P
I
M
S

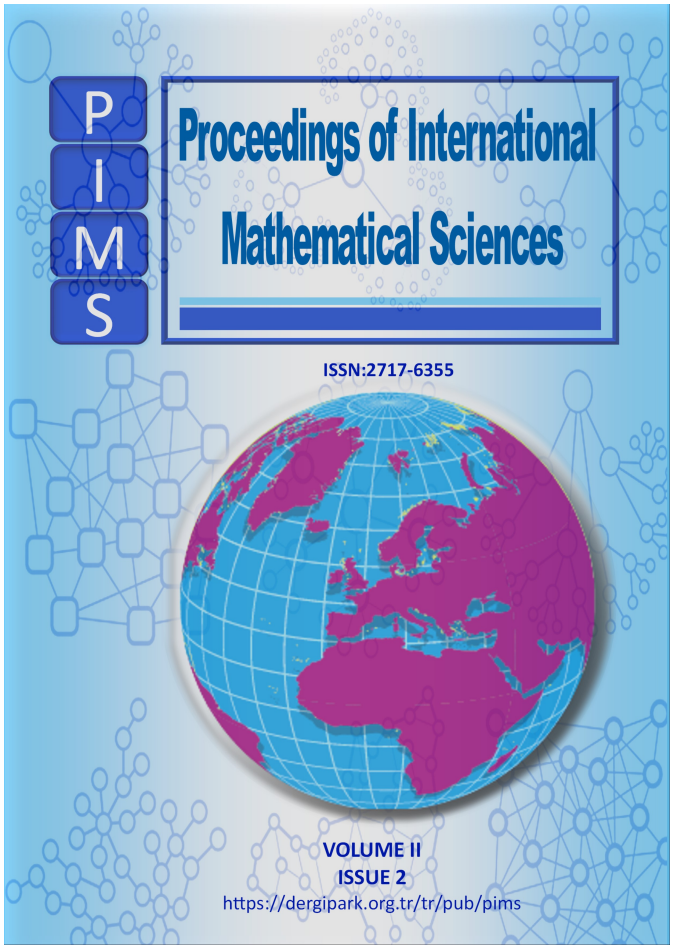
# Proceedings of International Mathematical Sciences

ISSN:2717-6355

VOLUME II
ISSUE 2
https://dergipark.org.tr/tr/pub/pims

VOLUME II ISSUE 2 December 2020
https://dergipark.org.tr/tr/pub/pims
ISSN:2717-6355

# PROCEEDINGS OF INTERNATIONAL MATHEMATICAL SCIENCES



## Editor-in-Chief

Hüseyin Çakallı
Maltepe University, Istanbul, Turkey
hcakalli@gmail.com

## Managing Editor

Fuat Usta
Düzce University, Düzce, Türkiye
fuatusta@duzce.edu.tr

## Editorial Board

---

## Publishing Board

---

# Contents

Proceedings of International Mathematical Sciences
ISSN:2717-6355, URL:https://dergipark.org.tr/tr/pub/pims
Volume II Issue 2 (2020), Pages 79-89. Doi: 10.47086/pims.827611

# THE HASSE-MINKOWSKI THEOREM AND LEGENDRE'S THEOREM FOR QUADRATIC FORMS IN TWO AND THREE VARIABLES

PHUC NGO*, MEHMET DIK**
*BELOIT COLLEGE, BELOIT, WI 53511, U.S.A ORCID NUMBER: 0000-0002-9658-4877
**BELOIT COLLEGE, BELOIT, WI 53511, U.S.A. ORCID NUMBER: 0000-0003-0643-2771

Abstract. Determining the solvability of equations has been an extended and fundamental study in Mathematics. The local-global principle states two objects are equivalent globally if and only if they are equivalent locally at all places. By applying this principle, the Hasse - Minkowski theorem is able to identify the existence of rational solutions of an equation. This paper explores the applications of the Hasse-Minkowski theorem to homogeneous quadratic forms in two and three variables. After providing some of the necessary proofs and definitions, we have been able to introduce some complete computer programs implementing the Hasse-Minkowski theorems and Legendre theorem with some supporting functions like the Eratosthenes sieve.

## 1. binary and ternary quadratic form

What follows has been inspired by *The Hasse-Minkowski Theorem in Two and Three Variables* by Hoehner, S [1].
A quadratic form is a polynomial with all the terms of degree two. The 2-variable quadratic form, which is also called binary form, has the following general form:

$$q(x, y) = ax^2 + bxy + cy^2. \tag{1.1}$$

Similarly, the 3-variable quadratic form is called the ternary form and has the general form of:

$$q(x, y, z) = ax^2 + bxy + cy^2 + dyz + ez^2 + fxz. \tag{1.2}$$

**Theorem 1.1.** *Every quadratic form q in n variables over a field of characteristic not equal to 2 is equivalent to a diagonal form:*

$$q(x) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2. \tag{1.3}$$

Since the general form is equivalent to diagonal form, we only need to consider the diagonal form to determine the integral solvability. Hence, we just need to look

2020 *Mathematics Subject Classification.* Primary: 11C04; Secondaries: 11C00.
*Key words and phrases.* Hasse-Minkowksi; quadratic form; algorithm.

Submitted on August 08th, 2020. Published on 12.30.2020. Communicated by Ahmet Mesut RAZBONYALI.

at the equations of form $q(x, y) = ax^2 + by^2$ for the binary case and $q(x, y) = ax^2 + by^2 + cz^2$, where a, b and c are integers.
Consider the binary diagonal form. If we have any rational coefficient, by the homogeneity of the equation $g(x, y) = 0$, we could clear the denominators to obtain an equation with integral coefficients. We also claim that the greatest common divisor of $a$ and $b$ is 1. Given that $gcd(a, b) = g$ and $g > 1$, we could divide $ax^2 + by^2 = 0$ by $g$ to get $q(x, y) = \frac{a}{g}x^2 + \frac{b}{g}y^2$ and obtain $gcd(\frac{a}{g}, \frac{b}{g}) = 1$.
Also, we assume that $a$ and $b$ are square-free. If $a$ is not square-free, $a = a's^2$, where $a'$ is an integer. Then, we have $a = ax^2 + by^2 = a'(sx)^2 + by^2 = 0$ . We could repeat the same process to clear all the squares from a and b which eventually leads to square-free coefficients.
Finally, we claim that $ab < 0$. If $ab = 0$, either one or both of the coefficients is 0 and we could not obtain a non-trivial solution. And, if $ab > 0$, the equation $f(x, y) = ax^2 + by^2$ will not have any solution since it would be either negative or positive.
Similarly, following the same reasoning, we get pairwise relatively prime, square-free coefficients for ternary form.

## 2. MODULAR ARITHMETIC

**Definition 2.1.** *An integer is called a quadratic residue modulo n if there exists an integer x such that*

$$x^2 \equiv q \ (mod\ n). \tag{2.1}$$

Due to the Legendre symbol, we could speed up the process of determining if a number is a quadratic residue modulo an odd prime. The Legendre symbol is defined as below.

**Definition 2.2.** *The Legendre symbol is a function of a and p, where p is an odd prime, defined as:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a non-quadratic residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases} \tag{2.2}$$

In addition, the Legendre symbol has the following properties:

(1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
(2) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
(4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
(5) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)\cdot(q-1)}$.

For the proof of above Legendre symbol properties, see pages 99, 100 and 102 in [3].
Furthermore, if an odd integer $n$ has the prime factorization of $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and

any integer $a$, we have a generalization of the Legendre symbol called the Jacobi symbol, stating that:

$$\left(\frac{a}{1}\right) = 1 \tag{2.3}$$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_k}\right)^{\alpha_k}. \tag{2.4}$$

Similar to the Legendre symbol, the Jacobi symbol also has some properties that we use to prove the Hasse-Minkowski theorem:

(1) $\left(\frac{a_1a_2}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right)$
(2) If $a_1 \equiv a_2 \pmod{n}$, then $\left(\frac{a_1}{n}\right) = \left(\frac{a_2}{n}\right)$
(3) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
(4) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$
(5) If $gcd(a,n) = 1$, then $\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{1}{4}(a-1)\cdot(n-1)}$

## 3. The Hasse-Minkowski theorem for binary forms

In order to prove the Hasse-Minkowski theorem for binary forms, we need the following theorems.

**Theorem 3.1.** *The Chinese Remainder Theorem. Suppose $n_i$ are pairwise coprime and $a_1$, $a_2$,...,$a_k$ is any sequence of integers, then there exists an integer $x$ such that:*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned} \tag{3.1}$$

*and the solution $x$ is unique modulo $n$, where $n = \prod_{i=1}^{k} n_i$.*

**Theorem 3.2.** *Suppose $a$ is an integer, $b$ is a natural number, and let $b = \prod_{i=1}^{n} p_i^{\varepsilon_i}$ be the prime factorization of $b$. Then $a$ is a quadratic residue modulo $b$ if and only if $a$ is a quadratic residue modulo $p_i^{\varepsilon_i}$ for $i = 1, \ldots, n$.*

*Proof for Theorem 3.2.* Suppose $a$ is a quadratic residue modulo $b$. We then have $a \equiv x^2 \pmod{b}$ for some integer $x$. Since $p_i^{\varepsilon_i} \mid b$, we also have $a \equiv x^2 \pmod{p_i^{\varepsilon_i}}$.
To prove the order direction, if $a$ is a quadratic residue modulo $p_i^{\varepsilon_i}$, we have $a \equiv x^2 \pmod{p_i^{\varepsilon_i}}$, if $j \neq k$, $gcd(p_j^{\varepsilon_j}, p_k^{\varepsilon_k})$. Thus, we could apply the Chinese Remainder Theorem to the congruences $x \equiv x_i \pmod{p_i^{\varepsilon_i}}$ where $i = 1, \ldots, n$. Obtaining $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{\varepsilon_i}}$ from the Chinese Remainder theorem, we thus have $x^2 \equiv a \pmod{\prod_{i=1}^{n} p_i^{\varepsilon_i}}$ or $a$ is a quadratic residue modulo $b$.

**Theorem 3.3.** *Dirichlet's Theorem on Arithmetic Progressions. For any two positive coprime integers $a$ and $d$, there are infinitely many primes of the form $a + nd$, where $n$ is also a positive integer*

**Theorem 3.4.** *The congruence $x^2 \equiv a \pmod{p}$ is solvable for every prime $p$ if and only if $a = b^2$ for some $b \in \mathrm{Z}$.*

*Proof for Theorem 3.4.* Suppose $a = b^2$ for some $b$, we have $x^2 \equiv a \equiv b^2 \pmod{p}$. Therefore, for all prime $p$, we have a solution $x \equiv b \pmod{p}$.
To prove the other direction, we try to prove an equivalent statement "if $a \neq b^2$ for some $b$, $a$ is not a quadratic residue modulo for every prime $p$."
Suppose $a$ is a positive non-square. Then, if $a = 2$, we could just choose $p = 5$ and apply property 4 from the Legendre symbol to get $\left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$. Otherwise, $a$ could be factored into $p_1 p_2 \dots p_k$ for $p_1, \dots, p_k$ prime. Also, $a$ has an odd prime divisor $p_k$. Now we choose a prime such that $p \equiv 1 \pmod{8}$, $p \equiv 1 \pmod{p_i}$ for $i = 1, 2, \dots, k-1$ and $p \equiv a \pmod{p_k}$. Such a prime number $p$ exists according to Theorem 3.3. Then, since $p_k$ is not a quadratic residue modulo $p$, $a$ is not a quadratic non residue modulo $p$. Thus, we have proved Theorem 3.4 for the case where $a$ is positive.
If a number is negative, it is not a square. We present all negative numbers in the form of $-a$ where $a$ is a positive integer. Let $p$ be a prime number and apply property 1 from the Legendre symbol to get $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$. We then apply property 3 to obtain $\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right)$. If $a$ is a square, we can choose $p = 3$ to get $(-1)^{\frac{3-1}{2}}\left(\frac{a}{p}\right) = (-1) \cdot 1 = -1$. If $a$ is a non square, we choose $p = 5$ to obtain $(-1)^{\frac{5-1}{2}}\left(\frac{a}{p}\right) = 1 \cdot (-1) = -1$.

**Theorem 3.5.** *The Hasse-Minkowski Theorem 1. Let $a$ and $b$ be nonzero, square-free, relatively prime integers of opposite signs. If for each prime $p$ the congruence $ax^2 + by^2 \equiv 0 \pmod{p}$ has a solution in integers $(x, y)$ both not divisible by $p$, then $ax^2 + by^2 = 0$ has a nontrivial integral solution.*

Consider the first case where $p \nmid ab$, we claim that $gcd(x, p) = 1$. We can prove this statement by using contradiction. Suppose $gcd(x, p) > 1$, then we have $p \mid x$. Hence, $ax^2 + by^2 \equiv by^2 \equiv 0 \pmod{p}$. Also, we could see that either $p \mid b$ or $p \mid y$. Since we assume that $p \nmid ab$, we have $p \mid y$. Now that we have $p \mid x$ and $p \mid y$, this contradicts our assumption that the solution $(x, y)$ to nontrivial modulo $p$, establishing our claim that $gcd(x, p) = 1$. Now, from $ax^2 + by^2 \equiv 0 \pmod{p}$, we have $ax^2 \equiv -by^2 \pmod{p}$ and by multiplying the congruence on both sides by $-b$, we obtain $-bax^2 \equiv (by)^2 \pmod{p}$. Since $gcd(x, p) = 1$, we could divide $-bax^2 \equiv (by)^2$ by $x^2$ to obtain $-ba \equiv (\frac{by}{x})^2$. Thus, $-ba$ is a quadratic residue modulo $p$ for all $p \nmid ab$. Now, assume $p \mid ab$. We have $-ab \equiv 0^2 \pmod{p}$, therefore $-ab$ is a quadratic residue modulo $p$ for all $p \mid ab$.
Thus, $-ba$ is a quadratic residue modulo for all primes $p$. According to Theorem 3.4, we have $-ba = d^2$ for some integer $d$. Plugging the pair of integer $(b, d)$ into $f(x, y)$, we obtain $f(b, d) = ab^2 + bd^2 = ab^2 + b(-ab) = 0$. Hence, we have found a nontrivial integral solution to equation $f(x, y) = 0$.

## 4. THE HASSE-MINKOWSKI THEOREM FOR TERNARY FORMS

**Theorem 4.1.** *Legendre's Theorem. Suppose $a$, $b$, $c$ are non-zero square-free, pairwise relatively prime integers not all of the same sign. Then the equation $ax^2 + by^2 + cz^2 = 0$ has a non-trivial solution if and only if the following conditions are satisfied: (i) $-bc$ is a quadratic residue modulo $|a|$, (ii) $-ab$ is a quadratic residue modulo $|c|$, and (iii) $-ac$ is a quadratic residue modulo $|b|$.*

**Definition 4.1.** *Let $(x_0, y_0, z_0)$ be a nontrivial integral solution to the congruence $ax^2 + by^2 + cz^2 \equiv 0$ (mod p), and at most one of $x_0, y_0, z_0$ is divisible by p, then we call $(x_0, y_0, z_0)$ a p-focused solution.*

**Theorem 4.2.** *Hasse-Minkowski 2. Let $a$, $b$, $c$ be nonzero, square-free, pairwise relatively prime integers not all the same sign. If for each odd prime $p \mid abc$ the congruence $ax^2 + by^2 + cz^2 \equiv 0$ (mod m) has a p-focused solution in integers ($x$, $y$, $z$), then $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integral solution.*

*Proof for theorem 4.2.* Let $p$ be an odd prime, $p \mid a$ and $f(x, y, z) \equiv 0 \pmod{p}$ has a $p$-focused solution. According to Theorem 3.2, to prove $-bc$ is a quadratic residue modulo $|a|$, it suffices to show $-bc$ is a quadratic residue modulo $p$ for all $p \mid a$.

