Functiones et Approximatio
60.2 (2019), 143–153
doi: 10.7169/facm/1697

A NOTE ON FIBONOMIAL COEFFICIENTS

Víctor C. García, Florian Luca

Abstract: We show that for most primes p, the set of Fibonomials forms an additive basis of order 8 for the group of residue classes modulo p.

Keywords: Fibonacci numbers, sum-product phenomenon.

1. Introduction

Let $\mathbf{F} = \{F_n\}_{n\geqslant 1}$ be the sequence of Fibonacci numbers given by $F_0 = 0,\ F_1 = 1$ and

$$F_{n+2} = F_{n+1} + F_n, \qquad \text{for all} \quad n \geqslant 0. \tag{1}$$

The nth Fibonacci number F_n is also given by Binet's formula

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad \text{where} \quad (\alpha, \beta) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right) \tag{2}$$

are the roots of the characteristic polynomial

$$f(x) = x^2 - x - 1. \tag{3}$$

For $n \geqslant 1$, we put:

$$[n]_F = \prod_{k=1}^{n} F_k.$$

We also put $[0]_F = 1$ by convention. For $n \geqslant k \geqslant 0$, the Fibonomial coefficient is given by

$$\binom{n}{k}_F = \frac{[n]_F}{[k]_F[n-k]_F} = \frac{F_{n-k+1}\cdots F_n}{F_1 F_2 \cdots F_k}.$$

2010 Mathematics Subject Classification: primary: 11B39, 11B50

It is known that $\binom{n}{k}_F$ is an integer (see [7] for a more general result). By convention, we extend the definition of the Fibonomial coefficient and put

$$\binom{n}{k}_F = 0, \qquad \text{for} \;\; n < k.$$

Clearly, $\binom{n}{k}_F = \binom{n}{n-k}_F$. In [8], it was shown that

$$\binom{n}{k}_F \neq \binom{m}{l}_F, \qquad \text{when} \;\; 1 \leqslant k \leqslant n/2 \;\; \text{and} \;\; 1 \leqslant l \leqslant m/2.$$

That is, in the Pascal like triangle for the Fibonomials $\{\binom{n}{k}_F : n \geqslant k \geqslant 0\}$, the entries in the left–half of it, aside from the first edge of 1's, consist of distinct integers. This is not true for the classical Pascal triangle formed of binomial coefficients in which some values appear multiple times as a binomial coefficient such as in

$$\binom{78}{2} = \binom{15}{5} = \binom{16}{6} = 3003,$$

or

$$\binom{F_{2i+2}F_{2i+3}}{F_{2i}F_{2i+3}} = \binom{F_{2i+2}F_{2i+3}-1}{F_{2i}F_{2i+3}+1} \qquad \text{for} \;\; i = 1, 2, \ldots .$$

Put

$$\mathcal{F} = \left\{ \binom{n}{k}_F : 1 \leqslant k \leqslant n/2 \right\} = \{f_1, f_2, \ldots\},$$

where $1 = f_1 < f_2 < \cdots$ are all elements of $\mathcal{F}$ arranged increasingly. The first few elements of $\mathcal{F}$ are

$$\mathcal{F} = \{1, 2, 3, 5, 6, 8, 13, 15, 21, 34, 40, 55, 60, 89, 104, \ldots\}.$$

In [8], it was shown that $f_{n+1} - f_n \gg \sqrt{\log f_n}$ holds for all n and determined all n such that $f_{n+1} - f_n \leqslant 100$.

In this paper we look at Fibonomials modulo prime numbers. Recall that given an abelian group $(A, +)$ and a subset B of elements of it, we say that B is a basis of order k for A if for every $a \in A$ there exist $b_1, \ldots, b_k$ such that

$$b_1 + \cdots + b_k = a.$$

Showing that such a k exists for given A and B and finding the optimal (smallest one) is usually refereed to as Waring's problem. Our main result is the following.

Theorem 1. *For almost all primes p, each residue class λ modulo p can be written as*

$$\binom{u_1}{v_1}_F + \cdots + \binom{u_8}{v_8}_F \equiv \lambda \pmod{p},$$

for positive integers $u_1, v_1 \ldots, u_8, v_8 \ll p^{3/2} \log^2 p$.

