A NOTE ON BALANCING SEQUENCES AND APPLICATION TO CRYPTOGRAPHY

K. ANITHA(1), I. MUMTAJ FATHIMA(2) AND A R VIJAYALAKSHMI(3)

ABSTRACT. In this paper, we prove the lower bound for the number of balancing non-Wieferich primes in arithmetic progressions. More precisely, for any given integer \( r \geq 2 \) there are \( \gg \log x \) balancing non-Wieferich primes \( p \leq x \) such that \( p \equiv \pm 1 \pmod{r} \), under the assumption of the \( abc \) conjecture for the number field \( Q(\sqrt{2}) \). Further, we discuss some applications of balancing sequences in cryptography.

1. INTRODUCTION

In 1909, Arthur Wieferich [25] established the connection between first case of Fermat’s last theorem and Wieferich primes. More precisely, if the first case of Fermat’s last theorem fails for an odd prime \( p \), then \( p \) is a Wieferich prime for base 2. The Wieferich primes are defined below:

Let \( b \geq 2 \) be an integer. An odd prime \( p \) is called a Wieferich prime for base \( b \) if

\[
b^{p-1} \equiv 1 \pmod{p^2}.
\]

Otherwise it is called a non-Wieferich prime for base \( b \). As of today, the only known Wieferich primes for base 2 are 1093 and 3511.

A search for the Wieferich prime is one of the long-standing problems in number theory. It is still unknown whether there are finitely or infinitely many Wieferich primes that exist for any base \( b \geq 2 \). However, Silverman [19] established the conditional results on non-Wieferich primes. Assuming the \( abc \) conjecture [9], he proved the infinitude of non-Wieferich primes for any base \( b \).

For any fixed \( b \in \mathbb{Q}^* \), where \( \mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \) and \( b \neq \pm 1 \), if the \( abc \) conjecture is true, then

\[
|\{\text{primes } p \leq x : b^{p-1} \not\equiv 1 \pmod{p^2}\}| \gg_b \log x.
\]

In 2013, Graves and Ram Murty [8] improved Silverman’s result to certain arithmetic progressions. They showed that, if \( b \) and \( r \) are positive integers and assume the \( abc \) conjecture, then

\[
|\{\text{primes } p \leq x : p \equiv 1 \pmod{r}, b^{p-1} \not\equiv 1 \pmod{p^2}\}| \gg \frac{\log x}{\log \log x}.
\]
Then, there has been further enhancement made by Chen and Ding \cite{3}.

\[
\left\{ \text{primes } p \leq x : p \equiv 1 \pmod{r}, b^{p-1} \not\equiv 1 \pmod{p^2} \right\} \gg \frac{\log x (\log \log \log x)^M}{\log \log x},
\]

where \( M \) is any fixed positive integer. Recently, Ding \cite{4} further strengthened the lower bound as

\[
\left\{ \text{primes } p \leq x : p \equiv 1 \pmod{r}, b^{p-1} \not\equiv 1 \pmod{p^2} \right\} \gg \log x.
\]

In this paper, we prove the similar lower bound for non-Wieferich primes in balancing numbers \( \{B_n\} \) (defined in Section 2.1), assuming the abc conjecture for the number field \( \mathbb{Q}(\sqrt{2}) \).

In 1999, Behera and Panda \cite{1} first proposed the concept of balancing numbers and studied their properties. Then, Rout \cite{18} defined the balancing Wieferich primes as follows:

An odd prime \( p \) is called a balancing Wieferich prime if it satisfies the congruence

\[
B_{p-(\frac{8}{p})} \equiv 0 \pmod{p^2},
\]

where \( \left( \frac{8}{p} \right) \) denotes the Legendre symbol. Otherwise, it is called a balancing non-Wieferich prime. Recently, Wang and Ding \cite{24} proved that there are \( \gg \log x \) balancing non-Wieferich primes, assuming the abc conjecture for the number field \( \mathbb{Q}(\sqrt{2}) \). Earlier, Rout \cite{18} and Dutta et al. \cite{5} proved some lower bounds for the number of balancing non-Wieferich primes \( p \) such that \( p \equiv 1 \pmod{r} \), where \( r \geq 2 \) be a fixed integer. However, Wang and Ding \cite{24} remarked that their results had some gaps. To the best of our knowledge, the main theorem in this paper is the first result in this direction which addresses the problem of balancing non-Wieferich primes in arithmetic progressions.

More precisely, we prove the following main theorem:

**Theorem 1.1.** Let \( r \geq 2 \) be any fixed integer and let \( n > 1 \) be any integer. Assume that the abc conjecture for the number field \( \mathbb{Q}(\sqrt{2}) \) is true. Then

\[
\left\{ \text{primes } p \leq x : p \equiv \pm 1 \pmod{r}, B_{p-(\frac{8}{p})} \not\equiv 0 \pmod{p^2} \right\} \gg_{a,r} \log x.
\]

Further, as an application in cryptography, the various studies related to public key encryption-decryption schemes based on the recurrence sequences have been noted. In 2014, Ray et al. \cite{17} developed a scheme using finite state machines, recurrence relation of balancing sequences, and balancing matrices. Viswanath and Ranjith kumar \cite{22} proposed the concept of public-key cryptography using Hill cipher techniques and developed the cryptosystem using rectangular matrices. Then, further enhancement made by Sundarayya and Prasad \cite{21} using Affine-Hill cipher techniques. Recently, Prasath and Mahato \cite{14} proposed a public-key cryptosystem using Affine-Hill cipher with generalized Fibonacci matrix and discussed its strength.

In Section 4, we propose a public-key cryptosystem using **Affine-Hill ciper** with a generalized balancing matrix with large power \( k \), i.e., \( Q^k_{B_n} \) as a key. We exchange the key matrix \( K = Q^k_{B_n} \) of order \( s \times s \) for encryption-decryption scheme with the help
of balancing sequences under prime modulo. Instead of exchanging a key matrix, in this scheme we simply need to trade a pair of numbers \((s, k)\), which results in a wide key-space and lower time and space complexity.

