers. Then there exist integers m and n

such that $a = 2m + 1$ and $b = 2n + 1$.

Thus, $a + b = (2m + 1) + (2n + 1) = 2m + 2n + 2 = 2(m + n + 1)$.

Since, $m + n + 1$ is an integer. (Closure law of integer addition)

Then, $a + b = 2p$ with $p = m + n + 1 \in I$.

Therefore, $a + b$ is even. (Definition of even integer) #

Even and Odd Number Theorems (cont.)

Theorem 2: Let n be an integer. If n is even, then $n^2$is even.

Proof: Assume n is an even integer.

Then $n = 2k$ for some $k \in I$. (Definition. of an even integer)

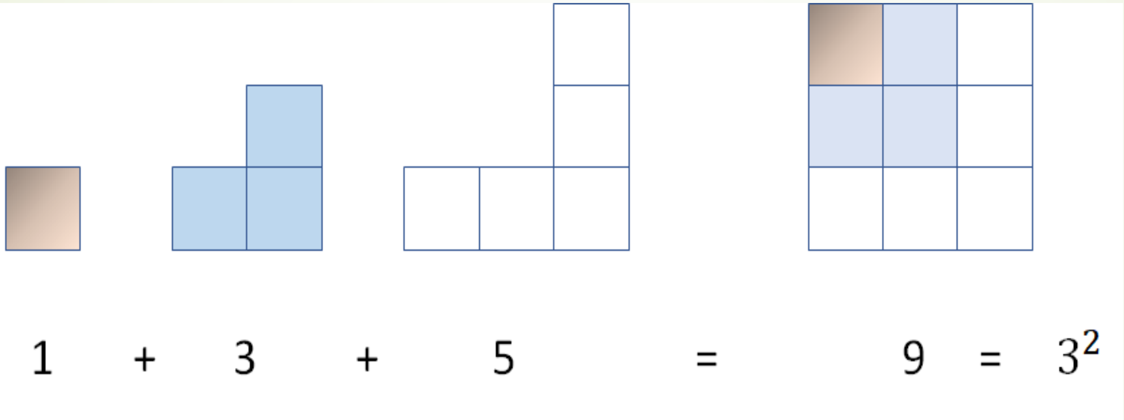
Squaring both sides, we get $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

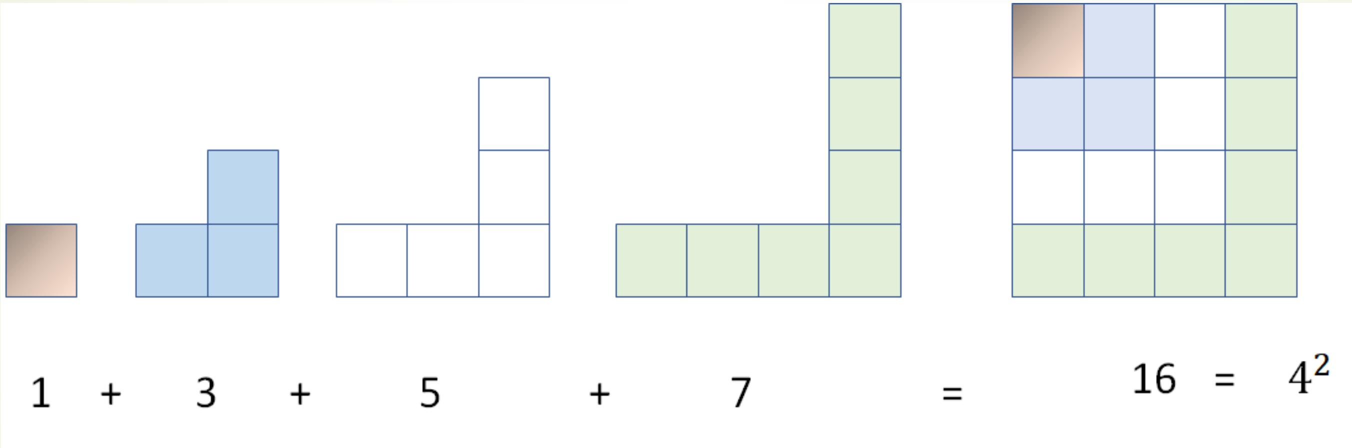
Since k is an integer, so is $2k^2$. (Closure law of integer multiplication)

Hence $n^2 = 2p$ with $p = 2k^2 \in I$.

