ACTA ARITHMETICA
L (1988)

On Sophie Germain type criteria for Fermat's Last Theorem

by

ANDREW GRANVILLE (Kingston, Ont.) and BARRY POWELL (Kirkland, Wash.)

0. Introduction. The First Case of Fermat's Last Theorem is said to be true for $n > 2$ when

(FLT1)$_n$ *If x, y, z are non-zero integers such that $x^n + y^n = z^n$ then the highest common factor of n and xyz is greater than 2.*

Terjanian [13] showed that (FLT1)$_n$ is true for even exponents, so we may take n to be odd. Furthermore, if n divides m and (FLT1)$_n$ is true then it is clear that (FLT1)$_m$ is also true. Thus, it suffices to prove (FLT1)$_p$ is true for each odd prime p.

We shall prove a technical theorem, from which we deduce that (FLT1)$_n$ is true when $n = p^a$ or $p^a q^b$ (where p, q are distinct odd primes and a, b are sufficiently large). We shall also obtain other interesting results, some of which have previously been obtained using different methods. In fact, the technical development appears in Sections 1–3 and the main results in Sections 4–5; these may be read without references to Sections 1–3.

We note that if n is odd and x, y, z satisfy $x^n + y^n = z^n$ then $x, y, -z$ satisfy the equation

$$(1)_n \qquad X^n + Y^n + Z^n = 0.$$

Moreover, we may assume that x, y and z are pairwise relatively prime.

The following results will be used:

ABEL'S RELATIONS ([1]). *Suppose that p is an odd prime, $t \geqslant 1$, and a, b, c are non-zero pairwise relatively prime integers such that $a^{p^t} + b^{p^t} + c^{p^t} = 0$. If p divides a then p divides $b + c$ and there exist integers r, s such that*

$$a + b = r^{p^t}, \quad a + c = s^{p^t}.$$

POLLACZEK'S THEOREM ([11]). *If p is an odd prime, and a, b, c are non-zero pairwise relatively prime integers such that $a^p + b^p + c^p = 0$ then $p \nmid ab + bc + ca$.*

Actually Pollaczek's theorem was proved under the additional condition that $p \nmid abc$. However, it holds also if $p|abc$ (for if $p|a$ then $p|ab+ca$ and so $p \nmid ab+bc+ca$).

AZUHATA'S THEOREM ([4]). *Suppose that p is an odd prime, $t \geqslant 1$ and a, b, c are non-zero pairwise relatively prime integers such that $a^{p^t}+b^{p^t}+c^{p^t} = 0$. If q is a prime and one of the following conditions is satisfied:*

(i) $q|a$ *and* $p \nmid a$,

(ii) $q|a^2-bc$ *and* $p \nmid ab+bc+ca$,

then $q^p \equiv q \pmod{p^{2t}}$.

Note that $ab+bc+ca \equiv (ab)^{p^t-1}+(bc)^{p^t-1}+(ca)^{p^t-1} \pmod p$, so, in view of Pollaczek's theorem, the second condition in (ii) above is automatically satisfied.

We also need the following easy lemma:

LEMMA 1. *Let $m, t \geqslant 1$, and p, q be odd primes such that $q = 1+mp^t$. For any integer $k \geqslant 0$, $q^p \equiv q \pmod{p^{t+k}}$ if and only if $p^k|m$.*

Proof. If $m = m'p^k$ then $q \equiv 1 \pmod{p^{k+t}}$, so $q^2 \equiv q \pmod{p^{k+t}}$, ..., $q^p \equiv q^{p-1} \pmod{p^{k+t}}$ hence $q^p \equiv q \pmod{p^{k+t}}$. Conversely, let $m = m'p^h$ with $h \geqslant 0$, $p \nmid m'$. So $q = 1+m'p^{h+t}$ and therefore $q^p = 1+m'p^{h+t+1}+lp^{2h+2t+1}$. If $q^p-q = up^{t+k}$ then $m'p^{h+t}(p-1)+lp^{2h+2t+1} = up^{t+k}$. Hence $t+k \leqslant h+t$, so that $k \leqslant h$ and p^k divides m. ∎

1. The first theorem.

THEOREM 1. *Let p, q be odd primes such that $p|q-1$; let $t \geqslant 1$ be such that $p^{t+1} \nmid q-1$. If there exist non-zero pairwise relatively prime integers x, y, z such that $x^{p^t}+y^{p^t}+z^{p^t} = 0$ with $q|x$ then $pq|y+z$.*

Proof. Let $q = 1+mp^n$ where $p \nmid m$ and $1 \leqslant n \leqslant t$.

By Azuhata's theorem, $p|x$, otherwise $q^p \equiv q \pmod{p^{2t}}$, so that $1+mp^{n+1} \equiv 1+mp^n \pmod{p^{2n}}$ and $p|m$, contrary to the hypothesis.

