Math. Proc. Camb. Phil. Soc. (1985), 98, 5
Printed in Great Britain

Refining the conditions on the Fermat quotient

BY ANDREW J. GRANVILLE
Trinity College, Cambridge University

(*Received* 10 *July* 1984; *revised* 6 *December* 1984)

The aim of this paper is to establish a result on a family of congruences arising from the Fermat quotient: this result has an interesting application to the Fermat problem. For over 150 years the Fermat problem has been divided into two cases; the First Case being the assertion that for each odd prime p,

$$x^p + y^p + z^p = 0 \quad (p \nmid xyz), \tag{1}$$

has no solution in non-zero integers x, y, z. Kummer's work on ideal numbers led, in 1847, to the complete solution of the Fermat problem for regular primes. His studies also furnished improved criteria for the validity of the First Case, but these criteria still involved the Bernoulli numbers. These were eliminated by Mirmanoff in 1905 by the introduction of the polynomials

$$T + 2^j T^2 + \ldots + (p-1)^j T^{p-1} \quad (0 \leqslant j < p-1);$$

he thereby reduced Kummer's criteria to a family of elementary congruences. Building on Mirmanoff's ideas, Wieferich in 1909 established the elegant result that whenever (1) has solutions,

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

Mirmanoff, Frobenius and a series of authors over the next twenty years generalized this to

$$q^{p-1} \equiv 1 \pmod{p^2} \tag{2}$$

for each prime $q \leqslant 31$*. The integer $(q^{p-1}-1)/p$ is known as the 'Fermat Quotient'.

Recent investigations on Wieferich's criterion, by computational methods, due to Lehmer, have shown that (1) has no solutions for $p < 6 \cdot 10^9$ [4]. Adleman and Heath-Brown [1] and Fouvry [2] have used Sophie Germain's Theorem to show that (1) has no solutions for some unspecified sequence of primes. We shall prove that if (1) does have solutions for *all* sufficiently large primes p, then the criteria (2) may be improved to

$$q^{p-1} \equiv 1 \pmod{p^3}$$

for an *infinite sequence* of primes p. Our method is developed from that of Puccioni [5]: he demonstrated the case $q \not\equiv \pm 1 \pmod 8$ although his argument appears incomplete. The actual result that we establish is as follows.

THEOREM 1. *Suppose that q is a prime such that for all sufficiently large primes p, with $p \equiv 1 \pmod 4$, we have $q^{p-1} \equiv 1 \pmod{p^2}$. Then there is an infinite sequence of primes p such that $q^{p-1} \equiv 1 \pmod{p^3}$.*

In fact we prove a more general theorem: it is to be noted that here we no longer require that every prime p satisfies $q^{p-1} \equiv 1 \pmod{p^2}$, but only a particular infinite sequence.

* Morishima's proof for $q = 37$, 41 and 43 has been disputed by Gunderson.

THEOREM 2. *Let m and n be fixed integers, $m, n > 1$. Suppose that q is a prime such that for all primes p with $p \equiv 1 \pmod{2^n}$ we have $q^{p-1} \equiv 1 \pmod{p^m}$. Then there is an infinite sequence of primes p such that $q^{p-1} \equiv 1 \pmod{p^{m+1}}$.*

Theorem 1 is an immediate deduction from Theorem 2. The elementary theory of congruences, together with Dirichlet's Theorem, form the ingredients for the proof of Theorem 2. First though, we require a technical lemma.

