Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Víctor Cuauhtemoc GARCÍA

On the distribution of sparse sequences in prime fields and applications

Tome 25, n° 2 (2013), p. 317-329.

<http://jtnb.cedram.org/item?id=JTNB_2013__25_2_317_0>

Journal de Théorie des Nombres de Bordeaux **25** (2013), 317–329

On the distribution of sparse sequences in prime fields and applications

par Víctor Cuauhtemoc GARCÍA

Résumé. Dans cet article, nous étudions les propriétés de distribution de suites parsemées modulo presque tous le nombres premiers. On obtient des résultats nouveaux pour une large classe de suites parsemées avec applications aux problèmes additifs et au problème de Littlewood discret en rapport avec l'estimation des bornes inférieures de la norme L_1 de sommes trigonométriques.

Abstract. In the present paper we investigate distributional properties of sparse sequences modulo almost all prime numbers. We obtain new results for a wide class of sparse sequences which in particular find applications on additive problems and the discrete Littlewood problem related to lower bound estimates of the L_1-norm of trigonometric sums.

1. Introduction

Throughout the paper $\{x_n\}$ denotes an increasing sequence of positive integers. The study of distributional properties of the sequence

$$x_n \pmod p; \quad n = 1, 2, \dots ,$$

and additive problems connected with such sequences are classical questions in number theory with a variety of results in the literature. When $\{x_n\}$ grows rapidly the problem becomes harder for individual moduli, but it is possible to obtain strong results modulo p for most primes p. We mention the work of Banks *et al.*, [1], where a series of results on distribution of Mersenne numbers $M_q = 2^q - 1$ in residue classes have been obtained. This question has also been considered by Bourgain in [3]. General results on the distribution of sequences of type $2^{x_n} \pmod p$, for almost all primes p, (and generally of the form λ^{x_n}) have been obtained by Garaev and Shparlinski [10], and by Garaev [8]. For instance, Garaev [8] established a non-trivial upper bound for the exponential sum

$$\max_{(a,p)=1} \left| \sum_{n \le T} e^{2\pi i \frac{a}{p} \lambda^{x_n}} \right| ,$$

for $\pi(N)(1+o(1))$ primes $p \le N$ and $T = N(\log N)^{2+\varepsilon}$, where $\{x_n\}$ is any strictly increasing sequence of positive integers satisfying $x_n \le n^{15/14+o(1)}$. Banks *et al.*, [2] obtained uniform distributional properties of the sequences

$$f_\lambda(n) = \frac{\lambda^{n-1}-1}{n}, \qquad h_\lambda(n) = \frac{\lambda^{n-1}-1}{P(n)},$$

where λ and n are positive integers, n is composite and $P(n)$ is the largest prime factor of n.

Now consider a simpler sequence

$$2^n \pmod p; \qquad n = 1, 2, \dots .$$

From a result of Erdős and Murty [6] it is well-known that, for $\pi(N)(1+o(1))$ primes $p \le N$, 2 has multiplicative order $t_p \ge N^{1/2+o(1)}$. Combining this with a result of Glibichuk [12] it follows that for almost all primes p every residue class modulo p can be represented in the form

$$2^{n_1} + \cdots + 2^{n_8} \pmod p,$$

for certain positive integers $n_1, \dots, n_8$.

We remark the work of Schoen and Shkredov [20]. Here, from a more general result, it follows that for all sufficiently large prime p if R is any multiplicative subgroup of $\mathbb{F}_p^*$ satisfying $|R| > p^{1/2}$, then $\mathbb{F}_p^* \subseteq 6R$. As a direct consequence one has that for most primes p, every nonzero residue class modulo p can be written as

$$2^{n_1} + \cdots + 2^{n_6} \pmod p.$$

In the work [11], the authors applied similar arguments as Erdős and Murty [6] to obtain analogous results for the sequence of Fibonacci numbers

$$F_n \pmod p; \qquad n = 1, 2, \dots ,$$

where

$$F_{n+2} = F_{n+1} + F_n, \qquad n \ge 1,$$

with $F_1 = F_2 = 1$. They proved that for almost all primes p, every residue class modulo p is a sum of 32 Fibonacci numbers.

