Bull. Aust. Math. Soc. **83** (2011), 413–419
doi:10.1017/S0004972710001693

ON SUMS OF FIBONACCI NUMBERS MODULO p

VICTOR C. GARCÍA, FLORIAN LUCA ✉ and V. JANITZIO MEJÍA HUGUET

(Received 24 May 2010)

Abstract

Here, we show that for most primes p, every residue class modulo p can be represented as a sum of 32 Fibonacci numbers.

2000 *Mathematics subject classification*: primary 11B39; secondary 11B50.
Keywords and phrases: Fibonacci numbers.

1. Introduction

Let F_n be the nth Fibonacci number. Recall that $F_0 = 0$, $F_1 = 1$ and

$$F_{n+2} = F_{n+1} + F_n \quad \text{holds for all } n \geq 0. \tag{1.1}$$

We put $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$ for the roots of the characteristic equation $x^2 - x - 1 = 0$. It is then well known that

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{holds for all } n \geq 0. \tag{1.2}$$

In particular, $F_n < \alpha^n$ holds for all positive integers n. It is convenient to extend the Fibonacci sequence $\{F_n\}_{n\geq 0}$ to negative integers, either using recurrence (1.1) directly or allowing n to be negative in formula (1.2). Either way, once this is done then $F_{-n} = (-1)^{n-1} F_n$ holds for all $n \geq 0$.

It is also well known that every positive integer n can be written as a sum of Fibonacci numbers

$$n = F_{m_1} + \cdots + F_{m_k} \quad \text{with } m_1 \geq m_2 \geq \cdots \geq m_k \geq 1. \tag{1.3}$$

If we impose the condition that the inequality $m_i - m_{i+1} \geq 2$ holds for all $i = 1, 2, \ldots, k-1$ then, up to identifying F_1 and F_2 (both equal to 1), the resulting representation (1.3) is unique and is called the *Zeckendorf representation of* n.

During the preparation of this paper, V.C.G. was supported by Grant UAM-A 2232508, F.L. was supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508, and V.J.M.H. was supported in part by Grant UAM-A 2232508 and a postdoctoral position at the IFM of UMSNH.

As with representations in base b (where $b > 1$ is an integer), most positive integers n have a large k in representation (1.3). In fact, it is easy to prove that the inequality $k \gg \log n$ holds on a set of asymptotic density 1.

Here, we look at the analogous problem modulo p. It turns out that for most primes p, every residue class can be represented as a sum of a bounded number of Fibonacci numbers.

THEOREM 1.1. *The set of primes p such that every residue class modulo p is a sum of 32 Fibonacci numbers is of relative asymptotic density 1.*

Before proceeding to the proof of Theorem 1.1, a few comments are in order. First of all, the conclusion of Theorem 1.1 does not hold for all primes. For example, it fails for the prime $p = F_{509}$. By the arguments from the proof of the Theorem 1.1 below, the Fibonacci sequence is periodic with period $4 \cdot 509$ modulo p. Thus, the totality of the number of residues modulo p which are a sum of at most 32 Fibonacci numbers is at most $(4 \cdot 509)^{32} < p$, therefore not all residues modulo p are a sum of 32 Fibonacci numbers. More generally, if n is a positive integer such that F_n has a prime factor $p > (4n)^{32}$, then the conclusion of Theorem 1.1 fails for p. We conjecture that there should exist infinitely many primes p with the above property, but a proof of this seems to be out of reach. It is quite likely that for every given constant K, starting with some large n the number F_n has a prime factor $p > n^K$. If this is true, then the conclusion of Theorem 1.1 would fail for infinitely many primes p even if the number 32 were replaced by any arbitrary constant K. However, our theorem only addresses the situation of most primes p, not of all primes p.

Our proof uses recent results from additive combinatorics. A different approach suggested to us by the referee would be to use recent results on explicit bounds on short exponential sums with exponential functions. We did not use this approach. This alternative approach might allow one to even obtain uniform distribution results regarding sums of K Fibonacci numbers (with K some sufficiently large but otherwise fixed number) modulo p valid on a subset of primes p of relative density 1. We leave these questions as future projects for the interested reader.

Throughout the paper, we use the classical notation $A = O(B)$, $A \ll B$ and $A \asymp B$ with their regular meaning. The constants implied by them are absolute. For a set $\mathcal{A}$ of positive integers and a positive real number x we write $\mathcal{A}(x)$ for $\mathcal{A} \cap [1, x]$.

2. Orders of appearance of primes

For a positive integer k we write $z(k)$ for the minimal positive integer ℓ such that $k | F_\ell$. The number $z(k)$ exists for all positive integers k and has the important property that $k | F_\ell$ if and only if $z(k) | \ell$. The number $z(k)$ is called the *order of appearance of* k.

