# ON THE INFINITUDE OF FIBONACCI PSEUDO-PRIMES

EMMA LEHMER
University of California, Berkeley, California

A Fermat pseudo-prime is usually defined to be a composite number m which satisfies the Fermat congruence

$$\text{(1)} \qquad a^{m-1}-1 \equiv 0(\text{mod } m), \qquad (a, m) = 1$$

thus showing that the converse of Fermat's theorem does not hold without further conditions on m. Hardy and Wright (Theory of Numbers, p. 72) show that there are infinitely many composite numbers m which satisfy (1).

The Lucas congruence for Fibonacci numbers which can be thought of as a generalization of the Fermat's congruence (1) states

$$\text{(2)} \qquad U_{m-\epsilon_m} = 0(\text{mod } m), \qquad (m, 10) = 1$$

where $U_n = U_{n-1} + U_{n-2}$, $U_0 = 0$, $U_1 = 1$ are the Fibonacci numbers and $\epsilon_m = 1$ if $m = 10n \pm 1$, while $\epsilon_m = -1$ if $m = 10m \pm 3$. Congruence (2) holds for m a prime. We next show that it also holds for an infinitude of composite numbers, which we call Fibonacci pseudo-primes. Let $p > 5$ be a prime, and let $m = U_{2p} = U_p V_p$, where $V_n$ is the series $V_0 = 2$, $V_1 = 1$, $V_n = V_{n-1} + V_{n-2}$. Hence m is composite. Also m is odd since the only even Fibonacci numbers have subscripts which are multiples of 3 and $p \neq 3$. From the known expansions

$$\text{(3)} \qquad \begin{cases} 2^{p-1} U_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} 5^k \\ 2^{p-1} V_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k} 5^k \end{cases}$$

it follows, since all the binomial coefficients are divisible by p, that

$$U_p \equiv 5^{\frac{p-1}{2}} \equiv \epsilon_p \pmod p$$

$$V_p \equiv 1 \pmod p$$

Hence $m = U_{2p} \equiv \epsilon_p \pmod p$ and, since $U_{2p}$ is odd, $2p$ divides $m - \epsilon_p$, hence $U_{2p}$ divides $U_{m-\epsilon_p}$. It remains to show that $\epsilon_m = \epsilon_p$ or that $m \equiv p \pmod{10}$. Taking (3) modulo 5 we have

$$4^{p-1} U_p V_p \equiv (-1)^{p-1} U_{2p} = U_{2p} \equiv p \pmod 5, \quad \text{and}$$

since $m = U_{2p}$ and $p$ are both odd ($p \neq 3$) we have $m = p(\bmod 10)$ or $\epsilon_p = \epsilon_m$ and the result follows.

XXXXXXXXXXXXXXX

## TWO VERY SPECIAL NUMBERS

J. A. H. HUNTER
Toronto, Ontario

Stimulated by my derivation of the two 17-digit automorphic numbers (*Recreational Mathematics Magazine, No. 14*), Mr. R. A. Fairbairn of Willowdale, Ontario, has derived the two 100-digit automorphics.

The labor involved in this tremendous task would deter most enthusiasts, since the results were achieved (and of course checked) using no help other than a simple desk adding machine.

An automorphic number is distinguished by having its square *end with* the number itself.

The two 100-digit automorphic numbers, never before published so far as I know, are:

3, 953, 007, 319, 108, 169, 802, 938, 509, 890, 062, 166,
509, 580, 863, 811, 000, 557, 423, 423, 230, 896, 109,
004, 106, 619, 977, 392, 256, 259, 918, 212, 890, 625

and

6, 046, 992, 680, 891, 830, 197, 061, 490, 109, 937, 833,
490, 419, 136, 188, 999, 442, 576, 576, 769, 103, 890,
995, 893, 380, 022, 607, 743, 740, 081, 787, 109, 376