ON A SEQUENCE OF PRIME NUMBERS

C. D. COX and A. J. VAN DER POORTEN

(Received 17 April 1967)

Euclid's scheme for proving the infinitude of the primes generates, amongst others, the following sequence

$$\{p_i\} = \{2, 3, 7, 43, 139, 50207, \cdots\} \tag{1}$$

defined by $p_1 = 2$ and p_{n+1} is the highest prime factor of $p_1p_2\cdots p_n+1$.

We have obtained an interesting sufficient condition for the non-occurrence of a prime in this sequence. In particular the presence of the first six terms given in (1) already determines that the only primes < 53 that occur in the sequence are precisely 2, 3, 7 and 43.

Let

$$\{q_i\} = \{2, 3, 5, 7, \cdots\}$$

be the sequence of all primes arranged in monotonic increasing order.

Let $r > 1$; clearly q_r occurs in the sequence (1) if and only if for some positive integer k

$$p_1p_2\cdots p_k+1 = q_1^{k_1}q_2^{k_2}\cdots q_r^{k_r} \tag{2}$$

for integers $k_1, k_2, \cdots, k_{r-1} \geqq 0$, $k_r > 0$.

Hence necessarily

$$q_1^{k_1}q_2^{k_2}\cdots q_r^{k_r} \equiv 1 \pmod{p_i} \tag{3}$$

and since obviously $p_1, p_2, \cdots, p_k$ all differ

$$q_1^{k_1}q_2^{k_2}\cdots q_r^{k_r} \not\equiv 1 \pmod{p_i^2} \qquad (i = 1, 2, \cdots, k) \tag{4}$$

The congruences (4) and (3) imply the weaker but more useful conditions

$$k_i = 0 \text{ when } q_i \text{ is one of } p_1, p_2, \cdots, p_k; \tag{5}$$

hence in particular $k_1 = 0$ for $r > 1$,

$$q_2^{k_2}\cdots q_r^{k_r} \not\equiv 1 \pmod 4, \tag{6}$$

whence $q_2^{k_2}\cdots q_1^{k_r}$ contains an odd number of prime divisors (counted according to multiplicity) congruent to -1 modulo 4, and

https://doi.org/10.1017/S1446788700006236 Published online by Cambridge University Press

(7) $q_2^{k_2} \cdots q_r^{k_r}$ is a quadratic residue modulo p_i,

whence it contains an even number of prime divisors (counted according to multiplicity) which are quadratic non-residues of

$$p_i \qquad (i = 2, 3, \cdots, k).$$

Hence the congruences (8) must be solvable for non-negative integers $k_2, \cdots, k_r$, with $k_i = 0$ when q_i is one of $p_2, \cdots, p_k$.

$$(8) \qquad \begin{aligned} a_{12}k_2 + \cdots + a_{1r}k_r &\equiv 1 \pmod 2 \\ a_{1j} &= \begin{cases} 1, & q_j \equiv -1 \pmod 4 \\ 0, & q_j \equiv 1 \pmod 4 \end{cases} \\ a_{i2}k_2 + \cdots + a_{ir}k_r &\equiv 0 \pmod 2 \\ 2a_{ij} &= 1 - \left(\frac{q_j}{p_i}\right) \qquad (i = 2, 3, \cdots, k,\ j = 2, 3, \cdots, r) \end{aligned}$$

We may of course easily evaluate the Legendre symbols (q_j/p_i) by virtue of the quadratic reciprocity law. We have thus established

THEOREM 1. *If for some k the congruences* (8) *are inconsistent* (*henceforth we assume* (5)) *then*

a) *the prime q_r does not occur in the sequence* (1), *and indeed*

b) *nor do the primes q_j $(j < r)$ unless of course q_j is already one of $p_1, p_2, \cdots, p_k$.*

Part b) follows immediately since if the congruences (8) are inconsistent then they certainly have no solution with $k_{j+1} = k_{j+2} = \cdots = k_r = 0$.

COROLLARY. *The primes* 5, 11, 13, 17, 19, 23, 29, 31, 37, 41 *and* 47 *do not occur in the sequence* (1).

For if we take $q_r = 53$ and $k = 6$ then the congruences (8) imply that $k_r \neq 0$ whence the congruences are inconsistent if $k_r = 0$.