Since $x+y+z \equiv 0 \pmod p$ then $p|y+z$ and, by Abel's relations, there exist r, s such that $x+y = r^{p^t}$, $x+z = s^{p^t}$. Since $q|x$ then $q \nmid zy$ and $y \equiv r^{p^t} \pmod q$, $z \equiv s^{p^t} \pmod q$ and $y^{p^t}+z^{p^t} \equiv 0 \pmod q$. Let k be an integer such that $kz \equiv -y \pmod q$. Then $k^{p^t} \equiv (-y/z)^{p^t} \equiv 1 \pmod q$. But $q-1|mp^t$ so $y^m \equiv r^{mp^t} \equiv 1 \pmod q$, and, similarly, $z^m \equiv 1 \pmod q$ so that $k^m \equiv 1 \pmod q$. Since $p \nmid m$ we have $k \equiv 1 \pmod q$ so that $q|y+z$. ∎

2. Preparation for the second theorem. For any field K and $\alpha \in K$ let $N_{K|Q}(\alpha)$ denote the norm of α.

Let m be an even positive integer and let ξ be a primitive mth root of 1; $A = Z[\xi]$.

If i, j are non-negative integers, let $h = h_{m,i,j} = \gcd(m, i, j)$. Define $N_{m,i,j}$ as follows:

If $m \nmid i+j$, let $N_{m,i,j} = N_{Q(\xi^h)|Q}(1+\xi^i+\xi^j)$.

If $m|i+j$, let $N_{m,i,j} = N_{Q(\xi^{h+\xi-h})|Q}(1+\xi^i+\xi^j)$.

Let $T_m = \{(i,j)|\ 1+\xi^i+\xi^j = 0,\ 0 \leqslant i,j < m\}$. For every prime q, let

$$t_{m,q} = \max\{v_q(N_{m,i,j})|\ 0 \leqslant i,j < m,\ (i,j) \notin T_m\}$$

(here v_q denotes the q-adic valuation). Note that if $(i,j) \notin T_m$ then $N_{m,i,j} \neq 0$; therefore $t_{m,q}$ is a non-negative integer as $(0,0)$ is clearly not an element of T_m.

Let $S(m) = \{q \text{ prime}|\ q \equiv 1 \pmod m \text{ and } t_{m,q} \geqslant 1\}$. Thus

$$S(m) = \bigcup_{\substack{(i,j)\notin T_m \\ 0\leqslant i,j<m}} \{q \text{ prime}|\ q \equiv 1 \pmod m \text{ and } q|N_{m,i,j}\},$$

so that $S(m)$ is a finite set.

LEMMA 2. (i) *If* $3 \nmid m$ *then* $T_m = \emptyset$; *if* $3|m$ *then*

$$T_m = \{(m/3, 2m/3), (2m/3, m/3)\}.$$

(ii) *If* q *is any odd prime then* $t_{q-1,q} \geqslant 1$.

Proof. (i) If α_1, α_2 are roots of unity such that $1+\alpha_1+\alpha_2 = 0$ then $\alpha_1 = \omega$, $\alpha_2 = \omega^2$, or $\alpha_1 = \omega^2$, $\alpha_2 = \omega$, where $\omega = \cos(2\pi/3)+i\sin(2\pi/3)$. (For if $\alpha_1 = x+iy$ and $\alpha_2 = a+ib$ then $y = -b$, so $|a| = |x|$ and $a+x = -1$; thus $a = x = -1/2$ and $y = -b = \pm\sqrt{3}/2$). So, if $(i,j) \in T_m$, then $3|m$ and so $\xi^i = \xi^{m/3}$, $\xi^j = \xi^{2m/3}$, or $\xi^i = \xi^{2m/3}$, $\xi^j = \xi^{m/3}$.

(ii) We calculate $N_{m,0,d}$ where $d|m$; by definition

$$N_{m,0,d} = N_{Q(\xi^d)|Q}(2+\xi^d) = \prod_{\substack{1\leqslant a\leqslant m/d \\ \gcd(a,m/d)=1}} (2+\xi^{ad}).$$

Then

$$\prod_{d|m} N_{m,0,d} = \prod_{d|m} \prod_{\substack{1\leqslant a\leqslant m/d \\ \gcd(a,m/d)=1}} (2+\xi^{ad}) = \prod_{b=1}^{m} (2+\xi^b) = 2^m - 1,$$

since m is even. Taking $m = q-1$ there exists d such that $q|N_{q-1,0,d}$, since $q|2^{q-1}-1$; and so this implies that $t_{q-1,q} \geqslant 1$, as $N_{m,0,0} = N_{m,0,m}$. ∎

LEMMA 3. *If* m *is even and* q *is any prime, then*

$$t_{m,q} \leqslant [\varphi(m)\log 3/\log q].$$

Proof. To begin we note the general fact: if $Q \subseteq K' \subseteq K$, $K|Q$ and $K'|Q$ are Galois extensions of finite degree, and $\alpha \in K'$, then $N_{K'|Q}(\alpha)$ divides $N_{K|Q}(\alpha)$. Thus, for every $(i,j) \notin T_m$, $0 \leqslant i,j < m$,

$$N_{m,i,j} \text{ divides } N_{Q(\xi)|Q}(1+\xi^i+\xi^j) = \prod_{\substack{1\leqslant a<m \\ \gcd(a,m)=1}} (1+\xi^{ai}+\xi^{aj})$$

and so

$$q^{v_q(N_{m,i,j})} \leqslant |N_{m,i,j}| \leqslant 3^{\varphi(m)}.$$

Hence

$$v_q(N_{m,i,j}) \leqslant \varphi(m) \log 3/\log q,$$

so that

$$t_{m,q} \leqslant [\varphi(m) \log 3/\log q]. \blacksquare$$

The following is well known and it is included only for the sake of completeness:

LEMMA 4. *Let m, t be positive integers and q be a prime with $q \equiv 1 \pmod m$. There exist exactly $\varphi(m)$ integers r, such that $1 \leqslant r \leqslant q^t - 1$ and order $(r \bmod q^t) = m$.*

LEMMA 5. *Let m, t be positive integers, with m even, and q be a prime with $q \equiv 1 \pmod m$. Let r be an integer such that $1 \leqslant r \leqslant q^t - 1$ and order $(r \bmod q^t) = m$. If i and j are non-negative integers and $q^t \mid 1 + r^i + r^j$ then $q^t \mid N_{m,i,j}$.*

Proof. Since $q \equiv 1 \pmod m$, we know that Aq is totally decomposed as the product of $\varphi(m)$ distinct prime ideals of A; that is

$$Aq = \prod_{k=1}^{\varphi(m)} Q_k.$$

Thus

$$Aq^t = \prod_{k=1}^{\varphi(m)} Q_k^t.$$

Now, for each k, $Z/Zq \simeq A/Q_k$, so that $Z/Zq^t \simeq A/Q_k^t$. But, by Lemma 4, there are exactly $\varphi(m)$ elements of order m in Z/Zq^t, and so the same is true for A/Q_k^t. We claim that the set of elements of order m in A/Q_k^t is precisely the set

$$\{\xi^a : 0 \leqslant a < m, (a, m) = 1\}.$$

It suffices to show that if $\xi^a \equiv \xi^b \pmod{Q_k^t}$ then $\xi^a = \xi^b$.

Now suppose that $\xi^b = \xi^a + \alpha$ where $\alpha \in Q_k^t$ and $\alpha \neq 0$. Then $X^m - 1 = (X - \xi^a)(X - \xi^a - \alpha) g(X)$ with $g(X) \in A[X]$. Taking derivatives at $X = \xi^a$ we get

$$m\xi^{a(m-1)} = -\alpha g(\xi^a) \in Q_k^t$$

which is clearly impossible as $q \nmid m$ and ξ is a unit.

Now r has order $m \pmod{q^t}$, so that there exists an integer a, $0 \leqslant a \leqslant m$, $(a, m) = 1$ such that

$$r \equiv \xi^a \pmod{Q_k^t}.$$

Thus $1 + \xi^{ai} + \xi^{aj} \equiv 1 + r^i + r^j \equiv 0 \pmod{Q_k^t}$, and so $Q_k^t \mid 1 + \xi^{ai} + \xi^{aj}$ which di-

vides $N_{m,i,j}$ (in the ring A). But this holds for each $k = 1, 2, \ldots, \varphi(m)$ and, as the ideals Q_k^t are pairwise relatively prime, we have:

$$Aq^t = \prod_{k=1}^{\varphi(m)} Q_k^t \quad \text{divides} \quad N_{m,i,j}.$$

LEMMA 6. *Let q be an odd prime and m, $u \geqslant 1$, $t \geqslant 0$ be such that m is even, u is odd, with $(q-1)q^t | mu$ and $m|(q-1)$. Assume that $x, y, z \neq 0$ are such that $q \nmid xyz$ and $x^u + y^u + z^u = 0$. If $t \geqslant t_{m,q}$ then $3|m$ and there exists ω, $0 \leqslant \omega < q$ such that order $(\omega \bmod q) = 3$, $(y/x)^u \equiv \omega \pmod q$, $(z/x)^u \equiv \omega^2 \pmod q$.*

Proof. We have $1 + (y/x)^u + (z/x)^u \equiv 0 \pmod{q^{t+1}}$. Note that $(y/x)^{um} \equiv 1 \pmod{q^{t+1}}$ since $(q-1)q^t | mu$; similarly $(z/x)^{um} \equiv 1 \pmod{q^{t+1}}$.

Let r be such that $1 \leqslant r < q^{t+1}$ and order $(r \bmod q^{t+1}) = m$; such an element exists because m divides $(q-1)$.

Therefore, there exist integers i, j, $0 \leqslant i, j < m$ such that $(y/x)^u \equiv r^i \pmod{q^{t+1}}$, $(z/x)^u \equiv r^j \pmod{q^{t+1}}$ and hence $1 + r^i + r^j \equiv 0 \pmod{q^{t+1}}$.

By Lemma 5, if $(i, j) \notin T_m$ then $q^{t+1} | N_{m,i,j}$, that is $t_{m,q} \geqslant t+1$, contrary to the hypothesis.