In the present paper using a different approach we obtain new results on additive properties for general sparse sequences for almost all prime moduli. In particular we prove that for $\pi(N)(1+o(1))$ primes $p \le N$ every residue class is a sum of 16 Fibonacci numbers F_n, with $n \le N^{1/2+o(1)}$, improving upon the mentioned result of [11]. Moreover, we establish that for any $\varepsilon > 0$ there is an integer $s = \mathcal{O}(1/\varepsilon)$ such that for $\pi(N)(1+o(1))$ primes, $p \le N$, every residue class can be written as

$$F_{n_1} + \cdots + F_{n_s} \pmod p,$$

with $1 \le n_1, \dots, n_s \le N^\varepsilon$. We note that the value s has the optimal order $s = \mathcal{O}(1/\varepsilon)$.

Solving the Littlewood conjecture, Konyagin [15], and McGehee, Pigno and Smith [17] proved that for any finite subset $\mathcal{A}$ of integers with T elements, the following estimate holds

$$\int_0^1 \left| \sum_{a \in \mathcal{A}} e^{2\pi i \alpha a} \right| \mathrm{d}\alpha \gg \log T. \tag{1.1}$$

This bound reflects the best possible lower bound in general settings, as it shown by the example $\mathcal{A} = \{1, 2, 3, \dots, T\}$. However for a very wide class of integer valued sequences x_n, estimate (1.1) has been improved, see for example Garaev [7], Karatsuba [14] and Konyagin [16].

Green and Konyagin [13] established a variant of the Littlewood problem in prime fields $\mathbb{F}_p$. Theorem 1.2 states that if $\mathcal{A}$ is a subset of $\mathbb{F}_p$, with $|\mathcal{A}| = (p-1)/2$, then

$$\frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{a \in \mathcal{A}} e^{2\pi i \frac{x}{p} a} \right| \gg (\log p / \log\log p)^{1/3}.$$

In this spirit, combining ideas of Karatsuba [14] and Theorem 2.1, we improve the mentioned result of [13] for exponential sums involving the sequence $\{F_n\}$ of Fibonacci numbers for most primes. More precisely, we prove that given any positive real $\gamma < 1/3$ there are positive constants $c_1 = c_1(\gamma), c_2 = c_2(\gamma)$ such that for $\pi(N)(1 + o(1))$ primes $p \le N$ the following estimate holds

$$c_1 N^{\gamma/2} \le \frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \le N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right| \le c_2 N^{\gamma/2}.$$

2. Results

Throughout the paper N and M denote sufficiently large integer parameters.

The first result of our present paper relies on ideas of arithmetic combinatorics and the combination with estimates of rational exponential sum techniques.

Theorem 2.1. *Let $\Delta = \Delta(N)$ be a function with $\Delta(N) \to \infty$, as $N \to \infty$. Let $\mathcal{X}$ be any subset of $\{1, \dots, 10^M\}$ such that*

$$|\mathcal{X}| \le \frac{\pi(N) \log M}{M \Delta^2}.$$

Then for $\pi(N)\,(1+\mathcal{O}(\Delta^{-1}))$ *of primes* $p \le N$ *we have*

$$\#\{x \pmod p \,:\, x \in \mathcal{X}\ \} = |\mathcal{X}|\left(1+\mathcal{O}\left(\Delta^{-1}\right)\right). \tag{2.1}$$

The work of Elsholtz [5] establishes a result of a similar flavour. If $\mathcal{A} \subset [1,x]$ is a set pf integers with $|\mathcal{A}| \gg (\log x)^r$, then

$$|\{a \pmod p \,:\, a \in \mathcal{A}\}| \gg p^{\frac{r}{r+1}},$$

for most primes $p \le (\log x)^{r+1}$.

Theorem 2.1 allow us to deal with sparse sets. If $\Delta \to \infty$ as $x \to \infty$ and $\mathcal{A} \subset [1,x]$ with $|\mathcal{A}| \ll (\log x)^r/\Delta$, then

$$|\{a \pmod p \,:\, a \in \mathcal{A}\}| = |\mathcal{A}|\,(1+o(1)),$$

for most primes $p \le (\log x)^{r+1}$.

Theorem 2.1 finds applications to additive problems for well known rapidly increasing sequences. For example the following theorems on additive properties of the Fibonacci sequence $\{F_n\}$.

Theorem 2.2. *For* $\pi(N)(1+o(1))$ *primes* $p \le N$, *every residue class* $\lambda \pmod p$ *can be written as*

$$F_{n_1} + \cdots + F_{n_{16}} \equiv \lambda \pmod p,$$

where $1 \le n_1, \ldots, n_{16} \le N^{1/2+o(1)}$.

