GENERALIZED FIBONACCI PRIMITIVE ROOTS, AND CLASS NUMBERS OF REAL QUADRATIC FIELDS*

R. A. MOLLIN
Mathematics Department, University of Calgary
2500 University Drive N.W., Calgary, Alberta, Canada, T2N 1N4

(Submitted June 1986)

1. INTRODUCTION

It is the purpose of this paper to generalize the concept of Fibonacci primitive roots introduced by Shanks in [22]. This work was motivated by attempts to prove a conjecture of S. Chowla on class numbers of certain real quadratic fields. The generalized Fibonacci primitive roots which we introduce are interesting in their own right. Moreover, it turns out that Chowla's conjecture is more closely related to a generalized sequence of Fibonacci numbers which we introduce in §2 as a precursor to the generalized Fibonacci primitive roots. Thus, we first establish the generalized Fibonacci primitive roots and several of their properties in §2 before displaying the connection with the motivating work on Chowla's conjecture, at the end of the paper in §3.

2. GENERALIZED FIBONACCI PRIMITIVE ROOTS

Linear recurring sequences of the second order have been extensively explored since the last century. We have such sequences of integers $\{G_i\}$ defined by $G_i = mG_{i-1} + nG_{i-2}$ for $i > 1$, where G_0, G_1, m and n are given integers. There has more recently been a plethora of papers dealing with these sequences as generalized Fibonacci numbers. As evidence, the reader may consult any of [1]-[4], [6]-[17], [20]-[21], and [26]-[31]. However, heretofore, there has been no generalization of Fibonacci primitive roots in the literature.

We consider the particular case of the G_i where $m = 1$ and $n > 0$. Set $G_i = F_i(n)$ and let $F_0(n) = 1$ and $F_1(n) = g$, a positive integer. Thus,

$$F_i(n) = F_{i-1}(n) + nF_{i-2}(n), \text{ for } i > 1.$$

*The author's research is supported by N.S.E.R.C. Canada, grant #A8484.

Call $\{F_i(n)\}$ the n^{th}-*Fibonacci sequence with base* g (or simply the n^{th}-FS base g). The first Fibonacci sequence with base 1 is the ordinary Fibonacci sequence. Now let p be a prime and let g be a primitive root modulo p. We call g an n^{th}-*Fibonacci primitive root modulo* p (or simply an n^{th}-FPR mod p) if satisfies:

$$x^2 \equiv x + n \pmod{p}, \tag{1}$$

where g.c.d. $(p, n) = 1$. The $n = 1$ case yields the ordinary Fibonacci primitive roots introduced by Shanks [22] and for which properties were developed in [23] and [24] which, among others, we will have occasion to generalize later.

For the remainder of the paper we assume that p is an odd prime and n is a positive integer.

Lemma 1: If the positive integer g is a solution of (1), then

$$F_i(n) \equiv gF_{i-1}(n) \equiv g^i \pmod{p}$$

for all positive integers i.

Proof: We use induction on i. If $i = 1$, then $F_1(n) = g = gF_0(n)$. By definition of the n^{th}-FS base g, we have that $F_i(n) = F_{i-1}(n) + nF_{i-2}(n)$ for $i > 1$. By induction hypothesis:

$$F_{i-1}(n) \equiv gF_{i-2}(n) \equiv g^{i-1} \pmod{p}. \tag{2}$$

Therefore, $F_i(n) \equiv (g + n)F_{i-2}(n) \pmod{p}$. Thus, from (1), we obtain:

$$F_i(n) \equiv g^2F_{i-2}(n) \pmod{p}.$$

Hence, from (2) again, we get:

$$F_i(n) \equiv gF_{i-1}(n) \equiv g^i \pmod{p}. \quad \text{Q.E.D.}$$

As an illustration of Lemma 1, we have:

Example 1: Let $n = 5$, $p = 101$, and $g = 42$; 42 is a 5^{th}-FPR mod 101. Moreover:

$$F_0(5) = 1,\ F_1(5) = 42,\ F_2(5) = 47 = 42 + 5 \equiv 42^2,$$
$$F_3(5) = 257 = 47 + 5 \cdot 42 \equiv 42 \cdot 47 \equiv 42^3,$$
$$F_4(5) = 492 = 257 + 5 \cdot 47 \equiv 42 \cdot 257 \equiv 42^4,$$
$$F_5(5) = 1777 = 492 + 5 \cdot 257 \equiv 42 \cdot 492 \equiv 42^5,$$

etc. (where $\equiv$ denotes congruence modulo 101).