So (i, j) is an element of T_m. Thus by Lemma 2, $3|m$, and there exists ω, $0 \leqslant \omega < q$ such that order $(\omega \bmod q) = 3$ and $(y/x)^u \equiv \omega \pmod q$, $(z/x)^u \equiv \omega^2 \pmod q$. ∎

3. The second theorem. The following theorem, which is rather technical, will have many interesting corollaries.

THEOREM 2. *Let $n \geqslant 1$ be odd, and q be an odd prime such that $q \equiv 1 \pmod n$ and, if $n > 1$, suppose that $n^2 \nmid q-1$. Let $m = (q-1)/n$.*

(a) *If $t_{m,q} = 0$ and $3|m$, then, for every odd prime p, such that $p \nmid m$, let $k = k(p)$ be the smallest positive integer such that $q^p \not\equiv q \pmod{p^{2k}}$; let $l = l(p) = p^k$. If $x, y, z \neq 0$ are such that $x^{nl} + y^{nl} + z^{nl} = 0$ then $qp|x$ (or $qp|y$ or $qp|z$).*

(b) *If $t_{m,q} \neq 0$ or $3 \nmid m$ then let $l = q^{t_{m,q}}$. If $x, y, z \neq 0$ are such that $x^{nl} + y^{nl} + z^{nl} = 0$ then $q|x$ (or $q|y$ or $q|z$) and if $n > 1$ there exists a prime p dividing n such that $p|x$ (or resp. $p|y$, or $p|z$).*

Proof. Let $t = t_{m,q}$, $u = nl$, so that u is odd. Note that q^t divides l, $(q-1)q^t | mu$ and $m|(q-1)$ in both cases (a) and (b).

Assume that $x, y, z \neq 0$, $x^u + y^u + z^u = 0$ and $q \nmid xyz$.

Since $t = t_{m,q}$, we have $3|m$ by Lemma 6, and there exists ω, $0 \leqslant \omega < q$, such that order $(\omega \bmod q) = 3$, with $(y/x)^{nl} \equiv \omega \pmod q$, $(z/x)^{nl} \equiv \omega^2 \pmod q$.

In case (a), $t = 0$. Let $a = x^n$, $b = y^n$, $c = z^n$, so that $a^l + b^l + c^l = 0$. Now

$$(a^2/bc)^l \equiv (x^2/yz)^{nl} \equiv \omega^2 \cdot \omega \equiv 1 \pmod q$$

and

$$(a^2/bc)^m \equiv (x^2/yz)^{mn} \equiv (x^2/zy)^{q-1} \equiv 1 \pmod q.$$

But $l = p^k$ where $p \nmid m$, so $a^2/bc \equiv 1 \pmod q$; that is $q | a^2 - bc$.

But by Azuhata's theorem $q^p \equiv q \pmod{p^{2k}}$, so we have a contradiction.

Thus $q | xyz$, say $q | x$. Then $p | x$, else by Azuhata's theorem, $q^p \equiv q \pmod{p^{2k}}$.

In case (b), $t > 0$, $l = q^t$; let $s = nl/q$, $a = x^s$, $b = y^s$, $c = z^s$. Then

$$a^q + b^q + c^q = 0$$

and

$$(b/a) \equiv (y/x)^s \equiv (y/x)^{nl} \equiv \omega \pmod q,$$

and

$$(c/a) \equiv (z/x)^s \equiv (z/x)^{nl} \equiv \omega^2 \pmod q.$$

Hence

$$ab + bc + ca \equiv a^2(\omega + \omega^2 + 1) \equiv 0 \pmod q;$$

contradicting Pollaczek's theorem.

Thus $q | xyz$, say $q | x$.

Suppose that $n > 1$ and $\gcd(n, x) = 1$. If $p | n$ then $p \nmid x$. Let $l = v_p(n)$, and $n = p^l n'$ $(p \nmid n')$, so that

$$(x^{ln'})^{p^l} + (y^{ln'})^{p^l} + (z^{ln'})^{p^l} = 0.$$

Since n is odd, so is p. By Azuhata's theorem $q^p \equiv q \pmod{p^{2l}}$. As $q = 1 + mn'p^l$, we know, by Lemma 1, that $p^l | m$, for every prime p dividing n. Thus $n | m$ and n^2 divides $nm = q - 1$, which is against the hypothesis.

Thus there exists a prime p dividing n and x. ∎

4. The corollaries.

COROLLARY 1. *Let $p \geqslant 3$ and q be primes such that $p | q - 1$.*

There exist integers $t_1 \geqslant 1$, $t_2 \geqslant 0$ (both depending on p and q) such that if $u = p^{t_1} q^{t_2}$, and x, y, z are non-zero integers such that $x^u + y^u + z^u = 0$ then pq divides x (or y, or z).

Furthermore, if $t_1 \geqslant t = v_p(q-1)$ then pq divides $x+y$ (or $y+z$ or $x+z$).

Determination of t_1, t_2: let $m = (q-1)/p^t$, $t_2 = t_{m,q}$.

