COMPLETE FIBONACCI SEQUENCES IN FINITE FIELDS

Owen J. Brison
Faculdade de Ciências, Rua Ernesto de Vasconcelos, Bloco C1, Piso 3, 1700 Lisbon, Portugal
(Submitted November 1990)

1. Introduction

In certain finite fields $\mathbb{F}_p$ of prime order p, it is possible to write the set of nonzero elements, without repetition, in such an order that they form a closed Fibonacci-type sequence. For example, in $\mathbb{F}_{11}$ we may write

1, 8, 9, 6, 4, 10, 3, 2, 5, 7,

which evidently has the required property. In [1], a similar example is given for $\mathbb{F}_{109}$. It is implicit in [1], [12], that such sequences exist in $\mathbb{F}_p$ if $\mathbb{F}_p$ contains a so-called Fibonacci Primitive Root, or FPR: see below for definitions. Here we show (Theorem 4.2) that such sequences exist in $\mathbb{F}_p$ if and only if $\mathbb{F}_p$ contains an FPR; moreover, when $\mathbb{F}_p$ does contain an FPR, we show that the only such sequences to exist are the "natural" ones: that is, the sequences of successive powers of FPRs. Of course, it was shown in [1] that if the sequence of successive powers of an element is to have this Fibonacci property, then the element in question must be an FPR, but here we allow for any sequence of elements.

We also prove (Theorem 4.4) analogous results for Fibonacci-type sequences of the set of (nonzero) squares of $\mathbb{F}_p$. In this context, the sequence

1, 4, 5, 9, 3,

is a Fibonacci-type sequence of the squares of $\mathbb{F}_{11}$.

It will be shown that, except for the fields $\mathbb{F}_4$ and $\mathbb{F}_9$, these phenomena only occur in the fields of prime order.

We wish to thank the referee for pointing out several references, and in particular for the information that part of Theorem 2.5 below is proved in [10].

2. Preliminaries

In this section we collect some preliminaries from [3], [7], [8], [14], and [15]; p will always denote a prime, q will stand for a power of p, $\mathbb{F}_q$ will denote the field of order q, $\mathbb{F}_q^*$ will denote the multiplicative group of $\mathbb{F}_q$, while F_n and L_n will, respectively, denote the n^{th} Fibonacci and n^{th} Lucas number. In addition, if z is an integer, then $\overline{z}$ will denote the image of z in $\mathbb{F}_p$ (in situations where the prime p is understood). If g is an element of a group, then $|g|$ will denote the order of g.

A Φ-sequence in a finite field $\mathbb{F}$ is defined to be a sequence

$$\mathfrak{S} = (s_0, s_1, s_2, \ldots) \quad (s_i \in \mathbb{F}),$$

where

$$s_{n+2} = s_{n+1} + s_n \text{ for } n = 0, 1, 2, \ldots .$$

Any Φ-sequence in $\mathbb{F}_q$ is periodic with period $r \le q^2 - 1$: see [7, Th. 8.7]. This means that

$$s_{n+r} = s_n \text{ for } n = 0, 1, 2, \ldots,$$

and that r is the least natural number for which this holds. Following Wall [15], we write $k(p)$ for the period of the Fibonacci sequence (mod p); note that De Leon [3] writes $A(p)$ for this number, while Vajda [14] writes $P(p, F)$.

Theorem 2.1: ([7, Th. 8.16]). If r is the period of some Φ-sequence in $\mathbb{F}_q$, where $q = p^n$, then $r \mid k(p)$. $\square$

Theorem 2.2: (Wall, [15]; see also [14, p. 91]). Let p be a prime. Then

(a) $k(p) \mid p - 1$ if $p \equiv \pm 1 \pmod 5$.

(b) $k(p) \mid 2(p + 1)$ if $p \equiv \pm 2 \pmod 5$. $\square$

The polynomial $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$ is what is called [7, p. 198], the *characteristic polynomial* of a Φ-sequence. We have

Theorem 2.3: ([7, Th. 8.21]). Let $p \neq 5$ be a prime. Let $s_0, s_1, \ldots,$ be a Φ-sequence in $\mathbb{F}_q$. Let $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$ and suppose that g, h are the roots of $f(t)$ in a splitting field $\mathbb{F} \supset \mathbb{F}_q$. Then there exist $\alpha, \beta \in \mathbb{F}$ such that

$$s_i = \alpha g^i + \beta h^i, \text{ for } i = 0, 1, 2, \ldots . \quad \square$$

Lemma 2.4: Let p be an odd prime and let $n \in \mathbb{N}$ be such that

$$(p^n - 1)/2 \mid 2(p + 1).$$

Then $p \leq 5$ and $n \leq 2$.