Therefore $n^2$is even (Definition. of an even integer) #

The sum of consecutive odd numbers





The Fibonacci Sequence

The Fibonacci sequence of natural numbers is listed as follows:

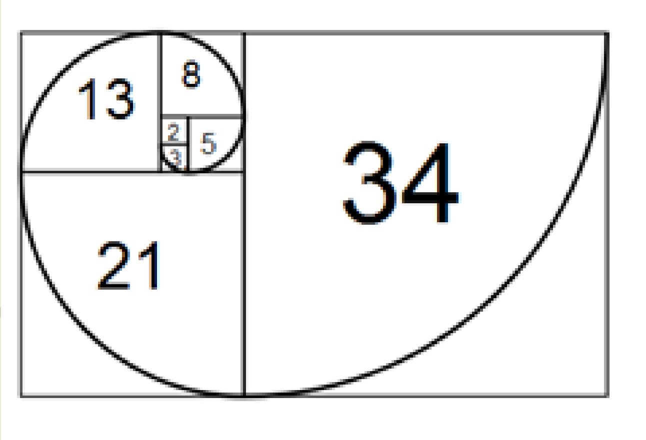
$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots,$$

Where each new term is formed by adding the last term to its predecessor. Thus, $2 = 1 + 1$, $3 = 2 + 1$, $5 = 3 + 2$, $8 = 5 + 3$, ….

So, we can write the rule:

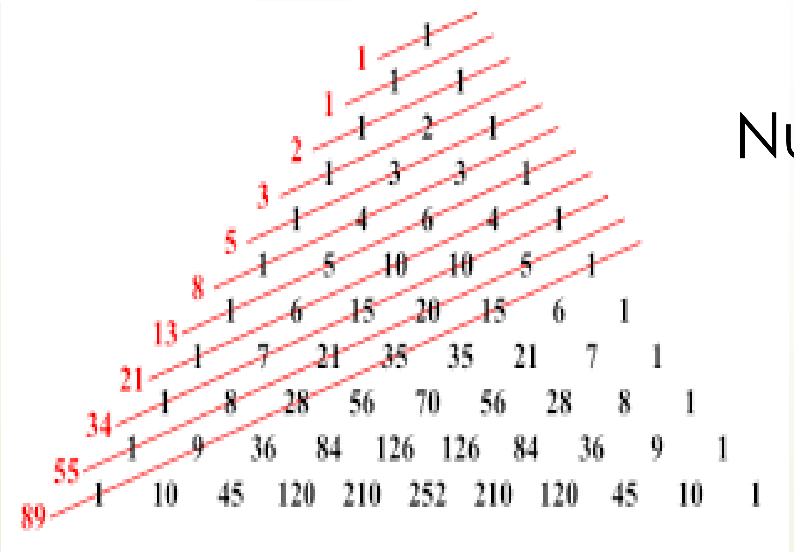
$$x_n = x_{n-1} + x_{n-2}$$

Fibonacci sequence and application

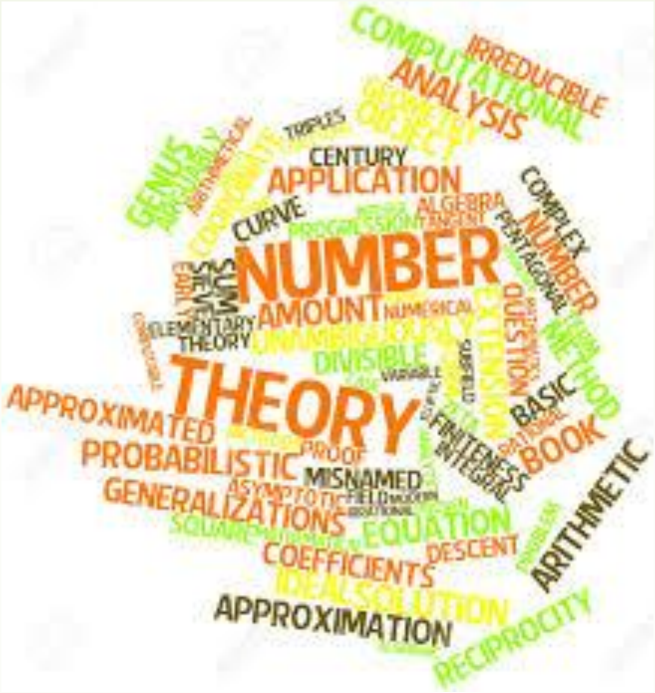


Arts

Number of petals of flower



Binomial coefficient



Practice 4.1 (page 6)