2. Preliminaries

2.1. Balancing numbers. The sequence of balancing numbers \(\{B_n\}\) is defined by the recurrence relation

\[ B_{n+1} = 6B_n - B_{n-1} \]  

for \(n \geq 1\) with initial conditions \(B_0 = 0\) and \(B_1 = 1\).

**Definition 2.1.** [1] A positive integer \(n\) is called a balancing number if

\[ 1 + 2 + \ldots + (n-1) = (n+1) + (n+2) + \ldots + (n+l), \]

where \(l \in \mathbb{Z}^+\) is called the balancer corresponding to the balancing number \(n\).

In other words, \(n \in \mathbb{Z}^+\) is a balancing number if and only if \(n^2\) is a triangular number, i.e., \(8n^2 + 1\) is a perfect square.

The Binet formula for balancing number is

\[ B_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \]

where \(\alpha = 3 + 2\sqrt{2}\) and \(\beta = 3 - 2\sqrt{2}\).

Throughout this paper, we take \(\alpha = 3 + 2\sqrt{2}\) and \(\beta = 3 - 2\sqrt{2}\). Further we note that, for any prime \(p > 2\), \(B_p \equiv (\frac{8}{p}) \equiv 0 \pmod{p}\) [13].

2.2. The abc conjecture. The abc conjecture was formulated by Oesterlé [12] and Masser [11]. We state the abc conjecture [9] below:

For any given real number \(\epsilon > 0\), there is a constant \(C_\epsilon\) which depends only on \(\epsilon\) such that for every triple of positive integers \(a, b, c\) satisfying \(a + b = c\) with \(\gcd(a, b) = 1\), we have

\[ c < C_\epsilon \left(\text{rad}(abc)\right)^{1+\epsilon}, \]

where \(\text{rad}(abc) = \prod_{p|abc} p\).

We now recall the definition of Vinogradov symbol.

**Definition 2.2.** [23] Let \(f\) and \(g\) are two non-negative functions. If \(f < cg\) for some positive constant \(c\), then we write \(f \ll g\) or \(g \gg f\). It is also called Vinogradov symbol.

2.2.1. The abc conjecture for number fields [23, 9]. Let \(K\) be an algebraic number field and \(K^* = K \setminus \{0\}\). Let \(V_K\) be the set of primes on \(K\), that is any \(v \in V_K\) is an equivalence class of non-trivial norms on \(K\) (finite or infinite). Let \(\|x\|_v := N_{K/Q}(p)^{-\nu_p(x)}\), if \(v\) (finite) is defined by a prime ideal \(p\) of the ring of integers \(O_K\) in \(K\) and \(\nu_p\) is the corresponding valuation, where \(N_{K/Q}\) is the absolute value norm. For \(v\) is infinite and let \(\|x\|_v := |\rho(x)|^e\) for all non-conjugate embeddings \(\rho : K \to \mathbb{C}\) with \(e = 1\) if \(\rho\) is real and \(e = 2\) if \(\rho\) is complex.
The *height* of any triple \((a, b, c) \in K^*\) is
\[
H_K(a, b, c) := \prod_{v \in V_K} \max(\|a\|_v, \|b\|_v, \|c\|_v).
\]

The *radical* of the triple \((a, b, c) \in K^*\) is
\[
\text{rad}_K(a, b, c) := \prod_{p \in I_K(a, b, c)} N_{K/Q}(p)^{\nu_p(p)},
\]
where \(p\) is a rational prime with \(p \mathbb{Z} = p \cap \mathbb{Z}\) and \(I_K(a, b, c)\) is the set of all prime ideals \(p\) of \(O_K\) for which \(\|a\|_v, \|b\|_v, \|c\|_v\) are not equal.

The *abc* conjecture for algebraic number field \(K\) states that for any \(\varepsilon > 0\) there exists a positive constant \(C_{K, \varepsilon}\) such that
\[
H_K(a, b, c) \leq C_{K, \varepsilon}(\text{rad}_K(a, b, c))^{1+\varepsilon},
\]
for all \(a, b, c \in K^*\) satisfying \(a + b + c = 0\).

2.3. **Cyclotomic polynomial.** We now recall the cyclotomic polynomial and some of its properties.

**Definition 2.3.** [15] For any integer \(m \geq 1\), the \(m^{th}\) cyclotomic polynomial is
\[
\Phi_m(X) = \prod_{i=1 \atop \gcd(i,m)=1}^m (X - \zeta_m^i),
\]
where \(\zeta_m\) is the primitive \(m^{th}\) root of unity.

It follows that the recursion formula for cyclotomic polynomial is
\[
X^m - 1 = \prod_{d|m} \Phi_d(X).
\] (2.2)

The following lemma characterizes the prime divisors of \(\Phi_m(\alpha, \beta)\), where
\[
\Phi_m(\alpha, \beta) = \prod_{i=1 \atop \gcd(i,m)=1}^m (\alpha - \zeta_m^i \beta).
\]

**Lemma 2.4.** (Stewart [20] Lemma 2) Let \((\alpha + \beta)^2\) and \(\alpha \beta\) be coprime non-zero integers with \(\alpha/\beta\) not a root of unity. If \(m > 4\) and \(m \neq 6, 12\) then \(P(m/\gcd(3, m))\) divides \(\Phi_m(\alpha, \beta)\) to at most the first power. All other prime factors of \(\Phi_m(\alpha, \beta)\) are congruent to \(\pm 1\) (mod \(m\)). Further, if \(m > e^{152.4^{0.7}}\) then \(\Phi_m(\alpha, \beta)\) has at least one prime factor congruent to \(\pm 1\) (mod \(m\)).
A NOTE ON BALANCING SEQUENCES AND APPLICATION TO CRYPTOGRAPHY

Here, \( P(k) \) denotes the greatest prime factor of \( k \) with the convention that \( P(0) = P(\pm 1) = 1 \). We note that, Yu. Bilu et al. [2] reduced the above lower bound \( e^{452.4^{67}} \) to 30. In the Lemma 2.4 Stewart [20] considered the cyclotomic polynomial

\[
\alpha^m - \beta^m = \prod_{d|m} \Phi_d(\alpha, \beta).
\] (2.3)

Since \( \beta \) is a unit in \( \mathbb{Q}(\sqrt{2}) \), we notice that the prime divisors of \( \Phi_m(\alpha, \beta) \) and the prime divisors of \( \Phi_m(\alpha/\beta) \) are the same. Thus by using above Lemma 2.4 the prime divisors of \( \Phi_m(\alpha/\beta) \) are congruent to \( \pm 1 \pmod{m} \).