In [3], it was shown that for most p, the set of Fibonacci numbers form an additive basis of order 32. The number 32 was improved to 16 in [4]. See also [2] for results on the Waring problem modulo p with various numbers appearing in combinatorics such as binomial coefficients and Apéry numbers.

2. Auxiliary lemmas

The following result from arithmetic combinatorics is due to Glibichuk [5].

Lemma 2. *Let A, B subsets of $\mathbb{F}_p$ with $|A||B| > 2p$. Then*

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

For a positive integer m we let $z(m)$ denotes the order of appearance of m in the sequence of Fibonacci numbers, namely

$$z(m) := \min\{k \geqslant 1 \colon m \mid F_k\}.$$

This exists for every positive integer m.

The following lemma is a consequence of a Theorem due to Hu and Sun [6].

Lemma 3. *Let m, n, s, t be integers with $0 \leqslant s, t < z(p)/2$. Then*

$$\binom{2mz(p)+2s}{2nz(p)+2t}_F \equiv \binom{2m}{2n}\binom{2s}{2t}_F \pmod{p}. \tag{4}$$

3. Strategy of the proof

In this section, we indicate the strategy of the proof as a sequence of lemmas. In fact, by the end of this section we would have proved Theorem 1 modulo the proofs of the lemmas which are deferred to the next section. We need only a lower bound on $z(p)$ valid for most primes p. This can be deduced from [3, Section 2].

Lemma 4. *For every constant $\rho_0 \in (0,1)$ there are $\pi(x)(1+o(1))$ primes $p \leqslant x$ such that*

$$z(p) \geqslant p^{1/2} \exp\left(\log^{\rho_0} p\right). \tag{5}$$

By [3, Lemma 2.2], the function indicated as $o(1)$ in the statement of Lemma 4 can be taken to be $O_{\rho_0}((\log x)^{-\delta(1-\rho_0)}(\log\log x)^{3/2})$, where

$$\delta = 1 - \frac{1+\log\log 2}{\log 2}.$$

From now on, we can work with primes p satisfying inequality (5) with $\rho_0 = 1/2$.

We next need information on the value set of binomial coefficients modulo p. In the recent paper [1], Garaev and Hernández studied ratios of two factorials proving that for any integer N in the range $p^{1/2+\varepsilon} < N \leqslant 0.1p$ we have

$$\#\left\{\frac{m!}{n!} \pmod{p} \colon 1 \leqslant m, n \leqslant N\right\} \gg_\varepsilon N \log(p/N).$$

Following [1], we give a lower bound on the set of values of binomial coefficients modulo p and we also improve slightly the range of the parameter N in the above estimate by making the exponent ε of the lower bound for N explicit.

Lemma 5. *Let N be an integer such that $e^{200}p^{1/2}\log^2 p < N < e^{-200}p$. Then the inequality*

$$\#\left\{\binom{m}{n} \pmod p \colon 1 \leqslant n \leqslant m \leqslant N\right\}$$
$$> c_0 N \min\left\{\log\left(\frac{p}{N}\right), \log\left(\frac{N}{p^{1/2}\log^2 p}\right)\right\}.$$

holds with some absolute constant $c_0 > 0$.

We include the proof of the above Lemma 5 in Section 4.1 for completeness. Taking $N = \lfloor e^{201}p^{1/2}(\log^2 p)\rfloor$ in Lemma 5 we have the following corollary.

Corollary 6. *For all large enough primes p we have*

$$\#\left\{\binom{2m}{2n} \pmod p \colon 1 \leqslant n \leqslant m \leqslant e^{201}p^{1/2}(\log p)^2\right\} \gg p^{1/2}\log^2 p.$$

We also obtain a lower bound for the value set of a certain subset of the Fibonomial coefficients modulo p.

Lemma 7. *Let N, t be positive integers with $2t \leqslant N < z(p)/4$. Then the inequality*

$$\#\left\{\binom{s}{t}_F \pmod p \colon 1 \leqslant s \leqslant N - t\right\} \geqslant c_1 \frac{N}{t},$$

holds with some positive constant $c_1 > 0$.

