

General Public

What are prime numbers?

A prime number is an integer that is only divisible by one and itself. One is not a prime number. Two is the only even prime; all other primes are odd.

What is a composite number?

An integer which is not prime must be composite. The only exception is the number one. Every composite can be represented as a finite product of primes. For example, $4 = 2 \times 2$ and $6 = 2 \times 3$.

What are semiprimes?

Semiprimes are composite numbers which consist of only two prime factors. Such factors have the same number of decimal digits but are numerically different. An example of a semiprime is the number 71501. It is the product of 127 and 563 where each prime factor has three decimal digits.

What is number theory?

Number theory is a branch of mathematics that deals with the integers and their properties. Prime numbers are a major concern of number theory.

What is elementary number theory?

Elementary number theory is an area of mathematics that uses principles from arithmetic, geometry and algebra to solve problems in number theory.

What is theoretical physics?

The objective of theoretical physics is to build models that represent reality. Such models are always based on some form of mathematics.

What is cryptography?

Cryptography is the science behind making and breaking codes. If you send someone a secret message consisting of five sequences of numbers, but it actually means “meet me at central park” such is an example of cryptography since each number corresponds to a specific letter of the English alphabet.

What is meant by “pattern” in mathematics?

Mathematics is usually defined as the science of patterns. For example, the even integers follow a pattern since they start at zero and continue forever by increments of two.

General Public

What is meant by “random distribution”?

The concept of distribution is usually associated with that of division. For example, if we hear someone comment that the inheritance was evenly distributed to her three sons, it means, that each of them got an equal share. In mathematical terms, we can translate this to a simple equation such as $S = I \div 3$ where S is the amount inherited by each son and I stands for total inheritance. On the other hand, the term “random distribution” is applied to any phenomena (real or abstract) where its mathematical nature is unknown. In other words, such occurrence does not follow any mathematical equation. During more than two thousand years, the location of the prime numbers among the positive integers was always considered as randomly distributed, that is, lacking order or pattern. Today, we know that the distribution of prime numbers obeys a fractal binary pattern.

What is experimental mathematics?

Experimental mathematics consists in using computers to help solve mathematical problems. For example, many computers are used in the search for Mersenne primes which are currently the largest known primes.

What are Mersenne primes?

Mersenne primes are of the form $2^p - 1$ where p is a prime. For example, the first such prime is $2^2 - 1 = 3$ where $p = 2$. Presently, the largest known prime is $2^{43112609} - 1$ which is a Mersenne prime. Such prime is really gigantic since it consists of 12,978,189 decimal digits.

What is a conjecture?

A conjecture is a mathematical statement believed to be true but which has not been proved. One of the most famous conjectures in number theory is known as the Goldbach conjecture.

What is the Goldbach conjecture?

The Goldbach conjecture was defined by the Prussian mathematician Christian Goldbach (1690 - 1764) and states that every even number greater than two is the sum of two primes. For example, $4 = 2 + 2$ and $8 = 3 + 5$. Try it with another number!

What is computational number theory?

Computational number theory implies using computers to help solve problems in number theory. Such requires the development of efficient algorithms for each specific task.

What is an algorithm?

An algorithm is a finite sequence of logical steps in order to achieve a precise objective. An example is the RSA algorithm.

General Public

What does RSA stand for?

RSA stands for Rivest, Shamir and Adleman. In 1978 at the Massachusetts Institute of Technology, they invented an algorithm for public-key cryptography.

What is public-key cryptography?

Public-key cryptography is a technique to transmit and receive confidential information in a secure manner among computers on the Internet. This method is widely used since it has resisted to all sorts of attacks from both academia and the computer industry.

What is cryptanalysis?

Cryptanalysis is the art and science of breaking codes. For example, if someone finds a practical solution to the integer factorization problem such would render RSA obsolete.

What is the integer factorization problem?

The integer factorization problem consists in finding the prime factors of a given composite number. For example, given 15 it is trivial to find the prime factors 3 and 5 but for very large numbers it is extremely difficult to obtain such factors. In fact, the RSA algorithm and, consequently, an entire industry has been created based upon this assumption.

What is the Collatz problem?

The Collatz problem was formulated in 1937 by the German mathematician Lothar Collatz (1910 – 1990) and is defined as follows: take any positive integer; if it is odd, multiply it by three and add one; if the number you chose is even, divide it by two. Collatz stated that if we continuously repeat this procedure it must always terminate in one for every positive integer. For example, if you start with the number 3, the corresponding sequence is $3 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1$, as expected. Try it with another number!

What is a primality test?

A primality test is a mathematical procedure to verify if a number is prime or not. The most ancient primality test invented by the Chinese states that if p is prime then $2^p - 2$ is divisible by p . For example, if $p = 3$ then $2^3 - 2 = 8 - 2 = 6$ which is divisible by 3 and, consequently, three is a prime. Unfortunately, such test does not work with many numbers.

What are Carmichael numbers?

Carmichael numbers in honor of the American mathematician Robert D. Carmichael (1879 – 1967) are positive integers that satisfy a specific primality test but are not prime. The first Carmichael number is 561 which is composite because $561 = 3 \times 11 \times 17$.

General Public

What are twin primes?

Twin primes have the form $(p, p + 2)$ where p is a prime. An example of a twin prime is $(5, 7)$ where $p = 5$.

What are Gaussian primes?

Gaussian primes are primes such as 7 that cannot be expressed as the sum of two squares. They have the general form $4n + 3$ where n is a positive integer. For example, $7 = 4n + 3$ where $n = 1$.

What are ordinary primes?

Ordinary primes are primes that can be expressed as the sum of two squares. For example, 2 and 5 are ordinary primes since $2 = 1^2 + 1^2$ and $5 = 1^2 + 2^2$, respectively.

What is meant by “formal proof” in mathematics?

Formal proof is a valid demonstration of a specific mathematical statement through the use of logic and reasoning.

What is *Mathematica*?

Mathematica is a computational software program created and developed by Wolfram Research Inc. since 1988. It is also a programming language and much more.