Primes and Composites

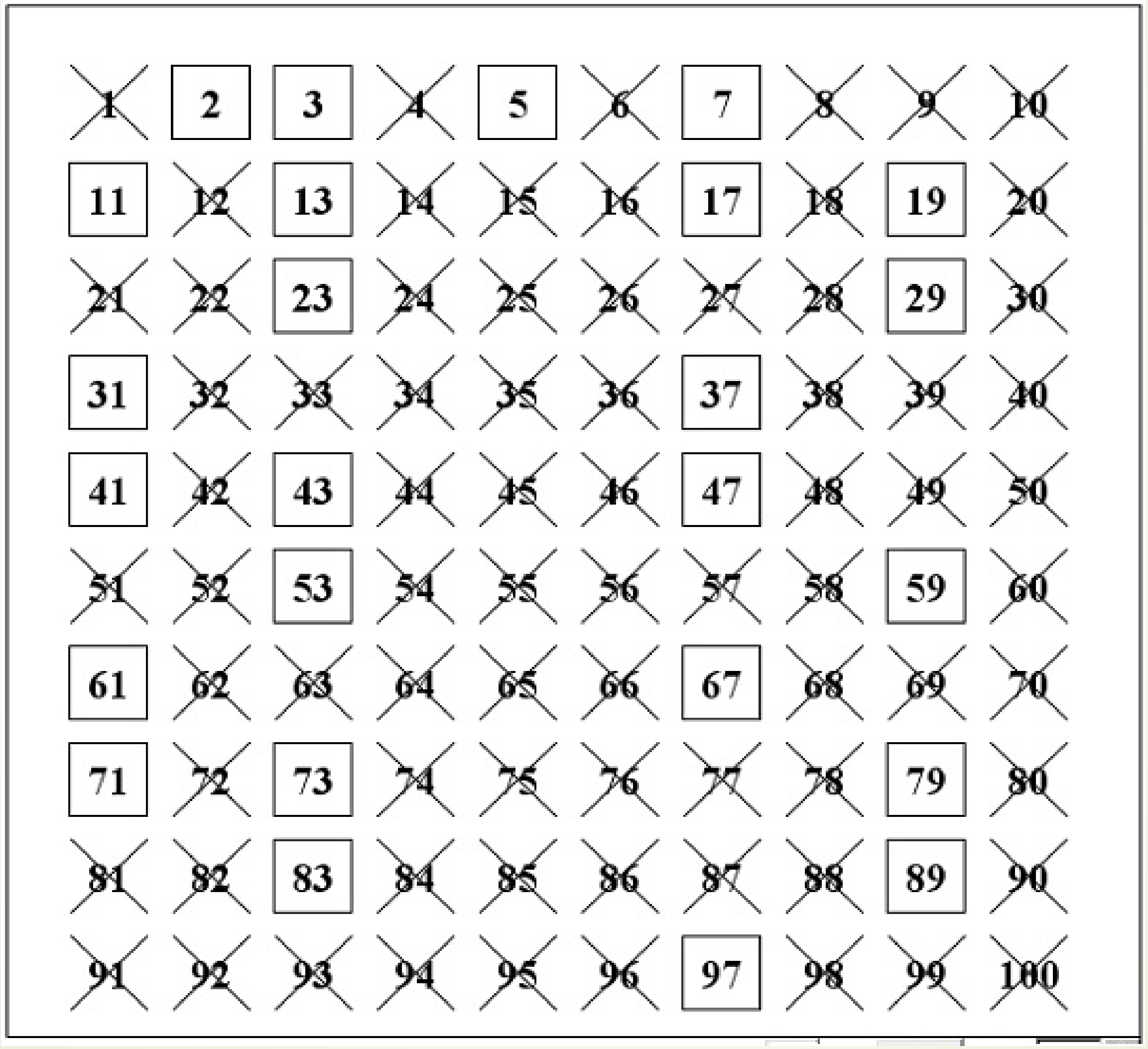
Definition 5: A ***prime number*** *p* is a positive integer greater than 1 whose only factors are 1 and itself.

