ON INTEGER SEQUENCES IN PRODUCT SETS

SAI TEJA SOMU

Abstract. Let B be a finite set of natural numbers or complex numbers. Product set corresponding to B is defined by $B.B := \{ab : a, b \in B\}$. In this paper we give an upper bound for longest length of consecutive terms of a polynomial sequence present in a product set accurate up to a positive constant. We give a sharp bound on the maximum number of Fibonacci numbers present in a product set when B is a set of natural numbers and a bound which is accurate up to a positive constant when B is a set of complex numbers.

1. Introduction

In [4] and [5] Zhelezov has proved that if B is a set of natural numbers then the product set corresponding to B cannot contain long arithmetic progressions. In [4] it was shown that the longest length of arithmetic progression is at most $O(|B| \log |B|)$. We try to generalize this result for polynomial sequences. Let $P(x) \in \mathbb{Z}[x]$ be a non constant polynomial with positive leading coefficient. Let R be the longest length of consecutive terms of the polynomial sequence contained in the product set $B.B$, that is,

$$R = max\{n : \text{there exists an } x \in \mathbb{N} \text{ such that } \{P(x+1), \cdots, P(x+n)\} \subset B.B\}.$$

We prove that R cannot be large for a given non constant polynomial $P(x)$. In section 3 we consider the question of determining maximum number of Fibonacci and Lucas sequence terms in a product set. Let $A \times B$ denote the cartesian product of sets A and B.As in [4] we define an auxiliary bipartite graph $G(A, B.B)$ and auxiliary graph $G'(A, B.B)$ which are constructed for any sets A and B whenever $A \subset B.B$. The vertex set of $G(A, B.B)$ is a union of two isomorphic copies of B namely $B_1 = B \times \{1\}$ and $B_2 = B \times \{2\}$ and vertex set of $G'(A, B.B)$ is one isomorphic copy of B namely $B_1 = B \times \{1\}$. For each $a \in A$we pick a unique representation $a = b_1 b_2$ where $b_1, b_2 \in B$ and place an edge joining $(b_1, 1)$, $(b_2, 2)$ in $G(A, B.B)$ and place an edge joining $(b_1, 1)$, $(b_2, 1)$ in $G'(A, B.B)$. Note that the number of vertices in $G(A, B.B)$ is $2|B|$ where as number of vertices in $G'(A, B.B)$ is $|B|$. Number of edges in both $G(A, B.B)$ and $G'(A, B.B)$ is $|A|$. Observe that $G'(A, B.B)$ can have self loops and $G(A, B.B)$ cannot have self loops and that $G(A, B.B)$ is necessarily a bipartite graph where as $G'(A, B.B)$ may not be a bipartite graph.

2. Polynomial sequences

We deal the problem, given a non constant polynomial $P(x)$ with positive leading coefficient and integer coefficients what can we say about the longest length of consecutive terms in the product set $B.B$. Since there can be at most finitely many

Date: April 2 , 2017.

natural numbers r such that $P(r) \leq 0$ or $P'(r) \leq 0$ there exists an l such that $P(r+l) > 0$ and $P'(r+l) > 0$ for all $r \geq 1$. Hence we can assume without loss of generality that every irreducible factor $g(x)$ of $P(x)$ we have $g(x) > 0$ and $g'(x) > 0 \ \ \forall x \geq 1$, as this assumption only effects R by a constant. From now on we will be assuming that for every irreducible divisor $g(x)$ of $P(x)$, $g(x) > 0$ and $g'(x) > 0$ for all natural numbers x. We prove three lemmas in order to obtain an upper bound on R. From now we let $f(x) \in \mathbb{Z}[x]$ denote an irreducible polynomial divisor of $P(x)$. If $f(x)$ is a polynomial of degree ≥ 2. Let D be the discriminant of $f(x)$. Let d be the greatest common divisor of the set $\{f(n) : n \in \mathbb{N}\}$. Let $f_1(x) = \frac{f(x)}{d}$. Denote $|D|d^2$ by M. If p is a prime divisor of M such that $p^e||M$, that is $p^e|M$ and $p^{e+1} \nmid M$, then $p^e \nmid d$ and hence there exists an a_p, such that $f_1(x)$ is not divisible by p for all $x \equiv a_p (\mod p^e)$. From Chinese remainder theorem there exists an integer a such that $a \equiv a_p (\mod p^e)$ for all primes p dividing M and hence there exists an a such that $f_1(x)$ is relatively prime to M for all $x \equiv a(\mod M)$.