Proof: We have

$$(p - 1)(p^{n-1} + \cdots + 1)\ 4(p + 1).$$

But $(p - 1, p + 1) = 2$, because p is odd. Thus $(p - 1) \mid 8$, and so $p \in \{3, 5\}$. If $n \geq 3$ we may easily derive a contradiction, and the assertion follows.

The first four parts of the following theorem are a combination of results from [3], [10], [11], and [12] (but note that we are working in an extension field $\mathbb{F} \supset \mathbb{F}_p$ rather than in $\mathbb{F}_p$). Proofs of parts (a)-(c) can be found in Phong [10, pp. 68-69], or can be extracted from a careful reading of De Leon [3], together with Wall's result that $k(p)$ is even for $p > 2$: [11, Th. 4]. Part (d) is proved by Shanks [12, p. 164]. We supply proofs for completeness.

Theorem 2.5: Let $p \geq 7$ be a prime. Let g, h be the roots, in a suitable extension field $\mathbb{F} \supseteq \mathbb{F}_p$, of the polynomial

$$f(t) = t^2 - t - 1 \in \mathbb{F}_p[t].$$

Then

(a) Not both $|g|$ and $|h|$ can be odd. If, say, $|h|$ is odd, then $|g| = 2|h|$.

(b) If both $|g|$, $|h|$ are even, then $|g| = |h|$ is divisible by 4.

(c) If $|g|$, say, is even, then $|g| = k(p)$. In particular, $k(p)$ is even.

(d) We have $g, h \in \mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod 5$.

(e) If $|g|$, say, is of the form $p^n - 1$ or $(p^n - 1)/2$, for $n \in \mathbb{N}$, then $n = 1$, $g \in \mathbb{F}_p$, and $p \equiv \pm 1 \pmod 5$.

Proof: Since g, h are the roots of $f(t) = t^2 - t - 1$, then $g = -1/h$. Write $|g| = a$ and $|h| = b$.

(a) Suppose that b is odd, and note that $b = |1/h|$. Since $|-1| = 2$, it follows that $|g| = 2|1/h|$, and thus that $a = 2b$.

(b) Suppose that a, b are both even. Then we have

$$1 = g^a = (-1)^a/h^a = 1/h^a$$

and so $h^a = 1$. Similarly, $g^b = 1$, and so $a = b$. Suppose that $a = 2d$ with d odd. Then $|g^d| = 2$ and so $g^d = -1$, the unique element of order 2 in $\mathbb{F}_p^*$. But then

$$h^d = (-1)^d/g^d = -1/-1 = 1,$$

and so b is odd, contrary to hypothesis. Assertion (b) now follows.

(c) We adapt the proof of [3, Lem. 1]. It follows by induction that $g^n = \overline{F}_n g + \overline{F}_{n-1}$ for any natural number n (and similarly for h^n). Since $\overline{F}_{k(p)} = 0$ and $\overline{F}_{k(p)-1} = 1$, it follows that $g^{k(p)} = 1$ and thus that $a|k(p)$. Similarly, $b|k(p)$. In particular, $k(p)$ must be even. If $\overline{F}_a = 0$, then $1 = g^a = \overline{F}_{a-1}$; thus, $k(p)|a$ and so $k(p) = a$. Similarly, if $\overline{F}_b = 0$, then $k(p) = b$. Suppose then that $\overline{F}_a \neq 0$ and $\overline{F}_b \neq 0$. Then $1 = g^a = \overline{F}_a g + \overline{F}_{a-1}$ and so $g = (1 - \overline{F}_{a-1})/\overline{F}_a$. Thus, as in [3], we have

$$\begin{aligned} 0 &= (g^2 - g - 1)\overline{F}_a^2 \\ &= -(\overline{F}_a^2 - \overline{F}_a\overline{F}_{a-1} - \overline{F}_{a-1}^2) - (\overline{F}_a + 2\overline{F}_{a-1}) + 1 \\ &= (-1)^a - \overline{L}_a + 1. \end{aligned}$$

Thus, $\overline{L}_a = 1 + (-1)^a$. Similarly, $\overline{L}_b = 1 + (-1)^b$.

Now, if a is even, then $\overline{L}_a = 2$. But $\overline{L}_a^2 - 5\overline{F}_a^2 = 4$ and so $\overline{F}_a = 0$, a contradiction. Thus, a must be odd. Similarly, b must also be odd. But this is in contradiction to (a). It follows that at least one of $\overline{F}_a$, $\overline{F}_b$ must be zero, and assertion (c) follows.

(d) We have $(2g - 1)^2 = 5 \in \mathbb{F}_p$. On the other hand, if $w \in \mathbb{F}_p$ satisfies $w^2 = 5$, then $(1 \pm w)/2$ are the roots of $f(t)$. Thus, $g, h \in \mathbb{F}_p$ if and only if the element 5 is a square in $\mathbb{F}_p$, and this occurs if and only if $p \equiv \pm 1 \pmod 5$, by the quadratic reciprocity law [5, Ths. 97 and 98].

