Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 27, No. 1, September 1987
Printed in Belgium

Sophie Germain's Theorem for Prime Pairs p, $6p+1$

ANDREW GRANVILLE

Department of Mathematics and Statistics,
Queen's University, Kingston, Ontario, Canada K7L 3N6

Communicated by H. Zassenhaus

Received August 19, 1985; revised April 28, 1986

In 1823, Sophie Germain (*Mem. Acad. Sci. Inst. France* **6** (1823), 1–60) showed that if p, $2p+1$ are both odd primes then the so-called "First Case" of Fermat's Last Theorem holds for p. This was extended by Legendre, Wendt, Vandiver, Denes, and others to prime pairs p, $mp+1$, where $6 \nmid m$ and p is sufficiently large (depending on m). The cases where 6 divides m are fraught with an inescapable technical difficulty, and, as we shall see in this paper, it requires quite sophisticated techniques to even find a partial resolution for prime pairs p, $6p+1$.

INTRODUCTION

The first case of Fermat's Last Theorem is said to be false for prime p, if there exist integers X, Y, Z such that

$$X^p + Y^p + Z^p = 0 \qquad \text{and} \qquad p \nmid XYZ\cdots. \tag{1}_p$$

Throughout this paper we use the following notation: Let p and $q = 6p+1$ be odd primes ($p \neq 3$ or 7). Thus we may assume that $q \equiv 3 \pmod 4$, $q \equiv 4$ or $7 \pmod 9$, and $q \not\equiv 1 \pmod 7$.

Let $\omega = (-1+\sqrt{-3})/2$, a root of $\omega^2+\omega+1=0$ in C.

We choose e to be any integer of order 6 (mod q). Note that if $t \in Q$ with $v_q(t)=0$ (v_q is the q-adic valuation) then there exists an integer i, $0 \leqslant i \leqslant 5$, such that $t^p \equiv e^i \pmod q$.

Let C be the least positive residue of $(q-1)/3 \pmod 3$ and A and B be integers for which $4q = A^2 + 27B^2$ and $A \equiv 1 \pmod 3$. Then A is uniquely defined and B is uniquely defined up to sign (see [6, Prop. 8.3.2]).

Let $\pi_1 = (A+3B)/2 + 3B\omega$, which is prime in $Q(\omega)$. Note that $q = \pi_1 \cdot \bar{\pi}_1$. Let $\pi_2 = -1-3\omega = (-\omega)^2(3+2\omega)$, which is prime in $Q(\omega)$ also. Note that $7 = \pi_2 \cdot \bar{\pi}_2$. Let α be the integer, $0 < \alpha < q$, such that $\alpha \equiv 1+2\omega \equiv \sqrt{-3} \pmod{\pi_1}$.

0022-314X/87 $3.00

Now suppose γ and $\rho \in Q(\omega)$ with ρ prime and $N\rho \nmid N\gamma$, $N\rho \neq 2$ or 3. Define

$$\left[\frac{\gamma}{\rho}\right]_2 = (-1)^m, \qquad \text{where} \qquad \gamma^{(N\rho-1)/2} \equiv (-1)^m \pmod{\rho},$$

and

$$\left[\frac{\gamma}{\rho}\right]_3 = \omega^m, \qquad \text{where} \qquad \gamma^{(N\rho-1)/3} \equiv \omega^m \pmod{\rho}.$$

If $\gamma \in Q$, let $(\gamma/N\rho) = [\gamma/\rho]_2$. This definition coincides with that of the Legendre symbol.

We shall prove the following theorem:

THEOREM 1. *Let p, q, A, B, and C be as above; determine the sign of B by taking $B \equiv 1 \pmod 4$, if A is odd and $B \equiv q+3 \pmod 8$, if A is even.*

If the first case of Fermat's Last Theorem is false for p then either $7 \mid A+B+C$ and $3 \mid B-1$ or $7 \mid A+B+2C$ and $3 \mid B-2$.

We will have need of the following two theorems, each of which rely on sophisticated techniques. In each we assume that there exist solutions X, Y, Z to $(1)_p$.

