COMPLETE PADOVAN SEQUENCES IN FINITE FIELDS

Juan B. Gil
Department of Mathematics and Statistics, Penn State Altoona, 3000 Ivyside Park, Altoona, PA 16601

Michael D. Weiner
Department of Mathematics and Statistics, Penn State Altoona, 3000 Ivyside Park, Altoona, PA 16601

Catalin Zara
Department of Mathematics, University of Massachusetts Boston, 100 Morrissey Blvd., Boston, MA 02125
(Submitted July 2005-Final Revision February 2006)

ABSTRACT

Given a prime $p \geq 5$, and given $1 < \kappa < p-1$, we call a sequence $(a_n)_n$ in $\mathbb{F}_p$ a Φ_κ-sequence if it is periodic with period $p-1$, and if it satisfies the linear recurrence $a_n + a_{n+1} = a_{n+\kappa}$ with $a_0 = 1$. Such a sequence is said to be a complete Φ_κ-sequence if in addition $\{a_0, a_1, \ldots, a_{p-2}\} = \{1, \ldots, p-1\}$. For instance, every primitive root b mod p generates a complete Φ_κ-sequence $a_n = b^n$ for some (unique) κ. A natural question is whether every complete Φ_κ-sequence is necessarily defined by a primitive root. For $\kappa = 2$ the answer is known to be positive. In this paper we reexamine that case and investigate the case $\kappa = 3$ together with the associated cases $\kappa = p-2$ and $\kappa = p-3$.

1. INTRODUCTION

For a prime number $p \geq 5$ and a number $\kappa \in \{2, \ldots, p-2\}$, a sequence $(a_n)_{n\in\mathbb{Z}}$ of elements of $\mathbb{F}_p$ is said to be a Φ_κ-*sequence* if

$$a_0 = 1 \quad \text{and} \quad a_{n+\kappa} = a_n + a_{n+1} \ \text{ for all } n \in \mathbb{Z}, \tag{1}$$

where "=" means (throughout this paper) equality in $\mathbb{F}_p$. A Φ_κ-sequence is called *complete* if

$$(a_n)_n \ \text{ is periodic, with period } p-1, \text{ and} \tag{2}$$

$$\{a_1, \ldots, a_{p-2}\} = \{2, \ldots, p-1\}. \tag{3}$$

The case $\kappa = 2$ has been studied by Brison [1]. A Φ_2-sequence satisfies a Fibonacci recurrence, so it is completely determined by the value of a_1. A complete Φ_2-sequence is called a *complete Fibonacci sequence*; for example, the only complete Fibonacci sequence in $\mathbb{F}_5$ is

$$\ldots, 4, 2, 1, 3, 4, 2, 1, 3, 4, \ldots$$

with $a_0 = 1$ and $a_1 = 3$. Moreover, $x = 3$ is a primitive root mod 5, and it is a solution (in $\mathbb{F}_5$) of the equation $x^2 = x + 1$ (hence $x = 3$ is a *Fibonacci primitive root*), so the sequence can also be described as

$$\ldots, 3^{-2}(=4), 3^{-1}(=2), 3^0(=1), 3, 3^2(=4), 3^3(=2), 3^4(=1), \ldots$$

The main result of [1], stated here in a slightly weaker form, generalizes this observation. In Section 2 we will give an elementary proof of this theorem in order to motivate our approach.

Theorem 1: (Brison) *Let $p \geq 5$ be a prime number. A Φ_2-sequence $(a_n)_n$ is a complete Fibonacci sequence if and only if $a_n = b^n$ for all n, where b is a Fibonacci primitive root.*

The new results of this paper concern the case $\kappa = 3$. Because of the specific recurrence satisfied by Φ_3-sequences ($a_{n+3} = a_{n+1} + a_n$), complete Φ_3-sequences will be called *complete Padovan sequences* [4]. Similar to the case $\kappa = 2$, we will say that a primitive root b in $\mathbb{F}_p$ is a *Padovan primitive root* if it satisfies the condition $b^3 = b + 1$. Note that if b is a Padovan primitive root, then the sequence

$$\dots, b^{-1}(= b^{p-2}), 1, b, b^2, b^3, b^4, \dots, b^{p-2}, b^{p-1}(= 1), \dots$$

is a complete Padovan sequence. A natural question is whether these are the only examples of complete Padovan sequences in $\mathbb{F}_p$. Our results state that this is the case, at least for certain prime numbers.

Let ϱ_p be the number of distinct roots of $X^3 - X - 1$ in $\mathbb{F}_p$. The main results of this paper are the following two theorems.

