

Some Exercises in Recreational Arithmetics

R. G. Panday (e-mail: romes_12000@yahoo.com)

Abstract: This paper was written with the purpose of communicating a few new things: proof of the Beal conjecture and new approach to Goldbach's conjecture amongst others along with few other new theorems and conjectures as well as the publication of a new deterministic test for general primes. To connect them together the paper is written as a tutorial.

Contents

1. Introduction

2. Factorization

3. Congruences

4. Fractions

5. Divisibility and modularity

6. Continued fractions and series

7. Factorials

8. Figurate numbers or polygonal (n-gonal) numbers

9. More on polynomial numbers

10. Prime number theorems

11. Primality tests

Appendix

1. Introduction

In **elementary number theory**, integers are studied without use of techniques from other mathematical fields. We are usually concerned with the properties of the integers, or

whole numbers: $Z = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$.

Questions of divisibility, use of the Euclidean algorithm to compute greatest common divisors, integer factorizations into prime numbers, investigation of perfect numbers and congruences belong here. Several important discoveries of this field are Fermat's little theorem, Euler's theorem, the modular and polynomial remainder theorems and the law of quadratic reciprocity. The properties of multiplicative functions such as the Möbius function and Euler's φ function, integer sequences, factorials, and Fibonacci numbers all also fall into this area. Many questions in number theory can be stated in elementary number theoretic terms, but they may require very deep consideration and new approaches outside the realm of elementary number theory to solve. Examples include:

- Goldbach's conjecture concerning the expression of even numbers as sums of two primes.
- Mihăilescu's theorem or Catalan's conjecture, regarding successive integer powers.
- The twin prime conjecture about the infinitude of prime pairs.
- The Collatz conjecture concerning a simple iteration.
- Fermat's Last Theorem (stated in 1637, but not proven until 1994) concerning the impossibility of finding nonzero integers x, y, z such that $x^n + y^n = z^n$ for some integer n greater than 2.
- The theory of Diophantine equations has even been shown to be *undecidable*.

In **algebraic number theory**, the concept of a number is expanded to the algebraic numbers which are roots of polynomials with rational coefficients. These domains contain elements analogous to the integers, the so-called algebraic integers. In this setting, the familiar features of the integers (e.g. unique factorization) need not hold. The virtue of the machinery employed—Galois theory, group cohomology, class field theory, group representations and L-functions—is that it allows one to recover that order partly for this new class of numbers.

Many number theoretic questions are best attacked by studying them *modulo* p for all primes p . This leads to the construction of the p -adic numbers; this field of study is called local analysis and it arises from algebraic number theory.

Diophantine Equations

Diophantine equation is an indeterminate polynomial equation that allows the variables to be integers only. Examples of Diophantine equations (x, y , and z are the unknowns, the other letters being given are constants):

- $ax + by = 1$ A linear Diophantine equation.
- $x^n + y^n = z^n$ for $n = 2$ there are infinitely many solutions (x, y, z) , the Pythagorean triples, which are generated by the formulas $l^2 - m^2$, $2ml$, and $l^2 + m^2$, (and n are two positive integers, with $m < l$)

	m=1	2	3	4	5	6	7	8	9
N=1	[3,4,5]								
n=3	[8,6,10]	[5,12,13]							
n=4	[15,8,17]	[12,16,20]	[7,24,25]						
n=5	[24,10,26]	[21,20,29]	[16,30,34]	[9,40,41]					
n=6	[35,12,37]	[32,24,40]	[27,36,45]	[20,48,52]	[11,60,61]				
n=7	[48,14,50]	[45,28,53]	[40,42,58]	[33,56,65]	[24,70,74]	[13,84,85]			
n=8	[63,16,65]	[60,32,68]	[55,48,73]	[48,64,80]	[39,80,89]	[28,96,100]	[15,112,113]		
n=9	[80,18,82]	[77,36,85]	[72,54,90]	[65,72,97]	[56,90,106]	[45,108,117]	[32,126,130]	[17,144,145]	
n=10	[99,20,101]	[96,40,104]	[91,60,109]	[84,80,116]	[75,100,125]	[64,120,136]	[51,140,149]	[36,160,164]	[19,180,181]

- For larger values of n , Fermat's Last Theorem states that no positive integer solutions (x, y, z) satisfying the equation exist.
- $x^2 + y^2 = \pm 1$ Pell's equation, after John Pell. First studied by Brahmagupta in the 7th century, also by Fermat in the 17th century.

- $\frac{4}{n} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}$ the Erdős–Straus conjecture states that, for every positive integer $n \geq 2$, there exists a solution with x, y , and z all positive integers. Although not usually stated in polynomial form, this example is equivalent to the polynomial equation $4xyz = yzn + xzn + xyn = n(yz + xz + xy)$.

History of study of Diophantine Equations

Number theory was a favorite study among the Greek mathematicians of the late Hellenistic period (3rd century AD) in Alexandria, who were aware of the Diophantine equation concept in numerous special cases. The first Greek mathematician to study these equations was Diophantus.

Diophantus also looked for a method of finding integer solutions to linear indeterminate equations, equations that lack sufficient information to produce a single discrete set of answers. The equation $x + y = 5$ is such an equation. Diophantus discovered that many indeterminate equations can be reduced to a form where a certain category of answers is known even though a specific answer is not.

Diophantine equations were extensively studied by mathematicians in medieval India, who were the first to systematically investigate methods for the determination of integral solutions of Diophantine equations. Aryabhata (499) gave the first explicit description of the general integral solution of the linear Diophantine equation $ay + bx = c$, which occurs in his text *Aryabhatiya*. This *kuttaka* algorithm is considered to be one of the most significant contributions of Aryabhata in pure mathematics, which found solutions to Diophantine equations by means of continued fractions. The technique was applied by Aryabhata to give integral solutions of simultaneous linear Diophantine equations, a problem with important applications in astronomy. He also found the general solution to the indeterminate linear equation using this method.

Brahmagupta in 628 handled more difficult Diophantine equations. He used the *chakravala* method to solve quadratic Diophantine equations, including forms of Pell's equation, such as $61x^2 + 1 = y^2$. His *Brahma Sphuta Siddhanta* was translated into Latin in 1126. The equation $61x^2 + 1 = y^2$ was later posed as a problem in 1657 by the French mathematician Pierre de Fermat. The general solution to this particular form of Pell's equation was found over 70 years later by Leonhard Euler, while the general solution to Pell's equation was found over 100 years later by Joseph Louis Lagrange in 1767. Meanwhile, the general solution to Pell's equation was recorded by Bhaskara II in 1150, using a modified version of Brahmagupta's *chakravala* method, which he also used to find the general solution to other indeterminate quadratic equations and quadratic Diophantine equations. Bhaskara's *chakravala* method for finding the general solution to Pell's equation was much simpler than the method used by Lagrange over 600 years later. Bhaskara also found solutions to other indeterminate quadratic, cubic, quartic, and higher-order polynomial equations. Narayana Pandit further improved on the *chakravala* method and found more general solutions to other indeterminate quadratic and higher-order polynomial equations.

Solutions of linear Diophantine equations

Consider the general linear Diophantine equation

$$ax + by = c$$

where a , b and c are integers. Assume that a and b are both non-zero (so the equation genuinely involves two variables). Let

$$d = \gcd(a, b).$$

Then d divides both a and b so we may write

$$a = da_1 \text{ and } b = db_1 \text{ for some integers } a_1 \text{ and } b_1.$$

Suppose that we do have a solution (x_0, y_0) to the equation. This means

$$ax_0 + by_0 = c. \text{ Now since } d \text{ divides } a \text{ and } b, \text{ we deduce } d \mid (ax_0 + by_0); \text{ that is, } d \mid c.$$

Conversely suppose $d \mid c$. Write $c = dc_1$.

There exist integers u and v such that

$$d = ua + vb.$$

Upon multiplying c_1 we obtain $uac_1 + vbc_1 = dc_1$;

that is, $a(uc_1) + b(vc_1) = c$. Therefore (uc_1, vc_1) is a solution of the equation. Conclusion: The equation has a solution if and only if $d \mid c$.

Example to find all solutions of $77x + 42y = 35$, first $\gcd(77, 42)$ using the Euclidean algorithm:

$$77 = 42 \cdot 1 + 35$$

$$42 = 35 \cdot 1 + 7$$

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

$$\text{So } \gcd(77, 42) = 7.$$

Since 7 does divide 35, this means that the linear Diophantine equation has integer solutions.

To find the solutions first reverse the steps in the Euclidean Algorithm:

$$7 = 42 - 35$$

$$= 42 - (77 - 42)$$

$$= (-1) \cdot 77 + 2 \cdot 42.$$

So we take $u = -1$ and $v = 2$. One solution is then $x_0 = (-1) \cdot 35/7 = -5$, $y_0 = 2 \cdot 35/7 = 10$. All the solutions are given by
 $x = x_0 + (42/7)t = -5 + 6t$
 $y = y_0 - (77/7)t = 10 - 11t$
 where $t \in \mathbb{Z}$.

Theorem

Let a and b be coprime positive integers.
 Then every number $c \geq a \cdot b$ can be expressed as $\lambda a + \mu b$ with λ and μ non-negative integers.

Composition Theorem

Given a quadratic form

$$Q(x,y) = x^2 + y^2$$

then

$$Q(x,y) \cdot Q(x', y') = Q(x \cdot x' - y \cdot y', x' \cdot y + x \cdot y') = (x^2 + y^2) \cdot (x'^2 + y'^2) = (x \cdot x' - y \cdot y')^2 + (x' \cdot y + x \cdot y')^2 = x^2 \cdot x'^2 + y^2 \cdot y'^2 + x'^2 \cdot y^2 + x^2 \cdot y'^2$$

Fundamental theorem of arithmetic

Every positive integer $n > 1$ can be expressed as a product of primes

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r}$$

where p_1, p_2, \dots, p_n are distinct primes and a_1, a_2, \dots, a_n are positive integers. This factoring is unique apart from the order of the prime factors.

A number N is perfect if the sum of its divisors, including 1 but excluding itself, add up to N .

So, for example, 28 is perfect because $1 + 2 + 4 + 7 + 14 = 28$.

Conjecture : There is no odd perfect number.

Square of Squares

A square is magic if each of the rows, columns, and diagonals add up to the same total. So, for example, the square

25 4 19

10 16 22

13 28 7

is magic, since every row, column, and diagonal adds up to 48. Of the nine entries, three (4, 16 and 25) are perfect squares.

The problem is to find a 3 by 3 magic square all of whose entries are distinct perfect squares, or prove that such a square cannot exist.

Euler Brick

An Euler Brick is just a cuboid, or a rectangular box, in which all of the edges (length, depth, and height) have integer dimensions; and in which the diagonals on all three sides are also integers.

So if the length, depth and height are a , b , and c respectively, then a , b , and c are integers, as are the quantities $\sqrt{a^2+b^2}$ and $\sqrt{b^2+c^2}$ and $\sqrt{c^2+a^2}$.

The problem is to find a four dimensional Euler Brick, in which the four sides a , b , c , and d are integers, as are the six face diagonals $\sqrt{a^2+b^2}$ and $\sqrt{a^2+c^2}$ and $\sqrt{a^2+d^2}$ and $\sqrt{b^2+c^2}$ and $\sqrt{b^2+d^2}$ and $\sqrt{c^2+d^2}$, or prove that such a cuboid cannot exist .

Grimm conjecture

Grimm's conjecture states that to each element of a set of consecutive composite numbers one can assign a distinct prime that divides it.

For example, for the range 242 to 250, one can assign distinct primes as follows:

242: 11 243: 3 244: 61 245: 7 246: 41 247: 13 248: 31 249: 83 250: 5

Legendre's Conjecture

Legendre's Conjecture states that there is at least one prime number between every pair of consecutive squares.

Between 13^2 (=169) and 14^2 (=196) there are five primes (173, 179, 181, 191, and 193); between 30^2 (=900) and 31^2 (=961) there are eight primes (907, 911, 919, 929, 937, 941, 947, and 953); between 35^2 (=1225) and 36^2 (=1296) there are ten primes (1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, and 1291).

definition

The abundancy of n is the rational number $\sigma(n) / n$, in which σ denotes the divisor function (the sum of all divisors). n is a friendly number if there exists $m \neq n$ such that $\sigma(m) / m = \sigma(n) / n$. Note that abundancy is not the same as abundance which is defined as $\sigma(n) - 2n$.

If n is a positive natural number, $\sigma(n)$ is the sum of its divisors. For example, 10 is divisible by 1, 2, 5, and 10, and so $\sigma(10) = 1 + 2 + 5 + 10 = 18$.

The abundancy of n can also be written as $\sigma_{-1}(n) = \sigma(n) / n = \sigma_1(n) / n$, where σ is the divisor function.

Numbers are mutually friendly if they share their abundancy. For example, 6, 28 and 496 all have abundancy 2. They are all perfect numbers, and therefore mutually friendly. As another example, (30, 140) is a friendly pair, because 30 and 140 have the same abundancy:

$$\sigma(30) / 30 = 1+2+3+5+6+10+15+30 / 30 = 12/5$$

$$\sigma(140) / 140 = 1+2+3+5+7+10+14+20+28+35+70+140 / 140 = 12/5$$

Being mutually friendly is an equivalence relation, and thus induces a partition of the positive naturals into "clubs" (equivalence classes) of mutually friendly numbers.

Theorem (Arithmetic-Mean-Geometric-Mean Inequality)

Let a_1, a_2, \dots, a_n be nonnegative real numbers. Then

$$\sqrt[n]{a_1 a_2 \dots a_n} \leq \frac{a_1 + a_2 + \dots + a_n}{n}$$

Theorem (Euclid).

The number of primes is infinite.

Proof. Suppose there were only a finite number of primes p_1, p_2, \dots, p_r . Then form the integer $n = 1 + p_1 p_2 \dots p_r$

Since $n > p_i$ for all i , it must be composite. Let q be the smallest prime factor of n . As p_1, p_2, \dots, p_r represent all existing primes, then q is one of them, say $q = p_1$ and $n = p_1 m$. Now we can write

$$1 = n - p_1 p_2 \dots p_r = p_1 m - p_1 p_2 \dots p_r = p_1 (m - p_2 \dots p_r):$$

We see that $p_1 > 1$ is a factor of 1, which is a contradiction.

Theorem

(Bertrand's Postulate, proved by Chebyschef). For every positive integer $n > 1$ there is a prime

p such that $n < p < 2n$.

Theorem

Let p_i be the i^{th} prime. Then

$$\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_n} \rightarrow \infty$$

as $n \rightarrow \infty$.

Twin primes

There are infinitely many primes p such that $p + 2$ is also prime. In 1849 de Polignac made the more general conjecture that for every natural number k , there are infinitely many prime pairs p and p' such that $p' - p = 2k$. The case $k = 1$ is the twin prime conjecture.

The **twin primes conjecture** states that there are an infinite number of pairs of primes of the form $2n-1, 2n+1$. That is, they differ by 2; for example, 41 and 43.

All twin primes except (3, 5) are of the form $6n \pm 1$.

Brun's theorem states that the number obtained by adding the reciprocals of the odd twin primes,

$$B \equiv \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \left(\frac{1}{17} + \frac{1}{19}\right) + \dots,$$

converges to a definite number ("Brun's constant"), which expresses the scarcity of twin primes and for twin primes up to 10^{16} converges to 1.902160583104.

Diophantine equations

An equation which requires integer solutions is called a *diophantine equation*. By the Bachet-Bezout Theorem, we see that the linear diophantine equation $ax+by = c$

has a solution in integers if and only if $(a,b)|c$. The Euclidean Algorithm is an efficient means to find a solution to this equation.

Fermat's infinite descent method was the first general proof of diophantine questions. Fermat's Last Theorem was posed as a problem in 1637, a proof of which wasn't found until 1994. Fermat also posed the equation $61x^2 + 1 = y^2$ as a problem in 1657 and Euler in the eighteenth century found a general solution to the equation $61x^2 + 1 = y^2$. Lagrange found a solution to the more general Pell's equation. Euler and Lagrange solved these Pell equations by means of continued fractions, though this was more difficult than the Indian *chakravala* method.

Around the beginning of the nineteenth century books of Legendre (1798), and Gauss put together the first systematic theories in Europe. Gauss's *Disquisitiones Arithmeticae* (1801) may be said to begin the modern theory of numbers.

The formulation of the theory of congruences starts with Gauss's *Disquisitiones*. He introduced the notation

$$a \equiv b \pmod{c}$$

and explored most of the field. Chebyshev published in 1847 a work on the subject.

Besides summarizing previous work, Legendre stated the law of quadratic reciprocity. This law, discovered by induction and enunciated by Euler, was first proved by Legendre in his *Théorie des Nombres* (1798) for special cases. Independently of Euler and Legendre, Gauss discovered the law about 1795, and was the first to give a general proof. The following have also contributed to the subject: Cauchy; Dirichlet whose *Vorlesungen über Zahlentheorie* is a classic; Jacobi, who introduced the Jacobi symbol; Liouville, Zeller, Eisenstein, Kummer, and Kronecker. The theory extends to include cubic and quartic reciprocity, (Gauss, Jacobi who first proved the law of cubic reciprocity, and Kummer).

To Gauss is also due the representation of numbers by binary quadratic forms.

Cauchy, Poinsoot (1845), and notably Hermite have added to the subject. Smith gave a complete classification of ternary quadratic forms, and extended Gauss's researches concerning real quadratic forms to complex forms. The investigations concerning the representation of numbers by the sum of 4, 5, 6, 7, 8 squares were advanced by Eisenstein and the theory was completed by Smith. Dirichlet proved Fermat's Last Theorem:

$$x^n + y^n \neq z^n \quad (x, y, z \neq 0, n > 2)$$

for the cases $n = 5$ and $n = 14$ (Euler and Legendre had already proved the cases $n = 3$ and $n = 4$ and therefore by implication, all multiples of 3 and 4).

Theorem Prove that if a, b, n are positive integers, then

$$(a, b) = (a + nb, b).$$

Proof: Set $d = (a, b), c = (a + nb, b)$. As $d|a, d|b$, it follows that $d|(a + nb)$. Thus d is a common divisor of both $(a + nb)$ and b . This implies that $d|c$. On the other hand, $c|(a + nb), c|b$ imply that $c|((a + nb) - nb) = a$. Thus c is a common divisor of a and b , implying that $c|d$. This completes the proof.

Theorem (Frobenius)

Let a, b be positive integers. If $(a, b) = 1$ then the number of positive integers m that cannot be written in the form $ar + bs = m$ for nonnegative integers r, s equals $(a-1)(b-1)/2$.

Theorem

Let a, b be relatively prime positive integers. Then the equation $ax + by = n$ is unsoluble in nonnegative integers x, y for $n = ab - a - b$. If $n > ab - a - b$, then the equation is soluble in nonnegative integers.

irreducibility

Example: We consider the equation:

$$\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}$$

for factor (x^5-1) we obtain the normal form (reduce the the rational function to the lowest terms) : $(x - 1)(x^4 + x^3 + x^2 + x + 1)$

To factor the polynomial with rational coefficients into irreducible factors over the ring of integers, . for example for $(x^{12}-1)$, will not give

$$(x - 1)(x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

, but:

$$(x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)(x^2 + 1)(x^4 - x^2 + 1)$$

$$(x - 1) \left(\sum_{i=0}^{p-1} x^i \right)$$

If $n=p$, is a prime, then *factor* (x^p-1) will always give

. Hence the

$$\sum_{i=0}^{p-1} x^i$$

polynomial must be irreducible.

Gaussian integer

A **Gaussian integer** is a complex number whose real and imaginary part are both integers. The Gaussian integers, with ordinary addition and multiplication of complex numbers, form an integral domain, usually written as $\mathbf{Z}[i]$. The Gaussian integers are a special case of the quadratic integers. This domain does not have a total ordering that respects arithmetic.

Gaussian integers are the set $\mathbf{Z}[i] = \{a + b i \mid a, b \text{ elements of } \mathbf{Z}\}$

The *norm* of a Gaussian integer is the natural number defined as

$$N = (a + bi)(a - bi) = a^2 + b^2 .$$

One definition of the norm of a Gaussian integer is its complex modulus

$$|a - i b| = \sqrt{a^2 + b^2} .$$

("a-bi" is the complex conjugate of a + bi.)

The norm is multiplicative, i.e.

$$N(z.w) = N(z).N(w)$$

The units of $\mathbf{Z}[i]$ are thus precisely those elements with norm 1, i.e. the elements ± 1 and $\pm i$.

Gaussian integers can be uniquely factored in terms of other Gaussian integers (known as Gaussian primes) up to powers of i and rearrangements.

Interestingly, 17 is no longer prime, as it is the product of $4+i \times 4-i$. Yet $4+i$ is prime. It has a norm of 17, and if it were the product of x and y , the norm of x times the norm of y would equal 17. Yet 17 is still prime in the positive integers, so we can't have $|x| \times |y| = 17$, unless x or y is trivial, with norm 1. Thus $4+i$ and $4-i$ are both prime in the gaussian integers.

Theorem:

$$n^2 < 2^n \quad \text{for } n \geq 5$$

Proof: The statement holds for $n=5$. Assume that for a number $n \geq 5$ there holds $n^2 < 2^n$. We show that for $(n+1)$: $(n+1)^2 < 2^{n+1}$:

$$(n+1)^2 = n^2 + 2n + 1 < n^2 + 4n + 2 + n^2 = 2.n^2 < 2.2^n \quad ,$$

So : $(n+1)^2 < 2^{n+1}$ with which the proof has been completed.

as a consequence of above example $n^2 < 2^n$ for $n \geq 5$

$$(n+1)^2 < 2^n \quad \text{for each natural number } n \geq 6.$$

Proof: The statement holds for $n=6$. Assume that for a number $n \geq 6$ there holds $(n+1)^2 < 2^n$. We show that for $(n+1)$: $(n+2)^2 < 2^{n+1}$:

$$(n+2)^2 = n^2 + 4n + 4 < n^2 + 4n + 2 + n^2 = 2.(n+1)^2 < 2.2^n \quad ,$$

So : $(n+2)^2 < 2^{n+1}$ with which the proof has been completed.

Theorem :

$$a + a.r + \dots + a.r^n = a \frac{1 - r^{n+1}}{1 - r} \quad \text{for } a \in \mathbf{R}, r \in \mathbf{R} \setminus \{1\}$$

Proof: The equation holds for $n=0$. We assume it also holds for $n \geq 0$. Then for $n+1$:

$$a + a.r + \dots + a.r^n = a \frac{1 - r^{n+1}}{1 - r} + a.r^{n+1} = a \frac{1 - r^{n+1} + r^{n+1} - r^{n+2}}{1 - r} = a \frac{1 - r^{n+2}}{1 - r}$$

with which the proof is completed.

Theorem:

Let a be a real number with $a > -1$ and $a \neq 0$. For each natural number $n \geq 2$ there holds:

$$(1+a)^n > 1 + n.a \quad (\text{Bernoulli's inequality})$$

Proof: for $n=2$ there holds: $(1+a)^2 = 1+2.a + a^2 > 1 + 2.a$. We assume $(1+a)^n > 1 + n.a$ for each $n \geq 2$. Then: $(1+a)^{n+1} = (1+a).(1+a)^n$. Because $a > -1$ there follows from the induction :

$$(1+a).(1+a)^n > (1+a).(1+n.a) = 1 + (n+1)a + n.a^2. \text{ From this there follows:}$$

$$(1+a)^{n+1} > 1 + (n+1).a \quad \text{with which the proof has been completed.}$$

Collatz conjecture or $3n + 1$ conjecture

Define a function $f(n)$:

$$f(n) = \begin{cases} n/2 & \text{if } n \equiv 0 \pmod{2} \\ 3n+1 & \text{if } n \equiv 1 \pmod{2} \end{cases}$$

(If n =even, divide it by two and if n =odd, multiply by 3 and add 1). Then form a sequence by performing this operation repeatedly, starting with any positive integer, and take the outcome of each step as the input at the next:

$$a_i = \begin{cases} f(a_{i-1}) & \text{if } i > 0 \\ n & \text{if } i = 0 \end{cases}$$

Then this process will eventually reach the number 1, regardless of which positive integer is chosen initially.

$$(\forall n \in \mathbb{N}, \exists i \in \mathbb{N})(a_0 = n, a_i = 1)$$

In other words: Take any positive integer: if the number is even, divide it by two; if the number is odd, triple it and add one (for example, if this operation is performed on 26, the result is 13; if it is performed on 5, the result is 16). Perform this operation repeatedly, beginning with any positive integer, and taking the result at each step as the input at the next. The Collatz conjecture is: this process will eventually reach the number 1, regardless of which positive integer is chosen initially.

Examples:

Starting at 11, the sequence goes 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1.

Starting at 23: 70, 35, 106, 48, 24, 12, 6, 3, 10, 5, 16, 8, 4, 2, 1

Starting at : 72, 36, 18, 9, 28, 14, 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1

Starting with $n = 6$, we get the sequence 6, 3, 10, 5, 16, 8, 4, 2, 1.

and if we take $n = 11$, the sequence gets longer: 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1.

2. Factorization

Any composite number can be presented as a product of prime factors by the single way. For example,

$$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3, \quad 225 = 3 \cdot 3 \cdot 5 \cdot 5, \quad \text{etc.}$$

Consider the number 1463. Look over prime numbers one after another from the table: and stop, if the number is a factor of 1463. According to the divisibility criteria, we see that numbers 2, 3 and 5 aren't factors of 1463. But this number is divisible by 7, really, $1463 : 7 = 209$. By the same way we test the number 209 and find its factor: $209 : 11 = 19$. The last number is a prime one, so the found prime factors of 1463 are: 7, 11 and 19, i.e. $1463 = 7 \cdot 11 \cdot 19$. We can write this as follows:

Number	Factor
1463	7
209	11
19	19

Common factor of some numbers - a number, which is a factor of each of them. For example, numbers 36, 60, 42 have common factors 2 and 3. Among all common factors there is always the greatest one, in our case this is 6. This number is called a ***greatest common factor*** (GCF).

To find a ***greatest common factor*** (GCF) of some numbers it is necessary:

- 1) to express each of the numbers as a product of its *prime factors*, for example: $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$,
- 2) to write *powers of all prime factors* in the factorization as: $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5^1$,
- 3) to write out all *common factors* in these factorizations;
- 4) to take *the least power* of each of them, meeting in the all factorizations;
- 5) to multiply these powers.

Example. Find GCF for numbers: 168, 180 and 3024.

$$168 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 = 2^3 \cdot 3^1 \cdot 7^1,$$

$$180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5^1,$$

$$3024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 = 2^4 \cdot 3^3 \cdot 7^1.$$

Write out the least powers of the common factors 2 and 3 and multiply them: $\text{GCF} = 2^2 \cdot 3^1 = 12$.

Common multiple of some numbers is called a number, which is divisible by each of them. For example, numbers 9, 18 and 45 have as a common multiple 180. But 90 and 360 are also their common multiples. Among all common multiples there is always the least one, in our case this is 90. This number is called a ***least common multiple*** (LCM).

To find a ***least common multiple*** (LCM) of some numbers it is necessary:

- 1) to express each of the numbers as a product of its *prime factors*, for example: $504 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$,
- 2) to write *powers of all prime factors* in the factorization as: $504 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 = 2^3 \cdot 3^2 \cdot 7^1$,
- 3) to write out *all prime factors*, presented at least in one of these numbers;
- 4) to take *the greatest power* of each of them, meeting in the factorizations;
- 5) to multiply these powers.

Example . Find LCM for numbers: 168, 180 and 3024.

$$\text{Solution . } 168 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 = 2^3 \cdot 3^1 \cdot 7^1,$$

$$180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5^1,$$

$$3024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 = 2^4 \cdot 3^3 \cdot 7^1.$$

Write out the greatest powers of all prime factors: $2^4, 3^3, 5^1, 7^1$ and multiply them: $\text{LCM} = 2^4 \cdot 3^3 \cdot 5 \cdot 7 = 15120$.

Example

With the formulas:

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2)$$

$$x^3 - y^3 = (x - y)(x^2 + xy + y^2)$$

We can factorise:

$$\begin{aligned} 64x^3 + 125 &= (4x)^3 + (5)^3 \\ &= (4x + 5)[(4x)^2 - (4x)(5) + (5)^2] \\ &= (4x + 5)[16x^2 - 20x + 25] \end{aligned}$$

and

$$\begin{aligned} 8x^3 - 27 &= (2x)^3 - (3)^3 \\ &= (2x - 3)[(2x)^2 + (2x)(3) + 3^2] \\ &= (2x - 3)(4x^2 + 6x + 9) \end{aligned}$$

Etc.

Example:

We wish factor the expression $a^p + b^p$, where p is a prime. We look for the root of $(x^4 + x^3 + x^2 + x + 1)$ for $p=5$;

We obtain: $(a + b \zeta)(a + b \zeta^3)(a - b - b \zeta - b \zeta^2 - b \zeta^3)(a + b \zeta^2)(a + b)$

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0 \qquad a - b - b \zeta - b \zeta^2 - b \zeta^3 = a - b \zeta^4$$

But , and so

3. Congruences

Definition: If a and b are integers and m is a positive integer, then a is said to be *congruent* to b modulo m if m divides $(a - b)$. We use the notation $a \equiv b \pmod{m}$ to indicate a is congruent to b modulo m . Also $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

$$\begin{aligned} 12 \bmod 7 &= 5 \quad \text{also } 12 \bmod 7 = -2 \\ 1/7 \bmod 9 &= 4 \\ 1/289 \bmod 326 &= 185 \\ (13-1)! \bmod 13 &= 12 \\ (4001-1)! \bmod 4001 &= 4000 = -1 \end{aligned}$$

Definition. Let $m \neq 0$ be an integer. We say that two integers a and b are *congruent modulo m* if there is an integer k such that $a - b = km$, and in this case we write

$$a \equiv b \pmod{m}.$$

Notice that the condition " $a - b = km$ for some integer k " is equivalent to the condition " m divides $a - b$ ".

The numbers that exist in mod M arithmetic are $0, 1, 2, 3, \dots, M-1$. For example, in mod 5 arithmetic, the different numbers are represented by $0, 1, 2, 3$, and 4 . But 5 is *not* considered a separate number because $5 \equiv 0 \pmod{5}$. (Both 5 and 0 have the same remainder when divided by 5 : the remainder is 0 .)