The following observations will prove to be useful, and they generalize Shanks [23, A-D, p. 164].

Remark 1: If g is an n^{th}-FPR mod p, then either

$$4n \equiv -1 \pmod{p} \quad \text{or} \quad ((4n + 1)/p) = 1,$$

where $(*/*)$ denotes the Legendre symbol. This is verified from the observation that $(2g - 1)^2 \equiv 4n + 1 \pmod{p}$ if (1) is satisfied by g.

Remark 2: If $(-n/p) = -1$, then there exists at most one n^{th}-FPR mod p. To see this, we observe that the two solutions of (1) are

$$g_1 = (1 + \sqrt{4n + 1})/2 \quad \text{and} \quad g_2 = (1 - \sqrt{4n + 1})/2;$$

whence, $g_1 g_2 \equiv -n \pmod{p}$. Therefore, one of g_1 or g_2 is a quadratic residue and the other is not. Hence, there is at most one n^{th}-FPR mod p. We now give examples of each case.

Example 2: If $n = 4$ and $p = 19$, $g = 13$ is a 4^{th}-FPR mod 19. Since $(-4/19) = -1$, $g = 13$ is the only 4^{th}-FPR mod 19 by Remark 2.

Example 3: If $n = 1$ and $p = 3$, then $((4n + 1)/p) = (5/3) = -1$, whence 3 has no 1^{st}-FPR by Remark 1.

Remark 3: If $(-n/p) = 1$, there may be two, one, or no n^{th}-FPR's mod p. The following examples illustrate the three cases.

Example 4: If $n = 2$ and $p = 41$, the solutions of (1) are $g_1 = 2$ and $g_2 = 40$, both of which are quadratic residues modulo 41. Hence, 41 has no 2^{nd}-FPR's.

Example 5: If $n = 3$ and $p = 13$, $g = 7$ is a 3^{rd}-FPR mod 13. However, $7^2 \equiv -3 \pmod{13}$ and $7x \equiv -3 \pmod{13}$ has only one solution. Hence, there is exactly one 3^{rd}-FPR mod 13.

Example 6: If $n = 6$ and $p = 7$, then $g_1 = 3$ and $g_2 = 5$ are 6^{th}-FPR's mod 7.

Remark 4: If two n^{th}-FPR's mod p exist, say g_1 and g_2 with $0 < g_i < p$ for $i = 1, 2$, then $g_1 + g_2 = 1 + p$. This follows from Remark 2. As an instance of this, see Example 6, where $g_1 + g_2 = 8 = p + 1$.

In Remarks 2 and 3, we saw that it is possible that no n^{th}-FPR's mod p exist. We now provide a class of primes p for which an n^{th}-FPR mod p always exists. First we need a preliminary result that generalizes an idea of Shanks and Taylor [24].

Lemma 2: Suppose that either $n = 1$ or $p > n > 2$ and $p = 1 + 2q$ where q is prime and n has order q modulo p. If g is a solution of (1), then g is a primitive root modulo p if and only if $g - 1$ is one.

Proof: If $n = 1$, then $g(g - 1) \equiv 1 \pmod{p}$ implies that g and $g - 1$ have the same order modulo p. Now we assume $p > n > 2$, $p = 2q + 1$, and n has order q modulo p. Since $g(g - 1) \equiv n \pmod{p}$ from (1), we get $g^q \equiv (g - 1)^{-q} \pmod{p}$. If g is a primitive root modulo p, then $(g - 1)^q \equiv -1 \pmod{p}$. We cannot have $g - 1 \equiv -1 \pmod{p}$, whence $g - 1$ is a primitive root modulo p. Conversely, if $g - 1$ is a primitive root modulo p, then $g^q \equiv -1 \pmod{p}$. If $g \equiv -1 \pmod{p}$, then from (1) we get that $n \equiv 2 \pmod{p}$, contradicting the hypothesis. Q.E.D.