A similar argument as the one used in the proof of Lemma 7 shows that the conclusion of Lemma 7 remains valid even if we impose that s, t have the same parity (maybe with a different value of the constant c_1). Applying Lemma 4 with $N = 4\lfloor p^{1/2}\exp(\log^{1/2} p)\rfloor$, we get the following corollary.

Corollary 8. *Let $t_0 = \lfloor \exp(\log^{1/2} p)\rfloor$. For all primes $p \leqslant x$ except $o(\pi(x))$ of them as $x \to \infty$, the following inequality holds*

$$\#\left\{\binom{2s}{2t_0}_F \pmod p \colon 1 \leqslant s \leqslant p^{1/2}\exp(\log^{1/2} p)\right\} \gg p^{1/2}.$$

Applying now Lemma 2 with

$$A = \left\{\binom{2m}{2n} \pmod p \colon 1 \leqslant n \leqslant m \leqslant e^{201}p^{1/2}(\log p)^2\right\},$$
$$B = \left\{\binom{2s}{2t_0}_F \pmod p \colon 1 \leqslant s \leqslant p^{1/2}\exp(\log^{1/2} p)\right\},$$

it follows that for almost all $p \leqslant x$ except $o(\pi(x))$ of them as $x \to \infty$, we have $|A||B| \gg p\log^2 p > 2p$. Thus, every residue class modulo p can be written as

$$\binom{2m_1}{2n_1}\binom{2s_1}{2t_0}_F + \cdots + \binom{2m_8}{2n_8}\binom{2s_8}{2t_0}_F \pmod p,$$

where $m_i, n_i \ll p^{1/2}\log^2 p$ and $s_i \ll p^{1/2}\exp(\log^{1/2} p)$ for all $i = 1, 2, \ldots, 8$. Finally, from Lemma 3, we have

$$\binom{2m_i}{2n_i}\binom{2s_i}{2t_0}_F \equiv \binom{2m_i z(p) + 2s_i}{2n_i z(p) + 2t_0}_F \pmod p,$$

for all $i = 1, 2, \ldots, 8$. Theorem 1 now follows with $u_i = 2m_i z(p) + 2s_i$ and $v_i = 2n_i z(p) + 2t_0$ for $i = 1, 2, \ldots, 8$.

It remains to prove lemmas 5 and 7.

4. Proofs of the lemmas

4.1. Proof of Lemma 5

For $e^{200}p^{1/2}\log^2 p < N < e^{-200}p$, let

$$K = \min\left\{\left(\frac{p}{N}\right)^{1/3}, \left(\frac{N}{p^{1/2}\log^2 p}\right)^{1/4}\right\}.$$

For any $2 \leqslant k \leqslant K$ set

$$B_k = \left\{\binom{x+k}{k} \pmod p \colon 1 \leqslant x \leqslant N-k\right\}.$$

Given $\lambda \in B_k$, let $J_k(\lambda)$ denotes the number of solutions of the congruence

$$\binom{k+x}{k} \equiv \lambda \pmod p, \qquad 1 \leqslant x \leqslant N-k.$$

It is clear that

$$\sum_{\lambda \in B_k} J_k(\lambda) = N - k,$$

By the Cauchy-Schwartz inequality, we get

$$(N-k)^2 \leqslant \#B_k \sum_{\lambda \in B_k} J_k^2(\lambda).$$

Note that the last summatory is the number of solutions of the congruence

$$\binom{k+x}{k} \equiv \binom{k+y}{k} \pmod p, \qquad 0 \leqslant x, y \leqslant N-k, \tag{6}$$

which we denote it by J_k. Therefore,

$$\#B_k \geqslant \frac{(N-k)^2}{J_k}. \tag{7}$$

Clearly, congruence (6) is equivalent to

$$\prod_{i=1}^{k}(x+i) \equiv \prod_{j=1}^{k}(y+j) \pmod p, \qquad 1 \leqslant x, y \leqslant N-k.$$