LEMMA. *Suppose that r is a prime and M is an even integer divisible by r. Then, for each prime q, there exists a prime factor s of $q^M + 1$ with $s \equiv 1 \pmod{r}$.*

Proof. We first note that $q^M + 1$ is not a power of 2, and thus it has at least one odd prime factor. The lemma is trivial when $r = 2$. We shall suppose that the lemma is false, so that r is odd and for each odd prime factor s of $q^M + 1$ we have $s \not\equiv 1 \pmod{r}$. We now write $M = ar^b$ with $r \nmid a$, so that a and b are both positive integers by the hypothesis. For each prime factor s of $q^M + 1$ we have $s \mid q^a + 1$ since $s \not\equiv 1 \pmod{r}$ and, moreover, if $s \neq r$ then s occurs to the same power in $q^M + 1$ and $q^a + 1$. Hence $q^M + 1 = r^c(q^a + 1)$ for some $c \geqslant 0$; in fact $c > 0$ as $M > a$. The proof is completed by establishing that $c = b$, for the equation $q^{ar^b} + 1 = r^b(q^a + 1)$ is insoluble in positive integers a, b, q, r, with $a, q, r \geqslant 2$. However r divides $q^M + 1$ and thus divides $q^a + 1$ as above, so we may write $q^a + 1 = dr^e$ for some $r \nmid d$, $e \geqslant 1$. In that case $q^M + 1 = dr^{e+c}$ and $q^M = (q^a)^{r^b} \equiv -1 + dr^{e+b} \pmod{r^{e+b+1}}$ and so $c = b$ as required. ∎

Proof of Theorem 2. We wish to construct an infinite sequence of primes p such that $q^{p-1} \equiv 1 \pmod{p^{m+1}}$. The primes that we choose are factors of integers of the form $q^{tM} + 1$, where M henceforth denotes the lowest common multiple of m and 2^{n-1}, and t is any prime lying in a certain congruence class of integers, to be specified.

First we consider a prime factor of m, r say. By the Lemma there exists a prime factor, s, of $q^M + 1$ such that $s \equiv 1 \pmod{r}$. By Dirichlet's Theorem there is an infinite set of primes which are not rth powers modulo s: discarding those which divide $q^M + 1$ leaves a set of primes t_j, $j \geqslant 1$, say.

We define $A_j = q^{Mt_j} + 1$, for $j \geqslant 0$, where we write $t_0 = 1$ so that $A_0 = q^M + 1$. The crucial step is to establish that for each $j \geqslant 1$ there is a prime p_j such that p_j^{m+1} divides A_j. First we shall show that for all odd primes p dividing A_j, $j \geqslant 0$, p^m divides A_j. We first note that t_j does not divide A_j, since $A_j \equiv A_0 \pmod{t_j}$, and $t_j \nmid A_0$, by the construction above. Thus we may take $p \mid A_j$ to be an odd prime different from t_j.

We wish to prove initially that $p \equiv 1 \pmod{2^n}$. For let a denote the highest power of 2 dividing $p - 1$ and suppose instead that $a < n$. We write $Mt_j = 2^b c$ with c odd, and so $b \geqslant n - 1$. Since $p \mid A_j$, $q^{2^b c} \equiv -1 \pmod{p}$ and q has even order modulo p. We shall write the order of q, modulo p, as $2^d e$ with e odd, $d \geqslant 1$, that is $o_p(q) = 2^d e$. Since $o_p(q) \mid p - 1$, we have $d \leqslant a$; further, since $q^{2^{d-1}e} \equiv -1 \pmod{p}$, e divides c and $b = d - 1$. However $b \geqslant n - 1$ and $d \leqslant a < n$ so that $b \geqslant d$. Hence $a \geqslant n$ so 2^n divides $p - 1$ as required.

We now wish to prove that p^m divides A_j. By our hypothesis $p^m \mid q^{p-1} - 1$; that is $o_{p^m}(q) \mid p - 1$. Let a now denote the highest power of p dividing A_j, and suppose instead that $a < m$. Since $p^a \mid q^{2Mt_j} - 1$, $o_{p^a}(q) \mid 2Mt_j$. Furthermore, since $a < m$, $o_{p^{a+1}}(q) \mid o_{p^m}(q)$ and so $o_{p^{a+1}}(q) < p$. However $o_{p^{a+1}}(q)/o_{p^a}(q) = 1$ or p, so $o_{p^{a+1}}(q) \mid 2Mt_j$ and $p^{a+1} \mid q^{2Mt_j} - 1$. But p is odd, so a is the highest power of p dividing $A_j(A_j - 2) = q^{2Mt_j} - 1$, which contradicts the assumption that $a < m$: hence we have shown that p^m divides A_j as required.