It is fairly easy to show that for any integers a, b, c , and $m \neq 0$, the following properties hold:

- reflexivity: $a \equiv a \pmod{m}$.
- symmetry: If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- transitivity: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Therefore congruence modulo m is an equivalence relation, and this relation partitions the integers into m equivalence classes:

$$mn + 0, mn + 1, mn + 2, \dots, mn + (m - 1).$$

(Since $0 \equiv m \pmod{m}$, we can either choose 0 or m as a representative for the first class. It is conventional to choose 0 .) To be a little more formal than we were above, we can write the equivalence class of an integer a as $[a]$. The brackets signify that this is an equivalence *class* and not simply a number. In this way we can write

$$\begin{aligned} \dots &= [-3m] = [-2m] = [-m] = [0] = [m] = [2m] = [3m] = \dots, \\ \dots &= [-3m + 1] = [-2m + 1] = [-m + 1] = [1] = [m + 1] = [2m + 1] = [3m + 1] = \dots, \\ \dots &= [-3m + 2] = [-2m + 2] = [-m + 2] = [2] = [m + 2] = [2m + 2] = [3m + 2] = \dots, \\ \dots &= [-3m + 3] = [-2m + 3] = [-m + 3] = [3] = [m + 3] = [2m + 3] = [3m + 3] = \dots, \\ &\quad \vdots \\ \dots &= [-2m - 1] = [-m - 1] = [-1] = [m - 1] = [2m - 1] = [3m - 1] = [4m - 1] = \dots \end{aligned}$$

(Notice that each congruence symbol " \equiv " has been replaced by equality " $=$ ".) With this notation, we have the following property for any integers a and b , which justifies "reduction under addition":

$$[a + b] = [a] + [b].$$

Similarly, for any integers a and b we have

$$[a \cdot b] = [a] \cdot [b],$$

justifying "reduction under multiplication".

If you are adding, subtracting, or multiplying numbers that are larger than the modulus M , you can replace them with a smaller equivalent number before carrying out the addition, subtraction, or multiplication. For example, when working out $14 \cdot 18 \pmod{5}$, we could compute that $14 \cdot 18 = 252$ and $252 \equiv 2 \pmod{5}$. But it's easier to see that $14 \equiv 4 \pmod{5}$, and $18 \equiv 3 \pmod{5}$, and $4 \cdot 3 = 12$ and $12 \equiv 2 \pmod{5}$.

Sometimes it can simplify your calculations in modular arithmetic to replace one number with a smaller *negative* number. For example, suppose you wanted to compute $33 \cdot 32 \pmod{35}$. You could work out that $33 \cdot 32 = 1056$ and that 1056 has remainder 6 when divided by 35. But notice that:

$$33 \equiv -2 \pmod{35}$$

$$32 \equiv -3 \pmod{35}$$

Therefore,

$$33 \cdot 32 \equiv (-2) \cdot (-3) \equiv 6 \pmod{35} \text{ which is much easier to work out by hand.}$$

Suppose you are working in mod 10 and you want to compute 4 divided by 2 or find a number x such that $2 \cdot x \equiv 4 \pmod{10}$. The obvious answer, $x=2$, fits the equation. But there is another number, 7, such that $2 \cdot 7 \equiv 14 \equiv 4 \pmod{10}$. So division is not uniquely defined, because there are two numbers that can multiply by 2 to give 4.

Examples for amusement only

We can use the multiplication and modulo rules to construct the following set of series:

$1 \times 9 + 2 = 11$	$9 \times 9 + 7 = 88$
$12 \times 9 + 3 = 111$	$98 \times 9 + 6 = 888$
$123 \times 9 + 4 = 1111$	$987 \times 9 + 5 = 8888$
$1234 \times 9 + 5 = 11111$	$9876 \times 9 + 4 = 88888$
$12345 \times 9 + 6 = 111111$	$98765 \times 9 + 3 = 888888$
$123456 \times 9 + 7 = 1111111$	$987654 \times 9 + 2 = 8888888$
$1234567 \times 9 + 8 = 11111111$	$9876543 \times 9 + 1 = 88888888$
$12345678 \times 9 + 9 = 111111111$	$98765432 \times 9 + 0 = 888888888$
$123456789 \times 9 + 10 = 1111111111$	

$1 \times 8 + 1 = 9$	$9 \times 8 + 7 = 79$
$12 \times 8 + 2 = 98$	$98 \times 8 + 6 = 790$
$123 \times 8 + 3 = 987$	$987 \times 8 + 5 = 7901$
$1234 \times 8 + 4 = 9876$	$9876 \times 8 + 4 = 79012$
$12345 \times 8 + 5 = 98765$	$98765 \times 8 + 3 = 790123$
$123456 \times 8 + 6 = 987654$	$987654 \times 8 + 2 = 7901234$
$1234567 \times 8 + 7 = 9876543$	$9876543 \times 8 + 1 = 79012345$
$12345678 \times 8 + 8 = 98765432$	$98765432 \times 8 + 0 = 790123456$
$123456789 \times 8 + 9 = 987654321$	

$1 \times 7 + 0 = 7$	$9 \times 7 + 7 = 70$
$12 \times 7 + 1 = 85$	$98 \times 7 + 6 = 692$
$123 \times 7 + 2 = 863$	$987 \times 7 + 5 = 6914$
$1234 \times 7 + 3 = 8641$	$9876 \times 7 + 4 = 69136$
$12345 \times 7 + 4 = 86419$	$98765 \times 7 + 3 = 691358$
$123456 \times 7 + 5 = 864197$	$987654 \times 7 + 2 = 6913580$
$1234567 \times 7 + 6 = 8641975$	$9876543 \times 7 + 1 = 69135802$
$12345678 \times 7 + 7 = 86419753$	$98765432 \times 7 + 0 = 691358024$
$123456789 \times 7 + 8 = 864197531$	$98765432 \times 7 + -1 = 6913580246$

Etc

But also

$1 \times 1 = 1$
$11 \times 11 = 121$
$111 \times 111 = 12321$
$1111 \times 1111 = 1234321$
$11111 \times 11111 = 123454321$
$111111 \times 111111 = 12345654321$

Etc

Cyclic numbers

A **cyclic number** is an integer in which cyclic permutations of the digits are successive multiples of the number or **all** successive multiples be cyclic permutations. The most widely known is 142857:

$$\begin{aligned}
 142857 \times 1 &= 142857 \\
 142857 \times 2 &= 285714 \\
 142857 \times 3 &= 428571 \\
 142857 \times 4 &= 571428 \\
 142857 \times 5 &= 714285 \\
 142857 \times 6 &= 857142
 \end{aligned}$$

a cyclic number is of the form $\frac{b^{p-1} - 1}{p}$ where b is the number base (10 for decimal), and p is a prime that does not divide b . (Prime numbers p that give cyclic numbers are called full repetitor primes or long primes). For example, the case $b = 10$, $p = 7$ gives the cyclic number 142857.

Not all values of p will yield a cyclic number using this formula; for example $p=13$ gives 076923076923. These failed cases will always contain a repetition of digits (possibly several).

The first values of p for which this formula produces cyclic numbers in decimal are :

7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, 223, 229, 233, 257, 263, 269, 313, 337, 367, 379, 383, 389, 419, 433, 461, 487, 491, 499, 503, 509, 541, 571, 577, 593, 619, 647, 659, 701, 709, 727, 743, 811, 821, 823, 857, 863, 887, 937, 941, 953, 971, 977, 983 ...

Properties of cyclic numbers

- When cyclic numbers are multiplied by their generating prime, results in a sequence of 9's. $142857 \times 7 = 999999$
- When cyclic numbers are split in half by its digits and added the result is a sequence of 9's. $142 + 857 = 999$
- All cyclic numbers are divisible by 9.

A cyclic number of length L is the digital representation of

$$1/(L + 1).$$

Conversely, if the digital period of $1/p$ (where p is prime) is

$$p - 1,$$

then the digits represent a cyclic number.

For example:

$$1/7 = 0.142857\ 142857\ \dots$$

Multiples of these fractions exhibit cyclic permutation:

$$\begin{aligned} 1/7 &= 0.142857\ 142857\ \dots \\ 2/7 &= 0.285714\ 285714\ \dots \\ 3/7 &= 0.428571\ 428571\ \dots \\ 4/7 &= 0.571428\ 571428\ \dots \\ 5/7 &= 0.714285\ 714285\ \dots \\ 6/7 &= 0.857142\ 857142\ \dots \end{aligned}$$

4. Fractions

Definition

A part of a unit or some equal parts of a unit is called a vulgar (simple) fraction. Example in the fraction $3/7$ were 3 – a numerator, 7 – a denominator.

the numerator is less than a denominator, then the fraction is less than 1 and called a proper fraction. If a numerator is equal to a denominator, the fraction is equal to 1. If a numerator is greater than a denominator, the fraction is greater than 1. In both last cases the fraction is called an improper fraction. If a numerator is divisible by a denominator, then this fraction is equal to a quotient: $63 / 7 = 9$. If a division is executed with a remainder, then this improper fraction can be presented as a mixed number:

$$\frac{65}{7} = 9 \frac{2}{7}$$

Decimal fractions

Repetor or Repetend is the part of an infinite decimal fraction which is continually repeated ad infinitum. Thus in $0.\overline{18} = 0.181818181818$ the repetor is 18 and marked $\overline{18}$. The repetors arise when reducing vulgar fractions to decimals.

exercise

Convert fraction to an equivalent fraction with a denominator that is a power of ten before converting to a decimal.

$$1/2 = 5/10 = 0.5 \quad ; \quad 3/20 = 15/100 = 0.15; \quad 1/8 = 125/1000 = 0.125 \quad \text{etc}$$

The decimal equivalent of a proper or improper fraction can be calculated by dividing the numerator by the denominator. The result will be a **terminating** or **repeating** decimal.

$3/4 = 0.75$	terminating decimal
$3/8 = 0.375$	terminating decimal
$4/15 = 0.0666\dots$	repeating decimal

For converting Terminating Decimals to Fractions : use place value to convert the terminating decimal to a fraction that is a power of ten. Reduce to lowest terms.

$$0.5 = 5/10 = 1/2$$

$$0.2 = 2/10 = 1/5$$

$$0.15 = 15/100 = 3/20$$

$$0.125 = 125/1000 = 1/8$$

The denominator of a fraction converted from a **terminating decimal** will be a multiple of 2 and/or 5. If the denominator of a common fraction contains some prime factor other than 2 or 5, the fraction cannot be converted completely to a decimal. When such fractions are converted according to the foregoing rule, the decimal resulting will never terminate. Consider the fraction $1/3$. Applying the rule, we have

$$\begin{array}{r} .333 \dots \\ 3 \overline{) 1.0000} \\ \underline{9} \\ 10 \\ \underline{9} \\ 10 \\ \underline{9} \end{array}$$

The division will continue indefinitely. Any common fraction that cannot be converted exactly yields a decimal that will never terminate and in which the digits sooner or later recur. In the previous example, the recurring digit was 3. In the fraction $5/11$, we have

$$\begin{array}{r} .4545 \\ 11 \overline{) 5.0000} \\ \underline{44} \\ 60 \\ \underline{55} \\ 50 \\ \underline{44} \\ 60 \\ \underline{55} \end{array}$$

The recurring digits are 4 and 5. When a common fraction generates such a repeating decimal, it becomes necessary to arbitrarily select a point at which to cease the repetition.

Summary

there are 3 types of fractions: terminating fractions, semi-repeating fractions and repeating fractions (with or without a lead).

1 terminating fractions:

$1/2$, $2/5$, $1/4$ are all examples of this kind. when you do the division, it stops after a small amount of decimal places.

$$\begin{array}{r} \dots 0.25 \\ \hline 4 \overline{) 1.00000} \\ \dots 8 \\ \dots \text{-----} \\ \dots 20 \\ \dots 20 \\ \dots \text{-----} \\ \dots 0 \text{ <----desired} \end{array}$$

2. semi- repeating fractions:

$1/3$ is the usual example:

....0.333

$$\begin{array}{r} \dots \\ \hline 1 \mid 1.000000 \\ \dots 9 \\ \hline \dots 10 \\ \dots 9 \\ \hline \dots 10 \\ \dots 9 \\ \hline \dots 1 \text{ (this goes).} \end{array}$$

3. repeating fractions" like 1/7:

.....0.142857 (repeating)

$$\begin{array}{r} \dots \\ \hline .7 \mid 1.00000000 \\ \dots 7 \\ \hline \dots 30 \\ \dots 28 \\ \hline \dots 20 \\ \dots 14 \\ \hline \dots 60 \\ \dots 56 \\ \hline \dots 40 \\ \dots 35 \\ \hline \dots 50 \\ \dots 49 \\ \hline \dots 1 \text{ (it repeats!).} \end{array}$$

Some fractions have a repeating part, and a non-repeating part that comes first, like

$1/6 = 0.16666666$ (the 6's repeat, but there's that one 1 at the beginning).

$1/44 = 0.02 \underline{27}272727$ (the 27s repeat)

$1/48 = 0.0208 \underline{3}33333$ (the 3s repeat and 0208 is the lead)

A decimal that is neither terminating nor repeating represents an irrational number (which cannot be expressed as a fraction of two integers), such as the square root of 2 or the number π . Conversely, an irrational number always has a non-terminating non-repeating decimal representation.

The digits of some specific integers permute or shift cyclically when they are multiplied by a number n . Examples are:

- $142857 \times 3 = 428571$ (shifts cyclically one place left)
- $142857 \times 5 = 714285$ (shifts cyclically one place right)
- $128205 \times 4 = 512820$ (shifts cyclically one place right)
- $076923 \times 9 = 692307$ (shifts cyclically two places left)

These specific integers, known as **transposable integers**, can be but are not always cyclic numbers.

A **cyclic number** is an integer in which cyclic permutations of the digits are (all) successive multiples of the number. The most widely known is 142857:

$$\begin{aligned}142857 \times 1 &= 142857 \\142857 \times 2 &= 285714 \\142857 \times 3 &= 428571 \\142857 \times 4 &= 571428 \\142857 \times 5 &= 714285 \\142857 \times 6 &= 857142\end{aligned}$$

If leading zeros are not permitted on numerals, then 142857 is the only cyclic number in decimal. Allowing leading zeros, the sequence of cyclic numbers begins:

$$\begin{aligned}142857 & \text{ (6 digits)} \\0588235294117647 & \text{ (16 digits)} \\052631578947368421 & \text{ (18 digits)} \\0434782608695652173913 & \text{ (22 digits)} \\0344827586206896551724137931 & \text{ (28 digits)} \\0212765957446808510638297872340425531914893617 & \text{ (46 digits)} \\0169491525423728813559322033898305084745762711864406779661 & \text{ (58 digits)} \\016393442622950819672131147540983606557377049180327868852459 & \text{ (60 digits)}\end{aligned}$$

Cyclic numbers are related to the recurring digital representations of unit fractions. A cyclic number of length L is the digital representation of

$$1/(L + 1).$$

Conversely, if the digital period of $1/p$ (where p is prime) is

$$p - 1,$$

then the digits represent a cyclic number.

For example:

$$1/7 = 0.142857\ 142857\dots$$

Every *proper* multiple of a cyclic number (that is, a multiple having the same number of digits) is a rotation. Multiples of these fractions exhibit cyclic permutation:

$$\begin{aligned}1/7 &= 0.142857\ 142857\dots \\2/7 &= 0.285714\ 285714\dots \\3/7 &= 0.428571\ 428571\dots \\4/7 &= 0.571428\ 571428\dots \\5/7 &= 0.714285\ 714285\dots \\6/7 &= 0.857142\ 857142\dots\end{aligned}$$

From the relation to unit fractions, it can be shown that cyclic numbers are of the form

$$\frac{b^{p-1} - 1}{p}$$

where b is the number base (10 for decimal), and p is a prime that does not divide b . (Primes p that give cyclic numbers are called full reptend primes or long primes).

For example, the case $b = 10$, $p = 7$ gives the cyclic number 142857.

Not all values of p will yield a cyclic number using this formula; for example $p=13$ gives 076923076923. These failed cases will always contain a repetition of digits (possibly several).

The first values of p for which this formula produces cyclic numbers in decimal are:

7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, 223, 229, 233, 257, 263, 269, 313, 337, 367, 379, 383, 389, 419, 433, 461, 487, 491, 499, 503, 509, 541, 571, 577, 593, 619, 647, 659, 701, 709, 727, 743, 811, 821, 823, 857, 863, 887, 937, 941, 953, 971, 977, 983 ...

The decimal representation of a rational number is ultimately periodic because it can be determined by a long division process, which must ultimately become periodic as there are only finitely many different remainders and so eventually it will find a remainder that has occurred before. On the other hand, each repeating decimal number satisfies a linear equation with integral coefficients, and its unique solution is a rational number. The number $\alpha = 5.8144144144\dots$ above satisfies the equation $10000\alpha - 10\alpha = 58144.144144\dots - 58.144144\dots = 58086$, whose solution is $\alpha = 58086/9990 = 3227/555$.

A decimal representation written with a repeating final 0 is said to *terminate* before these zeros. Instead of "1.585000..." one simply writes "1.585". The decimal is also called a **terminating decimal**. Terminating decimals represent rational numbers of the form $k/(2^n 5^m)$. For example, $1.585 = 317/200 = 317/(2^3 5^2)$. A terminating decimal can be written as a decimal fraction: $317/200 = 1585/1000$. However, a terminating decimal also has a representation as a repeating decimal, obtained by decreasing the final (nonzero) digit by one and appending an infinitely repeating sequence of nines. $1 = 0.999999\dots$ and $1.585 = 1.584999999\dots$ are two examples of this.

Every rational number is either a terminating or repeating decimal.

Theorem: When a fraction $1/n$ repeats the repetend contains a maximum of $n-1$ digits.

A fraction in lowest terms with a prime denominator other than 2 or 5 (i.e. coprime to 10) always produces a repeating decimal. The period of the repeating decimal of $1/p$ is equal to the order of 10 modulo p . If 10 is a primitive root modulo p , the period is equal to $p - 1$; if not, the period is a factor of $p - 1$. This result can be deduced from Fermat's little theorem, which states that $10^{p-1} = 1 \pmod{p}$.

The base-10 repetend (the repeating decimal part) of the reciprocal of any prime number greater than 5 is divisible by 9

If the period of the repeating decimal of $1/p$ for prime p is equal to $p - 1$ then the repeating decimal part is called a **cyclic number**.

Examples of fractions belonging to this group are:

- $1/7 = 0.142857$; 6 repeating digits
- $1/17 = 0.0588235294117647$; 16 repeating digits
- $1/19 = 0.052631578947368421$; 18 repeating digits

Some reciprocals of primes that do not generate cyclic numbers are:

- $1/3 = 0.333\dots$ which has a period of 1.
- $1/11 = 0.090909\dots$ which has a period of 2.
- $1/13 = 0.076923\dots$ which has a period of 6.

An integer that is not co-prime to 10 but has a prime factor other than 2 or 5 has a reciprocal that is eventually periodic, but with a non-repeating sequence of digits that precede the repeating part.

Coupled cycles

When we compare fractions which of which one is a multiple of the other the digit pattern of the other we notice this in the pattern: e.g.

$1/20 = 0.05$ or 0.050 is twice that of $1/40 = 0.025$.

$1/30 = 0.0\overline{333}$ is twice that of $1/60 = 0.01\overline{66}$.

$1/24 = 0.041\overline{6666}$ is twice that of $1/48 = 0.0208\overline{666}$ and thrice $1/72 = 0.013\overline{888}$

Because reciprocity is defined by a fraction (or one divided by a number) of we can notice that e.g. :

$1/18 = 0.0\overline{5555}$ and $1/55$ is $0.01\overline{81818}$

$1/25 = 0.4$ and $1/4 = 0.25$ and $1/40 = 0.025$

$1/27 = 0.0\overline{37037037}$ and $1/37 = 0.0\overline{27027}$

$1/22 = 0.04\overline{5}$ and $1/45$ is $0.\overline{22}$

$1/30 = 0.\overline{33}$ and $1/33 = 0.0\overline{30}$

$1/54 = 0.01\overline{85}$ and $1/185 = 0.00\overline{54}$

If we compare e.g. $1/7 = 0.\underline{142857}14..$ to $1/14 = 0.07\underline{14257}14285..$ which is half of $1/7$ we notice that the digit pattern is shifted to digits to the right because $1/7$ is cyclic (see above). But $1/21 = 0.\underline{047619}047619$ has no shift pattern relative to $1/7$, neither has $1/28 = 0.\underline{3571428}$ but $1/35 = 0.\underline{0285714}$ has. Because $1/7$ is cyclic multiples of $1/71$ are also and also fractions the following fractions $\frac{1}{2} \times 1/7$, $1/5 \times 1/7$, $1/10 \times 1/7$ etc.

The multiples of $1/13$ can be divided into two sets, with different repeating decimal parts. The first set is:

- $1/13 = 0.076923...$
- $10/13 = 0.769230...$

where the repeating decimal part of each fraction is a cyclic re-arrangement of 076923. The second set is:

- $2/13 = 0.153846...$
- $7/13 = 0.538461...$

In general, the set of reciprocals of a prime p will consist of n sets each with period k , where $nk = p - 1$.

examples

$x = 0.31707313170731...$

$$\begin{array}{r} 100,000x = 31707.31707 \\ - 1x = .31707 \\ \hline 99,999x = 31,707 = 3(10,569) \dots \\ \hline 99,999 \quad 99,999 \quad 3(33,333) \dots \end{array}$$

Until we found that $x = 13/41$. In finding the fraction, take the number of 9's to be how often it repeats. For example, with $x = 0.55555...$, $10x - x = 5$, so $9x = 5$, so $x = 5/9$.

For $x = 0.12121212...$, since it repeats every 2, take $10^2 = 100$. From this, $100x - x = 12$, so $99x = 12$, so $33x = 3$, so $x = 4/33$.

For $0.468468468...$, note repetition every 3 digits, so use 10^3 . It is known that $10^3 = 1,000$, so we have $1,000x - x = 468$. That gives $999x = 468$; dividing by 9 gives $111x = 52$. 111 and 52 have no common factors, $x = 52/111$.

For $0.425342534253...$, note repetition occurs every 4 digits; this means to use 10^4 , which is 10,000. This gives us $10,000x - x = 4253$. Since 4253 is not divisible by 2 or 5 (the factors of 10,000 are $2 \times 2 \times 2 \times 5 \times 5 \times 5 \times 5$), $x = 4253/10,000$.

In this case, we have a repetition every 5 digits. That is, $x = 0.317073170731707...$, and that is 31707 repeated. In this case, $100,000x - x = 31707$, so that works out to be $99,999x = 31,707$. Now 31,707 has the digits 3, 1, 7, 0, and 7, and these add to 18, which is divisible by 9, so 31,707 is divisible by 9.

5. divisibility and modularity

Theorem

Let m be a positive integer. The integers a and b are congruent modulo m iff there is an integer k such that $a = b + km$.

Theorem

Let b be an integer. Then an integer a

1. is divisible by $(b-1)$ if and only if the sum of digits in its expansion $(a)_b$ is divisible by $(b-1)$
2. is divisible by $(b+1)$ if and only if the alternating sum of digits in its expansion $(a)_b$ is divisible by $(b+1)$

The proof is based on Modulo Arithmetic. Thus we have $b-1=0 \pmod{(b-1)}$ which implies $b=1 \pmod{(b-1)}$. Therefore, for every $i>0$, $b^i = 1 \pmod{(b-1)}$. Multiplying this by c_i and summing up for $i=0,1, \dots, k$ we get the first assertion.

Similarly, $b+1=0 \pmod{(b+1)}$ hence $b=-1 \pmod{(b+1)}$. Therefore, for $i>0$, $b^i = (-1)^i \pmod{(b+1)}$. Multiplying this by c_i and summing up for $i=0,1, \dots, k$ we get the second assertion.

Example 1

Let $a=164 = 125+25+2\cdot 5+4=(1124)_5$. The sum of digits is $1+1+2+4=8$ and is divisible by 4. Therefore 164 is divisible by 4.

On the other hand, $164=2\cdot 81+0\cdot 27+0\cdot 9+0\cdot 3+2=(20002)_3$. The alternating sum of digits is $2-0+0-0+2=4$ and is divisible by 4. Therefore, again, 164 is divisible by 4.

For divisibility by 7 in base c there are two criteria:

1. $a = (a)_c = c_k c^k + c_{k-1} c^{k-1} + \dots + c_1 c^1 + c_0$ is divisible by 7 iff the alternating sum of digits $(-1)^k c_k + (-1)^{k-1} c_{k-1} + \dots + c_0$ is divisible by 7.
2. $a = (a)_c = c_k c^k + c_{k-1} c^{k-1} + \dots + c_1 c^1 + c_0$ is divisible by 7 iff the sum of digits $c_k + c_{k-1} + \dots + c_0$ is divisible by 7.

Example 2

$512=8^3$. Therefore $(512)_{10}=(1000)_8$. This implies that divided by 7 the remainder will be 1. Then, for example, 511 is divisible by 7.

$1296=6^4$. Therefore $(1296)_{10}=(10000)_6$. From here $(1296+6)_{10}=(10010)_6$. Its alternating sum of digits is $1-0+0-1+0=0$. As a result, 1302 is divisible by 7.

Example 3:

$5 \cdot 3^{4n+1} - 2^{2n}$ is divisible by 7.

Proof: $n=0$ satisfies the equation, because 14 is divisible by 7. We assume that the equation also holds for $n \in \mathbb{N}$. We now show that it also holds for $n+1$:

$5 \cdot 3^{4n+5} - 2^{2n+2}$ is divisible by 7.

$$5 \cdot 3^{4n+5} - 2^{2n+2} = 5 \cdot 81 \cdot 3^{4n+1} - 4 \cdot 2^{2n} = 81 \cdot (5 \cdot 3^{4n+1} - 2^{2n}) + 77 \cdot 2^{2n}$$

Because both terms 81 and 77 of the sum are divisible by 7, $5 \cdot 3^{4n+5} - 2^{2n+2}$ is divisible by 7.

Example 4:

$3^{2n+1} + 2^{n-1}$ is divisible by 7.

Proof: $n=1$ satisfies the equation, because 24 is divisible by 7. We assume that the equation also holds for $n \geq 1$. We now show that it also holds for $n+1$:

$3^{2(n+1)+1} + 2^n$ is divisible by 7.

$$3^{2n+3} + 2^n = 9 \cdot 3^{4n+1} + 2^{2n} = 9 \cdot (5 \cdot 3^{4n+1} + 2^{2n}) - 7 \cdot 2^{2n}$$

Because both $5 \cdot 3^{4n+1} + 2^{2n}$ and 9 are divisible by 7, $3^{2n+1} + 2^{n-1}$ is divisible by 7.

Divisibility of numbers

There are 2 kinds of divisibility criteria:

- allowing to determine the remainder a number yields, being divided by certain divisor;
- answering only whether or not a number is divisible with no way to determine the remainder in the latter case.

The general approach for the first type is the following: let

$N = d_0 + d_1 \cdot b + d_2 \cdot b^2 + d_3 \cdot b^3 + \dots + d_s \cdot b^s$ is a natural number, written in arbitrary base $b = 2, 3, \dots$, its digits $d_0, d_1, d_2, \dots, d_s = 0, 1, 2, \dots, b-1$; leading digit $d_s > 0$.

To find the remainders r_0, r_1, \dots the degrees of b yield, being divided by an arbitrary natural divisor m (there are at most $m-1$ distinct of them):

$$b^0 \equiv r_0 \equiv 1 \pmod{m};$$

$$b^1 \equiv r_1 \pmod{m};$$

$$b^2 \equiv r_2 \pmod{m};$$

$$b^3 \equiv r_3 \pmod{m} \text{ etc., then}$$

$$N \equiv d_0 + d_1 \cdot r_1 + d_2 \cdot r_2 + d_3 \cdot r_3 + \dots + d_s \cdot r_s \pmod{m}$$

This is the relationship every criterion to be derived from (any base, any divisor).

Divisibility formulas:

$$\text{for 2 is } 2X + L$$

$$\text{for 3 is } 4X + L$$

$$\text{for 4 is } 6X + L$$

$$\text{for 5 is } 5X + L$$

for 6 is $2X + L$ and $4X + L$ -- in other words, the formulas for 2 and 3 must work before the number is divisible by 6.
 for 7... and $3X + L$ and $4X - L$
 for 9 is $X + L$
 for 11 is $X - L$
 for 12 is $2X - L$
 for 13 is $3X - L$
 for 14 is $4X - L$ and $2X + L$ -- in other words, the formulas for 7 and 2 must work before the number is divisible by 14.
 for 17 is $7X - L$
 for 21 is $X - 2L$
 for 23 is $3X - 2L$
 for 31 is $X - 3L$

Where L = last digit and X = everything in front of last digit.

Generally speaking, for an integer base b the same number a will be written as

$$a = (a)_b = c_k b^k + c_{k-1} b^{k-1} + \dots + c_1 b^1 + c_0$$

Consider an integer a in decimal:

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10^1 + a_0$$

a is divisible by 9 if and only if the sum of the digits $a_n + a_{n-1} + \dots + a_1 + a_0$ is divisible by 9.

a is divisible by 11 if and only if the alternating sum of the digits $(-1)^n a_n + (-1)^{n-1} a_{n-1} + \dots - a_1 + a_0$ is divisible by 11.

Example:

A binary number is the sum of selected powers of 2. If the bits are, say, abcdef, then the number is

$$\begin{aligned} f \cdot 2^0 &= 1f = 1f \pmod{5} \\ e \cdot 2^1 &= 2e = 2e \pmod{5} \\ d \cdot 2^2 &= 4d = -1d \pmod{5} \\ c \cdot 2^3 &= 8c = -2c \pmod{5} \\ b \cdot 2^4 &= 16b = 1b \pmod{5} \\ a \cdot 2^5 &= 32a = 2a \pmod{5} \\ \hline \text{abcdef} &= 2(e-c+a) + (f-d+b) \pmod{5} \end{aligned}$$

$$\{a,b,c,d,e,f\} = \{1,,2, -1, -2\}$$

$$\text{Mod4: } \{a,b,c,d,e,f\} = \{1,,2, 0, \}$$

$$\text{Mod 5: } \{a,b,c,d,e,f\} = \{1,,2, -1, -2\}$$

$$\text{Mod6: } \{a,b,c,d,e,f\} = \{1,,2, -2, 2, -2\}$$

$$\text{Mod7: } \{a,b,c,d,e,f\} = \{1,,2, -3, 1, 2, -3\}$$

Mod 8: {a,b,c,d,e,f} = {1,,2, 4, 0, 0, 0, 0}
 Mod 9: {a,b,c,d,e,f} = {1,,2, 4, -1, -2, -4, 1, 2}
 Mod 10: {a,b,c,d,e,f} = {1,,2, 4, -2, -4, 2, 4, -2, -4}
 Mod 11: {a,b,c,d,e,f} = {1,,2, 4,-3, 5, 1,,2, -4, 3,-5}

Etc. given in the table below for the first part of the symmetric pattern

11																5	-3	4	2	1				
13																6	3	-5	4	2	1			
15															4	2	1	-7	4	2	1			
17															-8	-4	-2	-1	-	4	2	1		
																		9=8						
19															9	-	-	-6	-3	8	4	2	1	
																24=5	12=7							
21															-5	8	4	2	1

Theorem

$2^p+2^q+2^0$ is not a prime for p and p even

Conjecture

2^p+1 is a prime if p is divisble by 4 and not a prime if divisible by 6.

Theorem

If $x = 2^k$ for some positive integer k, and y is an odd integer, then x and y are relatively prime.

