CONGRUENCES MODULO PRIMES OF THE FORM 10N+1

Nasri Cheaito
Department of Pure Mathematics, Faculty of Sciences I, Lebanese University, Beirut, Lebanon
Mar.cheaito@hotmail.com

(Received 5 January 2005 - Accepted 26 November 2005)

ABSTRACT

The equation $x^n+y^n+z^n=0$ had been shown to be impossible in $\mathbb{Z}$-{0}. This result is known as Fermat's Last Theorem. This paper shows that the above equation is also impossible in $\mathbb{Z}/p\mathbb{Z}$-{0}, where p is a prime of the form p=10n+1.

Keywords: prime, equation, congruence, modulo

INTRODUCTION

The end of the second thousand had witnessed the proof of Fermat's Last Theorem (Edwards, 1977). This proof was searched by mathematicians during hundreds of years. Thousands of important articles were written in this subject. In this work we look for a generalization of Fermat's Last Theorem to congruences modulo primes, that is, given a prime p, does the equation

$$x^n+y^n+z^n=0$$

have solution in $\mathbb{Z}/p\mathbb{Z}$-{0}, for every n ? The answer is positive if p=3, for take x=y=z=1. But if p≠3, the answer seems to be negative, for if $p=2^s n+1$ is prime with 1≤s≤4 and n>2, then the equation $x^n+y^n+z^n=0$ has no solution in $\mathbb{Z}/p\mathbb{Z}$-{0}, by Theorem A' (Cheaito, 2001). In other words if $p=2^s n+1$ is prime with 1≤s≤4, n>2 and if x, y and z are integers such that $x^n+y^n+z^n\equiv 0 \pmod p$, then p divides one of x, y and z.

Thus as for n=5, we have that 2n+1=11 and $2^3 n+1=41$ are prime, we get that the equation $x^5+y^5+z^5=0$ is impossible in $\mathbb{Z}/11\mathbb{Z}$-{0} and in $\mathbb{Z}/41\mathbb{Z}$-{0}, that is if x, y and z are integers such that $x^5+y^5+z^5\equiv 0 \pmod{11}$, then 11 divides one of x, y and z and also if $x^5+y^5+z^5\equiv 0 \pmod{41}$, then 41 divides one of x, y and z.

In this paper we shall show

Theorem A: Let n be an odd number ≥5. If p=10n+1 is prime and if x, y and z are integers such that $x^n+y^n+z^n\equiv 0 \pmod p$, then p divides one of x, y and z. ∎

As a corollary to Theorem A we state the following

Corollary 1: If n is an odd number ≥5, and if p=10n+1 is prime, then the equation

$$x^n + y^n + z^n = 0$$

is impossible in $\mathbb{Z}/p\mathbb{Z}-\{0\}$. ∎

The proof of Theorem A is an immediate consequence of the following theorem:

Theorem 1: Let n be an odd number ≥5. If p=10n+1 is prime and

$$u+v+w \equiv 0 \pmod{p}) \text{ and } u^{10} \equiv v^{10} \equiv w^{10} \pmod{p})$$

then p divides one of u, v and w.

Proof of Theorem 1:

All congruences are modulo p.

Assume that p does not divide uvw. If $u \equiv v$, then we get $2u \equiv -w$, and so

$$2^5 \equiv \pm 1$$

hence either $33 \equiv 0$ or $31 \equiv 0$. If $33 \equiv 0$, then 10n+1=3 or 10n+1=11, which gives that 10n=2 or 10n=10, which is impossible. If $31 \equiv 0$, then 10n+1=31, and so n=3, impossible. Therefore $u \equiv v$, $u \equiv w$ and $v \equiv w$ are impossible.

We have $u^{10} \equiv v^{10} \equiv w^{10}$, hence and because of symmetry, we get

$$u^5 \equiv v^5 \equiv w^5 \text{ or } u^5 \equiv v^5 \equiv -w^5 .$$

Suppose that

$$u^5 \equiv v^5 \equiv w^5 .$$

Then $u^5 - w^5 \equiv 0$ and $v^5 - w^5 \equiv 0$. But

$$u^5 - w^5 = (u-w)(u^4 + u^3 w + u^2 w^2 + uw^3 + w^4)$$

and

$$v^5 - w^5 = (v-w)(v^4 + v^3 w + v^2 w^2 + vw^3 + w^4)$$

and so as $u \equiv w$ and $v \equiv w$ are impossible, then

$$u^4 + u^3 w + u^2 w^2 + uw^3 + w^4 \equiv 0$$

and

$$v^4 + v^3 w + v^2 w^2 + vw^3 + w^4 \equiv 0.$$

This implies

$$(u^4 - v^4) + (u^3 - v^3)w + (u^2 - v^2)w^2 + (u-v)w^3 \equiv 0$$

hence

$$(u-v)(u+v)(u^2 + v^2) + (u-v)(u^2 + v^2 + uv)w + (u-v)(u+v)w^2 + (u-v)w^3 \equiv 0$$

But $u+v \equiv -w$ and $u \equiv v$ is impossible, hence

$$-(u^2+v^2)w+(u^2+v^2+uv)w \equiv 0$$

whence

$$uvw \equiv 0$$

which is impossible.

