The Cyclic Groups via Bezout Matrices

Ömür Deveci¹, Yeşim Aküzüm¹, Erdal Karaduman² & Özgür Erdağ¹
¹Kafkas University, Department of Mathematics Faculty of Science and Letters, 36100 Kars, Turkey
²Department of Mathematics, Faculty of Science, Atatürk University, 25240 Erzurum, Turkey
Correspondence: Ömür Deveci, Kafkas University, Department of Mathematics Faculty of Science and Letters, 36100 Kars, Turkey. E-mail: odevci36@hotmail.com

Received: February 25, 2015   Accepted: March 11, 2015   Online Published: March 22, 2015
doi:10.5539/jmr.v7n2p34   URL: http://dx.doi.org/10.5539/jmr.v7n2p34

Abstract
In this paper, we define the Bezout matrices by the aid of the characteristic polynomials of the $k$-step Fibonacci, the generalized order-$k$ Pell and the generalized order-$k$ Jacobsthal sequences then we consider the multiplicative orders of the Bezout matrices when read modulo $m$. Consequently, we obtain the rules for the order of the cyclic groups by reducing the Bezout matrices modulo $m$.

Keywords: Bezout Matrix, cyclic group, order

2010 Mathematics Subject Classification: 15B36, 15A15, 20H20, 20Kxx,

1. Introduction and Preliminaries

Let $D$ be an integral domain and $P(x), Q(x) \in D[x]$ with $\text{deg}(P(x)) = n$ and $\text{deg}(Q(x)) = m$, we assume $n \geq m$.

$$P(x) = u_n x^n + u_{n-1} x^{n-1} + \cdots + u_1 x + u_0,$$

$$Q(x) = v_m x^m + v_{m-1} x^{m-1} + \cdots + v_1 x + v_0.$$ 

The Bezout matrix associated to the polynomials $P(x)$ and $Q(x)$ is the symmetric matrix:

$$B_n(P, Q) = \begin{bmatrix} b_{ij} \end{bmatrix}_{n \times n}$$

where the entries $b_{ij}$ are obtained by the identity

$$\frac{P(x)Q(y) - P(y)Q(x)}{x-y} = \sum_{i,j=1}^{n} b_{ij} x^i y^j.$$

It is important to note that the Bezout matrix $B_n(P, Q)$ is in $D^{\text{even}}$ and the entries $b_{ij}$ are defined by the formula

$$b_{ij} = \sum_{k=0}^{m_{ij}} u_{i+k} v_{j-k} - u_{i+k} v_{j-k-1}$$

such that $m_{ij} = \min \{i, n+1-j\}$ for each $i, j = 1, 2, \ldots, n$.

For more information on the Bezout matrix, see (Cayley, 1857; Barnett, 1972; Householder, 1970; Sylwester,
The \( k \)-step Fibonacci sequence \( \{ \mathcal{F}^k_n \} \) is defined recursively by the equation

\[
\mathcal{F}^k_{n+k} = \mathcal{F}^k_{n+k-1} + \mathcal{F}^k_{n+k-2} + \cdots + \mathcal{F}^k_n
\]

for \( n \geq 0 \), where \( \mathcal{F}^k_0 = \mathcal{F}^k_1 = \mathcal{F}^k_{k-2} = 0 \) and \( \mathcal{F}^k_{k-1} = 1 \).

For more information on the \( k \)-step Fibonacci sequence \( \{ \mathcal{F}^k_n \} \), see (Kalman, 1982; Slone).

In (Kilic & Tasci, 2006), Kilic and Tasci defined the generalized order-\( k \) Pell sequence \( \{ \mathcal{P}^k_n \} \) as follows:

For \( n > 0 \),

\[
\mathcal{P}^k_n = 2\mathcal{P}^k_{n-1} + \mathcal{P}^k_{n-2} + \cdots + \mathcal{P}^k_{n-k}
\]

with initial conditions \( \mathcal{P}^k_{n-k} = 1 \) and \( \mathcal{P}^k_{n-2}, \cdots, \mathcal{P}^k_0 = 0 \).