Theorem

If $d | ab$ and $\gcd(d, a) = 1$, then $d | b$.
 If $a | c$, $b | c$, and $\gcd(a, b) = 1$, then $ab | c$.

Theorem

$x \text{ mod } n = y \text{ mod } n$ iff $n | (x - y)$ iff $(x - y) \text{ mod } n = 0$

Summary

- **Remainders Modulo 2**

Observe $10^k = 5^k 2^k = 0$, modulo 2, for all whole numbers $k > 0$. Therefore

- $243 = 2 \times 10^2 + 4 \times 10 + 3 = 0 + 0 + 3 = 3 = 3 = 1$, modulo 2.
- $6825 = 6 \times 10^3 + 8 \times 10^2 + 2 \times 10 + 5 = 0 + 5 = 1$, modulo 2.
- $52300 = 5230 \times 10 = 0$, modulo 2

In general, the remainder, modulo 10, of a n-digit decimal whole number equals the remainder modulo 2 of the last digit. For example,

$$479 = 47 \times 10 + 9 = 0 + 9 = 1, \text{ modulo } 2$$

- **Remainders, Modulo 3**

$10 \equiv 1 \pmod{3}$
 $100 = 10^2 \equiv 1^2 = 1 \pmod{3}$
 $1000 = 10^3 \equiv 1^3 = 1 \pmod{3}$

Repeated calculations (mathematical induction) implies

$10^k \equiv 1 \pmod{3}$ for all natural numbers k .

Again, do the calculations for $k = 0, 1, 2, 3, 4$ and 5 , or apply mathematical induction.

Therefore with equalities modulo 3

$243 = 2 \times 10^2 + 4 \times 10 + 3 \equiv 2 \cdot 1 + 4 \cdot 1 + 3 = 2 + 4 + 0 = 6 \equiv 0 \pmod{3}$.

Therefore with equalities modulo 3,

modulo 3: $6821 = 6 \times 10^3 + 8 \times 10^2 + 2 \times 10 + 1 \equiv 6 + 8 + 2 + 1 = 0 + 8 + 3 = 8 \equiv 2 \pmod{3}$

The foregoing implies $6819 = 6821 - 2 \equiv 0 \pmod{3}$.

Note: Putting modulo 3 before the sequence of equalities provides an immediate context for them while putting them after delays the justification. We may use both.

Computational short cuts may be possible. For instance, remainder on division by 3 is given by the sum of digits, modulo 3, as $10^k \equiv 1 \pmod{3}$, for all natural numbers k . But in the sum of those digits, we may replace 0, 3, 6 and 9 by zero, 2, 5 and 8 by 2 and 1, 4 and 7 by 1.

Take a look at the first 10 square numbers and their remainders when divided by 3:

Square number	1	4	9	16	25	36	49	64	81	100
Remainder when divided by 3	1	1	0	1	1	0	1	1	0	1

It appears that the remainders follow a pattern, and also that they do not contain any 2's. We can see why this is the case if you consider that every integer m can be written either as $3k$, $3k+1$, or $3k+2$ for some integer k (depending on whether the remainder is 0, 1, or 2 when you divide m by 3). Then when you take these different possibilities and square them:

m	m²	Remainder when divided by 3
$3k$	$9k^2$	0, since 9 is divisible by 3
$3k+1$	$9k^2 + 6k + 1$	1, since $9k^2$ and $6k$ are divisible by 3
2	$9k^2 + 12k + 4$	1, since $9k^2$ and $12k$ are divisible by 3, and 4 divided by 3 has remainder 1

This explains why the remainders follow the (1, 1, 0) cycle, and also why they do not contain any 2's.

This problem is an example of *modular arithmetic* -- in examining all possible integers, we looked only at their remainder when divided by 3. For our purposes, the numbers 2, 5, 14, for example, all had the same important property: they can all be written as $3k+2$, i.e. their remainder when divided by 3 is 2. In terms of modular

arithmetic, we would say that 2, 5, and 14 are *equivalent modulo 3* or *equivalent mod 3*, written:

$$2 \equiv 5 \equiv 14 \pmod{3}$$

(sometimes written using the equals sign), In mod 3 arithmetic we would write:

$$2^2 \equiv 1 \pmod{3}$$

It says that *any* number that is equivalent to 2 mod 3, has a square that is equivalent to 1 mod 3. That property is true for that entire class of numbers, and that class of numbers is represented in the equation by its smallest positive member, the number 2. When actually *working out* problems in modular arithmetic, it's easiest just to work with an actual number, e.g. 2, and forget about the fact that it's representing an "entire class of numbers". For example, in figuring out $2^3 \pmod{3}$, we compute that $2^3 = 8$, and $8 \equiv 2 \pmod{3}$, so $2^3 \equiv 2 \pmod{3}$.

Similarly, in figuring out $14^3 \pmod{3}$, we could first replace 14 with 2 (because in mod 3 arithmetic, they are "the same number"), and then compute $2^3 \equiv 2 \pmod{3}$.

Note: When we say that 2, 5, and 14 represent "the same number" in the mod 3 universe, and that you can replace any one of them with any other, that only applies when they are written in the base: for example, $5^{17} \equiv 14^{17} \pmod{3}$. That does not apply when they are written in the exponent -- for example, you **cannot** assume that $2^5 \equiv 2^{14} \pmod{3}$, and in fact that statement is wrong.

- **Remainders, Modulo 4**

The remainder, modulo 4, of a n-digit decimal whole number equals the remainder modulo 4 of the last 2 digits. For example

$$6821 = 68 \times 10^2 + 21 = 68 \times 0 + 21 = 0 + 5 \times 4 + 1 = 1 \pmod{4}.$$

- **Remainders Modulo 5**

Observe $10^k = 5^k 2^k = 0$, modulo 5, for all whole numbers $k > 0$. Therefore

- $243 = 2 \times 10^2 + 4 \times 10 + 3 = 0 + 0 + 3 = 3 = 3 \pmod{5}$.
- $6821 = 6 \times 10^3 + 8 \times 10^2 + 2 \times 10 + 1 = 0 + 3 = 3$, modulo 5.
- $475 = 47 \times 10 + 5 = 0$, modulo 5
- $52300 = 5230 \times 10 = 0$, modulo 5

In general, the remainder, modulo 5, of a n-digit decimal whole number equals the remainder modulo 5 of the last digit. For example,

$$479 = 47 \times 10 + 9 = 0 + 9 = 4, \pmod{5}$$

- **Remainders Modulo 6**

The remainder modulo 6 of a n digit whole number N is 0 if N is a multiple of both 2 and 3. The decimal representation of N implies $N = q10 + r$. Then $q = a3+b$ where b is 0, 1 or 2. Therefore

$$\text{modulo } 6, N = q10 + r = (a3+b)10 + r = 30a + b10 + r = b10 + r,$$

where b is 0, 1 or 2 and r is a single digit number 0 to 9.

Example 1: For the number 6835, we have

$$\text{modulo } 3, 683 = 6 + 8 + 3 = 8 = 2$$

Therefore $b = 2$, and modulo 6, $6825 = 682 \cdot 10 + 5 = 2 \cdot 10 + 5 = 25 = 1$.

Example 2: For the number 23558 we have

$$\text{modulo } 3, 23455 = 2 + 3 + 5 + 5 = 15 = 0$$

Hence with $b = 0$, we have modulo 6, $23558 = 2355 \times 10 + 8 = 0 + 8 = 2$

- **Remainders, Modulo 7**

The first 7 multiples of 7 are 7, 14, 21, 28, 35, 42 and 49. Therefore $50 = 1$ modulo 7 and $100 = 2$ modulo 7. We may use the foregoing to form and simplify a sequence of equalities, modulo 7, to compute the remainder after division by 7.

first example

$$\begin{aligned} 34569 &= 345 \times 100 + 50 + 19 \text{ modulo } 7 = 345 \times 2 + 1 + 5 \text{ modulo } 7 = 696 \text{ modulo } 7 = \\ &= 6 \times 100 + 50 + 46 \text{ modulo } 7 \\ &= 6 \times 2 + 1 + 4 \text{ modulo } 7 = 17 \text{ modulo } 7 = 3 \end{aligned}$$

second example,

$$\begin{aligned} 654321 &= 6543 \times 100 + 21 \text{ modulo } 7 = 6543 \times 2 + 0 \text{ modulo } 7 = 13086 \text{ modulo } 7 = \\ &= 130 \times 100 + 50 + 36 \text{ modulo } 7 \\ &= 260 + 1 + 1 \text{ modulo } 7 = 262 \text{ modulo } 7 = 2 \times 100 + 50 + 12 \text{ modulo } 7 = 4 + 1 + \\ &= 5 \text{ modulo } 7 = 10 \text{ modulo } 7 = 3. \end{aligned}$$

- **Remainders, Modulo 8**

The remainder, modulo 8, of a n-digit decimal whole number equals the remainder modulo 8 of the last 3 digits. For example

$$76827 = 76 \times 10^3 + 827 = 6 \cdot 0 + 827 = 0 + 206 \times 4 + 3 = 3 \text{ modulo } 4.$$

- **Remainders, Modulo 9**

Now we calculate a few remainders modulo 9. For that, observe

$$10 \equiv 1 \pmod{9}$$

$$100 = 10^2 \equiv 1^2 = 1 \pmod{9}$$

$$1000 = 10^3 \equiv 1^3 = 1 \pmod{9}$$

Repeated calculations (mathematical induction) implies

$$10^k \equiv 1 \pmod{9} \text{ for all natural numbers } k.$$

$$243 = 2 \times 10^2 + 4 \times 10 + 3 = 2 \cdot 1 + 4 \cdot 1 + 3 = 2 + 4 + 3 = 9 \equiv 0 \pmod{9}$$

$$6821 = 6 \times 10^3 + 8 \times 10^2 + 2 \times 10 + 1 = 6 + 8 + 2 + 1 = 17 = 10 + 7 = 1 + 7 = 8$$

The foregoing implies modulo 9, $6822 = 6821 + 1 = 8 + 1 = 0$.

Computational short cuts may be possible. For instance, Remainder on division by 9 is given by the sum of digits, modulo 9, as $10^k \equiv 1 \pmod{9}$, for all natural numbers k . But in the sum of those digits, we may replace 9 by zero

Statement : For each positive integer A , if B is the sum of the digits in A , then A and B have the same remainder when divided by 9. In other words,
 $A \equiv [\text{sum of digits in } A] \pmod{9}$

For example: $761 \equiv 5 \pmod{9}$. And if you add up the digits of 761, $7+6+1 = 14$, and $14 \equiv 5 \pmod{9}$, the same result.

The number 4329 for example could be written as: $(4 * 1000) + (3 * 100) + (2 * 10) + 9$

we can substitute any numbers that are equivalent to each other (as long as we're not substituting them in the exponent). So for each of 1000, 100, and 10, we can substitute just 1, because they are all equivalent to 1. So:

$$(4 * 1000) + (3 * 100) + (2 * 10) + 9 \equiv 4 + 3 + 2 + 9 \pmod{9}$$

Here, the value on the left is the original number A , and the value on the right is the sum of the digits of A .

Algorithm to find the remainder of a positive number when divided by 9:

1. Add up the digits of the number.
2. If the result is a two-digit number, then add up the digits of the result. Repeat until your result is a 1-digit number.
3. The final result is the remainder of the original number. (UNLESS the final result is 9, in which case the remainder of the original number is 0.)

For example, to find $829 \pmod{9}$, we find $8 + 2 + 9 = 19$. Then take the digits of 19 and add them: $1 + 9 = 10$. Then take the digits of 10 and add them: $1 + 0 = 1$. So the remainder of $829 \equiv 1 \pmod{9}$.

- **Remainders, Modulo 10**

The remainder, modulo 10, of a n -digit decimal whole number equals the remainder modulo 10 of the last digit. For example

$$76827 = 7682 \times 10 + 7 = 7682 \times 0 + 7 = 7, \text{ modulo } 10.$$

- **Remainders, Modulo 11**

Now we calculate a few remainders modulo 11. For that, observe

$$10 = -1, \text{ modulo } 11$$

$$100 = 10^2 = (-1)^2 = 1, \text{ modulo } 11.$$

$$1000 = 10^3 = (-1)^3 = -1, \text{ modulo } 11.$$

Repeated calculations (mathematical induction) implies

$$10^k = (-1)^k, \text{ modulo } 11, \text{ for all natural numbers } k.$$

Therefore

$$\text{modulo } 11: 243 = 2 \times 10^2 + 4 \times 10 + 3 = -2 + 4 - 3 = -1 = 10$$

$$\text{modulo } 11, 6821 = 6 \times 10^3 + 8 \times 10^2 + 2 \times 10 + 1 = -6 + 8 - 2 + 1 = 1$$

Note $10^k = (-1)^k$, modulo 11, implies the ones column ($k=0$) makes a positive contribution, the tens column ($k=1$) makes a negative contribution, and the sign of the columns alternates. So instead of writing

$$\text{modulo } 11: 6821 = -6 + 8 - 2 + 1 = 1$$

starting from the left, we can may write the alternating sum

$$\text{modulo } 11: 6821 = 1 - 2 + 8 - 6 = 1$$

starting at the right with the one's digit.

$$\text{Example: Modulo } 11: 76823 = 3 - 2 + 8 - 6 + 7 = 10$$

- **Remainder Calculations for Negative Numbers**

Observe if $m > 0$ is a whole number with $m = r$, modulo d , then $-m = -r = n-r$, modulo d ,

For example $18 = 3$ modulo 5. Therefore,

$$\text{modulo } 5: -18 = -3 = 0 - 3 = 5 - 3 = 2.$$

$$\text{Observe } 18 = 3 \times 5 + 3 \text{ while } -18 = -20 + 2 = (-4) \times 5 + 2.$$

Each negative integer is also equivalent to some positive integer mod 3 -- but be careful when working these out. For example, -5 is not equivalent to 2 mod 3. -5 is equivalent to 1 mod 3 -- because the nearest multiple of 3 below -5 is the number -6, and -5 is 1 greater than -6. See the table below which shows all the multiples of 3 in bold:

...	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	...
-----	----	-----------	----	----	-----------	----	----	----------	---	---	----------	---	---	----------	---	---	-----

The numbers which are equivalent to 1 mod 3, are just those numbers that are 1 greater than a multiple of 3, shown in bold here:

...	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	...
-----	----	----	-----------	----	----	-----------	----	---	----------	---	---	----------	---	---	----------	---	-----

Like the multiples of 3, the numbers equivalent to 1 mod 3 are, of course, spaced evenly apart. The negative numbers in this class (-2, -5, etc.) are not the same as the positive numbers in this class (1, 4, 7, etc.).

Remark: For every divisor $d > 0$ and every number N , there is a unique integer q such that $qd \leq N < (q+1)d$ so that $r = N - qd$ satisfies $0 \leq r < d$. With the aid of a calculator, if N is positive, the whole number part of the decimal representation of the computed value of N/d gives $q > 0$. But if N is negative, the whole number part of the decimal representation of the computed value of N/d gives $q+1 \leq 0$, and q is one less than the whole number part of N/d .

Modular arithmetic with large exponents

Suppose you wanted to find the value of $12^{346} \pmod{10}$ -- in other words, the last digit of the number 12^{346} . First, remember that even in mod 10, you *cannot* replace the exponent with its mod 10 equivalent, i.e. you cannot substitute 6 for 346.

You can, however, replace the base with its mod 10 equivalent. So $12^{346} \equiv 2^{346} \pmod{10}$.

The key to the next step is that powers of 2 follow a cycle in mod 10. We know that:

$$2^1 \equiv 2 \pmod{10}$$

$$2^2 \equiv 4 \pmod{10}$$

$$2^3 \equiv 8 \pmod{10}$$

$$2^4 \equiv 6 \pmod{10} \text{ (because } 2^4 = 16, \text{ and } 16 \equiv 6 \pmod{10}\text{)}$$

After this, the values of $2^n \pmod{10}$ begin to repeat themselves. Since $2^4 \equiv 6 \pmod{10}$, that means

$$2^5$$

$$\equiv 2^4 * 2 \text{ (using the usual laws of exponents)}$$

$$\equiv 6 * 2 \text{ (replacing } 2^4 \text{ with 6 since we showed they were equivalent)}$$

$$\equiv 12 \equiv 2 \pmod{10}$$

And since $2^5 \equiv 2 \pmod{10}$, we're back to the first value we started with for 2^1 . Then $2^6 \equiv 2 * 2 \equiv 4 \pmod{10}$, which is the same as the value for 2^2 , and so on. The values of $2^n \pmod{10}$ follow a cycle, as you can see in the bottom row of the following table:

Number in 2^n form	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	...
Value	2	4	8	16	32	64	128	256	512	1024	2048	4096	...

Mod 10 equivalent (i.e., remainder when divided by 10)	2	4	8	6	2	4	8	6	2	4	8	6	...
---	---	---	---	---	---	---	---	---	---	---	---	---	-----

There's actually a straightforward logical argument why the numbers $a^n \bmod b$ must repeat themselves in a cycle for successive values of n , for any pair of numbers a and b :

- Each value of a^n depends only on the *previous* value -- it is equal to the previous value multiplied by a , mod b , since by the normal laws of exponents, $a^{n+1} \equiv a^n * a \pmod b$
- The sequence of numbers a^1, a^2, a^3 , etc. mod b must eventually contain a repeat value, because there are only finitely many values mod b , and eventually you will run out of available numbers to choose without using repeats. For example, we showed that the first repeat value of $2^n \bmod 10$ was $2^5 \equiv 2 \pmod{10}$.
- Once you hit the first repeat, *all* values after that will be repeats of values seen earlier, and in the same order, because each number is determined by the number immediately before it.

So, back to the original problem: finding $2^{346} \bmod 10$. In the repeating table above, we showed that for all n divisible by 4, $2^n \equiv 6 \pmod{10}$. Therefore, $2^{344} \equiv 6 \pmod{10}$ since 344 is divisible by 4. So

$$\begin{aligned}
 &2^{346} \\
 &\equiv 2^{344} * 2^2 \text{ (by usual laws of exponents)} \\
 &\equiv 6 * 2^2 \text{ (since we showed } 2^{344} \equiv 6 \pmod{10}\text{)} \\
 &\equiv 24 \equiv 4 \pmod{10}
 \end{aligned}$$

Note that to solve this problem, we *did* in fact do modular arithmetic with the exponent -- we know that the values of 2^n repeated themselves every 4 values, so what we cared about was the remainder when 346 was divided by 4. But even though our original problem was in mod 10, when we simplified the exponent, we looked at its value mod 4, *not* mod 10. So in general, when finding $a^n \bmod b$ for large values of n , you will often do modular arithmetic with the exponent n , but the modulus is *not* b . Instead, the modulus is the length of the cycle that it takes for values of $a^n \bmod b$ to repeat themselves.

Sometimes the repeating cycle does not include the number that you started with. Consider the bottom row of this table, which shows the values of $2^n \bmod 12$:

Number in 2^n form	2^1	2^2	2^3	2^4	2^5	2^6	2^7	...
Value	2	4	8	16	32	64	128	...
Mod 12 equivalent (i.e., remainder when divided by 12)	2	4	8	4	8	4	8	...

In the bottom row, once the $\{4, 8\}$ cycle begins, it repeats forever, but the number 2 is never seen again after the first occurrence. However, this pattern can still be used to find values of $2^n \bmod 12$ for large values of n , since the pattern always holds *after* the first exception, 2^1 . You can still observe that for all n other than 1, $2^n \equiv 4 \pmod{12}$ if n is even, and $8 \pmod{12}$ if n is odd.

And of course if $a^n \equiv 0 \pmod{b}$ for any value of n , then for any larger exponent $m > n$, $a^m \equiv 0 \pmod{b}$ as well. For example, consider the values of $6^n \pmod{24}$:

Number in 2^n form	6^1	6^2	6^3	6^4	6^5	...
Value	6	36	216	1296	7776	...
Mod 24 equivalent (i.e., remainder when divided by 24)	6	12	0	0	0	...

Once you hit $6^3 \equiv 0 \pmod{24}$, the bottom row will always be 0 for any exponent greater than 3. The reason of course is that each value is obtained by multiplying the previous value by 6, and 0 multiplied by anything is always 0.

Remainder Theorems

polynomial remainder theorem

The polynomial Remainder Theorem states that the remainder of an unnamed polynomial $f(x)$, divided by a linear factor or linear divisor $x - a$, where a is just some number is equal to $f(a)$. As a result of the long polynomial division, we obtain the quotient polynomial answer $q(x)$ and a polynomial remainder $r(x)$.

Example 1

Polynomial division of $f(x) = x^3 - 12x^2 - 42$ by $x - 3$ gives the quotient $x^2 - 9x - 27$ and the remainder -123 . Therefore $f(3) = -123$.

Example 2

Polynomial division of $f(x) = x^3 - 7x - 6$, by the linear factor $x - 4$ gives the quotient $q(x) = x^2 + 4x + 9$ with a remainder of $r(x) = 30$.

modular remainder theorem

The modular remainder theorem or (also called Chinese remainder theorem) is a statement about simultaneous congruences

Let r and s be positive integers which are relatively prime and let a and b be any two integers. Then there is an integer N such that

$$N \equiv a \pmod{r} \quad \text{and} \quad N \equiv b \pmod{s}.$$

N is uniquely determined modulo rs . An equivalent statement is that if $(r,s)=1$, then every pair of residue classes modulo r and s corresponds to a simple residue class modulo rs .

The theorem can be generalized as follows. Given a set of simultaneous congruences

$$x \equiv a_i \pmod{m_i}$$

For $i=1, \dots, r$ and for which the m_i are pairwise relatively prime, the solution of the set of congruences is

$$x \equiv a_1 b_1 \frac{M}{m_1} + \dots + a_r b_r \frac{M}{m_r} \pmod{M},$$

where $M = m_1 m_2 \dots m_r$ and the b_i are determined from

$$b_i \frac{M}{m_i} \equiv 1 \pmod{m_i}.$$

example

We want to find an integer x such that

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 4 \pmod{4} \\ x &\equiv 1 \pmod{5} \end{aligned}$$

We use the extended Euclidean algorithm for x modulo 3 and 20 $[4 \times 5]$, and find $(-13) \times 3 + 2 \times 20 = 1$, i.e. $e_1 = 40$. For x modulo 4 and 15 $[3 \times 5]$, we get $(-11) \times 4 + 3 \times 15 = 1$, i.e. $e_2 = 45$. Finally, for x modulo 5 and 12 $[3 \times 4]$, we get $5 \times 5 + (-2) \times 12 = 1$, i.e. $e_3 = -24$. A solution x is therefore $2 \times 40 + 3 \times 45 + 1 \times (-24) = 191$. All other solutions are congruent to 191 modulo 60, $[3 \times 4 \times 5 = 60]$ which means that they are all congruent to 11 modulo 60.

Russian peasant algorithm

suppose you want to find the value of $7^{17} \pmod{34}$ then you could write out a table to find when the values of $7^n \pmod{34}$ begin to repeat themselves:

Number in 7^n form	7^1	7^2	7^3	7^4	7^5	7^6	7^7	7^8	7^9	7^{10}	7^{11}	7^{12}	7^{13}	7^{14}	7^{15}	7^{16}	7^{17}
value mod 34	7	15	3	21	11	9	29	33	27	19	31	13	23	25	5	1	7

To obtain each value, we take the previous value, multiply by 7, and find the remainder mod 34. However, we have to go all the way to 7^{17} before we see a repeat value. There is a shorter method which, the "Russian peasant algorithm". Observe that the exponent, 17, is close to $16 = 2^4$. So if we can calculate $7^{16} \pmod{34}$, we can easily calculate $7^{17} \pmod{34}$, by multiplying it by another 7. To find $7^{16} \pmod{34}$, we can start with $7 \pmod{34}$ and then square it repeatedly, keeping in mind the familiar law of exponents that $a^{bc} = (a^b)^c$:

$$7^2 \equiv 49 \equiv 15 \pmod{34}$$

$$7^4 \equiv (7^2)^2 \equiv 15^2 \equiv 225 \equiv 21 \pmod{34} \quad (\text{by substituting the value } 7^2 \equiv 15 \pmod{34} \text{ that we})$$

obtained in the previous step)

$7^8 \equiv (7^4)^2 \equiv 21^2 \equiv 441 \equiv 33 \pmod{34}$ (by substituting the value $7^4 \equiv 21 \pmod{34}$ that we obtained in the previous step)

Here we use a technique that we mentioned earlier: replace a number with a smaller negative number that is equivalent. In this case, $33 \equiv -1 \pmod{34}$, so:

$7^8 \equiv 33 \equiv (-1) \pmod{34}$

which means: $7^{16} \equiv (7^8)^2 \equiv (-1)^2 \equiv 1 \pmod{34}$ (by substituting the value $7^8 \equiv -1 \pmod{34}$ that we obtained in the previous step)

and now, using 7^{16} to get 7^{17} :

$7^{17} \equiv 7^{16} * 7 \equiv 1 * 7 \equiv 7 \pmod{34}$

example, suppose you wanted to compute $7^{49} \pmod{34}$. Since $49 = 2^4 * 3 + 1$, these steps would be fastest (note that in each step, you are only using values obtained in previous steps):

- compute 7^2
- compute $7^4 = (7^2)^2$
- compute $7^8 = (7^4)^2$
- compute $7^{16} = (7^8)^2$
- compute $7^{48} = 7^{16} * 7^{16} * 7^{16}$
- compute $7^{49} = 7^{48} * 7$

Often it is a matter of guesswork to find the fastest route to compute a given exponent. For example, to compute $7^{56} \pmod{34}$, this route would be efficient:

- compute $7^3 = 7 * 7 * 7$
- compute $7^9 = 7^3 * 7^3 * 7^3$
- compute $7^{27} = 7^9 * 7^9 * 7^9$
- compute $7^{54} = 7^{27} * 7^{27}$
- compute 7^2
- compute $7^{56} = 7^{54} * 7^2$

So, when finding $a^n \pmod{b}$ for large values of n , the Russian peasant algorithm is useful when:

- b is large (e.g., 34), which means there are many possible values mod b , and the values of a^n might cycle through many different numbers before you see your first repeat, so the method of looking for a repeating cycle might be cumbersome
- the exponent n is equal to, or slightly larger than, a number that can be obtained by multiplying powers of small numbers like 2 and 3.

Wilson's theorem is a simple result that leads to a number of interesting observations in elementary number theory. It states that, if p is prime then

$$1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv p - 1 \pmod{p}$$

We know the inverse of $p - 1$ is $p - 1$, so each other number can be paired up by its inverse and *eliminated*. For example, let $p = 7$, we consider

$$1 \times 2 \times \dots \times 6 \equiv (2 \times 4) \times (3 \times 5) \times 1 \times 6 = 6$$

6. Continued fractions and series

Goldbach-Euler series

Theorem 1 of Euler series

$1 = \frac{1}{3} + \frac{1}{7} + \frac{1}{8} + \frac{1}{15} + \frac{1}{24} + \frac{1}{26} + \frac{1}{31} + \frac{1}{35} + \text{etc} = \frac{1}{m^n + 1}$ where m and n are integers greater than 1.

Proof by Euler.

Euler takes x to be the sum of the following harmonic series (not favoured by mathematicians today):

$$x = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \text{etc}$$

from which he subtracts the geometric series:

$$1 = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32} + \text{etc}$$

giving

$$x - 1 = 1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{9} + \frac{1}{10} + \text{etc}$$

Subtracting another geometric series

$$\frac{1}{2} = \frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \frac{1}{81} + \frac{1}{243} + \text{etc}$$

will give

$$x - 1 - \frac{1}{2} = 1 + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{10} + \frac{1}{11} + \text{etc}$$

Subtracting another geometric series

$$\frac{1}{4} = \frac{1}{5} + \frac{1}{25} + \frac{1}{125} + \text{etc}$$

from it will give:

$$x - 1 - \frac{1}{2} - \frac{1}{4} = 1 + \frac{1}{6} + \frac{1}{7} + \frac{1}{10} + \text{etc}$$

Euler skipped subtracting the geometric series $\frac{1}{3} = \frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \frac{1}{256} + \text{etc}$ because 3 is a power less than 4 and the series of power $\frac{1}{4}$ is a subseries of powers of $\frac{1}{2}$. He skipped 7 because it is one less than the cube 8, skip 8 because it is one less than the square 9, 15 because it is one less than the square 16, etc. This method eliminated all terms on the right, leaving

$$x - 1 - \frac{1}{2} - \frac{1}{4} - \frac{1}{5} - \frac{1}{6} - \frac{1}{9} - \text{etc} = 1 \quad \text{so that} \quad x - 1 = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{9} + \frac{1}{10} + \text{etc}.$$

Because x is the sum of the harmonic series, Euler assumed that the 1 on the left is equal to the terms of the harmonic series that are missing on the right: the ones with denominators one less than powers, so that Euler concluded:

$$1 = \frac{1}{3} + \frac{1}{7} + \frac{1}{8} + \frac{1}{15} + \frac{1}{24} + \frac{1}{26} + \frac{1}{31} + \frac{1}{35} + \text{etc} = \frac{1}{m^n + 1}$$

Theorem 2 of Euler series

$$\frac{1}{3} + \frac{1}{7} + \frac{1}{15} + \frac{1}{31} + \frac{1}{35} + \frac{1}{63} + \text{etc} = \ln 2 = \frac{1}{2} + \frac{1}{4} + \frac{1}{24} + \dots = \sum_{n=1}^{\infty} \frac{1}{n \cdot 2^n}$$

Theorem 3 of Euler series

$$1 - \frac{1}{8} - \frac{1}{24} + \frac{1}{28} - \frac{1}{48} - \frac{1}{80} - \frac{1}{120} - \frac{1}{124} - \frac{1}{168} - \frac{1}{224} + \frac{1}{244} - \frac{1}{288} - \text{etc} = \frac{\pi}{4}$$

Theorem 4 of Euler series

$$1 - x + x^2 - x^3 + \dots = \frac{1}{1+x}$$

Theorem 5 of Euler

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots + (-1)^k \frac{x^{2k+1}}{(2k+1)!} + \dots$$

Theorem 6 of Euler series

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}. \quad (\text{the Basel problem})$$

Euler also found a remarkable infinite product formula that relates pi to the nth prime number.

$$\pi = \frac{2}{\prod_{n=2}^{\infty} \left[1 + \frac{(-1)^{(p_n-1)/2}}{p_n} \right]}$$

theorem

The series $\sum_{n=0}^{\infty} \frac{1}{n!}$ is called Euler's series. It converges to Euler's number e .