Assume that

$$u^5 \equiv v^5 \equiv -w^5 .$$

Then

$$u^5+w^5 \equiv 0 \text{ and } v^5+w^5 \equiv 0.$$

But

$$u^5+w^5 = (u+w)(u^4-u^3w+u^2w^2-uw^3+w^4)$$

and

$$v^5+w^5 = (v+w)(v^4-v^3w+v^2w^2-vw^3+w^4)$$

and so as $u \equiv -w$ and $v \equiv -w$ are impossible, then

$$u^4-u^3w+u^2w^2-uw^3+w^4 \equiv 0$$

and

$$v^4-v^3w+v^2w^2-vw^3+w^4 \equiv 0.$$

This implies that

$$(u^4-v^4)-(u^3-v^3)w+(u^2-v^2)w^2-(u-v)w^3 \equiv 0$$

hence

$$(u-v)(u+v)(u^2+v^2)-(u-v)(u^2+v^2+uv)w+(u-v)(u+v)w^2-(u-v)w^3 \equiv 0$$

But $u+v \equiv -w$ and $u \equiv v$ is impossible, hence

$$-(u^2+v^2)w-(u^2+v^2+uv)w-2w^3 \equiv 0$$

whence

$$-2(u^2+v^2)-uv-2w^2 \equiv 0$$

which gives

$$2(u^2+v^2)+uv+2w^2 \equiv 0$$

hence as $u^2+v^2=(u+v)^2-2uv \equiv w^2-2uv$, then

$$2(w^2-2uv)+uv+2w^2 \equiv 0$$

and so

$$4w^2-3uv \equiv 0$$

whence

$$4w^2 \equiv 3uv .$$

On the other hand we have $u^5-v^5 \equiv 0$ and $u \equiv v$ is impossible, hence

$$u^4+u^3v+u^2v^2+uv^3+v^4 \equiv 0$$

and so

$$u^4+v^4+uv(u^2+v^2)+u^2v^2 \equiv 0 .$$

However

$$u^2+v^2=(u+v)^2-2uv \equiv w^2-2uv .$$

Therefore

$$u^4+v^4 \equiv (u^2+v^2)^2-2u^2v^2 \equiv (w^2-2uv)^2-2u^2v^2 \equiv w^4-4uvw^2+2u^2v^2$$

and so

$$w^4-4uvw^2+2u^2v^2+uv(w^2-2uv)+u^2v^2 \equiv 0$$

which gives

$$w^4-3uvw^2+u^2v^2 \equiv 0$$

hence

$$w^2(w^2-3uv)+u^2v^2 \equiv 0$$

and so as $4w^2 \equiv 3uv$, then

$$w^2(w^2-4w^2)+u^2v^2 \equiv 0$$

whence

$$-3w^4+u^2v^2 \equiv 0$$

and so

$$9(-3w^4+u^2v^2) \equiv 0$$

which gives $-27w^4+(3uv)^2 \equiv 0$, and hence $-27w^4+(4w^2)^2 \equiv 0$, whence $-11w^4 \equiv 0$, which yields that $w^4 \equiv 0$, impossible. Thus p divides uvw. ∎

Proof of Theorem A:

Take $u = x^n$, $v = y^n$ and $w = z^n$. Then

$$u+v+w \equiv 0 \pmod{p}.$$

Since p is prime, $\mathbb{Z}/p\mathbb{Z}-\{0\}$ is a finite group of order p-1. But as $p-1=10n$, then $\alpha^{10n}=1$, for every α in $\mathbb{Z}/p\mathbb{Z}-\{0\}$, and so

$$u^{10} = v^{10} = w^{10} = 1$$

whence $u^{10} \equiv v^{10} \equiv w^{10} \pmod{p}$. It follows from Theorem 1 that p divides uvw, and so p divides $(xyz)^n$. As p is prime, then p divides xyz, and so it divides one of x, y and z. ∎

REFERENCES

Cheaito, N. 2001. Congruences modulo primes of the form $2^s n+1$. *Lebanese Science Journal*, 2(1): 139-150.

Edwards, H.M. 1977. *Fermat's last theorem*. G.T.M. 50, Springer-Verlag.