Suppose $(x_0, y_0, z_0)$ is a $p$-focused solution to the congruence. Since $p \mid a$, we have $by_0^2 + cz_0^2 \equiv 0 \pmod{p}$. If $p = 2$ or $p \mid bc$, we have $-bc \equiv 0 \pmod{p}$ and it is a quadratic residue modulo $p$. If $p \nmid bc$, we obtain $\gcd(b, p) = \gcd(c, p) = 1$. We also know that at most one of $x_0, y_0, z_0$ is divisible by $p$. First, suppose $p$ doesn't divide $x_0$, $y_0$ or $z_0$. We have

$$-by_0^2 \equiv cz_0^2 \pmod{p}. \tag{4.1}$$

Divide both sides by $z_0^2$ to get

$$-b(y_0 z_0^{-1})^2 \equiv c \pmod{p}. \tag{4.2}$$

Multiply both sides by $-b$ to obtain

$$-bc \equiv (by_0 z_0^{-1})^2 \pmod{p}. \tag{4.3}$$

Now suppose p divides exactly one of $x_0$, $y_0$, $z_0$. In the case where $p \mid x_0$, we are done. Suppose $p \mid y_0$ and $p \nmid z_0$, we have

$$cz_0^2 \equiv 0 \pmod{p}. \tag{4.4}$$

Divide both sides by $z_0$ to get

$$c \equiv 0 \pmod{p}. \tag{4.5}$$

Multiply both sides by $-b$ to obtain

$$-bc \equiv 0 \pmod{p}. \tag{4.6}$$

So, we have $-bc$ a quadratic modulo $p$. Hence, $-bc$ is a quadratic residue modulo $p$. The case where $p \mid z_0$ and $p \nmid y_0$ could be proved using a similar procedure. Since the congruence $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a $p$-focused solution for all $p \mid a$, we have $-bc$ a quadratic residue modulo $|a|$. Similarly, we can determine that $-ac$ is a quadratic residue modulo $|b|$ and $-ab$ is a quadratic modulo $c$.

We do not need to consider the case where $p$ is even or $p = 2$ since $-bc$, $-ac$, $-ad$

are either odd and even. Thus, they are congruent to 0 or 1 modulo 2 and both 0 and 1 are squares.
Finally, we need to show that if $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a $p$-focused solution for all odd $p \mid abc$, then $f(x, y, z) = 0$ has a nontrivial integral solution. Since $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a $p$-focused solution for all odd $p \mid abc$, it has a $p$-focused solution for all odd $p \mid a$, $p \mid b$ and $p \mid c$. We can also determine that $-bc$ is a quadratic residue modulo $|a|$, $-ac$ is a quadratic residue modulo $|b|$, $-ab$ is a quadratic residue modulo $|c|$. Hence, according to the Legendre's Theorem, the equation $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integral solution.

## 5. HASSE-MINKOWSKI AND LEGENDRE THEOREM IMPLEMENTATION

Let $f(x, y, z) = ax^2 + by^2 + cz^2$. Obviously, since checking whether a congruence $f(x, y, z) \equiv 0 \pmod{p}$ has a $p$-focused solution is a tedious task in real life, especially when $abc$ has a lot of prime factors or when $a$, $b$, $c$ are large, we could write a computer program to check it.

**Eratosthenes Sieve**

Eratosthenes Sieve is an old algorithm used to rapidly identify all the primes to a certain limit. The program first gets the integers $a$, $b$ and $c$ from the keyboard. Then, it creates the Eratosthenes sieve of primes that are odd and divide $abc$. The code below is the modified Eratosthenes sieve function written in C++.
The parameter *upperBound* is the maximum number which we would check if it is a prime number. The program always calls the function with $upperBound = abc$. Then, we create a bitset, a data structure that stores bits, named *flag*. Suppose $i$ is a number from 2 to *upperBound*, given that $flag[i] = 1$, then $i$ is prime, and vice versa. Next, we reset our bitset which would set all the value of *flag* to 1. Our first loop iterates from 2 to *upperBound* and for every number, if *flag[i]* $= 1$. Next, we process the second loop that iterates every multiple of that prime number to *upperBound*. For every multiples of that prime, we set the corresponding $flag$ value to 0 since the multiple of a prime can not be a prime. After the second loop, we would append our prime to a vector named *primes* to store it.

**Function.** *sieve*(*upperBound*)

**Pseudocode**

Input. *upperBound*, the maximum number to check if it is a prime number.
Determine. Every prime less than or equal to $upperBound + 1$.

```
(1)  primes ← an empty dynamic array, flag ← an bitset
(2)  upperBound ← |upperBound|
(3)  for i ← 0 to 1000009
(4)     flag_i ← 1
(5)  for i ← 2 to upperBound + 1
(6)     if flag_i = 1
(7)        j ← 2i
(8)        while j <= sievesize
(9)           flag_j ← 0
(10)       if i ≠ 2 and flag_i ≡ 0 (mod upperBound)
(11)          append i to primes
```

**C++ Implementation**

```
bitset<10000010> flag;
vector<int> primes;
int a, b, c;

void sieve(long upperBound) {
    upperBound = abs(upperBound);
    flag.set();
    flag[0] = flag[1] = 0;
    for (long long i = 2; i <= upperBound; i++)
        if (flag[i]) {
            for (long long j = i * i; j <= upperBound; j += i) flag[j] = 0;
            if(i != 2 && upperBound % i == 0) primes.push_back((int)i);
        }
}
```

**The Hasse-Minkowski Theorem 2**

Suppose $p$ is a prime that divides $abc$. To check for $p$-focused solution, we write a boolean method, *pFocusedCheck*, with parameter *primes*, the prime to check. *pFocusedCheck* has three loops that create every combination of $x$, $y$, $z$, where $x$, $y$, $z$ are integer and less than *primes*. For every combination, if it is a *primes*-focused solution we immediately return true. After it finishes three loops, we would haven't found a *primes*-focused solution, thus return false.

**Function.** *pFocusedCheck*(*prime*)

**Pseudocode**

Input. *primes*, the prime number to look for a *primes*-focused solution to the congruence.

Output. Return true if there is a *primes*-focused solution, otherwise returns false.

(1) $x \leftarrow$ an int, $y \leftarrow$ an int, $z \leftarrow$ an int
(2) for $x \leftarrow 0$ to $prime - 1$
(3) for $y \leftarrow 0$ to $prime - 1$
(4) for $z \leftarrow 0$ to $prime - 1$
(5) if $ax^2 + by^2 + cz^2 \equiv 0 \pmod{primes}$ and at most one of $x$, $y$, $z$ is divisible by *primes*.
(6) return true
(7) return false

**C++ Implementation**

```
bool pFocusedCheck(int prime){
    int x, y, z;
    for(x = 0; x < prime; ++x){
        for(y = 0; y < prime; ++y){
            for(z = 0; z < prime; ++z){
                if((((a * (x * x))  + (b * (y * y)) + (c * (z * z))) % prime == 0)
                   && (((x % prime) == 0) + ((y % prime) == 0) + ((z % prime) == 0) <= 1)){
                    return true;
                }
            }
        }
```

```
    }
    return false;
}
```

Then, we create a function named $HasseMinkowski2Check$ that loops through the *sieve* vector to check whether the congruence $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a $p$-focused solution. The function returns true if the congruence has a $p$-focused solution to every $p$, otherwise, returns false.

**Function.** $HasseMinkowski2Check()$

**Pseudocode**

Output. Returns true if for every $p$, the congruence $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ has a $p$-focused solution, otherwise, returns false.

(1) for every prime in *primes*
(2) if not *pFocusedCheck*(prime)
(3) return false
(4) return true

### C++ Implementation

```
bool HasseMinkowski2Check(){
    for(int i = 0; i < primes.size(); ++i){
        if(!pFocusedCheck(primes[i])){
            return false;
        };
    }
    return true;
}
```

**Legendre's Theorem.**

Initially, we want to implement the Legendre's symbol. We define *LegendreSymbol* function with two parameters, *toCheck* and *modulo*. The function returns 0 if *toCheck* $\equiv 0 \pmod{modulo}$ and returns 1 if there exists an $x$ such that $x^2 \equiv$ *toCheck* $\pmod{modulo}$, elsewise returns -1.

First, if *toCheck* $\equiv 0 \pmod{modulo}$, the function immediately returns 0. Next, if *toCheck* is negative, applying property 1 and 3 of the Legendre symbol, we can calculate $\left(\frac{-1}{p}\right)$ and save the result to a variable named *offset*. Otherwise, *offset* is set as 1. We, then, apply property 2 of the Legendre symbol to make *toCheck* less than *modulo*. Now, we make a loop that iterates from 1 to $modulo - 1$. If there exists a number $i$ in that range such that $i^2 \equiv$ *toCheck* $\pmod{modulo}$, we return $1 \cdot$*offset*. Otherwise, after finishing the loop, we return $-1 \cdot$*offset*

**Function.** *LegendreSymbol()*

**Pseudocode**

Input. *toCheck*, the number to check if it is a quadratic residue
*modulo*, the modulo

Output. Returns 0 if *toCheck* $\equiv 0 \pmod{modulo}$ and returns 1 if *toCheck* is a quadratic residue modulo *modulo*, elsewise returns -1.

(1) if *toCheck* $\equiv 0 \pmod{modulo}$
(2) return 0
(3) if *toCheck* $< 0$

(4) $offset \leftarrow -1^{\frac{modulo-1}{2}}$
(5) else $offset \leftarrow 1$
(6) $toCheck \leftarrow |toCheck|$
(7) while $toCheck > modulo$
(8) $toCheck \leftarrow toCheck \bmod modulo$
(9) for $i \leftarrow 1$ to $modulo$
(10) if $i^2 \equiv toCheck \pmod{modulo}$
(11) return $1 \cdot offset$
(12) return $-1 \cdot offset$

### C++ Implementation

```
int LegendreSymbol(int toCheck, int modulo){
    if(toCheck % modulo == 0) return 0;
    int offset = (toCheck < 0) ?  (int)(pow(-1, (modulo - 1) / 2)) : 1;
    toCheck = aflag(toCheck);
    while (toCheck > modulo){
        toCheck %= modulo;
    }

    for(int i = 1; i < modulo; ++i){
        if((i * i) % modulo == toCheck) return 1 * offset;
    }
    return -1 * offset;
}
```

Next, we only need to to write the Legendre theorem function. We will name it *LegendreCheck*.

**Function.** *LegendreCheck()*

**Pseudocode**

Output. return true if $-bc$ is a quadratic residue modulo $|a|$, $-ab$ is a quadratic residue modulo $|c|$ and $-ac$ is a quadratic residue modulo $|b|$. Otherwise, return false.

(1) bool $ans$
(2) temp $\leftarrow LegendreSymbol(-b * c, abs(a))$
(3) $ans \leftarrow temp = 0$ or $temp = 1$
(4) temp $\leftarrow LegendreSymbol(-a * b, abs(c))$
(5) $ans \leftarrow (temp = 0$ or $temp = 1)$ and $ans$
(6) temp $\leftarrow LegendreSymbol(-a * c, abs(b))$
(7) $ans \leftarrow temp = 0$ or $temp = 1$ and $ans$
(8) reuturn $ans$

### C++ Implementation

```
bool LegendreCheck(){
    int temp = LegendreSymbol(-b * c, abs(a));
    bool ans = (temp == 0 || temp == 1);
    temp =  LegendreSymbol(-a * b, abs(c));
    ans &= (temp == 0 || temp == 1);
    temp = LegendreSymbol(-a * c, abs(b));
```

```
    return (ans & ((temp == 0 || temp == 1)));
}
```

**Sample Program Run**

We now add a few print functions to the code and try running two inputs in order to test our program.

**Input 1**

Input.

```
a = 1
b = 1
c = -3
```

Output.

```
Legendre Theorem Check
-bc is  a quadratic residue modulo |a|
-ab is not a quadratic residue modulo |c|
-ac is  a quadratic residue modulo |b|
There is no nontrivial integral solution to f(x, y, z) = 0

Hasse-Minkowski Theorem Check
There is no 3-focused solution
There is no nontrivial integral solution to f(x, y, z) = 0
```

**Input 2**

Input.

```
a = -7
b = 15
c = 13
```

Output.

```
Legendre Theorem Check
-bc is a quadratic residue modulo |a|
-ab is a quadratic residue modulo |c|
-ac is a quadratic residue modulo |b|
There are nontrivial integral solutions to f(x, y, z) = 0

Hasse-Minkowski Theorem Check
There is a 3-focused solution: x = 1, y = 0, z = 1
There is a 5-focused solution: x = 1, y = 0, z = 2
There is a 7-focused solution: x = 0, y = 1, z = 1
There is a 13-focused solution: x = 1, y = 6, z = 0
There are nontrivial integral solutions to f(x, y, z) = 0
```

We can see that in both cases the result is the same as the Legendre theorem and the Hasse-Minkowski theorem. We can also modify the program or add more functions depending on the task we intend to apply them to.

## 6. CONCLUSION

We have proved two Hasse-Minkowski theorems which facilitate the problem of determining the integral solvability of quadratic forms. After the Hasse-Minkowski theorem, in the binary form, we could find a prime $p$ which $f(x, y) \equiv 0 \pmod{p}$

does not have a solution $(x, y)$ both not divisible by $p$ to show that $f(x, y) = 0$ does not have nontrivial integral solutions. In the ternary form, the Hasse-Minkowski theorem reduces the problem to determining if there is a $p$-focused solution to the congruence $f(x, y, z) = 0 \pmod{p}$, which $p$ is finite. The crux of this paper is the introduction of a complete program implementing the Hasse-Minkowski theorems and Legendre theorem with some supporting functions like the Eratosthenes sieve and the Legendre symbol.

**Acknowledgments.** I wish to record my deep sense of gratitude and profound thanks to Dr. Mehmet Dik for guiding me in every stage of this research paper. Without his support, guidance, and encouragement, it would have been difficult for me to complete this paper.

## References

[1] S. D. Hoehner, *The Hasse-Minkowski Theorem in Two and Three Variables* (2012).
etd.ohiolink.edu/!etd.send_file?accession=osu1338317481
[2] G. A. Jones and J. M. Jones, *Elementary Number Theory* (Springer, 1998).
[3] W. J. LeVeque, *Fundamentals of Number Theory* (Dover Publications, 1977).

Phuc Ngo,
Beloit College, 700 College St., Beloit, WI 53511, U.S.A, (+1)248-759-0828, Orcid number:0000-0002-9658-4877
*Email address*: ngoph@beloit.edu

Mehmet Dik,
Beloit College, 700 College St., Beloit, WI 53511, U.S.A, (+1)815-986-9524, Orcid number:0000-0003-0643-2771
*Email address*: dikm@beloit.edu

Proceedings of International Mathematical Sciences
ISSN:2717-6355, URL:https://dergipark.org.tr/tr/pub/pims
Volume II Issue 2 (2020), Pages 90-95. Doi: 10.47086/pims.778004

# ON THE STABILITY OF NONLOCAL BOUNDARY VALUE PROBLEM FOR SCHRÖDINGER-PARABOLIC EQUATIONS

YILDIRIM OZDEMIR* AND MUSTAFA ALP**
*DUZCE UNIVERSITY, DUZCE, TURKEY. ORCID NUMBER:0000-0003-2767-522X
**DUZCE UNIVERSITY, DUZCE, TURKEY. ORCID NUMBER:0000-0001-7299-4487

Abstract. In the present article, a problem for a Schrödinger-parabolic equation with nonlocal boundary condition is considered. The stability estimates are established for the solution of nonlocal boundary value problem for Schrödinger-parabolic equation. The first and second order of accuracy difference schemes are used for approximate solutions of nonlocal boundary value problem. An example is considered and some error results of numerical experiments are presented in order to verify theoretical statements.

