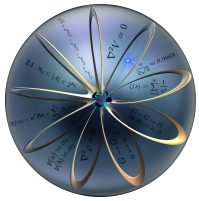

planetmath.org

Math for the people, by the people.

Schinzel's theorem

Canonical name	SchinzelsTheorem
Date of creation	2013-03-22 12:03:42
Last modified on	2013-03-22 12:03:42
Owner	alozano (2414)
Last modified by	alozano (2414)
Numerical id	10
Author	alozano (2414)
Entry type	Theorem
Classification	msc 20K01

Definition 1. *Let A and B be integers such that $(A, B) = 1$ with $AB \neq \pm 1$. A prime p is called a* primitive divisor *of $A^n - B^n$ if p divides $A^n - B^n$ but $A^m - B^m$ is not divisible by p for all positive integers m that are less than n.*

Or, more generally:

Definition 2. *Let A and B be algebraic integers in a number field K such that $(A, B) = 1$ and A/B is not a root of unity. A prime ideal $\wp$ of K is called a* primitive divisor *of $A^n - B^n$ if $\wp | A^n - B^n$ but $\wp \nmid A^m - B^m$ for all positive integers m that are less than n.*

The following theorem is due to A. Schinzel (see [**?**]):

Theorem. *Let A and B be as before. There is an effectively computable constant n_0, depending only on the degree of the algebraic number A/B, such that $A^n - B^n$ has a primitive divisor for all $n > n_0$.*

By putting $B = 1$ we obtain the following corollary:

Corollary. *Let $A \neq 0, \pm 1$ be an integer. There exists a number n_0 such that $A^n - 1$ has a primitive divisor for all $n > n_0$. In particular, for all but finitely many integers n, there is a prime p such that the multiplicative order of A modulo p is exactly n.*

References

[1] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II. J. Reine Angew. Math. 268/269 (1974), 27–33.