POWERFUL NUMBERS AND FERMAT'S LAST THEOREM

Andrew Granville

Presented by P. Ribenboim F.R.S.C.

A powerful number $n$ is a positive integer with the property that $p^2$ divides $n$ whenever prime $p$ divides $n$.

Mollin and Walsh conjectured [4] that there does not exist three consecutive powerful numbers and gave some strong numerical evidence.

Recently Adleman and Heath-Brown [1], using a result of Fouvy [3] on the Brun-Titchmarsh inequality, showed that the first case of Fermat's Last Theorem is true for infinitely many primes $p$.

We shall show that if the conjecture of Mollin and Walsh is true then the Adleman-Heath-Brown theorem follows immediately.

Lemma

If $p$ is a prime such that $p^2$ divides $2^{p-2}$ and $m$ is a positive integer for which $p$ divides $2^m-1$ then $p^2$ divides $2^m-1$.

Proof: Let $r$ be the greatest common divisor of $m$
and $p-1$. Clearly $p$ divides $2^r - 1$.

Suppose $2^r = 1 + a \, p$.

Then $2^{p-1} = (2^r)^{(p-1)/r} = (1 + a \, p)^{(p-1)/r}$

$\equiv 1 + \frac{a \, (p-1)}{r} \, p \mod p^2$.

But $2^{p-1} \equiv 1 \mod p^2$, so that $p$ divides $a$.

Thus $2^r \equiv 1 \mod p^2$ and as $r$ divides $m$,

$2^m \equiv 1 \mod p^2$.

**Theorem**

If the conjecture of Mollin and Walsh is true then there exists an infinite sequence of primes $p$ for which $p^2$ does not divide $2^{p-2}$.

Proof: Suppose $p^2$ divides $2^{p-2}$ for all primes $p > p_0$.

Let $t = \pi \, p$, and $A = 2^{t \phi(t)}$ where $\phi(\cdot)$ is Euler's function. We claim that $A^{n-1}$ is powerful for any positive integer $n$.

For, if $2 < p \leq p_0$, $p-1|t \phi(t)$ and so $A \equiv 1 \mod p^2$.

Thus $A^n \equiv 1 \mod p^2$ for each positive integer $n$. 
If \( p > p_0 \) and \( p | A^{n-1} \) then \( p^2 | 2^{nt\phi(t)} - 1 \). By the lemma \( p^2 | 2^{nt\phi(t)} - 1 \) that is \( p^2 \) divides \( A^{n-1} \).

Thus \( A^{n-1} \) is powerful.

So \( A-1 \) and \( A^2-1 \) are both powerful.

But \( \gcd(A-1, A+1) = \gcd(2, A-1) = 1 \) as 2 divides \( A \).

Thus, as \( A^2-1 = A-1 \). \( A+1 \), we know \( A+1 \) is also powerful. But then \( A-1, A, A+1 \) are three consecutive powerful numbers, which contradicts the conjecture of Mollin and Walsh.

Wieferich [5] showed the following:

If \( x, y \) and \( z \) are positive integers and \( p \) is a prime, for which

\[
x^p + y^p = z^p \quad \text{with} \quad p \nmid xyz
\]

then \( p^2 \) divides \( 2^{p-2} \).

(See a recent elegant proof by Agoh [2].)

So, by the theorem and Wieferich's criteria, we can immediately state the following.

Corollary

If the conjecture of Mollin and Walsh is true then there exists an infinite sequence of primes \( p \) for which the First
A. Granville

Case of Fermat's Last Theorem is true.

References


Received 12 February, 1986

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