Theorem 2: *Let $p \geq 5$ be a prime number such that $\varrho_p < 3$. A Φ_3-sequence $(a_n)_n$ is a complete Padovan sequence if and only if $a_n = b^n$ for all n, where b is a Padovan primitive root.*

In the case when $\varrho_p = 3$, we denote by α, β, and γ the roots of $X^3 - X - 1$ in $\mathbb{F}_p$. Further we let

$$N_p = \min\{|\alpha/\beta|, |\beta/\gamma|, |\gamma/\alpha|\}. \tag{4}$$

Theorem 3: *Let $p \geq 5$ be a prime number such that $\varrho_p = 3$ and $p \leq N_p^2 + 1$. A Φ_3-sequence $(a_n)_n$ is a complete Padovan sequence if and only if $a_n = b^n$ for all n, where b is a Padovan primitive root.*

We strongly believe that this theorem holds even if $p > N_p^2 + 1$. In fact, in Section 4 we will see that our condition on p can be relaxed, see (19). Numerical computations show that among all primes less than 10^5, there are only 4 numbers that cannot be handled by our proof of Theorem 3, cf. Section 5. Nonetheless, for these cases one can manually check that the statement of our theorem is still true.

In contrast to the Fibonacci case, the Padovan recurrence is of order three, so in addition to $a_0 = 1$, one needs values for both a_1 and a_2 to completely determine a Φ_3-sequence. It is therefore rather surprising that complete Padovan sequences are determined by only one parameter. If $(a_n)_n$ is a complete Padovan sequence, one can use an approach similar to the Fibonacci case to get one condition relating a_1 and a_2. The difficulty resides in proving a *second* relation.

The ultimate goal will be to connect Φ_κ-sequences in $\mathbb{F}_p$ with primitive roots of p. It is easy to see that if $p \geq 5$ is a prime, and $b \in \mathbb{F}_p$ is a primitive root mod p, then there exists a unique value $\kappa \in \{2, 3, \dots, p-2\}$ such that $b^\kappa = b + 1$. Therefore the sequence

$$\dots, b^{-1}(= b^{p-2}), 1, b, b^2, \dots, b^{\kappa-1}, b^\kappa, \dots, b^{p-2}, b^{p-1}(= 1), \dots$$

is a complete Φ_κ-sequence. Data collected so far suggests that these are in fact the only complete Φ_κ-sequences. For a fixed value $\kappa \in \{2, \dots, p-2\}$, we say that a primitive root b in $\mathbb{F}_p$ is a *Φ_κ-primitive root* if $b^\kappa = b + 1$.

Conjecture: *Let $p \geq 5$ be a prime number. A Φ_κ-sequence $(a_n)_n$ is complete if and only if $a_n = b^n$ for all n, where b is a Φ_κ-primitive root.*

At the end of the paper we briefly discuss the relation between the conjugate cases κ and $p - \kappa$ and prove the statement for $\kappa = p - 2$, $\kappa = p - 3$, $\kappa = \frac{p-1}{2}$, and $\kappa = \frac{p+1}{2}$.

2. FIBONACCI PRIMITIVE ROOTS

In this section we discuss the characterization of complete Fibonacci sequences in terms of Fibonacci primitive roots, and give an elementary proof of Theorem 1. The key argument is the same as in [1], but our approach is more direct.

Proof of Theorem 1: It is not hard to see that a Fibonacci primitive root generates a complete Fibonacci sequence: If b is a Fibonacci primitive root and $a_1 = b$, then $a_2 = a_0 + a_1 = 1 + b = b^2$, and, by induction, $a_m = b^m$ for all integers m. Since b is a *primitive* root, it follows that the sequence $(a_n)_n$ satisfies both the periodicity and the completeness conditions, hence it is a complete Fibonacci sequence.

The less trivial part is to show that for every complete Fibonacci sequence, a_1 is a Fibonacci primitive root. The case $p = 5$ can be checked separately, so from now on we assume that $p \geq 7$. Let $(a_n)_n$ be a complete Fibonacci sequence in $\mathbb{F}_p$ and let $b = a_1$. Let

$$P(X) = \sum_{n=0}^{p-2} a_n X^n \in \mathbb{F}_p[X]. \tag{5}$$

Then the recurrence of a_n implies

$$(1 - X - X^2)P(X) = \left(1 - X^{p-1}\right)(1 + a_{p-2}X)\,. \tag{6}$$

The right-hand side of (6) is identically zero on $\mathbb{F}_p^*$, while $P(X)$ can have at most $p - 2$ roots in $\mathbb{F}_p^*$. Therefore, $1 - X - X^2$ has at least one root in $\mathbb{F}_p^*$, and thus it has both roots in $\mathbb{F}_p^*$.