The generalized order-\( k \) Jacobsthal sequence \( \{ \mathcal{J}^k_n \} \) is defined (Yilmaz & Bozkurt, 2009) recursively by the equation

\[
\mathcal{J}^k_n = \mathcal{J}^k_{n-1} + 2\mathcal{J}^k_{n-2} + \cdots + \mathcal{J}^k_{n-k}
\]

for \( n > 0 \), where \( \mathcal{J}^k_{n-1} = 1 \) and \( \mathcal{J}^k_{n-2}, \cdots, \mathcal{J}^k_0 = 0 \).

In (Deveci & Akuzum, 2014; Deveci & Karaduman, 2012; Deveci & Karaduman, in press; Deveci, et al., in press; Lü & Wang, 2007; Ozkan, 2014; Tas, et al., 2014; Tas & Karaduman, 2014), the authors obtained the cyclic groups via some special matrices. In this paper, we define the Bezout matrices by the aid of the characteristic polynomials of the \( k \)-step Fibonacci, the generalized order-\( k \) Pell and the generalized order-\( k \) Jacobsthal sequences. Further, we consider the multiplicative orders of the Bezout matrices according to modulo \( m \) and so we obtain the rules for the orders of the cyclic groups which are produced using the Bezout matrices as generators by reducing their elements according to modulo \( m \).

### 2. Main Results and Proofs

It is easy to see that the characteristic polynomials of the \( k \)-step Fibonacci, the generalized order-\( k \) Pell and the generalized order-\( k \) Jacobsthal sequences are as follows, respectively:

\[
P^\mathcal{F}_k(x) = x^k - x^{k-1} - \cdots - x - 1,
\]

\[
P^\mathcal{P}_k(x) = x^k - 2x^{k-3} - x^{k-2} - \cdots - x - 1
\]

and

\[
P^\mathcal{J}_k(x) = x^k - x^{k-1} - 2x^{k-2} - x^{k-3} - \cdots - 1.
\]

Then we can write the following Bezout matrices for the polynomials \( P^\mathcal{F}_k(x), P^\mathcal{P}_k(x) \) and \( P^\mathcal{J}_k(x) \).

**Definition 2.1.** For every positive integer \( k \geq 3 \), the Bezout matrix \( B_k(P^\mathcal{F}_k(x), P^\mathcal{P}_{k-1}(x)) = \left[ b^k_{ij} \right]_{i,j \leq k} \) is as follows:
\[
b_{k(\ell)}(i, t, k) = \begin{cases} 
0, & i < t < k, \\
2, & i = t < k, \\
1, & (0 < t < i < k): \ (t = 0 \text{ and } i = k), \\
-1, & (t = 0 \text{ and } i < k); \ (t < k \text{ and } i = k).
\end{cases}
\]

That is,
\[
B_{k}(P_{\ell}^{F}(x), P_{k-1}^{F}(x)) = \begin{bmatrix}
-1 \\
-1 \\
\vdots \\
-1
\end{bmatrix}
\end{bmatrix}^{T}.
\]

where \( M \) is a square matrix of order \( k-1 \) such that
\[
M = \begin{bmatrix}
0 & \cdots & 0 & 2 \\
0 & \cdots & 0 & 2 & 1 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 2 & 1 & \cdots & 1 \\
2 & 1 & 1 & \cdots & 1
\end{bmatrix}
\]
Let \( k \geq 5 \), then the Bezout matrices \( \mathbf{B}_k\left(P^p_k(x), P^p_{k-1}(x)\right) = \left[b_{ij}\right]_{k \times k} \) are defined by the following form:

\[
\begin{cases}
0, & 1 \leq i < t < k - 1, \\
-1, & (1 \leq i = t < k - 1); (1 \leq i < k - 1 \text{ and } t = -1); (i = k \text{ and } 1 \leq t < k - 1), \\
2, & (2 \leq i < k - 1 \text{ and } t = i - 1 \text{ or } t = 0); (i = k - 1 \text{ and } 2 \leq t \leq k - 2), \\
-2, & (i = k - 1 \text{ and } t = -1); (i = k \text{ and } t = 0), \\
3, & (i = 1 \text{ and } t = 0); (i = k - 1 \text{ and } t = k - 2), \\
4, & i = k - 1 \text{ and } t = 0, \\
1, & \text{otherwise}.
\end{cases}
\]

