CONGRUENCES MODULO PRIMES OF THE FORM $p=2^s n+1$ AND APPLICATIONS TO FERMAT'S LAST THEOREM

Nasri Cheaito
Department of Mathematics
Faculty of Sciences, Section I
Lebanese University
Hadath

(Received 1 November 1998 Accepted 25 July 2000)

INTRODUCTION

Using the fact that for every odd prime p the multiplicative group $G=\mathbb{Z}/p\mathbb{Z}-\{0\}$ is a finite cyclic group of order p-1, we prove the following:

Theorem A: Let n be an odd natural number, such that $p=2^s n+1$ is prime for some $s\geq 1$. Let u, v and w be integers, such that $u+v+w \equiv 0 \pmod{p}$ and
$u^{2^r} \equiv v^{2^r} \equiv w^{2^r} \pmod{p}$, for some $1\leq r\leq s$.
Then we have

(i) If $1\leq r\leq 4$, then p divides one of u, v and w.

(ii) If r = 5 and p does not divide any of u, v and w, then n=3 or (s = 5 and n = 3) or (s = 6 and n = 7).

As consequences of Theorem A, we prove the following:

Theorem A': Let n be an odd natural number, such that $p=2^s n+1$ is prime for some $s\geq 1$. If x, y and z are integers, such that $x^n+y^n+z^n \equiv 0 \pmod{p}$, then

(i) If $1\leq s\leq 4$, then p divides one of x, y and z.

(ii) If $s=5$ and $n\neq 3$, then p divides one of x, y and z.

Theorem A'': If n is an odd prime and $2^s n+1$ is prime, for some $1\leq s\leq 5$, then Case I of Fermat's Last Theorem holds, that is if n is an odd prime, such that $2^s n+1$ is prime for some $1\leq s\leq 5$ and if x, y and z are integers, such that n does not divide any of them, then the equation $x^n+y^n+z^n = 0$ is impossible.

BASIC RESULTS

Let n be an odd natural number and suppose that $p=2^s n+1$ is prime for some $s\geq 1$. Let x, y and z be integers, such that

(i) $x+y+z \equiv 0 \pmod{p}$.

(ii) $x^{2^r} \equiv y^{2^r} \equiv z^{2^r} \pmod{p}$, for some $1\leq r\leq s$.

(ii) p does not divide any of x, y and z.

In the rest all congruences are supposed modulo p.

Lemma 2.1. The following hold

(i) $x \equiv -y$ is impossible.

(ii) If $x \equiv y$, then there exists $1\leq t\leq r-1$, such that p divides $2^{2^t}+1$.

Proof:

(a) Assume that $x \equiv -y$. Then $x+y \equiv 0$, and so $z \equiv 0$, a contradiction. Therefore $x \equiv -y$ is impossible.

(b) Suppose that p does not divide $2^{2^t}+1$, for all $1 \le t \le r-1$. Then as $x+y+z \equiv 0$, we get that $2x \equiv -z$, and so $2^{2^r} x^{2^r} \equiv z^{2^r}$. But $x^{2^r} \equiv z^{2^r}$ and $x^{2^r} \neq 0 \pmod{p}$, hence $2^{2^r} \equiv 1$.

Since $2^{2^r}-1 = (2+1)(2^2+1)(2^{2^2}+1)....(2^{2^{r-1}}+1)$, $\exists 1 \le t \le r-1$, such that p divides $(2^{2^t}+1)$, a contradiction. Therefore (ii) holds.

Lemma 2.2.

(a) If $x^2 \equiv y^2$, then there exists $1 \le t \le r-1$, such that p divides $2^{2^t}+1$.

(b) If $x^2 \equiv -y^2$, then $r \ge 2$ and there exists $1 \le t \le r-2$, such that p divides $2^{2^t}+1$.

Proof:

(i) Suppose that p does not divide $2^{2^t}+1$, for all $1 \le t \le r-1$. Since $x^2 \equiv y^2$, either $x \equiv y$, which is impossible, by lemma 2.1, or $x \equiv -y$, which is also impossible, by lemma 2.1.

