ON THE QUADRATIC CHARACTER OF THE FIBONACCI ROOT

Emma Lehmer
Berkeley, Calif.

Let $\theta = (1+\sqrt{5})/2$ be a root of the quadratic equation

$$x^2 - x - 1 = 0 \; .$$

The n-th term of the Fibonacci sequence can be given by

$$F_n = \frac{\theta^{2n} - (-1)^n}{\sqrt{5}\,\theta^n} \tag{1}$$

Hence for any prime $p \neq 5$ we can state the criterion:

$$F_n \equiv 0 \pmod{p} \text{ \underline{if} \underline{and} \underline{only} \underline{if} } \theta^{2n} \equiv (-1)^n \pmod{p} \; . \tag{2}$$

If we define $\varepsilon = \pm 1$ in terms of the Legendre symbol as

$$\varepsilon = \left(\frac{5}{p}\right) \equiv 5^{\frac{p-1}{2}} \pmod{p} \qquad p \neq 5 \tag{3}$$

then a special case of Lucas' theorem [1] states

$$F_{p-\varepsilon} \equiv 0 \pmod{p} \tag{4}$$

while a special case of a theorem of Lehmer [2] gives

$$F_{\frac{p-\varepsilon}{2}} \equiv 0 \pmod{p} \text{ if and only if } p = 4m+1 \; . \tag{5}$$

Both (4) and (5) follow immediately from the criterion (2) and the easily verifiable congruence

$$\theta^{p-\varepsilon} \equiv \varepsilon \pmod{p} \tag{6}$$

It is the purpose of this note to give a criterion for the quadratic character of θ and to apply it to find the condition for the divisibility of

$$F_{\frac{p-\varepsilon}{4}}$$

by p.

In the first place, if p divides

$$F_{\frac{p-\varepsilon}{4}},$$

then it must also divide

$$F_{\frac{p-\varepsilon}{2}}$$

and therefore by (5) we have $p = 4m+1$, but since $(p - 6)/4$ must be an integer, $\varepsilon = 1$, so that $p = 20m+1, 9$. The quadratic character of θ for such primes is contained in the following lemma.

Lemma

(7) $$\theta^{\frac{p-1}{2}} = \left(\frac{\theta}{p}\right) = \begin{cases} \left(\sqrt{\frac{5}{p}}\right) & \text{if } p = 10m+1 \\ -\left(\sqrt{\frac{5}{p}}\right) & \text{if } p = 10m-1 \end{cases}$$

Proof. Let α be a primitive fifth root of unity so that $\alpha^5 = 1$, while $\alpha \neq 1$, then it is well known that

(8) <u>α is an integer modulo p if and only if</u> $p = 10m+1$.

It is also clear that we can write $\Theta = -(\alpha + \alpha^{-1})$ so that $\alpha^2 + \alpha + 1 = 0$ and hence

(9) $$\alpha = \frac{-\Theta \pm \sqrt{\theta^2 - 4}}{2}$$

Considering (9) as a congruence modulo p and remembering that is an integer for the primes under consideration we see that α will be an integer modulo p only when $\theta^2 - 4$ is a quadratic residue. But

(10) $$\theta^2 - 4 = (\theta - 2)(\theta + 2) = -(\theta - 1)^2 \theta\sqrt{5} \quad .$$

Hence α is an integer modulo p if and only if 5 is a quadratic residue of p. Hence by (8) we obtain

(11) $$\left(\frac{\theta\sqrt{5}}{p}\right) = \begin{cases} 1 & \text{if } p = 10m+1 \\ -1 & \text{if } p = 10m-1 \end{cases}$$

from which (7) and the lemma follow at once.

But the quadratic character of $\sqrt{5}$ is the same as the quartic character of 5 and this has been expressed in terms of the quadratic partition

(12) $$p = a^2 + b^2 \,, \quad a \equiv 1 \pmod 4)$$

as follows [3] :

5 *is a quartic residue of* $p = 4m+1$ *if and only if* $b \equiv 0 \pmod 5$

5 *is a quadratic, but not a quartic residue of* p *is and only if* $a = 0 \pmod 5$.