That is,

\[
\begin{bmatrix}
3 & -1 \\
2 & -1 \\
\vdots & \vdots \\
2 & -1 \\
3 & 2 & \cdots & 2 & 4 & -2 \\
-1 & -1 & \cdots & -1 & -2 & \mathbf{1}_{(k-2)(k-2)}
\end{bmatrix}
\]

for \( k \geq 5 \). Where \( M \) is a square matrix of order \( k - 2 \) such that

\[
\begin{bmatrix}
0 & \cdots & 0 & 0 & -1 \\
0 & \cdots & 0 & -1 & 2 \\
0 & \cdots & -1 & 2 & 1 \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & -1 & 2 & 1 & \cdots & 1 \\
-1 & 2 & 1 & \cdots & 1 \\
\end{bmatrix}_{(k-2)(k-2)}
\]

Example.

\[
\begin{bmatrix}
0 & 0 & 0 & -1 & 3 & -1 \\
0 & 0 & -1 & 2 & 2 & -1 \\
0 & -1 & 2 & 1 & 2 & -1 \\
-1 & 2 & 1 & 1 & 2 & -1 \\
3 & 2 & 2 & 2 & 4 & -2 \\
-1 & -1 & -1 & -1 & -2 & 1 \\
\end{bmatrix}
\]

We easily derive that

\[
\det \mathbf{B}_k\left(P^p_k(x), P^p_{k-1}(x)\right) = \det \mathbf{B}_k\left(P^p_k(x), P^p_{k-1}(x)\right) = \begin{cases}
-1, & \text{if } k \equiv 0, 3 \mod 4, \\
1, & \text{otherwise},
\end{cases}
\]

for \( k \geq 3 \).

**Definition 2.3.** For every positive integer \( k \geq 3 \), the Bezout matrices \( \mathbf{B}_k\left(P^p_k(x), P^p_{k-1}(x)\right) = \left[b_{ij}\right]_{k \times k} \) are as follows:
If \( k = 3 \), the Bezout matrix \( B_3 \left( P_3^t(x), P_3^r(x) \right) \) is
\[
\begin{bmatrix}
3 & 3 & -2 \\
3 & 1 & -1 \\
-2 & -1 & 1
\end{bmatrix}
\]

If \( k = 4 \), the Bezout matrix \( B_4 \left( P_4^t(x), P_4^r(x) \right) \) is
\[
\begin{bmatrix}
0 & 3 & 3 & -2 \\
3 & 6 & 1 & -2 \\
3 & 1 & 1 & -1 \\
-2 & -2 & -1 & 1
\end{bmatrix}
\]

Let \( k \geq 5 \), then the Bezout matrices \( B_k \left( P_k^t(x), P_k^r(x) \right) = \left[ b_{ij} \right]_{k \times k} \) are defined by the following form:

\[
b_{i(k-1)+1} = \begin{cases} 
0, & \text{if } 1 \leq i < t < k - 1, \\
3, & \text{if } (1 \leq i = t < k - 1); (i = k - 1 \text{ and } t = k - 2); (i = 1 \text{ and } t = 0), \\
6, & \text{if } 2 \leq i < k - 1 \text{ and } t = i - 1, \\
1, & \text{if } (2 \leq i < k - 1 \text{ and } t = i - 1 \text{ or } t = 0); (i = k \text{ and } t = -1), \\
-1, & \text{if } (i = k - 1 \text{ and } t = -1); (i = k \text{ and } t = 0), \\
-2, & \text{if } (1 \leq i < k - 1 \text{ and } t = -1); (i = k \text{ and } 1 \leq t < k - 1), \\
4, & \text{otherwise.} 
\end{cases}
\]

That is,
\[
B_k \left( P_k^t(x), P_k^r(x) \right) = \begin{bmatrix} 3 & -2 \\ 1 & -2 \\ \vdots & \vdots \\ 1 & -2 \\ 3 & 1 & \cdots & 1 & 1 & -1 \\ -2 & -2 & \cdots & -2 & -1 & 1 \end{bmatrix}_{k \times k}
\]

for \( k \geq 5 \). Where \( M \) is a square matrix of order \( k - 2 \) such that
\[
M = \begin{bmatrix}
0 & \cdots & 0 & 0 & 3 \\
0 & \cdots & 0 & 0 & 3 & 6 \\
0 & \cdots & 0 & 3 & 6 & 4 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 3 & 6 & 4 & \cdots & 4 \\
3 & 6 & 4 & \cdots & 4 \\
\end{bmatrix}_{(k - 2) \times (k - 2)}
\]

For given a matrix \( A = \left[ a_{ij} \right] \) with \( a_{ij} \)'s being integers, \( A \pmod{m} \) means that every entries of \( A \) are reduced modulo \( m \), that is, \( A \pmod{m} = \left( a_{ij} \pmod{m} \right) \). Let \( \langle A \rangle_n = \left\{ (A)^n \pmod{m} \mid n \geq 0 \right\} \). If
\((\det A, m) = 1\). \(\langle A \rangle_m\) is a cyclic group. We denote the order of the set \(\langle A \rangle_m\) by \(\|A\|_m\).