(c) Since $x^2 \equiv -y^2$ and $x^{2^r} \equiv y^{2^r}$, we then have that $r \ge 2$. Assume that p does not divide $2^{2^t}+1$, for all $1 \le t \le r-2$. We have $x+y \equiv -z$, hence $x^2+y^2+2xy \equiv z^2$, and so

$$2xy \equiv z^2 .$$

This implies that

$$2^{2^{r-1}} x^{2^{r-1}} y^{2^{r-1}} \equiv (z^2)^{2^{r-1}} .$$

But $x^{2^{r-1}} \equiv y^{2^{r-1}}$, hence $2^{2^{r-1}} x^{2^r} \equiv z^{2^r}$. However $x^{2^r} \equiv z^{2^r}$ and $x^{2^r} \neq 0 \pmod{p}$. Hence $2^{2^{r-1}} \equiv 1$, and so there exists $1 \le t \le r-2$, such that p divides $2^{2^t}+1$, a contradiction.

Lemma 2.3

(i) If $x^{2^2} \equiv y^{2^2}$, then there exists $1 \le t \le r-1$, such that p divides $2^{2^t}+1$.

(ii) If $x^{2^2} \equiv -y^{2^2}$, then $r \ge 3$ and there exists an integer a, such that

$$a^{2^{r-1}} \equiv 1 \text{ and } 2a^2 - 4a + 1 \equiv 0 .$$

Proof:

(i) If $x^{2^2} \equiv y^{2^2}$, then either $x^2 \equiv y^2$ or $x^2 \equiv -y^2$, and so there exists $1 \le t \le r-1$, such that p divides $2^{2^t}+1$, by lemma 2.2.

(ii) Since $x^{2^2} \equiv -y^{2^2}$ and $x^{2^r} \equiv y^{2^r}$, we then get that $r \ge 3$. We have $x+y \equiv -z$ so that $x^2+y^2 \equiv z^2 - 2xy$, and so

$$x^4 + y^4 + 2x^2y^2 \equiv z^4 - 4xyz^2 + 4x^2y^2 .$$

This yields that

$$z^4 - 4xyz^2 + 2x^2y^2 \equiv 0.$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field and $z \not\equiv 0 \pmod{p}$, we then get that there exists an integer a, such that $xy \equiv az^2$.

We have

$$z^4 - 4az^4 + 2a^2z^4 \equiv 0$$

hence as $z^4 \not\equiv 0 \pmod{p}$, then $1 - 4a + 2a^2 \equiv 0$.

On the other hand we have $x^{2^{r-1}} y^{2^{r-1}} \equiv a^{2^{r-1}} (z^2)^{2^{r-1}}$, so that as $x^{2^{r-1}} \equiv y^{2^{r-1}}$, then $x^{2^r} \equiv a^{2^{r-1}} z^{2^r}$. But $x^{2^r} \equiv z^{2^r}$ and $x^{2^r} \not\equiv 0 \pmod{p}$, whence $a^{2^{r-1}} \equiv 1$. This completes the proof of (ii).

PROOF OF THEOREM A

Let n be an odd natural number and suppose that $p = 2^s n + 1$ is prime for some $s \ge 1$. Let u, v and w be integers, such that

(i) $u + v + w \equiv 0$

(ii) $u^{2^r} \equiv v^{2^r} \equiv w^{2^r}$, for some $1 \le r \le s$.

Proof of part(i) of Theorem A: Because r≤4, we have $u^{16} \equiv v^{16} \equiv w^{16}$, so that there exist x,y,z∈{u,v,w}, such that

$$\{x,y,z\} = \{u,v,w\} \text{ and } x^8 \equiv y^8 .$$

This implies

$$x^{2^2} \equiv y^{2^2} \text{ or } x^{2^2} \equiv -y^{2^2} .$$

Assume that p does not divide any of u, v and w. Then p does not divide any of x, y and z. But

$$x+y+z \equiv 0 \text{ and } x^{2^r} \equiv y^{2^r} \equiv z^{2^r}$$

then we get from lemma 2.3 that

$$p \text{ divides } 2^{2^t}+1, \text{ for some } 1\le t\le r-1$$

or

$$r\ge 3 \text{ and there exists an integer a, such that } a^{2^{r-1}} \equiv 1 \text{ and } 2a^2-4a+1 \equiv 0.$$

