PlanetMath.org

Math for the people, by the people.

"Integer Factorization"

John Smith

integer factorization (Definition)

Given an integer n, its *integer factorization* (or *prime factorization*) consists of the primes p_i which multiplied together give n as a result. To put it algebraically,

$$n=\prod_{i=1}^{\omega(n)} p_i^{a_i},$$

with each p_i distinct, all $a_i>0$ but not necessarily distinct, and $\omega(n)$ being the value of the number of distinct prime factors function. Theoretically, an integer is a product of all the prime numbers,

$$n=\prod_{i=1}^{\infty} p_i^{a_i},$$

with many $a_i=0$.

For example, the factorization of 32851 is $7\times 13\times 19\times 19$, more usually expressed as $7\times 13\times 19^2$. Because of the commutative propertyof multiplication, it does not matter in what order the prime factors are stated in, but it is customary to give them in ascending order, and to groupthem together by the use of exponents.

The factorization of a positive integer is unique (this is the fundamental theorem of arithmetic). For a negative number $n<0$ one could take the factorization of $|n|$ and randomly give negative signs to one (or any odd number) of the prime factors. Alternatively, the factorization can be given as $-1\cdot p_1^{a_1}\cdot\cdots$ (this is what Mathematica opts for).

The term ``factorization'' is often used to refer to the actual process of determining the prime factors. There are several algorithms to choose from, with trial division being the simplest to implement.

"integer factorization" is owned by PrimeFan.

(view preamble | get metadata)

View style:

Other names: prime factorization

This object's parent.

Log in to rate this entry.
(view current ratings)

Attachments:

trial division (Algorithm) by CompositeFan

Fermat method (Algorithm) by PrimeFan

$p-1$

Pollard's algorithm (Algorithm) by PrimeFan

ρ

Pollard's algorithm (Algorithm) by PrimeFan

table of integer factorizations

$0 < n < 1001$

for (Data Structure) by PrimeFan

prime signature (Definition) by PrimeFan

Cross-references: trial division, algorithms, term, Mathematica, odd number, negative, negative number, fundamental theorem of arithmetic, positive, exponents, group, prime factors, order, multiplication, property, commutative, product, number of distinct prime factors function, primes, integer
There are 37 references to this entry.

This is version 5 of integer factorization, born on 2007-02-02, modified 2009-03-21.
Object id is 8857, canonical name is IntegerFactorization.
Accessed 5732 times total.

Classification:
AMS MSC: 11A41 (Number theory :: Elementary number theory :: Primes)

Pending Errata and Addenda

None.

[View all 2]

Discussion

Style: Expand: Order:

forum policy

Contrasting and comparing PrimeFan, CompositeFan by Mravinci on 2007-02-22 16:19:39

I just noticed that CompositeFan attached her entry on trial division to the entry on composite numbers, while PrimeFan attached his entry on the Fermat method to the entry on primes. (I think attaching to integer factorization would make more sense).

There are other interesting similarities and differences between the two: PrimeFan will contribute something to Wikipedia first and then PlanetMath, while CompositeFan will contribute something to PlanetMath first and then Wikipedia. PrimeFan is an old man who served in the Navy in the pointful Second World War, while CompositeFan is a young woman who served in the Navy in the pointless First Gulf War. PrimeFan hates classical music but is interested in opus sequences, while CompositeFan loves classical music but couldn't care less for opus sequences. etc.