## 1. introduction

In the present paper, the nonlocal boundary value problem (NBVP)

$$\begin{cases} \dfrac{du(t)}{dt} + Au(t) = f(t)\,(0 \le t \le 1), \\ i\dfrac{du(t)}{dt} + Au(t) = g(t)\,(-1 \le t \le 0), \\ u(-1) = \alpha u(\mu) + \varphi, 0 < \mu \le 1 \end{cases} \tag{1.1}$$

for differential equations of Schrödinger-parabolic type in a Hilbert space $H$ with self-adjoint positive definite operator $A$ is considered.

It is well known that various NBVPs for the Schrödinger-parabolic equations can be reduced to problem (1.1).

A function $u(t)$ is called a solution of the problem (1.1) if the following conditions are satisfied:

**i.** $u(t)$ is continuously differentiable on the segment $[-1, 1]$. The derivative at the endpoints of the segment are understood as the appropriate unilateral derivatives.

**ii.** The element $u(t)$ belongs to $D(A)$ for all $t \in [-1, 1]$, and the function $Au(t)$ is continuous on the segment $[-1, 1]$.

**iii.** $u(t)$ satisfies the equations and nonlocal boundary condition (1.1).

2020 *Mathematics Subject Classification.* 2010 MSC: 65L10, 34B10, 65M12.
*Key words and phrases.* partial differential equation; nonlocal boundary value problem; stability.

Submitted on August 07th, 2020. Published on 12.30.2020. Communicated by Sahin UYAVER.

In this study, the stability estimates for the solution of the problem (1.1) for the Schrödinger-parabolic equation are established.

Methods of solutions of NBVPs for PDEs and PDEs of mixed type have been studied extensively by many researches (see, e.g., [1]-[12] and the references given therein).

## 2. THE MAIN THEOREM ON STABILITY

The goal of this section is to obtain the stability estimates for Schrödinger-parabolic equations. In applications, the stability estimates of mixed type NBVP for Schrödinger-parabolic equations are constructed. On the other hand, all theoretical statements are supported by the results of numerical experiments.

**Theorem 2.1.** *Let $\varphi \in D(A)$. Let $f(t)$ and $g(t)$ are continuously differentiable functions on $[0,1]$ and $[-1,0]$, respectively. Then, problem (1.1) has a unique solution and*

$$\max_{-1\leq t\leq 1}\|u(t)\|_H \leq M\left[\|\varphi\|_H + \max_{-1\leq t\leq 0}\|g(t)\|_H + \max_{0\leq t\leq 1}\|f(t)\|_H\right], \tag{2.1}$$

$$\max_{-1\leq t\leq 1}\|Au(t)\|_H \leq M\{\|A\varphi\|_H + \|g(0)\|_H \tag{2.2}$$

$$+ \max_{-1\leq t\leq 0}\|g'(t)\|_H + \|f(0)\|_H + \max_{0\leq t\leq 1}\|f'(t)\|_H\Big\},$$

*inequalities hold. Here $M$ is independent of $f(t)$, $t\in[0,1]$, $g(t)$, $t\in[-1,0]$ and $\varphi$.*

**Proof.** First of all, we will obtain a formula for the solution of problem (1.1). It is very well known that there are unique solutions of the initial value problems

$$\frac{du(t)}{dt} + Au(t) = f(t)\,(0\leq t\leq 1), u(0) = u_0 \tag{2.3}$$

and

$$i\frac{du(t)}{dt} + Au(t) = g(t)\,(-1\leq t\leq 0), u(-1) = u_{-1} \tag{2.4}$$

that is,

$$u(t) = e^{-tA}u(0) + \int_0^t e^{-(t-s)A}f(s)\,ds, 0\leq t\leq 1 \tag{2.5}$$

and

$$u(t) = e^{i(t+1)A}u_{-1} - i\int_{-1}^t e^{i(t-s)A}g(s)\,ds, -1\leq t\leq 0, \tag{2.6}$$

respectively. Using formula (2.6), we get

$$u(0) = e^{iA}u_{-1} - i\int_{-1}^0 e^{-isA}g(s)\,ds, -1\leq t\leq 0. \tag{2.7}$$

After that we can write

$$u(t) = e^{-tA}\left[e^{iA}u_{-1} - i\int_{-1}^0 e^{-isA}g(s)\,ds\right] + \int_0^t e^{-(t-s)A}f(s)\,ds, 0\leq t\leq 1. \tag{2.8}$$

Now, using the nonlocal boundary condition

$$u(-1) = \alpha u(\mu) + \varphi,$$

we obtain the operator equation

$$\left\{I-\alpha e^{iA}e^{-\mu A}\right\}u_{-1} \tag{2.9}$$
$$=\left\{\alpha-ie^{-\mu A}\int_{-1}^{0}e^{-isA}g\left(s\right)ds+\int_{0}^{\mu}e^{-(\mu-s)A}f(s)ds\right\}+\varphi.$$

Here, the operator

$$I-\alpha e^{iA}e^{-\mu A}$$

has an inverse,

$$T=\left(I-\alpha e^{iA}e^{-\mu A}\right)^{-1}$$

and

$$\left\|T\right\|_{H\to H}\leq M \tag{2.10}$$

holds. The proof of this inequality is based on the following estimate

$$\left\|-\alpha e^{-(\mu+i)A}\right\|_{H\to H}<1.$$

We have that

$$\left\|-\alpha e^{-(\mu+i)A}\right\|_{H\to H}\leq\left|-\alpha\right|\left|e^{-\mu\delta}\right|\left|e^{-i\delta}\right|\leq 1.$$

Then, it can be written that

$$\left\|T\right\|_{H\to H}\leq\left\|\left(I-\alpha e^{iA}e^{-\mu A}\right)^{-1}\right\|_{H\to H}\leq\frac{1}{1-\left|\alpha\right|e^{-\delta}}.$$

Here, using the following definition

$$\left(I-\alpha e^{iA}e^{-\mu A}\right)^{-1}u=\int_{\delta}^{\infty}\frac{1}{1-\alpha e^{i\lambda}e^{-\mu\lambda}}dE_{\lambda}u,$$

we get

$$\left\|\left(I-\alpha e^{iA}e^{-\mu A}\right)^{-1}\right\|_{H\to H}\leq\sup_{\delta\leq\lambda\leq\infty}\frac{1}{\left|1-\alpha e^{i\lambda}e^{-\mu\lambda}\right|}$$
$$\left|1-\alpha e^{i\lambda}e^{-\mu\lambda}\right|\geq 1-\left|\alpha\right|\left|e^{i\lambda}\right|\left|e^{-\mu\lambda}\right|\geq 1-\left|\alpha\right|\left|e^{-\mu\lambda}\right|$$
$$\geq 1-\left|\alpha\right|\left|e^{-\lambda}\right|=1-\left|\alpha\right|e^{-\delta}.$$

Therefore,

$$\left\|\left(I-\alpha e^{iA}e^{-\mu A}\right)^{-1}\right\|\leq\frac{1}{1-\left|\alpha\right|e^{-\delta}}\leq M.$$

So, it has been proven the estimate (2.10).

Hence, we obtain the following formula from the operator equation (2.9)

$$u_{-1}=T\left(\alpha\left\{-ie^{-\mu A}\int_{-1}^{0}e^{-isA}g\left(s\right)ds+\int_{0}^{\mu}e^{-(\mu-s)A}f(s)ds\right\}+\varphi\right). \tag{2.11}$$

Therefore, formulas (2.8), (2.6) and (2.11) are obtained for the solution of the problem (1.1). The proof of first part of the main theorem has been finished.

In the second part, proofs of estimates (2.1) and (2.2) will be given. Because of the symmetry properties of the operator $A$, we have the following estimates

$$\left\|e^{\pm itA}\right\|_{H\to H}\leq 1, t\geq 0. \tag{2.12}$$

Firstly, the proof of the estimate (2.1) will be obtained. Using formula (2.11), we get

$$\|u_{-1}\|_H \leq \left\{ \left\| \left(I - \alpha e^{iA} e^{-\mu A}\right)^{-1} \right\|_{H\to H} \left( |i|\,|\alpha| \left\|e^{-\mu A}\right\|_{H\to H} \int_{-1}^{0} \left\|e^{iAs}\right\|_{H\to H} \right.\right.$$
$$\left.\left. \times \|g(s)\|_H\, ds + |\alpha| \int_0^{\mu} \left\|e^{-(\mu-s)A}\right\|_{H\to H} \|f(s)\|_H\, ds + \|\varphi\|_H \right) \right\}$$
$$\leq M \left[ \int_{-1}^{0} \|g(s)\|_H\, ds + \int_0^{\mu} \|f(s)\|_H\, ds + \|\varphi\|_H \right].$$

Hence,

$$\|u_{-1}\|_H \leq M \left[ \|\varphi\|_H + \max_{-1\leq t\leq 0} \|g(t)\|_H + \max_{0\leq t\leq 1} \|f(t)\|_H \right]. \tag{2.13}$$

Using formula (2.8), we obtain

$$\|u(t)\|_H \leq \|u_{-1}\|_H + \int_{-1}^{0} \|g(s)\|_H\, ds + \int_0^{t} \|f(s)\|_H\, ds.$$

Hence,

$$\|u\,(t)\|_H \leq M \left[ \|\varphi\|_H + \max_{-1\leq t\leq 0} \|g(t)\|_H + \max_{0\leq t\leq 1} \|f(t)\|_H \right], 0 \leq t \leq 1. \tag{2.14}$$

Using formula (2.6), we get

$$\|u(t)\|_H \leq \|u_{-1}\|_H + \int_{-1}^{t} \|g(s)\|_H\, ds, -1 \leq t \leq 0.$$

Hence,

$$\|u(t)\|_H \leq M \left[ \|\varphi\|_H + \max_{-1\leq t\leq 0} \|g(t)\|_H + \max_{0\leq t\leq 1} \|f(t)\|_H \right]. \tag{2.15}$$

Therefore, using inequalities (2.14) and (2.15), we complete proof of inequality (2.1).

Secondly, the proof of the estimate (2.2) will be obtained. Using fomula (2.11) and integration by parts, we obtain

$$\|Au_{-1}\|_H \leq M \left\{ \|A\varphi\|_H + \|g\,(0)\|_H + \max_{-1\leq t\leq 0} \|g'\,(t)\|_H \right. \tag{2.16}$$
$$\left. + \|f\,(0)\|_H + \max_{0\leq t\leq 1} \|f'\,(t)\|_H \right\}$$

Now, we consider $-1 \leq t \leq 0$. Using formula (2.6) and integration by parts, we get

$$\|Au\,(t)\|_H \leq \|Au_{-1}\|_H + \|g\,(0)\|_H + \max_{-1\leq t\leq 0} \|g'\,(t)\|_H$$

Therefore, for $-1 \leq t \leq 0$ we obtain

$$\|Au\,(t)\|_H \leq M \left[ \|A\varphi\|_H + \|g\,(0)\|_H + \max_{-1\leq t\leq 0} \|g'\,(t)\|_H \right. \tag{2.17}$$
$$\left. + \|f\,(0)\|_H + \max_{0\leq t\leq 1} \|f'\,(t)\|_H \right].$$

Finally, we consider $0 \leq t \leq 1$. Using formula (2.8) and integration by parts, we get

$$\|Au\,(t)\|_H \leq M \left\{ \|A\varphi\|_H + \|g\,(0)\|_H + \max_{-1\leq t\leq 0} \|g'\,(t)\|_H \right. \tag{2.18}$$

$$+\left\|f\left(0\right)\right\|_{H}+\max_{0\leq t\leq 1}\left\|f'\left(t\right)\right\|_{H}\Bigg\}.$$

Using estimates (2.16), (2.17) and (2.18), we obtain (2.2). This completes the proof of the main theorem.

## 3. NUMERICAL RESULTS AND ERROR ANALYSIS

In this section, the nonlocal boundary value problem

$$\begin{cases} u_t - u_{xx} + u = (2-2t)\, e^{-t^2} \sin x, 0 < t < 1, 0 < x < \pi, \\ iu_t - u_{xx} + u = (2-2it)\, e^{-t^2} \sin x, -1 < t < 0, 0 < x < \pi, \\ u\left(0^+, x\right) = u\left(0^-, x\right);\ u_t\left(0^+, x\right) = u_t\left(0^-, x\right), \\ u(-1, x) = u(1, x) + 2e^{-1} \sin x, 0 \leq x \leq \pi, \\ u(t, 0) = u(t, \pi) = 0, -1 \leq t \leq 1 \end{cases} \tag{3.1}$$

for a one dimensional Schrödinger-parabolic equation is considered. The first and second order of accuracy difference schemes are constructed for approximate solutions of nonlocal boundary value problem (3.1). We have second order difference equations with respect $n$ with matrix coefficients. For the computations modified Gauss elimination method [13] is applied.

The errors between exact and approximate solutions are computed by the formula

$$E_M^N = \max_{1\leq k\leq N-1} \left( \sum_{n=1}^{M-1} \left| u\left(t_k, x_n\right) - u_n^k \right|^2 h \right)^{1/2}.$$

Numerical solutions are recorded for different values of $N$ and $M$, where $u(t_k, x_n)$ represents the exact solution and $u_n^k$ represents the numerical solution at $(t_k, x_n)$. The results are shown in the Table 1 for $N = M =$ 20, 40, 80 and 160.

| Method | $N = M = 20$ | $N = M = 40$ | $N = M = 80$ | $N = M = 160$ |
|---|---|---|---|---|
| FO DS | 0.0244 | 0.0133 | 0.0069 | 0.0035 |
| SO DS | 0.0060 | 0.0015 | $3.774 \times 10^{-4}$ | $9.4410 \times 10^{-5}$ |

TABLE 1. Comparison of errors for the approximate solution of difference schemes

Hence, based on the numerical results of numerical experiments, one can conclude that the second order of accuracy difference schemes are more accurate than the first order of accuracy difference scheme.

**Acknowledgments.** The author would like to sincerely thank Prof. Dr. Hüseyin ÇAKALLI and Prof. Dr. Allaberen ASHYRALYEV for his valuable supports.

## References


[1] A. Ashyralyev, and H. O. Fattorini, *On uniform difference schemes for the second-order singular perturbation problem in Banach spaces*, SIAM. J. Math. Anal., **23** (1992) 29-54.

[2] A. Ashyralyev, and N. Aggez, *A note on the difference schemes of the nonlocal boundary value problems for hyperbolic equations*, Numer. Func. Anal. Op., **25** (2004) 439-462.

[3] A. Ashyralyev, and Y. Ozdemir, *Stability of difference schemes for hyperbolic-parabolic equations*, Comput. Math. Appl., **50** (2005), 1443-1476.

[4] A. Ashyralyev, *Nonlocal boundary-value problems or abstract parabolic equations: well-posedness in Bochner spaces*, J. Evol. Equ., **6** (2006), 1-28.

[5] A. Ashyralyev, and Y. Ozdemir, *On nonlocal boundary value problems hyperbolic-parabolic equations* Taiwan. J. Math., **4** (2007), 1075-1089.

[6] A. Ashyralyev, and O. Gercek, *Nonlocal boundary value problems of elliptic-parabolic differential and difference equations*, Discrete. Dyn. Nat. Soc., **2008** (2008), 1-16.