Definition 6: A ***composite number*** *q* is a positive integer greater than 1 which is not prime.

Primes and Composites (cont.)

Number	Explanation	Prime/Composite
1	not a prime number by definition	-
2	factors are 1 and 2	Prime
3	factors are 1 and 3	Prime
4	factors are 1, 2, and 4	Composite
5	factors are 1 and 5	Prime
6	factors are 1, 2, 3, and 6	Composite
7	factors are 1 and 7	Prime
8	factors are 1, 2, 4, and 8	Composite
9	factors are 1, 3, 9	Composite
10	factors are 1, 2, 5, and 10	Composite

The Sieve of Eratosthenes



Distribution of Primes

From 1 to 1,000

Number from	1	100	200	300	400	500	600	700	800	900
to	100	200	300	400	500	600	700	800	900	1000
Number of primes	25	21	16	16	17	14	16	14	15	14

Distribution of Primes (cont.)

From 10^{12} to $10^{12} + 1{,}000$

Number from	$10^{12} +$	0	100	200	300	400	500	600	700	800	900
to	$10^{12} +$	100	200	300	400	500	600	700	800	900	1000
Number of primes		4	6	2	4	2	4	3	5	1	6

Distribution of Primes (cont.)

If we wish to have 1000 consecutive numbers, we can start from 1001! as follows:

$$1001! + 2, 1001! + 3, 1001! + 4, \ldots, 1001! + 1001$$

Where the notation 1001! means

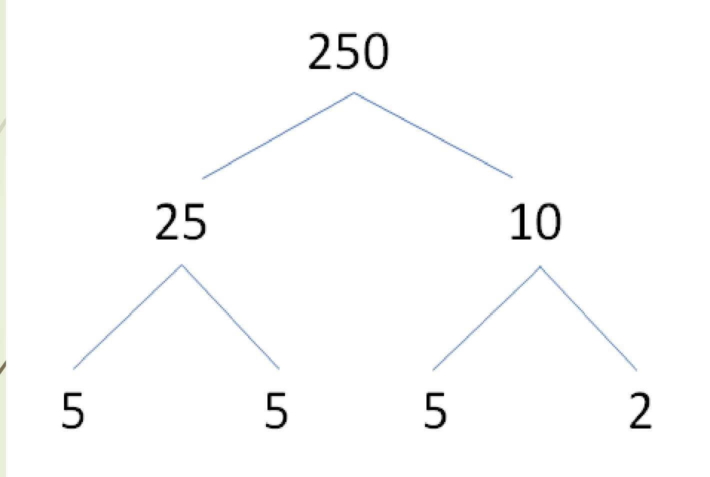
$$(1001)(1000)(999)(998)(997) \ldots (5)(4)(3)(2)(1).$$

Fundamental Theorem of Arithmetic

Fundamental theorem of arithmetic proved by Carl Friedrich Gauss in 1801.

Fundamental theorem of arithmetic states that: Any integer greater than 1 can be expressed as the product of prime numbers in only one way.

Factor Tree for Prime Factorization



$$250 = 5 \times 5 \times 5 \times 2$$

$$250 = 2 \times 5 \times 5 \times 5$$

$$250 = 2 \times 5^3$$

Remark: We can change the order in which the prime factors occur but the set of prime factors is unique.

Euclid Proof Infinity of Number of Primes

1. Assume there are a finite number n of primes $p_i, i = 1, 2, 3, \dots, n$, i.e. $p_1, p_2, p_3, \dots, p_n$, where the largest prime is p_n.
2. Consider the number that is the product of these, plus one:

   $$N = p_1 p_2 p_3 \dots p_n + 1$$

3. Divide N by $p_1, p_2, p_3, \dots, p_n$ leaves a remainder of 1.
4. Hence it is either prime itself, or divisible by another prime greater than p_n, contradicting the assumption.
5. Therefore, we reject the assumption of the largest prime and conclude that the number of primes is infinite.