**Lemma 2.5.** (Rout [18, Lemma 2.10]) For any real number \( b \) with \( |b| > 1 \), there exists \( C > 0 \) such that

\[
|\Phi_m(b)| \geq C|b|^\phi(m),
\]

where \( \phi(m) \) is Euler’s totient function.

2.4. Some lemmas. We state some of the important lemmas from [18], [24] and [4].

**Lemma 2.6.** (Rout [18, Lemma 2.12]) Suppose that \( B_n \) factored into \( X_n Y_n \), where \( X_n \) and \( Y_n \) are square-free and powerful part of \( B_n \) respectively. If \( p|X_n \), then

\[
B_{p^e-(\frac{a}{p})} \not\equiv 0 \pmod{p^2}.
\]

**Lemma 2.7.** (Rout [18, Lemma 2.9]) For any \( n \geq 2 \), the \( n \)th balancing number satisfies the following inequality.

\[
\alpha^{n-1} < B_n < \alpha^n.
\]

**Lemma 2.8.** (Rout [18]) If the abc conjecture for the number field \( \mathbb{Q}(\sqrt{2}) \) is true, then \( Y_{nr} \ll_\epsilon B_{2e}^{2e} \).

This result is part of the proof of [18, Theorem 3.1].

**Lemma 2.9.** (Wang and Ding [24, Lemma 2.4]) If \( m < n \), then \( \gcd(X'_n, X'_m) = 1 \) or a power of \( \sqrt{2} \).

**Lemma 2.10.** (Ding [4, Lemma 2.5]) For any given positive integers \( r \) and \( n \), we have

\[
\sum_{n \leq x} \phi(nr) = c(r)x + O(\log x),
\]

where \( c(r) = \prod_{p} \left(1 - \frac{\gcd(p, r)}{p^2}\right) > 0 \) and the implied constant depends on \( r \).
2.5. **Hill-Cipher.** The idea of the Hill cipher is to use matrices to encrypt blocks of characters by replacing a block of a small number of letters with another block of the same size. The Hill encryption scheme replaces \( n \) consecutive plaintext letters with \( n \) ciphertext letters. The matrix representation for plaintext \( A \), key matrix \( K \), and cipher text \( C \) are given as

\[
A = \begin{pmatrix} A_1 & A_2 & \cdots & A_m \end{pmatrix},
\]

\[
K = \begin{pmatrix} K_{1,1} & K_{1,2} & \cdots & K_{1,n} \\
K_{2,1} & K_{2,2} & \cdots & K_{2,n} \\
\vdots & \vdots & \ddots & \vdots \\
K_{n,1} & K_{n,2} & \cdots & K_{n,n} \end{pmatrix},
\]

\[
C = \begin{pmatrix} C_1 & C_2 & \cdots & C_m \end{pmatrix},
\]

where \( A_i \) and \( C_i \) are block matrices of size \( 1 \times n \). Thus the Hill cipher is described as follows:

For encryption

\[ \text{Enc}(A) : C_i \equiv A_i K \pmod{p}. \]

For decryption

\[ \text{Dec}(A) : A_i \equiv K^{-1} C_i \pmod{p}, \]

where \( p \) is a rational prime and \( \gcd(\det(K), p) = 1 \).

2.6. **Affine cipher.** An affine cipher of blocklength one is given by

\[ \text{Enc}(x_i) : y_i \equiv (ax_i + b) \pmod{26}, \]

where \( a, b \in \mathbb{Z}_{26} \). For decryption, we have to solve the function for \( x_i \). So that, \( a^{-1} \pmod{26} \) must exist, but \( b \) can be any element of \( \mathbb{Z}_{26} \).

2.7. **Affine-Hill Cipher.** Affine-Hill Cipher is a polygraphic block cipher that extends the concept of Hill cipher by using the following encryption and decryption techniques.

For encryption

\[ \text{Enc}(A) : C_i \equiv (A_i K + B) \pmod{p}. \]

For decryption

\[ \text{Dec}(A) : A_i \equiv (C_i - B) K^{-1} \pmod{p}, \]

where \( A_i, C_i, \) and \( B \) are \( 1 \times n \) matrices and \( K \) is \( n \times n \) key matrix. Here, \( p \) is prime greater than number of different characters used in plaintext.

2.8. **Key exchange Technique (ElGamal algorithm).** The ElGamal \([6, 7]\) cryptosystem can be constructed using any cyclic group in which the discrete-log problem is hard or believed to be hard. It will be broken if the discrete-log problem is solved. The cyclic group \( \mathbb{F}_p^\times \) can be a multiplicative group of integers modulo \( p \). In this technique, the global elements are the selected prime \( p \) and chosen primitive root modulo \( p \).
2.9. **Key Generation.** Choose a private key $G$ between 2 and $p - 2$ and select $g$ from primitive root modulo $p$, i.e., $g$ be the generator of $\mathbb{F}_p^\times$. Now we assign $E_1 = g$. Computes $E_2 = g^G \pmod{p}$. Suppose that Alice and Bob want to exchange key. Bob’s public key is $(p, E_1, E_2)$ and his private key is $G$.