[7] A. Ashyralyev, and A. Sirma, *Nonlocal boundary value problems for Shrödinger equations*, Comput. Math. Appl., **55** (2008), 392-407.

[8] A. Ashyralyev, and B. Hicdurmaz, *A note on the fractional Schrödinger differential equatios*, Kybernetes, **40** (2011), 736-750.

[9] A. Ashyralyev and O. Yıldırım, *On multipoint nonlocal boundary value problems for hyperbolic differential and difference equations*, Taiwan. J. Math., **14** (2010), 165-194.

[10] Y. Ozdemir, and M. Kucukunal, *A note on nonlocal boundary value problems for hyperbolic Schrödinger equations*, Abstr. Appl. Anal., **2012** (2012), 1-12.

[11] A. Ashyralyev, and O. Yıldırım, *A note on the second order accuracy stable difference schemes for the nonlocal boundary value hyperbolic problem*, Abstr. Appl. Anal., **2012** (2012), 1-29.

[12] A. Ashyralyev, I. Karatay, and P. E. Soboloevskii, *On well-posedness of the nonlocal boundary value problem for parabolic difference equations*, Discrete. Dyn. Nat. Soc., **2** (2004), 273-286.

[13] A. A. Samarskii, and E. S. Nikolaev, Numerical Methods for Grid Equations, Vol. 2 Iterative Methods, Birkäuser, Basel, 1989.



Yildirim Ozdemir,

Duzce University, Konuralp Campuss, Faculty of Arts and Sciences, Duzce, Turkey. Phone: +(90) 544 686 5722, Orcid number:0000-0003-2767-522X

*Email address*: yozdemir28@gmail.com

Mustafa Alp,

Duzce University, Duzce, Turkey. E-mail: mmustafa.alpp@gmail.com Orcid number:0000-0001-7299-4487

*Email address*: yozdemir28@gmail.com

Proceedings of International Mathematical Sciences
ISSN:2717-6355, URL:https://dergipark.org.tr/tr/pub/pims
Volume II Issue 2 (2020), Pages 96-102. Doi: 10.47086/pims.689633

# CHARACTERIZATION OF ABSOLUTELY NORM ATTAINING COMPACT HYPONORMAL OPERATORS

BENARD OKELO
ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY, BONDO, KENYA.
ORCID NUMBER:0000-0003-3963-1910

Abstract. General characterization of Hilbert space operators has been a subject of interest to many mathematicians for decades. In this paper, we characterize absolute norm-attainability for compact hyponormal operators. We give necessary and sufficient conditions for a bounded linear compact hyponormal operator on an infinite dimensional complex Hilbert space to be absolutely norm attaining. Moreover, we discuss the structure of compact hyponormal operators when they are self-adjoint and normal. Lastly, we discuss in general, other properties of compact hyponormal operators when they are absolutely norm attaining and their commutators.

## 1. Introduction

The study of norm attaining operators has been interesting to many mathematicians and researchers over decades( see [1], [2] and [5]). The class of absolutely norm attaining operators between complex Hilbert spaces was introduced by [1] and they discussed several important examples and properties of these operators. The class of absolutely norm attaining operators is denoted by $\mathcal{AN}(H)$. A synonymous class called norm-attainable operators have also been discussed by Okelo in [4] and it has been determined that they share similar characteristics. In this paper, we give necessary and sufficient conditions for an operator to be hyponormal and belongs to $\mathcal{AN}(H)$. In fact, we show that a bounded operator $T$ defined on an infinite dimensional Hilbert space is hyponormal and belongs to $\mathcal{AN}(H)$ if and only if there exists a unique triple $(K, F, \alpha)$, where $K$ is a positive compact operator, $F$ is a positive finite rank operator, $\alpha$ is positive real number such that $T = K - F + \alpha I$ and $KF = 0,\ F \leq \alpha I$. In fact, here $\alpha = m_e(T)$, the essential minimum modulus of $T$. Moreover, we give explicit structure of self-adjoint and $\mathcal{AN}$-operators as well as hyponormal and $\mathcal{AN}$-operators. Finally, we also obtain structure of general $\mathcal{AN}$-operators. In the process we also prove several important properties of $\mathcal{AN}$-operators. Unless otherwise stated, the hyponormal operators in

2010 *Mathematics Subject Classification.* Primary: 47A75; Secondaries: 47A10 .
*Key words and phrases.* Norm-attainability ; Compactness; Hyponormal operators.

Submitted on 15-February, 2020 Published on December 30th, 2020. Communicated by Ekrem SAVAS.
The author is thankful to the reviewers for their useful comments .

this work are compact. We organize the article as follows: Section 1: Introduction; Section 2: Preliminaries and notations; Section 3: Main results.

## 2. Preliminaries

In this section, we give the preliminaries. These include the basic terms, definitions and notations which are useful in the sequel. Throughout the paper, we consider all Hilbert spaces to be infinite dimensional and complex. We denote inner product and the induced norm by by $\langle .,. \rangle$ and $\|\cdot\|$ respectively. The unit sphere of a closed subspace $M$ of $H$ is denoted by $S_M := \{x \in M : \|x\| = 1\}$ and $P_M$ denote the orthogonal projection $P_M : H \to H$ with range $M$. The identity operator on $M$ is denoted by $I_M$. See details in [1] and the references therein.

**Definition 2.1.** *An operator $T : H_1 \to H_2$ is said to be bounded if there exists a $C > 0$ such that $\|Tx\| \leq C\|x\|$, for all $x \in H_1$. If $T$ is bounded, the quantity $\|T\| = \sup\{\|Tx\| : x \in S_{H_1}\}$ is finite and is called the norm of $T$.*

We denote the space of all bounded linear operators between $H_1$ and $H_2$ by $\mathcal{B}(H_1, H_2)$. In general, the set of all bounded linear operators on $H$ is denoted by $\mathcal{B}(H)$.

**Definition 2.2.** *For $T \in \mathcal{B}(H_1, H_2)$, there exists a unique operator denoted by $T^* : H_2 \to H_1$ called the adjoint operator satisfying $\langle Tx, y\rangle = \langle x, T^*y\rangle$, for all $x \in H_1$ and for all $y \in H_2$.*

**Definition 2.3.** *An operator $T \in \mathcal{B}(H_1, H_2)$ is said to be norm attaining if there exists a $x \in S_{H_1}$ such that $\|Tx\| = \|T\|$. We denote the class of norm attaining operators by $\mathcal{N}(H_1, H_2)$.*

**Remark.** *It is known that $\mathcal{N}(H_1, H_2)$ is dense in $\mathcal{B}(H_1, H_2)$ with respect to the operator norm of $\mathcal{B}(H_1, H_2)$. We refer to* [2] *for more details.*

**Definition 2.4.** *(*[1]*). An operator $T \in \mathcal{B}(H_1, H_2)$ is said to be absolutely norm attaining or $\mathcal{AN}$-operator (shortly), if $T|_M$, the restriction of $T$ to $M$, is norm attaining for every non zero closed subspace $M$ of $H_1$. That is $T|_M \in \mathcal{N}(M, H_2)$ for every non zero closed subspace $M$ of $H_1$.*

**Definition 2.5.** *An operator $T \in \mathcal{B}(H)$ is said to be hyponormal if $\|T^*x\| \leq \|Tx\|$, for all $x \in H$.*

**Remark.** *This class contains $\mathcal{K}(H_1, H_2)$, and the class of partial isometries with finite dimensional null space or finite dimensional range space.*

In the remaining part of this section, we give standard terminologies and notations found in [3]. Let $T \in \mathcal{B}(H)$. Then $T$ is said to be normal if $T^*T = TT^*$, self-adjoint if $T = T^*$. If $T$ is self-adjoint and $\langle Tx, x\rangle \geq 0$, for all $x \in H$, then $T$ is called positive. It is well known that for a positive operator $T$, there exists a unique positive operator $S \in \mathcal{B}(H)$ such that $S^2 = T$. We write $S = T^{\frac{1}{2}}$ and is called as the positive square root of $T$. If $S, T \in \mathcal{B}(H)$ are self-adjoint and $S - T \geq 0$, then we write this by $S \geq T$. If $P \in \mathcal{B}(H)$ is such that $P^2 = P$, then $P$ is called a projection. If Null space of $P$, $N(P)$ and range of $P$, $R(P)$ are orthogonal to each other, then $P$ is called an orthogonal projection. It is a well known fact that a projection $P$ is an orthogonal projection if and only if it is self-adjoint if and only if it is normal. We call an operator $V \in \mathcal{B}(H_1, H_2)$ to

be an isometry if $\|Vx\| = \|x\|$, for each $x \in H_1$. An operator $V \in \mathcal{B}(H_1, H_2)$ is said to be a partial isometry if $V|_{N(V)^\perp}$ is an isometry. That is, $\|Vx\| = \|x\|$ for all $x \in N(V)^\perp$. If $V \in \mathcal{B}(H)$ is isometry and onto, then $V$ is said to be a unitary operator. If $T \in \mathcal{B}(H)$ is a self-adjoint operator, then $T = T_+ - T_-$, where $T_\pm$ are positive operators. Here $T_+$ is called the positive part and $T_-$ is called the negative part of $T$ . Moreover, this decomposition is unique. In general, if $T \in \mathcal{B}(H_1, H_2)$, then $T^*T \in \mathcal{B}(H_1)$ is positive and $|T| := (T^*T)^{\frac{1}{2}}$ is called the modulus of $T$. In fact, there exists a unique partial isometry $V \in \mathcal{B}(H_1, H_2)$ such that $T = V|T|$ and $N(V) = N(T)$. This factorization is called the polar decomposition of $T$. If $T \in \mathcal{B}(H)$, then $T = \frac{T+T^*}{2} + i(\frac{T-T^*}{2i})$. The operators $Re(T) := \frac{T+T^*}{2}$ and $Im(T) := \frac{T-T^*}{2i}$ are self-adjoint and called the real and the imaginary parts of $T$ respectively. A closed subspace $M$ of $H$ is said to be invariant under $T \in \mathcal{B}(H)$ if $TM \subseteq M$ and reducing if both $M$ and $M^\perp$ are invariant under $T$. For $T \in \mathcal{B}(H)$, the set $\rho(T) := \{\lambda \in \mathbb{C} : T - \lambda I : H \to H$ is invertible and $(T - \lambda I)^{-1} \in \mathcal{B}(H)\}$ is called the resolvent set and the complement $\sigma(T) = \mathbb{C} \setminus \rho(T)$ is called the spectrum of $T$. The spectral radius of $T$ is given by $m(T) = \sup\{|\lambda| \in \mathbb{C} : \lambda \in \rho(T)\}$. It is well known that $\sigma(T)$ is a non empty compact subset of $\mathbb{C}$. The point spectrum of $T$ is defined by $\sigma_p(T) = \{\lambda \in \mathbb{C} : T - \lambda I$ is not one-to-one$\}$. Note that $\sigma_p(T) \subseteq \sigma(T)$. A self-adjoint operator $T \in \mathcal{B}(H)$ is positive if and only if $\sigma(T) \subseteq [0, \infty)$. If $T \in \mathcal{B}(H_1, H_2)$, then $T$ is said to be compact if for every bounded set $S$ of $H_1$, the set $T(S)$ is pre-compact in $H_2$. Similarly, for every bounded sequence $(x_n)$ of $H_1$, $(Tx_n)$ has a convergent subsequence in $H_2$. We denote the set of all compact operators between $H_1$ and $H_2$ by $\mathcal{K}(H_1, H_2)$. In case if $H_1 = H_2 = H$, then $\mathcal{K}(H_1, H_2)$ is denoted by $\mathcal{K}(H)$. A bounded linear operator $T : H_1 \to H_2$ is called finite rank if $R(T)$ is finite dimensional. The space of all finite rank operators between $H_1$ and $H_2$ is denoted by $\mathcal{F}(H_1, H_2)$ and we write $\mathcal{F}(H, H) = \mathcal{F}(H)$. These standard facts can be obtained in [3] and the references therein.

## 3. Main Results

In this section, we give the main results of this work. We begin with the following auxiliary propositions.

**Proposition 3.1.** *Let $T \in \mathcal{B}(H_1, H_2)$ be compact and hyponormal. Then*

(i). $m(T) = m(|T|)$
(ii). $m(T) = d(0, \sigma(|T|))$
(iii). $m(T) > 0$ *if and only if $R(T)$ is closed and $T$ is one-to-one ($T$ is bounded below)*
(iv). *in Particular if $H_1 = H_2 = H$ and $T^{-1} \in \mathcal{B}(H)$, then* $m(T) = \dfrac{1}{\|T^{-1}\|}$
(v). *if $H_1 = H_2 = H$ and $T$ is normal, then*
  (a) $m(T) = d(0, \sigma(T))$
  (b) $m(T) = m(T^*)$
  (c) $m(T^n) = m(T)^n$ *for each $n \in \mathbb{N}$*
(vi). *if $T \geq 0$, then $m(T) = m(T^{\frac{1}{2}})^2$.*

*Proof.* The proof is analogous to the proof of Carvajal and Neves. See [1] for proof. □

**Proposition 3.2.** *Let $T = K + F + \alpha I$, where $K$ is a positive compact hyponormal operator, $F$ is a self-adjoint finite rank normal operators and $\alpha > 0$. Then the following holds:*

(i). *$R(T)$ is closed*
(ii). *$N(T)$ is finite dimensional. In fact, $N(T) \subseteq R(F)$*
(iii). *$T$ is one-to-one if $K \geq F$*
(iv). *if $T$ is not a finite rank operator, there exists $a > 0, b > 0$ such that $\alpha \in (a\gamma(T), b\gamma(T))$*
(v). *if $T$ is a finite rank operator, then $H$ is finite dimensional.*

*Proof.* By proposition 3.2 above and analogous to the proof in [1] the proof is complete. □

**Proposition 3.3.** *Let $T \in \mathcal{B}(\mathcal{H})$ be compact and hyponormal and $\beta \in W_e(S)$ where $\alpha > 0$. Then there exists an operator $S \in \mathcal{B}(\mathcal{H})$ such that $\|S\| = \|Z\|$, $\|S - Z\| < \alpha$ and $T$ is absolutely norm attaining. Furthermore, there exists a vector $\eta \in H$, $\|\eta\| = 1$ such that $\|Z\eta\| = \|Z\|$ with $\langle Z\eta, \eta\rangle = \beta$.*