FURTWÄNGLER'S THEOREM [4]. *If $r \mid XYZ$ then $r^{p-1} \equiv 1 \pmod{p^2}$.*

MCDONNELL'S THEOREM [8]. *If $r \mid X^2 - YZ \cdot Y^2 - XZ \cdot Z^2 - XY$ then $r^{p-1} \equiv 1 \pmod{p^2}$.*

(McDonnell's Theorem is usually stated with the added criteria that $p \nmid XY+YZ+ZX$—however, this was always shown to be true by Pollaczek [9].)

For a complete introduction to these theorems, and those mentioned in the abstract, the reader is referred to Ribenboim [10].

LEMMA 1. *If a, b, and c are integers for which*

$$a^p + b^p + c^p \equiv 0 \pmod q$$

then either q divides abc or there exists an integer u, of order 3 (mod q), such that

$$b^p/a^p \equiv c^p/b^p \equiv u \pmod q.$$

Proof. Suppose that q does not divide abc. As $(b^p/a^p)^6 \equiv (c^p/a^p)^6 \equiv 1 \pmod q$ there exists integers i and j, $0 \leqslant i, j \leqslant 5$, such that $b^p/a^p \equiv e^i \pmod q$ and $c^p/a^p \equiv e^j \pmod q$.

Hence $1+e^i+e^j \equiv (a^p+b^p+c^p)/a^p \equiv 0 \pmod q$.

Now, if $(i, j) \neq (2, 4)$ or $(4, 2)$ then

$$-3^4 \cdot 7^3 \cdot 4^3 \equiv \prod_{\substack{i=0 \\ (i,j)\neq(2,4) \text{ or } (4,2)}}^{5} \prod_{j=0}^{5} 1+e^i+e^j \equiv 0 \pmod q.$$

Thus $q = 6p+1 = 3$ or 4 or 7 which is clearly impossible. So $(i, j) = (2, 4)$ or $(4, 2)$. Let $u = e^i$. Then u has order 3 $\pmod q$ and $b^p/a^p \equiv c^p/b^p \equiv u \pmod q$.

PROPOSITION 1. *If* $(1)_p$ *has solutions then there exist integers* a *and* b, *with* $a^2 \equiv -3 \pmod q$ *and* $b^6 \equiv 1 \pmod q$ *such that* $X \equiv b/2 \pmod q$, $Y \equiv ab/2 \pmod q$, *and* $Z \equiv -b(a+2)/2 \pmod q$.

Proof. We first note that q does not divide XYZ else, by Furtwängler's Theorem, $1+6p = q \equiv q^p \equiv 1+6p^2 \equiv 1 \pmod{p^2}$, so that $p \mid 6$, which is impossible.

Similarly q does not divide $X^2 - YZ \cdot Y^2 - XZ \cdot Z^2 - XY$ by use of McDonnell's Theorem.

Barlow [1] established that there exist integers r, s, t such that

$$X+Y = t^p, \qquad X+Z = s^p, \qquad \text{and} \qquad Y+Z = r^p.$$

As $q \nmid rst$ (else $q \mid XYZ$), there exist integers i and j, $0 \leqslant i, j \leqslant 5$, such that

$$(s/r)^p \equiv e^i \pmod q \qquad \text{and} \qquad (t/r)^p \equiv e^j \pmod q.$$

Therefore

$$2X/r^p \equiv e^i + e^j - 1 \pmod q, \qquad 2Y/r^p \equiv 1 + e^j - e^i \pmod q,$$

and

$$2Z/r^p \equiv e^i + 1 - e^j \pmod q.$$

Now $i \neq 0$, $j \neq 0$, and $i \neq j$ else $X \equiv Y \pmod q$, $X \equiv Z \pmod q$, or $Y \equiv Z \pmod q$ and, by Lemma 1, there would exist an integer u, of order 3 $\pmod q$, such that $u \equiv 1 \pmod q$, which would imply that q divides 3.

Also i and j are not equal to 1 and 2, or 1 and 5, or 4 and 5, else $q \mid XYZ$.