Proof:

We use the ratio test:

$$\lim_{n \rightarrow \infty} \frac{1/(n+1)!}{1/n!} = \lim_{n \rightarrow \infty} \frac{n!}{(n+1)!} = \lim_{n \rightarrow \infty} \frac{1}{n+1} = 0$$

Hence, the series converges by the ratio test. The proof that this sum equals that limit is very similar to the proof that the Euler sequence converges. We use the binomial theorem to expand the expression

$$\begin{aligned} \left(1 + \frac{1}{n}\right)^n &= 1 + \frac{n}{1} \left(\frac{1}{n}\right) + \frac{n(n-1)}{2!} \left(\frac{1}{n}\right)^2 + \frac{n(n-1)(n-2)}{3!} \left(\frac{1}{n}\right)^3 + \dots + \frac{n(n-1)\dots 1}{n!} \left(\frac{1}{n}\right)^n = \\ &= 1 + 1 + \frac{1}{2!} \frac{n(n-1)}{n \cdot n} + \frac{1}{3!} \frac{n(n-1)(n-2)}{n \cdot n \cdot n} + \dots + \frac{1}{n!} \frac{n(n-1)\dots 1}{n \cdot n \cdot \dots \cdot n} = \\ &= 1 + 1 + \frac{1}{2!} \left(1 - \frac{1}{n}\right) + \frac{1}{3!} \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) + \dots + \frac{1}{n!} \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \dots \left(1 - \frac{n-1}{n}\right) \end{aligned}$$

From this expansion it is clear that

$$\left(1 + \frac{1}{n}\right)^n \leq \sum_{k=0}^n \frac{1}{k!}$$

because each term in parenthesis is smaller than one. We also have:

$$\begin{aligned} \left(1 + \frac{1}{n}\right)^n &= 1 + 1 + \frac{1}{2!} \left(1 - \frac{1}{n}\right) + \frac{1}{3!} \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) + \dots + \frac{1}{n!} \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \dots \left(1 - \frac{n-1}{n}\right) \\ &\geq 1 + 1 + \frac{1}{2!} \left(1 - \frac{1}{n}\right) + \frac{1}{3!} \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) + \dots + \frac{1}{N!} \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \dots \left(1 - \frac{N-1}{n}\right) \end{aligned}$$

for $N < n$, because each term in parenthesis is greater than zero. But then, taking the limit as n approaches infinity, we have:

$$\lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n \geq 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{N!} \geq \left(1 + \frac{1}{N}\right)^N$$

Hence, taking the limit as N approaches infinity, we have the sum squeezed in between the limit of Euler's sequence, which we know is equal to e .

Continued Fractions

Any fraction, P/Q (P and Q are whole, positive numbers) expressing it in the form of a **continued fraction** as follows:

$$\frac{P}{Q} = a + \frac{1}{b + \frac{1}{c + \frac{1}{d + \dots}}} = a + 1/(b + 1/(c + 1/(d + \dots))) = a + \frac{1}{b + \frac{1}{c + \frac{1}{d + \dots}}}$$

where a, b, c, d, e , etc are all whole numbers. If P/Q is less than 1, then the first number, a , will be 0. (Instead of letters a, b, c, d , also the letters a_0, a_1, a_2, a_3 , etc... are used).

We can write down any continued fraction such as

$$P/Q = a + 1/(b + 1/(c + 1/(d + \dots)))$$

just as a list of the numbers a, b, c, \dots . Since the *first* number, a , is the whole number part of the value it is separated from the rest by a semicolon (;) and the rest are written as a list with comma separators (,) :

$$P/Q = [a; b, c, d, \dots]$$

Notice: $[\dots, a, b] = [\dots, a + 1/b]$

if $[a_0, a_1, \dots, a_{n-1}, a_n]$ is A/B and

$[a_0, a_1, \dots, a_{n-1}]$ is C/D then

$[a_n, a_{n-1}, \dots, a_0] = A/C$

For example: $[1, 1, 1, 2] = 8/5$ and $[1, 1, 1] = 3/2$ so $[2, 1, 1, 1] = 8/3$

If the fraction is less than 1, we use its reciprocal and then we can split it into a whole-number part plus another fraction which will be less than 1 and repeat. We stop when the fraction has a numerator *or* a denominator of 1.

examples: $7/30$ is already less than 1 so we start off by writing it as

$$\begin{aligned}
7/30 &= 0 + 1/(30/7) \\
&= 0 + 1/(4 + 2/7) \\
&= 0 + 1/(4 + 1/(7/2)) \\
&= 0 + 1/(4 + 1/(3 + 1/2)) \\
&= 0 + 1/(4 + 1/(3 + 1/(1 + 1/1)))
\end{aligned}$$

$$\begin{aligned}
1/8 &= 0.125 = 0, 8 && = 0, 7, 1 \\
2/8 &= 0.25 = 0, 4 && = 0, 3, 1 \\
3/8 &= 0.375 = 0, 2, 1, 2 && = 0, 2, 1, 1, 1 \\
4/8 &= 0.5 = 0, 2 && = 0, 1, 1 \\
5/8 &= 0.625 = 0, 1, 1, 1, 2 && = 0, 1, 1, 1, 1, 1 \\
6/8 &= 0.75 = 0, 1, 3 && = 0, 1, 2, 1 \\
7/8 &= 0.875 = 0, 1, 7 && = 0, 1, 6, 1
\end{aligned}$$

$$\begin{aligned}
2.25 &= 9/4 = [2; 4] \\
1/2.25 &= 4/9 = [0; 2, 4]
\end{aligned}$$

2·875 to an equivalent fraction we get 2875/1000 and Euclid's algorithm gives:

$$\begin{aligned}
2875 &= 2 \times 1000 + 875 \\
1000 &= 1 \times 875 + 125 \\
875 &= 7 \times 125
\end{aligned}$$

$$\text{so } 2875/1000 = [2; 1, 7]$$

One of the often studied algorithms in computing science is *Euclid's Algorithm for finding the greatest common divisor (gcd) of two numbers*. The *greatest common divisor* (often just abbreviated to **gcd**) also called *the highest common factor* (or just **hcf**) in *Euclid's Algorithm* can be found with continued fractions.

Example: 45/16.

45	=	2 x	16	+	13	:	45 is a multiple of 16 with 13 left over
16	=	1 x	13	+	3	:	16 is a multiple of 13 with 3 left over
13	=	4 x	3	+	1	:	13 is a multiple of 3 with 1 left over
3	=	3 x	1	+	0	:	3 is a multiple of 1 exactly.
L	=	Nx	S	+	R		

The (N) are the continued fraction numbers. The L column is the Longest side of each rectangle and S the Shortest side and R being the Remainder. The method works for any two numbers and always terminates since each time L, R and S are reduced until eventually S is 1 and R is 0.

$$a = [a_0; a_1, a_2, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_n}}}}$$

is the simple (i.e. with all nominators equal to 1) finite continued fraction. Let

$\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n]$ be the n^{th} convergent of a . If the sequence p_n/q_n converges to some limit a when $n \rightarrow \infty$ then the infinite continued fraction $[a_0; a_1, a_2, \dots, a_n]$ converges to the same limit a . The sufficient and necessary condition for convergence of this continued fraction is the divergence of the series $\sum_{n=1}^{\infty} a_n$. If the infinite continued fraction is convergent then the values of the convergents p_k/q_k approximate the value of a with accuracy $1/q_k q_{k+1}$:

$$\left| a - \frac{p_k}{q_k} \right| < \frac{1}{q_k q_{k+1}}$$

If we put $a_n = p_n$ where p_n denotes the n^{th} primes: $[0; 2, 3, 5, 7, 11, 13, \dots]$. Since there is an infinity of primes the above condition is fulfilled and the limit of the continued fraction

$$a = [0; 2, 3, 5, 7, 11, \dots] = \frac{1}{2 + \frac{1}{3 + \frac{1}{5 + \frac{1}{7 + \frac{1}{11 + \dots}}}}}$$

can be calculated up to a given prime number. M. Wolf (in continued fractions constructed from prime numbers, 2010) found that $u = [0, 2, 3, 5, 7, \dots, 9973] = 0.4323320871 \dots$

Generating a few number series with continued fractions

We consider the following **irregular** continued fractions

$$\alpha = 1 + \frac{b-2}{2 - \frac{b+2}{b+1 - \frac{1}{b - \frac{1}{b - \frac{1}{b - \dots}}}}} \quad (b \geq 2) \quad (\text{eq. \#})$$

and

$$\beta = \frac{1}{b - \frac{1}{b - \frac{1}{b - \dots}}}$$

Which is easily shown to be equal to $\beta = \frac{1}{2}(b - \sqrt{b^2 - 4})$, so that it follows that $\alpha = \frac{1}{2}(b + \sqrt{b^2 - 4})$ and α is the conjugate of β so that $\alpha = 1/\beta$, where α and β are the roots of the quadratic $x^2 - bx + 1 = 0$ and also satisfy $\alpha + \frac{1}{\alpha} = \beta + \frac{1}{\beta} = b$.

The **simple** continued fraction expansions of α and β are:

$$\alpha = b - 1 + \frac{1}{1 + \frac{1}{b - 2 + \frac{1}{1 + \frac{1}{b - 2 + \dots}}}}$$

$$\beta = \frac{1}{b - 1 + \frac{1}{1 + \frac{1}{b - 2 + \frac{1}{1 + \frac{1}{b - 2 + \dots}}}}}$$

In certain cases $\sqrt{\alpha}$ and $\sqrt{\beta}$ are also quadratic irrationals and not quartic (biquadratic) irrationals, because

$$\sqrt{\alpha} = (\sqrt{b} + \sqrt{b^2 - 4}) / \sqrt{2} = \frac{1}{2}(\sqrt{b+2} + \sqrt{b-2})$$

$$\sqrt{\beta} = (\sqrt{b} - \sqrt{b^2 - 4}) / \sqrt{2} = \frac{1}{2}(\sqrt{b+2} - \sqrt{b-2})$$

If $b = x^2 + 2$ then

$$\sqrt{\alpha} = \frac{1}{2}(x + \sqrt{x^2 + 4}) = x + \frac{1}{x + \frac{1}{x + \frac{1}{x + \dots}}} ; \quad \sqrt{\beta} = \frac{1}{2}(\sqrt{x^2 + 4} - x) = \frac{1}{x + \frac{1}{x + \frac{1}{x + \dots}}}$$

If $b = x^2 - 2$ then

$$\sqrt{\alpha} = \frac{1}{2} \left(x + \sqrt{x^2 - 4} \right) = x - \frac{1}{1 + \frac{1}{x - 2 + \frac{1}{1 + \frac{1}{x - 2 + \frac{1}{1 + \frac{1}{x - 2 + \dots}}}}} ;$$

$$\sqrt{\beta} = \frac{1}{2} \left(x - \sqrt{x^2 - 4} \right) = \frac{1}{x - 1 + \frac{1}{1 + \frac{1}{x - 2 + \frac{1}{1 + \frac{1}{x - 2 + \frac{1}{1 + \frac{1}{x + 2 + \dots}}}}}}$$

Determining the convergents p_n/q_n of the continued fractions gives:

$$p_1/q_1 = 1/1 \quad ; \quad p_2/q_2 = b/2 \quad ; \quad p_3/q_3 = (b^2 - 2)/b$$

and also for $n > 1$ there holds that $p_n = q_{n+1}$

If we consider the Fibonacci-like sequence defined by the second order recurrence

$$a_n = b a_{n-1} - a_{n-2} ; \quad a_0 = 2 \quad ; \quad a_1 = b$$

then by theory of difference equations it can be shown that

$$a_n = \left[\frac{1}{2} (b + \sqrt{b^2 - 4}) \right]^n - \left[\frac{1}{2} (b - \sqrt{b^2 - 4}) \right]^n$$

From above equation we can show that $a_{2n} = a_n^2 - 2$.

Be Cause we found that $\alpha = \frac{1}{2} (b + \sqrt{b^2 - 4})$ and $\beta = \frac{1}{2} (b - \sqrt{b^2 - 4})$, it follows that

$$a_n = \alpha_n + \beta_n \text{ and also by induction it follows that } a_n = p_{n+1} = q_{n+2}.$$

- the case $b=3$

$$\text{If } b=3 \text{ then } \alpha = \frac{1}{2} (3 + \sqrt{5}) = \Phi + 1 \text{ where } \Phi \text{ is the golden ratio and } \beta = \frac{1}{2} (3 - \sqrt{5}) = 2 - \Phi$$

The sequence of numerators p_n for the continued fraction (eq.#) becomes:

$$3, 7, 18, 47, 123, 322, 843, 2207, \dots$$

For $n > 1$, $p_n = L_{2n-2}$, where L_n is the Lucas sequence defined by $L_0=2, L_1=1, L_n=L_{n-1} + L_{n-2}$

Another sequence studied by Lucas is $P_{2^n+1} = r_n$ defined by $r_0=3$, $r_{n+1}=r_n^2-2$ and giving the sequence P_n

3, 7, 47, 2207, 4870847

which was used to test the primality of Mersenne numbers of the form $2^{4m+3}-1$, where $4m+3$ is a prime number. Sierpinski found that

$$\beta = \frac{1}{2}(3 - \sqrt{5}) = 2 - \phi = \frac{1}{r_0} + \frac{1}{r_0 r_1} + \frac{1}{r_0 r_1 r_2} + \frac{1}{r_0 r_1 r_2 r_3} + \dots$$

I will use the sequence P_n to test general primes in the section on primality tests.

- the case $b=4$

If $b=4$ then $\alpha = 2 + \sqrt{3}$ and $\beta = 2 - \sqrt{3}$ and the sequence p_n is given by

4, 14, 52, 194, 724, 2702, 10084, 37634,

Another sequence studied by Lucas is $P_{2^n+1} = S_n$ defined by $s_0=4$, $s_{n+1}=s_n^2-2$ used to test the primality of Mersenne numbers. The test was improved by Lehmer to the form:

If n is an odd prime then 2^n-1 is prime if and only if it evenly divides s_{n-1} , whereby s_n is given by:

4, 14, 194, 37634, 1416317954, ...

- the case $b=5$

If $b=5$ then $\alpha = 5/2 + 1/2\sqrt{21}$ and $\beta = 5/2 - 1/2\sqrt{21}$ and the sequence p_n is given by

5, 23, 52, 110, 527, 2525, 12098,

while for $b=\sqrt{5}$ the values become $\alpha = \frac{1}{2}(1 + \sqrt{5}) = \Phi$ and $\beta = \frac{1}{2}(-1 + \sqrt{5}) = \Phi - 1$ and the sequence becomes: $\sqrt{5}, 3, 2\sqrt{5}, 7, 5\sqrt{5}, 18, 13\sqrt{5}, 47, \dots$

Form the equation $a_n = \left[\frac{1}{2}(b + \sqrt{b^2 - 4}) \right]^n - \left[\frac{1}{2}(b - \sqrt{b^2 - 4}) \right]^n$ it can be shown that

$p_{2n}/\sqrt{5} = F_{2n-1}$, where F_n is the Fibonacci sequence defined by $F_0=0$, $F_1=1$, $F_n = F_{n-1} + F_{n-2}$. Also that $p_{2n+1} = L_{2n}$ where L_n is the Lucas sequence defined by $L_0=0$, $L_1=1$, $L_{n+2} = L_{n+1} + L_n$:

2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843

The beginning few terms of the Fibonacci series are :

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, ...

- the case $b=6$

If $b=6$ then $\alpha = 3 + 2\sqrt{2}$ and $\beta = 3 - 2\sqrt{2}$ and the sequence p_n is given by

6, 34, 198, 1154, 6726, 39202, ...

This sequence is used to determine if the product of three consecutive triangular numbers

$T_{n-1}T_nT_{n+1}$ is a square, which is the case if $n = (3p_k - 2)/4$.

Lucas also studied the sequence $P_{2^n+1} = V_n$ to test the primality of Fermat numbers

$2^{2^n} + 1$, whereby $v_0 = 6$ and $v_{n+1} = v_n^2 - 2$ and the sequence v_n is given by:

6, 34, 1154, 1331714, ...

The convergents p_n/q_n of $\alpha = 1 + \frac{b-2}{2 - \frac{b+2}{b+1 - \frac{1}{b - \frac{1}{b - \frac{1}{b - \dots}}}}}$

for $b=2,3,4,5,6$ and $n=1,2,3,4,5,6,7,8,9$ are given in the table below.

b/n	1	2	3	4	5	6	7	8	9
2	$\frac{1}{1}$	$\frac{2}{2}$	$\frac{2}{2}$	$\frac{2}{2}$	$\frac{2}{2}$	$\frac{2}{2}$	$\frac{2}{2}$	$\frac{2}{2}$	$\frac{2}{2}$
3	$\frac{1}{1}$	$\frac{3}{2}$	$\frac{7}{3}$	$\frac{18}{7}$	$\frac{47}{18}$	$\frac{123}{47}$	$\frac{322}{123}$	$\frac{843}{322}$	$\frac{2207}{843}$
4	$\frac{1}{1}$	$\frac{4}{2}$	$\frac{14}{4}$	$\frac{52}{14}$	$\frac{194}{52}$	$\frac{724}{194}$	$\frac{2702}{724}$	$\frac{10084}{2702}$	$\frac{37634}{10084}$
5	$\frac{1}{1}$	$\frac{5}{2}$	$\frac{23}{5}$	$\frac{110}{23}$	$\frac{527}{110}$	$\frac{2525}{527}$	$\frac{12098}{2525}$	$\frac{57965}{12098}$	$\frac{277727}{57965}$
6	$\frac{1}{1}$	$\frac{6}{2}$	$\frac{34}{6}$	$\frac{198}{34}$	$\frac{1154}{198}$	$\frac{6726}{1154}$	$\frac{39202}{6726}$	$\frac{228486}{39202}$	$\frac{1331714}{228486}$

Golden ratio, Fibonacci and Lucas numbers

The simultaneously additive and multiplicative nature of the golden section is expressed in the simple quadratic equation $a^2 - a = 1$ which has two solutions, one positive, one negative, namely Φ and $-\Phi^{-1}$.

$$a_1 = \frac{1}{2} + \frac{1}{2} \sqrt{5} \quad ; \quad a_2 = \frac{1}{2} - \frac{1}{2} \sqrt{5}$$

$$\text{thus } \Phi = \frac{1}{2} + \frac{1}{2} \sqrt{5} = 1.61803398874989484882..$$

$$\text{and } 1/\Phi = -\frac{1}{2} + \frac{1}{2} \sqrt{5} = 0.61803398874989484882.. = \varphi$$

This also give the following identities:

$$\Phi = 1 + \frac{1}{\Phi} \quad \text{and} \quad \Phi = \sqrt{1 + \Phi}$$

Taking the eq. $\Phi = 1 + \frac{1}{\Phi}$ and repeatedly substituting for Φ produces the simplest continued fraction:

$$\Phi = 1 + \frac{1}{1 + \frac{1}{\Phi}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\Phi}}} = \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\Phi}}}} = [1; 1, 1, 1, 1, \dots]$$

$$\frac{1}{\Phi} = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\Phi}}} = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\Phi}}}} = [0; 1, 1, 1, 1, \dots]$$

Taking the eq. $\Phi = \sqrt{1 + \Phi}$ and repeatedly substituting for Φ produces the simplest nested root or radical:

$$\Phi = \sqrt{1 + \sqrt{1 + \Phi}} = \sqrt{1 + \sqrt{1 + \sqrt{1 + \Phi}}} = \sqrt{1 + \sqrt{1 + \sqrt{1 + \sqrt{1 + \sqrt{1 + \dots}}}}}$$

We know that

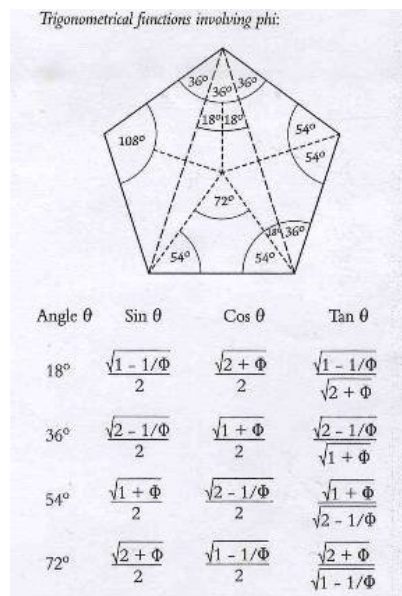
$\Phi^{-1} = \Phi - 1$
$\Phi^1 = \Phi + 0$
$\Phi^2 = \Phi + 1$
$\Phi^3 = \Phi + 2 = \Phi^2 + 1$
$\Phi^4 = \Phi + 3 = \Phi^2 + 2 = \Phi^3 + 1$
Etc

- Richard Feynman found that $e^{i\pi} = \Phi^{-1} - \Phi$

- We also have the two results $2 \sin(i \ln \Phi) = i$ and $2 \sin(\pi/2 - i \ln \Phi) = \sqrt{5}$

- Φ is connected to the binary “rabbit sequence” which never contains 00 or 111:
1011010110 1101011010 1101101011 0110101101 0110110101 1010110110

-Lindemann in 1872 proofed that π is transcendental. An approximation of circle quadrature was by making a square with sides of π , which is calculated by $\pi = \frac{6(1 + \Phi)}{5}$



In the 10th century, it was attempted to classify all even perfect numbers (numbers equal to the sum of their proper divisors) as those of the form $2^{k-1}(2^k - 1)$ where $2^k - 1$ is prime, which led to state Wilson's theorem, namely that if p is prime then $1 + (p - 1)!$ is divisible by p . It is called Wilson's theorem because of a comment made by Edward Waring in 1770 that John Wilson had noticed the result but Lagrange gave the first proof in 1771.

In the 13th century, Leonardo de Pisa (better known as Fibonacci), wrote one of his greatest works, the *Liber Quadratorum*. In this work he deals with Pythagorean triple. He noted that square numbers can be constructed as sums of odd numbers. He defined the concept of a

congruum, a number of the form $ab(a + b)(a - b)$, if $a + b$ is even, and 4 times this if $a + b$ is odd. Fibonacci proved that a congruum must be divisible by 24 and he also showed that for x, c such that $x^2 + c$ and $x^2 - c$ are both squares, then c is a congruum. He also proved that a square cannot be a congruum. His contribution to number theory were so great that it has been said that the Liber quadratorum alone ranks Fibonacci as the major contributor to number theory in Europe between Diophantus and the 17th-century French mathematician Pierre de Fermat.

The Fibonacci series is given by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ and the Fibonacci sequence is given by

$$F_n = 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181$$

The formula for the n^{th} number in the Fibonacci Sequence is

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} \quad \text{where} \quad \alpha = \frac{1 + \sqrt{5}}{2} \quad \text{and} \quad \beta = 1 - \frac{\sqrt{5}}{2} \quad \text{or}$$

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right]$$

We can also write for $F_n = \frac{[\Phi^n - (-\Phi^{-n})]}{\sqrt{5}}$ (Binet's formula)

If we compute this for $n=19$, we obtain:

$$F_{19} := \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{19} - \left(\frac{1 - \sqrt{5}}{2} \right)^{19} \right) = 4181$$

Lagrange proved that

$$F_{n+60} \equiv F_n \pmod{10}.$$

Thus the last digit of a Fibonacci number recurs in cycles of length 60.

Also

$$F_{2n+1} \equiv F_{n+1}^2 \pmod{F_n^2}$$

Cassini formula for Fibonacci numbers is

$$(F_{n-1})(F_{n+1}) - (F_n)^2 = (-1)^n$$

Negative termed Fibonacci numbers are given by:

$$F_{-n} = (-1)^{n+1} \cdot F_n$$

Every n^{th} Fibonacci number is a multiple of F_n , so F_n is a factor of every n^{th} Fibonacci number. This $F_3=2$ divides every 3rd Fibonacci number, meaning that every third Fibonacci number is even; $F_4=3$ means that every 4th Fibonacci number is divisible by 3; $F_5=5$ divides

every 5th Fibonacci number; $F_6=8$ divides every 6th Fibonacci number. Also if n is a factor of m , then F_n will be a factor of F_m .

The sum of the first n Fibonacci numbers

$$\sum_n F_n = F_{(n+2)} - 1$$

is one less than the $n+2^{\text{nd}}$ Fibonacci number. Odd-numbered Fibonacci terms sum to the next even-numbered Fibonacci term while even-termed Fibonacci numbers sum to one less than the next odd-numbered term.

The sum of the squares of the first n Fibonacci numbers is equal to the product of the n^{th} and the $n+1^{\text{th}}$ numbers:

$$\sum_n (F_n)^2 = F_n \cdot F_{(n+1)} - F_{(n-1)}$$

The sum of the squares of 2 consecutive Fibonacci numbers is

$$(F_n)^2 + (F_{n+1})^2 = (F_{2n+1})$$

We saw that the Lucas series is defined by :

$$L_0=2, L_1=1 \text{ and } L_{n+2}=L_{n+1} + L_n$$

The first few Lucas numbers are:

$$L_n = 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322..$$

The Binet formula for Lucas numbers is given by :

$$L_n = \Phi^n + (-\Phi^{-n})$$

negative termed Lucas numbers are given by : $L_{-n} = (-1)_n \cdot L_n$

and the Cassini formula for Lucas numbers is given by :

$$(L_n)^2 - (L_{n+1}) \cdot (L_{n-1}) = 5(-1)^n$$

which means that each Fibonacci number is the approximate geometric mean of its two adjacent numbers, alternately needing correction by +1 and -1 and that each Lucas number is the approximated geometric mean of its two neighbours alternately corrected by -5 or +5. The

two are further related by the expansion of Binet's formula as $\Phi_n = \frac{L_n + F_n \sqrt{5}}{2}$.

Lucas numbers are converted into Fibonacci number by :

$$L_n = F_{n+1} + F_{n-1}$$

The n^{th} Lucas number is the sum of the $n+1^{\text{th}}$ and $n-1^{\text{th}}$ Fibonacci numbers. Related to this is :

$$L_n = F_{n+2} + F_{n-2}$$

We also have $L_n = F_n + 2F_{n-1}$ and any four consecutive Fibonacci numbers sum to a Lucas number. Also there holds that $F_{2n} = F_n L_n$ and $L_n + F_n = 2F_{n+1}$

From Binet's formula it can be derived that

$$L_{2n} = 2/\cosh(n \ln \Phi) \quad \text{and} \quad L_{2n+1} = 2 \sinh(n \ln \Phi)$$

In 2003 Alexey Stakhov found that

$$\sin F_n + \cos F_n = \sin F_{n+1} \quad \text{and} \quad \sin L_n + \cos L_n = \cos L_{n+1}$$

7. Factorials

The **factorial** of a positive integer n , denoted by $n!$, is the product of all positive integers less than or equal to n . For example,

$$3! = 1 \times 2 \times 3 = 6$$

In general:

$$n! = \prod_{k=1}^n k = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$$

$0!$ is a special case that is explicitly defined to be 1. There also holds

$$(n + 1)n! = (n + 1)!, \quad n > 0 \quad (\text{eq. *})$$

The interpolation of factorial, therefore, consisted in finding an analytical expression, such that by entering into a formula should provide positive number in the output value of the factorial, which was supposed to make sense even if a whole n but not fractional (rational). Euler noted that if n is a positive integer then the factorial can be written as:

$$\left[\left(\frac{2}{1} \right)^n \cdot \frac{1}{n+1} \right] \left[\left(\frac{3}{2} \right)^n \cdot \frac{2}{n+2} \right] \left[\left(\frac{4}{3} \right)^n \cdot \frac{3}{n+3} \right] \dots = n!$$

If we put $n = 4 \frac{1}{2}$ in the previous formula (eq. *) get $(4 \frac{1}{2} + 1)! = 5 \frac{1}{2} (4 \frac{1}{2})!$

$$\left(5 \frac{1}{2}! \right) = \left(\frac{3}{2} \right) \left(\frac{5}{2} \right) \left(\frac{7}{2} \right) \left(\frac{9}{2} \right) \left(\frac{11}{2} \right) \left(\frac{1}{2} \right)!$$

Since $(1/2)! = \frac{1}{2} \sqrt{\pi}$ we can solve this, likewise:

$$\left(-5 \frac{1}{2}! \right) = \left(\frac{2}{1} \right) \left(-\frac{2}{1} \right) \left(-\frac{2}{3} \right) \left(-\frac{2}{5} \right) \left(-\frac{2}{7} \right) \left(-\frac{2}{9} \right) \left(\frac{1}{2} \right)!$$

Euler noticed that when you enter the value $n = \frac{1}{2}$ you get on the right side the "infinite product" by John Wallis

$$\left(\frac{2 \cdot 2}{1 \cdot 3} \right) \left(\frac{4 \cdot 4}{3 \cdot 5} \right) \left(\frac{6 \cdot 6}{5 \cdot 7} \right) \left(\frac{8 \cdot 8}{7 \cdot 9} \right) \dots = \frac{\pi}{2}$$

In general:

$$\left(n + \frac{1}{2} \right)! = \sqrt{\pi} \frac{(2n+1)!}{2^{2n+1} n!}$$

So $3\frac{1}{2}! = \sqrt{\pi} \frac{105}{16} \approx 11.63$

The gamma function defined for all complex numbers (except negative integers -1,-2,-3) :

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt$$

for integer numbers is a shifted version of the factorial function:

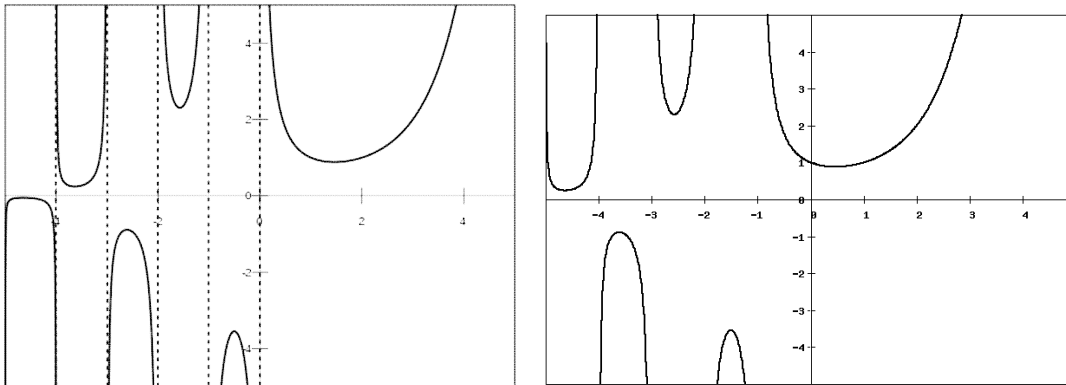
$$\Gamma(n + 1) = n!$$

There also holds:

$$\Gamma(n + 1) = n\Gamma(n)$$

Euler's gave his original formula for the Gamma function as:

$$\Gamma(z) = \lim_{n \rightarrow \infty} \frac{n^z n!}{\prod_{k=0}^n (z + k)}$$



The Gamma function on the real axis (left) and the factorial function (right) generalized to all complex numbers except negative integers.