Moreover, given $\varepsilon > 0$ it is natural to ask if there exist a fixed integer $s = s(\varepsilon)$, such that for every sufficiently large prime p every residue class modulo p can be written as

$$F_{n_1} + \cdots + F_{n_s} \pmod p, \quad \text{with} \quad n_i \le N^{\varepsilon}, \quad i = 1, \ldots, s.$$

For similar additive problems see [4], [12] and [21]. Combining Theorem 2.1 with exponential sum techniques (Lemma 3.3) we obtain the following result.

Theorem 2.3. *Let* $0 < \varepsilon < 1/2$. *For* $s = 4([8/\varepsilon]-1)$ *and for* $\pi(N)(1+o(1))$ *primes* $p \le N$, *every residue class* λ *can be written as*

$$F_{n_1} + \cdots + F_{n_s} \equiv \lambda \pmod p,$$

where $n_i \le N^{\varepsilon}$, $i = 1, \ldots, s$.

Note that $s = s(\varepsilon)$ has the expected order $\mathcal{O}(1/\varepsilon)$.

As we have already mentioned in the Introduction, following ideas of Karatsuba's work [14], we obtain another application of Theorem 2.1 .

Theorem 2.4. *Let $0 < \gamma < 1/3$. There are two positive absolute constants $c_1 = c_1(\gamma), c_2 = c_2(\gamma)$ such that for $\pi(N)(1 + o(1))$ primes, $p \le N$, we have*

$$c_1 N^{\gamma/2} \le \frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \le N^\gamma} e^{2\pi i \frac{x}{p} F_n} \right| \le c_2 N^{\gamma/2}.$$

3. Notation and lemmas

For given subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathbb{F}_p$ and any integer $k \ge 2$, as usual, we denote

$$\begin{aligned} \mathcal{A} + \mathcal{B} &= \{a + b \ : \ a \in \mathcal{A},\ b \in \mathcal{B}\}, \\ \mathcal{A} \cdot \mathcal{B} &= \{ab \ : \ a \in \mathcal{A},\ b \in \mathcal{B}\}, \\ k\mathcal{A} &= \{a_1 + \ldots + a_k \ : \ a_1, \ldots, a_k \in \mathcal{A}\}. \end{aligned}$$

For any finite subset of integers $\mathcal{X}$ we denote

$$\mathcal{X} \pmod p = \{x \pmod p \ : \ x \in \mathcal{X}\}.$$

The next lemma is a result of Glibichuk [12].

Lemma 3.1. *Let $\mathcal{A}, \mathcal{B}$ be subsets of $\mathbb{F}_p$ such that $|\mathcal{A}||\mathcal{B}| > 2p$. Then*

$$8\mathcal{A} \cdot \mathcal{B} = \mathbb{F}_p.$$

Given a fixed prime number p, we denote by t_p the *multiplicative order* of 2 modulo p. That is

$$t_p = \min\{\ell \ : \ 2^\ell \equiv 1 \pmod p\}.$$

From [6, Theorem 3], the mentioned work of Erdös–Murty, it follows that for $\pi(N)(1 + o(1))$ primes, $p \le N$, we have $t_p > p^{1/2} e^{(\log p)^{\rho_0}}$, for some $\rho_0 > 0$. Indeed, it is possible to prove that if ρ is any positive function $\rho(N) \to 0$, as $N \to \infty$, then for $\pi(N)(1 + o(1))$ primes we have $t_p > N^{1/2+\rho}$. As usual, we employ the notation $N^{o(1)}$ instead N^ρ. For a more general results on this topic see the work [18].

We present an analogous result for the *order of appearance,* defined by

$$z(k) = \min\{\ell \ : \ F_\ell \equiv 0 \pmod k\},$$

where k is a fixed integer $k \ge 2$ and F_n denotes the nth term of the sequence of Fibonacci numbers.

Lemma 3.2. *For almost all primes $p \le N$, we have*

$$z(p) \ge N^{1/2+o(1)}.$$

We require the following lemma which follows from exponential sums estimates, see for example the proof of [9, Theorem 1.1] or [19].