2.9.1. **Enciphering Stage.**

1. Alice can access Bob’s public key $(p, E_1, E_2)$.
2. Alice chooses a random number $e$ such that $1 < e < p - 1$ and computes signature $k = E_1^e \pmod{p}$.
3. Computes secret key $s = E_2^e \pmod{p}$.
4. Calculates the cipher text $C = As \pmod{p}$.
5. Thus Alice can send encrypt message $(k, C)$ to Bob.

2.9.2. **Deciphering Stage.** Bob uses his secret key to compute $s$.

\[
\begin{align*}
s & \equiv (E_2^e) \pmod{p} \\
& \equiv (E_1^G)^e \pmod{p} \\
& \equiv (E_1^e)^G \pmod{p} \\
& \equiv k^G \pmod{p}.
\end{align*}
\]

Since both $k$ and $G$ are known to Bob, he can securely receive secret key $s$. Then by using Euclidean algorithm, $s^{-1}$ can be calculated. Thus, Bob will decrypt the cipher text $C$ and recover the plaintext $A = s^{-1}C$.

3. **Main Results**

Let $r \geq 2$ be a given fixed integer and let $n > 1$ be any integer. Let us take,

\[
\begin{align*}
X_{nr}' &= \gcd(X_{nr}, \Phi_{nr}(\alpha/\beta)), \\
Y_{nr}' &= \gcd(Y_{nr}, \Phi_{nr}(\alpha/\beta)).
\end{align*}
\]

The following theorem closely follows the proof of [18, Theorem 3.1]. For the purpose of completeness we give the proof.

**Theorem 3.1.** Assume that the abc conjecture for the number field $\mathbb{Q}(\sqrt{2})$ is true. Then for any $\varepsilon > 0$, $X_{nr}' \gg_{\varepsilon} B_{\phi(r)}^{\mathbb{Q}(\sqrt{2})-\varepsilon}$.
Proof. By the recursion formula (2.2) we write,
\[ \Phi_{nr}(\alpha/\beta) = \frac{B_{nr} \Phi_1(\alpha/\beta)}{\beta^{nr-1} \prod_{d|nr} \Phi_d(\alpha/\beta)}. \]

It follows that
\[ \Phi_{nr}(\alpha/\beta) | B_{nr} \alpha^{nr-1}. \]

That is,
\[ \Phi_{nr}(\alpha/\beta) | X_{nr} Y_{nr} \alpha^{nr-1}. \]

Since \( \alpha \) is a unit in \( \mathbb{Q}(\sqrt{2}) \), we have \( \Phi_{nr}(\alpha/\beta) \nmid \alpha \). Thus, \( \Phi_{nr}(\alpha/\beta) | X_{nr} Y_{nr} \).

As \( \gcd(X_{nr}, Y_{nr}) = 1 \), we obtain either \( \Phi_{nr}(\alpha/\beta) | X_{nr} \) or \( \Phi_{nr}(\alpha/\beta) | Y_{nr} \).

We suppose that \( \Phi_{nr}(\alpha/\beta) | X_{nr} \), it follows that
\[ X'_{nr} = \gcd(X_{nr}, \Phi_{nr}(\alpha/\beta)) = \Phi_{nr}(\alpha/\beta) \]
and \( Y'_{nr} = \gcd(Y_{nr}, \Phi_{nr}(\alpha/\beta)) = 1 \). Similar argument for \( \Phi_{nr}(\alpha/\beta) | Y_{nr} \) implies that \( X'_{nr} = 1 \) and \( Y'_{nr} = \Phi_{nr}(\alpha/\beta) \). For any of these cases, we finally get
\[ X'_{nr} Y'_{nr} = \Phi_{nr}(\alpha/\beta). \] (3.1)

By using Lemma 2.5 we write,
\[ |X'_{nr} Y'_{nr}| = |\Phi_{nr}(\alpha/\beta)| \geq C|\alpha/\beta|^\phi(nr) \]
\[ = C|\alpha^2|^\phi(n). \] (3.2)

Since \( \{B_{nr}\} \) is a sequence of positive integers, by using Lemma 2.7 we get,
\[ X'_{nr} Y'_{nr} \geq C\alpha^{2\phi(nr)} \]
\[ \geq C(\alpha^{\phi(r)})^{2\phi(n)} \]
\[ > CB^{2\phi(r)}. \] (3.7)

Now by combining Lemma 2.8 with equation (3.7), we obtain
\[ X'_{nr} B^{2r} \gg \varepsilon X'_{nr} Y_{nr} \geq X'_{nr} Y'_{nr} \gg \varepsilon B^{2\phi(n)} \]
\[ X'_{nr} \gg \varepsilon B^{2\phi(r)}/B_{nr}^{2\phi(r)} \]

After simplification we write,
\[ X'_{nr} \gg \varepsilon B^{2\phi(n) - \varepsilon}. \]

This completes the proof of Theorem 3.1. \( \square \)

Let us take \( T = \{ n : X'_{nr} > nr \} \) and \( T(x) = |T \cap [1, x]| \). The following lemma is an analogous result of [4 Lemma 2.6] for the balancing sequences.

Lemma 3.2. We have \( T(x) \gg x \), where the implied constant depends only on \( \alpha, r \).
Proof. Let \( R = \{ n : \phi(nr) > \frac{2c(r)}{3} nr \} \) and \( R(x) = |R \cap [1, x]| \).