(e) Suppose that $|g| = p^n - 1$ or $(p^n - 1)/2$. Then $|g|$ divides $k(p)$ by (a) and (c) above. Suppose that $p \equiv \pm 2 \pmod 5$. Then $k(p)|2(p + 1)$ by 2.2(b). Thus, in either case, $(p^n - 1)/2|2(p + 1)$. This is impossible by Lemma 2.4, because $p \geq 7$. Therefore, we must have $p \equiv \pm 1 \pmod 5$, and so $g \in \mathbb{F}_p$ by (d). But now $k(p)|(p - 1)$ by 2.2(a), whence $(p^{n-1} + \cdots + 1)|2$ and it follows that $n = 1$. □

3. Fibonacci Primitive Roots

Definition 3.1: Let $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t] \subset \mathbb{F}_q[t]$ where q is a power of p. Suppose that $g \in \mathbb{F}_q$ is a root of $f(t)$.

(a) (Shanks, [12]). We call g a *Fibonacci Primitive Root* (*FPR*) *in* $\mathbb{F}_q$ if $|g| = q - 1$; that is, if g is a primitive root in $\mathbb{F}_q$.

(b) We call g a *Fibonacci Square-Primitive Root* (*FSPR*) *in* $\mathbb{F}_q$ if g generates the subgroup of squares in $\mathbb{F}_q$; if q is odd, this means that

$$|g| = (q - 1)/2.$$

Fibonacci Primitive Roots and related topics have an extensive literature: see, for example, references [1], [3], [6], and [9]-[15].

In part (b) of the following result, the criterion for the existence of an FPR is proved in Theorem 1 of De Leon [3], while the assertions on the number of FPRs are proved by Shanks [15, pp. 164-65]. The exceptional cases to this theorem ($p < 7$) will be dealt with in 3.3 below.

Theorem 3.2: Let $p \geq 7$ be a prime and let $q = p^n$ where $n \in \mathbb{N}$.

(a) If $\mathbb{F}_q \supset \mathbb{F}_p$ possesses an FPR or an FSPR, then $\mathbb{F}_q = \mathbb{F}_p$ and $p \equiv \pm 1 \pmod 5$.

(b) $\mathbb{F}_p$ possesses an FPR iff $k(p) = p - 1$. Further, if $k(p) = p - 1$, then
 (i) if $p \equiv 1 \pmod 4$, there are two FPRs;
 (ii) if $p \equiv -1 \pmod 4$, there is just one FPR (and one FSPR).

(c) $\mathbb{F}_p$ possesses an FSPR iff either

(i) $k(p) = p - 1$ and $p \equiv -1 \pmod 4$, when there is a unique FSPR; or

(ii) $k(p) = (p - 1)/2$. In this case, we must have $p \equiv 1 \pmod 4$, then

(α) if $p \equiv 1 \pmod 8$ there are two FSPRs;

(β) if $p \equiv 5 \pmod 8$, there is a unique FSPR.

Proof: Again write $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$, and suppose that g, h are the roots of $f(t)$ in the field $\mathbb{F}_q \supset \mathbb{F}_p$.

(a) Suppose that g is an FPR or an FSPR in $\mathbb{F}_q$. Then $|g| = p^n - 1$ or $(p^n - 1)/2$, and so by 2.5(e), $p \equiv \pm 1 \pmod 5$ and $n = 1$. Thus, $\mathbb{F}_q = \mathbb{F}_p$.

(b) If g is an FPR in $\mathbb{F}_p$, then $|g| = p - 1$ is even and so $k(p) = p - 1$ by 2.5(c). Further, $p \equiv \pm 1 \pmod 5$ by 2.5(d).

Conversely, suppose $k(p) = p - 1$. Let g be an even-order root of $f(t)$; then $|g| = p - 1$, by 2.5(c), and so $g \in \mathbb{F}_p$ by 2.5(e). Thus, g is an FPR in $\mathbb{F}_p$. Now, if $p \equiv 1 \pmod 4$, then $4 \mid p - 1$, whence $|g| = |h|$ by 2.5(c), and so g, h are both FPRs. However, if $p \equiv -1 \pmod 4$, then $p - 1$ is twice an odd number. Thus, by 2.5(a) and 2.5(c), g has order $p - 1$, and so is an FPR, while $h \in \mathbb{F}_p$ has order $(p - 1)/2$, and so is an FSPR.