Suppose that the former holds. Since 1≤r≤4, $2^{2^t}+1$ is prime, for all 1≤t≤r-1, and so $p = 2^{2^t}+1$, which yields that $2^s n = 2^{2^t}$, which is impossible, because n is odd. Assume that the latter holds. Then

$$a^8 \equiv 1 \text{ and } 2a^2-4a+1 \equiv 0.$$

We have either $a^4 \equiv 1$ or $a^4 \equiv -1$. If $a^4 \equiv 1$, then either $a^2 \equiv 1$ or $a^2 \equiv -1$. But

$$a^2 \equiv 1 \Rightarrow a \equiv 1 \text{ or } a \equiv -1 \Rightarrow -1\equiv 0 \text{ or } 7\equiv 0 \Rightarrow p=7 \Rightarrow s=1 \text{ and } n=3$$

and

$$a^2 \equiv -1 \Rightarrow -4a \equiv 1 \Rightarrow -16\equiv 1 \Rightarrow 17\equiv 0 \Rightarrow 2^s n = 16$$

hence either s=1 or $2^s n = 16$, which is impossible because s≥ r≥3 and n is odd. It follows that $a^4 \equiv -1$. Now

$2a^2 \equiv 4a-1 \Rightarrow 4a^4 \equiv (4a-1)^2 \Rightarrow 4a^4 \equiv 16a^2-8a+1 \Rightarrow 16a^2-8a+5\equiv 0 \Rightarrow 8(2a^2)-8a+5\equiv 0$

$\Rightarrow 8(4a-1)-8a+5\equiv 0 \Rightarrow 24a-3\equiv 0 \Rightarrow 8a\equiv 1 \Rightarrow 64a^2 \equiv 1 \Rightarrow 32(4a-1)\equiv 1$

$\Rightarrow 128a\equiv 33 \Rightarrow 16(8a)\equiv 33 \Rightarrow 16\equiv 33 \Rightarrow 17\equiv 0 \Rightarrow p = 17 \Rightarrow 2^s n = 16$

so that n is even, impossible. Therefore p divides one of u, v and w.

Proof of part(ii) of Theorem A:

We have $u^{32} \equiv v^{32} \equiv w^{32}$, so that there exist x,y,z∈{u,v,w}, such that {x,y,z} = {u,v,w} and either

$$x^{16} \equiv y^{16} \equiv z^{16} \text{ or } x^{16} \equiv y^{16} \equiv -z^{16} .$$

If $x^{16} \equiv y^{16} \equiv z^{16}$, then p divides one of x, y and z, by 3.1, and so p divides one of u, v and w, a contradiction. Hence

$$x^{16} \equiv y^{16} \equiv -z^{16}.$$

This yields either $x^8 \equiv y^8$ or $x^8 \equiv -y^8$. Suppose that $x^8 \equiv y^8$. Then $x^4 \equiv y^4$ or $x^4 \equiv -y^4$, and so we get from lemma 2.3 that

$$p \text{ divides } 2^{2^t}+1, \text{ for some } 1 \le t \le r-1$$

or

$$r \ge 3 \text{ there exists an integer a, such that } a^{2^{r-1}} \equiv 1 \text{ and } 2a^2-4a+1 \equiv 0.$$

Suppose that the former holds. Since $1 \le t \le 4$, $2^{2^t}+1$ is prime, whence $p = 2^{2^t}+1$, and so $2^s n = 2^{2^t}$, which is impossible, because n is odd. Assume that the latter holds. Then as r =5, we get

$$a^{16} \equiv 1 \text{ and } 2a^2-4a+1 \equiv 0.$$

We have

$$2a^2-4a+1 \equiv 0 \Rightarrow 2a^2 \equiv 4a-1 \Rightarrow 4a \equiv 2a^2+1 \Rightarrow 16a^2 \equiv 4a^4+4a^2+1 \Rightarrow 12a^2 \equiv 4a^4+1$$
$$\Rightarrow 144a^4 \equiv 16a^8+8a^4+1 \Rightarrow 136a^4 \equiv 16a^8+1.$$