By equation (3.5) we have,
\[
X'_{nr} Y'_{nr} \gg \alpha^{2\phi(nr)}.
\]

(3.8)

By using Lemmas 2.7 and 2.8 we obtain,
\[
Y'_{nr} \leq Y_{nr} \ll_{\epsilon} B_{nr}^{2\epsilon} < (a^{nr})^{2\epsilon}.
\]

(3.9)

On substituting equation (3.9) in (3.8) we get,
\[
X'_{nr} \gg \epsilon \alpha^{2(\phi(nr) - c(nr)/3)}.
\]

(3.10)

Let \( \epsilon = \frac{c(r)}{3} \) in (3.10) and we get \( X'_{nr} \gg r \alpha^{2(\phi(nr) - c(r)/nr/3)} \). For any \( n \in R \), we have \( \phi(nr) > \frac{2c(r)nr}{3} \). Therefore,
\[
X'_{nr} \gg r \alpha^{2(\phi(nr) - c(r)/nr/3)} > \alpha^{\frac{2c(r)nr}{3}} > nr.
\]

Therefore there exists an integer \( n_0 \) depending only on \( \alpha, r \) such that, if \( n \geq n_0 \) and \( n \in R \), then \( X'_{nr} > nr \). Hence we obtain,
\[
T(x) = \sum_{n \leq x} 1 \geq \sum_{n \leq x} 1 = \sum_{n \leq x} 1 = 1.
\]

Since we note that,
\[
\sum_{n \leq x} \frac{\phi(nr)}{nr} \leq \sum_{n \leq x} \frac{2c(r)}{3} \leq \frac{2c(r)}{3} x.
\]

(3.11)

Hence by Lemma 2.10 and equation (3.11) we obtain,
\[
T(x) \geq \sum_{n \leq x} \frac{\phi(nr)}{nr} \geq \sum_{n \leq x} \frac{\phi(nr)}{nr} \geq c(r)x + O(\log x) - \frac{2c(r)}{3} x \gg_{\alpha,r} x.
\]

This completes the proof of Lemma 3.2. \( \square \)
3.1. **Proof of Theorem 1.1.** The main idea of this theorem is to count number of primes $p$ such that $p$ divides $X'_{nr} \leq x$. For any $n \in T$, it follows that there exists an odd prime $p_n$ such that $p_n | X'_{nr}$ and $p_n \nmid nr$. Since $X'_{nr} | X_{nr}$ and $p_n | X'_{nr}$, by using Lemma 2.6 we obtain

$$B_{p_n - \left(\frac{n}{p_n}\right)} \not\equiv 0 \pmod{p_n^2}.$$

We note that $p_n | X'_{nr}$, $X'_{nr} | \Phi_{nr}(\alpha/\beta)$ and $p_n \nmid nr$. Therefore, by using Lemma 2.4 we obtain

$$p_n \equiv \pm 1 \pmod{nr}.$$

By Lemma 2.9 we get $p_n (n \in T)$ are distinct primes. Thus we find that,

$$\left|\{\text{primes } p \leq x : p \equiv \pm 1 \pmod{r}, B_{p_n - \left(\frac{n}{p_n}\right)} \not\equiv 0 \pmod{p_n^2}\}\right| \geq \left|\{n : n \in T, X'_{nr} \leq x\}\right|.$$ 

Since $X'_{nr} \leq X_{nr} \leq B_{nr} < \alpha^{nr}$, we write

$$\left|\{n : n \in T, X'_{nr} \leq x\}\right| \geq \left|\{n : n \in T, \alpha^{nr} \leq x\}\right|$$

$$= \left|\{n : n \in T, n \leq \frac{\log x}{r \log \alpha}\}\right|$$

$$= T\left(\frac{\log x}{r \log \alpha}\right).$$

Hence by Lemma 3.2 we conclude that,

$$\left|\{\text{primes } p \leq x : p \equiv \pm 1 \pmod{r}, B_{p_n - \left(\frac{n}{p_n}\right)} \not\equiv 0 \pmod{p_n^2}\}\right| \geq T\left(\frac{\log x}{r \log \alpha}\right) \gg_{\alpha, r} \log x.$$

### 4. Application to Cryptography

4.1. **Balancing Matrices.** Ray [16] introduced the balancing $Q_B$—matrix of order 2 whose entries are first three balancing numbers 0, 1, and 6 as follows:

$$Q_B = \begin{pmatrix} B_2 & -B_1 \\ B_1 & B_0 \end{pmatrix} = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix}$$

Without loss of generality, we interchange the diagonal elements, i.e.,

$$Q_{B_2} = \begin{pmatrix} B_0 & -B_1 \\ B_1 & B_2 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 6 \end{pmatrix}$$

The $n^{th}$ power of the balancing $Q_{B_2}$—matrix is

$$Q^n_{B_2} = \begin{pmatrix} -B_{n-1} & -B_n \\ B_n & B_{n+1} \end{pmatrix}$$

with $n > 0$.

The Cassini Formula [17] for balancing number is

$$B_n^2 - B_{n+1}B_{n-1} = 1. \quad (4.1)$$
Thus \( \det(Q^n_{B_2}) = 1 \) and \( Q^n_{B_2} \) is a non-singular matrix for all \( n \). Therefore inverse must exist.

\[
(Q^n_{B_2})^{-1} = Q^{-n}_{B_2} = \begin{pmatrix} B_{n+1} & B_n \\ -B_n & -B_{n-1} \end{pmatrix}
\]

We now extend the balancing \( Q_B \)-matrix of order 3,

\[
Q^n_{B_3} = \begin{pmatrix} -B_{n-1} & -B_n & 0 \\ B_n & B_{n+1} & 0 \\ \sum_{t=0}^{n-1} B_t & \sum_{t=1}^{n} B_t & 1 \end{pmatrix}
\]

with \( Q_{B_3} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 6 & 0 \\ 0 & 1 & 1 \end{pmatrix} \),

where \( n > 0 \). By continuing this process,

\[
Q_{B_s} = \begin{pmatrix} 0 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 6 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix}
\]

The \( \det(Q_{B_s}) = 1 \) guaranteed the existence of inverse.