*Proof.* Consider $S \in \mathcal{B}(\mathcal{H})$ to be contractive then we may assume that $\|S\| = 1$ by ignoring the strict inequality. and also that $0 < \alpha < 2$. Let $x_n \in H$ $(n = 1, 2, ...)$ be such that $\|x_n\| = 1$, $\|Sx_n\| \to 1$ and also $\lim_{n\to\infty}\langle Sx_n, x_n\rangle = \beta$. Let $S = GL$ be the polar decomposition of $S$. Here $G$ is a partial isometry and we write $L = \int_0^1 \beta dE_\beta$, the spectral decomposition of $L = (S^*S)^{\frac{1}{2}}$. Since $\lim_{n\to\infty}\|Sx_n\| = \|S\| = \|L\| = 1$, we have that $\|Lx_n\| \to 1$ as $n$ tends to $\infty$ and $\lim_{n\to\infty}\langle Sx_n, x_n\rangle = \lim_{n\to\infty}\langle GLx_n, x_n\rangle = \lim_{n\to\infty}\langle Lx_n, G^*x_n\rangle$. Now for $H = \overline{R(L)} \oplus KerL$, we can choose $x_n$ such that $x_n \in \overline{R(L)}$ for large $n$. Indeed, let $x_n = x_n^{(1)} \oplus x_n^{(2)}$, $n = 1, 2, ...$ Then we have that $Lx_n = Lx_n^{(1)} \oplus Lx_n^{(2)} = Lx_n^{(1)}$ and that $\lim_{n\to\infty}\|x_n^{(1)}\| = 1$, $\lim_{n\to\infty}\|x_n^{(2)}\| = 0$ since $\lim_{n\to\infty}\|Lx_n\| = 1$. Replacing $x_n$ with $\frac{x_n^{(1)}}{\|x_n^{(1)}\|}$, we obtain $\lim_{n\to\infty}\left\|L\frac{1}{\|x_n^{(1)}\|}x_n^{(1)}\right\| = \lim_{n\to\infty}\left\|S\frac{1}{\|x_n^{(1)}\|}x_n^{(1)}\right\| = 1$, and we also obtain that $\lim_{n\to\infty}\left\langle S\frac{1}{\|x_n^{(1)}\|}x_n^{(1)}, \frac{1}{\|x_n^{(1)}\|}x_n^{(1)}\right\rangle = \beta$. Now assume that $x_n \in \overline{RL}$. Since $G$ is a partial isometry from $\overline{R(L)}$ onto $\overline{R(S)}$, we have that $\|Gx_n\| = 1$ and $\lim_{n\to\infty}\langle Lx_n, G^*x_n\rangle = \beta$. Since $L$ is a positive operator, $\|L\| = 1$ and for any $x \in H$, $\langle Lx, x\rangle \leq \langle x, x\rangle = \|x\|^2$. Replacing $x$ with $L^{\frac{1}{2}}x$, we get that $\langle L^2x, x\rangle \leq \langle Lx, x\rangle$, where $L^{\frac{1}{2}}$ is the positive square root of $L$. Therefore we have that $\|Lx\|^2 = \langle Lx, Lx\rangle \leq \langle Lx, x\rangle$. It is obvious that $\lim_{n\to\infty}\|Lx_n\| = 1$ and that $\|Lx_n\|^2 \leq \langle Lx_n, x_n\rangle \leq \|Lx_n\|^2 = 1$. Hence, $\lim_{n\to\infty}\langle Lx_n, x_n\rangle = 1 = \|L\|$. Moreover, Since $I - L \geq 0$, we have $\lim_{n\to\infty}\langle (I - L)x_n, x_n\rangle = 0$. thus $\lim_{n\to\infty}\|(I - L)^{\frac{1}{2}}x_n\| = 0$. Indeed, $\lim_{n\to\infty}\|(I - L)x_n\| \leq \lim_{n\to\infty}\|(I - L)^{\frac{1}{2}}\|.\|(I - L)^{\frac{1}{2}}x_n\| = 0$. For $\alpha > 0$, let $\gamma = [0, 1 - \frac{\alpha}{2}]$ and let $\rho = (1 - \frac{\alpha}{2}, 1]$. We have $L = \int_\gamma \mu dE_\mu + \int_\rho \mu dE_\mu = LE(\gamma) \oplus LE(\rho)$. Next we show that $\lim_{n\to\infty}\|E(\gamma)x_n\| = 0$. If there exists a subsequence $x_{n_i}, (i = 1, 2, ...,)$ such that $\|E(\gamma)x_{n_i}\| \geq \epsilon > 0$, $(i = 1, 2, ...,)$, then since $\lim_{i\to\infty}\|x_{n_i} - Lx_{n_i}\| = 0$, it follows from [4] that $\lim_{i\to\infty}\|x_{n_i} - Lx_{n_i}\|^2 = \lim_{i\to\infty}(\|E(\gamma)x_{n_i} - LE(\gamma)x_{n_i}\|^2 + \|E(\rho)x_{n_i} - LE(\rho)x_{n_i}\|^2) = 0$. Hence we have that $\lim_{i\to\infty}\|E(\gamma)x_{n_i} - LE(\gamma)x_{n_i}\|^2 = 0$. Now it is clear that $\|E(\gamma)x_{n_i} - LE(\gamma)x_{n_i}\| \geq \|E(\gamma)x_{n_i}\| - \|LE(\gamma)\|.\|E\gamma)x_{n_i}\| \geq (I - \|LE(\gamma)\|)\|E(\gamma)x_{n_i}\| \geq \frac{\alpha}{2}\epsilon > 0$. This is a contradiction. Therefore, $\lim_{n\to\infty}\|E(\gamma)x_n\| = 0$. Since $\lim_{n\to\infty}\langle Lx_n, x_n\rangle = 1$, we have that $\lim_{n\to\infty}\langle LE(\rho)x_n, E(\rho)x_n\rangle = 1$ and $\lim_{n\to\infty}\langle E(\rho)x_n, G^*E(\rho)x_n\rangle = \beta$. It

is easy to see that $\lim_{n\to\infty}\|E(\rho)x_n\| = 1$, $\lim_{n\to\infty}\left(L\frac{E(\rho)x_n}{\|E(\rho)x_n\|}, \frac{E(\rho)x_n}{\|E(\rho)x_n\|}\right) = 1$ and $\lim_{n\to\infty}\left(L\frac{E(\rho)x_n}{\|E(\rho)x_n\|}, G^*\frac{E(\rho)x_n}{\|E(\rho)x_n\|}\right) = \beta$ Replacing $x$ with $\frac{E(\rho)x_n}{\|E(\rho)x_n\|}$, we can assume that $x_n \in E(\rho)H$ for each $n$ and $\|x_n\| = 1$. Let $J = \int_\gamma \mu dE_\mu + \int_\rho \mu dE_\mu = J_1 \oplus E(\rho)$. Then it is evident that $\|J\| = \|S\| = \|L\| = 1, Jx_n = x_n$ and $\|J - L\| \leq \frac{\alpha}{2}$. If we can find a contraction $V$ such that $V - G \leq \frac{\alpha}{2}$ and $\|Vx_n\| = 1$ and $\langle Vx_n, x_n\rangle = \beta$, for a large $n$ then letting $Z = VJ$, we have that $\|Zx_n\| = \|VJx_n\| = 1$, and that $\langle Zx_n, x_n\rangle = \langle VJx_n, x_n\rangle = \langle Vx_n, x_n\rangle = \beta$ $\|S - Z\| = \|GL - VJ\| = \alpha$. To complete the proof, we now construct the desired contraction $V$. Clearly, $\lim_{n\to\infty}\langle x_n, G^*x_n\rangle = \beta$, because $\lim_{n\to\infty}\langle Lx_n, G^*x_n\rangle = \beta$ and $\lim_{n\to\infty}\|x_n - Lx_n\| = 0$. Let $Gx_n = \phi_n x_n + \varphi_n y_n$, $(y_n \perp x_n,\ \|y_n\| = 1)$ then $\lim_{n\to\infty}\phi_n = \beta$, because $\lim_{n\to\infty}\langle Gx_n, x_n\rangle = \lim_{n\to\infty}\langle x_n, G^*x_n\rangle = \beta$ but $\|Gx_n\|^2 = |\phi_n|^2 + |\varphi_n|^2 = 1$, so we have that $\lim_{n\to\infty}|\varphi_n| = \sqrt{1 - |\beta|^2}$. Then by [4] and [5] the remaining part of the proof is analogous and this completes the proof. □

At this point, we consider absolute norm-attainability for commutators of compact hypomormal operators.

**Lemma 3.4.** *Let $E \in \mathcal{B}(H)$ be compact hyponormal then $EX - XE$ is absolutely norm attaining if there exists a vector $\zeta \in H$ such that $\|\zeta\| = 1$, $\|E\zeta\| = \|E\|$, $\langle E\zeta, \zeta\rangle = 0$.*

*Proof.* Let $x \perp \{\zeta, E\zeta\}$, and define a compact $X$ as follows $X : \zeta \to \zeta$, $E\zeta \to -E\zeta$, $x \to 0$. Since $X$ is a bounded operator on $H$ and $\|X\zeta\| = \|X\| = 1$, $\|EX\zeta - XE\zeta\| = \|E\zeta - (-E\zeta)\| = 2\|E\zeta\| = 2\|E\|$. It follows that $\|EX - XE\| = 2\|E\|$ by Proposition 3.1, because $\langle E\zeta, \zeta\rangle = 0 \in W_e(E)$. Hence we have that $\|EX - XE\| = 2\|E\|$. Therefore, $EX - XE$ is absolutely norm attaining. □

**Lemma 3.5.** *Let $S, T \in \mathcal{B}(H)$ be compact hyponormal. If there exists vectors $\zeta, \eta \in H$ such that $\|\zeta\| = \|\eta\| = 1$, $\|S\zeta\| = \|S\|$, $\|T\eta\| = \|T\|$ and $\frac{1}{\|S\|}\langle S\zeta, \zeta\rangle = -\frac{1}{\|T\|}\langle T\eta, \eta\rangle$, then $SX - XT$ is is absolutely norm attaining.*

*Proof.* Since $H$ has an orthonormal basis then by linear dependence of vectors, if $\eta$ and $T\eta$ are linearly dependent, i.e.,$T\eta = \phi\|T\|\eta$, then we have $|\phi| = 1$ and $|\langle T\eta, \eta\rangle| = \|T\|$. It follows that $|\langle S\zeta, \zeta\rangle| = \|S\|$ which implies that $S\zeta = \varphi\|S\|\zeta$ and $|\varphi| = 1$. Hence $\left\langle \frac{S\zeta}{\|S\|}, \zeta\right\rangle = \varphi = -\left\langle \frac{T\eta}{\|T\|}, \eta\right\rangle = -\phi$. Defining $X$ as $X : \eta \to \zeta$, $\{\eta\}^\perp \to 0$, we have $\|X\| = 1$ and $(SX - XT)\eta = \varphi(\|S\| + \|T\|)\zeta$, which implies that $\|SX - XT\| = \|(SX - XT)\eta\| = \|S\| + \|T\|$. By [2], it follows that $\|SX - XT\| = \|S\| + \|T\| = \|\delta_{S,T}\|$. That is $SX - XT$ is absolutely norm attaining. If $\eta$ and $T\eta$ are linearly independent, then $\left|\left\langle \frac{T\eta}{\|T\|}, \eta\right\rangle\right| < 1$, which implies that $\left|\left\langle \frac{S\zeta}{\|S\|}, \zeta\right\rangle\right| < 1$. Hence $\zeta$ and $S\zeta$ are also linearly independent. Let us redefine $X$ as follows: $X : \eta \to \zeta$, $\frac{T\eta}{\|T\|} \to -\frac{S\zeta}{\|S\|}$, $x \to 0$, where $x \in \{\eta, T\eta\}^\perp$. We show that $X$ is a partial isometry. Let $\frac{T\eta}{\|T\|} = \left\langle \frac{T\eta}{\|T\|}, \eta\right\rangle \eta + \tau h$, $\|h\| = 1$, $h \perp \eta$. Since $\eta$ and $T\eta$ are linearly independent, $\tau \neq 0$. So we have that $X\frac{T\eta}{\|T\|} = \left\langle \frac{T\eta}{\|T\|}, \eta\right\rangle X\eta + \tau Xh = -\left\langle \frac{S\zeta}{\|S\|}, \zeta\right\rangle \zeta + \tau Xh$, which implies that $\left\langle X\frac{T\eta}{\|T\|}, \zeta\right\rangle = -\left\langle \frac{S\zeta}{\|S\|}, \zeta\right\rangle + \tau\langle Xh, \zeta\rangle =$

$-\left\langle \frac{S\zeta}{\|S\|}, \zeta \right\rangle$. It follows then that $\langle Xh, \zeta\rangle = 0$ i.e., $Xh \perp \zeta (\zeta = X\eta)$. Hence we have that $\left\| \left\langle \frac{S\zeta}{\|S\|}, \zeta \right\rangle \zeta \right\|^2 + \|\tau Xh\|^2 = \left\| X \frac{T\eta}{\|T\|} \right\|^2 = \left| \left\langle \frac{T\eta}{\|T\|}, \eta \right\rangle \right|^2 + |\tau|^2 = 1$, which implies that $\|Xh\| = 1$. Now it is evident that $X$ a partial isometry and $\|(SX - XT)\zeta\| = \|SX - XT\| = \|S\| + \|T\|$, which is equivalent to $\|\delta_{S,T}(X)\| = \|S\| + \|T\|$. By Lemma 3.1 and [4], $\|SX - XT\| = \|S\| + \|T\|$. Hence $SX - XT$ is absolutely norm attaining. □

**Corollary 3.6.** *Let $S, T \in \mathcal{B}(H)$ If both $S$ and $T$ are absolutely norm attaining then the operator $SXT$ is also absolutely norm attaining.*

*Proof.* We can assume that $\|S\| = \|T\| = 1$. If both $S$ and $T$ are absolutely norm attaining, then there exists unit vectors $\zeta$ and $\eta$ with $\|S\zeta\| = \|T\eta\| = 1$. We can therefore define an operator $X$ by $X = \langle \cdot, T\eta\rangle\zeta$. Clearly, $\|X\| = 1$. Therefore, we have $\|SXT\| \geq \|SXT\eta\| = \|\|T\eta\|^2 S\zeta\| = 1$. Hence, $\|SXT\| = 1$, that is $SXT$ is also absolutely norm attaining. □

**Proposition 3.7.** *Let $T \in \mathcal{AN}(H)$ be a self-adjoint compact hyponormal operator. Then there exists an orthonormal basis consisting of eigenvectors of $T$.*

*Proof.* The proof follows in the analogously as in[1] but we include it for completeness. Let $\mathcal{B} = \{x_\alpha : \alpha \in I\}$ be the maximal set of orthonormal eigenvectors of $T$. This set is non empty, as $T = T^* \in \mathcal{AN}(H)$. Let $M = \overline{\text{span}}\{x_\alpha : \alpha \in I\}$. Then we claim that $M = H$. If not, $M^\perp$ is a proper non-zero closed subspace of $H$ and it is invariant under $T$. Since $T = T^* \in \mathcal{AN}(H)$, then we have either $||T|M^\perp||$ or $-||T|M^\perp||$ is an eigenvalue for $T|M^\perp$. Hence there is a non-zero vector, say $x_0$ in $M^\perp$, such that $Tx_0 = \pm||T|M^\perp||x_0$. Since $M \cap M^\perp = \{0\}$, we have arrived to a contradiction to the maximality of $\mathcal{B}$. □

Next, we need to do a characterization for self-adjoint hyponormal compact operators. We ask the following question: For a compact hyponormal self-adjoint operator, can we find $\alpha \in \mathbb{R}$ such that $K + \alpha I \in \mathcal{AN}(H)$. To solve this first we need to answer the question when $K + \alpha I \in \mathcal{N}(H)$. Here we have the following characterization.

**Lemma 3.8.** *Let $K \in \mathcal{K}(H)$ be self-adjoint and $a \in \mathbb{R}$. Let $K = diag(\lambda_1, \lambda_2, \lambda_3, \dots, )$ with respect to orthonormal basis of $H$. Then the following are equivalent:*

(i). $T \in \mathcal{N}(H)$
(ii). *there exists $n_0 \in \mathbb{N}$ such that $|\lambda_{n_0} + a| > |a|$.*

*Proof.* The proof is trivial. □

Consider $T = T^* \in \mathcal{B}(H)$ and have the polar decomposition $T = V|T|$. Let $H_0 = N(T)$, $H_+ = N(I - V)$ and $H_- = N(I + V)$. Then $H = H_0 \oplus H_+ \oplus H_-$ which are all invariant under $T$. Let $T_0 = T|_{N(T)}$, $T_+ = T|_{H_+}$ and $T_- = T|_{H_-}$. Then $T = T_0 \oplus T_+ \oplus T_-$. Further more, $T+$ is strictly positive, $T_-$ is strictly negative and $T_0 = 0$ if $N(T) \neq \{0\}$. Let $P_0 = P_{N(T)}$, $P_\pm = P_{H_\pm}$. Then $P_0 = I - V^2$ and $P_\pm = \frac{1}{2}(V^2 \pm V)$. Thus $V = P_+ - P_-$. For details see [3].