We are left with one case, namely $i = 1$, $j = 4$, noting that we do not affect the methods used by interchanging X, Y, and Z or mapping $e \to e^5$.

Let $b \equiv (-r)^p \pmod q$ so that $b^6 \equiv 1 \pmod q$, and $a \equiv 2e - 1 \pmod q$ so that

$$a^2 \equiv 4e^2 - 4e + 1 \equiv -3 + 4(1 + e^2 + e^4) \equiv -3 \pmod q.$$

Then $X \equiv b/2 \pmod q$, $Y \equiv ab/2 \pmod q$, and $Z \equiv -(a+2)b/2 \pmod q$.

COROLLARY 1. *If* $(1)_p$ *has solutions then there exists an integer* a *such that* q *divides* a^2+3 *and* q *divides* $1+a^p-(a+2)^p$.

Corollary 1 follows immediately from Proposition 1. We now prove a preparatory, technical lemma.

LEMMA 2. (i) $(\alpha/q)=(AB/q)$.

(ii) *If* B *is odd then* $B\equiv(\alpha/q) \pmod 4$. *If* B *is even then* $B\equiv 2(2\alpha/q) \pmod 8$.

(iii) $((2+\alpha)/q)=(\alpha/q)((A+B)/7)$.

(iv) $[3/\pi_1]_3=\omega^{2B}$.

(v) $[(2+\alpha)/\pi_1]_3\cdot[3/\pi_1]_3^2=\omega^{B+C}[((A+B)/2)/\pi_2]_3$.

Proof. (i) $[3B\alpha/\pi_1]_2=[(3B+6B\omega)/\pi_1]_2=[-A/\pi_1]_2$. As A, B, and α are integers, and $(-3/q)=(q/3)=1$, we have $(\alpha/q)=(3B/q)(3B\alpha/q)=(3B/q)(-A/q)=(AB/q)$.

(ii) Let $A=(-1)^{a_1}\cdot 2^{a_2}\cdot A_3$ and $B=(-1)^{b_1}\cdot 2^{b_2}\cdot B_3$, where A_3, $B_3>0$ and $2\nmid A_3\cdot B_3$. Now, if the prime r divides A_3, then

$$\left(\frac{r}{q}\right)=(-1)^{(r-1)/2}\left(\frac{q}{r}\right)=(-1)^{(r-1)/2}\left(\frac{4q}{r}\right)$$

$$=(-1)^{(r-1)/2}\left(\frac{27B^2}{r}\right)=(-1)^{(r-1)/2}\left(\frac{3}{r}\right)=\left(\frac{r}{3}\right).$$

Therefore $(A_3/q)=(A_3/3)=(A/3)\cdot(-1)^{a_1+a_2}=(-1)^{a_1+a_2}$ as $A\equiv 1 \pmod 3$.

Thus $(A/q)=(-1)^{a_2}(2/q)^{a_2}$.

Now, if prime r divides B_3, then

$$\left(\frac{r}{q}\right)=(-1)^{(r-1)/2}\left(\frac{4q}{r}\right)=(-1)^{(r-1)/2}\left(\frac{A^2}{p}\right)=(-1)^{(r-1)/2}.$$

Suppose that $B_3=\prod_{r\mid B_3} r^{a_r}$. Then

$$\left(\frac{B_3}{q}\right)=\prod_{r\mid B_3}\left(\frac{r}{q}\right)^{a_r}=(-1)^{\sum_{r\mid B_3} a_r\,(r-1)/2}=(-1)^{(B_3-1)/2}.$$

Thus $(B/q)=(-1)^{b_1}(2/q)^{b_2}\cdot(-1)^{(B_3-1)/2}\equiv(-1)^{b_1}(2/q)^{b_2}B_3 \pmod 4$. Therefore, by (i)

$$B/2^{b_2}\equiv(-1)^{b_1}\cdot B_3\equiv\left(\frac{2}{q}\right)^{b_2}\left(\frac{B}{q}\right)$$

$$\equiv\left(\frac{\alpha}{q}\right)\left(\frac{2}{q}\right)^{a_2+b_2}(-1)^{a_2} \pmod 4.$$