(a) *If $3 | m$ and $t_2 = 0$ let $t_1 = [1 + 3t/2]$.*

(b) *If $3 \nmid m$ or $t_2 > 0$ let $t_1 = t$.*

Proof. (a) If $3 | m$ and $t_2 = 0$, let $l = p^{t_1 - t}$. Note that $2(t_1 - t) > t$, so $p^{2(t_1-t)} \nmid q^p - q$ or else, by Lemma 1, $p | p^{2t_1 - 3t} | m$, contrary to the definition of m. Let $n = p^t$. Then $u = p^{t_1} q^{t_2} = p^{t_1} = nl$. By Theorem 2(a), $pq | x$ (or y, or z).

(b) If $3 \nmid m$ or $t_2 > 0$ let $l = q^{t_2}$ and $n = p^{t_1}$. By Theorem 2(b), $q | x$ (say) and since $n > 1$ (because $t_1 = t \geqslant 1$), $p | x$.

Furthermore, if $t_1 \geqslant t \geqslant 1$, since $q | x$ (say) $pq | y + z$, by Theorem 1. ∎

COROLLARY 2. *Let $p \geqslant 3$. There exists an integer $t = t(p)$, $1 \leqslant t \leqslant t_{p-1,p}$, such that if x, y, z are non-zero integers satisfying the equation $x^{p^t} + y^{p^t} + z^{p^t} = 0$, then $p \mid xyz$.*

Proof. By Lemma 2, $t_{p-1,p} \geqslant 1$. Let $l = p^{t_{p-1,p}}$, $n = 1$, $q = p$ and $u = nl = l$.

Then the result follows immediately from Theorem 2, (b). ∎

This corollary was originally proved by Maillet [10] with very different methods, involving the theory of cyclotomic fields. In fact, this is the first proof by elementary methods. References to other proofs of this corollary may be found in [12], pages 205–206.

COROLLARY 3. *There exists an infinite sequence of pairwise relatively prime exponents, which may be taken, for example, to be prime-powers, such that the first case of Fermat's Last Theorem is true for each such exponent.*

Proof. This follows at once from Corollary 2. ∎

It should be noted that using Faltings' theorem [5], it is possible to obtain stronger forms of Corollaries 1, 2 and 3.

We recall that, according to Faltings' theorem, for every $n \geqslant 3$ there exist only finitely many triples of pairwise relatively prime integers $x, y, z \neq 0$, such that $x^n + y^n = z^n$.

In [6], Filaseta showed that for every $n \geqslant 3$ there exists an integer $M(n) > 0$ such that if $m > M(n)$ then there does not exist integers $x, y, z \neq 0$, such that $x^{mn} + y^{mn} = z^{mn}$.

Choosing t_1, t_2, t such that $p^{t_1 - t} q^{t_2} > M(p)$, $p^{t-1} > M(p)$ we obtain the following consequence of Filaseta's result:

COROLLARY 1′. *Let $p \geqslant 3$, q be primes such that $p \mid q-1$. There exist integers $t_1 \geqslant 1$, $t_2 > 0$ such that if $u = p^{t_1} q^{t_2}$, then there does not exist non-zero integers x, y, z such that $x^u + y^u + z^u = 0$.*

COROLLARY 2′. *Let $p \geqslant 3$ be a prime. There exists an integer $t \geqslant 1$ such that there does not exist non-zero integers x, y, z with $x^{p^t} + y^{p^t} + z^{p^t} = 0$.*

Once more, from Corollary 2′, it follows:

COROLLARY 3′. *There exists an infinite sequence of pairwise relatively prime exponents, which may be taken for example to be prime powers, such that Fermat's Last Theorem is true for each such exponent.*

It is however important to stress that, contrary to the numbers t_1, t_2, t appearing in Corollaries 1, 2, those appearing in Corollaries 1′, 2′ are not effectively computable.

COROLLARY 4. *Let m be an even integer, not a multiple of 3, and t be an integer, $t \geqslant 1$. If $p \geqslant 3$ and $q = mp^t + 1$ are primes such that $q \notin S(m)$ and $p \nmid m$;*

and x, y, z are non-zero integers such that $x^{p^t}+y^{p^t}+z^{p^t}=0$, then pq divides $x+y$ (or $z+x$, or $z+y$).

Proof. Since $q \notin S(m)$ then $t_{m,q}=0$. Let $t_2=0$, $t_1=t=v_p(q-1)$ and $u=p^t$ so, by Corollary 1, $pq \mid x+y$ (or $x+z$, or $y+z$). ∎

Taking $t=1$ in the preceding corollary, we obtain a form of the classical Sophie Germain's theorem; due to Krasner [9]:

COROLLARY 5. *Let m be an even integer, not a multiple of 3. If $p \geqslant 3$ and $q=mp+1$ are primes such that $q \notin S(m)$ and $p \nmid m$; and x, y, z are non-zero integers such that $x^p+y^p+z^p=0$ then pq divides $x+y$ (or $x+z$ or $y+z$).*

Using Corollary 5 and a recent improvement of the Brun–Titchmarsh Theorem, due to Fouvry [7], Adleman and Heath-Brown [2] have shown that $(\mathrm{FLT1})_p$ holds for infinitely many primes p.