Thus

\[
Q_{B_s}^{-1} = \begin{pmatrix} 6 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ -1 & -1 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ (-1)^{s-2} & 0 & (-1)^{s-4} & \cdots & 1 & 0 \\ (-1)^{s-1} & 0 & (-1)^{s-3} & \cdots & -1 & 1 \end{pmatrix}
\]

Now the \( n^{th} \) power of \( Q_{B_s} \) is

\[
Q^n_{B_s} = \begin{pmatrix} M_1 \\ M_2 \\ M_3 \end{pmatrix}
\]

here \( Q^n_{B_s} \) is a block matrix and its blocks are

\[
M_1 = \begin{pmatrix} -B_{n-1} & -B_n & 0 \\ B_n & B_{n+1} & 0 \\ \sum_{t=0}^{n-1} B_t & \sum_{t=1}^{n} B_t & 1 \end{pmatrix}
\]
Now, the inverse of \( Q_{B_x}^n \) is

\[
Q^{-n}_{B_x} = \begin{pmatrix}
M_1^{-1} & 0 \\
M_2^{-1} & M_3^{-1}
\end{pmatrix},
\]

where

\[
M_1^{-1} = \begin{pmatrix}
B_{n+1} & B_n & 0 \\
-B_n & -B_{n-1} & 0 \\
\sum_{t=1}^{n} B_t & \sum_{t=0}^{n-1} B_t & 1
\end{pmatrix},
\]

\[
M_2 = \begin{pmatrix}
B_0(n-1) + B_1(n-2) + \cdots + B_{n-2} & B_1(n-1) + B_2(n-2) + \cdots + B_{n-1} & \cdots & n \\
B_0 \left( \sum_{n>4} \frac{(n-3)(n-4)}{2} + \sum_{n>4} \frac{(n-3)(n-4)}{2} \right) + \cdots + B_{n-4} & B_1 \left( \sum_{n>3} \frac{(n-2)(n-3)}{2} + \cdots + B_{n-3} \right) + \sum_{n>2} \frac{(n-1)(n-2)}{2} \\
\vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0
\end{pmatrix}
\]

and \( 0 \) is a zero matrix of order \( 3 \times (s - 3) \).
4.2.1. Algorithm. Enciphering Stage:

- (nB_1 + B_2(n-1) + \ldots + B_n) - (nB_0 + B_1(n-1) + \ldots + 2B_{n-2} + B_{n-1}) = -n

\[
M_2^{-1} = \begin{pmatrix}
B_1 \frac{n(n+1)}{2} + B_2 \frac{(n-1)n}{2} \\
+ \cdots + 3B_{n-1} + B_n \\
- (B_1 \sum_{i=1}^{n} \frac{(n+1)!}{(n-i)!i!} + B_2 \sum_{i=2}^{n} \frac{(n-2)!}{(n-2-i)!i!} \\
+ \cdots + 4B_{n-1} + B_n)
\end{pmatrix}
\]

- (B_0 \sum_{i=1}^{n} \frac{n(n-1)n}{2} + B_1 \sum_{i=2}^{n} \frac{n(n-1)n}{2} + \cdots + B_{n-1}) - (\sum_1^n \frac{(n+1)n}{2})

\[
M_3^{-1} = \begin{pmatrix}
1 & 0 & 0 & 0 & \cdots & 0 \\
-(n-1) & 1 & 0 & 0 & \cdots & 0 \\
(n+1) & -(n-1) & 1 & 0 & \cdots & 0 \\
-(n+2) & (n+1) & -(n-1) & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \ddots & \ddots \\
(-1)^{s-1} \binom{s+n-2}{n-1} & (-1)^{s-2} \binom{s+n-3}{n-1} & \cdots & \cdots & \cdots & 1
\end{pmatrix}
\]

4.2. Key Exchange Technique. Assume that Alice and Bob want to exchange a key. Bob (the receiver) generates the components of the public key \( E_1 \) and \( E_2 \) using his private key (session key) \( G \). Thus, the public key is \( pk(p, E_1, E_2) \). With the help of this public key \( pk(p, E_1, E_2) \), the secret key \( s \) can be calculated (see [2.9.1]). Then the key matrix \( K \) can be constructed using the secret key \( s \).

4.2.1. Algorithm. Enciphering Stage:

(1) Alice chooses secret number \( e \) such that \( 1 < e < p - 1 \).

(2) Signature: \( k \leftarrow E_1^e \pmod{p} \).

(3) Secret key: \( s \leftarrow E_2^k \pmod{p} \).
Key matrix: \( K \leftarrow Q_{B_s}^k \), where \( Q_{B_s}^k \) is a generalized balancing matrix of order \( s \times s \).

Encryption: \( \text{Enc}(A) : C_i \leftarrow (A_iK + B) \pmod p \).

Exchange \((k, C)\) to Bob.

Deciphering Stage:
Bob after obtaining \((k, C)\),
(1) Secret Key: \( s \leftarrow k^G \pmod p \), where \( G \) is Bob’s secret key.

(2) Key Matrix: \( K \leftarrow Q_{B_s}^k \).

(3) Decryption: \( \text{Dec}(C) : A_i \leftarrow (C_i - B)K^{-1} \pmod p \).

4.3. Numerical Example. Assuming Alice wants to send a message to Bob, she would first compute the key matrix \( K \) with the help of the above algorithm \([2,1]\) and then encrypt the plaintext \( A \) by using key matrix \( K = Q_{B_s}^k \).

Example 4.1. Let \( p = 31 \) and let Bob’s private key \( G = 17 \). Suppose that Alice wants to send a plaintext \( A = \text{WELCOMEANNIE} \). Bob chooses (primitive root modulo 31) \( g \) as 3. Assume that \( g = E_1 \) and computes \( E_2 \equiv E_1^G \pmod p \equiv 3^{17} \pmod {31} = 22 \). Thus Bob’s public key \( pk(p, E_1, E_2) = (31, 3, 22) \) and secret key \( G = 17 \).