Since $a^{16} \equiv 1$, either $a^8 \equiv 1$ or $a^8 \equiv -1$. But

$$a^8 \equiv 1 \Rightarrow 136a^4 \equiv 16a^8+1 \Rightarrow 136a^4 \equiv 17 \Rightarrow (136)^2 a^8 \equiv (17)^2 \Rightarrow (136)^2 \equiv (17)^2$$
$$\Rightarrow (136-17)(136+17) \equiv 0 \Rightarrow 119 \times 153 \equiv 0 \Rightarrow 17 \times 7 \times 17 \times 9 \equiv 0$$
$$\Rightarrow 17 \equiv 0 \text{ or } 7 \equiv 0 \text{ or } 3 \equiv 0 \Rightarrow 32n+1 \text{ divides one of 3, 7 and 17}$$

and

$$a^8 \equiv -1 \Rightarrow 136a^4 \equiv -16+1 \Rightarrow 136a^4 \equiv -15 \Rightarrow (136)^2 a^8 \equiv 225 \Rightarrow -(136)^2 \equiv 225$$
$$\Rightarrow (136)^2+225 \equiv 0 \Rightarrow 18721 \equiv 0 \Rightarrow 97 \times 193 \equiv 0 \Rightarrow 97 \equiv 0 \text{ or } 193 \equiv 0$$
$$\Rightarrow 32n+1=97 \text{ or } 32n+1=193 \Rightarrow 32n=96 \text{ or } 32n=192 \Rightarrow n=3 \text{ or } n=6 \Rightarrow n=3$$

hence we get n=3 in this case. Suppose that $x^8 \equiv -y^8$. Since $x+y \equiv -z$, we get

$$x^8+y^8 \equiv z^8-8xyz^6+20x^2y^2z^4-16x^3y^3z^2+2x^4y^4$$

and so

$$z^8-8xyz^6+20x^2y^2z^4-16x^3y^3z^2+2x^4y^4 \equiv 0.$$

Let a be an integer such that $xy \equiv az^2$. Then $z^8-8az^8+20a^2z^8-16a^3z^8-2z^8 \equiv 0$, and so

$$\boxed{16a^3+8a \equiv 20a^2-1.}$$

Since $x^8 y^8 \equiv -y^{16}$, we get $x^8 y^8 \equiv z^{16}$, and so $x^4 y^4 \equiv z^8$ or $x^4 y^4 \equiv -z^8$. Assume that $x^4 y^4 \equiv -z^8$. Then $a^4 \equiv -1$. We have

$16a^3 + 8a\ 20a^2 - 1 \Rightarrow 8a(2a^2+1) \equiv (20a^2-1) \Rightarrow 64a^2(2a^2+1)^2 \equiv (20a^2-1)^2$

$\Rightarrow 64a^2(4a^4+4a^2+1) \equiv 400a^4 - 40a^2 + 1$

$\Rightarrow 64a^2(-4+4a^2+1) \equiv -400-40a^2+1$

$\Rightarrow 64a^2(4a^2-3) \equiv -399-40a^2 \Rightarrow 256a^4 - 192a^2 \equiv -399-40a^2$

$\Rightarrow -256-192a^2 \equiv -399-40a^2 \Rightarrow 143 \equiv 152a^2$

$\Rightarrow (143)^2 \equiv (152)^2 a^4 \Rightarrow (143)^2 \equiv -(152)^2 \Rightarrow (152)^2 + (143)^2 \equiv 0$

$\Rightarrow 43553 \equiv 0 \Rightarrow 97 \times 449 \equiv 0 \Rightarrow 2^s n+1 = 97$ or $2^s n+1 = 449$

$\Rightarrow$ (s=5 and n=3) or (s=6 and n=7).