For large values n we can use the Stirling approximation:

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

For large values of the argument , the factorial can be approximated through the integral of the digamma functionm using the contined fraction :

$$\text{Fac}(z) = \exp(P(z))$$

$$P(z) = p(z) + \frac{\log(2\pi)}{a_0^2} - z + \left(z + \frac{1}{2}\right) \log(z)$$

$$p(z) = \frac{a_0^2}{z + \frac{a_1}{z + \frac{a_2}{z + \frac{a_3}{z + \dots}}}}$$

Other factorial rules are:

$$n! = (n - 1)! \cdot n$$

$$n! = \frac{(n + 1)!}{n + 1}$$

$$(n - 1)! = \frac{n!}{n}$$

$$(n + 1)! = (n + 1) \cdot n!$$

$$(n + k)! = \frac{[n + (k + 1)]!}{n + (k + 1)}$$

$$\frac{n!}{(n + 1)!} = \frac{1}{n + 1}$$

$$\frac{(n - 1)!}{n!} = \frac{1}{n}$$

$$\frac{(n + 1)!}{(n - 1)!} = n(n + 1)$$

$$(n!)^i = n^i [(n - 1)!]^i$$

$$(n!)^i = \frac{[(n + 1)!]^i}{(n + 1)^i}$$

$$[(n + 1)!]^i = (n!)^i \cdot (n + 1)^i$$

$$[(kn + 1)!]^i = [k(n!)]^i \cdot (kn + 1)^i$$

Double factorial

If we take only all odd values to some odd integer n, instead of all the integers we obtain the double factorial. For an odd integer $n=2k-1$, with $k \geq 1$:

$$(2k - 1)!! = \frac{(2k)!}{k! 2^k}$$

Note :

$$\Gamma\left(n + \frac{1}{2}\right) = \frac{(2n - 1)!!}{2^n} \sqrt{\pi}$$

If we extend the double factorial to complex numbers:

$$z!! = z(Z-2)\dots 3 = 2^{(z-1)/2} \left(\frac{z}{2}\right) \left(\frac{z-2}{2}\right) \dots \left(\frac{3}{2}\right) = 2^{(z-1)/2} \frac{\Gamma(\frac{z}{2} + 1)}{\Gamma(\frac{1}{2} + 1)}$$

Multifactorial

The k^{th} factorial is defined recursively for non-negative numbers as:

$$n!^{(k)} = \begin{cases} 1 & \text{if } 0 \leq n < k \\ n((n-k)!^{(k)}) & \text{if } n \geq k \end{cases}$$

With this definition: $(kn)!^{(k)} = k^n n!$

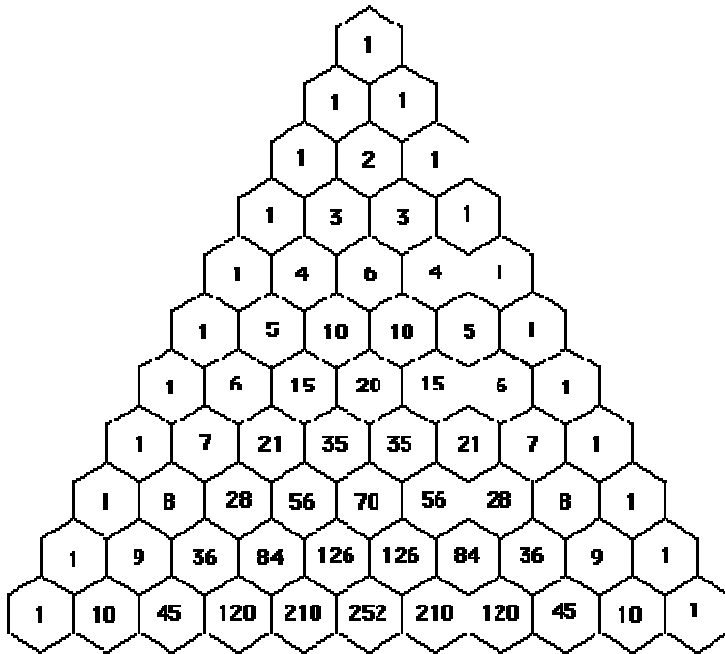
Extended to the complex numbers:

$$z!^{(k)} = z(Z-2)\dots 3 = k^{(z-1)/k} \left(\frac{z}{k}\right) \left(\frac{z-k}{k}\right) \dots \left(\frac{k+1}{k}\right) = k^{(z-1)/k}$$

8. Figurate numbers or polygonal (n-gonal) numbers

Pascal's triangle

Pascal's triangle is a triangular array of the binomial coefficients in a triangle.



The third diagonal (1, 3, 6, 10, 15, ...) has the triangular numbers. The fourth diagonal (1, 4, 10, 20, ...) has the tetrahedral numbers. Horizontal sums are powers of 2. The sum of the numbers in any row is equal to 2 to the n^{th} power or 2^n , when n is the number of the row. For example:

$$\begin{aligned} 2^0 &= 1 \\ 2^1 &= 1+1 = 2 \\ 2^2 &= 1+2+1 = 4 \\ 2^3 &= 1+3+3+1 = 8 \\ 2^4 &= 1+4+6+4+1 = 16 \end{aligned}$$

The numbers in the cells are formed by adding the number of the two above cells: the 2nd row: $0+1=1$; $1+1=2$; $1+0=1$ and the third: $0+1=1$; $1+2=3$; $2+1=3$; $1+0=1$. A number in the triangle can also be found by nCr (n Choose r) where n is the number of the row and r is the element in that row. For example, in row 3, 1 is the 0th element, 3 is element number 1, the next three is the 2nd element, and the last 1 is the 3rd element. The formula for nCr is:

$$nCr = \frac{n!}{r!(n-r)!}$$

In row i and column j : the number is c_{ij} , so that

$$\binom{n}{k} = c_{n-k,k}$$

Example: Row 4, term 2 in Pascal's Triangle is "6" ...

$$\binom{4}{2} = \frac{4!}{2!(4-2)!} = \frac{4!}{2!2!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1 \cdot 2 \cdot 1} = 6$$

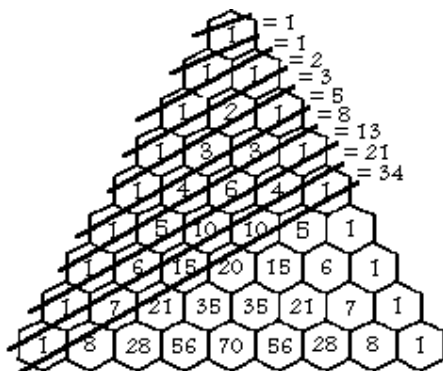
Another property is:

$$c_{ij} = c_{i-1,j} + c_{i,j-1}$$

If a row is made into a single number by using each element as a digit of the number (carrying over when an element itself has more than one digit), the number is equal to 11 to the n^{th} power or 11^n when n is the number of the row the multi-digit number was taken from.

Row #	Formula	=	Multi-Digit number	Actual Row
Row 0	11^0	=	1	1
Row 1	11^1	=	11	1 1
Row 2	11^2	=	121	1 2 1
Row 3	11^3	=	1331	1 3 3 1
Row 4	11^4	=	14641	1 4 6 4 1
Row 5	11^5	=	161051	1 5 10 10 5 1
Row 6	11^6	=	1771561	1 6 15 20 15 6 1
Row 7	11^7	=	19487171	1 7 21 35 35 21 7 1
Row 8	11^8	=	214358881	1 8 28 56 70 56 28 8 1

The sum of the numbers in the consecutive rows shown in the diagram are the first numbers of the Fibonacci Sequence. The Sequence can also be formed in a more direct way, very similar to the method used to form the Triangle, by adding two consecutive numbers in the sequence to produce the next number. The creates the sequence: 1,1,2,3,5,8,13,21,34, 55,89,144,233, etc



Square Numbers are found in the same diagonal as the triangular numbers (1,3,6,10,15,21, 28 etc). A Square Number is the sum of the two numbers in any circled area in the diagram. . The very first square number is 0^2 . The n^{th} square number is equal to the n^{th} triangular number plus the $(n-1)^{\text{th}}$ triangular number. (Any number outside the triangle is 0). The second is 1^2 , the third is 2^2 (4), the fourth is 3^2 (9), and so on.

For any prime numbered row, or row where the first element is a prime number, all the numbers in that row (excluding the 1's) are divisible by the prime. For example, in the seventh row (1 7 21 35 35 21 7 1) 7, 21, and 35 are all divisible by 7. Yet, in a composite numbered row, such as row 6 (1 6 15 20 15 6 1), 15 and 20 are not divisible by 6. In more mathematical terms it can be stated: "if n is a prime number, then all the middle terms (all terms except the two end terms) of the n^{th} row are divisible by n . On the other hand, if n is a composite number, then some terms in the n^{th} row will not be divisible by n .

Euler's $6n+1$ theorem

Euler's $6n+1$ theorem states that every prime of the form $6n+1$, (i.e., 7, 13, 19, 31, 37, 43, 61, 67, ..., which are also the primes of the form $3n+1$; (the series can be written in the form $x^2 + 3y^2$ with x and y positive integers).

theorem

If p be a prime and a be prime to p then $a^{p-1} - 1$ is divisible by p , that is, $a^{p-1} - 1 \equiv 0 \pmod{p}$. A proof of this, first given by Euler, is well known. A more general theorem is that $a^{\phi(n)} - 1 \equiv 0 \pmod{n}$, where a is prime to n and Euler's $\phi(n)$ function is the number of integers less than n and prime to it.

Definition Let $n > 1$. The $\Phi(n)$ integers $1 = a_1 < a_2 < \dots < a_{\Phi(n)} = n-1$ less than n and relatively prime to n are called the *canonical reduced residues* modulo n .

Definition A *reduced residue system* modulo n , $n > 1$ is a set of $\Phi(n)$ incongruent integers modulo n that are relatively prime to n .

Theorem The function Φ is multiplicative.

If p is a prime and m a natural number, the integers $p, 2p, 3p, \dots, p^{m-1}p$ are the only positive integers $\leq p^m$ sharing any prime factors with p^m . Thus $\Phi(p^m) = p^m - p^{m-1}$. Since f is multiplicative, if $n = p_1^{a_1} \dots p_k^{a_k}$ is the factorisation of n into distinct primes, then

$$\Phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \dots (p_k^{a_k} - p_k^{a_k-1})$$

For example, $\Phi(48) = \Phi(24 \cdot 2) = \Phi(24)\Phi(2) = (24-12)(2-1) = 12$, and $\Phi(550) = \Phi(2 \cdot 5^2 \cdot 11) = \Phi(2) \cdot \Phi(5^2) \cdot \Phi(11) = (2-1)(5^2-5)(11-1) = 1 \cdot 20 \cdot 10 = 200$.

Example: Let n be a natural number.

Then $\sum_{k=1}^n \Phi(k)$ Is the number of the fractions $1/n, 2/n, \dots, (n-1)/n, n/n$ that are irreducible.

Theorem

Let n be a positive integer. For each divisor d of n : $\sum_{d|n} \Phi(d) = n$ and also:

$$\Phi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

theorem

An odd prime can be expressed as the difference of two square integers in one and only one way. Fermat's proof is as follows. Let n be the prime, and suppose it equal to $x^2 - y^2$, that is, to $(x + y)(x - y)$. Now, by hypothesis, the only integral factors of n are n and unity, hence $x + y = n$ and $x - y = 1$. Solving these equations we get $x = \frac{1}{2}(n + 1)$ and $y = \frac{1}{2}(n - 1)$.

theorem

If p is a prime number congruent or 1 or 3 modulo 8 then there exist natural numbers x and y satisfying $p = x^2 + 2y^2$. For example:
 $3 = 1^2 + 2 \cdot 1^2$; $11 = 3^2 + 2 \cdot 1^2$; $17 = 3^2 + 2 \cdot 2^2$

theorem

If p is a prime number congruent or 1 modulo 3 then there exist natural numbers x and y satisfying $p = x^2 + 3y^2$. For example:
 $7 = 3^2 + 3 \cdot 1^2$; $13 = 1^2 + 3 \cdot 2^2$; $19 = 4^2 + 3 \cdot 1^2$

theorem

If p is a prime number congruent or 1 or 7 modulo 8 then there exist natural numbers x and y satisfying $p = x^2 - 2y^2$. For example:
 $7 = 3^2 - 2 \cdot 1^2$; $17 = 5^2 - 2 \cdot 2^2$; $23 = 5^2 - 2 \cdot 1^2$

For a prime number congruent or 3 or 5 modulo 8 there do not exist natural numbers x and y satisfying $p = x^2 - 2y^2$

theorem

Let n be a natural number which is not a square of another natural number. Then the equation $x^2 - Ny^2 = 1$ (the so-called Pellé equation) has infinitely many solutions.

Example: equation $x^2 - 2y^2 = 1$ has natural number solutions such as:

$$3^2 - 2 \cdot 2^2 = 1 ; 17^2 - 2 \cdot 12^2 = 1 ; 99^2 - 2 \cdot 70^2 = 1$$

Triangular Numbers.

Triangular numbers are of the form

$$n(n+1)/2 = \frac{1}{2}(n^2 + n)$$

The first few are 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, and 91. All numbers of such a type end in 0, 1, 3, 5, 6, or 8. The rows in a triangle of objects:

```
  o
 o o
 o o o
 o o o o
```

A triangular number be gotten by adding up all the numbers from 1 to a given number

Every perfect number has the form

$$(2^n - 1)2^{n-1}$$

so they are triangular numbers with the base number $(2^n - 1)$

The first few triangular numbers are:

```
*      1 = 1
*
* *    3 = 1 + 2
*
* *
* * *  6 = 1 + 2 + 3
*
* *
* * *
* * * * 10 = 1 + 2 + 3 + 4
```

The x^{th} triangular number is the sum of all the positive integers through x .

We write the first x integers in ascending order in one row, and then in descending order in the next row, and then add the numbers in each column:

```
 1  2  3  ...  x
x  x-1 x-2 ...  1
--- --- ---
x+1 x+1 x+1    x+1
```

Each column adds up to $x+1$. Since there are x of them, if we add these sums Horizontally, they're all equal to $x+1$, we get $x(x+1)$.

To get the sum of the first x positive integers, divide by two:

$$1 + 2 + 3 + \dots + x = x(x+1)/2$$

the formula for triangular numbers.

Square Numbers or Quadrangular numbers

Square numbers are of the form $n \cdot n$ or

$$\frac{1}{2} (2n^2 + 0 \cdot n)$$

The first few are 1, 4, 9, 16, 25, 36, 49, 64, and 81. All numbers of such a type end in 0, 1, 4, 5, 6, or 9.

We can prove easily that there are no square numbers that end in 2 or 8 as follows: these are the digits 2 to an odd power will end in.

To prove that there are none that end in 3 or 7, divide the squares by 5, and look at the remainders. They are

$$0, 1, 4, 4, 1, 0, 1, 4, 4, 1, 0, \dots$$

and they repeat with period 5. A number ending in 2, 3, 7, or 8, when divided by 5, will leave remainder 2 or 3, so can never be a square.

Pentagonal Numbers.

A **pentagonal number** is an integer number, which is found as the number of dots of common pentagons with a common edge e_n (partial) two common sides, and with an increasing number of dots per side. The n th pentagonal number p_n is the number of *distinct* dots in a pattern of dots consisting of the *outlines* of regular pentagons whose sides contain 1 to n dots, overlaid so that they share one vertex. For instance, the third one is formed from outlines comprising 1, 5 and 10 dots, but the 1, and 3 of the 5, coincide with 3 of the 10 – leaving 12 distinct dots, 10 in the form of a pentagon, and 2 inside...

Pentagonal numbers are of the form $n(3n-1)/2$. The first few are 1, 5, 12, 22, 35, 51, 70, and 92. All numbers of such a type end in 0, 1, 2, 5, 6, or 7.

p_n is given by the formula:

$$p_n = \frac{1}{2} (3n^2 - n)$$

for $n \geq 1$. The first few pentagonal numbers are:

1, 5, 12, 22, 35, 51, 70, 92, 117, 145, 176, 210, 247, 287, 330, 376, 425, 477, 532, 590, 651, 715, 782, 852, 925, 1001.

The n th pentagonal number is one third of the $3n-1$ th triangular number. Every pentagonal number is $1/3$ of a triangular

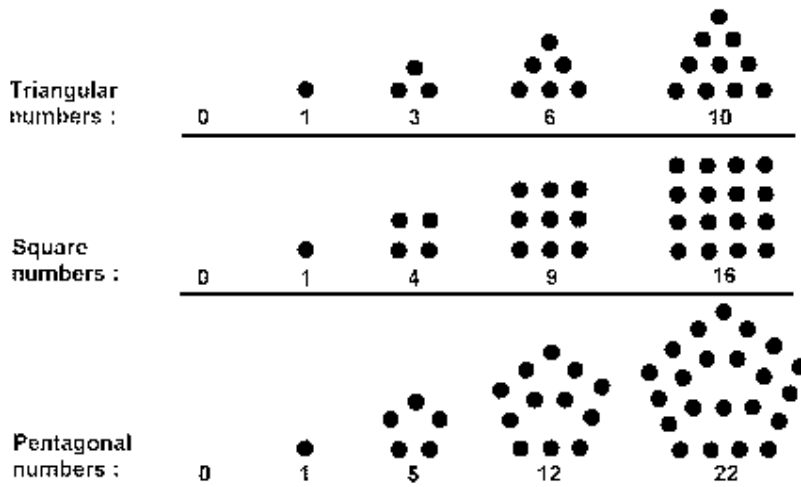
Proof: Triple the n -th pentagonal number,

$$\begin{aligned}
3 \cdot [n \cdot (3n-1)/2] &= (3n) \cdot [(3n)-1]/2 \\
&= (3n-1)(3n)/2 \\
&= (3n-1)(3n-1+1)/2 \\
&= (3n-1)((3n-1)+1)/2 \\
&= \text{the } (3n-1)\text{-th triangular number.}
\end{aligned}$$

One can test whether a positive integer x is a (non-generalized) pentagonal number by computing

$$n = 1/6 \cdot ((24x+1)^{1/2} + 1)$$

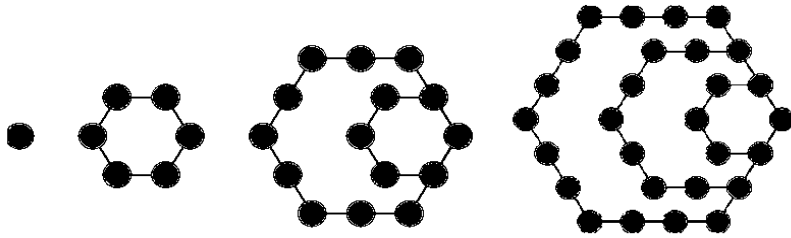
If n is a natural number, then x is the n th pentagonal number. If n is not a natural number, then x is not pentagonal.



Hexagonal numbers

Hexagonal numbers can be, like triangle and square numbers produced in the most obvious way. The n th hexagonal number will be the number of points in a hexagon with n regularly spaced points on a side.

Hexagonal numbers can be gotten by taking a triangular number, multiplying it by 6 and adding 1. The first few are 1, 7, 19, 37, 61 and 91. All numbers of such a type end in 1, 7, or 9.



For instance, the third one is formed from outlines comprising 1, 5 and 10 dots, but the 1, and 3 of the 5, coincide with 3 of the 10 – leaving 12 distinct dots, 10 in the form of a pentagon, and 2 inside.

The n -th hexagonal number is given by the formula

$$\frac{1}{2} \cdot (4n^2 - 2n) = n \cdot (2n - 1) = \frac{1}{2} [2n \cdot (2n - 1)]$$

The first few hexagonal numbers are:

1, 6, 15, 28, 45, 66, 91, 120, 153, 190, 231, 276, 325, 378, 435, 496, 561, 630, 703, 780, 861, 946.

Every hexagonal number is a triangular number, but only every *other* triangular number (the 1st, 3rd, 5th, 7th, etc.) is a hexagonal number. Like a triangular number, the digital root in base 10 of a hexagonal number can only be 1, 3, 6, or 9. The root pattern, repeating every nine terms, is "1 6 6 1 0 3 1 3 0".

Taking differences between the hex numbers we get:

x: 1----7----19----37----61----

d₁: ---6---12---18----24---

d₂: -----6----6-----6.....

Since the second difference d_2 is constant, the r^{th} term will be quadratic form: $ar^2 + br + c$, where a , b and c satisfy:

$$a + b + c = 1$$

$$4a + 2b + c = 7$$

$$9a + 3b + c = 19$$

Which gives $a=3$, $b=-3$ and $c=1$, hence the r^{th} term is: $3r^2 - 3r + 1$,

Using standard sums we find the sum of the first hexagonal numbers:

$$\sum_{r=1}^n (3r^2 - 3r + 1) = 3 \sum r^2 - 3 \sum r + \sum 1 = 3 \left[\frac{n}{6} (n+1) (2n+1) \right] - 3 \left[\frac{n}{2} (n+1) \right] + n =$$

$$= \frac{n}{2} (n+1) (2n+1) - \frac{3n}{2} (n+1) + n = n^3$$

Heptagonal number

A **heptagonal number** is a figurate number that represents a heptagon. The n -th heptagonal number is given by the formula

$$\frac{1}{2} (5n^2 - 3n)$$

The first few heptagonal numbers are:

1, 7, 18, 34, 55, 81, 112, 148, 189, 235, 286, 342, 403, 469, 540, 616, 697, 783, 874, 970, 1071, 1177, 1288, 1404, 1525, 1651, 1782, 1918, 2059, 2205, 2356, 2512, 2673, 2839, 3010, 3186, 3367, 3553, 3744, 3940, 4141, 4347, 4558, 4774, 4995, 5221, 5452, 5688

A **generalized heptagonal number** is obtained by the formula

$$T_n + T_{\lfloor n/2 \rfloor}$$

where T_n is the n th triangular number. The first few generalized heptagonal numbers are:

1, 4, 7, 13, 18, 27, 34, 46, 55, 70, 81, 99, 112

Every other generalized heptagonal number is a regular heptagonal number.

An **octagonal number** is a figurate number that represents an octagon. The octagonal number for n is given by the formula $3n^2 - 2n$, with $n > 0$. The first few octagonal numbers are:

1, 8, 21, 40, 65, 96, 133, 176, 225, 280, 341, 408, 481, 560, 645, 736, 833, 936

Octagonal numbers can be formed by placing triangular numbers on the four sides of a square. The n th octagonal number is

$$n^2 + 4 \sum_{k=1}^{n-1} k = 3n^2 - 2n = \frac{1}{2} (6n^2 - 4n)$$

which simplifies to the formulas given above.

The octagonal number for n can also be calculated by adding the square of n to twice the

$(n - 1)$ th pronic number, or, to put it algebraically, $O_n = 3n^2 - 2n$.

Octagonal numbers consistently alternate parity.

A **nonagonal number** or **enneagonal number** is a polygonal number that represents a nonagon. The nonagonal number for n is given by the formula:

$$\frac{1}{2} (7n^2 - 5n)$$

The first few nonagonal numbers are:

1, 9, 24, 46, 75, 111, 154, 204, 261, 325, 396, 474, 559, 651, 750, 856, 969, 1089, 1216, 1350, 1491, 1639, 1794, 1956, 2125, 2301, 2484, 2674, 2871, 3075, 3286, 3504, 3729, 3961, 4200, 4446, 4699, 4959, 5226, 5500, 5781, 6069, 6364, 6666, 6975, 7291, 7614, 7944, 8281, 8625, 8976, 9334, 9699.

The parity of nonagonal numbers follows the pattern odd-odd-even-even.

Letting $N(n)$ give the n th nonagonal number and $T(n)$ the n^{th} triangular number,

$$7N(n) + 3 = T(7n - 3).$$

A **decagonal number** is a figurate number that represents a decagon. The decagonal number for n is given by the formula

$$4n^2 - 3n = \frac{1}{2}(8n^2 - 6n)$$

with $n > 0$. The first few decagonal numbers are

1, 10, 27, 52, 85, 126, 175, 232, 297, 370, 451, 540, 637, 742, 855, 976, 1105, 1242, 1387, 1540, 1701, 1870, 2047, 2232, 2425, 2626, 2835, 3052, 3277, 3510, 3751, 4000, 4257, 4522, 4795, 5076, 5365, 5662, 5967, 6280, 6601, 6930, 7267, 7612, 7965, 8326

The decagonal number for n can also be calculated by adding the square of n to thrice the $(n - 1)$ th pronic number, or to put it algebraically, $D_n = n^2 + 3(n^2 - n)$.

Decagonal numbers consistently alternate parity.

Theorem

If $n \geq 3$, then any natural number can be expressed as the sum of less than or equal to n nonagonal numbers

Theorem

A triangular number different from 1 is not a cubic number

This follows from $\frac{1}{2} y(y+1) = x^3$

Theorem

From $y^2+2=x^3$:

The only case where a square number added to 2 becomes a cubic number is $5^2+2=3^3$.

Theorem

From $y^2+4=x^3$:

The only cases where a square number added to 4 become cubic number are $2^2+4=2^3$ and $11^2+4=5^3$.

Theorem

Given a triangle whose sides have rational lengths, there exist infinitely many triangles with rational sides that have the same area as the given triangle.

Example: triangles 3,4,5 and $7/10, 120/7, 1201/70$ have the same length 6.

Theorem

The area of a right triangle whose sides are integers is not a square.

This means that a rational triangle cannot be a rational square. In symbols, there do not exist integers x, y, z with

$x^2 + y^2 = z^2$ such that $xy/2$ is a square. From this it is easy to deduce the $n = 4$ case of Fermat's theorem.

Theorem

The area of a right triangle whose sides are integers is not twice a square.

Fermat's $4k+1$ Theorem or Fermat's two-square theorem

If a prime p is of the form $4k+1$ then it can be written as: a^2+b^2 or a prime number p can be represented in an essentially unique manner (up to the order of addends) in the form a^2+b^2 for integer a and b iff $p \equiv 1 \pmod{4}$ or $p=2$ (which is a degenerate case with $a=b=1$).

The first few primes p which are 1 or $2 \pmod{4}$ are 2, 5, 13, 17, 29, 37, 41, 53, 61, ... (with the only prime congruent to $2 \pmod{4}$ being 2). The numbers (a,b) such that a^2+b^2 equal these primes are (1, 1), (1, 2), (2, 3), (1, 4), (2, 5), (1, 6),

Genus Theorem

The Diophantine equation

$$a^2+b^2 = p$$

can be solved for p being a prime iff $p \equiv 1 \pmod{4}$ or $p=2$. The representation is unique except for changes of sign or rearrangements of a and b .

$$\text{Let } Q(a,b) = a^2 + b^2$$

then all relatively prime solutions (a,b) to the problem of representing $Q(a,b) = m$ for m any integer are achieved by means of successive applications of the genus theorem and composition theorem.

Theorem

If a prime is of the form $4k+3$ then it can not be written as: $a^2 + b^2$.

Proof: Every square is of the form $4k$ or $4k+1$. Hence the sum of two squares can only be of the form $4k$ or $4k+1$ or $4k+2$

theorem

A positive integer n can only be written as $x^2 + y^2$ if and only if

$$n = 2^a \cdot p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_r^{b_r} \cdot q_1^{2c_1} \cdot q_2^{2c_2} \cdot \dots \cdot q_r^{2c_r}$$

where p 's are primes of the form $4k+1$ and q 's are primes of the form $4k+3$

theorem

If a number does not have the form $4^k(8m+7)$ it can be expressed as a sum of three squares: $a^2 + b^2 + c^2$.

theorem

when the number has the form $8k+3$ it can be expressed as a sum of three squares, but subtracting a square we cannot obtain a number of the form $4k+1$.

9. more on polynomial numbers

Examples

Examples

$$2^2+2^2=2^3$$

$$3^2+3^2+3^2=3^3$$

$$3^2+19^2+31^2=11^3$$

$$3^2+691^2+2293^2=179^3$$

$$3^2+5869^2+54959^2=1451^3$$

$$3^2+24967^2+60169^2=3^2+28163^2+58741^2=1619^3$$

$$3^2+13127^2+121229^2=2459^3$$

$A^2+B^2+C^2 = D^2$, where D must be 3 modulo 8. If p is prime then $p=2$, $p=3$, or $p^2 = 1 \pmod{6}$. If $A^2 = 1 \pmod{6}$ then $A^2+B^2+C^2 = 3 \pmod{6}$, which doesn't work since the cube of a prime > 3 is $= 1$ or $= 5 \pmod{6}$. If $A=2$, $2^2+ B^2+C^2$, $B>A$ is ruled out with a parity argument. $A=B=2$ is ruled out since $2^2+2^2+2^2 = 3 \pmod{6}$. Therefore A must be 3.

$$4^2+4^2+4^2+4^2=4^3$$

$$4^2+6^2+5^2+0^2=5^3$$

Etc.

$2^1+1^1=3$		$2^2+1^2=5$	
	$d_1 = 1$		$d_1 = 3$
$2^1+2^1=4$		$2^2+2^2=8$	
	$d_2 = 1$		$d_2 = 5=d_1+2$
$2^1+3^1=5$		$2^2+3^2=13$	
	$d_3 = 1$		$d_3 = 7= d_2+2$
		$2^2+4^2=20$	

etc

$2^3+1^3=9$		$3^3+1^3=28$	
	$d_1 = 7$		$d_1 = 7$
$2^3+2^3=16$		$3^3+2^3=35$	
	$d_2 = 19$		$d_2 = 19$
$2^3+3^3=35$		$3^3+3^3=54$	
	$d_3 = 37$		$d_3 = 37$
$2^3+4^3=72$		$3^3+4^3=91$	
	$d_4 = 61$		$d_4 = 61$
$2^3+5^3=133$		$3^3+5^3=152$	

etc

$4^4+1^4=257$		$4^5+1^5=1025$	
	$d_1=15$		$d_1=31$
$4^4+2^4=272$		$4^5+2^5=1056$	
	$d_2=65$		$d_2=211$
$4^4+3^4=337$		$4^5+3^5=1267$	
	$d_3=175$		$d_3=781$
$4^4+4^4=512$		$4^5+4^5=2048$	
	$d_3=369$		$d_4=2101$
$4^4+5^4=881$		$4^5+5^5=4149$	

The differences are the so-called nexus numbers and are the same-value-powers of consecutive numbers.

Nexus numbers

A nexus number is a figurate number built up of the nexus of cells less than n steps away from a given cell. The n th d -dimensional nexus number is given by

$$N_d(n) = \sum_{k=0}^n \binom{d+1}{k} n^k$$

$$= (n+1)^{d+1} - n^{d+1},$$

where $\binom{n}{k}$ is a binomial coefficient. The symbolic representations and sequences for first few k -dimensional nexus numbers are given in the table below.

d	$N_d(n)$	name	$N_d(0), N_d(1), N_d(2), \dots$
0	1	unit	1, 1, 1, 1, 1, 1, 1, 1, 1, 1, ...
1	$2n+1$	odd number	1, 3, 5, 7, 9, 11, 13, 15, 17, 19, ...
2	$3n^2+3n+1$	hex number	1, 7, 19, 37, 61, 91, 127, 169, 217, ...
3	$4n^3+6n^2+4n+1$	rhombic dodecahedral number	1, 15, 65, 175, 369, 671, 1105, 1695, 2465, ...
4	$5n^4+10n^3+10n^2+5n+1$	nexus number	1, 31, 211, 781, 2101, 4651, 9031, 15961, ...