Lemma 2.1. *For sufficiently large $R$the number of numbers in the set $\{f_1(r+i) : 1 \leq i \leq R, r+i \equiv a \mod M\}$ with at least one prime factor greater than R is $\geq \frac{R}{3M}$ for every non negative integer r.*

Proof. Let

$$Q = \prod_{\substack{i=1 \\ r+i \equiv a \mod M}}^{R} f_1(r+i).$$

Let S be the largest divisor of Q such that all the prime factors of S are $\leq R$.Let e_p be the index of p in S, that is $p^{e_p}|S$ and $p^{e_p+1} \nmid S$. Let $\rho(p)$ denote the number of solutions modulo p of the congruence $f(x) \equiv 0(\mod p)$.We have,

$$\log S = \sum_{\substack{p \nmid M \\ p \leq R}} e_p \log p \tag{1}$$

$$= \sum_{\substack{p \nmid M \\ p \leq R}} \sum_{n=1}^{\lfloor \frac{\log f_1(r+R)}{\log p} \rfloor} \sum_{\substack{1 \leq i \leq R \\ r+i \equiv a \mod M \\ f_1(r+i) \equiv 0 \mod p^n}} \log p. \tag{2}$$

For a prime $p \nmid M$, as p does not divide the discriminant of $f(x)$, each root x of $f_1(x) \equiv 0(\mod p)$ is a simple root modulo p and each root x modulo p can be uniquely lifted to a solution x' modulo p^n of $f_1(x) \equiv 0(\mod p^n)$. Hence number of solutions modulo p^n of $f_1(x) \equiv 0(\mod p^n)$ is $\rho(p)$. From Chinese remainder theorem, each solution x modulo p^n such that $f_1(r+x) \equiv 0(\mod p^n)$ with an additional congruence $r+x \equiv a(\mod M)$ corresponds to a unique solution modulo Mp^n. Hence number of solutions x modulo Mp^n such that $f_1(r+x) \equiv 0(\mod p^n)$ and $r+x \equiv a(\mod M)$ is $\rho(p)$. From Lagrange's theorem, we have $\rho(p) \leq deg(f(x))$. Hence $\rho(p) = O(1)$. Let $a_1, \cdots, a_{\rho(p)}$ be distinct solutions modulo Mp^n of the congruences $f_1(r+x) \equiv 0(\mod p^n)$ and $r+x \equiv a(\mod M)$. As for any a_j,

$$\sum_{\substack{1 \leq i \leq R \\ i \equiv a_j (\mod Mp^n)}} 1 = \frac{R}{Mp^n} + O(1)$$

we have,

$$\sum_{\substack{1\le i\le R\\ r+i\equiv a(\bmod M)\\ f_1(r+i)\equiv 0(\bmod p^n)}} \log p = (\log p)\left(\sum_{j=1}^{\rho(p)} \sum_{\substack{1\le i\le R\\ i\equiv a_j(\bmod Mp^n)}} 1\right)$$
$$= (\log p)\left(\sum_{j=1}^{\rho(p)} \frac{R}{Mp^n} + O(1)\right)$$
$$= \frac{R\rho(p)\log p}{Mp^n} + O(\log p).$$

Combining the above result with (2) we get

$$\log S = \sum_{\substack{p\nmid M\\ p\le R}} \sum_{n=1}^{\lfloor \frac{\log f_1(r+R)}{\log p}\rfloor} \left(\frac{R\rho(p)\log p}{Mp^n} + O(\log p)\right) \tag{3}$$

$$= \frac{R}{M}\sum_{\substack{p\nmid M\\ p\le R}} \frac{\rho(p)\log p}{p} + \frac{R}{M}\left(\sum_{\substack{p\nmid M\\ p\le R}} \sum_{n=2}^{\lfloor \frac{\log f_1(r+R)}{\log p}\rfloor} \frac{\log p}{p^n}\right) + \sum_{\substack{p\nmid M\\ p\le R}} \sum_{n=1}^{\lfloor \frac{\log f_1(r+R)}{\log p}\rfloor} O(\log p) \tag{4}$$