(c) Suppose that $h \in \mathbb{F}_p$ is an FSPR. Then $|h| = (p - 1)/2$, and so

$$k(p) \in \{p - 1, (p - 1)/2\}$$

by 2.5(a) and 2.5(c). Suppose that $k(p) = p - 1$. Then, by part (b), $\mathbb{F}_p$ possesses an FPR, which must be the other root g of $f(t)$. But then g is a non-square in $\mathbb{F}_p$, while h is a square and $g = -1/h$. Thus, -1 is a non-square in $\mathbb{F}_p$ and $p \equiv -1 \pmod 4$ by quadratic reciprocity. This proves the "only if" part of (c).

If $k(p) = p - 1$ and $p \equiv -1 \pmod 4$, then there is a unique FSPR in $\mathbb{F}_p$ by (b). Suppose that $k(p) = (p - 1)/2$. Since $k(p)$ is even by 2.5, then $p \equiv 1 \pmod 4$.

(α) If $p \equiv 1 \pmod 8$, then $(p - 1)/2$ is divisible by 4 and so both roots of $f(t)$ have order $(p - 1)/2$ by 2.5(a)-(c). These roots belong to $\mathbb{F}_p$ by 2.5(e), and so there are two FSPRs in $\mathbb{F}_p$.

(β) If $p \equiv 5 \pmod 8$, then $(p - 1)/2$ is twice an odd number. By 2.5(a)-(c), one root of $f(t)$ has order $(p - 1)/2$ while the other has order $(p - 1)/4$. Again by 2.5(e), these roots belong to $\mathbb{F}_p$, and so there is a unique FSPR in $\mathbb{F}_p$.

Assertion (c) now follows, and the proof is complete. □

The following proposition lists a collection of easily-verifiable facts concerning FPRs for primes $p < 7$.

Proposition 3.3: We have

(a) $k(2) = 3$. Let ζ be a root in $\mathbb{F}_4$ of $f(t) = t^2 + t + 1 \in \mathbb{F}_2[t]$. Then $1 + \zeta$ is the other root of $f(t)$. We have $|\zeta| = |1 + \zeta| = 3$, and so ζ and $1 + \zeta$ are both FPRs in $\mathbb{F}_4$; they are also FSPRs because all elements of $\mathbb{F}_4$ are squares.

(b) $k(3) = 8$. Let ζ be a root in $\mathbb{F}_9$ of $p(t) = t^2 + 1 \in \mathbb{F}_3[t]$. Then $f(t) = t^2 - t - 1 \in \mathbb{F}_3[t]$ has roots $g = \eta - 1$ and $h = -\eta - 1$ in $\mathbb{F}_9$. Further, $|g| = |h| = 8$, and so g, h are FPR's in $\mathbb{F}_9$.

(c) $k(5) = 20$. Because $(t - 3)^2 = t^2 - t - 1 \in \mathbb{F}_5[t]$, then the element $3 \in \mathbb{F}_5$ is a double root of $f(t)$ in $\mathbb{F}_5$. Further, $|3| = 4$, so that 3 is the unique FPR in $\mathbb{F}_5$. Note that 2.5(c) definitely fails for $p = 5$. □

It should be noted that Brousseau [1] lists the FPR's for those primes $p < 300$ that possess such, while Wall [15] gives the values of $k(p)$ for all primes $p < 2000$. In section 5 below, we list the FPRs and FSPRs for those primes $p < 2000$ that possess such.

It is proved in [11], on the assumption of certain Riemann hypotheses, that, asymptotically, the proportion $C = 0.2657\ldots$ of all primes possess an FPR; since, apart from $p = 5$, the only eligible primes p satisfy $p \equiv \pm 1 \pmod 5$, then we are to expect that over half of these possess an FPR. It might be of interest to determine the proportion of primes that possess an FSPR. For example, there are 146 primes $p < 2000$ with $p \equiv \pm 1 \pmod 5$, of which 80 possess FPRs and 76 possess FSPRs (see the table in section 5).

4. Complete Φ-Sequences

Let p be a prime and let q be a power of p. Let $\mathfrak{S} = (s_0, s_1, s_2, \ldots)$ be a Φ-sequence of period r in $\mathbb{F}_q$. We call $\mathfrak{S}$ a *complete Φ-sequence in $\mathbb{F}_q$* if $r = q - 1$ and if $\{s_0, s_1, \ldots, s_{r-1}\}$ is precisely the set of nonzero elements of $\mathbb{F}_q$. If $\{s_0, s_1, \ldots, s_{r-1}\}$ is precisely the set of nonzero squares of $\mathbb{F}_q$, so that $r = (q - 1)/2$ if q is odd, then $\mathfrak{S}$ is called a *square-complete Φ-sequence in $\mathbb{F}_q$*.