Let α and β be the solutions of $x^2 = x + 1$ in $\mathbb{F}_p$. Then $\alpha \neq \beta$ (since $p \neq 5$), hence

$$a_n = A\alpha^n + B\beta^n$$

for all integers n, where

$$A = \frac{b - \beta}{\alpha - \beta} \quad \text{and} \quad B = \frac{b - \alpha}{\beta - \alpha}\,.$$

If k is an integer such that $1 \leq k \leq p - 2$, then

$$\sum_{n=0}^{p-2} a_n^k = \sum_{n=1}^{p-1} n^k = 0.$$

Therefore,

$$0 = \sum_{n=0}^{p-2} a_n^k = \sum_{n=0}^{p-2} (A\alpha^n + B\beta^n)^k = \sum_{j=0}^{k} \binom{k}{j} A^j B^{k-j} \sum_{n=0}^{p-2} (\alpha^j \beta^{k-j})^n\,. \tag{7}$$

However, if $x \neq 0$, then

$$\sum_{n=0}^{p-2} x^n = \begin{cases} 0, & \text{if } x \neq 1 \\ p-1, & \text{if } x = 1 \end{cases}.$$

The key ingredient in the proof is finding a value of k for which the last sum in (7) is zero for all but one j. Using $\alpha + \beta = 1$ and $\alpha\beta = -1$, we see that for all primes $p \geq 7$, the smallest such value is $k = 4$. In fact, we get

$$0 = \sum_{n=0}^{p-2} a_n^4 = -6A^2B^2, \tag{8}$$

which implies that one of A or B is zero. Without loss of generality, assume $A = 0$. Then $b = \beta$, so $b^2 = b + 1$. An inductive argument shows that $a_n = b^n$ for all integers n, and since $(a_n)_n$ is a complete Fibonacci sequence, b must be a primitive root, hence $a_1 = b$ is a Fibonacci primitive root. □

3. COMPLETE PADOVAN SEQUENCES AND PRIMITIVE ROOTS

Let $(a_n)_n$ be a complete Padovan sequence. Note that the periodicity (2) and the recurrence relation (1) (with $\kappa = 3$) imply, as in (6),

$$(1 - X^2 - X^3)P(X) = 0 \text{ on } \mathbb{F}_p^*.$$

Consequently, there must be at least one element $r \in \mathbb{F}_p$ that solves the equation $1-x^2-x^3 = 0$. Thus $1/r \in \mathbb{F}_p$ is a root of $f(X) = X^3 - X - 1$.

Proof of Theorem 2: We only need to prove that a complete Padovan sequence with initial values $(a_0, a_1, a_2) = (1, b, c)$ gives rise to a primitive root $b \in \mathbb{F}_p$ with $b^2 = c$ and $b^3 = b + 1$.

Case 1: f has exactly one root in $\mathbb{F}_p$.

In this case, $1 - X^2 - X^3$ must have exactly one root $r \in \mathbb{F}_p$. Thus the other $p-2$ nonzero elements of $\mathbb{F}_p$ are roots of $P(X)$ from (5), so

$$P(X) = a_{p-2} \prod_{\substack{i=1 \\ i \neq r}}^{p-1} (X - i). \tag{9}$$

Note that the periodicity of $(a_n)_n$ implies $(a_{p-1}, a_p, a_{p+1}) = (1, b, c)$, and by (1) we have $a_{p-2} = c - 1$ and $a_{p-3} = b - c + 1$. Comparing the constant term and the coefficient of X^{p-3} in (9), we conclude that

$$1 = a_{p-2}/r \quad \text{and} \quad a_{p-3} = a_{p-2}r,$$

and consequently,

$$c = r + 1 \quad \text{and} \quad b = r^2 + r.$$

Using that $1 - r^2 - r^3 = 0$ it is easy to check that $b^2 = c$ and $b^3 = b + 1$. Thus $a_n = b^n$, and because of (3), b is a primitive root.

Case 2: f has only two distinct roots in $\mathbb{F}_p$.