Now, if $2 \nmid B$, $a_2 = b_2 = 0$, so that $B \equiv (\alpha/q) \pmod 4$. If $2 \mid B$ then, as $q \equiv 3 \pmod 4$, $b_2 = 1$ so that

$$B \equiv (-1)^{a_2} \left(\frac{2}{q}\right)^{a_2} \cdot 2 \cdot \left(\frac{2\alpha}{q}\right) \pmod 8.$$

Now, if $q \equiv 3 \pmod 8$, then $B \equiv 2 \cdot (2\alpha/q) \pmod 8$.

Note that $(A/2)^2 \equiv q - 3(B/2)^2 \equiv 0 \pmod 8$, so that $4 \mid A/2$. Therefore

$$(A+3B)/2 \equiv 0 + 3.\ (2\alpha/q) \equiv (\alpha/q) \pmod 4 \ldots. \tag{2i}$$

If $q \equiv 7 \pmod 8$, then $(A/2)^2 \equiv 7 - 3 \cdot 1^2 \equiv 4 \pmod 8$. Thus $A/2 \equiv 2 \pmod 4$, so that $a_2 = 2$ and $B \equiv 2(2\alpha/q) \pmod 8$. Note that

$$(A+3B)/2 \equiv 2 - (\alpha/q) \equiv (\alpha/q) \pmod 4 \ldots. \tag{2ii}$$

(iii) Dörrie [3, pp. 68–71] gave the following law for quadratic reciprocity in $Q(\omega)$: If ρ_1 and ρ_2 are primes in $Q(\omega)$, but not in Q, with $N\rho_i = p_i$ and t_i an integer, $0 \leqslant t_i \leqslant 5$ such that $(-\omega)^{t_i} \rho_i \equiv \omega + 1$ or $\omega - 1 \pmod 4$ for each $i = 1, 2$ then

$$\left[\frac{\rho_1}{\rho_2}\right]_2 \left[\frac{\rho_2}{\rho_1}\right]_2 = (-1)^{(p_1+1+2t_2)(p_2+1+2t_1)/4 + (t_1+1)(t_2+1)}.$$

Now $\pi_2 = -1 - 3\omega \equiv \omega - 1 \pmod 4$ and suppose that $(-\omega)^t \pi_1 \equiv \omega \pm 1 \pmod 4$. Then

$$\left[\frac{\pi_1}{\pi_2}\right]_2 \left[\frac{\pi_2}{\pi_1}\right]_2 = (-1)^{t+1}.$$

But

$$\left[\frac{\pi_1}{\pi_2}\right]_2 = \left[\frac{(A+3B)/2 + 3B\omega}{-1-3\omega}\right]_2 = \left[\frac{(A+B)/2}{-1-3\omega}\right]_2$$

$$= \left(\frac{(A+B)/2}{7}\right) = \left(\frac{A+B}{7}\right) \qquad \text{as} \qquad \left(\frac{2}{7}\right) = 1.$$

Therefore

$$\left(\frac{2+\alpha}{q}\right) = \left[\frac{2+\alpha}{\pi_1}\right]_2 = \left[\frac{\pi_2}{\pi_1}\right]_2 = (-1)^{t+1} \left[\frac{\pi_1}{\pi_2}\right]_2$$

$$= (-1)^{t+1} \left(\frac{A+B}{7}\right).$$

Now, if $(-\omega)^t \pi_1 \equiv \omega + \varepsilon \pmod 4$, where $\varepsilon = 1$ or -1, then

$$(-\omega)^{-t} \bar{\pi}_1 \equiv \omega^2 + \varepsilon \pmod 4.$$

Thus $-1 \equiv q = \pi_1 \cdot \bar{\pi}_1 \equiv (\omega+\varepsilon)(\omega^2+\varepsilon) = 2+\varepsilon(\omega+\omega^2) = 2-\varepsilon \equiv \varepsilon \pmod 4$, so that $\varepsilon = -1$.