Lemma 4.1: Let $f(t) = t^2 - t - 1 \in \mathbb{F}[t]$ and let g be a root of $f(t)$ in a field $\mathbb{F} \supset \mathbb{F}_p$. Then the Φ-sequence $\mathfrak{S} = (s_0, s_1, \ldots)$ in $\mathbb{F}$ with $s_0 = 1$, $s_1 = g$ has period $a = |g|$, and

$$\{s_0, s_1, \ldots, s_{a-1}\} = \{1, g, \ldots, g^{-1}\}.$$

In particular, if g is an FPR, or FSPR, in $\mathbb{F}$, then $\mathfrak{S}$ is a complete- or square-complete Φ-sequence in $\mathbb{F}$, respectively.

Proof: This is clear. □

We now give our characterization of complete Φ-sequences for primes $p \geq 7$; the cases $p < 7$ are exceptional and will be dealt with later. It is worth observing that if $\mathfrak{S}$ is a complete Φ-sequence in $\mathbb{F}_p$, then the sequence formed by multiplying the terms of $\mathfrak{S}$ by a fixed nonzero element of $\mathbb{F}_p$ is essentially the same sequence $\mathfrak{S}$ with the terms all shifted by a fixed amount; we will thus not distinguish between such multiples.

Theorem 4.2: Let $p \geq 7$ be a prime and let $q = p^n$ where $n \in \mathbb{N}$. Then there is a complete Φ-sequence in $\mathbb{F}_q$ if and only if there is an FPR in $\mathbb{F}_q$, and for this to happen we must have $q = p$. Further, any complete Φ-sequence in $\mathbb{F}_p$ has the form $(1, j, j^2, \ldots)$ where j is an FPR in $\mathbb{F}_p$, and conversely.

Proof: Let $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$, let g, h be the roots of $f(t)$ in a splitting field $\mathbb{F} \supset \mathbb{F}_q$. Suppose without loss that $|g|$ is even; then $|g| = k(p)$ by 2.5(c).

If j is an FPR in $\mathbb{F}_q$, then the Φ-sequence $(1, j, j^2, \ldots)$ is complete (in $\mathbb{F}_q$) by Lemma 4.1.

Suppose now that $\mathfrak{S}$ is a complete Φ-sequence in $\mathbb{F}_q$. Then $\mathfrak{S}$ has period $q - 1$ and so $q - 1 \mid k(p)$ by 4.1. If $p \equiv \pm 2 \pmod 5$, then $k(p) \mid 2(p + 1)$ by 2.2. Thus, $q - 1 \mid 2(p + 1)$, which is impossible by 2.4 because $p \geq 7$. Therefore, we may assume that $p \equiv \pm 1 \pmod 5$. Then $k(p) \mid p - 1$ by 2.2; thus, $q - 1 \mid p - 1$, and so $q = p$ and $k(p) = p - 1$. Thus, g is an FPR in $\mathbb{F}_p$. Note now that $f(t)$ splits in $\mathbb{F}_p$. By 2.3, there exist $\alpha, \beta \in \mathbb{F}_p$ such that

$$\mathfrak{S} = (\alpha + \beta, \alpha g + \beta h, \alpha g^2 + \beta h^2, \ldots),$$

and because $\mathfrak{S}$ is complete,

$$\mathbb{F}_p^* = \{\alpha g^i + \beta h^i : 0 \leq i \leq p - 2\}.$$

But $h = -1/g = g^{(p-1)/2}g^{p-2} = g^{(3p-5)/2}$. Thus, the map

$$g^i \mapsto \alpha g^i + \beta g^{i(3p-5)/2},\ 0 \le i \le p-2,$$

is a permutation of $\mathbb{F}_p^*$. But then the polynomial

$$p(t) = \alpha t + \beta t^{(3p-5)/2} \in \mathbb{F}_p[t]$$

is a permutation polynomial of $\mathbb{F}_p$. But now Hermite's criterion for permutation polynomials (see [4, §84] or [7, Th. 7.4]) implies that, in particular, the reduction, $P(t)$ say, of $(p(t))^4 \pmod{t^p - t}$ has degree $d < p - 1$. A certain amount of calculation reveals that

$$P(t) = 6\alpha^2\beta^2t^{p-1} + Q(t),$$

where $Q(t) \in \mathbb{F}_p[t]$ has degree $e \le p - 2$. It follows that $\alpha\beta = 0$, and so the only possibilities for $\mathfrak{G}$ are (nonzero multiples of):

$$(1, g, g^2, \ldots),$$

and if, also, $|h| = p - 1$,

$$(1, h, h^2, \ldots).$$

This completes the proof. □

The next theorem characterizes the square-complete Φ-sequences for $p \ge 7$; again, the exceptional cases ($p < 7$) are dealt with later. The characterization is almost a word-for-word "translation" of the previous result, but there are a number of technical differences in the proof. Hermite's criterion is not directly applicable here, but we can apply ideas from its proof to get what we need. We will also need to know that the smallest prime $p \equiv \pm 1 \pmod 5$ for which $k(p) < p - 1$ is $p = 29$. This fact is given in Wall [15], but may easily be calculated by hand: we need only check the Fibonacci sequences mod 11 and mod 19.

