Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 7, Number 3 (2011), pp. 255-256

http://www.ripublication.com/gjpam.htm

On Divisors of a^m+1

Venkatesh Sripad

Department of Mathematics, ACE Engineering College
Ankushapur (V), Ghatkesar, R.R.District, Andhra Pradesh
Email: vanisri1978@gmail.com

Abstract

Can we find infinite number of primes which do not divide a^m+1?

In this paper we propose to answer the following question
Can we find infinite number of primes which do not divide a^m+1?
In what follows, p stands for odd prime and all the congruence's are mod p
Before proving the main theorem we prove the following two lemma's

Lemma 1: $a^x \equiv -1$ does not possess a solution whenever $a^m \equiv 1$ where m is odd.

Proof: Suppose assume the contrary, then

$$a^n \equiv -1 \tag{1}$$

$$a^{2n} \equiv 1$$

Therefore we have

$$a^d \equiv 1 \tag{2}$$

where $d = (2n, m)$. It clearly follows that $d \mid n$, so let $n = kd$ and from (2) we get

$$a^n \equiv 1 \tag{3}$$

From (1) & (3) we have $2 \equiv 0$ which is absurd.

Lemma 2: If p is of the form $4aq-1$ then a is a quadratic residue of p

Proof: Let $a = 2^x y$, where y is odd

let $y = 4r - 1$,then $\left(y\middle| p\right)\left(p\middle| y\right) = (-1)^{\frac{(p-1)(y-1)}{4}}$
$= (-1)^{(2aq-1)(2r-1)} = -1$

so that $\left(y\middle| p\right) = \frac{-1}{\left(p\middle| y\right)} = \frac{-1}{-1} = 1$

Note that here $\left(p\middle| y\right) = \left(-1\middle| y\right)$, since $y|a$ we have $p \equiv -1 (\text{mod } y)$

Let $y = 4r + 1$,then $\left(y\middle| p\right)\left(p\middle| y\right) = (-1)^{\frac{(p-1)(y-1)}{4}}$
$= (-1)^{\frac{(4r)(4am-2)}{4}} = 1$

so that $\left(y\middle| p\right) = \frac{1}{\left(p\middle| y\right)} = \frac{1}{\left(-1\middle| y\right)} = \frac{1}{1} = 1$

If a is even, $p = 8r - 1$, then $\left(2^x\middle| p\right)\left(y\middle| p\right) = 1.1 = 1$

Thus the lemma is proved

Theorem: A prime of the form $4aq - 1$ does not divide $a^m + 1$

Proof: Let $p = 4aq - 1$, then by lemma 2, $\left(a\middle| p\right) = 1$, by Euler's criterion

$\left(a\middle| p\right) \equiv a^{\frac{p-1}{2}}$ this in other words says
$1 \equiv a^{2aq-1}$

so by lemma 1, $a^x \equiv -1$ possesses no solution thereby proving the theorem.

In particular for $a = 2$, a prime number of the form $8q - 1$ does not divide $2^m + 1$ for every m

References

[1] Elementary Number Theory - David M Burton
[2] Analytical Number Theory – Tom M Apostol