The polynomial $\prod_{i=1}^{k}(x+i) \in \mathbb{F}_p[x]$ is monic of degree k. Hence, for each $1 \leqslant y \leqslant N-k$ fixed, the above congruence has at most k solutions in the unknown x. Thus, $J_k \leqslant k(N-k)$ and in view of (7), we get

$$\#B_k \geqslant \frac{N-k}{k}. \tag{8}$$

In order to estimate the value set of

$$B(N) := \left\{\binom{m}{n} \pmod p \colon 1 \leqslant n \leqslant m \leqslant N\right\},$$

we note that

$$B(N) \supseteq \bigcup_{k=1}^{K} B_k = B_1 \cup \bigcup_{k=2}^{K}(B_k \backslash (B_1 \cup \cdots \cup B_{k-1})),$$

where B_1, and $(B_k \backslash (B_1 \cup \cdots \cup B_{k-1}))$ are pairwise disjoint sets for $2 \leqslant k \leqslant K$. Then,

$$\begin{aligned}\#B(N) \geqslant \#B_1 + \sum_{k=2}^{K} \#\left(B_k \backslash (B_1 \cup \cdots \cup B_{k-1})\right) \geqslant \\ \geqslant \#B_1 + \sum_{k=2}^{K}\left(\#B_k - (\#(B_1 \cap B_k) + \cdots + \#(B_{k-1} \cap B_k))\right).\end{aligned} \tag{9}$$

For any $\ell \leqslant k-1$, we have $|B_\ell \cap B_k| \leqslant J_{k,\ell}$, where $J_{k,\ell}$ counts the number of solutions of the congruence

$$\binom{k+x}{k} \equiv \binom{\ell+y}{\ell} \pmod p, \quad 1 \leqslant x \leqslant N-k, \quad 1 \leqslant y \leqslant N-\ell.$$

The above congruence is equivalent to

$$\prod_{i=1}^{k}(x+i) \equiv (k-\ell)! \prod_{j=1}^{\ell}(y+j) \pmod p, \qquad 1 \leqslant x \leqslant N-k,\ 1 \leqslant y \leqslant N-\ell.$$

Note that $(k-\ell)! \not\equiv 0 \pmod p$ is a constant for $k > \ell$ fixed. The polynomial

$$P_{k,\ell}(X,Y) = \prod_{i=1}^{k}(X+i) - (k-\ell)! \prod_{j=1}^{\ell}(Y+j)$$

in $\mathbb{F}_p[X,Y]$ has degree k. Clearly,

$$J_{k,\ell} \leqslant \sum_{\substack{1\leqslant x\leqslant N-k\\ 1\leqslant y\leqslant N-\ell\\ P_{k,\ell}(x,y)=0}} 1.$$

Completing to the entire range for $x,\ y$, we have

$$J_{k,\ell} \leqslant \sum_{\substack{1\leqslant x\leqslant N-k\\ 1\leqslant y\leqslant N-\ell\\ P_{k,\ell}(x,y)=0}} 1 = \frac{1}{p^2}\sum_{a,b\in\mathbb{F}_p}\sum_{x,y}\sum_{\substack{u,v\in\mathbb{F}_p\\ P_{k,\ell}(u,v)=0}} \exp\left(\tfrac{a(u-x)+b(v-y)}{p}\right).$$

Separating the contribution of the term $a=b=0$, we get

$$\begin{aligned} J_{k,\ell} \leqslant \frac{N^2}{p^2} &\sum_{\substack{u,v\in\mathbb{F}_p\\ P_{k,\ell}(u,v)=0}} 1 \\ &+ \frac{1}{p^2}\sum_{\substack{a,b\in\mathbb{F}_p\\ (a,b)\neq(0,0)}} \left|\sum_{x=1}^{N-k}\exp\left(\tfrac{ax}{p}\right)\right|\left|\sum_{y=1}^{N-\ell}\exp\left(\tfrac{by}{p}\right)\right|\left|\sum_{\substack{u,v\in\mathbb{F}_p\\ P_{k,\ell}(u,v)=0}}\exp\left(\tfrac{au+bv}{p}\right)\right|. \end{aligned} \tag{10}$$

Note that

$$\sum_{\substack{u,v\in\mathbb{F}_p\\ P_{k,\ell}(u,v)=0}} 1 = \#\{(u,v)\in\mathbb{F}_p : P_{k,\ell}(u,v)=0\}.$$

