ON THE INFINITUDE OF PRIMES OF THE FORM $3k+1$

Neville Robbins

Mathematics Department, San Francisco State University, San Francisco, CA 94132

(Submitted May 2002)

Let a, b be natural numbers such that $(a, b) = 1$. Dirichlet's theorem (whose proof requires advanced methods) states that there are infinitely many primes of the form $ak + b$, where k is a natural number. The special case: $a = 4, b = 1$ can be proved by elementary means, making use of the properties of Fermat numbers, or of Fibonacci numbers. (See [1].) In this note, using a different second order linear recurrence, we dispose of the case: $a = 3$, $b = 1$. $(\frac{m}{p})$ denotes the Legendre symbol.

Theorem 1: There are infinitely many primes, p , such that $p \equiv 1 \pmod 3$.

Proof: Consider the linear second order recurrence:

$$u_0 = 0,\ u_1 = 1,\ u_n = u_{n-1} + 3u_{n-2} \quad for \quad n \geq 2.$$

Let the roots of the equation:

$$\lambda^2 - \lambda - 3 = 0$$

be: $\alpha = (1 + \sqrt{13})/2$, $\beta = (1 - \sqrt{13})/2$. Then

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \ . \tag{1}$$

It is easily established by induction on n that

$$3 \not| u_n \quad \forall n \geq 1 \tag{2}$$

$$(u_n, u_{n-1}) = 1 \quad \forall n \geq 2 \tag{3}$$

$$2|u_n \quad iff \quad 3|n \tag{4}$$

$$\alpha^n = \alpha u_n + u_{n-1}, \qquad \beta^n = \beta u_n + u_{n-1} \tag{5}$$

$$u_{kn+r} = \sum_{j=0}^{k} \binom{k}{j} u_n^j u_{n-1}^{k-j} u_{r+j}. \tag{6}$$

Using (6), we can prove

$$(u_{kn+r}, u_n) = u_r \tag{7}$$

from which it follows that

$$(u_m, u_n) = u_{(m,n)}. \tag{8}$$

Another consequence of (1) is the identity:

$$u_{2n+1} = u_{n+1}^2 + 3u_n^2. \tag{9}$$

If p is an odd prime, then in view of (3) and (9), we have

$$p|u_{2n+1} \rightarrow \left(\frac{-3}{p}\right) = 1 \rightarrow p \equiv 1 \pmod 3. \tag{10}$$

To complete the proof, we need a subsequence of $\{u_{2n+1}\}$ such that any pair of distinct terms is odd and relatively prime. Let

$$w_n = u_{q_n}$$

where $q_1 = 5$, $q_2 = 7$, $q_3 = 11$, $\cdots$, that is q_n is the n^{th} prime, starting with 5. If the natural numbers m, n are distinct, then $w_m = u_r$, $w_n = u_t$ for distinct primes r, t so that

$$(w_m, w_n) = (u_r, u_t) = u_{(r,t)} = u_1 = 1.$$

Since $u_n > 1 \quad \forall n \geq 3$, we have $w_n \geq 1 \quad \forall n \geq 1$. Since each w_n has a prime divisor, p, such that $p \equiv 1 \pmod 3$ and the members of $\{w_n\}$ are odd and pairwise relatively prime, we are done. $\square$

Remarks: Similarly, if $q > 3$ is a given prime, by recourse to the second order linear recurrence:

$$u_0 = 0,\, u_1 = 1,\, u_n = u_{n-1} + qu_{n-2} \quad for \quad n \geq 2$$

one can prove that there are infinitely many primes, p, such that $(\frac{-q}{p}) = 1$. In the case $q = 5$, this yields infinitely many primes, p, such that $p \equiv 1, 3, 7, or\, 9 \pmod{20}$.

REFERENCES

[1] N. Robbins. "On Fibonacci Numbers and Primes of the Form $4k+1$." *The Fibonacci Quarterly* **32** (1994): 15-16.

AMS Classification Numbers: 11B35

✠ ✠ ✠