Suppose that $x^4 y^4 \equiv z^8$. Then $x^2 y^2 \equiv z^4$ or $x^2 y^2 \equiv -z^4$, and so $a^2 \equiv 1$ or $a^2 \equiv -1$. But

$a^2 \equiv 1 \Rightarrow 16a + 8a \equiv 20 - 1 \Rightarrow 24a \equiv 19 \Rightarrow (24)^2 a^2 \equiv (19)^2 \Rightarrow (24)^2 \equiv (19)^2$

$\Rightarrow (24-19)(24+19) \equiv 0 \Rightarrow 5 \equiv 0$ or $43 \equiv 0 \Rightarrow p = 5$ or $p = 43 \Rightarrow 2^s n = 4$ or $2^s n = 42$

$\Rightarrow s=2$ or $s=1$

and

$a^2 \equiv -1 \Rightarrow -16a + 8a \equiv -20 - 1 \Rightarrow -8a \equiv -21 \Rightarrow 64a^2 \equiv 441 \Rightarrow -64 \equiv 441 \Rightarrow 505 \equiv 0$

$\Rightarrow 5 \equiv 0$ or $101 \equiv 0 \Rightarrow p = 5$ or $p = 101 \Rightarrow 2^s n = 4$ or $2^s n = 100 \Rightarrow s = 2$

hence we get that s=1 or s=2, which is impossible, because $s \geq r \geq 5$.

Therefore we have n=3 or (s=5 and n=3) or (s=6 and n=7).

Proof of Theorem A':

(i) Take $u = x^n$, $v = y^n$ and $w = z^n$. We have $u+v+w \equiv 0$ and $u^{2^s} \equiv v^{2^s} \equiv w^{2^s}$ with $1 \leq s \leq 4$, hence p divides one of u, v and w, by 3.1, and so p divides one of x, y and z.

(ii) Take $u = x^n$, $v = y^n$ and $w = z^n$. We have $u+v+w \equiv 0$ and $u^{2^s} \equiv v^{2^s} \equiv w^{2^s}$ with $1 \leq s \leq 5$, so that if p does not divide any of u, v and w, then n=3 or (s=5 and n=3) or (s=6 and n=7), by 3.2, which is impossible, and so p divides one of u, v and w. It follows that p divides one of x, y and z.

PROOF OF THEOREM A''

Lemma 1. The following hold

(i) $2^{2^s}+1$ is prime, for all $0\le s\le 4$.

(ii) If $n\ge 3$ is an odd natural number and $p=2^s n+1$ is prime, for some $s\ge 1$, then $2^{2^r}\equiv 1 \pmod{p}$ is impossible, for all $0\le r\le 5$.

(iii) If a is non-zero natural number and p is a prime dividing $a^{2^r}+1$, for some $r\ge 1$, then there exists a natural number k, such that $p=2^{r+1}k+1$.

Proof:

(i) We have that $2^{2^0}+1=3$, $2^{2^1}+1=5$, $2^{2^2}+1=17$, $2^{2^3}+1=257$ and $2^{2^4}+1=65537$,

hence $2^{2^s}+1$ is prime, for all $0\le s\le 4$.

(c) Assume that $2^{2^r}\equiv 1 \pmod{p}$, for some $0\le r\le 5$. If $r = 0$, we get that $2\equiv 1 \pmod{p}$, which gives that p divides $2-1$, impossible. Suppose that $1 \le r\le 5$. We have

$$2^{2^r}-1=(2-1)(2+1)(2^2+1)\ldots(2^{2^{r-1}}+1)=\prod_{t=0}^{r-1}(2^{2^t}+1)$$

so that there exists $0\le t\le r-1$, such that p divides $2^{2^t}+1$. But $r-1\le 4$, hence there exists $0\le t\le 4$, such that p divides $2^{2^t}+1$. Since $2^{2^t}+1$ is prime, by (i), we then get that $p = 2^{2^t}+1$, whence $2^s n+1 = 2^{2^t}+1$, and so 2 divides n, impossible. Therefore (ii) holds.