Thus,

$$\sum_{\substack{u,v\in\mathbb{F}_p\\ P_{k,\ell}(u,v)=0}} 1 \leqslant kp. \tag{11}$$

We also recall the well–known bound

$$\sum_{a\in\mathbb{F}_p}\left|\sum_{x\leqslant M}\exp\left(\tfrac{ax}{p}\right)\right| \leqslant p\log p, \qquad \text{for any}\ \ 1\leqslant M\leqslant p/2. \tag{12}$$

Combining the last two bounds (11) and (13) with (10), we get

$$J_{k,\ell} \leqslant \frac{kN^2}{p} + (\log p)^2 \max_{(a,b)\neq(0,0)}\left\{\left|\sum_{\substack{u,v\in\mathbb{F}_p\\ P_{k,\ell}(u,v)=0}}\exp\left(\tfrac{au+bv}{p}\right)\right|\right\}. \tag{13}$$

We next equire the following estimate (see [1, Lemma1]):

$$\left| \sum_{\substack{u,v\in\mathbb{F}_p \\ P_{k,\ell}(u,v)=0}} \exp\left(\frac{au+bv}{p}\right) \right| \leqslant 2k^2p^{1/2}. \tag{14}$$

Inserting (14) into (13), we obtain

$$J_{k,\ell} \leqslant \frac{kN^2}{p} + 2k^2(\log p)^2p^{1/2}. \tag{15}$$

Summing up (15) over $1 \leqslant \ell \leqslant k-1$ and $1 \leqslant k \leqslant K$, we end up with

$$\begin{aligned}
\sum_{k=1}^{K}\sum_{\ell=1}^{k-1} \#(B_\ell \cap B_k) &\leqslant \sum_{k=1}^{K}\sum_{\ell=1}^{k-1} J_{k,\ell} \leqslant \sum_{k=1}^{K}\left(\frac{k^2N^2}{p} + 2k^3(\log p)^2p^{1/2}\right) \\
&\leqslant \frac{K^3N^2}{p} + K^4(\log p)^2p^{1/2} \\
&\leqslant 2N\left(\left(\frac{K}{(p/N)^{1/3}}\right)^3 + \left(\frac{K}{(N/(p^{1/2}\log^2 p))^{1/4}}\right)^4\right) \\
&\leqslant 10N.
\end{aligned}$$

Therefore, in view of (8) and (9), we have

$$\begin{aligned}
\#B(N) &\geqslant \sum_{k=1}^{K} \#B_k - \sum_{k=2}^{K}(\#(B_1\cap B_k) + \cdots + \#(B_{k-1}\cap B_k)) \\
&\geqslant \frac{1}{2}N\log K - 10N \geqslant \frac{1}{4}N\log K.
\end{aligned}$$

The lemma follows by the choise of K.

4.2. Proof of Lemma 7

Let $t \geqslant 2$ be an integer. It is clear that

$$\left\{\binom{s}{t}_F \pmod p \colon t \leqslant s \leqslant N\right\} \supseteq \left\{\binom{x+t}{t}_F \pmod p \colon 1 \leqslant x \leqslant N-t\right\}.$$

Let

$$\mathcal{B}_t = \left\{\binom{x+t}{t}_F \pmod p \colon 1 \leqslant x \leqslant N-t\right\}.$$

Given $\lambda \in \mathcal{B}_t$, we denote by $I(\lambda)$ the number of solutions of the congruence

$$\binom{t+x}{t}_F \equiv \lambda \pmod p, \qquad 1 \leqslant x \leqslant N-t.$$

Clearly,

$$\sum_{\lambda\in\mathcal{B}_t} I(\lambda) = N - t,$$

and by the Cauchy-Schwartz inequality, we get

$$(N-t)^2 \leqslant \#\mathcal{B}_t \sum_{\lambda\in\mathcal{B}_t} I^2(\lambda).$$