The following example illustrates the above.

Example 7: Let $p = 47$, $g = 20$, and $n = 4$. 4 has order 23 modulo 47, 20 is a primitive root mod 47, and $g = 20$ is a solution of (1), whence 19 is a primitive root mod 47.

Now, we provide a sufficient condition for the existence of an n^{th}-FPR mod p. The following generalizes Mays's [18, Theorem, p. 111]. We follow Mays's reasoning in the initial part of the proof.

Theorem 1: Suppose that $n = 1$ or $p > n > 2$, and $((4n + 1)/p) = 1$ where $p = 1 + 2q$ is a prime with q an odd prime. Furthermore, suppose that either $n = 1$ or n has order q modulo p. Then p has an n^{th}-FPR.

Proof: Since $p \equiv 3 \pmod{4}$, at most one of α or $-\alpha$ is a primitive root modulo p for any α in the range $2 \leqslant \alpha \leqslant (p - 1)/2 = q$. But there are exactly

$$\phi(p - 1) = q - 1 = (p - 3)/2$$

primitive roots modulo p, so exactly one of α or $-\alpha$ is a primitive root modulo p. Since $((4n + 1)/p) = 1$, there are two distinct solutions of (1), namely, g and $1 - g$ (see Remarks 1 and 2). It suffices to show that either g or $1 - g$ is a primitive root modulo p. Suppose that g is not a primitive root modulo p. Then, by Lemma 2, $g - 1$ is not a primitive root modulo p. Also, $g - 1 \neq 0, \pm 1 \pmod{p}$ because g satisfies (1) and $n \neq 0, 2$. Consequently, $g - 1 \equiv \pm\beta \pmod{p}$ for some β satisfying $2 \leqslant \beta \leqslant (p - 1)/2 = q$; and so, $1 - g$ is a primitive root modulo p. Q.E.D.

The following generalizes Shanks-Taylor [24, Theorem, p. 159].

Theorem 2: Suppose that either $n = 1$ or $p > n > 2$, and $p = 1 + 2q$, where q is an odd prime and n has order q modulo p. If g is an n^{th}-FPR mod p, then $g - 1$ and $g - (n + 1)$ are primitive roots modulo p.

Proof: By Lemma 2, $g - 1$ is a primitive root modulo p. Therefore, since

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

we get

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

Since g.c.d. $(2q, 2 + q) = 1$, we see that $g - (n + 1)$ is a primitive root modulo p. Q.E.D.

Corollary 1: Suppose that n is a positive integer such that $((4n + 1)/p) = 1$, where $p = 1 + 2q$ is prime, with q an odd prime. Further, suppose that either $n = 1$ or $p > n > 2$, where n has order q modulo p. Then, there is an n^{th}-FPR mod p. If g is such an FPR, then $g - 1$ and $g - (n + 1)$ are primitive roots modulo p.

Proof: The proof follows immediately from Theorems 1 and 2.

The following illustrates Corollary 1.

Example 8: Let $n = 3$ and $p = 23$. Then,

$$((4n + 1)/p) = (13/23) = 1 \equiv 3^{11} \pmod{23}.$$

Thus, the hypothesis of Corollary 1 is satisfied and 15 is the 3^{rd}-FPR mod 23. Moreover, $14^{11} \equiv -1 \pmod{23}$ and $11^{11} \equiv -1 \pmod{23}$.

We close this section with the observation that it is possible to give a more restrictive generalization of Fibonacci primitive roots, albeit a natural one.

Let n be a positive integer and p a prime with $p \equiv 1 \pmod{n}$. Define g to be an n^{th}-FPR modulo p whenever g has order $(p - 1)/n$ modulo p and (1) is satisfied by g.

Example 9: If $n = 3$, $p = 103$, and $g = 31$, then 31 satisfies (1) and has order 34 modulo 103. Hence, under the preceding definition, 31 is a 3^{th}-FPR mod 103, but it is not one under the earlier definition.