Lemma 3.3. *Let X, Y and Z be subsets of $\{0, 1, \ldots, p-1\}$. Denote by T the number of solutions of the congruence*

$$xy + z_1 + z_2 \equiv \lambda \pmod{p}, \tag{3.1}$$

where

$$x \in X, \quad y \in Y, \quad z_1, z_2 \in Z.$$

Then, the asymptotic formula

$$T = \frac{|X||Y||Z|^2}{p} + \theta\sqrt{p|X||Y|}|Z|, \quad |\theta| \leq 1,$$

holds uniformly over λ. In particular Eq. (3.1) *has a solution if $|X||Y||Z|^2 > p^3$.*

We shall use some results concerning the values of Fibonacci sequence.

$$F_{u+v} = \frac{1}{2}(F_u L_v + L_u F_v), \tag{3.2}$$

$$F_{u-v} = \frac{(-1)^v}{2}(F_u L_v - L_u F_v), \tag{3.3}$$

where $\{L_m\}$ is the Lucas sequence given by

$$L_{m+2} = L_{m+1} + L_m, \quad L_1 = 1,\ L_2 = 3.$$

3.1. Proof of Theorem 2.1. In order to establish Theorem 2.1, we need to introduce an auxiliary lemma. Recall that N, M denote very large integer parameters and $\mathcal{X}$ is any subset of $\{1, 2, 3, \ldots, 10^M\}$. We denote by $\mathcal{J}(N)$ the number of solutions of the congruence

$$x \equiv y \pmod{p}; \qquad x, y \in \mathcal{X}, \quad p \leq N. \tag{3.4}$$

Lemma 3.4. *The following asymptotic formula holds*

$$\mathcal{J}(N) = \pi(N)|\mathcal{X}| + \mathcal{O}\left(\frac{|\mathcal{X}|^2 M}{\log M}\right). \tag{3.5}$$

Proof. If $x = y$ then Eq. (3.4) has $\pi(N)|\mathcal{X}|$ solutions. Therefore

$$\mathcal{J}(N) = \pi(N)|\mathcal{X}| + \mathcal{J}', \tag{3.6}$$

where $\mathcal{J}'$ denotes the number of solutions of (3.4) subject to $x \neq y$. Given x, y in $\mathcal{X}$ with $x \neq y$, the equation

$$pk = x - y, \qquad p \leq N,$$

has at most $\omega(|x-y|)$ solutions, where $\omega(n)$ denotes the number of prime divisors of n. If $4 \leq |x-y| \leq 10^M$, using the well-known estimate $\omega(n) \ll$

$(\log n)/(\log\log n)$, we obtain that (3.4) has at most $\mathcal{O}(|\mathcal{X}|^2 M/\log M)$ solutions. Otherwise, if $0 < |x-y| < 4$, then (3.4) has no more than $\mathcal{O}(|\mathcal{X}|)$ solutions. Thus

$$\mathcal{J}' \ll |\mathcal{X}|^2 \frac{M}{\log M}.$$

Inserting this upper bound for $\mathcal{J}'$ in (3.6), Lemma 3.4 follows. □

Proof. Let J_p be the number of solutions of the congruence

$$x \equiv y \pmod p; \quad x, y \in \mathcal{X}. \tag{3.7}$$

Note that $J_p \geq |\mathcal{X}|$, because the case $x = y$ satisfies (3.7). It is clear that

$$\mathcal{J}(N) = \sum_{p \leq N} J_p.$$

Let Δ be any strictly increasing function $\Delta = \Delta(N) \to \infty$ as $N \to \infty$. Denote by $\mathcal{R}$ the set of prime numbers $p \leq N$ such that

$$J_p - |\mathcal{X}| > \frac{|\mathcal{X}|^2 M}{\pi(N)\log M}\Delta.$$

If p runs through the set $\mathcal{R}$, recalling that $J_p - |\mathcal{X}| \geq 0$, we get

$$|\mathcal{R}|\frac{|\mathcal{X}|^2 M}{\pi(N)\log M}\Delta \leq \sum_{p\in\mathcal{R}}(J_p - |\mathcal{X}|) \leq \sum_{p\leq N}(J_p - |\mathcal{X}|) = \mathcal{J}(N) - \pi(N)|\mathcal{X}|.$$

Thus, applying Lemma 3.4, we derive that

$$|\mathcal{R}| \ll \frac{\pi(N)}{\Delta}.$$

If $\mathcal{Q}$ denotes the number of primes $p \leq N$ such that

$$J_p - |\mathcal{X}| \leq \frac{|\mathcal{X}|^2 M}{\pi(N)\log M}\Delta,$$

then

$$|\mathcal{Q}| = \pi(N) - |\mathcal{P}| = \pi(N)(1 + \mathcal{O}(\Delta^{-1})).$$

Therefore, we obtain the following lemma.