The discriminant of $f(X) = X^3 - X - 1$ is -23, so the only way for f to have only two distinct roots in $\mathbb{F}_p$ is when $p = 23$. We use the periodicity of $(a_n)_n$ to conclude that $1 = a_0 = a_{p-1} = a_{22} = 22c + 13b + 17$ and so $c = 13b + 16$ in $\mathbb{F}_{23}$. Note that because of (3) we have

$$\sum_{n=0}^{p-2} a_n^3 = \sum_{n=1}^{p-1} n^3 = 0 \text{ in } \mathbb{F}_p. \tag{10}$$

Using $c = 13b + 16$ we get the cubic equation

$$0 = \sum_{n=0}^{21} a_n^3 = 10b^3 + b^2 + 20$$

whose solutions in $\mathbb{F}_{23}$ are $b = 3$ and $b = 10$. However, the sequence generated by the initial values $(1, 3, 9)$ fails to be complete, so $b = 3$ is not an admissible choice for $b = a_1$. On the other hand, $b = 10$ is indeed a primitive root mod 23. □

Proof of Theorem 3: Let $\alpha, \beta, \gamma \in \mathbb{F}_p$ be the distinct roots of $f(X)$. Note that in this case p must be different from 23, so $2\alpha + 3$, $2\beta + 3$, and $2\gamma + 3$ are all different from 0. Note also that these roots satisfy the equations

$$\alpha + \beta + \gamma = 0, \quad \alpha\beta\gamma = 1, \text{ and } \alpha\beta + \alpha\gamma + \beta\gamma = -1. \tag{11}$$

The recurrence relation (1) with initial values $(1, b, c)$ gives the formula

$$a_n = A\alpha^n + B\beta^n + C\gamma^n \text{ for every } n,$$

where

$$A = \frac{\alpha^2 b + \alpha c + 1}{2\alpha + 3}, \quad B = \frac{\beta^2 b + \beta c + 1}{2\beta + 3}, \quad C = \frac{\gamma^2 b + \gamma c + 1}{2\gamma + 3}. \tag{12}$$

We make again use of (10) to get

$$\begin{aligned} 0 &= \sum_{n=0}^{p-2} (A\alpha^n + B\beta^n + C\gamma^n)^3 \\ &= \sum_{n=0}^{p-2} \sum_{i+j+k=3} \frac{3!}{i!j!k!} A^i B^j C^k (\alpha^i \beta^j \gamma^k)^n \\ &= \sum_{i+j+k=3} \frac{3!}{i!j!k!} A^i B^j C^k \sum_{n=0}^{p-2} (\alpha^i \beta^j \gamma^k)^n. \end{aligned}$$

Now, using (11) it can be easily seen that $\alpha^i\beta^j\gamma^k \neq 1$ unless $i = j = k = 1$. Thus, for $(i, j, k) \neq (1, 1, 1)$, we get

$$\sum_{n=0}^{p-2}(\alpha^i\beta^j\gamma^k)^n = \frac{1-(\alpha^i\beta^j\gamma^k)^{p-1}}{1-\alpha^i\beta^j\gamma^k} = 0 \text{ in } \mathbb{F}_p.$$

Finally, we arrive at the identity

$$0 = \sum_{n=0}^{p-2} a_n^3 = -6ABC \tag{13}$$

which implies that at least one of the factors must vanish, say $C = 0$, and so the closed form of a_n reduces to

$$a_n = A\alpha^n + B\beta^n \text{ for every } n. \tag{14}$$

Note that $C = 0$ implies $c = -\gamma b - \frac{1}{\gamma}$. If we can prove that $b = \alpha$ or $b = \beta$, then this condition on c together with (11) give the desired identities $b^2 = c$ and $b^3 = b + 1$ and the theorem is proved.

Given the numbers p, α, β as above, for $k \in \{1, \ldots, p-2\}$ we consider the set $I_k = \{j \in \mathbb{Z} | 0 \leq j \leq k \text{ and } \alpha^j\beta^{k-j} \equiv 1 \bmod p\}$. In the next section we will discuss some properties of this set and will prove (Corollary 1) that for p, α, β as in this theorem, there is always a k, $1 < k < p-1$, such that I_k contains exactly one element. If we let k in (7) be such that $I_k = \{j_0\}$, then we get

$$0 = \sum_{n=0}^{p-2} a_n^k = -\binom{k}{j_0} A^{j_0} B^{k-j_0} \tag{15}$$

since the sum $\sum_{n=0}^{p-2}(\alpha^j\beta^{k-j})^n$ vanishes in $\mathbb{F}_p$ for every j with $\alpha^j\beta^{k-j} \neq 1$. Therefore, either A or B must be zero. Now, together with the fact that $C = 0$, the equations (12) give $b = \alpha$ or $b = \beta$. This proves that $a_n = b^n$ for every n, and since $(a_n)_n$ is complete, b is a Padovan primitive root. □

4. SUM OF POWERS AND MINIMAL EXPONENT

A crucial idea in the proof of Theorem 1 and Theorem 3 is to consider the sum of powers $\sum_{n=0}^{p-2} a_n^k$ in $\mathbb{F}_p$ for some $k \in \{2, \ldots, p-2\}$. Since this sum is always zero, the aim is to find a suitable exponent k that allows us to extract useful information about the sequence. For instance, for the Fibonacci sequence the exponent $k = 4$ was a good choice. For a complete Padovan sequence, however, the situation is more subtle. In a first step, the choice $k = 3$ allowed us to reduce the closed form of a_n to a sum of two terms, cf. (14), but when working with the reduced form, the choice of k is not clear at all and depends on the prime number p at hand.