First we need a lemma; it is not new (see [4, §74]) but we indicate a proof.

Lemma 4.3: Let G be a subgroup of $\mathbb{F}_q^*$ with $|G| = m$. Then

(a) $\sum_{g \in G} g^m = m$ (considered as an element of $\mathbb{F}_q^*$), and

(b) $\sum_{g \in G} g^j = 0$, for $1 \le j \le m - 1$.

Proof:

(a) This follows because $g^m = 1$ for all $g \in G$.

(b) The elements of G are precisely the roots of $t^m - 1 \in \mathbb{F}_q[t]$. Then

$$\sum_{g \in G} g^j$$

is the sum of the j^{th} powers of these roots, and the assertion follows by Newton's formula [4, §74] and [7, Th. 1.75]. □

Theorem 4.4: Let $p \ge 7$ be a prime and let $q = p^n$ where $n \in \mathbb{N}$. Then there is a square-complete Φ-sequence in $\mathbb{F}_q$ if and only if there is an FSPR in $\mathbb{F}_q$, and for this to happen we must have $q = p$. Further, any square-complete Φ-sequence in $\mathbb{F}_p$ has the form $(1, j, j^2, \ldots)$ where j is an FSPR in $\mathbb{F}_p$, and conversely.

Proof: Let $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$, let g, h be the roots of $f(t)$ in a splitting field $\mathbb{F} \supset \mathbb{F}_q$. Suppose without loss that $|g|$ is even; then $|g| = k(p)$ by 2.5(c).

If j is an FSPR in $\mathbb{F}_q$, then the Φ-sequence $(1, j, j^2, \ldots)$ is square-complete (in $\mathbb{F}_q$) by Lemma 4.1.

Suppose now that $\mathfrak{S}$ is a square-complete Φ-sequence in $\mathbb{F}_q$. Then $\mathfrak{S}$ has period $(q-1)/2$, and so $(q-1)/2 \mid k(p)$ by 4.1. If $p \equiv \pm 2 \pmod 5$, then $k(p) \mid 2(p+1)$ by 2.2. Thus $(q-1)/2 \mid 2(p+1)$, which is impossible by 2.4 because $p \geq 7$. We may therefore assume that $p \equiv \pm 1 \pmod 5$, and so $g, h \in \mathbb{F}_p$. Then $k(p) \mid p-1$ by 2.2; thus $q - 1 \mid 2(p-1)$, and so $q = p$ and

$$k(p) \in \{p-1, (p-1)/2\}.$$

By 2.3, there exist $\alpha, \beta \in \mathbb{F}_p$ such that

$$\mathfrak{S} = (\alpha + \beta, \alpha g + \beta h, \alpha g^2 + \beta h^2, \ldots).$$

We consider separately the two possibilities for $k(p)$.

(i) Suppose that $k(p) = p - 1$. Since $\mathfrak{S}$ has period $(p-1)/2$, then

$$\alpha + \beta = \alpha g^{(p-1)/2} + \beta h^{(p-1)/2}.$$

But $|g| = p - 1$ and so $g^{(p-1)/2} = -1$. If also $|h| = p - 1$, then $h^{(p-1)/2} = -1$, and so $\alpha + \beta = -(\alpha + \beta) = 0$. But then $\mathfrak{S}$ contains the element 0, and so cannot be square-complete, a contradiction. Therefore $|h| = (p-1)/2$, by 2.5, and so $\alpha + \beta = -\alpha + \beta$. Thus $\alpha = 0$, and so $\mathfrak{S}$ must be (a nonzero, square multiple of)

$$(1, h, h^2, \ldots),$$

and h is an FSPR in $\mathbb{F}_p$.

(ii) Suppose that $k(p) = (p-1)/2$. By the Remark before Lemma 4.3, we may assume that $p \geq 29$. Since $|g| = k(p)$, then g is an FSPR in $\mathbb{F}_p$. By 3.2(c), $p \equiv 1 \pmod 4$, and so -1 is a square in $\mathbb{F}_p$. We then have $g^{-1} = g^{(p-3)/2}$ and $-1 = g^{(p-1)/4}$, whence $h = -1/g = g^{(3p-7)/4}$. Write Q for the subgroup of squares in $\mathbb{F}_p^*$; then $|Q| = (p-1)/2$. Since $\mathfrak{S}$ is square-complete, we have

$$\begin{aligned} Q &= \{\alpha g^i + \beta h^i : 0 \leq i \leq (p-1)/2\} \\ &= \{\alpha g^i + \beta g^{i(3p-7)/4} : 0 \leq i \leq (p-1)/2\} \\ &= \{\alpha c + \beta c^{(3p-7)/4} : c \in Q\}. \end{aligned}$$