If $2 \nmid B$,

$$(-\omega)(2-\omega) \equiv (-\omega)^4(2+\omega) \equiv (-\omega)^3(1-\omega)$$
$$\equiv (-\omega)^0(-1+\omega) \equiv \omega - 1 \pmod 4.$$

In each case, $(-1)^{t+1} \equiv -3B \equiv B \equiv (\alpha/q) \pmod 4$ by (ii). If $2 \mid B$,

$$(-\omega)^2(-1+2\omega) \equiv (-\omega)^5(1+2\omega) \equiv \omega - 1 \pmod 4,$$

so that

$$(-1)^{t+1} \equiv (A+3B)/2 \equiv \left(\frac{\alpha}{q}\right) \pmod 4 \qquad \text{by (2).}$$

Thus, in each case,

$$\left(\frac{2+\alpha}{q}\right) = (-1)^{t+1}\left(\frac{A+B}{7}\right) = \left(\frac{\alpha}{q}\right)\left(\frac{A+B}{7}\right).$$

(iv) and (v). Ireland and Rosen [6, pp. 112–114] give the following laws of cubic reciprocity in $Q(\omega)$: If ρ_1 and ρ_2 are prime in $Q(\omega)$, with ρ_1, $\rho_2 \notin Q$, and $\rho_1 \equiv \rho_2 \equiv 2 \pmod 3$, then

$$\left[\frac{\rho_1}{\rho_2}\right]_3 = \left[\frac{\rho_2}{\rho_1}\right]_3.$$

If $\rho_1 = c + d\omega$ then $[(1-\omega)/\rho_1]_3 = \omega^{2(c+1)/3}$. Now, note that $A \equiv A^4 \equiv (4q)^2 \equiv -2q^2 \equiv -q-1 \pmod 9$, and that $3 = -\omega^2(1-\omega)^2$. Thus

$$\left[\frac{3}{\pi_1}\right]_3 = \left[\frac{-\omega^2(1-\omega)^2}{\pi_1}\right]_3 = \left[\frac{\omega}{\pi_1}\right]_3^2\left[\frac{1-\omega}{\pi_1}\right]_3^2$$
$$= \omega^{2(q-1)/3} \cdot \omega^{2B+2(A+2)/3} = \omega^{2B}.$$

Now $\pi_1 \equiv A/2 \equiv 2 \pmod 3$ and $\pi_2 \equiv -1 \equiv 2 \pmod 3$. Therefore

$$\left[\frac{\pi_2}{\pi_1}\right]_3 = \left[\frac{\pi_1}{\pi_2}\right]_3 = \left[\frac{(A+3B)/2+3B\omega}{-1-3\omega}\right]_3$$
$$= \left[\frac{(A+B)/2}{-1-3\omega}\right]_3 = \left[\frac{(A+B)/2}{\pi_2}\right]_3$$

and so

$$\left[\frac{2+\alpha}{\pi_1}\right]_3 = \left[\frac{3+2\omega}{\pi_1}\right]_3 = \left[(-\omega)^4\frac{\pi_2}{\pi_1}\right]_3$$
$$= \left[\frac{\omega}{\pi_1}\right]_3\left[\frac{\pi_2}{\pi_1}\right]_3 = \omega^C\cdot\left[\frac{(A+B)/2}{\pi_2}\right]_3.$$

Thus

$$\left[\frac{2+\alpha}{\pi_1}\right]_3\left[\frac{3}{\pi_1}\right]_3^2 = \omega^{B+C}\left[\frac{(A+B)/2}{\pi_2}\right]_3.$$

PROPOSITION 2. *The following three statements are equivalent:*

(I) q *divides* $1+\alpha^p-(2+\alpha)^p$.

(II) (i) $(\alpha/q)=1$; (ii) $((2+\alpha)/q)=-1$; (iii) $[3/\pi_1]_3\neq 1$; (iv) $[(2+\alpha)/\pi_1]_3=[3/\pi_1]_3$.

(III) (i) *If* B *is odd,* $B\equiv 1 \pmod 4$; *if* B *is even,* $B\equiv 2(2/q) \pmod 8$; (ii) $((A+B)/7)=-1$; (iii) $3\nmid B$; (iv) $2^{B+C-2}(A+B)^2\equiv 1 \pmod 7$.