**Theorem 3.9.** *Let $T \in \mathcal{AN}(H)$ be compact hyponrmal and self-adjoint with the polar decomposition $T = V|T|$. Then the operator $T$ can be represented as $T =$*

$K - F + \alpha V$, *where* $K \in \mathcal{K}(H)$, $F \in \mathcal{F}(H)$ *are self-adjoint with* $KF = 0$ *and* $F^2 \leq \alpha^2 I$

*Proof.* Let $H = H_+ \oplus H_-$ and $T = T_+ \oplus T_-$. Since $H_\pm$ reduces $T$, we have $T_\pm \in \mathcal{B}(H_\pm)$. As $T \in \mathcal{AN}(H)$, we have that $T_\pm \in \mathcal{AN}(H_\pm)$. Hence by [2], we have that $T_+ = K_+ - F_+ + \alpha I_{H_+}$ such that $K_+$ is positive compact operator, $F_+$ is finite rank positive operator with the property that $K_+F_+ = 0$ and $F_+ \leq \alpha I_{H_+}$. As $T_+$ is strictly positive, $\alpha > 0$. Similarly, $T_- \in \mathcal{AN}(H_-)$ and strictly negative. Hence there exists a triple $(K_-, F_-, \beta)$ such that $-T_- = K_- - F_- + \beta I_{H_-}$, where $K_- \in \mathcal{K}(H_-)$ is positive, $F_- \in \mathcal{F}(H_-)$ is positive with $K_-F_- = 0$, $F_- \leq \beta I_{H_-}$ and $\beta > 0$. The rest follows from [1] and the proof is complete. □

**Theorem 3.10.** *A compact self adjoint hyponormal operator* $T \in \mathcal{AN}(H)$ *has a countable spectrum.*

*Proof.* Since $T = T_+ \oplus T_- \oplus T_0$ and all these operators $T_+, T_-$ and $T_0$ are $\mathcal{AN}$ operators. We know that $\sigma(T_+), \sigma(T_0)$ are countable, as they are positive. Also, $-T_-$ is positive $\mathcal{AN}$-operator and hence $\sigma(T_-)$ is countable. Hence we can conclude that $\sigma(T) = \sigma(T_+) \cup \sigma(T_-) \cup \sigma(T_0)$ is countable. □

Now we consider the structure of normal $\mathcal{AN}$-operators.We see this in the next lemma

**Lemma 3.11.** *Let* $T \in \mathcal{AN}(H)$ *be compact hyponormal with the polar decomposition* $T = V|T|$. *Then there exists a compact hyponormal operator* $K$, *a finite rank normal operator* $F \in \mathcal{B}(H)$ *such that* $V, K, F$ *are mutually commutative.*

*Proof.* We have $VK = VVK_1 = VK_1V = KV$ and $VF = VVF_1 = VF_1V = FV$. Also, $KF = 0 = FK$. □

**Theorem 3.12.** *Let* $T \in \mathcal{B}(H)$ *be compact hyponormal. Then* $T \in \mathcal{AN}(H)$ *if and only if* $T^* \in \mathcal{AN}(H)$.

*Proof.* We know that $T \in \mathcal{AN}(H)$ if and only if $T^*T \in \mathcal{AN}(H)$. Since $T^*T = TT^*$, by Corollary Lemma 3.4 again, it follows that $TT^* \in \mathcal{AN}(H)$ if and only if $T^* \in \mathcal{AN}(H)$. □

**Acknowledgement.** This work was partially supported financially by the DFG Grant No. 1603991000.

## References

[1] X. Carvajal and W. Neves, *Operators that achieve the norm*, I. Eq. Oper. Theory, **72**(2)(2012), 179–195.
[2] P. Enflo, J. Kover and L. Smithies, *Denseness for norm attaining operator-valued functions*, Linear Algebra Appl., **338**(2001), 139–144.
[3] P. R. Halmos, *A Hilbert space problem book*, Springer-Verlag, New York, 1982.
[4] N. B. Okelo, *The norm attainability of some elementary operators*, Appl. Math. E-Notes, **13**(2013), 1–7.
[5] G. Ramesh, *Absolutely Norm attaining Paranormal operators*, J. Math. Anal. Applic., **465**(1)(2018), 547–556.

Benard Okelo,
Department of Pure and Applied Mathematics, Jaramogi Oginga, Odinga University of Science and Technology, P. O. Box 210-40601, Bondo, Kenya
Orcid number:0000-0003-3963-1910
*Email address*: bnyaare@yahoo.com

Proceedings of International Mathematical Sciences
ISSN:2717-6355, URL:https://dergipark.org.tr/tr/pub/pims
Volume II Issue 2 (2020), Pages 103-128. Doi: 10.47086/pims.827108

# DIOPHANTINE ATTACK ON PRIME POWER WITH MODULUS $N = p^r q$

SAIDU ISAH ABUBAKAR*, ZAID IBRAHIM**, SADIQ SHEHU *** AND AHMAD RUFAI****
*DEPARTMENT OF MATHEMATICS, SOKOTO STATE UNIVERSITY , SOKOTO, NIGERIA. ORCID NUMBER:0000-0002-0201-0064:
**DEPARTMENT OF MATHEMATICS, SOKOTO STATE UNIVERSITY , SOKOTO, NIGERIA. ORCID NUMBER:0000-0002-0251-6495:
***DEPARTMENT OF MATHEMATICS, SOKOTO STATE UNIVERSITY , SOKOTO, NIGERIA. ORCID NUMBER: 0000-0001-5908-7452:
****DEPARTMENT OF MATHEMATICS, SOKOTO STATE UNIVERSITY , SOKOTO, NIGERIA. ORCID NUMBER:0000-0003-3223-9924:

Abstract. The importance of keeping information secret cannot be overemphasized especially in today,s digital world where eavesdroppers are rampant in our chanels of communication. This made the use of strong encryption schemes inevitable in order to safeguard the security of our system. RSA cryptosystem and its variants have been designed to provide confidentiality and integrity of data in our medium of communication. This paper reports new short decryption exponent attack on prime power with modulus $N = p^r q$ for $r \geq 2$ using continued fraction method which makes it vulnerable to Diophantine attack and breaks the security of the cryptosystem by factoring the modulus into its prime factors since the hardness relies on the integer factorization problem. The paper also shows that if the short decryption exponent $d < \frac{1}{\sqrt{2}}\sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$, then one of the convergents $\frac{k}{d}$ can be found from the continued fraction expansion of $\frac{e}{N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ which leads to the successful factorization of prime power modulus $N = p^r q$ in polynomial time. The second part of the paper presents new findings on simultaneous factorization of $t$ prime power with moduli $N_s = p_s^r q_s$ for $s = 1, \ldots, t$ using simultaneous Diophantine approximations and lattice basis reduction methods which produces the prime factors of the form $(p_s, q_s)$ for $s = 1, \ldots, t$ in polynomial time where solutions of four system of equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ are provided. Our results increases the short decryption exponent bounds of some reported works.

2020 *Mathematics Subject Classification.* 11A52 ; 11A54; 11A55.
*Key words and phrases.* Diophantine; Attacks; Prime Power; Modulus; Continued Fraction.

Submitted November 17th, 2020. Published on december 30th, 2020. Communicated by Sahin UYAVER.

## 1. INTRODUCTION

The RSA cryptosystem invented by Rivest, Shamir and Adleman is considered to be the most widely used public key cryptosystem in today's digital world, [1]. Since then it has being extensively used for many applications in government as well as commercial domains which include e-banking, secure telephone, smart cards and communications in different types of Networks [2].

The security of this cryptosystem relies on the integer factorization problem. This cryptosystem has also many variants for computational efficiency. In this paper, we will focus on one of the variants known as prime power RSA with modulus $N = p^r q$ for $r \geq 2$. Fujioka et al. was the first to use the modulus $N = p^2 q$ for digital signature whose computational speed is faster than the original RSA scheme, as reported in [3]. Also in 1998, Okamoto et al. proposed a public key cryptography scheme whose security is considered to be as difficult as factoring an RSA modulus of the form $N = p^2 q$, as reported [4].

This paper focuses on the first variant given as $ed \equiv 1 \pmod{p^{r-1}(p-1)(q-1)}$ Using the first prime power RSA variant, Takagi in 1999 proposed a fast CRT-RSA variant with modulus $N = p^r q$ which is considered to be less vulnerable to attacks than the original RSA scheme, [5]. Takagi (1999) showed that when $d < N^{\frac{1}{2(r+1)}}$ for $r \geq 2$, the modulus $N = p^r q$ can be factored efficiently using lattice based technique. May (2004), reported an improvement on the bound of Takagi, where he showed that the modulus $N = p^r q$ is insecure if the short secret exponent $d < N^{\max\{\frac{r}{(r+1)^2}, \frac{(r-1)^2}{(r+1)^2}\}}$ using generalized Coppersmith's method, as reported by [6]. Also, Sarkar (2014) reported the used of small secret exponent attack on prime power RSA with modulus $N = p^2 q$ where he proved that the cryptosystem is insecure if the decryption exponent bound $d < N^{0.395}$, [7]. Furthermore, Lu et. al (2015) improved May's bound to $d < N^{\frac{r(r-1)}{(r+1)^2}}$ by method of lattice construction, [8]. In another result, Sarkar (2016) reported an improved bound of Lu et al. for $2 \leq r \leq 4$, [9].

For the second variant of prime power modulus $N = p^r q$, Itoh et al. (2008) showed that the prime factors of the prime power RSA modulus $N = p^r q$ can be found in polyomial time if the bound $d < \frac{2-\sqrt{2}}{r+1}$, [10].

Also, Blomer and May (2004) reported generalized Wiener's attack using combination of continued fraction and lattice basis reduction techniques which showed that RSA modulus $N = pq$ is insecure when there exist some unknown integers $x, y, z$ such that equation $ex - y\phi(N) = z$ is satisfied where $x < \frac{1}{3} N^{\frac{1}{4}}$ and $|z| < exN^{\frac{-3}{4}}$, [11]. In his work, Hinek (2007) proved that $k$ instances of RSA moduli $N_i$ can be factored if $d < N^{\gamma}$ for $\gamma = \frac{k}{2(k+1)} - \varepsilon$ where $\varepsilon$ is a small constant determine based on the size of $\max\{N_i\}$, as reported in [12].

In another development, Nitaj et al. (2014) presented two scenarios which showed that $k$ instances of RSA moduli $N_i = p_i q_i$ can be factored simultaneously in polynomial time using simultaneous Diophantine approximation and LLL algorithm , [13]. In the first scenario, they showed that if the equation $e_i x - y_i \phi(N_i)$ is satisfied where $x < N^{\delta}$, $y_i < N^{\delta}$, $|z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{\frac{1}{4}}$ for $\delta = \frac{k}{2(k+1)}$, $N = \min\{N_i\}$ then $k$ RSA moduli can be factored simultaneously. For the second scenario, they proved that $k$ instances of RSA public key pairs $(N_i, e_i)$ satisfying $e_i d_i - y\phi(N_i) = z_i$ for unknown integers $x_i,\ y, z_i$ where $x < N^{\delta},\ y_i < N^{\delta},\ |z_i| < \frac{p_i - q_i}{3(p_i+q_i)} y_i N^{\frac{1}{4}}$ for

$\delta = \frac{k(2\alpha-1)}{2(k+1)}$, $N = \min\{N_i\}$ and $\min\{e_i\} = N^\alpha$. They used simultaneous Diophantine approximations and lattice basis reduction techniques and finally use the Coppersmith's method to compute prime factors $p_i$ and $q_i$ of RSA moduli $N_i$ in polynomial time.

Furthermore, Shehu and Ariffin (2017) also presented a polynomial time attack on $j$ instances of prime power RSA with modulus $N_i = p_i^r q_i$ using a good approximation of $\phi(N)$ in which they proved that for $j$, $r \geq 2$ and given public key pairs $(N_i, e_i)$ and $N = \min\{N_i\}$, then equation $e_i d - k_i \phi(N_i) = 1$ can be satisfied only if the unknown integer $d < N^\delta$ and $j$ integers $k_i < N^\delta$ where $\delta = \frac{j-\gamma j}{j+1}$ for $0 \leq \gamma < 1$, as reported in [14]. Also using equation $e_i d_i - k\phi(N_i) = 1$, Shehu and Ariffin (2014) showed that $j$ prime power RSA modulus $N_i = p_i^r q_i$ can be simultaneously factored if the $j$ integers $d_i < N^\delta$ and integer $k < N^\delta$, $N = \min\{N_i\}$, and $\min\{e_i\} = N^\beta$ where $\delta = \frac{j(\beta-\gamma)}{j+1}$ for $\gamma < \beta < 1$, [14].

The findings of this paper is reported in two parts. In the first part, we work on the first variant of prime power modulus with equation of the form $ed \equiv 1 \pmod{p^{r-1}(p-1)(q-1)}$ using continued fraction method. Firstly, we construct a lemma which gives approximation of $\phi(N)$ given by $\phi(N) > N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$ and formulate a theorem which shows that if the secret exponent $d < \frac{1}{\sqrt{2}} \sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$, then one of the convergents $\frac{k}{d}$ can be found from the continued fraction expansion of $\frac{e}{N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ which leads to the factorization of prime power modulus $N = p^r q$ in polynomial time for $r \geq 2$. The paper also gives numerical example to justify how Theorem 3.2 works.

The second part of this paper presents cryptanalysis attacks of factoring $t$ instances of prime power moduli $N_s = p_s^r q_s$ in which we show that the moduli can be factored simultaneously using simultaneous Diophantine approximations and lattice basis reduction techniques. We present four new attacks using system of equations of the form $e_s d - k_s \phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s \phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ for $s = 1, \ldots, t$, for $r \geq 2$ where the parameters $d$, $d_s$, $k$, $k_s$, and $z_s$ are unknown positive integers. In all the presented attacks, we have improved decryption exponent bound of some reported attacks.

The rest of the paper is organize as follows. In Section 2, we present review of some basic definitions of the terms used such as continued fraction, lattice basis reduction and some theorems that are related to our attacks. In Section 3 , we present the proofs of our main results with lemma and theorems and their respective numerical examples and finally in Section 4, we conclude the paper.

## 2. PRELIMINARIES

In this section, we present some basic definitions on continued fraction, lattice basis reduction and some theorems on continued fraction, LLL and simultaneous Diophantine approximations.

**Definition 2.1.** *( Continued fraction)The continued fraction of a real number $x$ is an expression of the form*

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}}$$

*This expression is often used in the form* $x = [a_0, a_1, a_2, \ldots,]$. *Any rational number* $\frac{a}{b}$ *can be expressed as a finite continued fraction* $x = [a_0, a_1, a_2....a_m]$. *For* $i \geq 0$, *we define the* $i^{th}$ *convergent of the continued fraction* $[a_0, a_1, a_2, \ldots,]$ *to be* $[a_0, a_1, a_2, \ldots, a_i]$. *Each convergent is a rational number.*

**Definition 2.2.** *Let* $\vec{b_1}, \cdots \vec{b_m} \in \mathcal{R}^n$. *The vectors* $b_i's$ *are said to be linearly dependent if there exist* $x_1, \ldots, x_m \in R$, *which are not all zero and such that*

$$\sum_{i}^{m} x_i b_i = 0.$$

*Otherwise, they are said to be linearly independent.*

**Definition 2.3.** *(Lenstra et al. 1982) Let* $n$ *be a positive integer. A subset* $\mathcal{L}$ *of an* $n$*-dimensional real vector space* $\mathcal{R}^n$ *is called a lattice if there exists a basis* $b_1 \ldots b_n$ *on* $\mathcal{R}^n$ *suchthat* $\mathcal{L} = \sum_{i=1}^{n} \mathcal{Z} b_i = \sum_{i=1}^{n} r_i b_i : r_i \in \mathcal{Z}, 1 \leq i \leq n$.
*In this situation, we say that* $b_1 \cdots b_n$ *are basis for* $\mathcal{L}$ *or that they span* $\mathcal{L}$, [15].