Note that the last summatory is the number of solutions of the congruence

$$\binom{t+x}{t}_F \equiv \binom{t+y}{t}_F \pmod p, \qquad 1 \leqslant x, y \leqslant N-t, \tag{16}$$

which is denoted by $I_t(N)$. Therefore,

$$\#\mathcal{B}_t \geqslant \frac{(N-t)^2}{I_t(N)}. \tag{17}$$

Clearly, congruence (16) is equivalent to

$$\prod_{i=1}^{t} F_{x+i} \equiv \prod_{j=1}^{t} F_{y+j} \pmod p, \qquad 1 \leqslant x, y \leqslant N-t. \tag{18}$$

We now use Binet's formula (2). Here, we assume that $p > 5$ and α, β are the roots of the polynomial (3) modulo p. In particular, they belong to $\mathbb{F}_p$ if $p \equiv 1, 4 \pmod 5$ and are quadratic over $\mathbb{F}_p$ if $p \equiv 2, 3 \pmod 5$. From now on we work over $\mathbb{F}_q$, where $q = p,\ p^2$ according to whether $p \equiv 1, 4 \pmod 5$ or $2, 3 \pmod 5$, so that $\alpha, \beta, \sqrt{5}$ are all in $\mathbb{F}_q$. Thus, $\mathbb{F}_q = \mathbb{F}_p(\sqrt{5})$. We have

$$\prod_{i=1}^{t} F_{x+i} = \frac{1}{5^{t/2}} \prod_{i=1}^{t} (\alpha^{x+i} - \beta^{x+i}) = \frac{1}{5^{t/2}\alpha^{tx}} \prod_{i=1}^{t} (\alpha^{2x}\alpha^i - (-1)^x\beta^i).$$

Analogously

$$\prod_{j=1}^{t} F_{y+j} = \frac{1}{5^{t/2}\alpha^{ty}} \prod_{j=1}^{t} (\alpha^{2y}\alpha^j - (-1)^y\beta^j).$$

Therefore,

$$\begin{aligned}\prod_{i=1}^{t} F_{x+i} - \prod_{j=1}^{t} F_{y+j} \\ = \frac{1}{5^{t/2}\alpha^{(x+y)t}} \left(\alpha^{ty} \prod_{i=1}^{t} (\alpha^{2x}\alpha^i - (-1)^x\beta^i) - \alpha^{tx} \prod_{j=1}^{t} (\alpha^{2y}\alpha^j - (-1)^y\beta^j)\right).\end{aligned}$$

For $\delta, \sigma \in \{0,1\}$, define the polynomials $P_{\delta\sigma}(X,Y) \in \mathbb{F}_q[X,Y]$ by

$$P_{\delta,\sigma}(X,Y) = Y^t \prod_{i=1}^{t}(X^2\alpha^i - (-1)^\delta \beta^i) - X^t \prod_{j=1}^{t}(Y^2\alpha^j - (-1)^\sigma \beta^j).$$

Such polynomials have total degree $3t$ and degree $2t$ in each one of the two indeterminates X and Y. For any δ, σ the monomials of $P_{\delta,\sigma}(X,Y)$ with highest degree are Y^tX^{2t} and X^tY^{2t} with nonzero leading coefficients $\alpha^{t(t+1)/2}/5^{t/2}$, $-\alpha^{t(t+1)/2}/5^{t/2}$, respectively.

Denote by $I_t(N,\sqrt{5})$ the sum of the number of solutions of the equations

$$P_{\delta,\sigma}(X,Y) = 0, \qquad \delta, \sigma \in \{0,1\}, \tag{19}$$

subject to the conditions $(X,Y) \in \mathbb{F}_q \times \mathbb{F}_q$, $X = \alpha^x$, $Y = \alpha^y$ and $1 \leqslant x, y \leqslant N - t$.