Lemma 3.5. *For $\pi(N)(1+\mathcal{O}(\Delta^{-1}))$ primes $p \leq N$, the asymptotic formula holds*

$$J_p = |\mathcal{X}| + \mathcal{O}\left(\frac{|\mathcal{X}|^2 M}{\pi(N)\log M}\Delta\right). \tag{3.8}$$

Now, given $\lambda \in \{x \pmod p : x \in \mathcal{X}\}$ denote by $J(\lambda)$ the number of solutions of the congruence

$$x \equiv \lambda \pmod p, \qquad x \in \mathcal{X}.$$

By Cauchy–Schwarz inequality it follows that

$$\left(\sum_{\lambda\in\{x \pmod p)\,:\,x\in\mathcal{X}\}} J(\lambda)\right)^2 \le \left(\sum_{\lambda\in\{x \pmod p)\,:\,x\in\mathcal{X}\}} 1\right) \times \times \left(\sum_{\lambda\in\{x \pmod p)\,:\,x\in\mathcal{X}\}} J^2(\lambda)\right).$$

Note that

$$|\mathcal{X}| = \sum_{\lambda\in\{x \pmod p)\,:\,x\in\mathcal{X}\}} J(\lambda),$$

$$J_p = \sum_{\lambda\in\{x \pmod p)\,:\,x\in\mathcal{X}\}} J^2(\lambda).$$

Therefore, we have obtained the relation

$$\#\{x \pmod p \,:\, x\in\mathcal{X}\} \ge \frac{|\mathcal{X}|^2}{J_p}.$$

Finally, substituting (3.8) and the assumption

$$|\mathcal{X}| \le \frac{\pi(N)\log M}{M\Delta^2},$$

Theorem 2.1 follows. □

3.2. Proof of Theorem 2.2. Lemma 3.2 allows us to establish the order of the value set of the Fibonacci sequence for most primes

$$\#\{F_n \pmod p \,:\, n\le \delta N^{1/2}\} \asymp \delta N^{1/2},$$

where $\delta = \delta(N) = N^{o(1)}$ is an increasing function $\delta\to\infty$. In order to establish the last relation, it is sufficient to prove that for

$$\mathcal{F} = \{F_{2n} \,:\, \delta N^{1/2}/10 < n \le \delta N^{1/2}/5\},$$

we have

$$|\mathcal{F} \pmod p| = |\mathcal{F}| = \frac{\delta N^{1/2}}{10} + \mathcal{O}(1). \tag{3.9}$$

Let n, n' be positive integers such that

$$F_{2n} \equiv F_{2n'} \pmod p; \quad \delta N^{1/2}/10 < n, n' \le \delta N^{1/2}/5. \tag{3.10}$$

Without loss of generality we can assume that $n \ge n'$. Substituting $u = n+n'$ and $v = n-n'$ in (3.2) and (3.3), we can obtain

$$F_{2n} - F_{2n'} = \frac{1}{2}\left((1-(-1)^{n-n'})F_{n+n'}L_{n-n'} + (1+(-1)^{n-n'})L_{n+n'}F_{n-n'}\right).$$

Suppose that $n-n' \equiv 0 \pmod 2$, from Eq. (3.10) it follows that

$$p | L_{n+n'}F_{n-n'}.$$

If $n \neq n'$, then $0 < n - n' < N^{1/2}\delta \leq z(p)$, which implies $(p, F_{n-n'}) = 1$. Thus

$$p | L_{n+n'}, \quad \text{in particular} \quad p | F_{n+n'} L_{n+n'},$$

where $F_{n+n'} L_{n+n'} = F_{2(n+n')}$. Hence $p | F_{2(n+n')}$, with $2(n+n') < z(p)$. This contradicts the choice of $z(p)$. Therefore in the case $n - n' \equiv 0 \pmod 2$ Eq. (3.10) has only trivial solutions $n = n'$. Similarly, it is possible to verify that (3.10) has no solutions if $n - n' \equiv 1 \pmod 2$.