Proof. (I) $\leftrightarrow$ (II): There exist integers i, j with $0\leqslant i, j\leqslant 5$, such that

$$\alpha^p\equiv e^i \pmod q \qquad \text{and} \qquad -(2+\alpha)^p\equiv e^j \pmod q.$$

Therefore

$$\left(\frac{\alpha}{q}\right)=\left(\frac{\alpha}{q}\right)^p=\left(\frac{e}{q}\right)^i \qquad \text{and} \qquad \left[\frac{3}{\pi_1}\right]_3^p=\left[\frac{\alpha}{\pi_1}\right]_3^{2p}=\left[\frac{e}{\pi_1}\right]_3^{2i}.$$

Also

$$\left(\frac{2+\alpha}{q}\right)=-\left(\frac{e}{q}\right)^j \qquad \text{and} \qquad \left[\frac{2+\alpha}{\pi_1}\right]_3^p=\left[\frac{-e^j}{\pi_1}\right]_3=\left[\frac{e}{\pi_1}\right]_3^j.$$

So, as $(e/q)=-1$,

$$\left(\frac{\alpha}{q}\right)=1 \qquad \text{and} \qquad \left(\frac{2+\alpha}{q}\right)=-1 \qquad \text{iff} \quad i\equiv j\equiv 0 \pmod 2.$$

As $[e/\pi_1]_3\neq 1$,

$$\left[\frac{3}{\pi_1}\right]_3=\left[\frac{2+\alpha}{\pi_1}\right]_3\neq 1 \qquad \text{iff} \quad j\equiv 2i\not\equiv 0 \pmod 3.$$

Therefore (II) holds iff $(i, j) = (2, 4)$ or $(4, 2)$,

iff there exists an integer u $(u = e^i)$, of order 3 (mod q), such that $\alpha^p \equiv u \pmod q$ and $-(2+\alpha)^p \equiv u^2 \pmod q$,

iff (I) holds (by Lemma 1).

Proof. (II) $\leftrightarrow$ (III): Now (II)(i) holds iff (III)(i) holds, by Lemma 2(ii). By (i), $(\alpha/q) = 1$. So, by Lemma 2(iii), $((2+\alpha)/q) = ((A+B)/7)$. By Lemma 2(iv), $[3/\pi_1]_3 \neq 1$ iff $3 \nmid B$. By Lemma 2(v),

$$\left[\frac{2+\alpha}{\pi_1}\right]_3 = \left[\frac{3}{\pi_1}\right]_3 \quad \text{iff} \quad \omega^{B+C}\left[\frac{(A+B)/2}{\pi_2}\right]_3 = 1$$

$$\text{iff} \quad \omega^{B+C}((A+B)/2)^2 \equiv 1 \pmod{\pi_2}.$$

Now $\omega \equiv -1/3 \equiv 2 \pmod{\pi_2 = -1-3\omega}$, so that $\omega^{B+C}((A+B)/2)^2 \equiv 1 \pmod{\pi_2}$ iff $2^{B+C-2}(A+B)^2 \equiv 1 \pmod{\pi_2}$ iff $2^{B+C-2}(A+B)^2 \equiv 1 \pmod 7$.

Proof of Theorem 1. If $(1)_p$ has solutions X, Y, Z then, by Corollary 1, there exists an integer a such that q divides a^2+3 and $1 + a^p - (a+2)^p$. Choose the sign of B so that $(B/q) = (Aa/q)$. Then, by Lemma 2(i), $a \equiv \alpha \pmod q$.

Now note that, as $q \equiv 3 \pmod 4$, we have $2(2/q) \equiv q+3 \pmod 8$. Thus, by Proposition 2, $B \equiv 1 \pmod 4$ (if B is odd), $B \equiv q+3 \pmod 8$ (if B is even). Also $3 \nmid B$.