Exercise and examples

$2^3+2^3=16=4^2-0^2$		$3^3+2^3=35=6^2-1^2$
	$d_1=6^2-1^2-4^2+0^2$	
$2^3+3^3=35=6^2-1^2$		$3^3+3^3=54=9^2-6^2$
	$d_2=9^2-3^2-6^2+1^2$	
$2^3+4^3=72=9^2-3^2$		$3^3+4^3=91=10^2-3^2$

	$d_3 = 13^2 - 6^2 - 9^2 + 3^2$	$3^3 + 5^3 = 152 = x$
$2^3 + 5^3 = 133 = 13^2 - 6^2$		
	$d_4 = 18^2 - 10^2 - 13^2 + 6^2$	
$2^3 + 6^3 = 224 = 18^2 - 10^2$		
	$d_4 = 24^2 - 15^2 - 18^2 + 10^2$	
$2^3 + 7^3 = 351 = 24^2 - 15^2$		

The difference $d_i = \sum_{j=1}^4 a_i = 1$

If in $a^n + b^n$ both a and b are (positive) odd or even then the result is even and sometimes it sometimes can be written as $c^n - d^n$, with c and d integers)

It becomes harder to find subtractives of variables for additive variables of powers greater than 4.

$4^3 + 2^3 = 72 = 9^2 - 3^2$		$5^3 + 2^3 = 133 = 13^2 - 6^2$
	$d_1 = 10^2 - 3^2 - 9^2 + 3^2$	
$4^3 + 3^3 = 91 = 10^2 - 3^2$ (or $6^3 - 5^3$)		$5^3 + 3^3 = 152 = x$ also $21^2 - 17^2$
	$d_2 = 12^2 - 4^2 - 10^2 + 3^2$	
$4^3 + 4^3 = 128 = 12^2 - 4^2$		$5^3 + 4^3 = 189 = 15^2 - 6^2$ also $17^2 - 10^2$
	$d_3 = 15^2 - 6^2 - 12^2 + 4^2$	
$4^3 + 5^3 = 189 = 15^2 - 6^2$		$5^3 + 5^3 = 250 =$ $17^2 - 7^2$
	$d_4 = 19^2 - 9^2 - 15^2 + 6^2$	
$4^3 + 6^3 = 280 = 19^2 - 9^2$		$5^3 + 6^3 = 341 = 21^2 - 10^2$
	$d_5 = 24^2 - 13^2 - 19^2 + 9^2$	
$4^3 + 7^3 = 407 = 24^2 - 13^2$		$5^3 + 7^3 = 468 =$ $22^2 - 4^2$

The Sum/Difference of Two Cubes method is used on cubic polynomials of the form:

$$a^3 \pm b^3$$

By factoring a - b out of the expression we get:

$$a^3 \pm b^3 = (a \pm b)(a^2 \mp ab + b^2)$$

If a and b are integers, since $a^3 + b^3$ can be always factored into $(a+b).(a^2 - b^2)$, the result will never be a prime number and we cannot extend Fermat's Theorem for two squares to a theorem for two cubes. (Theorem of Schreuder, named after Carla Else Schreuder who brought this to my attention)

As a consequence of Fermat's theorem we can make the following conclusion:

A prime number of the form a^4+b^4 where n is a multiple of 2 can be written in the form

16. $k+1$

Examples: $17=2^4 \times 1 + 1 = 2^4 + 1^4$; $97 = 2^4 \times 6 + 1 = 4^4 + 3^4$;

$2^4+1^4=17$
$2^4+2^4=32 = 2.(2^3+2^3)+ 0 \times 8$
$2^4+3^4=97 = 3.(2^3+3^3)+ 1 \times 8$
$2^4+4^4=272 = 4.(2^3+3^3)+ 2 \times 8$
$2^4+5^4=641 = 5.(2^3+3^3)+ (5-2) \times 8$
$2^4+6^4=1312 = 6.(2^3+3^3)+ (6-2) \times 8$
$2^4+7^4=2417 = 7.(2^3+3^3)+ (7-2) \times 8$ etc

For further examples on polynomial additions see the section on Beal conjecture

Hardy–Ramanujan-de Bessy numbers

Hardy–Ramanujan numbers or taxicab number is the smallest number that can be expressed as a sum of two positive cubes in n (two or more) distinct ways, up to order of summands. G. H. Hardy and E. M. Wright proved in 1954 that such numbers exist for all positive integers n , the first few of which are 1, 1729, 4104, 13832, 20683, 32832, 39312, 40033, 46683, 64232, ...

$$T_1=2=1^3+1^3$$

$$T_2=1729 = 1^3 + 12^3$$

$$= 9^3 + 10^3$$

, the factors of 1729 are 7, 13 and 19 so allowing negative cubes gives $91=(7 \times 13) = 6^3 + (-5)^3 = 4^3 + 3^3$

$$T = 4104 = 2^3 + 16^3 = 9^3 + 15^3$$

The list becomes:

$$T = 13832$$

$$T = 20683$$

$$T = 32832$$

$$T = 39312$$

$$T = 40033$$

$$T = 46683$$

$$T = 64232$$

$$T = 65728$$

$$T = 110656$$

$$T = 110808$$

T=134379
T=149389
T=165464
T=171288
T=195841
T=216027
T=216125
T=262656
T=314496
T=320264
T=327763
T=373464
T=402597
T=439101
T=443889
T=513000
T=513856

More examples (not sequential):

$$\begin{aligned} T=87539319 &= 167^3+436^3 \\ &= 228^3+423^3 \\ &= 255^3+414^3 \end{aligned}$$

$$\begin{aligned} T = 15170835645 &= \\ &= 517^3 + 2468^3 \\ &= 709^3 + 2456^3 \\ &= 1733^3 + 2152^3. \end{aligned}$$

$$\begin{aligned} T= 6963472309248 &=2421^3+ 19083^3 \\ &= 5436^3+ 18948^3 \\ &= 10200^3+ 18072^3 \\ &=13322^3 + 16630^3 \end{aligned}$$

$$\begin{aligned} T=48988659276962496 &= 38787^3+365757^3 \\ &= 107839^3+ 362753^3 \\ &= 205292^3+ 342952^3 \\ &= 221424^3+ 336588^3 \\ &= 231518^3+ 331954^3 \end{aligned}$$

$$\begin{aligned} T = 1801049058342701083 & \\ &= 92227^3 + 1216500^3 \\ &= 136635^3 + 1216102^3 \\ &= 341995^3 + 1207602^3 \\ &= 600259^3 + 1165884^3 \end{aligned}$$

$$\begin{aligned} T=24153319581254312065344 &= 582162^3+ 28906206^3 \\ &= 3064173^3 + 28894803^3 \\ &= 8519281^3+ 28657487^3 \\ &= 16218068^3+ 27093208^3 \\ &= 17492496^3+ 26590452^3 \end{aligned}$$

$$= 18289922^3 + 26224366^3$$

A more restrictive taxicab problem requires that the taxicab number be cubefree, which means that it is not divisible by any cube other than 1^3 . When a cubefree taxicab number T is written as $T = x^3 + y^3$, the numbers x and y must be relatively prime for all pairs (x, y) . Among the taxicab numbers T listed above, $T = 1$, $T = 1729$, $T = 15170835645$ and $T = 1801049058342701083$ are cubefree taxicab numbers.

Theorem

Let n be a natural number, then there exist integers, x, y, z such that $n = x^2 + y^2 + z^2 + u^2$
 Examples: $5 = 2^2 + 1^2 + 0^2 + 0^2$; $7 = 2^2 + 1^2 + 1^2 + 1^2$; $15 = 3^2 + 2^2 + 1^2 + 1^2$

Lagrange theorem

Every integer can be written as the sum of at most 4 squares. e.g.

$$89 = 9^2 + 2^2 + 2^2$$

$$103 = 10^2 + 1^2 + 1^2 + 1^2$$

Theorem

$$1^2 + 2^2 + 3^2 + 4^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof by induction:

Check $Q(1)$: $1 = 1 \times 2 \times 3 / 6 = 1$ which is true.

We now assume $Q(n) = \frac{n(n+1)(2n+1)}{6}$ is true, so we are going to prove $Q(n+1)$:

$$\begin{aligned}
 1 + 2^2 + 3^2 + \dots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \\
 &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} = \frac{(n+1)(n(2n+1) + 6(n+1))}{6} = \\
 &= \frac{(n+1)(2n^2 + n + 6n + 6)}{6} = \frac{(n+1)(2n^2 + 7n + 6)}{6} = \\
 &= \frac{(n+1)(n+2)(2n+3)}{6} = \frac{(n+1)(n+2)(2(n+1)+1)}{6}
 \end{aligned}$$

which is exactly property $Q(n+1)$.

Theorem for the k^{th} -Sum of squares

Define $S_k(n)$ to be the k^{th} sum of the squares up till n , so $S_k(n)$ is the sum of all $S_{k-1}(r)$ for $1 \leq r \leq n$. Then

$$S_k(n) = \frac{2n+k}{k+2} \binom{n+k}{k+1}$$

K=1

$$1^2=1=1*1$$

$$1^2+2^2=5=2*2.5$$

$$1^2+2^2+3^2=14=3*(4+2/3)$$

$$1^2+2^2+3^2+4^2=30=4*7.5$$

$$1^2+2^2+3^2+4^2+5^2=55=5*11$$

We see that the $S_1(n)$ is given by $n*$ (a number with a fraction that has either 3 or 2 in the denominator), so we multiply all the results by $6(=2*3)$:

$$1*6=1*6=1*2*3$$

$$5*6=2*15=2*3*5$$

$$14*6=3*28=3*4*7$$

$$30*6=4*45=4*5*9$$

We see that $6*S_1(n)=n(n+1)(2n+1)$, or : $S_1(n)=n(n+1)(2n+1)/6 = \frac{2n+1}{3} \binom{n+1}{2}$.

K=2

We sum the values of S_1 :

$$1=1=1*1$$

$$1+5=6=2*3$$

$$1+5+14=20=3*(6+2/3)$$

$$1+5+14+30=50=4*(12+1/2)$$

$$1+5+14+30+55=105=5*21$$

and again multiply them all by 6.

$$1*6=1*6=1*2*3$$

$$6*6=2*18=2*3*6$$

$$20*6=3*40=3*4*10$$

$$50*6=4*75=4*5*15$$

$$105*6=5*126=5*6*21$$

3,6,10,15,21 are all triangular numbers, and so we can find them by the formula: $(n+1)(n+2)/2$ (since we need the triangular numbers to start from 3 and not 1).

$$6*S_2(n)=n(n+1)(n+1)(n+2)/2 \quad \text{or} \quad S_2(n)=n(n+1)^2(n+2)/12 = \frac{n+1}{2} \binom{n+2}{3}$$

In general

$$S_k(n) = \frac{2n+k}{k+2} \binom{n+k}{k+1}$$

Proof by induction:

$$S_{k-1}(1) + S_{k-1}(2) + \dots + S_{k-1}(n) = S_k(n)$$

$$\frac{2+k-1}{k+1} \binom{1+k-1}{k} + \frac{4+k-1}{k+1} \binom{2+k-1}{k} + \dots + \frac{2n+(k-1)}{k+1} \binom{n+k-1}{k} = \frac{2n+k}{k+2} \binom{n+k}{k+1}$$

$$\frac{k+1}{k+1} \binom{k}{k} + \frac{k+3}{k+1} \binom{k+1}{k} + \dots + \frac{2n+(k-1)}{k+1} \binom{n+k-1}{k} = \frac{2n+k}{k+2} \binom{n+k}{k+1}$$

Checking for n=1:

$$\frac{k+1}{k+1} \binom{k}{k} = \frac{2*1+k}{k+2} \binom{1+k}{k+1}$$

Lets assume that it is true for n=m, a certain positive integer:

$$\frac{k+1}{k+1} \binom{k}{k} + \frac{k+3}{k+1} \binom{k+1}{k} + \dots + \frac{2m+(k-1)}{k+1} \binom{m+k-1}{k} = \frac{2m+k}{k+2} \binom{m+k}{k+1}$$

Now lets prove it for n=m+1, the consecutive integer, by adding the next term of the series to both sides:

$$\begin{aligned} & \frac{k+1}{k+1} \binom{k}{k} + \frac{k+3}{k+1} \binom{k+1}{k} + \dots + \frac{2m+(k-1)}{k+1} \binom{m+k-1}{k} + \frac{2(m+1)+(k-1)}{k+1} \binom{(m+1)+k-1}{k} \\ &= \frac{2m+k}{k+2} \binom{m+k}{k+1} + \frac{2(m+1)+(k-1)}{k+1} \binom{(m+1)+k-1}{k} \\ &= \frac{2m+k}{k+2} \binom{m+k}{k+1} + \frac{2m+k+1}{k+1} \binom{m+k}{k} = \frac{(2m+k)(m+k)!}{(k+2)(k+1)!(m-1)!} + \frac{(2m+k+1)(m+k)!}{(k+1)k!m!} \\ &= (m+k)! \left[\frac{(2m+k)}{(k+2)!(m-1)!} + \frac{(2m+k+1)}{(k+1)!m!} \right] = (m+k)! \left[\frac{m(2m+k) + (2m+k+1)(k+2)}{(k+2)!m!} \right] \\ &= (m+k)! \left[\frac{m(2m+k) + (2m+k)(k+2) + (k+2)}{(k+2)!m!} \right] = (m+k)! \left[\frac{(2m+k)(m+k+2) + (k+2)}{(k+2)!m!} \right] \\ &= (m+k)! \left[\frac{(2m+k)(m+k+1) + (k+2) + (2m+k)}{(k+2)!m!} \right] = (m+k)! \left[\frac{(2m+k)(m+k+1) + 2(m+k+1)}{(k+2)!m!} \right] \\ &= (m+k)! \left[\frac{(m+k+1)(2m+k+2)}{(k+2)!m!} \right] = \frac{(m+k+1)!(2m+k+2)}{(k+2)(k+1)!m!} = \frac{2m+k+2}{k+2} \binom{m+k+1}{k+1} \\ &= \frac{2(m+1)+k}{k+2} \binom{(m+1)+k}{k+1} \end{aligned}$$

Theorem

$$1^3 + 2^3 + 3^3 + 4^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2 \quad \text{also : } \mathbf{1^3 + 2^3 + \dots + n^3 = (1 + 2 + \dots + n)^2.}$$

Proof:

We want to prove:

$$S_n = \sum_{k=1}^n k^3 = \left(\sum_{k=1}^n k \right)^2$$

We evaluating the sum of the first n integers. We assert that

$$T_n = \sum_{k=1}^n k = \frac{n(n+1)}{2}$$

This eq. holds for $n=1$: $1=1$ and we assume that the statement above is true for the case n . We consider the case with $n+1$:

$$T_{n+1} = \sum_{k=1}^{n+1} k = \frac{n(n+1)}{2} + (n+1)$$

The last term on the right-hand side of this expression is simply the extra term that needs to be added to the sum of the first n integers and

$$\frac{n(n+1)}{2} + (n+1) = \frac{(n^2 + 3n + 2)}{2} = \frac{(n+1)(n+2)}{2}$$

$$\frac{n(n+1)}{2}$$

This is of the form $\frac{n(n+1)}{2}$ with $n+1$ instead of n or If our proposed result holds for the case n , then it also holds for the case $n+1$ and hence we have proved that

$$T_n = \sum_{k=1}^n k = \frac{n(n+1)}{2}$$

Therefore, proving our original statement requires us to prove that

$$S_n = \sum_{k=1}^n k^3 = \left(\sum_{k=1}^n k \right)^2 = \frac{n^2(n+1)^2}{4}$$

For the case $n=1$, the statement holds since the sum of cubes and the expression on the right-hand side is unity. We consider the statement with the case $n+1$:

$$S_{n+1} = \sum_{k=1}^{n+1} k^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3$$

where the last term on the right-hand side of this expression is just the extra term that needs to be added to the sum of the cubes of the first n integers. Manipulation shows that

$$\frac{n^2(n+1)^2}{4} + (n+1)^3 = \frac{(n+1)^2(n+2)^2}{4}$$

The right-hand side of the above expression is of the form

$$\frac{n^2(n+1)^2}{4}$$

with $n+1$ instead of n .

Theorem for the k^{th} -Sum of cubes

Lets $S_k(n)$ be the k^{th} -Sum of the cubes up till n . Then

$$S_k(n) = \frac{6n^2 + 6kn + k(k-1)}{(k+2)(k+3)} \binom{n+k}{k+1}$$

K=1

$$1^3=1$$

$$1^3+2^3=9$$

$$1^3+2^3+3^3=36$$

$$1^3+2^3+3^3+4^3=100$$

$$1^3+2^3+3^3+4^3+5^3=225$$

they are all square numbers and they are exactly the squares of the triangular numbers ($1^2, 3^2, 6^2, 10^2, 15^2 \dots$).

$$S_1(n) = \binom{n+1}{2}^2 = \frac{n^2+n}{2} \binom{n+1}{2}$$

K=2

$$1=1$$

$$1+9=10$$

$$1+9+36=46$$

$$1+9+36+100=146$$

$$1+9+36+100+225=371$$

by induction:

$$S_2(n) = \frac{3n^2 + 6k + 1}{10} \binom{n+2}{3}$$

etc. In general it can again be proven by induction that : $S_k(n) = \frac{6n^2 + 6kn + k(k-1)}{(k+2)(k+3)} \binom{n+k}{k+1}$

Sum of squares and cubes

Theorems

$$1+2^0+3^0+ \dots n^0 = 1+1+1+\dots 1 = n$$

$$1+2+3+4+\dots n = \frac{n(n+1)}{2}$$

$$1^2 + 2^2 + 3^2 + 4^2 + \dots n^2 = \frac{n(n+1)(2n+1)}{6}$$

$$1^3 + 2^3 + 3^3 + 4^3 + \dots n^3 = \left[\frac{n(n+1)}{2} \right]^2 \quad \text{also : } \mathbf{1^3 + 2^3 + \dots + n^3 = (1 + 2 + \dots + n)^2}.$$

By extrapolation:

$$1^4 + 2^4 + 3^4 + 4^4 + \dots n^4 = \frac{n(n+1)(2n+1)(3n^2 + 3n - 1)}{30}$$

$$1^5 + 2^5 + 3^5 + 4^5 + \dots n^5 = \frac{n^2(n+1)^2(2n^2 + 2n - 1)}{12}$$

$$1^6 + 2^6 + 3^6 + 4^6 + \dots n^6 = \frac{n.(n+1).(2n+1).(3n^4 + 6n^3 - 3n + 1)}{42}$$

Etc

Let n be a positive integer and let the kth power sum up to n-1 be

$$S_k(n) = \sum_{m=0}^{n-1} m^k, \quad k \in \mathbb{N}$$

Thus $S_0(n) = n$ while for $k > 0$ the term $0^k = 0$. The generating function for the power series having these sum as its coefficients is :

$$S(n, t) = \sum_{k=0}^{\infty} S_k(n) \frac{t^k}{k!}$$

Rearranging the double term gives :

$$S(n, t) = \frac{e^{nt} - 1}{t} \cdot \frac{t}{e^t - 1}$$

The second term is independent of n, its coefficients being the Bernoulli numbers:

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$$

The generating function can be written as:

$$S(n, t) = \sum_{\ell=1}^{\infty} n^{\ell} \cdot \frac{t^{\ell-1}}{\ell!} \sum_{j=0}^{\infty} B_j \frac{t^j}{j!} = \sum_{k=0}^{\infty} \left(\frac{1}{k+1} \sum_{j=0}^k \binom{k+1}{j} B_j n^{k+1-j} \right) \frac{t^k}{k!}$$

If we define the k^{th} Bernoulli polynomial as

$$B_k(x) = \sum_{j=0}^k \binom{k}{j} B_j X^{k-j}$$

,then comparing the first and last expressions for $S(n,t)$ shows that the k^{th} power sum is

$$S_k(n) = \frac{1}{k+1} (B_{k+1}(n) - B_{k+1})$$

The first Bernoulli numbers are $B_0=1$, $B_1= -\frac{1}{2}$, $B_2 = 1/6$, and $B_3=0$, etc and so the first Bernoulli polynomials are:

$$B_0(X)=1$$

$$B_1(X)=X - \frac{1}{2}$$

$$B_2(X) = X^2 - X + 1/6$$

$$B_3(X)=X^3 - 3/2X^2 + \frac{1}{2} X$$

The example $1^2+2^2+\dots+n^2=S_2(n+1)= 1/3.(B_3(n+1)-B_3)$ becomes: $(2n^3+3n^2+n)/6$.

The fully expanded polynomials are:

$$\begin{aligned} \sum_{m=1}^n m^0 &= n, \\ \sum_{m=1}^n m^1 &= \frac{1}{2}n^2 + \frac{1}{2}n, \\ \sum_{m=1}^n m^2 &= \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n, \\ \sum_{m=1}^n m^3 &= \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2, \\ \sum_{m=1}^n m^4 &= \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n, \\ \sum_{m=1}^n m^5 &= \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 - \frac{1}{12}n^2, \\ \sum_{m=1}^n m^6 &= \frac{1}{7}n^7 + \frac{1}{2}n^6 + \frac{1}{2}n^5 - \frac{1}{6}n^3 + \frac{1}{42}n. \end{aligned}$$

Proof:

We notice some patterns: The leading coefficient appears to be $1 / (p + 1)$, and the coefficient of n^p seems to always be $1 / 2$. Let B_k be the (signed) constant appearing in the expression for the coefficient of n^{p+1-k} . Note that the zero columns in the table of coefficients imply that for odd $k > 1$, $B_k = 0$. With the exception of understanding B_k , we have arrived at the following conjectural formula for $f_p(n)$:

$$\sum_{m=1}^n m^p = \frac{1}{p+1} n^{p+1} + \frac{1}{2} n^p + \frac{1}{p+1} \sum_{k=2}^p \binom{p+1}{k} B_k n^{p+1-k}.$$

It turns out that the coefficients B_k are simply the Bernoulli numbers:

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0, B_6 = \frac{1}{42},$$

$$B_7 = 0, B_8 = -\frac{1}{30}, B_9 = 0, B_{10} = \frac{5}{66}, B_{11} = 0, B_{12} = -\frac{691}{2730}, \dots$$

Furthermore, we can even bring the first two terms into the sum if we include a factor of $(-1)^k$ to take care of the fact that $B_1 = -1/2$ while the coefficient of n^p is $1/2$:

$$\sum_{m=1}^n m^p = \frac{1}{p+1} \sum_{k=0}^p \binom{p+1}{k} (-1)^k B_k n^{p+1-k}.$$

For $p \geq 1$, let $B_p(n)$ be a Bernoulli polynomial in n of degree p satisfying

$$B_p(n+1) - B_p(n) = p n^{p-1}.$$

This defines $B_p(n)$ up to its constant term; we define its constant term $B_p(0)$ to be the Bernoulli number B_p . The first few Bernoulli polynomials are

$$B_1(n) = n - \frac{1}{2},$$

$$B_2(n) = n^2 - n + \frac{1}{6},$$

$$B_3(n) = n^3 - \frac{3}{2}n^2 + \frac{1}{2}n,$$

$$B_4(n) = n^4 - 2n^3 + n^2 - \frac{1}{30},$$

$$B_5(n) = n^5 - \frac{5}{2}n^4 + \frac{5}{3}n^3 - \frac{1}{6}n,$$

$$B_6(n) = n^6 - 3n^5 + \frac{5}{2}n^4 - \frac{1}{2}n^2 + \frac{1}{42}.$$

An important property of the Bernoulli polynomials is that

$$B_p(n) = (B + n)^p = \sum_{k=0}^p \binom{p}{k} B_k n^{p-k},$$

where " B^k " is to be interpreted as B_k . Then considering $f_p(n-1)$ rather than $f_p(n)$ puts (2) in this form:

$$\begin{aligned}
f_p(n-1) &= f_p(n) - n^p = \frac{1}{p+1} \sum_{k=0}^p \binom{p+1}{k} B_k n^{p+1-k} \\
&= \frac{1}{p+1} \left(\sum_{k=0}^{p+1} \binom{p+1}{k} B_k n^{p+1-k} - B_{p+1} \right) \\
&= \frac{1}{p+1} ((B+n)^{p+1} - B_{p+1}) \\
&= \frac{1}{p+1} (B_{p+1}(n) - B_{p+1}),
\end{aligned}$$

or Bernoulli's form,

$$\sum_{m=1}^{n-1} m^{p-1} = \frac{1}{p} (B_p(n) - B_p).$$

This equation holds clearly for $n = 0$

$$\sum_{m=0}^0 m^{p-1} = 0 = \frac{1}{p} (B_p(1) - B_p).$$

We assume that it also holds for n . Then

$$\begin{aligned}
\sum_{m=1}^n m^{p-1} &= \frac{1}{p} (B_p(n) - B_p) + n^{p-1} \\
&= \frac{1}{p} (B_p(n) + p n^{p-1} - B_p) \\
&= \frac{1}{p} (B_p(n+1) - B_p)
\end{aligned}$$

by the of $B_p(n)$, it also holds for $n + 1$, completing the induction.

Catalan's conjecture / Mihăilescu's theorem

The Catalan problem dates back at least to Gersonides, who proved a special case of the conjecture in 1343 where x and y were restricted to be 2 or 3. It was conjectured by Eugène Charles Catalan in 1844 and proven in 2002 by Preda Mihăilescu:

$$x^a - y^b = 1$$

for $x, a, y, b > 1$ has solutions: $x = 3, a = 2, y = 2, b = 3$.

Notice that 2^3 and 3^2 are two powers of natural numbers, whose values 8 and 9 respectively are consecutive. This is the *only* case of two consecutive powers.

The Fermat-Catalan conjecture

The **Fermat–Catalan conjecture** combines ideas of Fermat's last theorem and the Catalan conjecture:

$x^p + y^q = z^r$ has only a finite number of solutions if x , y & z are coprimes and $1/p+1/q+1/r \leq 1$.

nowadays only 10 solutions are known:

$$1+2^3 = 3^2 \text{ (Catalan)}$$

$$2^5+7^2 = 3^4$$

$$7^3+13^2 = 2^9$$

$$2^7+17^3 = 71^2$$

$$3^5+11^4 = 122^2$$

$$17^7+76271^3 = 21063928^2$$

$$1414^3+2213459^2 = 65^7$$

$$9262^3+15312283^2 = 113^7$$

$$43^8+96222^3 = 30042907^2$$

$$33^8+1549034^2 = 15613^3$$

The abc conjecture implies the Fermat–Catalan conjecture and is stated in terms of three positive integers, a , b and c (whence comes the name), which have no common factor and satisfy $a + b = c$. If d denotes the product of the distinct prime factors of abc , the conjecture essentially states that d is rarely much smaller than c .

ABC conjecture

Let A , B , and C be three coprime integers (A , B , C have no common factor) such that

$$A + B = C$$

Now multiply together all the distinct primes that divide any of these numbers, and call the result $\text{rad}(ABC)$. For a positive integer n , the radical of n , denoted $\text{rad}(n)$, is the product of the distinct prime factors of n . If d denotes the product of the distinct prime factors of abc , the conjecture essentially states that d is rarely much smaller than c .

Example1

- $\text{rad}(16) = \text{rad}(2^4) = 2$,
- $\text{rad}(17) = 17$,
- $\text{rad}(18) = \text{rad}(2 \cdot 3^2) = 2 \cdot 3 = 6$.

Example2

If we start with $4 + 11 = 15$, we have 2 (which divides 4), 11 (which divides 11) and 3 and 5 (which divide 15), so $\text{rad}(ABC) = 2 \times 11 \times 3 \times 5 = 330$.

C is almost always smaller than $\text{rad}(ABC)$, but not always. If you start with $2 + 243 = 245$, the primes are 2 (which divides 2), 3 (which divides 243), and 5 and 7 (which divide 245). So $\text{rad}(ABC) = 2 \times 3 \times 5 \times 7 = 210$. In this case, C is much bigger than $\text{rad}(ABC)$.

Example3

Let a, b, c be integers such that $a^6 + 2b^6 = 4c^6$. Show that $a = b = c = 0$.

Solution: Clearly we can restrict ourselves to nonnegative numbers. Choose a triplet of nonnegative integers a, b, c satisfying this equation and with $\max(a, b, c) > 0$ as small as possible. If $a^6 + 2b^6 = 4c^6$ then a must be even, $a = 2a_1$. This leads to $32a_1^6 + b^6 = 2c^6$. Hence $b = 2b_1$ and so $16a_1^6 + 32b_1^6 = c^6$. This gives $c = 2c_1$, and so $a_1^6 + 2b_1^6 = 4c_1^6$. But clearly $\max(a_1, b_1, c_1) < \max(a, b, c)$. This means that all of them must be zero.

Euler - Riebach conjecture

If $x^p + y^q + z^r = A^b$ has only a finite number of solutions if x, y & z are coprimes $b > 1$ and $p, q, r \geq 1$.

$$3+2+1=6 ; 3^3+2^3+1^3=6^2.$$

$$3+2+5=10 ; 3^2+2^4+5^2=10^2.$$

$$5+4+3=12 ; 5^3+4^2+3^1=12^2.$$

$$4+2+3=9 ; 4^3+3^2+2^3=9^2.$$

etc

$x^4 + y^4 + z^4 = A^4$ has only 1 known integer solution:

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

Power equations or exponentiation

$$2^2=1+ 3 = 4$$

$$3^2=1+ 3 + 5= 9$$

$$4^2=1+ 3+ 5 +7 =16$$

$$1-----3-----5-----7$$

$$---2----2-----2$$

$$2^3=1+ 7 = 8$$

$$3^3=1+ 7 + 19= 27$$

$$4^3=1+ 7+ 19 +37 =60$$

$$5^3=1+ 7+ 19 +37 +61= 125$$

$$6^3=1+ 7+ 19 +37 +61+91= 216$$

$$1----7----19----37----61----91$$

$$--6----12----18----24----30$$

$$-----6-----6-----6-----6$$

$$2^4=1+ 15 = 16$$

$$3^4=1+ 15+65= 81$$

$$4^4=1+15+65+175=256$$

$$5^4=1+15+65+175+369=625$$

$$6^4=1+15+65+175+369+671=1269$$

$$1-----15-----5-----75-----369-----671$$

$$---14---50---110---194---302$$

$$-----36---60-----84-----108$$

$$-----24-----24-----24-$$

$$2^5=1+31=32$$

$$3^5=1+31+211=243$$

$$4^5=1+31+211+781=1024$$

$$5^5=1+31+211+781+2101=3125$$

$$6^5=1+31+211+781+2101+4651=7776$$

$$1-----31-----211-----781-----2101-----4651$$

$$---30---180---570---1320---2550---$$

$$-----150---390-----750-----1230-----$$

$$-----240---360-----480-----$$

$$-----120---120-----$$

Etc. This appears to be related to factorials n!

$$n! = \prod_{k=1}^n k = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$$

power	factor
1	1
2	2
3	6
4	24
5	120
6	720
7	5040
8	40320
9	362880
10	3628800
11	39916800
12	479001600
13	6227020800
14	87178291200
15	1307674368000
16	20922789888000
17	355687428096000
18	6402373705728000
19	121645100408832000
20	2432902008176640000

Theorem

Every fourth power >1 is the sum of 2 consecutive triangular numbers.