We now wish to show that for each $j \geqslant 1$ there is a prime p_j such that p_j^{m+1} divides A_j. Let us first consider $q = 2$ so that A_j is odd. If no such prime p_j exists then, by the previous paragraph, $A_j = a_j^m$ for some a_j and so $2^{Mt_j} = a_j^m - 1$. But M is a multiple of m, from its definition, and so this is not possible. We can now consider q to be an odd prime so that A_j is even but not divisible by 4. Thus if no such prime exists then $A_j = 2a_j^m$ for some a_j. We note also that $A_0 = 2a_0^m$ for some a_0: for otherwise A_0 is divisible by p_0^{m+1} for some odd prime p_0, which is impossible as $A_0 | A_j$. We recall that $t_j (j \geqslant 1)$ is not an mth power residue modulo s, where s is a specific prime factor of $q^M + 1$. Let us write $q^M + 1 = as^b$ with $s \nmid a$ and $b \geqslant 1$. Then

$$A_j/A_0 = (1 + (as^b - 1)^{t_j}/as^b \equiv t_j \pmod{s}$$

so that A_j/A_0 cannot be an mth power. But $A_j/A_0 = (a_j/a_0)^m$ which establishes a contradiction: hence, for each $j \geqslant 1$, there exists a prime p_j such that p_j^{m+1} divides A_j.

We can now show that $p_1, p_2, \ldots$ may be taken to be distinct. In fact we assert that for each $j \geqslant 1$ there is a prime p_j such that p_j^{m+1} divides A_j, but p_j^{m+1} does not divide A_k for any $k \neq j$. We first note that the highest common factor of A_j and A_k is A_0. So if our assertion is false, then for each prime p with p^{m+1} dividing A_j, $p^{m+1} | A_0$ also. Now A_j/A_0 is odd, so for each prime p dividing A_j/A_0, p is odd, and so $p^m | A_j$, by an earlier result. We recall that $t_j \nmid A_0$ so that A_0 and A_j/A_0 are coprime. Hence p^m must divide A_j/A_0. But $p^{m+1} \nmid (A_j/A_0)$, for otherwise p^{m+1} divides A_j and so by the above $p^{m+1} | A_0$, which is impossible as A_0 and A_j/A_0 are coprime.

$$\begin{aligned}\Big[\operatorname{hcf}(A_0, A_j/A_0) &= \operatorname{hcf}\Big(q^M + 1, \sum_{i=0}^{t_j-1} q^{iM}(-1)^{t_j-1-i}\Big) \\ &= \operatorname{hcf}\Big(q^M + 1, \sum_{i=0}^{t_j-1} (+1)\Big) \\ &= \operatorname{hcf}(q^M + 1, t_j) = 1.\Big]\end{aligned}$$

Hence A_j/A_0 can only be an mth power, but we have seen that that is not possible, in the previous paragraph. Hence we have established our assertion, and so we may choose $p_1, p_2, \ldots$, to be distinct primes such that $p_j^{m+1} | A_j$ for each $j \geqslant 1$.

We can now show that if $p_j \nmid 2M$ then p_j^{m+1} divides $q^{p_j - 1} - 1$. For we know that p_j^{m+1} divides $A_j | q^{2Mt_j} - 1$ and hence $o_{p_j^{m+1}}(q)$ divides both $2Mt_j$ and $p_j^m(p_j - 1)$. We recall that t_j does not divide A_j and so cannot be p_j; thus is $p_j \nmid 2M$ then $o_{p_j^{m+1}}(q) | p_j - 1$.