(iii) We have that $G = \mathbb{Z}/p\mathbb{Z}-\{0\}$ is a cyclic multiplicative group of order $p-1$, so that if p divides $a^{2^r}+1$, then p divides $a^{2^{r+1}}-1$, and so the order $|a|$ of a is a divisor of 2^{r+1}, whence $|a| = 2^t$, for some $t\le r+1$. Assume that $t\ne r+1$. Then 2^t divides 2^r, and so $a^{2^r}=1 \pmod{p}$, which then yields that $1=-1 \pmod{p}$, that is p divides 2, a contradiction to the fact that p is odd. Therefore $t = r+1$, and so $|a| = 2^{r+1}$. Since $|a|$ divides $|G|=p-1$, there exists $k\in\mathbb{Z}$, such that

p-1=k$|a|$ = 2^{r+1}k, which gives p = 2^{r+1}k+1. Û

Lemma 2. Let n be an odd prime. Suppose that p=2kn+1 is prime for some k≥1, such that the implication

$u^n+v^n+w^n \equiv 0 \pmod{p} \Rightarrow$ p divides one of u, v and w is true for all integers u, v and w. If x, y and z are integers, such that $x^n+y^n+z^n=0$ and if n does not divide any of x, y and z, then $(2k)^{2k} \equiv 1 \pmod{p}$.

Proof: Without loss of generality we may assume that x, y and z are pairwise relatively prime. Since $x^n+y^n+z^n=0$, we get that $x^n+y^n = -z^n$. Let u = x+y. Then

$$x^n+y^n = (u-y)^n+y^n = \sum_{t=0}^{n} C_n^t u^{n-t}(-y)^t+y^n$$

$$= u[\sum_{t=0}^{n-1} C_n^t u^{n-t-1}(-y)^t]$$

$$= u[\sum_{t=0}^{n-2} C_n^t u^{n-t-1}(-y)^t+n(-y)^{n-1}]$$

and so

$$\sum_{t=0}^{n-1}(-x)^t y^{n-t} = \sum_{t=0}^{n-2} C_n^t u^{n-t-1}(-y)^t+n(-y)^{n-1}.$$

if q is a prime dividing u = x+y and $\sum_{t=0}^{n-1}(-x)^t y^{n-t}$, then q divides u and n(-y)$^{n-1}$. But q divides z and n does not divide z, hence q does not divide n, and so q divides (-y)$^{n-1}$, whence it divides y, and thence it divides x = u-y, impossible. Therefore x+y and $\sum_{t=0}^{n-1}(-x)^t y^{n-t}$ are relatively prime, and so as (x+y)($\sum_{t=0}^{n-1}(-x)^t y^{n-t}$) = $x^n+y^n = -z^n$, then there exist two integers c and γ, such that c and γ are relatively prime and

$$x+y = \gamma^n, \quad \sum_{t=0}^{n-1}(-x)^t y^{n-t} = c^n \text{ and } z = -c\gamma.$$

Similarly there exist integers a, b, α and β, such that

$$z+y=\alpha^n,\ \sum_{t=0}^{n-1}(-z)^t y^{n-t}=a^n \text{ and } x=-a\alpha$$

and

$$z+x=\beta^n,\ \sum_{t=0}^{n-1}(-z)^t x^{n-t}=b^n \text{ and } y=-b\beta.$$

Let $p=2kn+1$. Since $x^n+y^n+z^n\equiv 0 \pmod{p}$, p divides xyz. Without loss of generality we may assume that p divides z. We have

$$2z=\alpha^n+\beta^n-\gamma^n$$

so that $\alpha^n+\beta^n+(-\gamma)^n\equiv 0 \pmod{p}$, and so p divides one of α, β and γ. But p divides z and z is relatively prime with x and y, and so as α divides x and β divides y, then p must divide γ. This yields that $x+y\equiv 0 \pmod{p}$, hence

$$x\equiv -y \pmod{p}.$$

Since $\sum_{t=0}^{n-1}(-x)^t y^{n-t}=c^n$, we then get

$$\sum_{t=0}^{n-1}(-x)^t y^{n-t}\equiv\sum_{t=0}^{n-1}(y)^t y^{n-t}\equiv ny^{n-1} \pmod{p}$$

and so

$$c^n\equiv ny^{n-1} \pmod{p}.$$

However $a^n=\sum_{t=0}^{n-1}(-z)^t y^{n-t}\equiv y^{n-1} \pmod{p}$. Therefore $c^n\equiv na^n \pmod{p}$, which gives that $(c^n)^{2k}\equiv n^{2k}(a^n)^{2k} \pmod{p}$, and so $1\equiv n^{2k} \pmod{p}$. But $2kn\equiv -1 \pmod{p}$, hence $(2kn)^{2k}\equiv 1 \pmod{p}$, which yields $(2k)^{2k}\equiv 1 \pmod{p}$.