Example 10: If $n = 2$ and $p = 5$, then 2 satisfies (1) but 2 is a primitive root modulo 5, so 2 is not a 2^{nd}-FPR mod 5 under the preceding definition but it is one under the earlier definition.

It would be of interest to see what developments would come out of a study of the latter definition.

3. CLASS NUMBERS OF REAL QUADRATIC FIELDS

In [5] S. Chowla conjectured that, if $p = m^2 + 1$ is prime and $m > 26$, then $h(p) > 1$ where $h(p)$ is the class number of $Q(\sqrt{p})$. In [19] we established that, if $r = m^2 + 1 > 17$ is square free where either r is composite or $m \neq 2q$ for an odd prime q, then $h(r) > 1$. Furthermore, we showed that in the remaining case, $h(r) = 1$ for at most finitely many q. Also we established

Theorem 3: Let $r = 4m^2 + 1$ be square free where m is a positive integer. Then the following are equivalent.

(a) $h(r) = 1$.

(b) p is inert in $Q(\sqrt{r})$ for all primes $p < m$.

(c) $f(x) = -x^2 + x + m^2 \not\equiv 0 \pmod{p}$ for all integers x and primes p satisfying $0 < x < p < m$.

(d) $f(x)$ is equal to a prime for all integers x satisfying $1 < x < m$.

The following links §2 and §3 and provides a criterion for the solvability of (1). For convenience, we let $F_i(n) = F_i$ in what follows.

Theorem 4: If n is a positive integer relatively prime to p, then g is a solution of (1) if and only if the n^{th}-FS base g satisfies $F_{i+1}F_{i-1} \equiv F_i^2 \pmod{p}$ for some $i > 1$. Moreover, if g is a solution of (1), then $F_{i+1}F_{i-1} \equiv F_i^2 \pmod{p}$ for all $i > 0$.

Proof: By Horadam [12, (27), p. 440]: $F_{i+1}F_{i-1} - F_i^2 = (-n)^{i-1}(g + n - g^2)$ for all $i > 0$. The result follows. Q.E.D.

Therefore, we have the following conjecture based on the preceding data.

Conjecture: If $n = q^2$, where $q > 13$ is an odd prime and $4q^2 + 1$ is prime, then there is an n^{th}-FS base g, $\{F_i(n)\}$, for some g satisfying $F_{i+1}F_{i-1} \equiv F_i^2 \pmod{p}$ for a prime p with $0 < g < p < q$.

ACKNOWLEDGMENT

The author welcomes the opportunity to thank the referee for many valuable comments and suggestions.

REFERENCES

1. R. V. Anderson. "Generalized Fibonacci Sequences as Powers of a Square Matrix." *Univ. Lisboa Revista Fac. Ci A 14* (1972-1973):113-21.
2. G. E. Bergum & V. E. Hoggatt, Jr. "An Application of the Characteristic of the Generalized Fibonacci Sequence." *The Fibonacci Quarterly 15*, no. 3 (1977):215-20.
3. G. Berzsenyi. "Sums of Products of Generalized Fibonacci Numbers." *The Fibonacci Quarterly 13*, no. 4 (1975):343-44.
4. M. W. Bunder. "A Special Case of the Generalized Fibonacci Sequence over an Arbitrary Ring with Identity." *The Fibonacci Quarterly 13*, no. 3 (1975): 280.
5. S. Chowla & J. Friedlander. "Class Numbers and Quadratic Residues." *Glasgow Math. J. 17* (1976):47-52.
6. D. E. Daykin, L. A. Presel, & A. J. W. Hilton. "The Structure of Second Order Sequences in a Finite Field." *J. Reine Angew. Math. 270* (1974):77-96.
7. L. E. Fuller. "Geometric Recurrence Relation." *The Fibonacci Quarterly 18*, no. 2 (1980):126-29.
8. L. E. Fuller. "Representations for r, s Recurrence Relations." *The Fibonacci Quarterly 18*, no. 2 (1980):129-35.
9. W. Gerdes. "Generalized Fibonacci Numbers and Their Convergent Sequences." *The Fibonacci Quarterly 16*, no. 3 (1978):269-75.
10. A. F. Horadam. "On Generating Functions for Powers of a Generalized Sequence of Numbers." *The Fibonacci Quarterly 12*, no. 4 (1974):348, 350, 353, 362.
11. A. F. Horadam. "Extensions of a Paper on Diagonal Functions." *The Fibonacci Quarterly 18*, no. 1 (1980):1, 3-8.
12. A. F. Horadam. "Generating Functions for Powers of a Certain Generalized Sequence of Numbers." *Duke Math. J. 32* (1965):437-46.
13. D. V. Jaisival. "Some Geometrical Properties of the Generalized Fibonacci Sequence." *The Fibonacci Quarterly 12*, no. 1 (1974):67-70.
14. B. W. King. "A Polynomial with Generalized Fibonacci Coefficients." *The Fibonacci Quarterly 11*, no. 6 (1973):527-32.
15. H. V. Krishna. "Identities of a Generalized Fibonacci Sequence." *A Collection of Manuscripts Related to the Fibonacci Sequence*. Santa Clara, Calif.: The Fibonacci Association, 1980, pp. 65-66.
16. H. V. Krishna. "Divisibility Properties of a Generalized Fibonacci Sequence." *Ibid.*, pp. 66-67.
17. C. L. Lau. "The Periodic Generating Sequence." *The Fibonacci Quarterly 15*, no. 2 (1977):178-82.

