A Miscellany of items in Number Theory

"Mathematics is the queen of science, and arithmetic the queen of mathematics." – Carl Friedrich Gauss (1777 - 1855)

Arithmetic - meaning: Number Theory

Handout: List of prime numbers up to 5,000

Calculators, scribble pads/notebooks should be brought to the talk.

Items marked Note should be entered in your paper notepad for retention

Items not so noted may also be Noted in your Notepad but could be entered in your scribble pad

Do you know how to find out if a number is divisible by 2, 3, 5, 9, 11?

Preliminaries

Inequality symbols

Brackets

Set, sequence

Fundamental Theorem of Arithmetic (unique factorization Theorem)

Mersenne numbers and Mersenne primes

Amicable numbers

Sociable numbers

Euclid's algorithm for finding the gcd (greatest common divisor) of two numbers (Important)

Pascal's Triangle

Factorial - Combinations and Permutations

Binomial Theorem or Binomial expansion (Note)

Do you know how to find the square root of a number - without a calculator? (Note)

Fermat's Little Theorem – involves modular arithmetic

Series (Note)

Series can be continued.

Preliminaries

In Mathematics letters are used to indicate unknown or unspecified quantities, e.g., n, p, x, y etc.

n - usually denotes a number

p - usually denotes a prime number - particularly in Number Theory

x, y - are general letters for unknown quantities or variables

In Mathematics one frequently uses subscripts and superscripts to the letters, e.g., p_7 may denote the seventh prime number, 13.

Then too a superscript often denotes the 'power' of a number - it is called the 'exponent', e.g., p_7^2 means p_7 squared, i.e., $13^2 = 169$.

But often too, a superscript just refers to a member of another set of quantities.

For example in x_4^2 the superscript 2 may refer to the navy where $1, 2, 3$ refer respectively to the army, navy and air force and the subscript 4 may mean the fourth in line so that x_4^2 would stand for a line of navy personnel (the 2) and x_4 would stand for the 4^{th} person (say from the left) in the line of navy personnel.

What is 2^1? What is 2^0? What is 2^{-1}?

Inequality symbols

$<$ - less than, $3 < 4$

$\leq$ - less than or equal to $3 \leq 3$, $3 \leq 4$

$>$ - greater than $4 > 3$

$\geq$ - greater than or equal to $3 \geq 3$, $4 \geq 3$

Modulus

If x is a number, mod x, written $|x|$ is the positive value of x. For example $|-3.2| = 3.2 = |3.2|$.

Then, for example $1 - |x| \geq 0$ means $|x| \leq 1$ that is, $-1 \leq x \leq 1$.

Brackets

There are three types of brackets:

( ) - parentheses

{ } - braces - also called curly brackets

[ ] - square brackets

Set, sequence

The elements of a **set** are *always* enclosed in braces, e.g. {23, elephant, Morrison, apple}, {a, is, Trump, moron} - the order of the elements is immaterial.

A sequence, is an ordered set of elements, e.g., $\{1, 1, 2, 3, 5, 8, 13, 21, 34, ...\}$ - braces may also be used.

The three dots ... called an *ellipsis*, means 'and so on' - which may continue to a finite number or to infinity.

A series is a sum of numbers, e.g., $1 + 10 + 100 + 1000 + \cdots$ (Notice the dots here are in the middle which means continuing addition of terms or numbers.

Fundamental Theorem of Arithmetic (unique factoriztion Theorem)

Every number greater than 1 is either a prime or a product of prime numbers − the product is unique, apart from the order of the factors.

For example $600 = 2.300 = 2^2.150 = 2^3.75 = 2^3.3.25 = 2^3.3.5^2 = 3.2^3.5^2$ etc.

Perfect number

Written By: The Editors of Encyclopaedia Britannica See Article History

Perfect number: a positive integer that is equal to the sum of its proper divisors. The smallest perfect number is 6, which is the sum of 1, 2, and 3. Other perfect numbers are ? ? ?. The discovery of such numbers is lost in prehistory. It is known, however, that the Pythagoreans (founded c. 525 bce) studied perfect numbers for their "mystical" properties.

Perfect numbers and Mersenne numbers

Most numbers are either "abundant" or "deficient." In an abundant number, the sum of its proper divisors (i.e., including 1 but excluding the number itself) is greater than the number; in a deficient number, the sum of its proper divisors is less than the number. The mystical tradition was continued by the Neo-Pythagorean philosopher Nicomachus of Gerasa (fl. c. 100 ce), who classified numbers as deficient, perfect, and superabundant according to whether the sum of their divisors was less than, equal to, or greater than the number, respectively. Nicomachus gave moral qualities to his definitions, and such ideas found credence among early Christian theologians. Often the 28-day cycle of the Moon around the Earth was given as an example of a "Heavenly," hence perfect, event that naturally was a perfect number. The most famous example of such thinking is given by St. Augustine, who wrote in The City of God (413–426):

Six is a number perfect in itself, and not because God created all things in six days; rather, the converse is true. God created all things in six days because the number is perfect.

The earliest extant mathematical result concerning perfect numbers occurs in Euclid's Elements (c. 300 bce), where he proves the proposition:

If as many numbers as we please beginning from a unit [1] be set out continuously in double proportion, until the sum of all becomes a prime, and if the sum multiplied into the last make some number, the product will be perfect.

Here "double proportion" means that each number is twice the preceding number, as in $1, 2, 4, 8, \ldots$.

For example, $1 + 2 + 4 = 7$ is prime; therefore, $7 \times 4 = 28$ ("the sum multiplied into the last") is a perfect number.