**Definition 2.4.** *(LLL Reduction)* [16] *Let* $\mathcal{B} = \langle b_1 \cdots b_n \rangle$ *be a basis for a lattice* $\mathcal{L}$ *and let* $B^* = \langle b_1^* \cdots b_n^* \rangle$ *be the associated Gram- Schmidt orthogonal basis. Let*

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \; for \; 1 \leq j < i.$$

*The basis* $\mathcal{B}$ *is said to be LLL reduce if it satisfies the following two conditions:*

(1) $\mu_{i,j} \leq \frac{1}{2}, \quad for \quad 1 \leq j < i \leq n.$
(2) $\frac{3}{4}||b_{i-1}^*||^2 \leq ||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \quad for \quad 1 \leq i \leq n$. *Equivalently, it can be written as*

$$||b_i^*||^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)||b_{i-1}^*||^2.$$

**Theorem 2.1.** *If* $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}, \ldots$ *are convergents of the simple continued fraction* $[a_1, a_2, \ldots, a_k, \ldots]$, *then the numerators and denominators of these convergents satisfy the following recursive relations:*

$$p_1 = a_1, \; p_2 = a_2 a_1 + 1, p_k = a_k p_{k-1} + p_{k-2},$$
$$q_1 = 1, q_2 = a_2, \; q_k = a_k q_{k-1} + q_{k-2},$$

*for* $k \geq 3$, [17].

**Theorem 2.2.** *Let* $\alpha$ *be an arbitrary real number. If the rational number* $\frac{p}{q}$ *satisfies*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{2q^2},$$

*then* $\frac{p}{q}$ *must be a convergent of* $\alpha$.

**Theorem 2.3.** *Let* $\mathcal{L}$ *be a lattice basis of dimension* $n$ *having a basis* $v_1 \cdots v_n$. *The LLL algorithm produces a reduced basis* $b_1 \cdots b_n$ *satisfying the following condition*

$$||b_1|| \leq ||b_2|| \leq \cdots \leq ||b_j|| \leq 2^{\frac{n(n-1)}{4(n+1-j)}} det(\mathcal{L})^{\frac{1}{n+1-j}}$$

*for all* $1 \leq j \leq n$, [15].

**Theorem 2.4.** *(Simultaneous Diophantine Approximations, [13]) Given any rational numbers of the form $\alpha_1, \ldots, \alpha_n$ and $0 < \varepsilon < 1$, there is a polynomial time algorithm to compute integers $p_1, \ldots, p_n$ and a positive integer $q$ such that*

$$\max_i |q\alpha_i - p_i| < \varepsilon \text{ and } q \leq 2^{\frac{n(n-3)}{4}}.3^n.\varepsilon^{-n}.$$

## 3. MAIN RESULTS

This section has two parts. The first part reports short decryption exponent attack on prime power modulus $N = p^r q$ using continued fraction method which leads to the successful factorization of the modulus in polynomial time. In the second part of the paper, we present cryptanalysis attacks using simultaneous Diophantine approximations and lattice basis reduction methods in factoring $t$ prime power modulus $N_s = p_s^r q_s$ using system of equations of the form $e_s d - k_s\phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ for $s = 1, \ldots, t$, for $r \geq 2$ where parameters $d$, $d_s$, $k$, $k_s$ and $z_s$ are unknown positive integers.

### 3.1. Cryptanalytic Attack Through Analyzing Approximation of $\phi(N)$ given by $N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$.

This section presents a lemma which shows that if $q < p < 2q$ and the prime power modulus $N = p^r q$, then $\phi(N) > N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$ where $p$ and $q$ are distinct prime factors of the modulus $N = p^r q$, for $r \geq 2$. The section also proves a theorem which shows that the prime factors $p$ and $q$ can be recovered efficiently if $d < \frac{1}{\sqrt{2}}\sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$.

**Lemma 3.1.** *Let $p$ and $q$ be prime numbers where $p < q < 2p$ and $N = p^r q$ for $r \geq 2$. If $e < \phi(N)$ and $N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$, then $\phi(N) > N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$.*

*Proof.* Let $N = p^r q$ and the condition $q < p < 2p$ holds, then multiplying by $p^r$ yields $N^{\frac{1}{r+1}} < p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$.
Using $\phi(N) = p^{r-1}(p-1)(q-1)$, gives the following

$$\begin{aligned} \phi(N) &= p^{r-1}(p-1)(q-1) \\ &= N - p^r - p^{r-1}q + p^{r-1} \\ N - \phi(N) &= p^r + p^{r-1}q - p^{r-1} \\ &< p^r + p^{r-1}q. \end{aligned}$$

Since $q < p$ and $p < 2^{\frac{1}{r+1}} N^{\frac{1}{r+1}}$, then we have

$$\begin{aligned} N - \phi(N) &< 2p^r \\ &< 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}. \end{aligned}$$

Hence $\phi(N) > N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}$. □

**Theorem 3.2.** *Let $p$ and $q$ be prime numbers satisfying $p < q < 2p$ and let $N = p^r q$ be prime power modulus where $(N, e)$ and $(N, d)$ are public and private keys pairs respectively with $e < \phi(N)$. If the decryption exponent $d < \frac{1}{\sqrt{2}}\sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$, then one of the convergents $\frac{k}{d}$ can be found from the continued fraction expansion of*

$\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ *which leads to the factorization of prime power modulus* $N = p^r q$ *for* $r \geq 2$ *in polynomial time.*

*Proof.* Observe

$$\begin{aligned} \frac{ed - k\phi(N)}{d\phi(N)} &= \frac{e}{\phi(N)} - \frac{k}{d} \\ &= \frac{1}{d\phi(N)} \\ &> 0 \end{aligned}$$

Taking $N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$ from Lemma 3.1 as approximation of $\phi(N)$ yields::

$$\begin{aligned} \frac{e}{\phi(N)} - \frac{k}{d} &= \frac{e}{N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil} - \frac{e}{\phi(N)} + \frac{e}{\phi(N)} - \frac{k}{d} \\ &= \frac{e\left(N - \phi(N) - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil\right)}{\phi(N)(N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil)} + \frac{e}{\phi(N)} - \frac{k}{d} \end{aligned}$$

Since $N - \phi(N) < \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$, let $\frac{e\left(N-\phi(N)-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil\right)}{\phi(N)(N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil)} = T < 0$, then

$$\begin{aligned} &= \frac{e}{\phi(N)} - \frac{k}{d} - T \\ &< \frac{e}{\phi(N)} - \frac{k}{d} \\ &= \frac{1}{d\phi(N)} \\ &< \frac{1}{\phi(N)}. \end{aligned}$$

It was shown from Lemma 3.1 that $\phi(N) > N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}$, this implies

$$\frac{1}{\phi(N)} < \frac{1}{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$$

Since $d < \frac{1}{\sqrt{2}} \sqrt{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$, then

$$\frac{1}{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}} < \frac{1}{2d^2}.$$

Hence,

$$\left| \frac{e}{N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}} - \frac{k}{d} \right| \quad < \quad \frac{1}{2d^2}.$$

This shows that Theorem 3.2 produces $\frac{k}{d}$ as one of the convergent of the continued fraction expansion of $\frac{e}{N-2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}}$. This terminates the proof. □

The section also outlines below the algorithm to be followed in factoring the prime power modulus $N = p^r q$ for $r \geq 2$.

**Algorithm 1** Theorem 3.2

1: Initialization: Input the size $n$ and $(e, N)$ satisfying Theorem 3.2.
2: Compute the continued fraction of $\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ for $r \geq 2$
3: **for each** convergent $\frac{k}{d}$ of $\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ **do**
4: $\quad \phi(N) := \frac{ed-1}{k}$.
5: $\quad p^{r-1} := \gcd\left(N, \frac{ed-1}{k}\right)$
6: **end for**
7: **if** $1 < p^{r-1} < N$ **then**
8: $\quad q := \frac{N}{p^r}$.
9: **end if**
10: **return** the private keys $(p, q)$ .

**Example 3.1.** *This example gives an illustration of how Theorem 3.2 works on prime power modulus $N = p^r q$ for $r = 3$.*

$$\begin{aligned}
\textit{Let } N = {} & 64678246809679914850939685949849066984528469181266198775447954764512899975949030092389431143550672950630682676159477346727505541\\
& 77691953695737158023409301972062940648475622585500471848562296576246425671326682796985765039149169432233422230426191901156305513911690643137255586285890252274214143777796475233050043697253070\\
e = {} & 55281000751499877009107259165123700376809649466944460805706223523089195654398883367721127616833362407742058300902057826829515125034066183663278580767186726153429453492047380587411856008249.
\end{aligned}$$

Taking the continued fraction expansion of $\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ for $r = 3$, gives the following: $[0, 87, 1, 1, 32, 1, 95, 1, 13, 1, 13, 1, 7, 2, 6, 2, 6, 2, 1, 2, 2, 4, 7, 580, 1, 22, 5, 3, 30, 1, 1, 3, 3, 1, 14, 12, 5, 2, 26, 2, 3, 2, 1, 1, 1, 1, 9, 1, 16, 4, 1, 2, 1, 1, 4, 5, 1, 1, 1, 32, 1, 76, 13, 1, 2, 1, 14, 1, 1, 22, 1, 5, 1, 40, 1, 5, 2, 2, 3, 1, 1, 4, 273, 3, 1, 40, 3, 15, 1, 3, 1, 10, 36, 1, 43, 1, 3, 2, 1, 1, 1, 4, 2, 2, 3, 3, 2, 3, 1, 2, 1, 10, 1, 10, 1, 1, 1, 1, 9, 1, 1, 5, 1, 4, 2, 1, 9, 10, 1, 6, 8, 2, 4, 4, 6, 1, \ldots,]$. Then the convergent $\frac{k}{d}$ is found from the continued fraction expansion of $\frac{e}{N-\left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil}$ as

$$\frac{k}{d} = \frac{528369155574929758734471178633 5}{462362453808524086451896135480609}.$$

From Algorithm 1, we compute $\phi(N) = \frac{ed-1}{k}$ as follows:

$$\begin{aligned}
\phi(N) = {} & 64678246809679914850939685949849066984528469181266198775447954734769\\
& 19313372348183843208998399569436036670863930678884295028399128045789\\
& 53081294203558977769396768768923146094038024821936125526310321010437018161613390372921479673079645463655977965218274984.
\end{aligned}$$

Finally, from Algorithm 1 the following computations reveal the prime factors $p$ and $q$ of the prime power modulus $N = p^r q$:

$p^{r-1} = \gcd(N, \phi(N))$

$p = 568411957220695483099546712094710810857461543921464398521916102 7$

$q = \frac{N}{p^3}$

$q = 352183190503750596342466341162994165841738914383679121520787819 7.$

From our result, one can observe that, this work yields $d \approx N^{0.1281}$ which is greater than Shehu-Ariffin's bound $d \approx N^{0.102}$, as reported in [14].

### 3.2. Cryptanalysis Attacks on $t$ Prime Power With Moduli $N_s = p_s^r q_s$ Using $N - 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}$ as Approximation of $\phi(N)$.

This section presents four successful cryptanalysis attacks of factoring $t$ prime power with moduli $N_s = p_s^r q_s$ using systems of equations $e_s d - k_s\phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ where the parameter $\phi(N) = N - (p^r + p^{r-1}q - p^{r-1})$ for $r \geq 2$ and $s = 1, \ldots, t$.

#### 3.2.1. *The Attack on t Prime Power Moduli $N_s = p_s^r q_s$ Satisfying System of Equation $e_s d - k_s\phi(N_s) = 1$.*

Taking $t \geq 2$, let $N_s = p_s^r q_s$, for $s = 1, \ldots, t$ and $r \geq 2$. The attack works for $t$ instances of the public key tuple $(N_s, e_s)$ when there exists an integer $d$ and $t$ integers $k_s$ satisfying equation $e_s d - k_s\phi(N_s) = 1$. It shows that $t$ prime factors $p_s$ and $q_s$ of $t$ prime power with moduli $N_s = p_s^r q_s$ for $s = 1, \ldots, t,, r \geq 2$ can be found efficiently for $N = \max\{N_s\}$ and $d < N^{\varrho}$, $k_s < N^{\varrho}$, for all $\varrho = \frac{t(1-\beta)}{t+1}$ for $0 < \beta < 1$. In this case, the instances $(N_s, e_s)$ shared common decryption exponent $d$.

**Theorem 3.3.** *Let $N_s = p_s^r q_s$ be prime power moduli for $r \geq 2$, $s = 1, \cdots, t$ and $t \geq 2$. Let $(N_s, e_s)$ be public key pair and $(d, N_s)$ be private key pair with condition $e_s < \phi(N_s)$ and the relation $e_s d \equiv 1 \mod \phi(N_s)$ is satisfied. Let $N = \max\{N_s\}$. If there exists positive integers $d < N^{\varrho}$, $k_s < N^{\varrho}$, for all $\varrho = \frac{t(1-\beta)}{t+1}$ such that equation $e_s d - k_s\phi(N_s) = 1$ holds, for $0 < \beta < 1$, then $t$ prime power moduli $N_s$ can successfully be factored in polynomial time for $\frac{1}{4} \leq \varrho \leq \frac{1}{2}$ and $0 < \beta < 1$.*

*Proof.* For $r, t \geq 2$ where $N_s = p_s^r q_s$ is prime power moduli. Suppose that $N = \max\{N_s\}$ and $k_s < N^{\varrho}$ for $s = 1, \ldots, t$. Then equation $e_s d - k_s\phi(N_s) = 1$ can be rewritten as follows:

$$e_s d - k_s(N_s - (N_s - \phi(N)_s)) = 1.$$

Let $\triangle = 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}}$

$$e_s d - k_s\left(N_s - \triangle + \triangle - (N_s - \phi(N_s))\right) = 1$$

$$\left|\frac{e_s}{N - \triangle} d - k_s\right| = \frac{|1 - k_s(N_s - \phi(N_s) - \triangle)|}{N_s - \triangle}. \tag{3.1}$$

Since $N = \max\{N_s\}$ and $k_s < N_s^{\varrho}$, $d < N^{\varrho}$ be positive integers. Observe

$$|N_s - \phi(N_s) - \triangle| < N_s^{\beta} < N^{\beta}$$

for $\beta \in (0,1)$ and

$$N_s - \triangle > \frac{1}{r+2}N,$$

then plugging into equation (3.1) gives

$$\begin{aligned}\left|\frac{1 - k_s(N_s - \phi(N_s) - \triangle)}{N_s - \triangle}\right| &< \frac{|1 + k_s(N_s - \phi(N_s) - \triangle)|}{N_s - \triangle} \\ &< \frac{1 + N^{\varrho}(N^{\beta})}{\frac{1}{r+2}N} \\ &= \frac{r + 2(1 + N^{\varrho+\beta})}{N} \\ &< \sqrt{2r}N^{\varrho+\beta-1}.\end{aligned}$$

Then, it follows that

$$\left|\frac{e_s}{N_s - \triangle}d - k_s\right| \quad < \quad \sqrt{2r}N^{\varrho+\beta-1}.$$

We proceed to show the existence of integer $d$ and $t$ integers $k_s$. Let $\varepsilon = \sqrt{2r}N^{\varrho+\beta-1}$, with $\varrho = \frac{t(1-\beta)}{t+1}$. Then it gives

$$N^{\varrho}\varepsilon^t = N^{\varrho}\left(\sqrt{2r}N^{\varrho+\beta-1}\right)^t = (2r)^{\frac{t}{2}}\, N^{\varrho+\varrho t+\beta t-t} = (2r)^{\frac{t}{2}}\,.$$

Following Theorem 2.4, $(2r)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $t, r \geq 3$, then $N^{\varrho}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that since $d < N^{\varrho}$ then $d < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \cdots, t$, yields

$$\left|\frac{e_s}{N_s - \triangle}d - k_s\right| < \varepsilon.$$

This clearly satisfies the conditions of Theorem 2.4, and proceeds to reveal the private key $d$ and $t$ integers $k_s$ for $s = 1, \ldots, t$. Next, from $e_s d - k_s\phi(N_s) = 1$ we perform the following computations:

$$\begin{aligned}\phi(N_s) &= \frac{e_s d - 1}{k_s} \\ p_s^{r-1} &= \gcd(\phi(N_s), N_s) \\ q_s &= \frac{N_s}{p_s^r}.\end{aligned}$$

Finally, the prime factors $p_s$ and $q_s$ can be revealed which leads to the factorization of $t$ prime power moduli $N_s$ for $s = 1, \cdots, t$ in polynomial time. □

Let

$$\begin{aligned}X_1 &= \frac{e_1}{N_1 - 2^{\frac{2r+1}{r+1}}N_1^{\frac{r}{r+1}}}, \\ X_2 &= \frac{e_2}{N_2 - 2^{\frac{2r+1}{r+1}}N_2^{\frac{r}{r+1}}}, \\ X_3 &= \frac{e_3}{N_3 - 2^{\frac{2r+1}{r+1}}N_3^{\frac{r}{r+1}}}.\end{aligned}$$

Define,

$$T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}].$$

Consider the lattice $\mathcal{L}$ spanned by the matrix,

$$M = \begin{bmatrix} 1 & -[T(X_1)] & -[T(X_2)] & -[T \times X_3] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Taking $r \geq 2$, the matrix $M$ can be used in computing the reduced basis after applying the LLL algorithm.