Let p be such that $X^3 - X - 1$ has three distinct roots α, β, γ in $\mathbb{F}_p$. Let $(a_n)_n \subset \mathbb{F}_p$ be a complete Padovan sequence with initial values $(1, b, c)$. Assume $\gamma^2 b + \gamma c + 1 = 0$, i.e., $C = 0$ in (12) so that a_n reduces to (14). Under these assumptions we consider the set

$$I_k = \{j \in \mathbb{Z} | 0 \leq j \leq k \text{ and } \alpha^j\beta^{k-j} \equiv 1 \bmod p\}$$

and its dual

$$I'_k = \{j \in \mathbb{Z} | 0 \le j \le k \text{ and } \alpha^{k-j}\beta^j \equiv 1 \bmod p\}.$$

Observe that $j \in I_k$ if and only if $k - j \in I'_k$ so that these sets essentially contain the same information.

Let $N = |\alpha/\beta|$ be the order of $\frac{\alpha}{\beta}$ in $\mathbb{F}_p$. That is, $\left(\frac{\alpha}{\beta}\right)^N = 1$ and $\left(\frac{\alpha}{\beta}\right)^j \neq 1$ for every $j \in \{1, \ldots, N-1\}$. In our situation it is easy to check that $N > 3$.

Observe that

$$1, \frac{\alpha}{\beta}, \left(\frac{\alpha}{\beta}\right)^2, \ldots, \left(\frac{\alpha}{\beta}\right)^{N-1}$$

are the (distinct) Nth roots of unity.

Lemma 1: *The order of α^N and β^N in $\mathbb{F}_p$ is $(p-1)/N$.*

Proof: Let $m \ge 1$ be such that $mN \le p-1$ and $\alpha^{mN} = 1$. Then $\beta^{mN} = 1$ and so by (14) we must have $a_{mN} = 1$. This implies $mN = p-1$ so $m = (p-1)/N$. □

Lemma 2: *$I_k \neq \varnothing$ for some $k \in \{1, \ldots, p-2\}$. Moreover, in this case, we have $k = \ell(p-1)/N$ for some $\ell \in \{1, \ldots, N-1\}$.*

Proof: Suppose $I_k = \varnothing$ for every k. Then, in particular, $\beta^k \neq 1$ for $k = 1, \ldots, p-2$, so that β must be a primitive root mod p. Let $1 < t < p-1$ be such that $\alpha = \beta^t$. Thus $\alpha^j\beta^{k-j} = \beta^{(t-1)j+k}$ for every j and k. If we pick $k = p-t$ and $j = 1$, then $\alpha\beta^{p-t-1} = \beta^{p-1} = 1$ which implies $I_{p-t} \neq \varnothing$ and we get a contradiction.

Now let k be such that $\alpha^j\beta^{k-j} = 1$ for some $0 \le j \le k$. Then

$$1 = (\alpha^j\beta^{(k-j)})^N = \left(\frac{\alpha}{\beta}\right)^{jN} \beta^{kN} = (\beta^N)^k$$

which by Lemma 1 implies that $(p-1)/N$ must divide k. □

Lemma 3: *Let $I_k \neq \varnothing$ and let $j_0 = \min(I_k)$. If $k < N + j_0$, then $I_k = \{j_0\}$.*

Proof: Let $j_1 > j_0$ be such that $\alpha^{j_1}\beta^{k-j_1} = 1$. Thus $\alpha^{j_1}\beta^{k-j_1} = \alpha^{j_0}\beta^{k-j_0}$ and so $\left(\frac{\alpha}{\beta}\right)^{j_1-j_0} = 1$. But this implies $j_1 - j_0 = \ell N$ for some $\ell \ge 1$. Hence $j_1 \ge N + j_0 > k$ and therefore $j_1 \notin I_k$. □

Let $k_{\min}$ denote the smallest k for which $I_k \neq \varnothing$.