From prime ideal theorem(See Theorem 3.2.1 of [3]), we have

$$\sum_{p\le x} \rho(p) = \text{li } x + O(xe^{-c\sqrt{\log x}})$$

for some constant $c > 0$. Using partial summation, we have

$$\sum_{p\le x} \frac{\rho(p)\log p}{p} = \log x + O(1).$$

Hence the first term of (4) is

$$\frac{R}{M}\sum_{\substack{p\nmid M\\ p\le R}} \frac{\rho(p)\log p}{p} = \frac{R\log R}{M} + O(R).$$

As $\left(\sum_{\substack{p\nmid M\\ p\le R}} \sum_{n=2}^{\lfloor \frac{\log f_1(r+R)}{\log p}\rfloor} \frac{\log p}{p^n}\right) = O(1)$ the second term of (4) is $O(R)$. As $\log f_1(r+R) = O(\log(r+R))$ and number of primes not dividing M and less than R is $O(\frac{R}{\log R})$ we have the following estimate of third term of (4)

$$\sum_{\substack{p\nmid M\\ p\le R}} \sum_{n=1}^{\lfloor \frac{\log f_1(r+R)}{\log p}\rfloor} O(\log p) = O\left(\frac{R\log(r+R)}{\log R}\right).$$

Combining the results of each term of (4), we have

$$\log S = \frac{R\log R}{M} + O\left(\frac{\log(r+R)R}{\log R}\right). \tag{5}$$

Let L be a subset of $\{f_1(r+i) : 1 \leq i \leq R, r+i \equiv a \mod M\}$ containing all the numbers which do not contain any prime factor greater than R and let l denote the cardinality of L. We have the inequality,

$$\log \prod_{\substack{i=1 \\ f_1(r+i)\in L}}^{R} f_1(r+i) \geq \log \prod_{i=1}^{l} f_1(r+i) \tag{6}$$

$$= n\sum_{i=1}^{l} \log(r+i) + O(l) \tag{7}$$

$$= nl\log(r+l) + O(l) \tag{8}$$

$$\geq 2l\log(r+l) + O(l), \tag{9}$$

where $n \geq 2$ is the degree of the polynomial $f(x)$.Hence as $\prod_{\substack{i=1 \\ f_1(r+i)\in L}}^{R} f_1(r+i)|S$, we have the inequality,

$$\log \prod_{\substack{i=1 \\ f_1(r+i)\in L}}^{R} f_1(r+i) \leq \log S.$$

Hence from (5) and (9) we have

$$2l\log(r+l) + O(l) \leq \frac{R\log R}{M} + O\left(\frac{\log(r+R)R}{\log R}\right).$$

Hence for sufficiently large R, l should be less than $\frac{2R}{3M} - 2$. The number of numbers in the set $\{f_1(r+i) : 1 \leq i \leq R, r+i \equiv a \mod M\}$ is $\geq \frac{R}{M} - 1$. Hence number of numbers belonging to the set $\{f_1(r+i) : 1 \leq i \leq R, r+i \equiv a \mod M\}$ with at least one prime factor greater than R is $\geq \frac{R}{3M}$. □

The following corollary immediately follows from Lemma 2.1.

Corollary 2.2. *If $P(x) \in \mathbb{Z}[x]$ has an irreducible divisor of degree ≥ 2. Then there exists a constant $c > 0$ which may depend on $P(x)$ and independent of R such that for sufficiently large R and any non negative integer r, there are at least cR numbers in the set $\{P(r+i) : 1 \leq i \leq R\}$ having at least one prime factor greater than R.*

Lemma 2.3. *If $f(x)$ is a linear polynomial. If $r \geq R^\gamma$ for a $\gamma > 1$ then there exists a constant $c > 0$ depending upon γ such that for sufficiently large R, number of numbers in the set $\{f(r+i) : 1 \leq i \leq R\}$ with a prime factor greater than R is greater than cR.*

Proof. The proof is similar to that of Lemma 2.1.Let $Q = \prod_{i=1}^{R} f(r+i)$and S be the largest divisor of Q such that all the prime factors $\leq R$, let $f(x) = sx + t$. Let

e_p be the index of prime p dividing S.