Theorem A'':

If n is an odd prime and $2^s n+1$ is prime, for some $1\le s\le 5$, then Case I of Fermat's Last Theorem holds.

Proof:

Assume that Case I of Fermat's Last Theorem does not hold. Then there exist integers x, y and z, such that

$$x^n+y^n+z^n=0 \text{ and } n \text{ does not divide any of } x, y \text{ and } z.$$

If n = 3, then as 2×3+1=7 is prime, we get from part (i) of Theorem A' that 3 satisfies the conditions of lemma 4.2, and so $(2)^2 \equiv 1 \pmod{7}$, which is impossible. Assume that n≠3. Since n satisfies the conditions of lemma 4.2, by Theorem A', we then have that

$$(2^s)^{2^s} \equiv 1 \pmod{p}.$$

If s=1, we get $4 \equiv 1 \pmod{2n+1}$, which gives 2n+1=3, and so n=1, impossible.

If s=2, then we get $2^{2^3} \equiv 1 \pmod{4n+1}$, which is impossible, by lemma 4.1(ii).

If s=3, then $(2^3)^{2^3} \equiv 1 \pmod{p}$, and so the order of 2 in $G=\mathbb{Z}/p\mathbb{Z}-\{0\}$ divides 3×2^3. If 3 divides the order of 2, then 3 divides p-1=8n, and so 3 divides n, which then yields that n=3, and hence p=25 is not a prime, impossible. Thus the order of 2 divides 2^3, and so $2^{2^3} \equiv 1 \pmod{p}$, which is impossible, by lemma 4.1(ii).

If s=4, then $2^{2^6} \equiv 1 \pmod{p}$. But $2^{2^5} \equiv 1 \pmod{p}$ is impossible, by lemma 4.1(ii), hence

$2^{2^5} \equiv -1 \pmod{p}$. It follows that p divides $2^{2^5}+1$, and so there exists a natural number k, such that p=64k+1, by lemma 4.1(iii). This implies that n=4k, impossible.

If s=5, then $(2^5)^{2^5} \equiv 1 \pmod{p}$. It follows that the order $|2|$ of 2 in $G=\mathbb{Z}/p\mathbb{Z}-\{0\}$ divides

5×2^5. If 5 divides $|2|$, then 5 divides p-1=32n, and so 5 divides n, which yields that n=5, and hence p=161 is not a prime. Thus $|2|$ divides 2^5, and so $2^{2^5} \equiv 1 \pmod{p}$, which is impossible, by lemma 4.1(ii). This completes the proof of Theorem A".

REFERENCES

Cassels, J., and Fröhlich, A. 1967. *Algebraic number theory*. Acad. Press, New York.

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

Hardy, G. H., and Wright, E. M. 1960. An introduction to the theory of numbers, 4th edit., New York: Oxford University Press,

Herstein, I.N. 1975. *Topics in algebra*. John Wiley & Sons, Inc. 2nd edit., New York.

Hungerford, T.W. 1984. *Algebra*. *G.T.M.* 73, Springer-Verlag, 3rd print.

Koblitz, N. 1977. *p-adic numbers, p-adic analysis, and zeta-functions*. G.T.M. 58, Springer-Verlag,

Lang, S. 1970. *Algebraic number theory*. Addison-Wesley.

Serre, J. P. 1978. *A course in arithmetic*. G.T.M. 7, 2nd edit., Springer-Verlag.
Serre, J. P. 1979. *Local fields.* G.T.M. 67, Springer-Verlag,