So if we now discard those primes that divide $2M$, we are left with an infinite sequence of primes p such that $q^{p-1} \equiv 1 \pmod{p^{m+1}}$. ∎

It has not as yet been established whether or not there exists a positive integer n such that

$$x^{p^n} + y^{p^n} + z^{p^n} = 0 \quad (p \nmid xyz) \tag{3}$$

has no solutions in integers x, y, z for an infinite number of different primes p with $p \equiv 1 \pmod 4$. However, in 1972, Hellegouarch [3] showed that if (3) does have solutions in integers x, y, z then

$$2^{p-1} \equiv 3^{p-1} \equiv 1 \pmod{p^{2n}}. \tag{4}$$

Thus we can easily deduce the following theorem from Theorem 2.

THEOREM 3. *Given a positive integer n, and a prime $q = 2$ or 3, such that for all sufficiently*

large primes with $p \equiv 1 \pmod 4$ *we have solutions to* (3). *Then we can find an infinite sequence of primes* p, *such that*

$$q^{p-1} \equiv 1 \pmod{p^{2n+1}}.$$

By using Theorem 2, we can obtain the following property stemming from the Fermat numbers.

THEOREM 4. *Suppose that we can find an infinite sequence of Fermat numbers* $F_n = 2^{2^n}+1$, *such that each of these Fermat numbers has no divisor that is a cube of a prime. Then to each of these Fermat numbers we can associate a prime* p_n, *with*

$$p_n \equiv 1 \bmod 2^{n+2} \quad (n \geqslant 3)$$

such that (1) *has no solution for* p_n.

Proof. Firstly we show that $p \equiv 1 \pmod{2^{n+2}}$ for all primes p that divide F_n $(n \geqslant 2)$.

Now $2^{2^n} \equiv -1 \bmod p$, so $o_p(2) = 2^{n+1}$. Thus $2^{n+1} | p-1$. Now suppose 2^{n+2} does not divide $p-1$. Then $2^{(p-1)/2} \equiv (2^{2^n})^{(p-1)/2^{n+1}} \equiv -1 \pmod p$, i.e. 2 is not a quadratic residue modulo p: but this is impossible as we have already ascertained that $p \equiv 1 \pmod 8$.

Thus 2^{n+2} divides $p-1$.

Now, by the statement of the Theorem, we know that for all primes p dividing F_n, $p^3 \nmid F_n$.

But $F_n = 2^{2^n}+1$ is not a square and so there exists a prime p_n dividing F_n such that $p_n^2 \nmid F_n$.

Thus $2^{2^n} \equiv -1 + ap_n \bmod p_n^2$ for some integer a, coprime with p_n.

Then
$$2^{p_n-1} = (2^{2^n})^{(p_n-1)/2^n} = (-1+ap_n)^{(p_n-1)/2^n}$$
$$\equiv 1 + ap_n \cdot \frac{p_n-1}{2^n} \not\equiv 1 \bmod p_n^2.$$

Thus by (2), it is clear that (1) has no solutions for p_n. ∎

Finally, I would like to thank Dr R. C. Mason for his efforts and help in preparing this paper for publication.

REFERENCES

[1] L. M. ADLEMAN and D. R. HEATH-BROWN. The first case of Fermat's last theorem. *Invent. Math.* **79** (1985), 409–416.

[2] E. FOUVRY. Théorème de Brun-Titchmarsh; application au théorème de Fermat. *Invent. Math.* **79** (1985), 383–407.

[3] Y. HELLEGOUARCH. Courbes elliptiques et equation de Fermat. Thesis, Bésançon, 1972.

[4] D. H. LEHMER. On Fermat's quotient base two. *Math. Comput.* **36**, 153 (1981), 289–290.

[5] S. PUCCIONI. Un teorema per una resoluzioni parziali del famoso problema di Fermat. *Archimede* **20** (1968), 219–220.

[6] P. RIBENBOIM. *Thirteen lectures on Fermat's last theorem* (Springer-Verlag, 1979).