If $t_k = 1 + 2 + \dots + k$ then

$$2^4 = 15 + 1 = t_5 + t_1$$

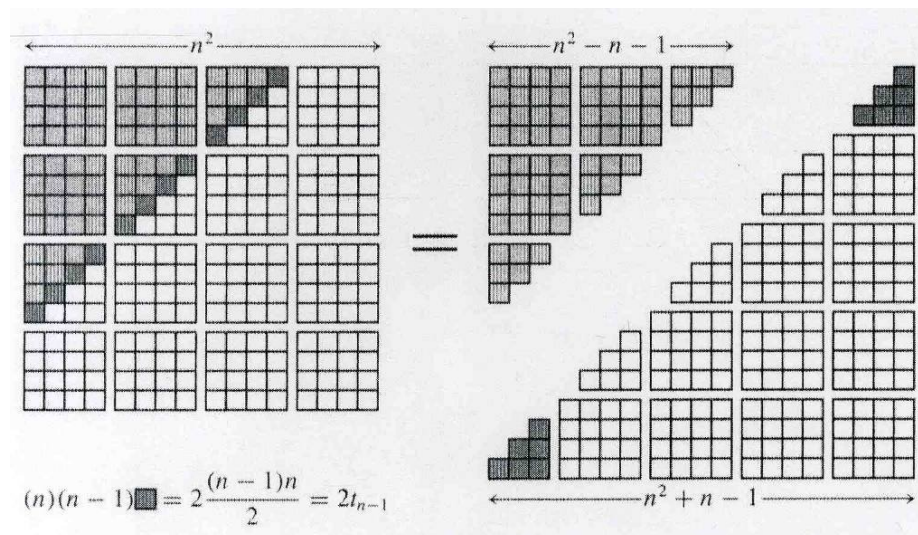
$$3^4 = 16 + 15 = t_{11} + t_5$$

$$4^4 = 190 + 66 = 256 = t_{19} + t_{11}$$

.

.

$$n^4 = t_{n^2+n+1}^2 + t_{n^2-n-1}^2$$



Since $k^2 = t_{k-1} + t_k$ we also have $n^4 = t_{n^2-n-1} + t_{n^2+n+1}$

Power additions

$1^2 = 1^1 + 1^0 \cdot 1$	$2^2 = 2^1 + 2^0 \cdot 2$	$3^2 = 3^1 + 3^0 \cdot 6$
$1^3 = 1^2 + 1^1 \cdot 1$	$2^3 = 2^2 + 2^1 \cdot 2$	$3^3 = 3^2 + 3^1 \cdot 6$
Etc	$2^4 = 2^3 + 2^2 \cdot 2$	$3^4 = 3^3 + 3^2 \cdot 6$
	Etc	$3^5 = 3^4 + 3^3 \cdot 6 = 3^3 + 3^2 \cdot 6 + 3^3 \cdot 6 = 3^3 + 6 \cdot (3^2 + 3^3) = 3^3 + 6^3$ etc

$4^2=4^1+$ $4^0.12$	$5^2=5^1+$ $5^0.20$	$6^2=6^1+ 6^0.30$
$4^3=4^2+$ $4^1.12$	$5^3=5^2+$ $5^1.20$	$6^3=6^2+ 6^1.30$
$4^4=4^3+$ $4^2.12$	$5^4=5^3+$ $5^2.20$	$6^4=6^3+ 6^2.30$
Etc	Etc	$6^5=6^4+ 6^3.30 = 6^3+ 6^2.30 + 6^3.30 = 6^2+ 6^1.30+ 6^2.30 + 6^3.30=6^1+$ $6^0.30+6^1.30+ 6^2.30 + 6^3.30= 6+ (6^0+6^1+ 6^2 +6^3).30 = 1 + (6^0+6^1+ 6^2$ $+6^3+6^4)5)$ Etc

$$(82)^5 = (82)^4 + 81. (82)^4 = (82)^4 + (3 \times 82)^4$$

Etc.

a	1	2	3	4	5	6	7	8	9
a.(a-1)		2	6	12	20	30	42	56	72

In general

$$a^x = a^{x-n} + \sum_{m=0}^{n-1} a^m .a(a-1)$$

(with $n < x$).

Proof:

$$a^x = a^{x-1} + a^{x-2}.q$$

since a^x must equal $a^{x-1} + a^{x-1}$ then $a^{x-2}.q$ must equal a^{x-1} . This gives $q = a^2 - a^1 = a(a-1)$

As can be seen from above examples with $a=6$ and $x = 4$ and $n=3$: $6^4 = 6^1 + (6^2 + 6^1 + 6^0).30$

$$\text{In general : } a^x = 1 + \sum_{m=0}^{x-1} a^m .(a-1)$$

for $a = 4$ and $x = 3,4,5$ we have:

$$\begin{aligned} 64 + 3(64) &= 256 (= 4^4) \\ 64 + 15(64) &= 1024 (= 4^5) \\ 64 + 63(64) &= 4096 (= 4^6), \end{aligned}$$

and, equivalently, $4^3 + (3)4^3 + (3)4^4 + (3)4^5 = 4^6$

$$a^p + (a-1)a^p + (a-1)a^{p+1} + (a-1)a^{p+2} + (a-1)a^{p+3} \dots + (a-1)a^{p+(n-1)} = a^{p+n},$$

or in general $a^1 + (a-1)a^1 + (a-1)a^2 + (a-1)a^3 + (a-1)a^4 \dots + (a-1)a^{n-1} = a^n$

above series can then be rewritten as:

$$\begin{aligned} 1^1 &: (1+1)^1 + [(1^1)^{-1}(1^1+1)]^1 = (2)^1 + (1 \times 2)^1 = (2)^2 ; \\ 1^2 &: (1+1)^2 + [(1^2)^{-2}(1^2+1)]^2 = (2)^2 + (1 \times 2)^2 = (2)^3 ; \\ 1^3 &: (1+1)^3 + [(1^3)^{-3}(1^3+1)]^3 = (2)^3 + (1 \times 2)^3 = (2)^4 ; \\ 1^4 &: (1+1)^4 + [(1^4)^{-4}(1^4+1)]^4 = (2)^4 + (1 \times 2)^4 = (2)^5 ; \\ 1^5 &: (1+1)^5 + [(1^5)^{-5}(1^5+1)]^5 = (2)^5 + (1 \times 2)^5 = (2)^6 ; \end{aligned}$$

etc.

$$\begin{aligned} 2^1 &: (2+1)^1 + [(2^1)^{-1}(2+1)]^1 = (3)^1 + (2 \times 3)^1 = (3)^2 ; \\ 2^2 &: (4+1)^2 + [(2^2)^{-2}(4+1)]^2 = (5)^2 + (2 \times 5)^2 = (5)^3 ; \\ 2^3 &: (8+1)^3 + [(2^3)^{-3}(8+1)]^3 = (9)^3 + (2 \times 9)^3 = (9)^4 ; \\ 2^4 &: (16+1)^4 + [(2^4)^{-4}(16+1)]^4 = (17)^4 + (2 \times 17)^4 = (17)^5 ; \\ 2^5 &: (32+1)^5 + [(2^5)^{-5}(32+1)]^5 = (33)^5 + (2 \times 33)^5 = (33)^6 ; \end{aligned}$$

etc.

$$\begin{aligned} 3^1 &: (3+1)^1 + [(3^1)^{-1}(3+1)]^1 = (4)^1 + (3 \times 4)^1 = (4)^2 ; \\ 3^2 &: (9+1)^2 + [(3^2)^{-2}(9+1)]^2 = (10)^2 + (3 \times 10)^2 = (10)^3 ; \\ 3^3 &: (27+1)^3 + [(3^3)^{-3}(27+1)]^3 = (28)^3 + (3 \times 28)^3 = (28)^4 ; \\ 3^4 &: (81+1)^4 + [(3^4)^{-4}(81+1)]^4 = (82)^4 + (3 \times 82)^4 = (82)^5 ; \\ 3^5 &: (243+1)^5 + [(3^5)^{-5}(243+1)]^5 = (244)^5 + (3 \times 244)^5 = (244)^6 ; \end{aligned}$$

etc.

All terms are ground whole-number powers, i.e., in the irreducible form with all external coefficients = 1 ,excluding other solutions

Example:

$$\begin{aligned} 4^2 &= 2^2 + 3 \cdot 2^2 ; & 6^2 &= 3^2 + 3 \cdot 3^2 = 3^2 + 3^3 ; \\ 4^3 &= 2^3 + 7 \cdot 2^3 ; & 14^3 &= 7^3 + 7 \cdot 7^3 = 7^3 + 7^4 \quad \text{etc} \\ 4^4 &= 2^4 + 15 \cdot 2^4 ; & 30^4 &= 15^4 + 15 \cdot 15^4 = 15^4 + 15^5 \quad \text{etc} \\ 4^5 &= 2^5 + 31 \cdot 2^5 ; & 62^5 &= 31^5 + 31 \cdot 31^5 = 31^5 + 31^5 \quad \text{etc} \end{aligned}$$

More examples:

$$\begin{aligned} 2+3 &= 5 \\ 2^2+3^2 &= 2 \cdot 5 + 3^1 = (3 \cdot 5 - 2^1) = 13 \\ 2^3+3^3 &= 2 \cdot 13 + 3^2 = (3 \cdot 13 - 2^2) = 35 \\ 2^4+3^4 &= 2 \cdot 35 + 3^3 = (3 \cdot 35 - 2^3) = 97 \\ \text{Etc} \\ 2^4+3^3 &= 2^3+3^3 + 2^3 = 2^4+3^4 - 2 \cdot 3^3 = 43 \\ 2^5+3^3 &= 2^3+3^3 + 2^3 + 2^4 = 2^4+3^3 + 2^4 = 2^5+3^5 - 2^3 \cdot 3^3 = 59 \end{aligned}$$

$$\begin{aligned} 4+3 &= 7 \\ 4^2+3^2 &= 3 \cdot 7 + 4 = (4 \cdot 7 - 3) \end{aligned}$$

$$4^3+3^3=3.(4^2+3^2) + 4^2 = (4.(4^2+3^2) - 3^2)$$

$$4^4+3^4=3.(4^3+3^3) + 4^3 = (4.(4^3+3^3) - 3^3)$$

Etc

$$4+5=9$$

$$4^2+5^2=4.9 + 5 = (5.9 - 4) = 41$$

$$4^3+5^3=4.(4^2+5^2) + 5^2 = (5.(4^2+5^2) - 4^2) = 189$$

$$4^4+5^4=4.(4^3+5^3) + 5^3 = (5.(4^3+5^3) - 4^3) = 781$$

Etc

$$4+7=13$$

$$4^2+7^2=4.13 + 13 = (7.13 - 2.13) = 65$$

$$4^3+7^3=4.(4^2+7^2) + 7^2 = (7.(4^2+7^2) - 4^2) = 407$$

$$4^4+7^4=4.(4^3+7^3) + 7^3 = (7.(4^3+7^3) - 4^3) = 781$$

Etc

In general:

$$a^m + b^m = a.(a^{m-1} + b^{m-1}) + b^{m-1} = b.(a^{m-1} + b^{m-1}) - b^{m-1}$$

For the example:

$$2^4+5^3 = 16+125 = 141 = 2.(2^2+5^2) + 5^2.3 + (2^4-2^3)$$

There holds :

$$a^m + b^n = a.(a^{m-2} + b^{n-2}) + b^{n-1}.(b-a) + (a^m - a^{m-1})$$

Beal Conjecture:

If $A^x + B^y = C^z$, where A, B, C, x, y and z are positive integers and x, y and z are all greater than 2, then A, B and C must have a common prime factor. A variation of the conjecture where x, y, z (instead of A, B, C) must have a common prime factor is not true.

$A^x + B^y = C^z$, is related to Fermat's Last Theorem that $A^x + B^x = C^x$ is impossible. If $A^x + B^x = C^x$ then either A, B, and C are co-prime or, if not co-prime that any common factor could be divided out of each term until the equation existed with co-prime bases. (Co-prime is synonymous with pairwise relatively prime and means that in a given set of numbers, no two of the numbers share a common factor.)

Just as Fermat's equation can be solved if the exponent n is equal to 1 or 2 (the best known solution for n=2 is the "Pythagorean triple" x=3, y=4, z=5, other examples are (5, 12, 13), (7, 24, 25), (8, 15, 17)), hence the reason why x, y and z in Beal's conjecture equation have to be greater than 2.

For any exponent n, the corresponding Fermat equation could only have a finite number of solutions, so too it is known that for any three exponents x, y, and z greater than 2, the

corresponding Beal equation has only a finite number of solutions. For Fermat's last theorem the finite number for any exponent is in fact zero. Solving the Beal equation is equivalent to solving $A + B = C$ under the condition that A be a x-th power, B be a y-th power, and C be a z-th power

a. $[(a^m+b^m)]^m + b \cdot [(a^m+b^m)]^m = (a^m+b^m)^{m+1}$ for any $a, b, m > 3$ has infinite many solutions, but no such solution of the equation is a counterexample to the Beal conjecture since the bases all have factor (a^m+b^m) in common.

Examples of the Beal Conjecture:

- The solution $3^6 + 6^3 = 3^5$ has bases with a common factor of 3 ($3^5 = 3^4 + 3^3 \cdot 6 = 3^3 + 3^2 \cdot 6 + 3^3 \cdot 6 = 3^3 + 6 \cdot (3^2 + 3^3) = 3^3 + 6^3$)
- The solution $7^6 + 7^7 = 98^3$ has bases with a common factor of 7 (proof: $7^3 \cdot 14^3 = 7^3 \cdot (7^3 + 7^4) = 7^6 + 7^7 = 98^3$)
- $3^9 + 54^3 = 3^{11}$ Common factor 3 ($3^{11} = 3^9 + 6 \cdot (3^8 + 3^9) = 3^9 + 54^3$)
- $27^4 + 162^3 = 9^7$ Common factor 3 ($9^7 = 9^6 + 8 \cdot 9 \cdot 9^5 = 9 \cdot 4 \cdot 3^4 + 2^3 \cdot 9^3 \cdot 9^3 = 27^4 + 162^3$)
- $34^5 + 51^4 = 85^4$ Common factor 17 ($17^5 = 17^4 (1+16) = 17^4 (81-64) = 17^4 (3^4 - 2^6) = 2^5 \cdot 17^5 + 3^4 \cdot 17^4 = 2^4 \cdot 17^4 = 85^4 = 34^5 + 51^4$)
- $19^4 + 38^3 = 57^3$ Common factor 19 ($19^5 = 19^4 + 19^3 \cdot 18 \cdot 19 = 19^4 + 19 \cdot 19^3 \rightarrow 19^4 + 2^3 \cdot 19^3 = 3^2 \cdot 19^3$)

we use the lemma from above section:

$$a^x = a^{x-n} + \sum_{m=0}^{n-1} a^m \cdot a(a-1)$$

Let a, and b be integers. Then for a and b there holds:

$$a^{x-1} + ((x-2) \cdot a)^{x-1} = a^x = 1 + \sum_{m=0}^{x-1} a^m \cdot (a-1) = \text{integer } a \text{ multiplied by some integer} =$$

prime factor multiplied by some integer

$$b^{x-1} + ((x-2) \cdot b)^{x-1} = b^x = 1 + \sum_{m=0}^{x-1} b^m \cdot (b-1) = \text{integer } b \text{ multiplied by some integer} =$$

prime factor multiplied by some integer

The above equation (***) can be rewritten as: $a^{x-n} + ((a-1) \cdot a)^{x-n} = a^x = b^y + c^z$, with $b^y = a^{x-n}$ and $c^z = ((a-1)^{n-x} \cdot a)^{x-n}$ ($n < x$) so that

$$b^y = a^{x-n} \text{ and } c^z = ((a-1)^{n-x} \cdot a)^{x-n} \text{ or}$$

$$b = a^{(x-n)/y} \text{ and } c = ((a-1)^{n-x} \cdot a)^{x-n/z}$$

This can only be the case if b and c share factor a as shows from above formulas and a may be composed into the least prime factor and $(x-n)/y$ and $(x-n)/z$ are integers

In the above example : $19^4 + 38^3 = 57^3$ with common factor 19 this can be rewritten as
 $:19^5 = 19^4 + 19^3 \cdot 18 \cdot 19 = 19^4 + 18 \cdot 19^4 \rightarrow$ here $x=n=5-1=4$ and $y=4$ so that $b = a^{(x-n)/y} = 19$ and
 $c = ((a-1)^{n-x} \cdot a)^{x-n/z} = F^1$ with $F=18^4 \cdot 19=9^2 \cdot 2^2 \cdot 19$, since $19=3^3 \cdot 2^3$ this can also be written as:

$$19^4 + 2^3 \cdot 19^3 = 3^3 \cdot 19^3$$

Q.E.D.

Theorem

$x^n - y^n$ is divisible by $x+y$ for each negative number n .

Proof: Show that $x^{2n} - y^{2n}$ is divisible by $x+y$.

Exercises: show that:

$$x^n - y^n = (x - y) \cdot \sum_{k=0}^{n-1} x^{n-1-k} \cdot y^k$$

Proof: $x^n - y^n = (x - y) \cdot (x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + x \cdot y^{n-2} + y^{n-1})$ Thus $x-y$ always divides $x^n - y^n$. We may assume that $x \neq y, xy \neq 0$, the result being otherwise trivial. In that case, the result follows at once from the identity

$$\sum_{k=0}^{n-1} a^k = \frac{a^n - 1}{a - 1}, \quad a \neq 1$$

upon letting $a = x/y$ and multiplying through by y^n .

E.g. from above we see that $8767^{2345} - 8101^{2345}$ is divisible by 666.

Also proof that

$$x^{2n} - y^{2n} = (x + y) \cdot \sum_{k=0}^{2n-1} (-1)^k \cdot x^{2n-1-k} \cdot y^k$$

$$x^{2n+1} + y^{2n+1} = (x + y) \cdot \sum_{k=0}^{2n} (-1)^k \cdot x^{2n-k} \cdot y^k$$

Theorem (of Grünert)

If x, y, z, n are natural numbers $n \geq z$, then the relation $x^n + y^n = z^n$ does not hold.

Proof: If the relation $x^n + y^n = z^n$ holds for natural numbers x, y, z then $x < z$ and $y < z$. By symmetry, we may suppose that $x < y$. So assume $x^n + y^n = z^n$ and $n \geq z$. Then
 $z^n - y^n = (z - y)(z^{n-1} + yz^{n-2} + \dots + y^{n-1}) \geq 1 \cdot nx^{n-1} > xn$, contrary to the assertion that $x^n + y^n = z^n$.

Theorem

The equation $x^n + y^n = z^n$ has no integer solutions for $n > 2$ and $x, y, z \neq 0$. (Fermat's Last Theorem).

The restriction $n > 2$ is obviously necessary since there are a number of elementary formulas for generating an infinite number of Pythagorean triples (x, y, z) satisfying the equation for $n = 2$,

$$x^2 + y^2 = z^2.$$

A first attempt to solve the equation can be made by attempting to factor the equation, giving

$$(z^{n/2} + y^{n/2})(z^{n/2} - y^{n/2}) = x^n.$$

Since the product is an exact power,

$$\begin{cases} z^{n/2} + y^{n/2} = 2^{n-1} p^n \\ z^{n/2} - y^{n/2} = 2 q^n \end{cases} \text{ or } \begin{cases} z^{n/2} + y^{n/2} = 2 p^n \\ z^{n/2} - y^{n/2} = 2^{n-1} q^n. \end{cases}$$

Solving for y and z gives

$$\begin{cases} z^{n/2} = 2^{n-2} p^n + q^n \\ y^{n/2} = 2^{n-2} p^n - q^n \end{cases} \text{ or } \begin{cases} z^{n/2} = p^n + 2^{n-2} q^n \\ y^{n/2} = p^n - 2^{n-2} q^n, \end{cases}$$

which give

$$\begin{cases} z = (2^{n-2} p^n + q^n)^{2/n} \\ y = (2^{n-2} p^n - q^n)^{2/n} \end{cases} \text{ or } \begin{cases} z = (p^n + 2^{n-2} q^n)^{2/n} \\ y = (p^n - 2^{n-2} q^n)^{2/n}. \end{cases}$$

However, since solutions to these equations in rational numbers are no easier to find than solutions to the original equation, this approach unfortunately does not provide any additional insight.

If an odd prime p divides n , then the reduction

$$(x^{n/p})^p + (y^{n/p})^p = (z^{n/p})^p$$

can be made, so redefining the arguments gives

$$x^{n/p} + y^{n/p} = z^{n/p}.$$

If no odd prime divides n , then n is a power of 2, so $4 | n$ and, in this case, the last two above equations work with 4 in place of p . Since the case $n = 4$ was proved by Fermat to have no solutions, it is sufficient to prove Fermat's last theorem by considering odd prime powers only.

Conclusions

- The equation $X^a + Y^b = Z^c$ has no solution in positive integers $X, Y, Z, a, b,$ and $c,$ with $a, b, c > 2,$ if X and Y have a common factor but each of them separately coprime with $Z,$ or at least any one of X and Y is coprime with $Z.$
- Let $X, Y, Z, a, b,$ and c be positive integers, with $a, b, c > 2.$ If X and Y coprime but each of them separately has common factor with $Z,$ or at least any one of X and Y has common factor with $Z,$ then $X^a + Y^b = Z^c.$
- Let $X, Y, Z, a, b,$ and c be positive integers, with $a, b, c > 2.$ Whether X and Y have a common factor or not, the equation $X^a + Y^b = Z^c$ has a solution if each of X and Y has common factor with $Z;$ and $X^a + Y^b = Z^c$ has no solution if each of X and Y separately coprime with $Z.$ If at least any one of X and Y is coprime with $Z,$ then $X^a + Y^b = Z^c$ has a solution if X and Y coprime; and $X^a + Y^b = Z^c$ has no solution if X and Y have a common factor.

Theorem:

There are no integer solutions of $x^4 + y^4 = z^2.$

PROOF: Suppose there are integers x, y, z such that $x^4 + y^4 = z^2.$

This can be written as a Pythagorean triple $(x^2)^2 + (y^2)^2 = z^2,$ from which it follows that $y^2 = 2pq, x^2 = p^2 - q^2,$ and $z = p^2 + q^2.$ Since $2pq$ is a square, we know that either p or q is even. Thus, from the Pythagorean triple $x^2 + q^2 = p^2$ we have $x = r^2 - s^2, q = 2rs,$ and $p = r^2 + s^2.$ Also, since $2pq$ is a square we can set $q = 2u^2$ and $p = v^2.$ Since $2u^2 = 2rs,$ we have $r = gu^2$ and $s = hu^2.$ These, along with $p = v^2,$ can be substituted back into $p = r^2 + s^2$ to give $v^2 = g^4 + h^4,$ where v is smaller than $z,$ contradicting the fact that there must be a smallest solution.

Theorem:

There are no integer solutions of $x^4 - y^4 = z^2.$

PROOF: Suppose there are integers x, y, z such that $x^4 - y^4 = z^2.$

This can be written as a Pythagorean triple $(x^2)^2 + z^2 = (y^2)^2,$ If z is even this implies $y^2 = p^2 - q^2, z = 2pq,$ and $x^2 = p^2 + q^2,$ where x and y are both odd, from which we have $p^4 - q^4 = (xy)^2.$ Therefore, the existence of a solution with even z implies the existence of a solution of the original equation with odd $z,$ so we need only prove that a solution with odd z is impossible.

Assuming odd $z,$ the Pythagorean triple implies $y^2 = 2pq, z = p^2 - q^2,$ and $x^2 = p^2 + q^2.$ Since $2pq$ is a square, we can set $q = 2u^2$ and $p = v^2.$ Also, from the Pythagorean triple $x^2 = p^2 + q^2$ we have $p = r^2 - s^2, q = 2rs,$ and $x = r^2 + s^2.$

Since $2u^2 = 2rs$, it follows that $r = g^2$ and $s = h^2$. These, along with $p = v^2$, can be substituted back into $p = r^2 - s^2$ to give $v^2 = g^4 - h^4$, where v is smaller than z , contradicting the fact that there must be a smallest solution.

10. Prime number theorems

Gaps between primes

For every prime p let $g(p)$ be the number of composites between p and the next prime. Letting p_n be the n th prime we have:

$$p_{n+1} = p_n + g(p_n) + 1.$$

That is, $g(p_n)$ is the (size of) gap between p_n and p_{n+1} .

E.g. gap between 7 and 11 is 3 and $g(p) = 1$ for twin primes $p, p+2$

Example: consider the following sequence of consecutive integers:

$$n!+2, n!+3, n!+4, n!+5, \dots, n!+n$$

Since 2 divides the first, 3 divides the second, ..., n divides the $n-1$ st, all of these numbers are composite! So if p is the largest prime less than $n!+2$ we have $g(p) > n-1$

theorem

$$\limsup g(n)/\log p_n = \text{infinity}$$

which means that for every $\beta > 0$ there are infinitely many primes p with $g(p) > \beta \log p$.

Goldbach conjecture

Every even number greater than 2 can be written as the sum of two prime numbers (whereby a prime number can be used twice) . This is called the strong Goldbach conjecture

In prenex normal form:

$$\forall n \exists p \exists q \forall a, b, c, d [(n > 1, a, b, c, d > 1) \Rightarrow ((p + q = 2n) \wedge (ab \neq p) \wedge (cd \neq q))]$$

A modern version of Goldbach's marginal conjecture is:

Every integer greater than 5 can be written as the sum of three primes.

The strong Goldbach conjecture implies the conjecture that all odd numbers greater than 7 are the sum of three odd primes, which is known today variously as the "weak" Goldbach conjecture, the "odd" Goldbach conjecture, or the "ternary" Goldbach conjecture.

Examples of the strong Goldbach conjecture:

$$\begin{aligned} 4 &= 2 + 2 \\ 6 &= 3 + 3 \\ 8 &= 3 + 5 \\ 10 &= 3 + 7 \text{ or } 5 + 5 \\ 12 &= 5 + 7 \end{aligned}$$

$14 = 3 + 11$ or $7 + 7$
 $16 = 3 + 13 = 5 + 11$
 $18 = 5 + 13 = 7 + 11$
 $20 = 3 + 17 = 7 + 13$
 $22 = 3 + 19 = 5 + 17 = 11 + 11$
 $24 = 5 + 19 = 7 + 17 = 11 + 13$
 $26 = 3 + 23 = 7 + 19 = 13 + 13$
 $28 = 5 + 23 = 9 + 19 = 11 + 17$
 $30 = 7 + 23 = 11 + 19 = 13 + 17$
 $32 = 3 + 29 = 9 + 23 = 13 + 19 = 15 + 17$
 $34 = 3 + 31 = 5 + 29 = 11 + 23 = 17 + 17$
 $36 = 5 + 31 = 7 + 29 = 13 + 23 = 17 + 19$

Etc (Every integer is the sum of at most 6 primes).

Observations:

Consider the prime series: $p_i\{3, 5, 7, 11, 17, 19, 23..\}$

$p_1+p_2=3+3=6$; $p_1+p_2=3+5=8$; $p_1+p_3=3+7=10$; $p_1+p_4=14$; $p_1+p_5=20$; $p_1+p_6=22$; $p_1+p_7=26$;
 $p_2+p_2=5+5=10$; $p_2+p_3=12$; $p_2+p_4=16$; $p_2+p_5=22$; $p_2+p_6=24$; $p_2+p_7=28$;
 $p_3+p_3=7+7=14$; $p_3+p_4=18$; $p_3+p_5=24$; $p_3+p_6=26$; $p_3+p_7=30$;
 $p_4+p_4=11+11=22$; $p_4+p_5=28$; $p_4+p_6=30$; $p_4+p_7=34$;
 $p_5+p_5=17+17=34$; $p_5+p_6=36$; $p_5+p_7=40$;
 $p_6+p_6=19+19=36$; $p_6+p_7=42$;
 $p_7+p_7=46$;

From above table it can be seen that for instance $2N=30$ can be made from the combinations: p_3+p_7 and $p_4+p_6=30$.

As we saw from Goldbach's conjecture : $36=5+31=7+29=13+23=17+19$

$\pi(36) = 10$, namely 3, 5, 7, 11, 13, 17, 19, 23, 29

Since 36 is a multiple (>2) of 3 this number cannot be used for combining the numbers. It's complement is 33 which is a multiple of 11 so that this number can't be used either.

$16 = 3 + 13 = 5 + 11$; $\pi(16) = 5$, namely 3, 5, 7, 11, 13. The middle number 7 cannot be combined with any other so it can not be used.

$18 = 5 + 13 = 7 + 11$; $\pi(18) = 6$, namely 3, 5, 7, 11, 13, 17. Since 18 is a multiple (>2) of 3 this number cannot be used for combining the numbers. It has no complement, but the last number 17 can't be used either since difference of $2N$ (here 18) and the last prime must be larger or equal to 3.

$24 = 5 + 19 = 7 + 17 = 11 + 13$; $\pi(24) = 7$, namely 3, 5, 7, 11, 13, 17, 19, 23. Since 24 is a multiple (>2) of 3 this number cannot be used for combining the numbers. It has no complement, but the last number 23 can't be used either since difference of $2N$ (here 24) and the last prime must be larger or equal to 3.

The function $\pi(x)$ is the number of prime numbers less or equal than a given value x :

$$\pi(x) = \# \{ p \leq x, \quad p \text{ is prime} \}.$$

For example, $\pi(11) = 5$ since there are 5 primes less than or equal to 11, which are 2, 3, 5, 7 and 11 and $\pi(100) = 25$, since there are 25 primes less than or equal to 100. For n very large $\pi(n)$ is approximately $n/\ln(n)$.