COROLLARY 6. *Let m be an even integer, not a multiple of 3. Let q be any prime, such that $q \equiv 1 \pmod m$, $n=(q-1)/m$ is odd and $q > \max\{3^{\varphi(m)}, m^2\}$. If x, y, z are non-zero integers such that $x^n+y^n+z^n=0$ then* $\gcd(n, xyz) \geqslant 3$.

Proof. We have $(q-1)^2/n^2=m^2 \leqslant q-1$ so $n^2 \geqslant q-1$; since n is odd, $n^2 > q-1$, so $n^2 \nmid q-1$. Also $q > 3\varphi(m)$, so that $\varphi(m)\log 3/\log q < 1$ and, therefore, by Lemma 3, $t_{m,q}=0$. It follows from Theorem 2(b), taking $l=1$, that there exists a prime p dividing n and xyz; since p must be odd, we have $\gcd(n, xyz) \geqslant 3$. ∎

Using Corollary 6 and the Siegel–Walfisz Theorem, Ankeny and Erdős [3] showed that the set of exponents n, for which $(\mathrm{FLT1})_n$ is true, has density one.

COROLLARY 7. *Let m be a multiple of 6, $t \geqslant 1$ and $t_1=[1+3t/2]$. If $p \geqslant 3$ and $q=mp^t+1$ are primes such that $q \notin S(m)$, $p \nmid m$; and x, y, z are non-zero integers such that $x^{p^{t_1}}+y^{p^{t_1}}+z^{p^{t_1}}=0$ then $pq \mid x+y$ (or $x+z$, or $y+z$).*

Proof. Since $q \notin S(m)$ and $q \equiv 1 \pmod m$ then $t_{m,q}=0$. Let $t_2=0$, $t_1=[1+3t/2] \geqslant t$; so, by Corollary 1, $pq \mid x+y$ (or $x+z$, or $y+z$). ∎

COROLLARY 8. *Let m be a multiple of 6. If $p \geqslant 3$ and $q=mp+1$ are primes such that $q \notin S(m)$, $p \nmid m$; and x, y, z are non-zero integers such that $x^{p^2}+y^{p^2}+z^{p^2}=0$ then $pq \mid x+y$ (or $x+z$, or $y+z$).*

Proof. We use Corollary 7 with $t=1$ so that $t_1=[1+3/2]=2$. ∎

Corollaries 7 and 8 are the first such results with m divisible by 6. A subject for further research would be to reduce the exponent in Corollary 8 to p. However, that does not seem possible with the methods used here.

5. Some computations. It is important to determine $S(m)$, where m is even. This is relatively easy when m is small. Thus

$$S(6)=\{7\},$$
$$S(12)=\{13\},$$
$$S(18)=\{19, 37, 73\}.$$

From these computations and Corollary 8, we obtain:

COROLLARY 9. *If $p \geqslant 3$ and $q = 6p+1$ (or $12p+1$, or $18p+1$) are prime and x, y, z are non-zero integers such that $x^{p^2}+y^{p^2}+z^{p^2} = 0$, then $p|xyz$.*

Proof. For $p = 3$, use Corollary 5 with $m = 2$. If $p \geqslant 5$ (and $m = 6$, 12 or 18) $p \nmid m$ and $q = mp+1 \notin S(m)$. So, by Corollary 8, p divides $x+y$ (or $x+z$, or $y+z$) and thus $p|z$ (or y or x). ∎

In the next result we shall use a theorem in Ireland and Rosen ([8], p. 98) on Fermat's congruence, to conclude that certain primes belong to $S(m)$.

Let q be an odd prime, F_q be the field with q elements, and

$$P = \#\{\text{projective solutions of } X^n+Y^n+Z^n = 0 \text{ in } F_q\}.$$

Then

$$|P-(q+1)| \leqslant (n-1)(n-2)\sqrt{q}.$$

PROPOSITION 1. *Let m and n be positive integers such that $m \geqslant n^3-6n^2+17n-3$. If $q = mn+1$ is prime then $q \in S(m)$.*

Proof. Choose r to be an integer, $0 \leqslant r < q$, of order m (mod q). Define a map E: $Z \to Z_m$ as follows. For $x \in Z$ let j be the unique integer, $0 \leqslant j < m$, such that $x^n \equiv r^j \pmod q$. Then $E(x) = j$.

Let

$$N = \#\{(x, y) |\ 1 \leqslant x, y \leqslant q-1, (E(x), E(y)) \notin T_m, q|1+x^n+y^n\}$$

and

$$N' = \#\{(x, y) |\ 1 \leqslant x, y \leqslant q-1, (E(x), E(y)) \in T_m, q|1+x^n+y^n\}.$$

We have

$$P = N+N'+\#\{\text{projective solutions } (x, y, z) \text{ of } X^n+Y^n+Z^n = 0 \text{ in } F_q, \text{ with } x, y \text{ or } z \text{ equal to } 0\}.$$

