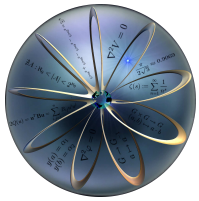

planetmath.org

Math for the people, by the people.

multiplicative order of an integer modulo m

Canonical name	MultiplicativeOrderOfAnIntegerModuloM
Date of creation	2013-03-22 16:20:38
Last modified on	2013-03-22 16:20:38
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	5
Author	alozano (2414)
Entry type	Definition
Classification	msc 13-00
Classification	msc 13M05
Classification	msc 11-00
Synonym	multiplicative order
Related topic	PrimitiveRoot
Related topic	PrimeResidueClass

Definition. *Let $m > 1$ be an integer and let a be another integer relatively prime to m. The* `http://planetmath.org/OrderGroup`*order of a modulo m (or the multiplicative order of $a \mod m$) is the smallest positive integer n such that $a^n \equiv 1 \mod m$. The order is sometimes denoted by $\operatorname{ord} a$ or $\operatorname{ord}_m a$.*

Remarks. Several remarks are in order:

1. Notice that if $\gcd(a, m) = 1$ then a belong to the units $(\mathbb{Z}/m\mathbb{Z})^\times$ of $\mathbb{Z}/m\mathbb{Z}$. The units $(\mathbb{Z}/m\mathbb{Z})^\times$ form a group with respect to multiplication, and the number of elements in the subgroup generated by a (and its powers) is the order of the integer a modulo m.

2. By Euler's theorem, $a^{\phi(m)} \equiv 1 \mod m$, therefore the order of a is less or equal to $\phi(m)$ (here ϕ is the Euler phi function).

3. The order of a modulo m is precisely $\phi(m)$ if and only if a is a primitive root for the integer m.