(10)
$$\log S = \sum_{p \le R} e_p \log p$$

(11)
$$= \sum_{p \le R} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \sum_{\substack{1 \le i \le R \\ f(r+i) \equiv 0 \mod p^n}} \log p$$

(12)
$$= \sum_{\substack{p \le R \\ p \nmid s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \sum_{\substack{1 \le i \le R \\ f(r+i) \equiv 0 \mod p^n}} \log p + \sum_{\substack{p \le R \\ p \mid s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \sum_{\substack{1 \le i \le R \\ f(r+i) \equiv 0 \mod p^n}} \log p.$$

If $p \nmid s$ then $f(r+x) \equiv 0(\mod p^n)$ has a unique solution modulo p^n. Let a_1 be the unique solution modulo p^n. Then

$$\sum_{\substack{1 \le i \le R \\ f(r+i) \equiv 0(\mod p^n)}} \log p = \sum_{\substack{1 \le i \le R \\ i \equiv a_1(\mod p^n)}} \log p$$
$$= \frac{R \log p}{p^n} + O(\log p).$$

Observe that $\log f(r+i) = O(\log(r+i))$. Hence the first term of (12) is

$$\sum_{\substack{p \le R \\ p \nmid s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \sum_{\substack{1 \le i \le R \\ f(r+i) \equiv 0 \mod p^n}} \log p = \sum_{\substack{p \le R \\ p \nmid s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \left(\frac{R \log p}{p^n} + O(\log p) \right) \tag{13}$$

$$= R \sum_{\substack{p \le R \\ p \nmid s}} \frac{\log p}{p} + R \sum_{\substack{p \le R \\ p \nmid s}} \sum_{n=2}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \left(\frac{\log p}{p^n} \right) + \sum_{\substack{p \le R \\ p \nmid s}} O(\log(r+R)) \tag{14}$$

We have

$$\sum_{\substack{p \le R \\ p \nmid s}} \frac{\log p}{p} = \log R + O(1),$$

$$\sum_{\substack{p \le R \\ p \nmid s}} \sum_{n=2}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \left(\frac{\log p}{p^n} \right) = O(1)$$

and

$$\sum_{\substack{p \le R \\ p \nmid s}} O(\log(r+R)) = O\left(\frac{R \log(r+R)}{\log R} \right).$$

Substituting the above results in (14) we obtain the value of first term of (12)

$$\sum_{\substack{p\le R\\ p\nmid s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \sum_{\substack{1\le i\le R\\ f(r+i)\equiv 0 \mod p^n}} \log p = R\log R + O\left(\frac{R\log(r+R)}{\log R}\right). \tag{15}$$

If $p|s$ such that $p^k|s$ and $p^{k+1}\nmid s$. Note that $p^k \le s$. The number of solutions of $f(r+x)\equiv 0(\mod p^n)$ is less than or equal to p^k. Let $a_1,\cdots,a_{s_1}$ be the distinct solutions modulo p^n. We have $|s_1|\le p^k\le s$ for all n. Note that

$$\begin{aligned}\sum_{\substack{1\le i\le R\\ f(r+i)\equiv 0(\mod p^n)}} \log p &= \sum_{j=1}^{s_1} \sum_{\substack{1\le i\le R\\ i\equiv a_j(\mod p^n)}} \log p\\ &= \sum_{j=1}^{s_1}(\log p)\left(\frac{R}{p^n}+O(1)\right)\\ &= s_1\left(\frac{R\log p}{p^n}+O(\log p)\right)\\ &\le s\left(\frac{R\log p}{p^n}+O(\log p)\right).\end{aligned}$$

Using the above result we obtain an estimate on second term of (12)

$$\sum_{\substack{p\le R\\ p|s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \sum_{\substack{1\le i\le R\\ f(r+i)\equiv 0 \mod p^n}} \log p \le \sum_{\substack{p\le R\\ p|s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} s\left(\frac{R\log p}{p^n}+O(\log p)\right). \tag{16}$$

As there are only $O(1)$ number of prime factors of s and $\log f(r+R) = O(\log(r+R))$ we have

$$\sum_{\substack{p\le R\\ p|s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} s\left(\frac{R\log p}{p^n}\right) = O(R)$$

and

$$\sum_{\substack{p\le R\\ p|s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} O(s\log p) = O(\log(r+R)).$$

Combining the above two results in (16) we have an estimate for the second term of (12)

$$\sum_{\substack{p\le R\\ p|s}} \sum_{n=1}^{\lfloor \frac{\log f(r+R)}{\log p} \rfloor} \sum_{\substack{1\le i\le R\\ f(r+i)\equiv 0 \mod p^n}} \log p = O(R+\log(r+R)). \tag{17}$$

