What Are Prime Factorisation

== Definition in number theory == 625480025b The first enormous distributed factorisation was RSA-129, a 129-digit challenge number described in the Scientific American article of 1977 which first popularised the RSA cryptosystem. It was factorised between September 1993 and April 1994, using MPQS, with relations contributed by about 600 people through the internet, and the final stages of the calculation performed on a MasPar supercomputer at Bell Labs. 625480025b

Factorization of polynomials 163–170 (2011). Polynomial factorization is one of the fundamental components of computer algebra systems. C. "On the factorisation of polynomials in a finite number of steps". ; Shepherdson, J. pp. Fröhlich, A. Mathematische Zeitschrift In mathematics and computer algebra, factorization of polynomials or polynomial factorization expresses a polynomial with coefficients in a given field or in the integers as the product of irreducible factors with coefficients in the same domain. (1955) 625480025b

× 625480025b K 625480025b In number theory, a strong prime is a prime number that is greater than the arithmetic mean of the nearest prime above and below (in other words, it is closer to the following than to the preceding prime). Or to put it algebraically, writing the sequence of prime numbers as (p1, p2, p3, ...) = (2, 3, 5, ...), pn is a strong prime if pn > pn − 1 + pn + 1/2. For example, 17 is the seventh prime: the sixth and eighth primes, 13 and 19, add up to 32, and half that is 16; 17 is greater than 16, so 17 is a strong prime. 625480025b 1.9 625480025b Number theory is one of the oldest branches of mathematics alongside geometry. One quirk of number theory is that it deals with statements that are simple to understand but are very difficult to solve. Examples of this are Fermat's Last Theorem, which was proved 358 years after the original formulation, and Goldbach's conjecture, which remains... 625480025b

Integer factorization records The difficulty depends on both the size and form of the number and its prime factors; it is currently very difficult to factorize large semiprimes (and, indeed, most numbers that have no small factors). numbers that have no small factors). The first enormous distributed factorisation was RSA-129, a 129-digit challenge number described in the Scientific Integer factorization is the process of determining which prime numbers divide a given positive integer. Doing this quickly has applications in cryptography 625480025b

Anton Felkel and Carl Hindenburg (independently of Felkel) build and use mechanical prime sieves based on the stencil method 625480025b

Strong prime The definitions of strong primes are different in cryptography and number theory. However, strong primes do not protect against modulus factorisation using newer algorithms such as Lenstra elliptic curve In mathematics, a strong prime is a prime number with certain special properties. RSA keys for digital signatures 625480025b

Ideal class group to complete proofs in the general case of Fermat's Last Theorem by factorisation using the roots of unity was for a very good reason: a failure of unique In mathematics, the ideal class group (or class group) of an algebraic number field 625480025b

Timeline of computational mathematics Lawrence's "Factorisation of numbers" is republished in French, sparking efforts to build a mechanical prime sieve. paper "Factorisation of numbers". This is a timeline of key developments in computational mathematics 625480025b

In January 2002, it was announced the factorisation of a 158-digit... 625480025b

Number theory Number theorists study prime numbers as well as the properties of mathematical objects constructed from integers (for example, rational numbers), or defined as generalizations of the integers (for example, algebraic integers). prime. What Number theory is a branch of mathematics devoted primarily to the study of the integers and arithmetic functions. (this is just another way of asking how many primes there are between one and a million). How many prime divisors will n have on average 625480025b

< 625480025b

Grimm's conjecture N. (1975). "On Grimm's problem relating to factorisation of a block of consecutive integers". ; Tijdeman, R. Shorey, T. It was first proposed by Carl Albert Grimm in 1969. Journal für die reine und angewandte In mathematics, specifically in number theory, Grimm's conjecture states that, for every set of consecutive composite numbers, there is an equally sized set of prime numbers, and a bijection that maps each composite in the former set to a prime in the latter set that it is divisible by 625480025b

The existence of this algorithm leads to the concept of safe primes, being primes for which p − 1 is two times a Sophie Germain prime q and thus minimally smooth. These primes are sometimes construed as "safe for cryptographic purposes", but they might be unsafe — in current recommendations for cryptographic strong primes (e.g. ANSI X9.31), it is necessary but not sufficient that p − 1 has at least one large prime factor. Most sufficiently large primes are strong; if a prime used for cryptographic purposes turns out to be non-strong, it is much more likely to be through malice than through an accident of random number... 625480025b

Pollard's p − 1 algorithm The factors it finds are ones for which the number preceding the factor, p − 1 Pollard's p − 1 algorithm is a number theoretic integer factorization algorithm, invented by John Pollard in 1974. It is a special-purpose algorithm, meaning that it is only suitable for integers with specific types of factors; it is the simplest example of an algebraic-group factorisation algorithm. it is the simplest example of an algebraic-group factorisation algorithm 625480025b

== Numbers of a general form == 625480025b Integers can be considered either in themselves or as solutions to equations (Diophantine geometry). Questions in number theory can often be understood through the study of analytical objects, such as the Riemann zeta function, that encode properties of the integers, primes or other number-theoretic objects in some fashion (analytic number theory). One may also study real numbers in relation to rational numbers, as for instance how irrational numbers can be approximated by fractions (Diophantine approximation). 625480025b The first few strong primes are 625480025b n 625480025b Between January and August 1999, RSA-155, a 155-digit challenge number prepared by the RSA company, was factorised using GNFS with relations again contributed by a large group, and the final stages of the calculation performed in just over nine days on the Cray C916 supercomputer at the SARA Amsterdam Academic Computer Center. 625480025b

Pierpont prime There are few restrictions from algebraic factorisations on the Pierpont primes, so there are no requirements like the Mersenne prime condition that In number theory, a Pierpont prime is a prime number of the form. 10100 625480025b

When the long-known finite step algorithms were first put on computers, they turned out to be highly inefficient. The fact that almost any uni- or multivariate polynomial of degree up to 100 and with coefficients of a moderate size (up to 100 bits) can be factored by modern algorithms in a few minutes of computer time indicates how successfully this problem has been attacked during the past fifteen years. (Erich Kaltofen, 1982) 625480025b The first polynomial factorization algorithm was published by Theodor von Schubert in 1793. Leopold Kronecker rediscovered Schubert's algorithm in 1882 and extended it to multivariate polynomials and coefficients in an algebraic extension. But most of the knowledge on this topic is not older than circa 1965 and

the first computer algebra systems: 625480025b 2 625480025b == 18th century == 625480025b == The model == 625480025b The factors it finds are ones for which the number preceding the factor, p − 1, is powersmooth; the essential observation is that, by working in the multiplicative group modulo a composite number N, we are also working in the multiplicative groups modulo all of N's factors. 625480025b Though still unproven, the conjecture has been verified for all 625480025b

Primon gas It is a quantum field theory of a set of non-interacting particles, the primons; it is called a gas or a free model because the particles are non-interacting. where log {\displaystyle {\textbf {log}}} is an algorithm for integer factorisation, analogous to the discrete logarithm, and F {\displaystyle F} is the In mathematical physics, the primon gas or Riemann gas discovered by Bernard Julia is a model illustrating correspondences between number theory and methods in quantum field theory, statistical mechanics and dynamical systems such as the Lee–Yang theorem. The idea of the primon gas was independently discovered by Donald Spector. Later works by Ioannis Bakas and Mark Bowick, and Spector explored the connection of such systems to string theory 625480025b