Now, consider the subset of the Lucas sequence

$$\mathcal{L} = \{L_{2m} \ : \ 1 \leq m \leq N^{1/2}/\sqrt{\delta}\}.$$

Taking in Theorem 2.1; $M = N^{1/2}/\sqrt{\delta}$ and $\Delta = \delta^{1/4}$ we obtain

$$|\mathcal{L} \pmod p| = \frac{N^{1/2}}{\sqrt{\delta}}(1 + \mathcal{O}(\delta^{-1/4})). \tag{3.11}$$

Observe that equalities (3.9) and (3.11) are valid respectively for most primes. Thus, for $\pi(N)(1 + o(1))$ primes $p \leq N$ we have

$$|\mathcal{F} \pmod p||\mathcal{L} \pmod p| \gg \sqrt{\delta} N \geq 2p.$$

Applying Lemma 3.1, we obtain that for almost all primes p every integer λ can be written as

$$F_{2n_1} L_{2m_1} + \cdots + F_{2n_8} L_{2m_8} \equiv \lambda \pmod p,$$

where

$$N^{1/2}\delta/10 < n_i \leq N^{1/2}\delta/5, \quad 1 \leq m_i \leq N^{1/2}/\sqrt{\delta}, \quad 1 \leq i \leq 8.$$

Using the identity

$$F_u L_v = F_{u+v} + (-1)^v F_{u-v},$$

for every $1 \leq i \leq 8$ we get

$$F_{2n_i} L_{2m_i} = F_{2(n_i+m_i)} + F_{2(n_i-m_i)}.$$

Thus, Theorem 2.2 follows. $\square$

3.3. Proof of Theorem 2.3. Let k be the minimal integer such that $1/(k+2) < \varepsilon/8$. Define the sets

$$\begin{aligned} X &= \{F_{2n_1-1} + \cdots + F_{2n_k-1} \ : \ 1 \leq n_1, \ldots, n_k \leq N^{\frac{1}{k+2}}\}, \\ Y &= \{L_m \ : \ \frac{1}{2} N^{\frac{7}{k+2}} < m \leq N^{\frac{7}{k+2}}\}, \\ Z &= \{F_{2\ell_1} + \cdots + F_{2\ell_k} \ : \ 1 \leq \ell_1, \ldots, \ell_k \leq N^{\frac{1}{k+2}}\}. \end{aligned}$$

Observe that $|Y| \gg N^{\frac{7}{k+2}}$ and there exists a positive constant $c = c(k) < 1$ such that

$$|X|, |Z| \geq c N^{\frac{k}{k+2}}.$$

In order to estimate the value set of $X \pmod p$ note that if $x \in X$, then $x \leq 10^{(\log k)N^{1/(k+2)}}$. Thus, applying Theorem 2.1 with $M = (\log k)N^{1/(k+2)}$, $\mathcal{X} = Z$ and $\Delta = (\log N)^A$, (for any integer $A > 0$), we have that for most of primes $p \leq N$

$$|X \pmod p| = |X|(1 + o(1)).$$

Analogously, we can obtain

$$|Y \pmod p| = |Y|(1 + o(1)), \qquad |Z \pmod p| = |Z|(1 + o(1)),$$

for almost all primes respectively. Therefore, there is a constant $c_1 = c_1(k)$, $0 < c_1 < 1$, such that for $\pi(N)(1 + o(1))$ primes $p \leq N$ we have

$$|X \pmod p||Y \pmod p||Z \pmod p|^2 \geq c_1 N^{3+\frac{1}{k+2}} > p^{3+\frac{1}{k+2}}.$$

Applying Lemma 3.3 it follows that for almost all primes every integer λ can be represented as

$$\sum_{i=1}^{k} L_m F_{2n_i - 1} + \sum_{j=1}^{k} (F_{2\ell_j} + F_{2\ell'_j}) \equiv \lambda \pmod p, \tag{3.12}$$

where

$$\frac{1}{2} N^{\frac{7}{k+2}} < m \leq N^{\frac{7}{k+2}},\ \ 1 \leq n_i \leq N^{\frac{1}{k+2}},\ \ 1 \leq \ell_j, \ell'_j \leq N^{\frac{1}{k+2}},\ \ (1 \leq i, j \leq k).$$