The next few results show that the inequality $z(p) > 6p^{1/2}$ holds for almost all primes p. One could easily replace the lower bound $6p^{1/2}$ with the lower bound $p^{1/2} \exp((\log p)^\rho)$ with some sufficiently small $\rho > 0$ in the above inequality and keep the conclusion, but the bound $6p^{1/2}$ is sufficient for our purposes. Our proof

https://doi.org/10.1017/S0004972710001693 Published online by Cambridge University Press

follows an argument of Erdős and Murty [1] who proved a similar lower bound when $z(p)$ is replaced by the multiplicative order of 2 modulo p (see also [4, 6], for example, for various extensions of the above result).

For a positive real number y we put

$$\mathcal{P}(y) := \{p : z(p) < y\}. \tag{2.1}$$

LEMMA 2.1. *The estimate*

$$|\mathcal{P}(y)| < y^2 \tag{2.2}$$

holds.

PROOF. Observe that

$$\prod_{p\in\mathcal{P}(y)} p \quad \text{divides} \quad \prod_{t\le y} F_t.$$

Hence,

$$2^{|\mathcal{P}(y)|} \le \prod_{p\in\mathcal{P}(y)} p \le \prod_{t\le y} F_t.$$

Taking logarithms and using the fact that the inequality $F_m < \alpha^m$ holds for all m, we get that

$$|\mathcal{P}(y)| \log 2 \le \sum_{t\le y} \log F_t \le (\log \alpha) \sum_{t\le y} t < (\log \alpha) y^2,$$

whence the desired conclusion follows. □

We shall need some information concerning the number of divisors of shifted primes which are in a given interval. Namely, let

$$H(x, y, z) := |\{n \le x : d \mid n \text{ for some } d \in (y, z)\}|,$$

and for a given nonzero integer λ put

$$H(x, y, z; P_\lambda) := |\{p \le x : d \mid p + \lambda \text{ for some } d \in (y, z)\}|.$$

The following result appears in [2].

LEMMA 2.2. *If* $100 \le y \le x^{1/2}$ *and* $2y \le z \le y^2$, *then*

$$H(x, y, z) \asymp x u^{\delta} (\log 2/u)^{-3/2},$$

where u *is defined implicitly by* $z = y^{1+u}$ *and*

$$\delta = 1 - \frac{1 + \log\log 2}{\log 2} = 0.086\,071\ldots.$$

Furthermore, let $1 \le y \le x^{1/2}$ *and* $y + (\log y)^{2/3} \le z \le x$. *The following estimate holds:*

$$H(x, y, z; P_\lambda) \ll_\lambda \frac{H(x, y, z)}{\log x}.$$

https://doi.org/10.1017/S0004972710001693 Published online by Cambridge University Press

Define

$$\mathcal{S} := \{p : z(p) > 6p^{1/2}\}. \tag{2.3}$$

LEMMA 2.3. *The estimate*

$$|\mathcal{S}(x)| = \pi(x)(1 + o(1)) \quad \textit{holds as } x \to \infty. \tag{2.4}$$

PROOF. We split the set of primes $p \le x$ as $\mathcal{Q}(x) \cup \mathcal{R}(x) \cup \mathcal{S}(x)$, where

$$\mathcal{Q}(x) := \{p \le x : z(p) < p^{1/2}/\log p\}$$

and

$$\mathcal{R}(x) := \{p \le x : p^{1/2}/\log p \le z(p) \le 6p^{1/2}\}.$$

From Lemma 2.1, we obtain

$$|\mathcal{Q}(x)| < \frac{x}{(\log x)^2}.$$

Let us suppose now that $p > 5$. Recalling that $z(p) \mid p \pm 1$, we observe that any prime $p \in \mathcal{R}(x)$ belongs to the set

$$\{p \le x : d \mid p \pm 1 \text{ for some } d \in [p^{1/2}/\log p, 6p^{1/2}]\}.$$

Hence,

$$\begin{aligned}\mathcal{R}(x) &\subseteq \left\{p \le \frac{x}{\log x}\right\} \\ &\quad \cup \left\{\frac{x}{\log x} < p \le x : d \mid p \pm 1 \text{ for some } d \in \left[\frac{p^{1/2}}{\log p}, 6p^{1/2}\right]\right\} \\ &\subseteq \left\{p \le \frac{x}{\log x}\right\} \\ &\quad \cup \left\{\frac{x}{\log x} < p \le x : d \mid p \pm 1 \text{ for some } d \in \left[\frac{x^{1/2}}{(\log x)^{3/2}}, 6x^{1/2}\right]\right\}.\end{aligned}$$