Encrypting Stage:
The plaintext \( A \) is WELCOMEANNIE and shifting vector is 
\[
B = (37 \ 17 \ 19 \ 13),
\]
At first, Alice chooses \( e = 24 \) and computes signature \( k \equiv 3^{24} \pmod {31} \equiv 2 \pmod {31} \). The secret key \( s \equiv E_2^e \pmod p \equiv 22^{24} \pmod {31} \equiv 4 \pmod {31} \). The key matrix \( K \) can be constructed using aforementioned data with help of generalized balancing matrix \( Q_{B_s}^k \).

i.e.,
\[
K = Q_{B_4}^2 = \begin{pmatrix}
-1 & -6 & 0 & 0 \\
6 & 35 & 0 & 0 \\
1 & 7 & 1 & 0 \\
0 & 1 & 2 & 1
\end{pmatrix}.
\]
The cipher text \( C \leftarrow AK + B \).
Now, the plaintext \( A \) can be divided into blocks.
i.e.,
\[
A_1 = (22 \ 4 \ 11 \ 2) ; \quad A_2 = (14 \ 12 \ 4 \ 0) ; \quad A_3 = (13 \ 13 \ 8 \ 4).
\]
\[ C_1 \equiv A_1K + B \pmod{31} \]
\[ \equiv \begin{pmatrix} 22 & 4 & 11 & 2 \end{pmatrix} \begin{pmatrix} -1 & -6 & 0 & 0 \\ 6 & 35 & 0 & 0 \\ 1 & 7 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix} + \begin{pmatrix} 37 & 17 & 19 & 13 \end{pmatrix} \pmod{31} \]
\[ \equiv (19 \ 11 \ 3 \ 15) \sim (T \ L \ D \ P) \]

\[ C_2 \equiv A_2K + B \pmod{31} \]
\[ \equiv \begin{pmatrix} 14 & 12 & 4 & 0 \end{pmatrix} \begin{pmatrix} -1 & -6 & 0 & 0 \\ 6 & 35 & 0 & 0 \\ 1 & 7 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix} + \begin{pmatrix} 37 & 17 & 19 & 13 \end{pmatrix} \pmod{31} \]
\[ \equiv (6 \ 9 \ 23 \ 13) \sim (G \ J \ X \ N) \]

\[ C_3 \equiv A_3K + B \pmod{31} \]
\[ \equiv \begin{pmatrix} 13 & 13 & 8 & 4 \end{pmatrix} \begin{pmatrix} -1 & -6 & 0 & 0 \\ 6 & 35 & 0 & 0 \\ 1 & 7 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix} + \begin{pmatrix} 37 & 17 & 19 & 13 \end{pmatrix} \pmod{31} \]
\[ \equiv (17 \ 20 \ 4 \ 17) \sim (R \ U \ E \ R) \]

Thus the cipher text \( C = (C_1C_2C_3) = (TLDPGJXNRUER) \). Alice now send this cipher text to Bob with her signature.

**Deciphering Stage:**
Bob can calculate decryption key \( K^{-1} \) with the help of secret key \( G \) and the signature \((k, B) = (2, (37 \ 17 \ 19 \ 13))\).

Thus
\[ s \equiv k^G \pmod{p} \]
\[ \equiv 2^{17} \pmod{31} \]
\[ \equiv 4 \pmod{31}. \]

\[ K^{-1} = Q_{B_4}^{-2} = \begin{pmatrix} 35 & 6 & 0 & 0 \\ -6 & -1 & 0 & 0 \\ 7 & 1 & 1 & 0 \\ -8 & -1 & -2 & 1 \end{pmatrix} \]
Now decryption is $A \leftarrow (C - B)K^{-1} \pmod{p}$

$A_1 \equiv (C_1 - B)K^{-1} \pmod{p}$

$= (19 \ 11 \ 3 \ 15) - (37 \ 17 \ 19 \ 13) \begin{pmatrix} 35 & 6 & 0 & 0 \\ -6 & -1 & 0 & 0 \\ 7 & 1 & 1 & 0 \\ -8 & -1 & -2 & 1 \end{pmatrix} \pmod{p}$

$= (22 \ 4 \ 11 \ 2) \sim (W \ E \ L \ C)$

$A_2 \equiv (C_2 - B)K^{-1} \pmod{p}$

$= (6 \ 9 \ 23 \ 13) - \begin{pmatrix} 35 & 6 & 0 & 0 \\ -6 & -1 & 0 & 0 \\ 7 & 1 & 1 & 0 \\ -8 & -1 & -2 & 1 \end{pmatrix} \pmod{p}$

$= (14 \ 12 \ 4 \ 0) \sim (O \ M \ E \ A)$

$A_3 \equiv (C_3 - B) \pmod{p}$

$= (17 \ 20 \ 4 \ 17) - (37 \ 17 \ 19 \ 13) \begin{pmatrix} 35 & 6 & 0 & 0 \\ -6 & -1 & 0 & 0 \\ 7 & 1 & 1 & 0 \\ -8 & -1 & -2 & 1 \end{pmatrix} \pmod{p}$

$= (13 \ 13 \ 8 \ 4) \sim (N \ N \ I \ E)$

Hence, Bob decipher the plaintext WELCOMEANNIE.

4.4. **Strength and security analysis.** We are working in the special linear group $SL_s(F_p)$ of degree $s$ over a field $F_p$, which consists of all invertible matrices of order $s \times s$ over $F_p$. Thus the order of $SL_s(F_p)$ is

$$1/(p-1)(p^s-1)(p^s-p)(p^s-p^2)\ldots(p^s-p^{s-1}).$$

It is more difficult to break the scheme due to the order of the key matrix and its large power $k$.

**Example 4.2.** Consider the key matrix $K = O_{B_{15}}^{17}$ over a field $F_{31}$. That is, $s = 15$ and $p = 31$. Thus the cardinality of invertible matrices with determinant 1 of order 15 × 15 over $F_{31}$ is

$$|SL_{15}(F_{31})| = 1/(31-1)(31^{15}-1)(31^{15}-31)(31^{15}-31^2)\ldots(31^{15}-31^{14})$$

$$= 1.160251664216324177237764 \times 10^{334}.$$ 

In this case, we need to check $10^{334}$ invertible matrices with determinant 1. It is impossible, if we deal with huge order $s$. 

Remark 4.3. The time complexity of matrix multiplication in worst case is $O(n^3)$, where $O$ represents big $O$ notation \[10\]. But in the case of generalized balancing matrices the time complexity reduces to $O(n)$.