From (12), (15) and (17) we have

$$\log S = R\log R + O\left(\frac{R\log(r+R)}{\log R}\right). \tag{18}$$

Let L be a subset of $\{1 \le i \le R\}$ containing all i such that $f(r+i)$ has all prime factors $\le R$. Let the cardinality of L be l.

$$\log \prod_{\substack{i=1 \\ i \in L}}^{R} f(r+i) \ge \log \prod_{i=1}^{l} f(r+i)$$
$$= l \log(r+R) + O(R).$$

As $\prod_{\substack{i=1 \\ i \in L}}^{R} f(r+i) | S$ we have $\log \prod_{\substack{i=1 \\ i \in L}}^{R} f(r+i) \le \log S$. From (18) and the above inequality we have

$$l \log(r+R) + O(R) \le R \log R + O\left(\frac{R \log(r+R)}{\log R}\right).$$

For sufficiently large R, l should be $\le \frac{(1+\gamma)}{2\gamma} R$. Hence for sufficiently large R number of numbers of the set $\{f(r+i) : 1 \le i \le R\}$ with at least one prime factor greater than R is $\ge \frac{(\gamma-1)R}{2\gamma}$. □

We have the following Corollary for Lemma 2.3.

Corollary 2.4. *If degree of every irreducible divisor of $P(x)$ is 1 and $\gamma > 1$ then there exists a positive constant c such that the number of elements of the set $\{P(r+i) : 1 \le i \le R\}$ having at least one prime factor greater than R is greater than cR for sufficiently large R, r satisfying the inequality $r \ge R^{\gamma}$.*

Lemma 2.5. *Let $f(x)$ be a linear polynomial.If $r \le R^{\gamma}$ for some $\gamma > 1$ then there are at least $c\frac{R}{\log R}$ numbers of the set $\{f(r+i) : 1 \le i \le R\}$ with at least one prime factor greater than $\frac{R}{2}$ for a constant $c > 0$ and sufficiently large R.*

Proof. Let $f(n) = sn + t$ then there are at least $c_1(\frac{R}{\log R})$ primes between $(\frac{R}{2}, R]$ which are coprime to s, for a constant $c_1 > 0$. Each prime in the interval $(\frac{R}{2}, R]$ has one or two $i \in [1, R]$ such that $p | f(r+i)$. For each $f(r+i)$ there are at most $O(1)$ prime divisors belonging to $(\frac{R}{2}, R]$. Hence there are at least $c\frac{R}{\log R}$ numbers with at least one prime factor greater than $\frac{R}{2}$ for sufficiently large R and for some constant $c > 0$. □

Corollary 2.6. *If degree of every irreducible divisor of $P(x)$ is 1 and $r \le R^{\gamma}$ then number of elements of the set $\{P(r+i) : 1 \le i \le R\}$ with at least one prime factor belonging to the range $(\frac{R}{2}, R]$ is greater than $c\frac{R}{\log R}$ for a constant $c > 0$ and for sufficiently large R.*

In a graph $G(V, E)$ for $v \in V$ we define $V(v)$ to be the set of all vertices adjacent to v. Now we require a graph theoretic result in order to obtain an upper bound on R.

Lemma 2.7. *If there is a bipartite graph (A, B, E) such that for all $a \in A$ and $b \in B$, degree of a is $\le n$ and degree of b is ≥ 1 then there exists a sequence of vertices $b_1, \cdots, b_k$ with $b_i \in B$ satisfying $V(b_1) \ne \phi$ and $V(b_i)/(\cup_{j=1}^{j=i-1} V(b_j)) \ne \phi$ for $2 \le i \le k$ and $k \ge \frac{|B|}{n}$.*