Mersenne Primes

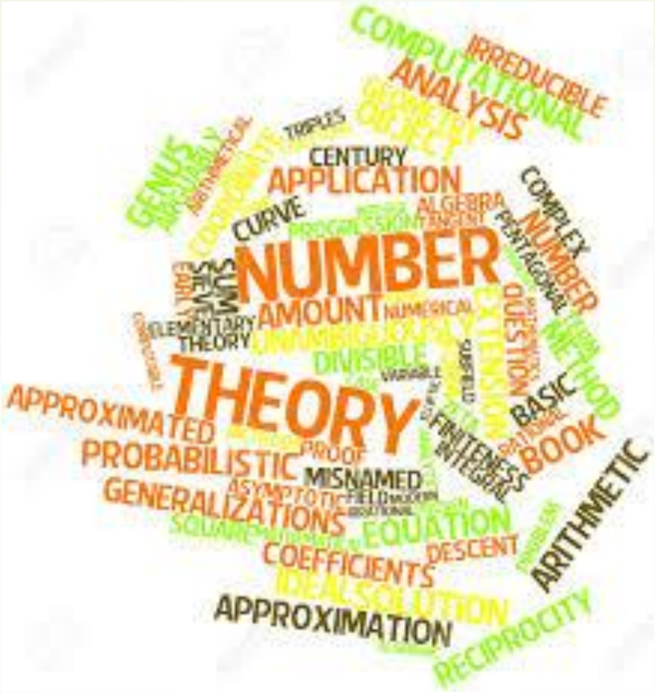
At the beginning of the 17$^{\text{th}}$ century, French monk Marin Mersenne defined the prime numbers $M_p = 2^p - 1$, where p is a prime number. Mersenne prime numbers are named for his name.

Mersenne Primes (cont.)

In 1996, George Woltman, from the Massachusetts Institute of Technology (MIT) founded the Great Internet Mersenne Prime Search (GIMPS), a distributed computing project that searches for new Mersenne primes and allows any user can participate by downloading the software Prime95, created by Woltman.

Mersenne Primes (cont.)

In 2018, Patrick Laroche of the Great Internet Mersenne Prime Search (GIMPS) found the largest known prime number $2^{82,589,933} - 1$, a number which has 24,862,048 digits when written in base 10.



Practice 4.2 (page 11)

Divisibility

Definition 8: Let $a, b \in I$ and $a \neq 0$, a ***divides*** b if there is an integer k such that $b = ak$. This is denoted by $a|\, b$.

A consequence of this definition is that b is ***divisible*** by a (without remainder). Alternative terms for a ***divides*** b are: a is a ***divisor*** of b, or a is a ***factor*** of b, or b is a ***multiple*** of a. The symbol $a \nmid b$ means a ***does not divide*** b.

Divisibility (cont.)

Property 1: If $a|\ b$ and $a|\ c$, then $a|\ (b+c)$.

Proof: Since $a|\ b$, there exists an integer k_1 such that $b = ak_1$ (Def. of divisor) … (1)

Since $a|\ c$, there exists an integer k_2 such that $c = ak_2$ (Def. of divisor) … (2)

(1)+ (2); $b + c = ak_1 + ak_2$ (Addition property)

$= a(k_1 + k_2)$ (Distributive law for addition)

Since, $k_1 + k_2$ is an integer (Closure law for addition)

Then, $a|\ (b+c)$. (Def. of divisor) #

Divisibility (cont.)

Property 2: If $a|\, b$ and $a|\, c$, then $a|\, bc$.

Property 3: If $a|\, b$ and $b|\, c$, then $a|\, c$.

Property 4: If $a|\, b$ and $a|\, c$, then $a|\, (mb + nc)$ whenever m and n are integers.

Practice

The Number of Divisors of a Natural Number

No.	Divisor/Factor	No. of Divisors/Factors	Factorization
15	1, 3, 5, 15	4	3×5
30	1, 2, 3, 5, 6, 10, 15, 30	8	$2 \times 3 \times 5$
60	1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60	12	$2^2 \times 3 \times 5$
144	1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 36, 48, 72, 144	15	$2^4 \times 3^2$

The Number of Divisors of a Natural Number (cont.)