5. Conclusions

In this paper, we consider balancing sequences and prove that under the assumption of the $abc$ conjecture for the number field $\mathbb{Q}(\sqrt{2})$, there are at least $O(\log x)$ as many balancing non-Wieferich primes $p$ such that $p \equiv \pm 1 \pmod{r}$ for any fixed integer $r \geq 2$.

Further, we suggest a public key cryptosystem using Affine-Hill cipher and generalized balancing matrix $Q_{B_s}^k$ with a large power $k$. We propose a key formation (i.e., exchange of the key matrix $K = Q_{B_s}^k$, of order $s \times s$ for the encryption-decryption scheme with the help of balancing sequences under prime modulo). In this scheme, instead of exchanging key matrix, we simply exchange a pair of numbers $(s, k)$, which results in a wide-key space and lower time and space complexity.

Acknowledgement. The author I. Muntaj Fathima would like to express her gratitude to Maulana Azad National Fellowship for minority students, UGC. This research work is supported by MANF-2015-17-TAM-56982, University Grants Commission (UGC), Government of India.

References

[1] A. Behera, G. K. Panda, *On the square roots of triangular numbers*, Fibonacci Quart., 37 (1999), 98–105.
[2] Yu. Bilu, G. Hanrot, P. M. Voutier (with an appendix by M. Mignotte), *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math., 539 (2001), 75–122.
[3] Y.-G. Chen, Y. Ding, *Non-Wieferich primes in arithmetic progressions*, Proc. Amer. Math. Soc., 145 (2017), 1833–1836.
[4] Y. Ding, *Non-Wieferich primes under the abc conjecture*, C. R. Math. Acad. Sci. Paris, 357 (2019), no. 6, 483–486.
[5] U. K. Dutta, B. K. Patel, P. K. Ray, *Balancing non-Wieferich primes in arithmetic progressions*, Proc. Indian Acad. Sci. (Math. Sci.), 129 (2019), no. 2, Paper No. 21.
[6] T. ElGamal, *A public key cryptosystem and signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, 31 (1985), 469–472.
[7] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms in advances in Cryptology-CRYPTO ’84*, Springer-Verlag, Berlin, LNCS 196 (1985), 10–18.
[8] H. Graves, M. Ram Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, J. Number Theory., 133 (2013), 1809–1813.
[9] K. Győry, *On the abc conjecture in algebraic number fields*, Acta Arith., 133 (2008), no. 3, 281–295.
[10] N. Koblitz, *A course in number theory and cryptography*, 2nd ed., Springer-Verlag, New York, 1994.
[11] D. W. Masser, *Open problems. In: W. W. L. Chen (ed.) Proceedings of the Symposium on analytic number theory*, Imperial College, London, 1985.
[12] J. Oesterlé, *Nouvelles approches du “théorème” de Fermat (French)*, Séminaire Bourbaki, Astérisque No. 161-162 (1988), Exp. No. 694, 165–186.
[13] G. K. Panda, S. S. Rout, *Periodicity of balancing numbers*, Acta Math. Hungar., 143 (2014), no. 2, 274–286.
[14] K. Prasad, H. Mahato, Cryptography using generalized Fibonacci matrices with Affine-Hill cipher, Journal of Discrete Mathematical Sciences and Cryptography, (2021), 1–12. https://doi.org/10.1080/09720529.2020.1838744

[15] M. Ram Murty, Problems in analytic number theory. 2nd ed., Graduate texts in mathematics, 206, Springer, New York, 2008.

[16] P. K. Ray, Certain matrices associated with balancing and Lucas-balancing numbers, Matematika, 28 (2012), no. 1, 15–22.

[17] P. K. Ray, G. K. Dial, B. K. Patel, Application of some recurrence relations to cryptography using finite state machine, International Journal of Computer Science and Electronics Engineering, 2 (2014), no. 4, 220–223.

[18] S. S. Rout, Balancing non-Wieferich primes in arithmetic progression and abc conjecture, Proc. Japan Acad. Ser. A Math. Sci., 92 (2016), no. 9, 112–116.

[19] J. H. Silverman, Wieferich’s criterion and the abc-conjecture, J. Number Theory., 30 (1988), 226–237.

[20] C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, III, J. London Math. Soc., 28 (1983), no. 2, 211–217.

[21] P. Sundarayya, G. V. Prasad, A public key cryptosystem using affine Hill cipher under modulation of prime number, Journal of information & optimization Sciences, 40 (2019), no. 4, 919–930.

[22] M. K. Viswanath, M. Ranjith Kumar, A public key cryptosystem using Hill’s cipher, Journal of Discrete Mathematical Sciences and Cryptography, 18 (2015), no. 1-2, 129–138.

[23] P. Vojta, Diophantine approximations and value distribution theory. Lecture notes in mathematics, 1239, Springer, Berlin, 1987.

[24] Y. Wang, Y. Ding, A note on balancing non-Wieferich primes, J. Anhui Norm. Univ. Nat. Sci., 43 (2020), no. 2, 129–133.

[25] A. Wieferich, Zum letzten Fermat’schen Theorem (German), J. Reine Angew. Math., 136 (1909), 293–302.

(1) DEPARTMENT OF MATHEMATICS, SRM IST RAMAPURAM, CHENNAI 600089, INDIA
(2) RESEARCH SCHOLAR, DEPARTMENT OF MATHEMATICS, SRI VENKATESWARA COLLEGE OF ENGINEERING, AFFILIATED TO ANNA UNIVERSITY, SRIPERUMBUDUR, CHENNAI 602117, INDIA
(3) DEPARTMENT OF MATHEMATICS, SRI VENKATESWARA COLLEGE OF ENGINEERING, SRIPERUMBUDUR, CHENNAI 602117, INDIA

Email address: (1) subramanianitha@yahoo.com
Email address: (2) tbm.fathima@gmail.com
Email address: (3) avijaya@svce.ac.in