Lemma 4: *If $k_{\min} > \frac{p-1}{N}$, then $k_{\min} < N + j_0$ and therefore $I_{k_{\min}} = \{j_0\}$.*

Proof: Let $k_{\min} = \ell(p-1)/N$ for some $1 < \ell < N$, so

$$1 = \alpha^{j_0}\beta^{k_{\min}-j_0} = \left(\frac{\alpha}{\beta}\right)^{j_0} \beta^{\ell(p-1)/N} = \left(\frac{\alpha}{\beta}\right)^{N+j_0} \beta^{\ell(p-1)/N}. \tag{16}$$

Moreover, since $\beta^{(p-1)/N}$ is a Nth root of unity, we have $\beta^{(p-1)/N} = \left(\frac{\alpha}{\beta}\right)^m$ for some $0 \leq m < N$. Therefore,

$$1 = \left(\frac{\alpha}{\beta}\right)^{j_0} \beta^{\ell(p-1)/N} = \left(\frac{\alpha}{\beta}\right)^{m+j_0} \beta^{(\ell-1)(p-1)/N} \tag{17}$$

which in particular implies $m + j_0 > (\ell - 1)(p-1)/N$ since $I_{(\ell-1)(p-1)/N} = \varnothing$.

Dividing (16) by (17) we get the equation

$$1 = \left(\frac{\alpha}{\beta}\right)^{N-m} \beta^{(p-1)/N}. \tag{18}$$

Now, if $k_{\min} = \ell(p-1)/N \geq N + j_0$, then we have

$$(\ell - 1)(\tfrac{p-1}{N}) < m + j_0 < N + j_0 \leq \ell \left(\frac{p-1}{N}\right)$$

which implies $N - m < (p-1)/N$. But the equation (18) would then imply that $I_{(p-1)/N} \neq \varnothing$ contradicting the minimality of $k_{\min} = \ell(p-1)/N$. □

Corollary 1: *Let N_p be as in (4). If $p \leq N_p^2 + 1$, then $I_{k_{\min}} = \{j_0\}$.*

Proof: By Lemma 4 we only need to check the case when $k_{\min} = \frac{p-1}{N}$. Let $k = k_{\min}$. If $j_0 = \min(I_k)$ and $j_0' = \min(I_k')$, then $(j_0, j_0') \neq (0,0)$. Otherwise it would imply $\alpha^k = \beta^k = 1$ and so $a_k = A\alpha^k + B\beta^k = 1$. But this contradicts the fact that, by definition, $a_k \neq 1$ for $0 < k < p-1$. Thus we can assume $j_0 > 0$. Then

$$p \leq N_p^2 + 1 \;\Rightarrow\; p - 1 \leq N^2 \;\Rightarrow\; k_{\min} = \frac{p-1}{N} \leq N < N + j_0.$$

The statement now follows from Lemma 3. □

Remark 1: According to our previous discussion, it is evident that the condition $p \leq N_p^2 + 1$ in Theorem 3 can be replaced by the weaker condition $\frac{p-1}{N} < N + j_0$, or equivalently,

$$p < N^2 + j_0 N + 1. \tag{19}$$

Observe that if $k_{\min} > \frac{p-1}{N}$, then (19) is automatically satisfied by Lemma 4. Thus we only need to request (19) for the cases when $k_{\min} = \frac{p-1}{N}$. Some examples will be discussed in the next section.

5. EXAMPLES AND FURTHER REMARKS

Throughout this section we let $f(X) = X^3 - X - 1 \in \mathbb{F}_p[X]$.

Example 1: The set of numbers

$$\{7, 11, 17, 37, 67, 83, 113, 199, 227, 241, 251, 271, 283, 367, 373, 401, 433, 457,$$

$$479, 569, 571, 593, 613, 643, 659, 701, 727, 743, 757, 769, 839, 919, 941, 977\}$$

contains all prime numbers < 1000 for which there is a complete Padovan sequence in $\mathbb{F}_p$ and $f(X)$ has exactly one root. For instance, for $p = 7$ this root is $b = 5$. It can be easily checked that $(a_0, a_1, a_2) = (1, 5, 4)$ generates a complete Padovan sequence, and that any other choice of initial values will not give such a sequence. Of course, $b = 3$ is also a primitive root mod 7 and $a_n = 3^n$ is a complete sequence, but $f(3) \neq 0$. However, $b = 3$ solves the equation $x^4 - x - 1 = 0$ in $\mathbb{F}_7$, so 3^n is a complete Φ_4-sequence in $\mathbb{F}_7$.

