A NOTE ON FIBONACCI PRIMITIVE ROOTS

MICHAEL E. MAYS
West Virginia University, Morgantown, WV 26506
(Submitted November 1980)

A prime p possesses a Fibonacci primitive root (FPR) g if g is a primitive root (mod p) satisfying

$$g^2 \equiv g + 1 \pmod{p}.$$

This definition was given in [2], and properties of FPRs were worked out in [2] and [3]. A good discussion of FPRs is contained in [4].

In [2] an asymptotic density for the set of primes having a FPR in the set of all primes was conjectured, and that this density is correct subject to a generalized Riemann Hypothesis was shown in [1], but it is still an open question as to whether or not infinitely many primes possess FPRs. The purpose of this note is to provide a sufficient condition that a prime should possess a FPR.

Theorem: If $p = 60k - 1$ and $q = 30k - 1$ are both prime, then p has a FPR.

Proof: $p \equiv 3 \pmod{4}$ implies that at most one of $\{a, -a\}$ is a primitive root of p for any a such that $2 \le a \le (p-1)/2 = q$; q prime implies that there are $q-1$ primitive roots of p in all, so exactly one of $\{a, -a\}$ is a primitive root of p.

$p \equiv -1 \pmod{10}$ implies that two solutions to the congruence

$$x^2 - x - 1 \equiv 0 \pmod{p}$$

exist. These solutions may be written as g and $1 - g$.

Shanks points out that since $g^2 - g - 1 \equiv 0 \pmod{p}$,

$$g(g - 1) \equiv 1 \pmod{p},$$

so that g is a primitive root iff $g-1$ is a primitive root. $g-1$ is a primitive root iff $-(g-1) = 1-g$ is not a primitive root. Thus exactly one of the solutions to the congruence is a FPR of p.

Conditions similar to that in this theorem occur frequently in theorems in the literature about existence or ordering of primitive roots. Theorems 38-40 in [4] are well-known instances of this. In [3] it is observed that primes p satisfying sufficient conditions to have two sets of three consecutive primitive roots (a FPR g, $g-1$, and $g-2$, and -2, -3, and -4) must be of the form $120k - 1$, with $60k - 1$ also prime. Using the theorem above, it is not necessary to presuppose that p has a FPR.

References

1. H. W. Lenstra, Jr. "On Artin's Conjecture and Euclid's Algorithm in Global Fields." *Inventiones Mathematicae* 42 (1977):201-224.
2. D. Shanks. "Fibonacci Primitive Roots." *The Fibonacci Quarterly* 10, no. 2 (1972):163-168, 181.
3. D. Shanks & L. Taylor. "An Observation on Fibonacci Primitive Roots." *The Fibonacci Quarterly* 11, no. 2 (1973):159-160.
4. D. Shanks. *Solved and Unsolved Problems in Number Theory*. 2nd ed. New York: Chelsea, 1978.

*****