Therefore, taking

$$y = \frac{x^{1/2}}{(\log x)^{3/2}} \quad \text{and} \quad z = 6x^{1/2},$$

we have, in view of Lemma 2.2,

$$\begin{aligned}|\mathcal{R}(x)| &\ll \frac{x}{\log^2 x} + H\left(x, \frac{x^{1/2}}{(\log x)^{3/2}}, 6x^{1/2}; P_1\right) + H\left(x, \frac{x^{1/2}}{(\log x)^{3/2}}, 6x^{1/2}; P_{-1}\right) \\ &\ll \frac{x}{\log^2 x} + \frac{x}{\log x}\frac{(\log\log x)^{\delta-3/2}}{(\log x)^{\delta}} = o(\pi(x)) \quad \text{as } x \to \infty,\end{aligned}$$

and so estimate (2.4) follows. □

https://doi.org/10.1017/S0004972710001693 Published online by Cambridge University Press

3. The subset $\{F_n\}_{n\geq 0}$ modulo p for most primes p

Let x be a large real number and let $p \leq x$. In light of the results from Section 2, we may assume that $p \in \mathcal{S}(x)$. Consider the set $\{F_{2n}\}_{n\geq 0}$ modulo p. It is easy to see that $4z(p)$ is the period of the Fibonacci sequence modulo p. Indeed, this can be obtained using the formula

$$2F_{a+b} = F_a L_b + F_b L_a \tag{3.1}$$

valid for all integers a and b, where $\{L_n\}_{n\geq 0}$ is the Lucas companion of the Fibonacci sequence given by $L_0 = 2$, $L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$. The formula for its general term is

$$L_n = \alpha^n + \beta^n \quad \text{for all } n \geq 0. \tag{3.2}$$

As for the case of the Fibonacci numbers, we can extend the sequence of Lucas numbers to negative integers by allowing n to be negative in formula (3.2). Taking $b = 4z(p)$ in (3.1) and using the fact that $F_{2n} = F_n L_n$ and $L_{2n} = 5F_n^2 + 2(-1)^n$, we get that

$$\begin{aligned} 2F_{a+4z(p)} &= F_a L_{4z(p)} + L_a F_{4z(p)} = F_a(5F_{2z(p)}^2 + 2) + L_a F_{2z(p)} L_{2z(p)} \\ &= F_a(5(F_{z(p)}L_{z(p)})^2 + 2) + L_a F_{z(p)} L_{z(p)} L_{2z(p)} \\ &\equiv 2F_a \mod p, \end{aligned}$$

because $p | F_{z(p)}$. Hence, for $p > 2$, we get that

$$F_{a+4z(p)} \equiv F_a \mod p \quad \text{for all integers } a.$$

We now take

$$\mathcal{F} = \{F_{2n} \bmod p : n \in \{0, 1, \ldots, 2z(p) - 1\}\}. \tag{3.3}$$

Let us count the number of distinct elements in $\mathcal{F}$. Assume that $F_m \equiv F_n \bmod p$ for some even integers $m, n \in [0, 4z(p))$. Using the fact that

$$F_m - F_n = F_{(m-\delta n)/2} L_{(m+\delta n)/2} \quad \text{for some } \delta \in \{\pm 1\},$$

(see [5, Lemma 2]), it follows that $p | F_{(m\pm n)/2}$ or $p | L_{(m\pm n)/2}$. Hence, p divides one of F_{m+n} or F_{m-n}, and therefore $m \equiv \pm n \bmod z(p)$. Since also m and n are even and in $[0, 4z(p))$, we conclude easily that

$$|\mathcal{F}| \geq \frac{2z(p)}{8} = \frac{z(p)}{4} > \sqrt{2}p^{1/2}.$$

For future use we record what we have shown.

LEMMA 3.1. *Let p be a prime and let $\mathcal{F}$ be the subset (3.3) modulo p. Then the inequality*

$$|\mathcal{F}| \geq \frac{2z(p)}{8} = \frac{z(p)}{4} > \sqrt{2}p^{1/2} \tag{3.4}$$

holds for all primes $p \in \mathcal{S}$, where this last set is shown in (2.3).

https://doi.org/10.1017/S0004972710001693 Published online by Cambridge University Press

4. Proof of the theorem

Here and in what follows, we use the standard notation

$$AB = \{ab \bmod p : a \in A, b \in B\}$$

and

$$A + B = \{a + b \bmod p : a \in A, b \in B\}.$$

We shall use the following result from [3].