Hence our lemma leads to the following theorem.

Theorem 1. Let $p = a^2 + b^2$ *with* $a \equiv 1 \pmod 4$, *then*

$$\theta^{\frac{p-1}{2}} = \left(\frac{\theta}{p}\right) = \begin{cases} 1 \text{ if } p=20m+1,\ b\equiv 0 \pmod 5 \text{ or } p=20m+9,\ a=0 \pmod 5 \\ -1 \text{ if } p=20m+1,\ a\equiv 0 \pmod 5 \text{ or } p=20m+9,\ b\equiv 0 \pmod 5 \end{cases}$$

Combining Theorem 1 with condition (2) for $n = (p-1)/4$ we obtain

Theorem 2. Let $p = a^2 + b^2$ *with* $a \equiv 1 \pmod 4$, *then*

$$F_{\frac{p-1}{4}} \equiv 0 \pmod p \quad \text{if and only if}$$

$$\text{either } p = 40m+1, 29 \quad \text{and} \quad b \equiv 0 \pmod 5$$

$$\text{or } p = 40m+9, 21 \quad \text{and} \quad a \equiv 0 \pmod 5$$

The primes $p < 1000$ satisfying theorem 2 are

p = 61, 89, 109, 149, 269, 389, 401, 421, 521, 661, 701, 761, 769, 809, 821, 829

The primes $p < 1000$ for which θ is a quadratic residue are

p = 29, 89, 101, 181, 229, 349, 401, 461, 509, 521, 541, 709, 761, 769, 809, 941

θ = 6, 10, 23, 14, 82, 144, 112, 22, 122, 100, 173, 171, 92, 339, 343, 228

For some of these primes the following theorem holds.

Theorem 3. If θ *is a quadratic, but not a higher power residue of a prime* $p = 10n\pm1$, *then all the quadratic residues of* p *can be generated by addition as follows:*

$$r_0 = 1,\ r_1 = \theta \pmod p,\ r_{n+1} = r_n + r_{n-1} \pmod p$$

This follows at once from the fact that $\theta^n + \theta^{n+1} = \theta^n(\theta + 1) = \theta^{n+2}$. For example for $p = 29$, $\theta = 6$, all the quadratic residues are

$$1, 6, 7, 13, 20, 4, 24, 28, 23, 22, 16, 9, 25, 5$$

after which the sequence repeats modulo p.

Further results along the lines of Theorems 1 and 2 are as follows.

Marguerite Dunton conjectured and the author proved for $p=30m+1$ that θ is a cubic residue of p, and hence that p divides

$$F_{\frac{p-1}{3}},$$

if and only if p is represented by the form

$$p = s^2 + 135\, t^2$$

The proof uses cyclotomic numbers of order 15 and is too long to give here. Such primes < 1000 are 139, 151, 199, 331, 541, 619, 661, 709, 811, 829 and 919. The author 4 has shown that θ is a quintic residue of p and hence that

$$F_{\frac{p-1}{5}}$$

is divisible by p if and only if p is an "artiad" of Lloyd Tanner [5]. The artiads < 1000 are 211, 281, 421, 461, 521, 691, 881 and 991.

REFERENCES

1. E. Lucas, Amer. Jn. of Math. 1, 1878, pp. 184-239, 289-321.
2. D. H. Lehmer, Annals of Math. 1930, v. 31, pp. 419-448.
3. Emma Lehmer, Matematika, v. 5, 1958, pp. 20-29.
4. Emma Lehmer, to appear in Jn. of Math. Analysis and Applications.
5. Lloyd Tanner, London Mat. Soc. Proc. 18 (1886-7), pp. 214-234. also v. 24, 1892-3, pp. 223-262.

XXXXXXXXXXXXXX