AN ANALYTIC CRITERION FOR THE EXISTENCE OF INFINITELY MANY PRIMES OF THE FORM $\frac{1}{2}(n^2 + 1)$

BY

DANIEL SHANKS

A well-known unsolved problem is that of proving the existence of infinitely many primes of the form $n^2 + 1$. Although there is much evidence that there exist infinitely many, e.g., [1], [2], [3], [4], a proof has not been found. A very similar problem is that of showing infinitely many primes of the form $\frac{1}{2}(n^2 + 1)$; in fact, the heuristic arguments, say of Bateman and Horn [5], and the known empirical evidence, both make it probable that the number of positive integers n between 1 and N such that $n^2 + 1$ is prime is asymptotic to the number of positive integers n between 1 and N such that $\frac{1}{2}(n^2 + 1)$ is prime.

The primes of the form $\frac{1}{2}(n^2 + 1)$ are not at all rare, and thousands of large primes such as

$$17019940501 = \tfrac{1}{2}(184499^2 + 1)$$

are known [1, page 82]. A few very much larger primes of this form have been discovered by Brillhart [6, page 427]. These include

$$\tfrac{1}{2}(M_n^2 + 1)$$

where $M_n = 2^n - 1$ and $n = 229, 184, 177$, etc.

In the theorem that follows we give an analytic criterion for the existence of infinitely many primes of the form $\frac{1}{2}(n^2 + 1)$. While we cannot assert that the criterion is "practical," in the sense that we know how to use it to settle the question, it is not precluded that it could be so used. The proof of the theorem is elementary.

THEOREM. *Let*

$$f(z) = 1 + z + z^3 + z^6 + z^{10} + z^{15} + \cdots,$$

and let

$$g(z) = f^2(z) - 3f(z).$$

If, for $m > 0$, the initial value of the m^{th} derivative of $g(z)$ is negative, that is, if

$$\left.\frac{d^m g(z)}{dz^m}\right|_{z=0} < 0,$$

then $4m + 1$ is a prime of the form $\frac{1}{2}(n^2 + 1)$, and conversely. There are thus infinitely many such primes if, and only if, there are infinitely many such derivatives.

Received January 21, 1963.

Proof. Since

$$g(z) = -2 + \{f(z) - 1\}^2 - \{f(z) - 1\}, \tag{1}$$

the condition

$$d^m g(z)/dz^m \mid_{z=0} < 0 \qquad (m \geqq 1)$$

implies that the corresponding coefficient in $\{f(z) - 1)\}^2$ vanishes, while that in $\{f(z) - 1\}$ equals one. Thus

$$m = \tfrac{1}{2}a(a + 1) \tag{2}$$

for some $a > 0$, but

$$m \neq \tfrac{1}{2}b(b + 1) + \tfrac{1}{2}c(c + 1) \tag{3}$$

for any b and $c > 0$. From (2),

$$4m + 1 = \tfrac{1}{2}\{(2a + 1)^2 + 1\} = \tfrac{1}{2}(n^2 + 1)$$

for $n = 2a + 1$. Now $4m + 1$ equals the sum of two squares:

$$4m + 1 = a^2 + (a + 1)^2,$$

and, since a is relatively prime to $a + 1$, if $4m + 1$ were composite, there would be at least one other representation:

$$4m + 1 = (2x)^2 + (2y + 1)^2, \qquad x \geqq 0, \quad y \geqq 0.$$

That implies $x \neq y$ and $x \neq y + 1$. But if $x < y$, consider

$$m = \tfrac{1}{2}(x + y)(x + y + 1) + \tfrac{1}{2}(y - x)(y - x + 1),$$

while if $x > y + 1$, consider

$$m = \tfrac{1}{2}(x + y)(x + y + 1) + \tfrac{1}{2}(x - y - 1)(x - y).$$

Since these are impossible by (3), $4m + 1$ must be prime.

Conversely, assume that

$$4m + 1 = \tfrac{1}{2}(n^2 + 1) = \tfrac{1}{2}\{(2a + 1)^2 + 1\}$$

is prime. Then, since

$$4m + 1 = a^2 + (a + 1)^2$$

is its only representation as a sum of two squares, it follows that we cannot have

$$4m + 1 = (b + c + 1)^2 + (b - c)^2, \qquad b \geqq c > 0$$

or

$$m = \tfrac{1}{2}b(b + 1) + \tfrac{1}{2}c(c + 1), \qquad b \geqq c > 0.$$

Hence, since $m = \tfrac{1}{2}a(a + 1)$, we have

$$d^m g(z)/dz^m \mid_{z=0} < 0.$$

References

1. Daniel Shanks, *A sieve method for factoring numbers of the form* $n^2 + 1$, MTAC, vol. 13 (1959), pp. 78–86.
2. ———, *On the conjecture of Hardy and Littlewood concerning the number of primes of the form* $n^2 + a$, Math. Comp., vol. 14 (1960), pp. 321–332.
3. ———, *A note on Gaussian twin primes*, Math. Comp., vol. 14 (1960), pp. 201–203.
4. ———, *On numbers of the form* $n^4 + 1$, Math. Comp., vol. 15 (1961), pp. 186–189, and *Corrigendum*, vol. 16 (1962), p. 513.
5. Paul T. Bateman and Roger A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp., vol. 16 (1962), pp. 363–367.
6. John Brillhart, *Concerning the numbers,* $2^{2p} + 1$, *p prime*, Math. Comp., vol. 16 (1962), pp. 424–430.

David Taylor Model Basin
Washington, D. C.