LEMMA 4.1. *Let A, B be subsets of $\mathbb{Z}_p$ with $|A||B| > 2p$. Then*

$$8AB = \mathbb{Z}_p.$$

Taking $A = B = \mathcal{F}$, it immediately follows from Lemma 3.1 that if $p \in \mathcal{S}$ every residue class $\lambda \bmod p$ can be written as

$$F_{n_1} F_{m_1} + \cdots + F_{n_8} F_{m_8} \mod p, \tag{4.1}$$

with even indices $m_1, n_1, \ldots, m_8, n_8$. We are interested in the representability of every residue class as a bounded sum of Fibonacci numbers, and we are almost there. The only slight problem is that a product of two Fibonacci numbers is not a Fibonacci number.

To deal with this, we prove another lemma.

LEMMA 4.2. *Assume that a and b are even. Then:*

(i) $$5F_a F_b = L_{a+b} - L_{a-b};$$

(ii) $$F_a L_b = F_{a+b} + F_{a-b}.$$

PROOF. The proof follows easily from relations (1.2) and (3.2). □

The above lemma implies at once that if x, y, z are all even, then

$$\begin{aligned} 5F_x F_y F_z &= (L_{x+y} - L_{x-y}) F_z \\ &= F_{x+y+z} + F_{-x-y+z} - F_{x-y+z} - F_{-x+y+z} \\ &= F_{x+y+z} + F_{-x-y+z} + F_{-x+y-z} + F_{x-y-z}, \end{aligned}$$

where in the above we also used the fact that $-F_n = F_{-n}$ for even values of n. Taking $x = 2$ above, we conclude that $5F_y F_z$ is a sum of four Fibonacci numbers of even indices. Keeping this in mind and assuming that $p > 5$, let us recall again (see (4.1)) that for every $\lambda \bmod p$ there exist Fibonacci numbers F_{m_i}, F_{n_i} with $i = 1, \ldots, 8$ such that

$$F_{m_1} F_{n_1} + \cdots + F_{m_8} F_{n_8} \equiv 5^{-1}\lambda \mod p,$$

where we use $5^{-1} \bmod p$ for the multiplicative inverse of 5 modulo p. Finally, every term $5F_{m_i} F_{n_i}$ for $i = 1, \ldots, 8$ in the representation

$$5F_{m_1} F_{n_1} + \cdots + 5F_{m_8} F_{n_8} \equiv \lambda \mod p$$

is a sum of four Fibonacci numbers, which concludes the proof.

https://doi.org/10.1017/S0004972710001693 Published online by Cambridge University Press

Acknowledgement

We thank the referee for suggestions which improved the quality of this paper and for providing us with some very useful references.

References

[1] P. Erdős and M. R. Murty, 'On the order of a (mod p)', in: *Number Theory (Ottawa, ON, 1996)*, CRM Proceedings and Lecture Notes, 19 (American Mathematical Society, Providence, RI, 1999), pp. 87–97.
[2] K. Ford, 'The distribution of integers with a divisor in a given interval', *Ann. of Math.* (2) **168** (2008), 367–433.
[3] A. Glibichuk, 'Combinatorial properties of sets of residues modulo a prime and the Erdős–Graham problem', *Mat. Zametki* **79** (2006), 384–395; English translation, *Math. Notes* **79**(3–4) (2006), 356–365.
[4] P. Kurlberg and C. Pomerance, 'On the periods of the linear congruential and power generators', *Acta Arith.* **119** (2005), 149–169.
[5] F. Luca and L. Szalay, 'Fibonacci numbers of the form $p^a \pm p^b + 1$', *Fibonacci Quart.* **45** (2007), 98–103.
[6] F. Pappalardi, 'On the order of finitely generated subgroups of $\mathbb{Q}^*$ (mod p) and divisors of $p - 1$', *J. Number Theory* **57** (1996), 207–222.

VICTOR C. GARCÍA, Departamento de Ciencias Básicas,
Universidad Autónoma Metropolitana-Azcapotzalco,
Av. San Pablo #180, Col. Reynosa Tamaulipas,
Azcapotzalco, C.P. 02200, México DF, México
e-mail: vc.garci@gmail.com

FLORIAN LUCA, Instituto de Matemáticas,
Universidad Nacional Autónoma de México,
C.P. 58089, Morelia, Michoacán, México
e-mail: fluca@matmor.unam.mx

V. JANITZIO MEJÍA HUGUET, Departamento de Ciencias Básicas,
Universidad Autónoma Metropolitana-Azcapotzalco,
Av. San Pablo #180, Col. Reynosa Tamaulipas,
Azcapotzalco, C.P. 02200, México DF, México
e-mail: vjanitzio@gmail.com