Calculation now reveals that

$$(\alpha c + \beta c^{(3p-7)/4})^8 = x(c),$$

where $x(t) \in \mathbb{F}_p[t]$ is a polynomial of degree at most $(p-3)/2$ with constant term $70\alpha^4\beta^4$. There are certain points that require care in the calculation here; for example, the second term in the expansion is

$$\begin{aligned} 8\alpha^7\beta c^7 c^{(3p-7)/4} &= 8\alpha^7\beta c^{(3p+21)/4} \\ &= 8\alpha^7\beta c^{(p-1)/2} c^{(p+23)/4}. \end{aligned}$$

Now $c^{(p-1)/2} = 1$ because $c \in Q$, while $1 \leq (p+23)/4 < (p-1)/2$ is the upper bound because $p \geq 29 > 25$. Thus, we obtain a term whose degree in c lies between 1 and $(p-3)/2$. The constant term arises naturally as the "middle" term of the expansion, and all other terms have degree between 1 and $(p-3)/2$. Now 4.3 gives both the first [since $(p-3)/2 \geq 8$] and the last equality in the following chain:

$$0 = \sum_{c \in Q} c^8 = \sum_{c \in Q} (\alpha c + \beta c^{(3p-7)/4})^8 = \sum_{c \in Q} x(c) = ((p-1)/2)70\alpha^4\beta^4.$$

It follows (because $p \geq 29$ cannot divide 70) that $\alpha\beta = 0$. Thus, the only possible square-complete Φ-sequences in $\mathbb{F}_p$ are (nonzero square multiples of)

$$(1, g, g^2, \ldots),$$

and if, also, h is an FSPR,

$(1, h, h^2, \ldots)$.

This completes the proof. □

The following result mirrors Proposition 3.3, and deals with the primes 2, 3, and 5.

Proposition 4.5:

(a) The field $\mathbb{F}_2$ possesses neither a complete Φ-sequence nor a square-complete Φ-sequence. If ζ is as in 3.3(a), then

$$1, \zeta, 1+\zeta, \quad \text{and} \quad 1, 1+\zeta, \zeta$$

are the only complete Φ-sequences in $\mathbb{F}_4$; they are also square-complete because all elements of $\mathbb{F}_4^*$ are squares.

(b) The field $\mathbb{F}_3$ possesses neither a complete Φ-sequence nor a square-complete Φ-sequence. If ω is any element in $\mathbb{F}_9$ that is *not* in $\mathbb{F}_3$ then the Φ-sequence with $s_0 = 1$, $s_1 = \omega$:

$$1, \omega, 1+\omega, 1+2\omega, 2, 2\omega, 2+2\omega, 2+\omega,$$

is in $\mathbb{F}_9$, but there are no square-complete Φ-sequences.

(c) The sequence 1, 3, 4, 2 is the unique complete Φ-sequence in $\mathbb{F}_5$, while this field possesses no square-complete Φ-sequence.

(d) If q is any of 2^n, $n \geq 3$, or 3^n, $n \geq 3$, or 5^n, $n \geq 2$, then $\mathbb{F}_q$ possesses neither a complete Φ-sequence nor a square-complete Φ-sequence.

Proof: Most of these assertions are straightforward to verify. For part (d), we use 2.1. □

5. List of FPRs and FSPRs for Primes $p < 2000$

We finish with a table of FPRs and FSPRs for those primes $p < 2000$ that possess such; as we have seen, the prime 5 is "singular" and we set it apart in the list. By 3.2, the only primes $p < 5$ eligible are those with $p \equiv \pm 1 \pmod 5$ and $k(p) \in \{p-1, (p-1)/2\}$; all other primes are thus omitted from the list. For each eligible prime, we give the respective root(s) in $\mathbb{F}_p$ of $f(t) = t^2 - t - 1 \in \mathbb{F}_p[t]$ when they are either primitive (denoted by P) or square-primitive (denoted by Q). We omit those roots that are not either primitive or square-primitive.