TABLE 1

$j =$	3	5	6	7	8	9	10	11	12	13	15	16	
$q_j =$	5	11	13	17	19	23	29	31	37	41	47	53	i
$q_j = ?\ (\text{mod } 4)$	1	−1	1	1	−1	−1	1	−1	1	1	−1	1	1
$(q_j/3)$	−1	−1	1	−1	1	−1	−1	1	1	−1	−1	−1	2
$(q_j/7)$	−1	1	−1	−1	−1	1	1	−1	1	−1	−1	1	3
$(q_j/43)$	−1	1	1	1	−1	1	−1	1	−1	1	1	1	4
$(q_j/139)$	1	1	1	−1	−1	−1	1	1	1	1	−1	−1	5
$(q_j/50207)$	−1	−1	1	−1	−1	1	−1	−1	−1	1	1	1	6

https://doi.org/10.1017/S1446788700006236 Published online by Cambridge University Press

We require the congruences (8) only for $i = 1, 4, 5$ and 6.

We thus obtain

$$\begin{array}{llllllll}
i=1 & & k_5+ & k_8+k_9+ & k_{11}+ & k_{15} & & \equiv 1 \pmod 2\\
i=4 & k_3+ & & k_8+ & k_{10}+ & k_{12} & & \equiv 0 \pmod 2\\
i=5 & & & k_7+k_8+k_9+ & & & k_{15}+k_{16} & \equiv 0 \pmod 2\\
i=6 & k_3+k_5+k_7+k_8+ & & & k_{10}+k_{11}+k_{12} & & & \equiv 0 \pmod 2
\end{array}$$

whence adding the congruences we have $k_{16} \equiv 1 \pmod 2$ and the assertion.

Theorem 1 provides a sufficient condition for the non-occurrence of a prime; further, if the condition excludes a prime it also excludes all smaller primes which have not already occurred. Hence it excludes the smallest N primes which do not occur, and fails to exclude all larger non-occurring primes, or it excludes all non-occurring primes. If the latter is true there is a finite decision procedure for occurrence or non-occurrence of a given prime q, and the set of primes generated is recursive.

It seems likely that

a) an infinite set of primes do not occur in (1) and

b) all absent primes yield inconsistent congruences (8).

We may show that these conjectures are not both false.

THEOREM 2. *If the only primes not generated by* (1) *are* $q_{i_1}, q_{i_2}, \cdots, q_{i_r}$ (*a finite set*), *then each yields an inconsistent set of congruences* (8).

By Theorem 1 b) it is sufficient to prove this for the largest non-occurring prime q_{i_r}.

By Dirichlet's theorem we may find a prime p_t such that

$$\begin{aligned} p_t &\equiv 1 \pmod{q_{i_1} q_{i_2} \cdots q_{i_r}} \\ p_t &\equiv -1 \pmod 4 \end{aligned} \tag{9}$$

and clearly p_t occurs in the sequence (1). Then

$$q_{i_j} \equiv \left(\frac{q_{i_j}}{p_t}\right) \pmod 4 \qquad j = 1, \cdots, r$$

whence in the congruences (8)

$$a_{1i_j} = a_{ti_j} \qquad j = 1, \cdots, r$$

and the left hand members of the congruences (8) for $i = 1$ and $i = t$ are identical whilst the right hand members are respectively 1 and 0.

We can modify this proof to show for example that an infinite number of primes do not occur in (1) if:

When $(a, b) = 1$ then there exists a number X so that if p is any prime greater than X, there is at least one positive prime q with the properties

https://doi.org/10.1017/S1446788700006236 Published online by Cambridge University Press

$$\text{(i)}\quad q < p, \qquad \text{(ii)}\quad q = b \ (\mathrm{mod}\ a), \qquad \text{(iii)}\quad \left(\frac{q}{p}\right) = 1.$$

The sequence (1) originally arose from a question of A. A. Mullin (*Bull. Amer. Math. Soc.* 69, (1963), 737) who asked if the set of primes so generated is recursive, if the sequence is monotonic increasing, and if not, does it contain all primes. R. R. Korfhage (*Bull. Amer. Math. Soc.* 70 (1964), 747) has shown on an IBM 7090 that

$p_7 = 340999$ and $p_8 = 3202139$ whilst it further appears that $p_9 > p_8$. It is not otherwise known if the sequence is monotonic.

Our thanks are due to Professor G. Szekeres for a simplification of our argument.

School of Mathematics
University of N.S.W.
Australia

https://doi.org/10.1017/S1446788700006236 Published online by Cambridge University Press