Given (x,y) a solution for (18) it is clear that (α^x, α^y) is a solution of (19) for some polynomial $P_{\delta,\sigma}(X,Y)$ with $\delta \equiv x \pmod 2$ and $\sigma \equiv y \pmod 2$. Let (x_1,y_1) and (x_2,y_2) be solutions for (18) such that $(\alpha^{x_1}, \alpha^{y_1}) = (\alpha^{x_2}, \alpha^{y_2})$. Hence, $\alpha^{2(x_1-x_2)} = 1$ and $\alpha^{2(y_1-y_2)} = 1$. This implies that $\beta^{2(x_1-x_2)} = 1$ and $\beta^{2(y_1-y_2)} = 1$. Thus,

$$F_{2(x_1-x_2)} \equiv 0 \pmod p, \qquad \text{and} \qquad F_{2(y_1-y_2)} \equiv 0 \pmod p.$$

Since $p \mid F_\ell$ if and only if $z(p) \mid \ell$, we get

$$2(x_1 - x_2) \equiv 0 \pmod{z(p)}, \qquad 2(y_1 - y_2) \equiv 0 \pmod{z(p)},$$

Recalling that $0 \leqslant 2|x_1 - x_2|, 2|y_1 - y_2| \leqslant 2N$ and $2N \leqslant z(p)/2$, it follows that $x_1 - x_2 \equiv 0 \pmod p$ and $y_1 - y_2 \equiv 0 \pmod p$. Thus, $I_t(N) \leqslant I_t(N,\sqrt{5})$.

Moreover, fixing $1 \leqslant y_0 \leqslant N - k$ and $\sigma_0 \equiv y_0 \pmod p$, for each δ the number of solutions of the equation

$$P_{\delta,\sigma_0}(\alpha^x, \alpha^{y_0}) = 0, \qquad \text{with} \;\; 1 \leqslant x \leqslant N - t, \; x \equiv \delta \pmod 2,$$

is at most $2t$, which is the degree of $P_{\delta,\sigma}(X, \alpha^{y_0})$ as a polynomial in $\mathbb{F}_q[X]$. Then $I_t(N) \leqslant I_t(N,\sqrt{5}) \leqslant 4t(N-t)$, and combining this with (17), we obtain

$$\#\mathcal{B}_t \geqslant \frac{(N-t)}{4t} \geqslant \frac{N}{8t},$$

which concludes the proof of the lemma.

Acknowledgements. This work was done while F. L. visited the Max Planck Institute for Mathematics in Bonn, Germany between January and July 2017. In addition, F. L. was supported in part by grants CPRR160325161141 from the NRF of South Africa, the Focus Area Number Theory Grant from CoEMaSS, Wits, and by Grant no. 17-02804S of the Czech Granting Agency. V. G. was supported by Project CB005-16 from UAM-A.

References

[1] M. Z. Garaev and J. Hernández, *A note on $n!$ modulo p*, Monatsh. Math. **182** (2017), 23–31.
[2] M. Z. Garaev, F. Luca and I. Shparlinski, *Catalan and Apéry numbers in residue classes*, J. Combin. Theory. **113** (2006), 851–865.
[3] V. C. García, F. Luca and J. Mejía, *On sums of Fibonacci numbers modulo p*, Bull. Aust. Math. Soc. **83** (2011), 413–419.
[4] V. C. García, *On the distribution of sparse sequences in prime fields and applications*, J. Théor. Nombres Bordeaux **25** (2013), 317–329.
[5] A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime an the Erdős–Graham problem*, Mat. Zametki **79** (2006), 384–395; English transl., Math. Notes **79** (2006), 356–365.
[6] Hong Hu and Zhi-Wei Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. **129** (2001), 3471–3478.
[7] D. E. Knuth and H. S. Wilf, *The power of a prime that divides a generalized binomial coefficient*, J. reine angew. Math. **396** (1989), 212–219.
[8] F. Luca, D. Marques and P. Stănică, *On the spacings between C-nomial coefficients*, J. Number Theory **130** (2010), 82–100.

Addresses: Víctor C. García: Departamento de Ciencias Básicas, Universidad Autónoma Metropolitana–Azcapotzalco, C.P. 02200, México D.F., México;
Florian Luca: School of Mathematics, University of the Witwatersrand, Private Bag X3, Wits 2050, South Africa; Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany; Department of Mathematics, Faculty of Sciences, University of Ostrava, 30 Dubna 22, 701 03 Ostrava 1, Czech Republic.

E-mail: vcgh@correo.azc.uam.mx, florian.luca@wits.ac.za

Received: 9 August 2017; **revised:** 26 September 2018