We recall the identity

$$L_u F_v = F_{u+v} + (-1)^{v+1} F_{u-v}.$$

Thus, for every $1 \leq i \leq k$ in (3.12) we get

$$L_m F_{2n_i - 1} = F_{m+2n_i-1} + F_{m-2n_i+1}.$$

taking $s = 4k$ (that is, $s = 4([8/\varepsilon] - 1)$), we conclude that for almost all primes every residue class λ has a representation in the form

$$F_{n_1} + \cdots + F_{n_s} \equiv \lambda \pmod p,$$

for some integers

$$1 \leq n_1, \ldots, n_s \leq N^{\varepsilon}. \quad \square$$

3.4. Proof of Theorem 2.4. Observe that the congruence

$$F_n \equiv F_{n'} \pmod p; \qquad 1 \leq n, n' \leq N^{\gamma},$$

has at least N^{γ} solutions. Therefore

$$N^{\gamma} \leq \frac{1}{p} \sum_{x=0}^{p-1} \left| \sum_{n \leq N^{\gamma}} e^{2\pi i \frac{x}{p} F_n} \right|^2.$$

From Hölder's inequality we obtain

$$\begin{aligned} N^{\gamma} &\leq \frac{1}{p}\sum_{x=0}^{p-1}\left|\sum_{n\leq N^{\gamma}} e^{2\pi i \frac{x}{p}F_n}\right|^{2/3}\left|\sum_{n\leq N^{\gamma}} e^{2\pi i \frac{x}{p}F_n}\right|^{4/3} \\ &\leq \frac{1}{p}\left(\sum_{x=0}^{p-1}\left|\sum_{n\leq N^{\gamma}} e^{2\pi i \frac{x}{p}F_n}\right|\right)^{2/3}\left(\sum_{x=0}^{p-1}\left|\sum_{n\leq N^{\gamma}} e^{2\pi i \frac{x}{p}F_n}\right|^4\right)^{1/3} \\ &\leq T_p^{1/3}\left(\frac{1}{p}\sum_{x=0}^{p-1}\left|\sum_{n\leq N^{\gamma}} e^{2\pi i \frac{x}{p}F_n}\right|\right)^{2/3}, \end{aligned} \tag{3.13}$$

where T_p denotes the number of solutions of the congruence

$$F_{n_1}+F_{n_2}\equiv F_{m_1}+F_{m_2} \pmod p; \quad 1\leq n_1,n_2,m_1,m_2\leq N^{\gamma}.$$

Let

$$\mathcal{X}=\{F_{n_1}+F_{n_2} \;:\; 1\leq n_1,n_2\leq N^{\gamma}\}.$$

Then $|\mathcal{X} \pmod p| \asymp N^{2\gamma}$. Applying Lemma 3.5 with $M=N^{\gamma}$ and $\Delta = N^{(1-3\gamma)/2}$ we get, for $\pi(N)(1+o(1))$ primes $p\leq N$, the estimate

$$T_p \ll N^{2\gamma}\left(1+N^{-(1-3\gamma)/2}\right).$$

Combining this estimation with relation (3.13) we conclude that there is a positive constant $c_1(\gamma)$ such that

$$\frac{1}{p}\sum_{x=0}^{p-1}\left|\sum_{n\leq N^{\gamma}} e^{2\pi i \frac{x}{p}F_n}\right| \geq c_1(\gamma)N^{\gamma/2}.$$

Finally, to obtain an upper bound of the same order, using the Cauchy-Schwarz inequality we have

$$\left(\frac{1}{p}\sum_{x=0}^{p-1}\left|\sum_{n\leq N^{\gamma}} e^{2\pi i \frac{x}{p}F_n}\right|\right)^2 \leq \frac{1}{p}\sum_{x=0}^{p-1}\left|\sum_{n\leq N^{\gamma}} e^{2\pi i \frac{x}{p}F_n}\right|^2, \tag{3.14}$$

where the right term is, indeed, the number of solutions of the congruence

$$F_n\equiv F_m \pmod p; \qquad 1\leq n,m\leq N^{\gamma}.$$

Applying again Lemma 3.5 with $M=N^{\gamma}$ and $\Delta = N^{(1-2\gamma)/2}$, we obtain, for $\pi(N)(1+o(1))$ primes $p\leq N$, the estimate

$$\frac{1}{p}\sum_{x=0}^{p-1}\left|\sum_{n\leq N^{\gamma}} e^{2\pi i \frac{x}{p}F_n}\right|^2 \leq N^{\gamma}\left(1+N^{-(1-2\gamma)/2}\right)\leq c_2(\gamma)N^{\gamma},$$

for some positive constant $c_2(\gamma)$. Combining this with (3.14) and taking the square root we conclude the proof. □

Acknowledgement

The author was supported by Grant UAM-A 2232508.