Thus, by Lemma 2,

$$P \leqslant N+2n^2+3n.$$

Hence

$$N \geqslant P-2n^2-3n \geqslant q+1-(n-1)(n-2)\sqrt{q}-2n^2-3n$$

and

$$N-1 \geqslant q-(n-1)(n-2)\sqrt{q}-(2n^2+3n).$$

Since

$$m \geqslant n^3-6n^2+17n-3,$$

$$q = mn+1 \geqslant n^4-6n^3+17n^2-3n+1 \geqslant n^4-6n^3+17n^2-6n+4$$

$$= (n-1)^2(n-2)^2+2(2n^2+3n).$$

The discriminant of the polynomial

$$F(T) = T^2-(n-1)(n-2)\,T-(2n^2+3n)$$

is

$$\delta = (n-1)^2(n-2)^2+4(2n^2+3n) > 0.$$

If

$$A = (n-1)(n-2), \qquad B = 2n^2+3n$$

then

$$A^2+2B \geqslant A\sqrt{A^2+4B} = A\sqrt{\delta}$$

so

$$\begin{aligned} 4q \geqslant 4(A^2+2B) &= A^2+(A^2+4B)+2(A^2+2B) \\ &\geqslant A^2+\delta+2A\sqrt{\delta} = (A+\sqrt{\delta})^2 \end{aligned}$$

so that

$$\sqrt{q} \geqslant (A+\sqrt{\delta})/2.$$

Therefore

$$N-1 \geqslant F(\sqrt{q}) \geqslant 0$$

and this concludes the proof. ∎

For m even, define

$$N_m = \prod_{\substack{0\leqslant i,j\leqslant m-1 \\ (i,j)\notin T_m}} (1+\xi^i+\xi^j),$$

so $N_m \neq 0$. Note that, for every $(i,j)\notin T_m$, the conjugates of $1+\xi^i+\xi^j$ (in the extension $Q(\xi^h)|Q$, or in the extension $Q(\xi^h+\xi^{-h})|Q$ – see the definition of $N_{m,i,j}$) are non-zero (else $\varphi_m(x)|1+x^i+x^j$) so that $N_{m,i,j}$ divides N_m.

Now we show:

LEMMA 7. (i) *If q is a prime and $q \equiv 1 \pmod m$ then $q\in S(m)$ if and only if q divides N_m.*

(ii) $\#\{q \text{ prime}|\ q\in S(m)\} \leqslant m^2 \log 3/\log(m+1)$.

Proof. (i) If $q\in S(m)$ there exist $(i,j)\notin T_m$, with $0\leqslant i,j\leqslant m-1$, such that q divides $N_{m,i,j}$. By the above remark, q divides N_m.

Conversely, suppose q divides N_m. Since N_m divides $\prod_{\substack{0\leqslant i,j\leqslant m-1 \\ (i,j)\notin T_m}} N_{m,i,j}$, there exist $(i,j)\notin T_m$ such that q divides $N_{m,i,j}$. By the hypothesis $q \equiv 1 \pmod m$, so that $q\in S(m)$.

(ii) Let $v = \#\{q \text{ prime}|\ q\in S(m)\}$. If $q\in S(m)$, then $q\equiv 1 \pmod m$, so

$q \geqslant m+1$. Also by (i), q divides N_m. Therefore $\prod_{q \in S(m)} q$ divides N_m. Hence

$$(m+1)^v \leqslant \prod_{q \in S(m)} q \leqslant |N_m| \leqslant 3^{m^2}.$$

We conclude that $v \leqslant m^2 \log 3/\log(m+1)$. ∎

The computation of N_m and of $N_{m,i,j}$ (for $(i,j) \notin T_m$) is laborious when m is not very small.

If $3 \nmid m$ (hence $T_m = \emptyset$) Wendt [14] noted that N_m is the determinant of a circulant matrix; however, if $3|m$, the corresponding circulant is zero.

We shall recall Wendt's result, modifying the definition when $3|m$, so that, in all cases, it is equal to N_m.

If $F(X) = a_0 + a_1 X + \ldots + a_{m-1} X^{m-1}$, it is well known that the determinant of the circulant with top row $a_0, a_1, \ldots, a_{m-1}$, is

$$\det \begin{vmatrix} a_0 & a_1 & \ldots & a_{m-1} \\ a_{m-1} & a_0 & \ldots & a_{m-2} \\ \ldots & \ldots & \ldots & \ldots \\ a_1 & a_2 & \ldots & a_0 \end{vmatrix} = \prod_{i=0}^{m-1} F(\xi^i).$$

The Wendt determinant W_m is the determinant obtained from the circulant defined with the coefficients of $(1+X)^m - X^m$. So

$$W_m = \prod_{i=0}^{m} [(1+\xi^i)^m - \xi^{im}] = \prod_{i=0}^{m} [(1+\xi^i)^m - 1].$$

As it is known, and easy to show, $W_m = 0$ if and only if 6 divides m.

So, if $6|m$ we shall define a modified Wendt determinant still denoted W_m. When $6|m$, X^2+X+1 divides $(1+X)^m - X^m$; so let W_m be the determinant obtained from the circulant defined with the coefficients of the polynomial

$$F_m(X) = \frac{(1+X)^m - X^m}{1+X+X^2}.$$

We prove:

LEMMA 8. (i) *If* $3 \nmid m$ *then* $N_m = W_m$.

(ii) *If* $3|m$ *then* $N_m = m^2 W_m$.