Euclid's formula forces any perfect number obtained from it to be even, and in the 18th century the Swiss mathematician Leonhard Euler showed that any even perfect number must be obtainable from Euclid's formula.

It is not known whether there are any odd perfect numbers.

The Editors of Encyclopaedia Britannica

Numbers of the form

$$2^{p-1}(2^p - 1) \qquad p \text{ prime}$$

are *perfect numbers.* This can be proved from knowing the sum of a G.P. (geometric progression).

All even perfect numbers are of this type.

No odd perfect numbers have been found !

Mersenne numbers and Mersenne primes

Numbers of the form

$$M_n = 2^n - 1 \qquad p \text{ prime}$$

are called *Mersenne numbers*. In n is a prime p

$$M_p = 2^p - 1 \qquad p \text{ prime}$$

and if M_p is prime it is called a $Mersenne$ prime.

Mersenne implied that the only values of p, not greater than 257, for which $2^p - 1$ is prime are

$$p = 2, 3, 5, 7, 13, 17, 19, 31, \mathbf{67}, 127, 257.$$

For the numbers

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$$

$2^p - 1$ is certainly a prime number.

For all other primes not exceeding 257, Mersenne numbers are composite except perhaps for some of the following six values:

$$137, 167, 193, 199, 227, 229$$

for which the character of $2^p - 1$ is unknown (at the time 1939).

Without finding a factor, Lucas demonstrated that M_{67} *is actually composite. No factor was found until a famous talk by Frank Nelson Cole in1903.*

Without speaking a word, he went to a blackboard and raised 2 to the 67th power, then subtracted one.

On the other side of the board, he multiplied $193,707,721 \times 761,838,257,287$ *and got the same number,*

then returned to his seat (to applause) without speaking!!

He later said that the result had taken him "three years of Sundays" to find. A correct list of all Mersenne primes in this number range was completed and rigorously verified only about three centuries after Mersenne published his list.

As of December 2018, 51 Mersenne primes are now known. The largest known prime number $2^{282,589,933} - 1$ is a Mersenne prime. Since 1997, all newly found Mersenne primes have been discovered by the Great Internet Mersenne Prime Search (GIMPS), a distributed computing project on the Internet.

Amicable numbers

If a and b are two numbers where the divisors of a add up to b and the divisors of b add up to a, then a and b are *amicable numbers*.

Try the numbers 220 and 284.

Sociable numbers

A chain of numbers is said to be *sociable* if the sum of the divisors of any number in the chain is equal to the next number in the chain and the divisors of the last number sum up to the first number in the chain.

For example

$$14,288 \quad 15,472 \quad 14,536 \quad 14,264 \quad 12,496$$

is a sociable chain.

Euclid's algorithm for finding the gcd (greatest common divisor) of two numbers (Important)

Given numbers a, b find the gcd of them. If d is the gcd of a and b this is written $(a, b) = d$. If $d = 1$, a and b are said to be *relatively prime* - they have no factor in common, except 1.

Find the gcd of $78,696$ and $19,332$.

$$\begin{array}{lllll} 14 & 19332 & 78696 & 4 \\ & \underline{19152} & \underline{77328} & \\ & 180 & 1368 & \end{array}$$

Pascal's Triangle

Triangle0

Before getting to the identities that we will use to tame binomial coefficients, let's take a peek at some small values. The numbers in Table 155 form the beginning of *Pascal's triangle*, named after Blaise Pascal (1623–1662)

Table 155 Pascal's triangle.

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$	$\binom{n}{8}$	$\binom{n}{9}$	$\binom{n}{10}$
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1

1.jpg

Factorial - Combinations and Permutations

$$n! = 1.2.3\ldots n \qquad \text{e.g. } 4! = 1.2.3.4 = 24$$
$$\binom{n}{r} = C_r^n = \frac{n!}{r!(n-r)!} \qquad P_r^n = \frac{n!}{r!(n-r)!}$$

How many ways can I select two items from 5 irrespective of their order. Let S={a,b,c,d,e}, so $n = 5$ and $r = 2$. We have

ab,ac,ad,ae,bc,bd,be,cd,ce,de. Note we do not count ba as the order of ab and ba is immaterial and only one is considered.

There are 10 ways to make the selection of 2 out of 5, as shown above. This is 'the number of *Combinations* of taking 2 items out of 5 - irrespective of the order of the items'. It is given by

$$\binom{5}{2} = \frac{5!}{2!(5-2)!} = \frac{1.2.3.4.5}{1.2 \times 1.2.3} = 10.$$

When order does matter, we have the number of Permutations of r items from n, given by the formula $P_r^n = \frac{n!}{(n-r)!}$. Ordering 2 out of 5 items there are 20 possibilities (the 10 above and 10 more with the letters reversed)

$$P_2^5 = \frac{5!}{(5-2)!} = \frac{5!}{3!} = 4.5 = 20.$$

We have the formula, easily verified in the table of Pascal's Triangle

$$\binom{n}{r} + \binom{n}{r+1} = \binom{n+1}{r+1}$$

Exercise: Verify this formula.

Binomial Theorem or Binomial expansion

Calculate $(a+b)^2 = (a+b).(a+b)$

$$\begin{array}{r} a+b \\ \underline{a+b} \\ a^2+ab \\ \quad ba+b^2 \\ a^2+2ab+b^2 \end{array}$$

Calculate $(a+b)^3$

triangle2

$$(a+b)^0 = 1$$
$$(a-b)^1 = a+b$$
$$(a+b)^2 = a^2+2ab+b^2$$
$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$$
$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$$
$$(a+b)^5 = a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$$

$_2.png$