Since \(\det B_k \left( P^F_k (x), P^F_{k+1} (x) \right) = \det B_k \left( P^P_k (x), P^P_{k+1} (x) \right) = \pm 1\) for \(k \geq 3\), it is clear that the sets \(\langle B_k \left( P^F_k (x), P^F_{k+1} (x) \rangle \rangle \) and \(\langle B_k \left( P^P_k (x), P^P_{k+1} (x) \rangle \rangle \) are cyclic for \(m \geq 2\).

Now we consider the cyclic groups which are generated by the matrices \(B_k \left( P^F_k (x), P^F_{k+1} (x) \right) \), \(B_k \left( P^P_k (x), P^P_{k+1} (x) \right) \) and \(B_k \left( P^P_k (x), P^P_{k+1} (x) \right) \). Suppose that \(\alpha\) is the largest positive integer and \(p\) is a prime such that

\[
(\det M, p) = 1 \quad \text{and} \quad \|M\|_p = \|M\|_{p^\alpha}.
\]

Then \(\|M\|_{p^\lambda} = p^{\lambda - \alpha} \cdot \|M\|_p\) for every \(\lambda \geq \alpha\).

**Proof.** Let us consider the cyclic group \(\langle B_k \left( P^F_k (x), P^F_{k+1} (x) \rangle \rangle \) for \(k \geq 3\) and \(m \geq 2\). Suppose that \(a\) is a positive integer and \(\langle B_k \left( P^F_k (x), P^F_{k+1} (x) \rangle \rangle\) is denoted by \(O(m)\). If

\[
\left( B_k \left( P^F_k (x), P^F_{k+1} (x) \right) \right)^{O(p^\alpha)} = I \left( \text{mod } p^{O(p^\alpha)} \right),
\]

then \(\left( B_k \left( P^F_k (x), P^F_{k+1} (x) \right) \right)^{O(p^\alpha)} = I \left( \text{mod } p^a \right)\) where \(I\) is the \(k \times k\) identity matrix. Thus we obtain that \(O(p^a)\) divides \(O(p^{a+1})\). Also, writing

\[
\left( B_k \left( P^F_k (x), P^F_{k+1} (x) \right) \right)^{O(p^\alpha)} = I + b_{(a)} \cdot p^a,
\]

by the binomial theorem, we obtain

\[
\left( B_k \left( P^F_k (x), P^F_{k+1} (x) \right) \right)^{O(p^\alpha)} = I + \sum_{i=0}^{p} \binom{p}{i} b_{(a)} \cdot p^a = I \left( \text{mod } p^{a+1} \right),
\]

which yields that \(O(p^{a+1})\) divides \(O(p^a) \cdot p\). Thus, \(O(p^{a+1}) = O(p^a)\) or \(O(p^{a+1}) = O(p^a) \cdot p\). It is clear that \(O(p^{a+1}) = O(p^a) \cdot p\) holds if and only if there is a \(b_{(a)}\) which is not divisible by \(p\). Since \(\alpha\) is the largest positive integer such that \(O(p) = O(p^a)\), \(O(p^a) \neq O(p^{a+1})\). There is an \(b_{(a+1)}\) which is not divisible by \(p\). So we get that \(O(p^{a+1}) \neq O(p^{a+2})\). The proof is completed by induction on \(\alpha\).

The proofs for the cyclic groups \(\langle B_k \left( P^F_k (x), P^F_{k+1} (x) \rangle \rangle \) and \(\langle B_k \left( P^P_k (x), P^P_{k+1} (x) \rangle \rangle \) are similar to the above and are omitted.