Information on the values of $k(p)$ necessary to find the eligible primes was taken from Wall [15]. Certain of the calculations were performed by computer using the finite field facility in the Group Theory Language CAYLEY [2], although much of the work was carried out using nothing more than a pocket calculator.

p	FPR (P) or FSPR (Q)		p	FPR (P) or FSPR (Q)	
5	3P				
11	8P	4Q	19	15P	5Q
29	6Q		31	13P	19Q
41	7P	35P	59	34P	26Q
61	18P	44P	71	63P	9Q
79	30P	50Q	89	10Q	80Q
101	23Q		109	11P	99P
131	120P	12Q	149	41P	109P
179	105P	75Q	181	168Q	
191	89P	103Q	229	148Q	
239	224P	16Q	241	52P	190P
251	134P	118Q	269	72P	198P

p	FPR (P) or FSPR (Q)		p	FPR (P) or FSPR (Q)	
271	255P	17Q	311	59P	253Q
349	206Q		359	106P	254Q
379	360P	20Q	389	152P	238P
401	112Q	290Q	409	130P	280P
419	399P	21Q	431	341P	91Q
439	370P	70Q	449	166P	284P
479	229P	251Q	491	74P	418Q
499	275P	225Q	509	388Q	
569	337P	233P	571	298P	274Q
599	575P	25Q	601	137P	465P
631	110P	522Q	641	279P	363P
659	201P	459Q	701	27P	675P
719	330P	390Q	739	119P	621Q
751	541P	211Q	761	92Q	670Q
821	213P	609P	839	498P	342Q
929	31P	899P	941	228Q	
971	798P	174Q	1019	526P	494Q
1021	458Q		1039	287P	753Q
1051	73P	979Q	1061	602Q	
1091	212P	880Q	1109	703Q	
1129	328P	802P	1171	1058P	114Q
1181	534P	648P	1201	78P	1124P
1229	745Q		1249	405Q	845Q
1259	1224P	36Q	1301	268P	1034P
1319	920P	400Q	1321	453P	869P
1361	83Q	1279Q	1399	240P	1160Q
1409	125Q	1285Q	1429	547P	883P
1439	701P	739Q	1451	283P	1169Q
1459	1293P	167Q	1481	39P	1443P
1489	681P	809P	1499	1291P	209Q
1531	88P	1444Q	1549	1020Q	
1559	1520P	40Q	1571	1044P	568Q
1609	636P	974P	1619	855P	765Q
1621	1446Q		1669	136Q	
1709	601Q		1741	321Q	
1759	859P	901Q	1789	1554Q	
1801	427P	1375P	1811	186P	1626Q
1831	1053P	779Q	1861	1498Q	
1879	1457P	423Q	1889	824P	1066P
1901	98P	1804P	1931	988P	944Q
1949	789P	1161P	1979	1935P	45Q

Acknowledgments

The author wishes to acknowledge partial support from "Projecto 87463 da JNICT" and from the "Centro de Algebra da Universidade de Lisboa do INIC."

References

Note that Chapter 8 of [7] corresponds closely to Chapter 6 of [8], to the extent that Theorem 8.n of [7] corresponds to Theorem 6.n of [8]; in the text we have thus limited the relevant references to [7].

1. Brother Alfred Brousseau. "Table of Indices with a Fibonacci Relation." *Fibonacci Quarterly* 10 (1972):182-84.
2. John J. Cannon. "An Introduction to the Group Theory Language, Cayley." In *Computational Group Theory*, ed. Michael D. Atkinson. London, Orlando: Academic Press, 1984, pp. 145-83.
3. M. J. De Leon. "Fibonacci Primitive Roots and the Period of the Fibonacci Numbers Modulo p." *Fibonacci Quarterly* 15 (1977):353-55.
4. Leonard Eugene Dickson. *Linear Groups with an Exposition of the Galois Field Theory*. Leipzig: Teubner, 1901; New York: Dover, 1958.
5. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 5th ed. Oxford: Clarendon Press, 1979.
6. P. Kiss & B. M. Phong. "On the Connection between the Rank of Apparition of a Prime p in Fibonacci Sequence and the Fibonacci Primitive Roots." *Fibonacci Quarterly* 15 (1977):347-49.
7. Rudolf Lidl & Harald Niederreiter. *Finite Fields*. Reading, Mass: Addison-Wesley, 1983; Cambridge: Cambridge University Press, 1984.
8. Rudolf Lidl & Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge: Cambridge University Press, 1986.
9. M. E. Mays. "A Note on Fibonacci Primitive Roots." *Fibonacci Quarterly* 20 (1982):111.
10. B. M. Phong. "Lucas Primitive Roots." *Fibonacci Quarterly* 29 (1991):66-71.
11. J. W. Sander. "On Fibonacci Primitive Roots." *Fibonacci Quarterly* 28 (1990):79-80.
12. Daniel Shanks. "Fibonacci Primitive Roots." *Fibonacci Quarterly* 10 (1972): 162-68.
13. Daniel Shanks & Larry Taylor. "An Observation on Fibonacci Primitive Roots." *Fibonacci Quarterly* 11 (1973):159-60.
14. S. Vajda. *Fibonacci & Lucas Numbers, and the Golden Section: Theory and Application*. Chichester: Ellis Horwood Ltd., 1989.
15. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* 67 (1960): 525-532.

*****