ON MODULAR FIBONACCI SETS

Mihai Caragiu

Ohio Northern University and Institute of Mathematics Bucharest
E-mail: m-caragiu1@onu.edu

William Webb

Department of Pure and Applied Mathematics, Washington State University, Pullman, WA 99164-3113
E-mail: webb@math.wsu.edu

(Submitted February 2001-Final Revision June 2001)

1. INTRODUCTION

For any prime p let us define the modular Fibonacci set Fib$[p]$ to be the subset of $\mathbf{F}_p = \{0, 1, \ldots, p-1\}$ (the finite field with p elements) consisting of *all the terms appearing in the Fibonacci sequence modulo p*. For example, when $p = 41$ we have the Fibonacci sequence modulo 41

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 14, 7, 21, 28, 8, 36, 3, 39, 1, 40, 0, 40, 40, 39,$$

$$38, 36, 33, 28, 20, 7, 27, 34, 20, 13, 33, 5, 38, 2, 40, 1, 0, \ldots$$

so that the corresponding modular Fibonacci set will be

$$\mathrm{Fib}[41] = \{0, 1, 2, 3, 5, 7, 8, 13, 14, 20, 21, 27, 28, 33, 34, 36, 38, 39, 40\} \subset \mathbf{F}_{41}.$$

Of course there are plenty of ways of picking up a special subset of $\mathbf{F}_p$ for any prime p. One possible choice would be to select within any finite prime field $\mathbf{F}_p$ the set of *all perfect squares modulo p*, say Sq$[p]$ so that, for example,

$$\mathrm{Sq}[11] = \{0, 1, 3, 4, 5, 9\}.$$

An interesting thing about the sets Sq$[p]$ is that they admit a uniform description by a first-order logical formula, namely

$$\Phi(X) \equiv (\exists Y)(X = Y^2)$$

The above $\Phi(X)$ is a first-order formula written in the language of rings such that for any prime p the subset Sq$[p]$ of $\mathbf{F}_p$ coincides with the set of all elements $x \in \mathbf{F}_p$ satisfying Φ:

$$\mathrm{Sq}[p] = \{x \in \mathbf{F}_p : \Phi(x) \text{ true}\}.$$

In a more technical language, we can say that *the perfect squares are first-order definable*.

At this moment the following natural question can be asked: is there a formula $\theta(X)$ that defines in each field $\mathbf{F}_p$ the set Fib$[p]$? By providing a *negative answer* to the above question, the present note establishes a worth noting, albeit negative, property of the family of modular Fibonacci sets. Our main result is the following:

Theorem 1: *There is no formula $\theta(x)$ written in the first-order language of rings that defines in each field $\mathbf{F}_p$ the set* Fib$[p]$.

For basic concepts of logic and model theory, including that of elementary formula one may consult [1]. An essential role in the proof of Theorem 1 will be played by the following result [2] estimating the number of points of definable subsets of finite fields:

Theorem 2: If $\theta(X)$ is a formula in one free variable X written in the first-order language of rings, then there are positive constants A, B, and positive rational numbers $0 < \mu_1 < \cdots < \mu_k \leq 1$ such that for any finite field $\mathbf{F}_q$, if $N_q(\theta)$ represents the number of elements $a \in \mathbf{F}_q$ such that $\theta(a)$ is true, either

$$N_q(\theta) \leq A$$

or

$$|N_q(\theta) - \mu_i q| \leq B\sqrt{q}$$

for some $i \in \{1, \ldots, k\}$.

Example. Consider

$$\theta(x) \equiv (\exists Y_1) \ldots (\exists Y_n)[(X + 1 = Y_1^2) \wedge \cdots \wedge (X + n = Y_n^2)]$$

so that $\theta(X)$ asserts that $X + 1, X + 2, \ldots, X + n$ are perfect squares within the field. In this case one can take $k = 2$ with $\mu_1 = 1/2^n$ and $\mu_2 = 1$. The first value, μ_1, stands for the fields of odd characteristic. Indeed, according to a classical result of Davenport, the number $N = N(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ of elements $x \in GF(q)$ for which the Legendre character takes n preassigned values $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ on $x + d_1,\ x + d_2, \ldots, x + d_n$, can be estimated ([4], p. 263) as $N = q/2^n + O(n\sqrt{q})$ with an absolute implied constant. The second value μ_2 stands for the finite fields of characteristic two, in which every element is a square.

2. PROOF OF THE MAIN RESULT

In order to apply Theorem 2 to the proof of our main result, we will need a result on the cardinalities of the modular Fibonacci sets Fib[p].

Proposition 3: For any $\varepsilon > 0$ there exists a prime p such that

$$|\mathrm{Fib}[p]| < p\varepsilon.$$

Proof: From [3] and [5] it follows that if $k(p)$ is the period of the Fibonacci sequence modulo p, then $p/k(p)$ is an unbounded function of the prime p. Proposition 3 is a straight-forward consequence of this fact.

We now proceed to the proof of Theorem 1. Let us suppose, by contradiction, that there exists some formula $\theta(X)$ in the first-order language of rings, with the property that for any prime p and any $x \in \mathbf{F}_p$

$$x \in \mathrm{Fib}[p] \Leftrightarrow \theta(x) \text{ true in } \mathbf{F}_p.$$

Let A, B and $0 < \mu_1 < \cdots < \mu_k \leq 1$ be the constants associated to the formula θ by Theorem 2. It follows then for any prime p, either

$$|\mathrm{Fib}[p]| \leq A \tag{1}$$

or

$$||\mathrm{Fib}[p]| - \mu_i p| \leq B\sqrt{p} \tag{2}$$

for some $i \in \{1, \ldots, k\}$. Note that (1) fails for all sufficiently large p, since the sequence of Fibonacci numbers is strictly increasing after the second term. Thus, for p big enough it is

(2) which must be true. However, by proposition 3, there are arbitrarily large p for which (2) fails for $i = 1, \ldots, k$. Thus a formula $\theta(X)$ as above cannot exist.

Remark: In the same way one can prove that there is no finite set $\{\theta_1(X), \ldots, \theta_n(X)\}$ of first-order formulas written in the language of rings such that for each prime p some formula $\theta_i(X)$ defines Fib$[p]$ in the field $\mathbf{F}_p$.

REFERENCES

[1] C.C. Chang and H.J. Keisler. *Model Theory*. Second Edition, North-Holland, Amsterdam, 1977.

[2] Z. Chatzidakis, L.v.d. Dries and A. Macintyre. "Definable Sets Over Finite Fields." *Crelle Journal* **427** (1992): 107-135.

[3] D. Jarden. "Unboundedness of the function [p-(5/p)]/a(p) in Fibonacci's sequence." *A.M. Monthly* **53** (1946): 426-427.

[4] R. Lidl and H. Niederreiter. *Finite Fields*. Second Edition, Cambridge University Press, 1997.

[5] J. Vinson. "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence." *The Fibonacci Quarterly* **1** (1963): 37-45.

AMS Classification Numbers: 11TXX, 11B50

✠ ✠ ✠