prime residue class

Canonical name	PrimeResidueClass
Date of creation	2013-03-22 15:43:12
Last modified on	2013-03-22 15:43:12
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	18
Author	pahio (2872)
Entry type	Definition
Classification	msc 20K01
Classification	msc 13M99
Classification	msc 11A07
Synonym	prime class
Related topic	MultiplicativeOrderOfAnIntegerModuloM
Related topic	NonZeroDivisorsOfFiniteRing
Related topic	GroupOfUnits
Related topic	PrimitiveRoot
Related topic	ResidueSystems
Related topic	Klein4Group
Related topic	EulerPhifunction
Related topic	SummatoryFunctionOfArithmeticFunction
Defines	residue class group

Let m be a positive integer. There are m residue classes $a+m\mathbb{Z}$ modulo m. Such of them which have

$$\gcd(a,\, m) \;=\; 1,$$

are called the *prime residue classes* or *prime classes modulo* m, and they form an Abelian group with respect to the multiplication

$$(a+m\mathbb{Z})\cdot(b+m\mathbb{Z}) \;:=\; ab+m\mathbb{Z}.$$

This group is called the *residue class group modulo* m. Its order is $\varphi(m)$, where φ means Euler's totient function. For example, the prime classes modulo 8 (i.e. $1+8\mathbb{Z}$, $3+8\mathbb{Z}$, $5+8\mathbb{Z}$, $7+8\mathbb{Z}$) form a group isomorphic to the Klein 4-group.

The prime classes are the units of the residue class ring $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ consisting of all residue classes modulo m.

Analogically, in the http://planetmath.org/ExamplesOfRingOfIntegersOfANumberFieldrin R of integers of any algebraic number field, there are the residue classes and the prime residue classes modulo an ideal $\mathfrak{a}$ of R. The number of all residue classes is $\mathrm{N}(\mathfrak{a})$ and the number of the prime classes is also denoted by $\varphi(\mathfrak{a})$. It may be proved that

$$\varphi(\mathfrak{a}) \;=\; \mathrm{N}(\mathfrak{a})\prod_{\mathfrak{p}|\mathfrak{a}}\left(1-\frac{1}{\mathrm{N}(\mathfrak{p})}\right);$$

N is the absolute norm of ideal and $\mathfrak{p}$ runs all distinct prime ideals dividing $\mathfrak{a}$ (cf. the first formula in the entry "http://planetmath.org/EulerPhiFunctionEuler phi function"). Moreover, one has the result

$$\alpha^{\varphi(\mathfrak{a})} \;\equiv\; 1 \pmod{\mathfrak{a}}$$

for $((\alpha),\, \mathfrak{a}) = (1)$, generalising the http://planetmath.org/EulerFermatTheoremEuler–Fermat theorem.