**Example.** \(\left| \langle B_5 \left( P^F_5 (x), P^F_4 (x) \rangle \rangle \right| = 48 \) and so \(\left| \langle B_5 \left( P^F_5 (x), P^F_4 (x) \rangle \rangle \right| = 1936973136 = 7^9 \cdot 48.\)

39
ii. \[ \| B_s (P^e (x), P^e (x)) \|_{11} = 12 \] and so \[ \| B_s (P^e (x), P^e (x)) \|_{11} = 73390908538097455492 = 11^{19} \cdot 12. \]

iii. \[ \| B_s (P^e (x), P^e (x)) \|_5 = 104 \] and so \[ \| B_s (P^e (x), P^e (x)) \|_5 = 634765625000 = 5^{14} \cdot 104. \]

**Theorem 2.2.** Let \( G_{n} \) be any of the cyclic groups \( \left\{ B_s (P^e (x), P^e (x), P^e (x)) \right\}_{m} \neq \left\{ B_s (P^e (x), P^e (x), P^e (x)) \right\}_{m} \) and \( \left\{ B_s (P^e (x), P^e (x)) \right\}_{m} \) and let \( m = \prod_{i=1}^{t} p_i^{e} \), \( t \geq 1 \) where \( p_i \)'s are distinct primes, then

\[ |G_{n}| = \text{lcm} \left[ G_{p_1^e}, G_{p_2^e}, \ldots, G_{p_t^e} \right]. \]

**Proof.** Let us consider the cyclic group \( B_s (P^e (x), P^e (x)) \), then \( 2 \mid m \). Let \( \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = u \)

for \( 1 \leq i \leq t \) and let \( \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = u \). Then we have

\[
\text{the entry } (i, j) \text{ of } \left\{ B_s (P^e (x), P^e (x)) \right\}^u = \begin{cases} p_i^{e} \epsilon_{ij}, & i > j, \\ p_i^{e} \epsilon_{ij} + 1, & i = j, \\ p_i^{e} \epsilon_{ij}, & i < j, \end{cases}
\]

and

\[
\text{the entry } (i, j) \text{ of } \left\{ B_s (P^e (x), P^e (x)) \right\}^u = \begin{cases} m \epsilon_{ij}, & i > j, \\ m \epsilon_{ij} + 1, & i = j, \\ m \epsilon_{ij}, & i < j, \end{cases}
\]

where \( \epsilon_{ij} \) and \( \epsilon_{ij}^e \) are integers for \( 0 \leq i, j \leq k \). Since \( m = c \cdot p_n^e \) for \( 1 \leq n \leq t \), \( u \) is of the form \( m = c \cdot u_n \). Thus we conclude that \( u = \text{lcm} [u_1, u_2, \ldots, u_t] \).

The proofs for the cyclic groups \( \left\{ B_s (P^e (x), P^e (x)) \right\}_{m} \) and \( \left\{ B_s (P^e (x), P^e (x)) \right\}_{m} \) are similar to the above and are omitted.

**Example i.** Since \( \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 5^2 \cdot 78 = 1950 \cdot \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 1330 \) and \( 1375 = 5^1 \cdot 11 \),

\[
\left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 259350 = \text{lcm} [1950, 1330].
\]

**ii.** Since \( \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 2^4 \cdot 7 = 112 \), \( \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 3^1 \cdot 26 = 702 \) and \( 2592 = 2^5 \cdot 3^4 \),

\[
\left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 39312 = \text{lcm} [112, 702].
\]

**iii.** Since \( \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 20 \), \( \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 104 \), \( \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 114 \) and \( 105 = 3 \cdot 5 \cdot 7 \), \( \left\| B_s (P^e (x), P^e (x)) \right\|_{\mathbb{D}} = 29640 = \text{lcm} [20, 104, 114]. \)
3. Conclusion

Let \( M \) be any of the matrices \( B_k\left( P_k^r(x), P_{k+1}^r(x)\right) \), \( B_k\left( P_k^o(x), P_{k+1}^o(x)\right) \) and \( B_k\left( P_k^i(x), P_{k+1}^i(x)\right) \) and let \( p \geq k \) be a prime such that \((\det M, p) = 1\). Then, we obtain that \( \|M\|_p \geq p^{k+1} - p^r \) for \( p \leq 2999 \) and \( 0 \leq r \leq k + 1 \).

**Open Problem.** Is the result above satisfied for every prime \( p \geq k \)?

**Acknowledgment**

This Project was supported by the Commission for the Scientific Research Projects of Kafkas University. The Project number, 2014-FEF-34.

**References**


**Copyrights**

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).