References

[1] W. D. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, *Exponential sums over Mersenne numbers*. Compos. Math. **140** (2004), no. 1, 15–30.
[2] W. D. Banks, M. Z. Garaev, F. Luca and I. E. Shparlinski, *Uniform distribution of fractional parts related to pseudoprimes*. Canad. J. Math. **61** (2009), no. 3, 481–502.
[3] J. Bourgain, *Estimates on exponential sums related to the Diffie–Hellman distributions*. Geom. Funct. Anal. **15** (2005), no. 1, 1–34.
[4] E. Croot, *Sums of the form $1/x_1^k + \cdots + 1/x_n^k$ modulo a prime*. Integers **4** (2004), A20, 6 pp.
[5] C. Elsholtz, *The distribution of sequences in residue classes*. Proc. Amer. Math. Soc. **130** (2002), no. 8, 2247–2250.
[6] P. Erdős and M. R. Murty, *On the order of $a \pmod p$*. Proc. 5th Canadian Number Theory Association Conf., Amer. Math. Soc., Providence, RI, 1999, 87–97.
[7] M. Z. Garaev, *Upper bounds for the number of solutions of a diophantine equation*. Trans. Amer. Math. Soc. **357** (2005), no. 6, 2527–2534.
[8] M. Z. Garaev, *The large sieve inequality for the exponential sequence $\lambda^{[O(n^{15/14+o(1)})]}$ modulo primes*. Canad. J. Math. **61** (2009), no. 2, 336–350.
[9] M. Z. Garaev and Ka–Lam Kueh, *Distribution of special sequences modulo a large prime*. Int. J. Math. Math. Sci. **50** (2003), 3189–3194.
[10] M. Z. Garaev and I. E. Shparlinski, *The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes*. Int. Math. Res. Not. **39** (2005), no. 39, 2391–2408.
[11] V. C. García, F. Luca and V. J. Mejía, *On sums of Fibonacci numbers modulo p*. Bull. Aust. Math. Soc. **83** (2011), 413–419.
[12] A. A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erdős–Graham problem*. Mat. Zametki. **79** (2006), no. 3, 384–395; English transl., Math. Notes. **79** (2006). no. 3–4, 356–365.
[13] B. Green and S. V. Konyagin, *On the Littlewood problem modulo a prime*. Canad. J. Math. **61** (2009), no. 1, 141–164.
[14] A. A. Karatsuba, *An estimate of the L_1-norm of an expontential sum*. Math. Notes **64** (1998), no. 3, 401–404.
[15] S. V. Konyagin, *On a problem of Littlewood*. Izv. Acad. Nauk SSSR Ser. Mat. [Math. USSR-Izv.] **45** (1981), no. 2, 243–265.
[16] S. V. Konyagin, *An estimate of the L_1-norm of an exponential sum*. The Theory of Approximations of Functions and Operators. Abstracts of Papers of the International Conference Dedicated to Stechkin's 80th Anniversary [in Russian]. Ekaterinburg, 2000, pp. 88-89.
[17] O. C. McGehee, L. Pigno and B. Smith, *Hardy's inequality and the L^1 norm of exponential sums*. Ann. of Math. (2) **113** (1981), no. 3, 613–618.
[18] F. Pappalardi, *On the order of finitely generated subgroups of $\mathbb{Q}^* \pmod p$ and divisors of $p-1$*. J. Number Theory **57** (1996), 207–222.
[19] A. Sárközy, *On sums and products of residues modulo p*. Acta Arith. **118** (2005), no. 4, 403–409.
[20] T. Schoen and I. Shkredov, *Additive properties of multiplicative subgroups of $\mathbb{F}_p$*. Quart. J. Math. **63** (2012), no. 3, 713–722.
[21] I. E. Shplarlinski, *On a question of Erdős and Graham*. Arch. Math. **78** (2002), 445–448.

Víctor Cuauhtemoc García
Departamento de Ciencias Básicas
Universidad Autónoma Metropolitana–Azcapotzalco
C.P. 02200, México D.F., México
E-mail: vc.garci@gmail.com