For every prime p let $G(p)$ be the number of composites between p and the next prime. If p_n is the n th prime we have:

$$p_{i+1} = p_i + G(p_i).$$

Then is, $G(p_i)$ is the (size of) gap between p_i and p_{i+1}

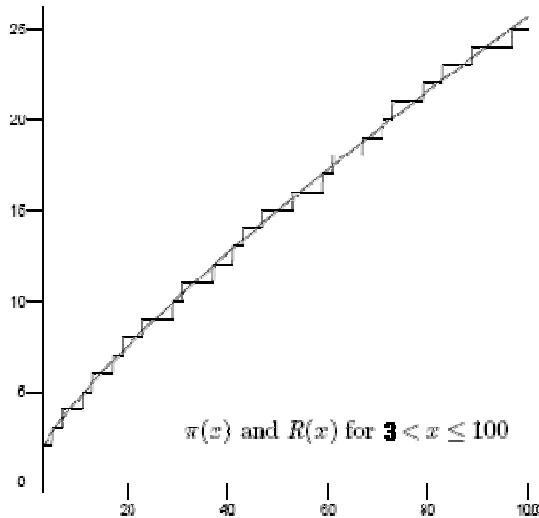
Example: $p_{i+1} = 17 = 13 + G(p_i)$. so that $G(13) = 4$

$G(p)$ can be arbitrarily large. Let n be *any* integer greater than one and consider the following sequence of consecutive integers:

$$n!+2, n!+3, n!+4, n!+5, \dots, n!+n$$

Since 2 divides the first, 3 divides the second, ..., n divides the $n-1$ st, all of these $n-1$ consecutive numbers are composite. So if p is the largest prime less than $n!+2$ we have $g(p) > n-1$. Therefore, there exist gaps between primes which are arbitrarily large, i.e. for any natural number " N ", there is an integer " i " with " $g(p_i) > N$ ". (Choose " i " so that " p_i " is the greatest prime number less than " $N! + 2$ "). On the other hand, the gaps get arbitrarily small in proportion to the primes: the quotient " $g(p_i)/p_i$ " approaches zero as " n " approaches infinity. (Note :the twin prime conjecture asserts that " $g(p_i) = 2$ " for infinitely many integers " i ".) Harald Cramér conjectured on probabilistic ideas, that the large values of $G(p_n)$ grow like $(\log p_n)^2$. Dorin Andrica conjectured that $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$, where p_n is the n^{th} prime number. If we substitute p_{n+1} by $p_n + g_n$ then this can be written as $g_n < \sqrt{p_n} + 1$, which was computed to hold up to $n=1,300 \times 10^{16}$ in 2008.

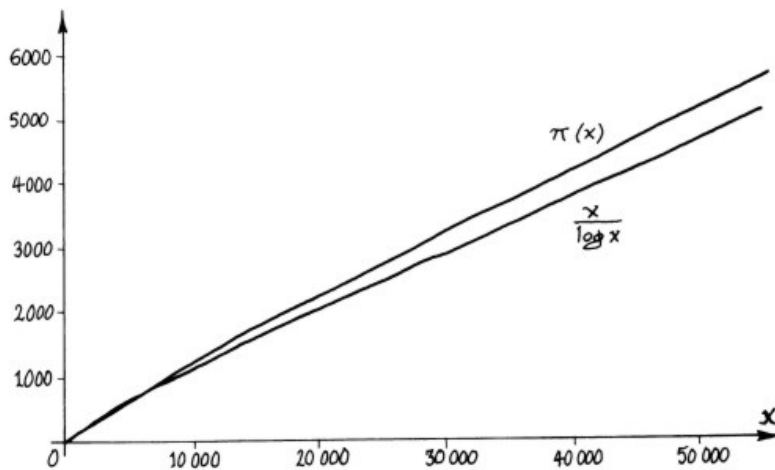
Prime number theorem



$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} Li(x^{1/n})$$

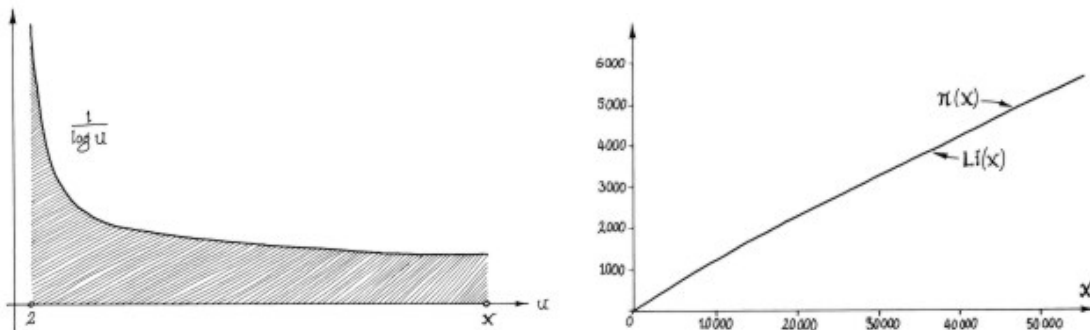
(definition for the function $R(x)$ is where $\mu(n)$ are the Möbius numbers. These are defined to be zero when n is divisible by a square, and otherwise to equal $(-1)^k$ where k is the number of distinct prime factors in n . As 1 has no prime factors, it follows that $\mu(1) = 1$.)

One of the mathematical breakthroughs of the nineteenth century has been the *prime number theorem*, proven independently by Hadamard and De La Vallée Poussin in 1896. Roughly speaking, it states that as x becomes big, $\pi(x)$ is close to $L(x) = x/\log(x)$ also written as $x/\ln(x)$ (in other words, a random number x has a "probability" $1/\log(x)$ to be prime).



The first improvement on $x/\log x$ we consider is the *logarithmic integral function* $Li(x)$, defined to be the area under the curve of the function $1/\log u$ between 2 and x . Gauss arrived at this from the empirical fact that *the probability of finding a prime number at an integer value near a very large number x is almost exactly $1/\log x$.*

L'Hopital's rule can be used to show that the ratio of $x/\log x$ to $\int_2^x \frac{du}{\log u}$ tends to 1 as x approaches infinity. Thus we may use either expression as an approximation to $\pi(x)$ in the statement of the prime number theorem.



The prime number theorem states that

$$\pi(x) = Li(x) + O(x \exp(-a \sqrt{\log(x)})), \quad \text{for some positive constant } a,$$

where

$$Li(x) = \int_2^x \frac{dt}{\log(t)}.$$

also written as

$$Li(x) = \int_2^x \frac{dx}{\ln(x)}.$$

$$\pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \dots \approx Li(x)$$

or, equivalently,

$$\pi(x) \approx Li(x) - \frac{1}{2}Li(x^{1/2}) - \frac{1}{3}Li(x^{1/3}) - \dots$$

Thus $Li(x)$ is a good approximation of $\pi(x)$. The error term is in fact related to one of the most famous mathematical unsolved problem, namely the *Riemann hypothesis*. If the Riemann hypothesis is true, then it was proved in 1901 by von Koch that we have the higher estimate

$$\pi(x) = Li(x) + O(\sqrt{x} \log(x)).$$

In other words, the Riemann hypothesis says that $\text{Li}(x)$ is a very good approximation to $\pi(x)$.
 Example:

$$\text{Li}(10000) = 1246.137216 \quad \text{and if we define : } f(x) = \frac{x}{\ln(x)} \quad \text{then } f(10000) = 1085.736205$$

Chebyshev in 1850 introduced a logarithmic prime count function $\psi(x)$.

Example: The prime power less than 20 are 2, 4, 8, 16, 3, 9 and the prime numbers are 5, 7, 11, 13, 17, 19. The prime numbers are of the form p^1 . To calculate $\psi(20)$ the four powers of 2 must be given the weight $\ln 2$, the two powers of 3 the weight $\ln 3$ and all other primes their logarithm as power:

$$\psi(20) = 4 \cdot \ln 2 + 2 \cdot \ln 3 + \ln 5 + \ln 7 + \ln 11 + \ln 13 + \ln 17 + \ln 19 \approx 19.226$$

$\psi(x)$ can be approximated by x , so that

$$\lim_{x \rightarrow \infty} \frac{\psi(x) - x}{x} = 0$$

According to the Riemann hypothesis:

$$\psi(x) = x - \ln(2\pi) - \sum_{\rho} \frac{x^{\rho}}{\rho}$$

with ρ the zeros of the zeta function. (The last term states that each zero has to be calculated and subtracted and the results added.)

The (Riemann) zeta function

$$\zeta(s) = 1 + 1/2^s + 1/3^s + 1/4^s + \dots = \sum_{n=1}^{\infty} n^{-s}$$

with $s = x + iy$ a complex number. The Riemann hypothesis states that all zeros of the zeta function lie on the critical line $x = 1/2$.

Euler discovered that

$$1 + 1/2^s + 1/3^s + 1/4^s + \dots = \frac{2^s}{2^s - 1} \cdot \frac{3^s}{3^s - 1} \cdot \frac{5^s}{5^s - 1} \cdot \frac{7^s}{7^s - 1} \dots \quad \text{so that}$$

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

Euler discovered a formula for $\zeta(2k)$:

$$\zeta(2n) = (-1)^{n-1} \frac{(2\pi)^{2n}}{2(2n)!} B_{2n}.$$

giving $\zeta(2)=\pi^2/6$ (Basel problem) and $\zeta(4)=\pi^4/90$, $\zeta(6) = \pi^6/945$ etc. Riemann extended $\zeta(s)$ to all complex numbers (except the pole at $s=1$ with residue 1), where Euler's product still holds if the real part of $s > 1$. The zeta function is related to the prime numbers by Euler's product formula:

$$\zeta(s) = \prod_{p=\text{prime}} (1 - p^{-s})^{-1} = \frac{\Gamma(1-s)}{2\pi i} \int_{-\infty}^{+\infty} \frac{(-x)^s}{(e^x - 1)x} dx$$

The zeta function can also be written as:

$$\zeta(s) = \frac{1}{1-2^{1-s}} \eta(s)$$

with which $\zeta(s)$ is also defined for all z in the half-plane to the right of the line $x=0$, except in the pole $s=1$, where the formula does not hold.

The Dirichlet eta function is defined as:

$$\eta(s) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^s} \quad \eta(s) = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{x^{s-1}}{e^x + 1} dx.$$

$$= (1 - 2^{1-s}) \cdot \zeta(s) \quad \text{or}$$

$$\eta(s) = \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^n (-1)^k \binom{n}{k} \frac{1}{(k+1)^s}.$$

also

$$\eta(-s) = 2\pi^{-s-1} s \sin\left(\frac{\pi s}{2}\right) \Gamma(s) \eta(s+1).$$

Some values

$$\eta(0) = \frac{1}{2} \quad \eta(-1) = \frac{1}{4}; \quad \eta(1) = \ln 2 \quad ; \quad \eta(2) = \frac{\pi^2}{12}$$

$$\eta(1-k) = \frac{2^k - 1}{k} B_k.$$

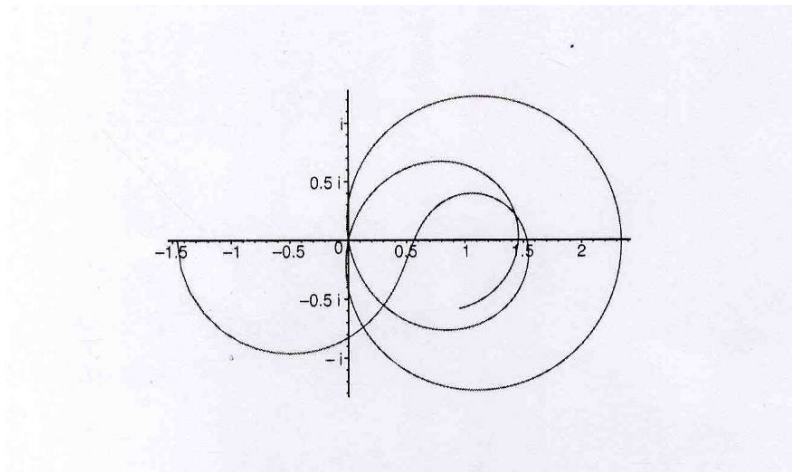
Riemann derived the functional relation the prime numbers by Euler's product formula:

$$\pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \pi^{-(1-s)/2} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s)$$

where the gamma function $\Gamma(s)$ is the extension of the factorial function : (with $\Gamma(n+1)=n!$ for all non-negative integers n):

$$\Gamma(s) = \int_0^{\infty} e^{-u} u^{s-1} du = \frac{1}{s} \prod_{n=1}^{\infty} \frac{e^{s/n}}{1 + s/n}$$

The integral form holds if the real part of s is greater than one, and the product form holds for all complex numbers s. The trivial zeros of the zeta function are at -2, -4, -6, while the nontrivial zeros of the zeta function lie on the line $x = 1/2$.



$\zeta(1/2 + iy)$ for $0 \leq y \leq 24$.

Mertens function

Square-free numbers in which all the factored prime numbers are different (e.g. $70=2 \times 5 \times 7$ is square free, while $75=2 \times 5 \times 5$ is not). A square free number is called P-even or prime even if it is a product of an even number of different prime numbers and is called P-odd if it is a product of an odd number of different primes (e.g. 70 is P-odd and $15 = 3 \times 5$ is P-even). Then the Mertens function $M(x)$ defined for all real numbers $x \geq 1$ is defined as:

$$M(x) = (\text{the number of P-even integers } \leq x) - (\text{the number of P-odd integers } \leq x)$$

e.g. $M(34) = 9 - 10 = -1$ because (the number of P-even integers $\leq x$) = 9 (being the numbers 6, 10, 14, 22, 6, 34, 15, 21 and 33) and (the number of P-odd integers $\leq x$) = 10 (being the numbers 2, 3, 7, 11, 13, 17, 23, 29, 31 and 30).

The Riemann hypothesis is equivalent to the following statement: for every $\epsilon > 0$ there exists a positive number C_ϵ such that:

$$|M(x)| = C_\epsilon x^{\frac{1}{2} + \epsilon}$$

Goldbach part 2

Let $p_n + q_n = 2N$, then $p_n < N$ and $q_n > N$.

Let $N - p_n = q_n - N = r_n$. (e.g. for take $p_n = 3$ and $q_n = 7$, $r_n = 2$.)

$\pi(N)$ is the number of primes less than or equal to N ; $\pi(N) \approx \frac{1}{2} \cdot \pi(2N)$

If $p_n + q_n$ need to be $2N$ then the number of possible combinations is $\frac{1}{2} \pi(2N)$.

In this prime series $p_i = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$ the gaps $G(p_i)$ are $\{2, 2, 4, 2, 4, 2, 4, 6, 2\}$

Suppose we take out 23 and 29 from the series then $p_i = \{3, 5, 7, 11, 13, 17, 19, 31\}$ and the gaps $G(p_i)$ are $\{2, 2, 4, 2, 4, 2, 12\}$. The $2N$ become: 8, 10, 12, 14, 16, 20, 22, 24, 26, 28, 30, 34, etc. The number $2N = 32$ is missing because the first and the last prime give 34 which is smaller than $17 + 19 = 36$. In order to add a new prime number to the series which will add a $2N$, the sum of last 2 primes added with 2 (the new $2N$) has to be greater than the combination of the new prime with the smallest prime.

So we have to prove that $p_i + p_{i-1} + 2 \geq p_{i+1} + p_0 (= p_i + 3)$.

with $p_{i+1} - p_i = G(p_{i+1})$ and $p_i - p_{i-1} = G(p_i)$

this relation can also be written as: $p_{i-1} \geq 1 + G(p_i)$.

From the prime number theorem we know that the average gap between primes near p_i is $\langle G \rangle \approx \ln(p_i)$, so p_{i-1} has to be larger than $1 + \ln(p_i)$ and because $p_i > p_{i-1}$ there must also hold that $p_i > 1 + \ln(p_i)$, which holds for all primes greater than 3 (starting with the prime number 5). This requirement is comprehensively satisfied by all of the prime numbers and gaps because of the sufficiently smooth nature of $\pi(N)$.

This is not a stringent proof but rather an argument of plausibility.

11. Primality tests

Trial division prime test

To test if a number n is prime divide by divide by all odd number up to $s = \sqrt{n}$ or by all of the primes less than the square root of n .

Divide by all odd numbers s up to $s = \sqrt{n}$. If

$n \equiv 0 \pmod{s}$ is true, then n is composite

else n is a prime.

For example, to show is 211 is prime, we just divide by 2, 3, 5, 7, 11, and 13 or more practical to divide by 2, 3 and 5; and then by all the numbers congruent to 1, 7, 11, 13, 17, 19, 23, and 29 modulo 30-- stopping when we reach the square root. This type of factorization is also called **wheel factorization** and requires more divisions (because some of the divisors will be composite), but does not require us to have a list of primes available.

Probabilistic prime test

Let p be a prime and b be an arbitrary integer. Then

$$b^p \equiv b \pmod{p}$$

If p does not divide b then

$$b^{p-1} \equiv 1 \pmod{p}$$

There are n such composite integer numbers for which

$$b^{n-1} \equiv 1 \pmod{n}$$

holds. In general if n is an odd composite number which is relative prime to b and satisfies the above congruence, then n is a pseudoprime for the base b . We speak of a Carmichael number if n is a pseudoprime for all bases to which they are relatively prime.

According to Fermat's Little Theorem, if n is a prime, then

$$b^{n-1} \equiv 1 \pmod{n}$$

If n is composite it is quite rare for the congruence to be satisfied for any b . For all prime factors q of $n-1$ there holds that

$$b^{(n-1)/q} \not\equiv 1 \pmod{n}$$

If $q=2$ and n is an odd prime number, then

* $b^{(n-1)/2} \equiv \pm 1 \pmod n$ for all integers b for which the greatest common divisor, $\gcd(b, n)$, equals 1;

** $b^{(n-1)/2} \equiv -1 \pmod n$ for at least one integer b .

Conversely, if n is an odd integer bigger than 1, for which * and ** hold, then n is prime.

Elliptic curve primality testing

We consider the elliptic curve $y^2 = ax^3 + bx + c$

If the discriminant $\Delta = -16(4a^3 + 27b^2)$ is nonzero then the curve is non-singular (the graph has no cusps, self-intersections, or isolated points) and has three distinct roots. .

Let $n \in \mathbb{N}$, $(6, N) = 1$, E_n is an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ and m, s are such integers that $s|m$. We assume that there is a point $P \in E_n$ such that $m \cdot P = O$ and $(m/q) \cdot P \neq O$ are valid for every prime factor q of s . Then for every prime divisor p of n the congruence

$E_n \equiv O \pmod s$ is true, and if

$$s > \left(\sqrt[4]{n} + 1\right)^2$$

Then n is a prime. (m and m/q are integers and $c \cdot P$ means c times repeated addition of point P).

AKS primality test

The test is based on the fact that from Fermat's little theorem for polynomials there follows that :

$$(x - a)^n \equiv (x^n - a) \pmod n$$

which is derived from Fermat's little theorem for polynomials in combination with the binomial theorem of Newton and

$$\binom{n}{k} \equiv 0 \pmod n \quad \text{for all } 0 < k < n \text{ if and only if } n \text{ is prime.}$$

In this form it works in exponential time. The AKS test uses the equivalence:

$$(x - a)^n \equiv (x^n - a) \pmod{n, x^r - 1}$$

which is:

$$(x-a)^n - (x^n - a) = n.f + (x^r - 1).g$$

for some polynomials f and g . This congruence can be checked in polynomial time. All primes satisfy this relation (choosing $g = 0$ in

$$(x-a)^n - (x^n - a) = n.f + (x^r - 1).g \quad \text{gives } (x-a)^n \equiv (x^n - a) \pmod{n}$$

, which holds for n prime), as well as some composite numbers. The proof of correctness for AKS consists of showing that there exists a suitably small r and suitably small set of integers A such that, if the congruence equation holds for all such a in A , then n must be prime.

1. Input: integer $n > 1$.
2. If $n = a^b$ for integers $a > 0$ and $b > 1$, output *composite*.
3. Find the smallest r such that $o_r(n) > \log^2(n)$.
4. If $1 < \text{greatest_common_divisor}(a, n) < n$ for some $a \leq r$, output *composite*.
5. If $n \leq r$, output *prime*.
6. For $a = 1$ to $\lfloor \sqrt{\varphi(r)} \log(n) \rfloor$ do
 if $(X+a)^n \not\equiv X^n + a \pmod{X^r - 1, n}$, output *composite*;
7. Output *prime*.

where $o_r(n)$ is the smallest number k such that $a^k \equiv 1 \pmod{r}$ (the multiplicative order of n modulo r), \log means the binary logarithm and $\varphi(r)$ is the Euler-phi totient function of r .

Fermat primality test

Fermat primes have the form :

$$F_p = 2^{(2^p)} + 1$$

where n is a nonnegative integer. The first few Fermat numbers are:

3, 5, 17, 257, 65537, 4294967297, ...

Factorizations of the first 6 Fermat numbers:

$$F_0 = 2^1 + 1 = 3 \text{ is prime}$$

$$F_1 = 2^2 + 1 = 5 \text{ is prime}$$

$$F_2 = 2^4 + 1 = 17 \text{ is prime}$$

$$F_3 = 2^8 + 1 = 257 \text{ is prime}$$

$$F_4 = 2^{16} + 1 = 65,537 \text{ is the largest known Fermat prime}$$

$$F_5 = 2^{32} + 1 = 4,294,967,297 \\ = 641 \times 6,700,417$$

$$F_6 = 2^{64} + 1 = 18,446,744,073,709,551,617$$

$$= 274,177 \times 67,280,421,310,721$$

According to Fermat's Little Theorem, if N is a prime, then

$$b^{N-1} \equiv 1 \pmod{N}$$

If N is composite it is quite rare for the congruence to be satisfied for any b . For all prime factors q of $N-1$ there holds that

$$b^{(N-1)/q} \not\equiv 1 \pmod{N}$$

Euler generalized Fermat's theorem by showing that for any integer N , prime or composite, there holds:

$$b^{\phi(N)} \equiv 1 \pmod{N}$$

for any integer b coprime to N , where $\phi(N)$ is Euler totient function, which represent the number of positive integers less than and coprime to N . If N is a prime then $\phi(N) = N-1$.

Example: we examine the residues \pmod{N} of the sequence

$$1 \quad b \quad b^2 \quad b^3 \quad b^4 \quad b^5 \quad \dots\dots\dots$$

Then it follows that $N-1$ must be a multiple of the fundamental period T , so that $N-1 = nT$ for some integer n . We know that $\phi(N)$ is less than or equal to $N-1$. If $T = N-1$, then $\phi(N) = N-1$, which is only the case if N is a prime. If we examine $b^{(N-1)/q}$ for every prime divisor q of $N-1$ we find that none of these values is congruent to 1 \pmod{N} , so that $\phi(N) = N-1$. This leads to Lucas primality criterion:

Lucas general primality test

If, for some integer b , the quantity $b^{(N-1)/q}$ is not congruent to 1 modulo N for any prime divisor q of $N-1$, then N is a prime.

Example: we take $n = 71$ than $n-1=70$ and the prime factors of 70 are 2, 5 and 7. We choose an arbitrary $a < n$, e.g. $a = 17$, then we calculate

$$17^{70} \equiv 1 \pmod{71}.$$

For all $a^{n-1} \equiv 1 \pmod{n}$, if and only if $\text{ord}(a) \mid (n-1)$, which means that the multiplicative order of 17 does not have to be 70 but a factor of 70 can also do. So we check 70 divided by its prime factors:

$$\begin{aligned}
17^{35} &\equiv 70 \not\equiv 1 \pmod{71} \\
17^{14} &\equiv 25 \not\equiv 1 \pmod{71} \\
17^{10} &\equiv 1 \equiv 1 \pmod{71}.
\end{aligned}$$

so that we still don't know if 71 is a prime number.

We now try $a = 11$.

$$11^{70} \equiv 1 \pmod{71}.$$

So we check 70 divided by its prime factors:

$$\begin{aligned}
11^{35} &\equiv 70 \not\equiv 1 \pmod{71} \\
11^{14} &\equiv 54 \not\equiv 1 \pmod{71} \\
11^{10} &\equiv 32 \not\equiv 1 \pmod{71}.
\end{aligned}$$

We see that the multiplicative order of 11 (mod 71) is equal to 70 and thus is 71 a prime number.

Pepin test

The Pepin test is used to test Fermat numbers $F_n = 2^{2^n} + 1$

Let $n \geq 1$. F_n is a prime number, if there holds $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$

The Fermat number $F_n = 2^{2^n} + 1$ where $n > 1$ is prime if and only if

$$5^{(F_n-1)/2} \equiv -1 \pmod{F_n} \quad \text{old version or}$$

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n} \quad \text{modern version}$$

Pepin had noted that the number 10 could be used instead of 5, while Proth noted that the number 3 could be used instead of 5, but offered no proof. Lucas stated that an arbitrary integer a could be used instead of 5 provided that the Jacobi symbol (a/F_n) has a value equal to -1 and in 1879 offered a proof.

Proof of the test : we assume that there holds: $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

Then, $3^{F_n-1} \equiv 1 \pmod{F_n}$, thus the multiplicative order of 3 modulo F_n divides

$F_n - 1 = 2^{2^n}$, a power of two. But the order does not divide $(F_n - 1) / 2$, and therefore it must be equal to $F_n - 1$. There are at least $F_n - 1$ numbers below F_n coprime to F_n , and this only occurs if F_n is prime. Now suppose that F_n is prime. By Euler's criterion,

$3^{(F_n - 1)/2} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}$, where $\left(\frac{3}{F_n}\right)$ is the Legendre symbol. By using law of reciprocity $(3/F_n) \cdot (F_n/3) = 1$ and squaring repeatedly, we find that $2^{2^n} \equiv 1 \pmod{3}$, thus, $F_n \equiv 2 \pmod{3}$, and $\left(\frac{F_n}{3}\right) = -1$. If $F_n \equiv 1 \pmod{4}$, we may conclude from the law of quadratic reciprocity. $\left(\frac{3}{F_n}\right) = -1$.

Example: We show that $F_3 = 2^8 + 1$ is a prime number. We calculate $3^{128} \pmod{257}$:

 $3^8 = 6561 \equiv -121 \pmod{257}$

 $3^{16} \equiv (-121)^2 \equiv -8 \pmod{257}$

 $3^{32} \equiv (-8)^2 \equiv 64 \pmod{257}$

 $3^{64} \equiv (64)^2 \equiv -16 \pmod{257}$

 $3^{128} \equiv (-16)^2 = 256 \equiv -1 \pmod{257}$

Lucas–Lehmer test for Mersenne primes

A Mersenne prime number M_p is given by:

$$M_p = 2^p - 1$$

Examples are: $M_7 = 127$; $M_{19} = 524287$;

The Lucas–Lehmer test is a primality test for Mersenne numbers: $M_p = 2^p - 1$ where p is an odd prime. (because p is exponentially smaller than M_p , we can use a simple algorithm like trial division for establishing its primality). Define a sequence $\{s_i\}$ for all $i \geq 0$ by

$$s_i = \begin{cases} 4 & \text{if } i = 0; \\ s_{i-1}^2 - 2 & \text{otherwise.} \end{cases}$$

The first few terms of this sequence are 4, 14, 194, 37634, Then M_p is prime iff

$$s_{p-2} \equiv 0 \pmod{M_p}$$

Else M_p is a composite number. The number $s_{p-2} \pmod{M_p}$ is called the **Lucas–Lehmer residue** of p . (Some authors equivalently set $s_1 = 4$ and test $s_{p-1} \pmod{M_p}$).

Example. We take: $M_5 = 2^5 - 1 = 31$

$$\begin{aligned}
 s_0 &\equiv 4 \pmod{31} \\
 s_1 &\equiv 4^2 - 2 \equiv 14 \pmod{31}
 \end{aligned}$$

$$s_2 \equiv 14^2 - 2 \equiv 8 \pmod{31}$$

$$s_3 \equiv 8^2 - 2 \equiv 0 \pmod{31}$$

$S_3 = 0$ so 31 is a prime number.

Proof of the test

Let $\omega=2+\sqrt{3}$ and $\omega^*=2-\sqrt{3}$. Then by induction it can be verified that $s_i = \omega^{2^i} + \omega^{*2^i}$ for all i .

$$s_0 = \omega^{2^0} + \omega^{*2^0} = 2 + \sqrt{3} + 2 - \sqrt{3} = 4$$

$$s_n = (\omega^{2^{n-1}} + \omega^{*2^{n-1}})^2 - 2 = \omega^{2^n} + \omega^{*2^n} + 2(\omega\omega^*)2^{n-1} - 2 = \omega^{2^n} + \omega^{*2^n}$$

Proth-test

A **Sierpinski** or **Sierpiński number** is an odd natural number k such that all integers of the form $k2^n + 1$ are composite, for all natural numbers n ; in 1960, W. Sierpiński proved that there are infinitely many odd integers k which have this property. Numbers in this set with odd k and $k < 2^n$ are called Proth numbers.

The Proth-test is used to test the Proth-numbers

$$P = k \cdot 2^n + 1$$

where n is an integer, k is an odd integer, and the condition $2^n > k$ must hold because else odd number > 1 would be an Proth number. If the Proth number is prime it is called a Proth prime.

The first Proth-number are:

$$P_0 = 2^1 + 1 = 3$$

$$P_1 = 2^2 + 1 = 5$$

$$P_2 = 2^3 + 1 = 9$$

$$P_3 = 3 \times 2^2 + 1 = 13$$

$$P_4 = 2^4 + 1 = 17$$

$$P_5 = 3 \times 2^3 + 1 = 25$$

$$P_6 = 2^5 + 1 = 33$$

The first Proth-primes are:

3, 5, 13, 17, 41, 97, 113, 193, 241, 257, 353, 449, 577, 641, 673, 769, 929, 1153, 1217, 1409, 1601, 2113, 2689, 2753, 3137, 3329, 3457, 4481, 4993, 6529, 7297, 7681, 7937, 9473, 9601, 9857.

A new Primality test for general primes

I discovered that the the P_n series, (see section on continued fractions), as given by

3, 7, 18, 47, 123, 322, 843 2207, 5778,

$$P_0 = 2$$

$$P_1 = 3$$

$$P_i = 3 * P_{i-1} - P_{i-2}$$

can be used to test whether or not the odd numbers 3, 5, 7, 9, 11, 13, .. are prime.

We define the sequence s_i for all $i > 0$ as $s_i = \sum_{n=1}^i P_n$

To test whether a number n is being prime:

Then n is prime iff

$$s_i \equiv 0 \pmod{n}$$

examples:

$$s_1 = 3 \equiv 0 \pmod{3}$$

$$s_2 = 10 \equiv 0 \pmod{5}$$

$$s_3 = 28 \equiv 0 \pmod{7}$$

$$s_4 = 75 \not\equiv 0 \pmod{9}$$

$$s_5 = 198 \equiv 0 \pmod{11}$$

$$s_6 = 520 \equiv 0 \pmod{13}$$

$$s_7 = 1363 \not\equiv 0 \pmod{15}$$

$$s_8 = 3570 \equiv 0 \pmod{17}$$

$$s_9 = 9348 \equiv 0 \pmod{19}$$

$$s_{10} = 24475 \not\equiv 0 \pmod{21}$$

$$s_{11} = 64078 \equiv 0 \pmod{23}$$

$$s_{12} = 167760 \not\equiv 0 \pmod{25}$$

etc

or

$$s_i = 3 * s_{i-1} + s_{i-2} + 1$$

A sketch of proof for the necessity of the criterion as suggested by Wolfgang Rump would be the following:

Firstly, one should interpolate the sequence s_n : Instead of 3,10,28,75,... take 0,2,3,6,10,17,28,... which is just the Lucas sequence L_n minus 1. Now it is in fact known that every prime p divides L_{p-1} , which shows that the necessity of the criterion is true.

However, the converse (that the divisibility is impossible unless p is a prime) has shown to be false: The non-prime 705 divides $s_{352}=L_{705} - 1$.

Appendix

to be continued