ON PRIME DIVISORS OF SEQUENCES OF INTEGERS INVOLVING SQUARES

M. G. MONZINGO
Southern Methodist University, Dallas, TX 75275

(Submitted May 1986)

The following problem appears on page 65 of *Elementary Number Theory* by David M. Burton:

> Show that 13 is the *largest* prime that can divide two successive integers of the form $n^2 + 3$.

In this note, it will be shown that 13 is the *only* prime that will divide two successive integers of the form $n^2 + 3$, and these pairs will be determined. In addition, the following questions will be investigated: Is the prime 13 unique? That is, if p is an odd prime, is there an integer a such that p is the *largest* prime that divides successive integers of the form $n^2 + a$? And, under what conditions will the prime p be the *only* divisor? Finally, precisely which pairs of successive integers are divisible by p?

The following theorem will answer these questions. The case $p = 13$ will be treated in a corollary following the theorem.

Theorem: Let p be an odd prime. If p is of the form $4k+1$, then p is the *only* prime that divides successive integers of the form $n^2 + k$, and p divides successive pairs precisely when n is of the form $bp + 2k$, for any integer b. If p is of the form $4k + 3$, then p is the *largest* prime that divides successive integers of the form $n^2 + (3k + 2)$, and p divides successive pairs precisely when n is of the form $bp + (2k + 1)$, for any integer b. Furthermore, p will be the *only* prime divisor if and only if $p = 3$.

Proof: In both cases, substitution can be used to show that the prescribed divisibility will hold; hence, only the necessity of the indicated forms will need to be shown.

Let p be of the form $4k + 1$, and suppose that q is any prime divisor of $n^2 + k$ and $(n + 1)^2 + k$. Since q divides the difference of these integers, q must divide $2n + 1$. Now,

$$4(n^2 + k) = (2n + 1)(2n - 1) + (4k + 1).$$

Since q divides both $n^2 + k$ and $2n + 1$, q divides $p = 4k + 1$. Hence, $q = p$, and p is the only such prime divisor. Since p must divide $2n + 1$, $2n + 1 \equiv 0 \pmod{p}$. This congruence has the unique solution, $n \equiv (p - 1)/2 \pmod{p}$; thus, n must be of the form $bp + 2k$, where b is any integer.

Let p be of the form $4k + 3$, and suppose that q is any prime divisor of $n^2 + (3k + 2)$ and $(n + 1)^2 + (3k + 2)$. As before, q must divide $2n + 1$. Now,

$$4(n^2 + (3k + 2)) = (2n + 1)(2n - 1) + 3(4k + 3).$$

As before, q must divide the last term $3(4k + 3)$, but in this case q can be 3 or p. If $p = 3$, then p is the only such prime divisor; if not, then p is simply the largest such prime divisor. (Of course, it should be noted that 3 does, in fact, divide some successive pairs in the case $k > 0$. This will be the case when n is of the form $3c + 1$, c any integer.) Finally, the same argument used previously can be used to show that n must be of the form $bp + (2k + 1)$, b any integer.

Corollary: The prime $p = 13$ is the only prime that divides successive terms of the form $n^2 + 3$ and does so precisely when n is of the form $13b + 6$, where b is any integer.

Proof: The first case of the Theorem applies with $k = 3$.

◆◇◆◇◆