By (III)(ii), $(A+B)^3 \equiv -1 \pmod 7$, so by (III)(iv) $(A+B) \equiv (A+B)\cdot(A+B)^2 \cdot 2^{B+C-2} \equiv -2^{B+C+1} \pmod 7$. So

if $B \equiv 1 \pmod 3$ and $C = 1$ then $A+B \equiv -1 \equiv -C \pmod 7$;
if $B \equiv 1 \pmod 3$ and $C = 2$ then $A+B \equiv -2 \equiv -C \pmod 7$;
if $B \equiv 2 \pmod 3$ and $C = 1$ then $A+B \equiv -2 \equiv -2C \pmod 7$;
if $B \equiv 2 \pmod 3$ and $C = 2$ then $A+B \equiv -4 \equiv -2C \pmod 7$.

Note that it is possible to extend Theorem 1 to all pairs n, $q = 6n+1$ where q is prime and $\gcd(n, 2\cdot 3\cdot 7) = 1$. Thus we may state

THEOREM 2. *Suppose that n is a given integer, $\gcd(n, 2\cdot 3\cdot 7) = 1$ with $q = 6n+1$ prime, and X, Y, Z are integers for which*

$$X^n + Y^n + Z^n = 0 \quad \textit{and} \quad \gcd(n, XYZ) = 1. \qquad (1)_n$$

Let A, B, and C be integers such that C is the least positive residue of $(q-1)/3 \pmod 3$, $4q = A^2 + 27B^2$, with $A \equiv 1 \pmod 3$ and $B \equiv 1 \pmod 4$ if A is odd, $B \equiv q+3 \pmod 8$ if A is even.

Then either $3 \mid B-1$ and $7 \mid A+B+C$ or $3 \mid B-2$ and $7 \mid A+B+2C$. $(2)_q$

Note that if 2 divides n then $(1)_n$ has no solutions by Terjanian's theorem [11]; if 3 or 7 divides n then $(1)_n$ has no solutions by Sophie Germain's theorem for $m=2$ or 4, respectively.

Now $\pi=(A+3B)/2+3Bw$ is a prime of $Q(w)$ and $q=\pi\bar{\pi}$.

It is not hard to show that $q\equiv 4$ or 7 (mod 9) and $A\equiv 1$ (mod 3) iff $\pi\equiv 2$ or 5 (mod $3(1+2w)$). Also that $B\equiv 1$ (mod 4) if A is odd, and $B\equiv q+3$ (mod 8) if A is even iff $\pi\equiv 1-w$, $2-w$ or $1+2w$ (mod 4). Finally that

$$q\equiv 1 \text{ (mod 7)} \quad \text{iff} \quad \pi\equiv 1 \text{ (2, 3, 4, 5 or 6) (mod } 1+3w)$$

and

$$\pi\equiv 1 \text{ (4, 5, 2, 3 or 6, respectively) (mod } 2+3w).$$

So Theorem 2 may be rewritten as follows:

THEOREM 2′. *Suppose that π is a prime in $Q(w)$ such that*

(a) $\pi\equiv 2$ *or* 5 (mod $3(1+2w)$)

(b) $\pi\equiv 1-w$, $2-w$ *or* $1+2w$ (mod 4)

(c) *if* $\pi\equiv 1/2/3/4/5/6$ (mod $1+3w$) *then* $\pi\not\equiv 1/4/5/2/3/6$ (*respectively*) (mod $2+3w$).

If $(1)_n$ has solutions where $n=(N_{Q(w)|Q}\pi-1)/6$ then one of the following holds:

(i) $\pi\equiv -1+3w$ (mod 9) and $\pi\equiv 3$ (mod $1+3w$)

(ii) $\pi\equiv -4-3w$ (mod 9) and $\pi\equiv 6$ (mod $1+3w$)

(iii) $\pi\equiv 2+3w$ (mod 9) and $\pi\equiv 6$ (mod $1+3w$)

(iv) $\pi\equiv -1-3w$ (mod 9) and $\pi\equiv 5$ (mod $1+3w$).

