without nilpotent elements is a field (cf. [1, Lemma 2]), but we shall not do this here.

REFERENCES


NORTHWESTERN UNIVERSITY

A NOTE ON RELATIVELY PRIME SEQUENCES

RICHARD BELLMAN

In volume 2 of Pólya-Szegö, Aufgaben und Lehrsätze aus der Analysis, pp. 133 and 342, there occurs the following result (appearing also in Hardy-Wright, Theory of numbers, p. 14):

THEOREM 1. No two numbers of the form \(2^{2n}+1, \ n=1, 2, \cdots\), have a common divisor greater than 1.

The numbers \(2^{2n}+1, \ n=1, 2, \cdots\), are the well known Fermat numbers, which may be generated by iteration of the quadratic polynomial \(\phi(x) = (x-1)^2+1\), choosing \(x\) equal to 3. This follows easily by induction, since, putting \(\phi_1(x) = \phi(x), \ \phi_{n+1}(x) = \phi(\phi_n(x))\), if \(\phi_n(x) = 2^{2n}+1\), then \(\phi_{n+1}(x) = 2^{2n+4}+1\).

The above observation leads to the following result of which Theorem 1 is a special case:

THEOREM 2. Let \(\phi(x)\) be a polynomial in \(x\) with integral coefficients

Received by the editors October 10, 1946, and, in revised form, February 18, 1947.
possessing the following properties:

1. \( \phi_n(0) = \phi(0), \quad n \geq 1, \quad \phi(0) \neq 0, \)
2. \( (x, \phi(0)) = 1 \rightarrow (\phi(x), \phi(0)) = 1. \)

Then if \( x \) is an integer and \( (x, \phi(0)) = 1, \) no two of the numbers \( x, \phi_1(x), \ldots, \phi_n(x), \ldots, \) have a common divisor greater than 1.

**Proof.** Let us assume that the theorem is false, so that for some \( m > 1, \) \( n > m, \) we have \( (\phi_n(x), \phi_m(x)) > 1. \) Since \( \phi_n(x) = \phi_{n-m}(\phi_m(x)) \equiv \phi_{n-m}(0) \mod \phi_m(x) \equiv \phi(0) \mod \phi_m(x), \) if \( (\phi_m(x), \phi_n(x)) > 1, \) \( (\phi_n(x), \phi(0)) > 1. \) However, since \( (x, \phi(0)) = 1, \) it follows that \( (\phi(x), \phi(0)) = 1, \) and thus that \( (\phi_n(x), \phi(0)) = 1, \) which is a contradiction.

The sequence \( x, \phi_1(x), \ldots, \phi_n(x), \ldots, \) will have an infinity of distinct prime divisors if there are an infinite number of terms of the sequence different from \( \pm 1. \) This is true if \( x \) is an integer such that for \( y \geq x, \phi(y) > y^1, \) or if \( x \) is such that \( \phi(x) > x \) and \( x \) is greater than the roots of \( \phi(x) = \pm 1, \) or, finally, if \( |\phi(\pm 1)| > 1. \)

It is easy to verify that \( \phi(x) = (x-1)^2 + 1 \) satisfies the conditions of Theorem 2. If we choose \( x = 3, \) we obtain the Fermat numbers, as mentioned above. Another admissible polynomial is \( (x-2)^4 - 12, \) where we shall choose \( x \) satisfying the conditions \( (x, 4) = 1, \) \( x \geq 5. \)

Theorem 2 leads one to consider the following question:

Consider an irreducible polynomial \( f(x) \) with integral coefficients, and choose an integer \( x \) so that all the iterates \( f_n(x) \) yield distinct numbers. Can all these numbers be primes?

That this question is probably very difficult to answer might be surmised from the fact that the primality of all the Fermat numbers was disproved by exhibiting a specific counter-example, and the behavior of the general term of the sequence \( 2^{2^n} + 1 \) is still undetermined.

**Princeton University**

---

1. These latter alternatives were suggested by the referee, who also pointed out some superfluous restrictions in the original statement of Theorem 2.
2. The case where \( f(x) \) is linear has been worked out by the author and H. N. Shapiro, and the answer is negative.