18. M. E. Mays. "A Note on Fibonacci Primitive Roots." *The Fibonacci Quarterly 20*, no. 2 (1982):111.

19. R. A. Mollin. "Necessary and Sufficient Conditions for the Class Number of a Real Quadratic Field To Be One, and a Conjecture of S. Chowla." (To appear in *Proc. Amer. Math. Soc.*)

20. J. C. Parnami & T. N. Shorey. "Subsequences of Binary Recursive Sequences." *Acta Arith. 40* (1981-1982):193-96.

21. H. J. A. Sallé. "A Maximum Value for the Rank of Apparition of Integers in Recursive Sequences." *The Fibonacci Quarterly 13*, no. 2 (1975):159-61.

22. D. Shanks. *Solved and Unsolved Problems in Number Theory*. 2nd ed. New York: Chelsea, 1978.

23. D. Shanks. "Fibonacci Primitive Roots." *The Fibonacci Quarterly 10*, no. 2 (1972):163-68, 181.

24. D. Shanks & L. Taylor. "An Observation on Fibonacci Primitive Roots." *The Fibonacci Quarterly 11*, no. 2 (1973):159-60.

25. A. G. Shannon & A. F. Horadam. "Reciprocals of Generalized Fibonacci Numbers." *The Fibonacci Quarterly 9*, no. 4 (1971):299-306, 312.

26. C. Smith & V. E. Hoggatt, Jr. "Primitive Periods of Generalized Fibonacci Sequences." *The Fibonacci Quarterly 14*, no. 4 (1976):343-47.

27. L. Somer. "Fibonacci-Like Groups and Periods of Fibonacci-Like Sequences." *The Fibonacci Quarterly 15*, no. 1 (1977):35-41.

28. M. N. S. Swamy. "On Generalized Fibonacci Quaternions." *The Fibonacci Quarterly 11*, no. 6 (1973):547-49.

29. M. E. Waddill. "Matrices and Generalized Fibonacci Sequences." *The Fibonacci Quarterly 12*, no. 4 (1974):381-86.

30. J. E. Walton & A. F. Horadam. "Some Aspects of Generalized Fibonacci Numbers." *The Fibonacci Quarterly 12*, no. 3 (1974):241-50.

31. J. E. Walton & A. F. Horadam. "Some Further Identities for the Generalized Fibonacci Sequence $\{H_n\}$." *The Fibonacci Quarterly 12*, no. 3 (1974):272-80.

Note added in proof: Since the writing of this paper, substantial progress has been made. The author and H. C. Williams have used a suitable Riemann hypothesis to prove the Chowla conjecture. In fact, we have found *all* real quadratic fields of Richaud-Degert-type having class number one.

◆◇◆◇◆