Example 2: The set of numbers

$$\{59, 101, 167, 173, 211, 271, 307, 317, 593, 599,$$

$$607, 691, 719, 809, 821, 829, 853, 877, 883, 991, 997\}$$

contains all prime numbers < 1000 for which there is a complete Padovan sequence in $\mathbb{F}_p$ and $f(X)$ has three distinct roots. With each number we can associate some data according to our discussion in the previous section. In the following table we show a few examples. Under "roots" we list pairs of roots of $f(X)$, say $\alpha, \beta \in \mathbb{F}_p$, that generate complete Padovan sequences. Recall that $N = |\alpha/\beta|$.

p	roots	N	$k_{\min}$	$\frac{p-1}{N}$	j_0	j_0'
59	13, 42	29	10	2	7	3
101	20, 89	20	20	5	16	4
101	89, 93	25	8	4	7	1
167	134,73	83	14	2	5	9
173	97,110	86	10	2	1	9
211	205,97	15	14	14	3	11
211	97,120	42	30	5	6	24
271	145,46	135	22	2	17	5
307	157,50	17	18	18	11	7
307	50,100	102	15	3	4	11
307	100,157	102	45	3	3	42

Note that for $p = 307$ with $N = 17$ we have $p > N^2 + 1$. Nonetheless, as discussed in Remark 1, Theorem 3 still holds since $N + j_0 > \frac{p-1}{N}$.

The relation between j_0, j_0', and $k_{\min}$ is not a coincidence. As a matter of fact, since $(\frac{\alpha}{\beta})^{k_{\min}} = (\frac{\alpha}{\beta})^{j_0 + j_0'}$, we have

$$k_{\min} = j_0 + j_0' + \ell N$$

for some integer $\ell \geq 0$. If $\ell = 0$, then $N + j_0 > \frac{p-1}{N}$ and our proof of Theorem 3 works.

Example 3: The set of numbers

$$\{307, 5851, 24697, 34961, 87623, 98801\}$$

contains all prime numbers $< 10^5$ for which there is a complete Padovan sequence in $\mathbb{F}_p$, $f(X)$ has three distinct roots, $p > N^2 + 1$, and $k_{\min} = \frac{p-1}{N}$ (cf. Remark 1). More precisely, we have

p	N	$k_{\min}$	j_0	j_0'	ℓ
307	17	18	11	7	0
5851	39	150	4	29	3
24697	63	392	59	18	5
34961	92	380	89	15	3
87623	227	386	175	211	0
98801	52	1900	47	33	35

As mentioned above, $p = 307$ and $p = 87623$ are covered by our current proof of Theorem 3. For the other four cases, the statement of the theorem can be checked by hand (computer).

Conjecture: *The statement of Theorem 3 is true even if* $p > N^2 + 1$.

Remark 2: In the case when $f(X)$ has three distinct roots in $\mathbb{F}_p$, we showed in the proof of Theorem 3 that a complete Padovan sequence $(a_n)_n$ with $a_n = A\alpha^n + B\beta^n + C\gamma^n$ reduces to $a_n = A\alpha^n + B\beta^n$ with A and B as in (12). Moreover, because of (11), a_n can be written as

$$a_n = -\gamma a_{n-1} - \frac{1}{\gamma} a_{n-2} \text{ for every } n,$$

thus it is in fact a generalized Fibonacci sequence with characteristic polynomial $g(t) = t^2 + \gamma t + \frac{1}{\gamma} = (t-\alpha)(t-\beta)$. According to [2], the set $\{1, a_1, \ldots, a_{p-2}\}$ is then a standard g-subgroup.

Remark 3: The first part of the proof of Theorem 1 works in a more general context: Let $(a_n)_n$ be a periodic sequence in $\mathbb{F}_p$, with period $p-1$, and satisfying a linear recurrence of order κ

$$a_{n+\kappa} = s_0 a_n + s_1 a_{n+1} + \cdots + s_{\kappa-1} a_{n+\kappa-1} \text{ for all } n,$$

with $a_0 = 1$. If

$$S(X) = 1 - s_{\kappa-1} X - \cdots - s_1 X^{\kappa-1} - s_0 X^\kappa \in \mathbb{F}_p[X],$$

and, as before,

$$P(X) = \sum_{n=0}^{p-2} a_n X^n = 1 + a_1 X + \cdots + a_{p-2} X^{p-2} \in \mathbb{F}_p[X],$$

then $S(X)P(X) = (1 - X^{p-1})Q(X)$ for some $Q(X) \in \mathbb{F}_p[X]$, so $S(X)$ has at least one root $r \in \mathbb{F}_p$. Since

$$X^\kappa - s_{\kappa-1} X^{\kappa-1} - \cdots - s_1 X - s_0 = X^\kappa S(1/X),$$

it follows that the characteristic polynomial of the linear recurrence has at least one root $1/r \in \mathbb{F}_p$. When $\kappa = 2$, this implies that both roots are in $\mathbb{F}_p$, but for $\kappa \geq 3$ (as we have seen for $\kappa = 3$), the situation is more complicated. Moreover, even if the roots are distinct and are all in $\mathbb{F}_p$, finding the right value(s) of k in order to get relation(s) of the form (8), (13), or (15) is not obvious.

