AN OBSERVATION ON FIBONACCI PRIMITIVE ROOTS

DANIEL SHANKS
Naval Ship R & D Center, Bethesda, Maryland
and
LARRY TAYLOR
UNIVAC Division, Sperry Rand Corporation, New York, New York

1. OBSERVATION

A prime p has a Fibonacci Primitive Root g if g is a primitive root of p that satisfies

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

Some properties of the F. P. R.'s are proven or conjectured in [1]. Another property that was not noticed then is given in the following.

Theorem. If $p \equiv 3 \pmod 4$ has g as a F. P. R., then $g - 1$ and $g - 2$ are also primitive roots of p.

Examples. From [1, Table 1, p. 164].

p = 11 has 8, 7, 6 as primitive roots;
p = 19 has 15, 14, 13 as primitive roots;
p = 31 has 13, 12, 11 as primitive roots.

Proof. Since

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

$g - 1$ is the inverse of g (mod p) and therefore is a primitive root of p if g is. Next,

$$(g - 1)^2 = g^2 - 2g + 1 \equiv -g + 2 \pmod{p}$$

from (1) and, since $p = 4k + 3$,

$$(g - 1)^{2k+1} \equiv -1 \pmod{p} .$$

Therefore,

$$(g - 1)^{2k+3} \equiv g - 2 \pmod{p} ,$$

and since $2k + 3$ is prime to $4k + 2$, $g - 2$ is also a primitive root of p.

2. ASYMPTOTIC DENSITY

What ratio r of all primes $p \equiv 3 \pmod 4$, asymptotically speaking, have such a triple of primitive roots? By [1, p. 167] it is immediate that the proper conjecture is

(2) $$r \overset{?}{=} \frac{18}{19} A = 0.35427\ 39286\ 91876$$

where A is Artin's constant. By the discussion in [1] there is little doubt that (2) is true even though it is not now provable.

3. OTHER TRIPLES

Another criterion, entirely different, for three consecutive primitive roots is this, cf. [2, p. 80, Ex. 61]. If

$$p = 8k + 7 \quad \text{and} \quad q = 4k + 3$$

are both prime, then

$$p - 2, \quad p - 3, \quad p - 4 \tag{3}$$

are primitive roots of p.

This is easily proven. As an example, $p = 23$ (having $q = 11$) has 21, 20, 19 as primitive roots.

Now, what primes p simultaneously satisfy both sufficient conditions, and thereby have both triples, that in (3) and the

$$g, \quad g - 1, \quad g - 2 \tag{4}$$

triple above? It is easily seen that any such p must satisfy $p \equiv 119 \pmod{120}$ and therefore that the run (3) extends, at least, to

$$p - 2, \quad p - 3, \quad p - 4, \quad p - 5, \quad p - 6. \tag{5}$$

The smallest example is $p = 359$ with primitive roots

(4a) 106, 105, 104, also 103,

and

(5a) 357, 356, 355, 354, 353 .

The next example is $p = 479$ with

(4b) 229, 228, 227, also 226,

and the powerful run

(5b) 477, 476, 475, 474, 473, also
472, 471, 470, 469, 468, 467.

The run of 11 in (5b) is due to the fact that 479 is a "negative square." See [3, Table II, p. 436] and the discussion there for an explanation of this last point.

REFERENCES

1. Daniel Shanks, "Fibonacci Primitive Roots," Fibonacci Quarterly, Vol. 10, 1972, pp. 163-181.
2. Daniel Shanks, Solved and Unsolved Problems in Number Theory, Vol. 1, Spartan, New York, 1962.
3. D. H. Lehmer, Emma Lehmer, and Daniel Shanks, "Integer Sequences Having Prescribed Quadratic Character," Math. Comp., Vol. 24, 1970, pp. 433-451.