Proof. The proof is by induction on n. For $n = 1$ the lemma is true since degree of $a \le 1\ \forall\, a \in A \implies V(b_1) \cap V(b_2) = \phi\ \forall\, b_1 \ne b_2 \in B$ and the sequence $b_1, \cdots, b_{|B|}$ will clearly satisfy $V(b_1) \ne \phi$ and $V(b_i)/(\cup_{j=1}^{i-1} V(b_j)) \ne \phi$ for $2 \le i \le k$.If the lemma is true for $n = r$ we have to prove for $n = r + 1$. Order the vertices of B as $b_1, \cdots b_{|B|}$. Let $S = \{a \in A : \text{degree of } a \geq 1\}$.Let $S_1 = V(b_1)$ and for $2 \leq i \leq |B|$, let $S_i = V(b_i)/(\cup_{j=1}^{i-1} V(b_j))$.Observe that $S = \cup_{i=1}^{|B|} S_i$.Let K be a set defined by $K = \{b_i : S_i \neq \phi\}$.If $|K| \geq \frac{|B|}{r+1}$ then we can choose the vertices in the set K arranged in a sequence which satisfies the hypothesis.If $|K| < \frac{|B|}{r+1}$ then consider the induced subgraph $A \cup (B/K)$ then degree of a is less than or equal to r for all $a \in A$. From the induction assumption there exists a sequence with length $\geq \frac{|B/K|}{r} > |B|(1 - \frac{1}{r+1})\frac{1}{r} = \frac{|B|}{r+1}$ in B/K satisfying the hypothesis which completes the proof by induction. $\square$

Now we prove the main theorem.

Theorem 2.8. *If $P(x) \in \mathbb{Z}[x]$ is a non constant polynomial with a positive leading coefficient and B is a set of complex numbers. If $\{P(r+1), \cdots, P(r+R)\}$ is contained in the product set $B.B$ for a nonnegative integer r and a natural number R. Then*
(1)If $P(x)$ has an irreducible factor of degree ≥ 2 then $R = O(|B|)$. In this case the implicit constant only depends on $P(x)$.
(2)If $P(x)$ has no irreducible factor of degree ≥ 2 and there exists a $\gamma > 1$ such that $r > R^\gamma$ then $R = O(|B|)$. In this case the implicit constant depends on $P(x)$ and γ.
(3)If $P(x)$ has no irreducible factor of degree ≥ 2 and there exists a $\gamma > 1$ such that $r \leq R^\gamma$ then $R = O(|B| \log |B|)$. In this case the implicit constant depends on γ and $P(x)$.

Proof. If $P(x)$ has an irreducible factor $f(x)$ of degree ≥ 2 or $P(x)$ has no irreducible divisor of degree ≥ 2 and $r > R^\gamma$ for some $\gamma > 1$ let

$$A = \{p : p \text{ is a prime, } p | P(r+i) \text{ for some } 1 \leq i \leq R,\, p > R\}$$

and let

$$C = \{P(r+i) : 1 \leq i \leq R, \exists \text{ prime } p > R \text{ such that } \quad p | P(r+i)\}.$$

If $P(x)$ has no irreducible divisor of degree ≥ 2 and $r \leq R^\gamma$ for some $\gamma > 1$ then let

$$A = \{p : p \text{ is a prime, } \frac{R}{2} < p \leq R \text{ and } p | P(r+i) \text{ for some } 1 \leq i \leq R\}$$

and let

$$C = \{P(r+i) : 1 \leq i \leq R, \exists \text{ prime } p \in (\frac{R}{2}, R] \text{ such that } p | P(r+i)\}.$$

In cases (1) and (2) from Corollaries 2.2 and 2.4 the size of C is greater than cR for some constant $c > 0$ (c depends only on $P(x)$ in case (1) and depends on $P(x)$ and γ in case (2)) and for sufficiently large R. In case (3) from Corollary 2.6 the size of C is greater than $c\frac{R}{\log R}$ for sufficiently large R and for some constant $c > 0$ which depends on γ and $P(x)$.If we consider a bipartite graph G between $A \cup C$ constructed such that there exits an edge $p \in A$ and $P(r+i) \in C$ if and only if $p | P(r+i)$. Let degree of $P(x)$ be d. In this graph, from Lagrange's theorem the degree of $a \in A$ is less than or equal to the degree of polynomial $P(x)$ in case (1) and (2) and less than twice the degree of polynomial $P(x)$ in case (3) . Hence from Lemma 2.7 there exists a sequence $c_1, c_2, \cdots, c_k \in C$ with $k \geq \frac{|C|}{2d}$ such that $V(c_1) \neq \phi$ and $V(c_i)/\cup_{j=1}^{k-1} V(c_j) \neq \phi$. Therefore every c_i has a prime divisor which does not divide any of c_j for $1 \leq j \leq i-1$. Let $C' = \{c_1, \cdots, c_k\}$. Note that in cases (1) and (2) we have $|C'| \geq \frac{c}{2d} R$ and in case (3) we have $|C'| \geq \frac{cR}{2d \log R}$ for sufficiently large R. Consider the bipartite auxiliary graph $G(C', B.B)$. We claim that there cannot be any cycle in this graph. Note that the vertex set of $G(C', B.B)$ is $B \times \{1\} \cup B \times \{2\}$ Suppose there was a cycle, since it is a bipartite graph, cycle length has to be an even number and there will be a cycle of the form $(b_1, 1)(b_2, 2) \cdots (b_{2k}, 2)(b_1, 1)$ where $b_i's$ belong to B then