(iii) *If* q *is a prime,* $q \equiv 1 \pmod m$ *then* $q \in S(m)$ *if and only if* q *divides* W_m.

Proof. (i) If $3 \nmid m$ then $T_m = \emptyset$ so

$$N_m = \prod_{i,j=0}^{m-1} (1+\xi^i+\xi^j) = \prod_{i=0}^{m-1} [(1+\xi^i)^m - 1] = W_m.$$

(ii) If $3|m$ then $T_m = \{(m/3, 2m/3), (2m/3, m/3)\}$. Now

$$N_m = \prod_{\substack{0 \leqslant i,j \leqslant m-1 \\ (i,j) \notin T_m}} (1+\xi^i+\xi^j)$$

$$= \prod_{i=0}^{m-1} \prod_{j \neq m/3, 2m/3} (1+\xi^i+\xi^j) \cdot \prod_{i \neq 2m/3} (1+\xi^i+\xi^{m/3}) \cdot \prod_{i \neq m/3} (1+\xi^i+\xi^{2m/3})$$

$$= \prod_{i=0}^{m-1} \frac{(1+\xi^i)^m - 1}{(1+\xi^i)^2 - (1+\xi^i)+1} \cdot \prod_{i \neq 2m/3} (\xi^{2m/3} - \xi^i) \cdot \prod_{i \neq m/3} (\xi^{m/3} - \xi^i)$$

$$= \prod_{i=0}^{m-1} \frac{(1+\xi^i)^m - 1}{\xi^{2i}+\xi^i+1} \cdot \frac{X^m-1}{X-\xi^{2m/3}}\bigg|_{X=\xi^{2m/3}} \cdot \frac{X^m-1}{X-\xi^{m/3}}\bigg|_{X=\xi^{m/3}}$$

$$= \prod_{i=0}^{m-1} F_m(\xi^i) \cdot \sum_{j=0}^{m-1} X^{m-1-j} \xi^{(2m/3)j}\Big|_{X=\xi^{2m/3}} \cdot \sum_{j=0}^{m-1} X^{m-1-j} \xi^{(m/3)j}\Big|_{X=\xi^{m/3}}$$

$$= W_m \cdot m\xi^{(m-1)(2m/3)} \cdot m\xi^{(m-1)(m/3)} = m^2 W_m.$$

(iii) By Lemma 7(i), $q \in S(m)$ if and only if $q | N_m$. If $3 \nmid m$, this is equivalent to $q | W_m$. If $3 | m$, this is equivalent to $q | m^2 W_m$. But if $q | m$ then $q \leqslant m \leqslant q-1$, which is absurd. So $q | W_m$. ∎

The authors would like to thank Dr. Paulo Ribenboim for his comments and help in the preparation of this paper.

References

[1] N. Abel, *Extraits de quelques lettres à Holmboe, Copenhague, l'an* $3\sqrt{6064321219}$ *(en comptant la fraction decimale)*; in: *Oeuvres complètes*, 2nd ed., vol. II, Grondahl, Christiania 1881, pp. 254–255.

[2] L. M. Adleman and D. R. Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math. 79 (1985), pp. 409–416.

[3] N. C. Ankeny and P. Erdős, *The insolubility of classes of diophantine equations*, Amer. J. Math. 76 (1954), pp. 488–496.

[4] T. Azuhata, *On Fermat's Last Theorem*, Acta Arith. 45 (1985), pp. 19–27.

[5] G. Faltings, *Endlichkeitssätze für Abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), pp. 349–366.

[6] M. Filaseta, *An application of Faltings' result to Fermat's Last Theorem*, C. R. Acad. Sci. Canada 6 (1984), pp. 31–32.

[7] E. Fouvry, *Théorème de Brun–Titchmarsh. Application au Théorème de Fermat*, Invent. Math. 79 (1985), pp. 383–407.

[8] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York 1982.

[9] M. Krasner, *A propos du critère de Sophie Germain-Furtwängler, pour le premier cas du théorème de Fermat*, Mathematica Cluj 16 (1940), pp. 109–114.

[10] E. Maillet, *Sur l'équation indéterminée* $ax^{\lambda^t} + by^{\lambda^t} = cz^{\lambda^t}$, Assoc. Française Avancement Science, St. Etienne, II, 26 (1897), pp. 156–168.

[11] F. Pollaczek, *Über den grossen Fermatschen Satz*, Sitzungsber. Akad. d. Wien, Abt IIa, 126 (1917), pp. 45–59.

[12] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York 1979.
[13] G. Terjanian, *Sur l'équation* $x^{2p}+y^{2p}=z^{2p}$, C. R. Acad. Sci. Paris 285 (1977), pp. 973–975.
[14] E. Wendt, *Arithmetischen Studien über den letzten Fermatschen Satz, welcher aussagt dass die Gleichung* $a^n=b^n+c^n$ *für* $n>2$, *in ganzen Zahlen nicht auflösbar ist*, J. Reine Angew. Math. 113 (1894), pp. 335–346.

Received on 25.3.1986
and in revised form on 24.7.1986 (1609)