Proposition 1: *Let $p \geq 5$ be a prime number. A Φ_κ-sequence $(a_n)_n$ is complete if and only if $(a_{p-1-n})_n$ is a complete $\Phi_{p-\kappa}$-sequence.*

Proof: Let $(a_n)_n$ be a complete Φ_κ-sequence. Let

$$\tilde{a}_n = a_{p-1-n} \text{ for every } n.$$

By definition, $(\tilde{a}_n)_n$ satisfies (2) and (3). So we only need to check (1):

$$\begin{aligned}\tilde{a}_n + \tilde{a}_{n+1} &= a_{p-1-n} + a_{p-1-n-1} \\ &= a_{p-1-n-1+\kappa} = a_{p-1-n-1+p-p+\kappa} \\ &= a_{p-1-(n+p-\kappa)} = \tilde{a}_{n+p-\kappa}.\end{aligned}$$

Thus $(\tilde{a}_n)_n$ is a complete $\Phi_{p-\kappa}$-sequence. □

This proposition together with Theorem 1, Theorem 2, and Theorem 3 give us the following corollaries.

Corollary: *Let $p \geq 5$ be a prime number. A Φ_{p-2}-sequence $(a_n)_n$ is a complete Φ_{p-2}-sequence if and only if $a_n = b^n$ for all n, where b is a Φ_{p-2}-primitive root.*

Corollary: *Let $p \geq 5$ be a prime number such that $\varrho_p < 3$. A Φ_{p-3}-sequence $(a_n)_n$ is a complete Φ_{p-3}-sequence if and only if $a_n = b^n$ for all n, where b is a Φ_{p-3}-primitive root.*

Corollary: *Let $p \geq 5$ be a prime number such that $\varrho_p = 3$ and $p \leq N_p^2 + 1$. A Φ_{p-3}-sequence $(a_n)_n$ is a complete Φ_{p-3}-sequence if and only if $a_n = b^n$ for all n, where b is a Φ_{p-3}-primitive root.*

We finish this section discussing the case $\kappa = \frac{p-1}{2}$. The corresponding statement for the case $\kappa = \frac{p+1}{2}$ follows by means of Proposition 1.

Theorem 4: *Let $p \geq 5$ be a prime number. A $\Phi_{\frac{p-1}{2}}$-sequence $(a_n)_n$ is complete if and only if $a_n = b^n$ for all n, where b is a $\Phi_{\frac{p-1}{2}}$-primitive root. Moreover, in this case $b = p - 2$.*

Proof: Let $(a_n)_n$ be a complete $\Phi_{\frac{p-1}{2}}$-sequence, so

$$a_n + a_{n+1} = a_{n+\frac{p-1}{2}} \text{ for every } n.$$

Then

$$\begin{aligned}a_{n-1} + 2a_n + a_{n+1} &= (a_{n-1} + a_n) + (a_n + a_{n+1}) \\ &= a_{n+\frac{p-1}{2}-1} + a_{n+\frac{p-1}{2}} = a_{n-1+p-1} = a_{n-1},\end{aligned}$$

so $2a_n + a_{n+1} = 0$ and therefore $a_{n+1} = -2a_n = (p-2)a_n$. But this implies

$$a_n = (p-2)^n \text{ for every } n.$$

Thus $p - 2$ is a $\Phi_{\frac{p-1}{2}}$-primitive root since $(a_n)_n$ is complete. □

Corollary: *Let $p \geq 5$ be a prime number. A $\Phi_{\frac{p+1}{2}}$-sequence $(a_n)_n$ is complete if and only if $a_n = b^n$ for all n, where b is a $\Phi_{\frac{p+1}{2}}$-primitive root. Moreover, in this case $b = \frac{p-1}{2}$.*

REFERENCES

[1] Owen Brison. "Complete Fibonacci Sequences in Finite Fields." *The Fibonacci Quarterly* **30.4** (1992): 295-304

[2] O. Brison and J. E. Nogueira. "Linear Recurring Sequence Subgroups in Finite Fields." *Finite Fields Appl.* **9.4** (2003): 413-422.

[3] Daniel Shanks. "Fibonacci Primitive Roots." *The Fibonacci Quarterly* **10.2** (1972): 163-168, 181.

[4] N. J. A. Sloane. *The on-line encyclopedia of integer sequences.* Sequence A000931 (Padovan sequence), http://www.research.att.com/projects/OEIS?Anum=A000931.

[5] Lawrence Somer. "Fibonacci-like Groups and Periods of Fibonacci-like Sequences." *The Fibonacci Quarterly* **15.1** (1977): 35-41.

AMS Classification Numbers: 11B37, 11B50