$$\begin{aligned} b_1 b_2 &= c_{n_1} \\ b_2 b_3 &= c_{n_2} \\ &. \\ &. \\ &. \\ b_{2k} b_1 &= c_{n_{2k}} \end{aligned}$$

for some n_i's such that $1 \leq n_i \leq k$ and $n_i \neq n_j$ for $i \neq j$. Then it is easy to observe the relation

$$\prod_{i=1}^{k} c_{n_{2i}} = \prod_{j=1}^{k} c_{n_{2j-1}} \tag{19}$$

let n_i be the largest element of the set $\{n_1, \cdots, n_{2k}\}$. There exists a prime p such that $p | c_{n_i}$ and $p \nmid c_{n_j}$ for $j \neq i$ and hence p divides exactly one side of (19) and hence (19) cannot be true. Thus there exists no cycle in $G(C', B.B)$. In any graph without self loops, if there exists no cycle then the numbers of edges is strictly less than number of vertices. Hence $|C'| \leq 2|B| - 1$. As in cases (1) and (2) we have $|C'| \geq \frac{c}{2d} R$ and in case (3) we have $|C'| \geq \frac{cR}{2d \log R}$ for sufficiently large R.Therefore $R = O(|B|)$ in cases (1),(2) and $R = O(|B| \log |B|)$ in case (3) which completes the proof of the theorem. □

3. Number of Fibonacci Numbers and Lucas Numbers in a Product set

Let B be a finite set of naural numbers. Let A be the set of Fibonacci numbers contained in the product set $B.B$. From [2] there are only two perfect square Fibonacci numbers, viz., 1 and 144. Hence there can be at most two self loops in the graph $G'(A, B.B)$. We give an upper bound on the cardinality of A by using the following lemma.

Lemma 3.1. *Let F_n and F_m be nth and mth Fibonacci numbers and $m < n$ and $n > 2$ then $gcd(F_n, F_m) < \sqrt{F_n}$.*

Proof. Let $d = gcd(m, n)$. From the strong divisibilty property of Fibonacci numbers $gcd(F_n, F_m) = F_d$. We know that $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Since $m < n$, clearly $d \leq \frac{n}{2}$. If $d = 1$ then the hypothesis is clearly true and if $d > 1$, we have

$$(F_d)^2 = \frac{(\alpha^d - \beta^d)^2}{(\alpha - \beta)^2} < \frac{(\alpha^{2d} - \beta^{2d})}{(\alpha - \beta)} \leq F_n.$$

Thus, $gcd(F_m, F_n) < \sqrt{F_n}$. □

Theorem 3.2. *There cannot be more than $|B|$ Fibonacci numbers in the product set $B.B$ when B is a set of natural numbers.*

Proof. We claim that in the graph $G'(A, B.B)$ there cannot any cycle other than self loops. Suppose there is a k-cycle of the form $(b_1, 1)(b_2, 1)\cdots(b_k, 1)(b_1, 1)$ where $b_i \in B$ for $1 \leq i \leq k$. We now have the information that $b_i b_{i+1}$ for $1 \leq i \leq k-1$ and $b_k b_1$ are distinct Fibonacci numbers in the set $B.B$. Without loss of generality let us assume $b_1 b_2 = F$ is the largest Fibonacci number among $b_i b_{i+1}$ for $1 \leq i \leq k-1$ and $b_k b_1$.From Lemma 3.1, we have

$$b_1 \leq gcd(b_1 b_2, b_1 b_k) < \sqrt{F},$$
$$b_2 \leq gcd(b_1 b_2, b_2 b_3) < \sqrt{F}.$$