The number of divisors or factors is found for the following rule:

Let the natural number N have the factorization

$$N = p^a q^b r^c \ldots$$

Where $p, q, r, \ldots$ are the prime factors raised to the powers $a, b, c, \ldots$, respectively. The number of divisors of N, denoted by $d(N)$, is found by the formula

$$d(N) = (a+1)(b+1)(c+1)\ldots$$

The Number of Divisors of a Natural Number (cont.)

Example

$144 = 2^4 \times 3^2$

Since, $p = 2, q = 3, a = 4, b = 2$

Then, $d(144) = (4 + 1)(2 + 1) = 15$ #

The Sum of the Divisor

Let the natural number N have the factorization: $N = p^a q^b r^c \ldots$

Where $p, q, r, \ldots$ are the prime factors raised to the powers $a, b, c, \ldots$, respectively. The sum of divisors of N, denoted by $\sigma(N)$, is found by the formula

$$\sigma(N) = (p^0 + p^1 + p^2 + \cdots + p^a)(q^0 + q^1 + q^2 + \cdots + q^b)(r^0 + r^1 + r^2 + \cdots + r^c) \ldots$$

or

$$\sigma(N) = (1 + p^1 + p^2 + \cdots + p^a)(1 + q^1 + q^2 + \cdots + q^b)(1 + r^1 + r^2 + \cdots + r^c) \ldots$$

The Sum of the Divisor (cont.)

Example 1: $30 = 2 \times 3 \times 5$

$$\sigma(30) = (1+2)(1+3)(1+5) = 3 \times 4 \times 6 = 72$$

Check the divisors from Table 4.4: $1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 = 72$ #

Example 2: $144 = 2^4 \times 3^2$

$$\sigma(144) = (1 + 2 + 2^2 + 2^3 + 2^4)(1 + 3 + 3^2) = 31 \times 13 = 403$$

Check the divisors from Table 4.4:

$1 + 2 + 3 + 4 + 6 + 8 + 9 + 12 + 16 + 18 + 24 + 36 + 48 + 72 + 144 = 403$ #

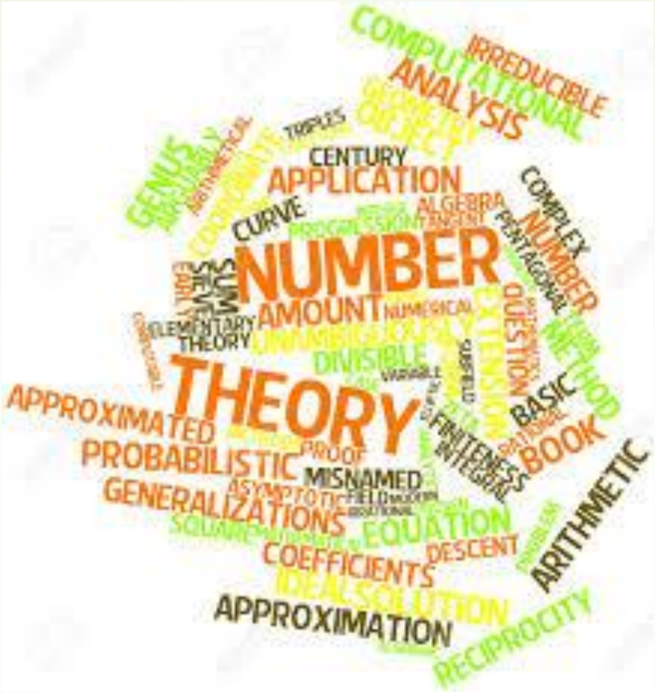
The Sum of the Divisor (cont.)

Remark: The formula for $\sigma(N)$ involves not only the exponents but also the prime factors themselves.

$$N = p^a q^b r^c \ldots$$

$$d(N) = (a+1)(b+1)(c+1)\ldots$$

$$\sigma(N) = (1 + p^1 + p^2 + \cdots + p^a)\left(1 + q^1 + q^2 + \cdots + q^b\right)(1 + r^1 + r^2 + \cdots + r^c)\ldots$$



Practice 4.3 (page 13)

Q & A

END