Now of the 540 equivalence classes, mod 252, permissible by (a), (b), and (c), only 60 satisfy one of the criteria (i), (ii), (iii), and (iv). By applying the Tchebotareff density theorem (see [2, Theorem 19.18]) we may state the following:

$$\lim_{x\to\infty}\frac{\#\{\text{primes } q\leqslant x:\ q\equiv 7 \text{ or } 31 \text{ (mod } 36),\ q\equiv 1 \text{ (mod } 7);\ q \text{ does not satisfy } (2)_q\}}{\#\{\text{primes } q\leqslant x:\ q\equiv 7 \text{ or } 31 \text{ (mod } 36),\ q\equiv 1 \text{ (mod } 7)\}}=\frac{8}{9}.$$

This is certainly borne out by experimental evidence: Of the 57,356 such primes $q\leqslant 6{,}000{,}000$ only 6,402 satisfy $(2)_q$.

Unfortunately the Tchebotareff density theorem cannot be applied to prime pairs p, $q=6p+1$. However, on computations of all such prime pairs with $p<1{,}000{,}000$ we found that of the 14,443 such primes p, 1615

satisfy the criteria of Theorem 1 (if the Tchebotareff density theorem held we would expect 1605 such primes to satisfy the criteria of Theorem 1).

It has been brought to my attention that J. M. Gandhi [5] claimed to have found an unconditional proof of Sophie Germain's theorem for prime pairs p, $6p+1$; which would evidently be stronger than the main theorem of this paper. In the notice he simply stated the theorem, writing that the main ingredients of his proof were Pollaczek's, Furtwängler's, and MacDonnell's theorems. This leads me to believe that he, in fact, proved only Proposition 1, inadvertently leaving out case (iii). Before his untimely death, Professor Gandhi did, indeed, confide to colleagues that his proof was incomplete.

ACKNOWLEDGMENTS

I thank Dr. K. S. Williams of Carleton University in Ottawa, who kindly outlined much of the proof of Lemma 2; and Greg Fee of the Symbolic Computation Group at Waterloo University for calculating how many primes satisfy the criteria of Theorem 1. I am also indebted to my supervisor, Dr. Paulo Ribenboim, for all the help and encouragement he has given me over the past year.

REFERENCES

1. P. BARLOW, Demonstration of a curious numerical proposition, *J. Nat. Philos. Chem. Arts* **27** (1810), 193–205.
2. H. COHN, "A Classical Invitation to Algebraic Numbers and Class Fields," Springer-Verlag, New York, 1978.
3. H. DÖRRIE, "Das quadratische Reciprocitäsgesetz in quadratischen Zahlkörper mit der Classenzahl 1," Dissertation, Göttingen, 1898.
4. P. FURTWÄNGLER, Letzter Fermatschen Satz und Eisenstein'sches Reziprozitätsgesetz, *Sitzungsber. Akad. Wiss. Wien. Abt. IIa* **121** (1912), 589–592.
5. J. M. GANDHI, On Fermat's Last Theorem, *Notices Amer. Math. Soc.* **21** No. 1 (1974), A–53.
6. K. IRELAND AND M. I. ROSEN, "Elements of Number Theory," Bogden & Quigley, New York, 1972.
7. A. M. LEGENDRE, Recherches sur quelques objects d'analyse indéterminée et particulièrement sur la théorème de Fermat, *Mem. Acad. Sci. Inst. France* **6** (1823), 1–60.
8. J. MACDONNELL, New Criteria associated with Fermat's Last Theorem, *Bull. Amer. Math. Soc.* **36** (1930), 553–558.
9. F. POLLACZEK, Über den großen Fermat'schen Satz, *Sitzungsber. Akad. Wiss. Wien. Abt. IIa* **126** (1917), 45–59.
10. P. RIBENBOIM, "13 Lectures on Fermat's Last Theorem," Springer-Verlag, New York, 1979.
11. G. TERJANIAN, Sur l'équation $X^{2p}+Y^{2p}=Z^{2p}$, *C.R. Acad. Sci. Paris* **285** (1977), 973–975.

Printed by Catherine Press, Ltd., Tempelhof 41, B-8000 Brugge, Belgium