Hence $F = b_1 b_2 < F$ which is a contradiction.Hence there cannot be any cycle. From [2] there cannot be more than 2 self loops.Hence the number of edges which equal number of Fibonacci numbers in the set $B.B$ cannot exceed $|B| + 1$. Now we prove that there cannot be $|B| + 1$ Fibonacci numbers in $B.B$. Suppose there are $|B| + 1$ Fibonacci numbers, as the graph cannot have any cycle there should be two self loops namely, $(1, 1)$ and $(12, 1)$, and $1, 12 \in B$ and the graph obtained by removing the two self loops should be connected tree of $|B|$ vertices. Since the graph is connected there should be a path between $(1, 1)$ and $(12, 1)$. Let the path be $(b_1, 1)(b_2, 1)\cdots(b_k, 1)$ which implies that $b_i b_{i+1}$ for $1 \leq i \leq k-1$ are Fibonacci numbers and without loss of generality assume $b_1 = 1$ and $b_k = 12$. Let l be the index of highest value of $b_i b_{i+1}$, that is $b_l b_{l+1}$ is the largest Fibonacci number among $b_i b_{i+1}$ for $1 \leq i \leq k-1$. Clearly $l \neq 1$ and if $2 \leq l \leq k-2$ then from Lemma 3.1 we have

$$b_l \leq gcd(b_l b_{l+1}, b_{l-1} b_l) < \sqrt{b_l b_{l+1}},$$
$$b_{l+1} \leq gcd(b_l b_{l+1}, b_{l+1} b_{l+2}) < \sqrt{b_l b_{l+1}}.$$

Which implies $b_l b_{l+1} < b_l b_{l+1}$. Hence $l = k-1$. Again from Lemma 3.1

$$b_{k-1} \leq gcd(b_{k-1} b_k, b_{k-2} b_{k-1}) < \sqrt{b_{k-1} b_k}$$

which implies $b_{k-1} < b_k = 12$ but there are no Fibonacci numbers of the form $12b$ with $b < 12$.Hence there cannot be $|B| + 1$ Fibonacci numbers. Thus number of Fibonacci numbers in the set $B.B$ is $\leq |B|$. $\square$

Now we consider the case where B is a set of complex numbers and try to give an upper bound on the number of Lucas sequence terms in the product set. Let A be the set of Lucas sequence terms with indices greater than 30 in the product set $B.B$.

Lemma 3.3. *There cannot be any cycle in $G(A, B.B)$.*

Proof. Suppose there was a cycle, then there will be a cycle of the form $(b_1, 1)(b_2, 2)\cdots(b_{2k}, 2)(b_1, 1)$.Then

$$b_1 b_2 = L_{n_1}$$
$$b_2 b_3 = L_{n_2}$$
$$.$$
$$.$$
$$.$$
$$b_{2k} b_1 = L_{n_{2k}},$$

where L_{n_i} are Lucas sequence terms with indices greater than 30, which implies

$$\prod_{i=1}^{k} L_{n_{2i}} = \prod_{j=1}^{k} L_{n_{2j-1}} \tag{20}$$

Let n_i be the largest index ≥ 31. Then from [1], L_{n_i} contains a primitive divisor p and hence p divides exactly one side of (20) and therefore (20) cannot be true. Thus there cannot be any cycle. $\square$

Theorem 3.4. *Let $(L_n)_{n=1}^{\infty}$ be a Lucas sequence. Then the number of distinct elements of $(L_n)_{n=1}^{\infty}$ in $B.B$ is less than $2|B| + 30$.*

Proof. Since the number of vertices in $G(A, B.B)$ is $2|B|$ and from Lemma 3.3 there cannot be a cycle in $G(A, B.B)$ and hence the number of edges in $G(A, B.B)$ is $\leq 2|B| - 1$. Hence the number of distinct terms in Lucas sequence of index ≥ 31 is $\leq 2|B| - 1$. Hence number of distinct Lucas sequence terms in $B.B$ is $\leq 2|B| + 29$. $\square$

References

1. Y. Bilu, G. Hanrot and P. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*. J. Reine Angew. Math. **539**(2001), 75-122.
2. Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers*, Ann. of Math. (2) **163**:3 (2006), 969-1018.
3. Cojocaru, A. C., Murty, M. R. (2005). *An introduction to sieve methods and their applications* (Vol. 66). Cambridge University Press.
4. D. Zhelezov, *Improved bounds for arithmetic progressions in product sets*, International Journal of Number Theory 11, no. 08(2015), 2295-2303.
5. D. Zhelezov, *Product sets cannot contain long arithmetic progressions*, Acta Arith. 163 (2014), 299-307.

Department of Mathematics, Indian Institute of Technology Roorkee,India 247667