**Algorithm 2** Theorem 3.3

Initialization: The public key tuple $(N_s, e_s, \varrho, \beta)$ satisfying Theorem 3.3.
Choose $r \geq 2$ and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
**for any** $(r, N, \varrho, \beta)$ **do**
    $\varepsilon := \sqrt{2r} N^{\varrho+\beta-1}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
**end for**
Consider the lattice $\mathcal{L}$ spanned by the matrix $M$ as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix $K$.
**for any** $(M, K)$ **do**
    $J := M^{-1}$
    $Q = JK$.
**end for**
Produce $d$, $k_s$ from $Q$
**for each** triplet $(d, k_s, e_s)$ **do**
    $\phi(N_s) := \frac{e_s d - 1}{k_s}$
    $p_s^{r-1} := \gcd(\phi(N_s), N_s)$.
    $q_s := \frac{N_s}{p_s^r}$
**end for**
**return** the prime factors $(p_s, q_s)$.

**Example 3.2.** *This example gives an illustration of how Theorem 3.3 works on 3 prime power moduli also their corresponding public exponents:*
*Let* $N_1 = 563382281374803858489382903716443474446580306437566005728878179$
$267676092551665191432331661132041057581935108036853538725342976031062566$
$064493977301796320064579931954653$

$N_2 = 110780160868938860790802031427539545689163771392478000053424961 7$
$140001335413025467235568243203922733387749142234285602245999359726144181$
$863789668190983522850626483669023$

$N_3 = 965401330168501605540050609837559483013713042769305626483689967 4$
$069160933238013628743471068194753666107834756424555627523960922969439392$
$110512678610069913809409216181 39$

$e_1 = 167644581477517488105562931315300218840429906809208126622351842 22$
$412584386285442254876550471043222816261798853928202440252160827176635480$

737937406061140259278673467716 1

$e_2 = 463152461180608542345912471172475221050879200856094014904488212481504858333502122923328285666380831883415086844453517642192115335016879503086688812611607958721881159677$

$e_3 = 417679330050262549730967902773056706769204590907920549790905313164765883718798498778729399201716067528829505703591869558941065895004395627923078418337259174212129372 61$

*Observe that* $N = \max\{N_1, N_2, N_3\}$

$N = 110780160868938860790802031427539545689163771392478000053424961714000133541302546723556824320392273338774914223428560224599935972614418186378966819098352285062648366902 3.$

Using Algorithm 2 for $t = 3$ $r = 3$ and $\beta = 0.75$ gives $\varrho = \frac{t(1-\beta)}{t+1} = 0.1875$ and $\varepsilon = \sqrt{2r}N^{\varrho+\beta-1} = 9.111089161 \times 10^{-39}$.
Applying Theorem 2.4 and using Algorithm 2 for $n = t = 3$, we compute

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}$$

$T = 1154165320000000000000000000000000000000000$
Consider the lattice $\mathcal{L}$ spanned by the matrix,

$$M = \begin{bmatrix} 1 & -[T(X_1)] & -[T(X_2)] & -[T \times X_3] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, it yields the reduced basis with the following matrix

$$K = \begin{bmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ B_{11} & B_{12} & B_{13} & B_{14} \\ C_{11} & C_{12} & C_{13} & C_{14} \\ D_{11} & D_{12} & D_{13} & D_{14} \end{bmatrix}$$

where
$A_{11} = 77702944695646214262857290487 13,\ A_{12} = -11866076834029234002241236377582$
$A_{13} = -32633775130445983893911306068132,\ A_{14} = -33280824901442008630692923529 13$
$B_{11} = 18663562246576439716517789824933,\ B_{12} = 15048857017191042713184735691338$
$B_{13} = 10286010869239647472878709783788,\ B_{14} = 18549844424135999309545228522867$
$C_{11} = -17095263517456624755229311937397,\ C_{12} = -17505448553655077987743164400 42$
$C_{13} = -34574596282163621534726127220 92,\ C_{14} = 25713796499666717792079771007197$
$D_{11} = -11796372669551527880579978498483,\ D_{12} = 49475532903151632120923767998362$
$D_{13} = -35068780855417302192076780015 88,\ D_{14} = 25794295789469667887502782206 83.$

Next, from Algorithm 2, we compute $Q = KJ$,

$$Q = \begin{bmatrix} E_{11} & E_{12} & E_{13} & E_{14} \\ F_{21} & F_{22} & F_{23} & F_{24} \\ G_{31} & G_{32} & G_{33} & G_{34} \\ H_{41} & H_{24} & H_{43} & H_{44} \end{bmatrix}$$

where
$E_{11} = 77702944695646214262857290487 13,\ E_{12} = 23121915746594298457024824360 55$
$E_{13} = 32486241033126945250515990107 54,\ E_{14} = 33618053828189170577559203770 1$
$F_{21} = 18663562246576439716517789824933,\ F_{22} = 55536803075731848864083277393 49$
$F_{23} = 78029086806670615508451743719 10,\ F_{24} = 80747601353944792193225355638 4$
$G_{31} = -17095263517456624755229311937397,\ G_{32} = -50870046722773312723339638803 73$
$G_{33} = -71472304341644208929859488736 97,\ G_{34} = -73962382170715466592557117283 7$
$H_{41} = -11796372669551527880579978498483,\ H_{42} = -35102239181429742670400054092 44$
$H_{43} = -49318569246078306806002308361 38,\ H_{44} = 51036816292572652503909634871 5.$

From the second row of the matrix $Q$, it yields the values for $d$, $k_1$, $k_2$ and $k_3$ as follows:

$d = 18663562246576439716517789824933,\ k_1 = 55536803075731848864083277393 49$
$k_2 = 78029086806670615508451743719 10,\ k_3 = 80747601353944792193225355638 4.$

Using Algorithm 2, $\phi(N_s) = \frac{e_s d-1}{k_s}$ for $s = 1, 2, 3$ can be computed as follows,

$\phi(N_1) = 56338228137480385848938290371644347444657821557016451499919943564437595515683558642235304837245791250135951344035856352576613910331257682743324996840534419133508898 2588$

$\phi(N_2) = 11078016086893886079080203142753954568916350420128548912405458621486173567251534621700628102364318928358025354874774274406689185786711145616433025239686363424063920829 04$

$\phi(N_3) = 96540133016850160554005060983755948301371063111771234924523131194182141715371111214562914838512984578211413625756392936014365359380504038220596586504243032123344765916 8.$

Next, from Algorithm 2, $p_s^{r-1}$ for $s = 1, 2, 3$ and $r = 3$ can be computed as follows,

$$\begin{aligned} p_1 &= 11720876728196985761402956937987 9515111959 \\ p_2 &= 12058019819639900134363121551161 50241125443 \\ p_3 &= 11655394061187804887158616519073008 62321907. \end{aligned}$$

Finally, from Algorithm 2, $q_s$ for $s = 1, 2, 3$ can be computed as follows,

$$\begin{aligned} q_1 &= 34988303815617434955503783366716292472 6907 \\ q_2 &= 63187912974577270249788026409319467912 2189 \\ q_3 &= 60971518167998350136625385645645532757 9473. \end{aligned}$$

This shows the factorization of 3 prime power moduli $N_s = p_s^r q_s$ for $s = 1, 2, 3$ and $r = 3$ in polynomial time. One can also observe that , our work yield $d \approx N^{0.18608}$ which is greater than $d \approx N^{0.1857}$, as reported in [14]. This shows that Shehu and Ariffin's attack can not yield the factorization of $t$ prime power moduli in our case.

3.2.2. *The Attack on t Prime Power Moduli $N_s = p_s^r q_s$ Satisfying System of Equation $e_s d_s - k\phi(N_s) = 1$.*

This section considers second case in which $t$ prime power moduli satisfies equations of the form $e_s d_s - k\phi(N_s) = 1$ for unknown positive integers $d_s$ and $k$ for $s = 1, \ldots, t$. In this case, every pair of the instances $(N_s, e_s)$ has its own unique decryption exponent $d_s$.

**Theorem 3.4.** *Let $N_s = p_s^r q_s$ be prime power moduli where $p_s$ and $q_s$ are prime numbers for $s = 1, \ldots, t$, $r, t \geq 2$. Let $(e_s, N_s)$ be public key pair and $(d_s, N_s)$ be private key pair with $e_s < \phi(N_s)$ and the relation $e_s d_s \equiv 1 \mod \phi(N_s)$ is satisfied. Let $e = \min\{e_s\} = N^{\alpha}$ be public exponent. If there exists $t$ integers $d_s < N^{\varrho}$ and integer $k < N^{\varrho}$, for all $\varrho = \frac{t(\alpha-\beta)}{t+1}$ such that $e_s d_s - k\phi(N_s) = 1$ holds, then prime factors $p_s$ and $q_s$ of $t$ prime power moduli $N_s$ can be successfully recovered in polynomial time for $0 < \varrho \leq \frac{1}{2}$, $0 < \beta < 1$ and $\beta < \alpha < 1$.*

*Proof.* For $r, t \geq 2$ and $N_s = p_s^r q_s$, be $t$ prime power moduli $e = \min\{e_s\} = N^{\alpha}$ be public exponent for $s = 1, \ldots t$ and suppose that $d_s < N^{\varrho}$. Then equation $e_s d_s - k\phi(N_s) = 1$ can be transformed into

$$e_s d_s - k(N_s - (N_s - \phi(N_s))) = 1$$

Let $\triangle = 2^{\frac{2r+1}{r+1}} N_s^{\frac{r}{r+1}}$

$$\begin{aligned} e_s d_s - k(N_s - \triangle + \triangle - (N_s - \phi(N_s))) &= 1 \\ e_s d_s - k(N_s - \triangle) &= 1 - k(N_s - \phi(N_s) - \triangle) \\ \left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| &= \frac{|1 - k\,(N_s - \phi(N_s) - \triangle)|}{e_s}. \end{aligned}$$

Since $N = \max\{N_s\}$ and $d_s < N^{\varrho}$, $k < N^{\varrho}$ are positive integers. Observe

$$N_s - \phi(N_s) - \triangle < N_s^{\beta} < N^{\beta}$$

for $\beta \in (0, 1)$. Since also $e = \min\{e_s\} = N^{\alpha}$, for $s = 1, \cdots, t$ then it gives

$$\begin{aligned} \frac{|1 - k\,(N_s - \phi(N_s) - \triangle)|}{e_s} &\leq \frac{|1 + k\,(N_s - \phi(N_s) - \triangle)|}{e_s} \\ &< \frac{1 + N^{\varrho}(N^{\beta})}{N^{\alpha}} \\ &= \frac{1 + N^{\varrho+\beta}}{N^{\alpha}} \\ &< \sqrt{r} N^{\varrho+\beta-\alpha}. \end{aligned}$$

Hence,

$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| < \sqrt{r} N^{\varrho+\beta-\alpha}.$$

We proceed to show the existence of integer $k$ and $t$ integers $d_s$. Taking $\varepsilon = \sqrt{r}N^{\varrho+\beta-\alpha}$ and $\varrho = \frac{t(\alpha-\beta)}{t+1}$. Then it gives

$$N^{\varrho}\varepsilon^t = N^{\varrho}\left(\sqrt{r}N^{\varrho+\beta-\alpha}\right)^t = (\sqrt{r})^t N^{\varrho+\varrho t+\beta t-\alpha t} = r^{\frac{t}{2}}.$$

Following Theorem 2.4, $r^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $r, t \geq 2$, then it gives $N^{\varrho}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $k < N^{\varrho}$ then $k < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \ldots, t$, yields

$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| < \varepsilon.$$

This clearly satisfies the conditions of Theorem 2.4, and proceeds to reveal the private keys $k$ and $t$ integers $d_s$ for $s = 1, \ldots, t$. Next from $e_s d_s - k\phi(N_s) = 1$ we make the following computations :

$$\begin{aligned} \phi(N_s) &= \frac{e_s d_s - 1}{k} \\ p_s^{r-1} &= \gcd(\phi(N_s), N_s) \\ q_s &= \frac{N_s}{p_s^r}. \end{aligned}$$

Finally, the prime factors $p_s$ and $q_s$ can be revealed which lead to the factorization of $t$ prime power moduli $N_s$ for $s = 1, \ldots, t$ and $r \geq 2$. □

Let

$$\begin{aligned} X_1 &= \frac{N_1 - 2^{\frac{2r+1}{r+1}} N_1^{\frac{r}{r+1}}}{e_1} \\ X_2 &= \frac{N_2 - 2^{\frac{2r+1}{r+1}} N_2^{\frac{r}{r+1}}}{e_2} \\ X_3 &= \frac{N_3 - 2^{\frac{2r+1}{r+1}} N_3^{\frac{r}{r+1}}}{e_3}. \end{aligned}$$

Define,

$$T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}].$$

Consider the lattice $\mathcal{L}$ spanned by the matrix,

$$M = \begin{bmatrix} \mathbf{1} & -[T(X_1)] & -[T(X_2)] & -[T(X_3)] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Taking $r \geq 2$, the matrix $M$ can be used in computing the reduced basis after applying the LLL algorithm

**Algorithm 3** Theorem 3.4

Initialization: The public key tuple $(N_s, e_s, \alpha, \beta, \varrho)$ satisfying Theorem 3.4.
Choose $r \geq 2$ and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
**for any** $(r, N, \alpha, \beta, \varrho)$ **do**
    $\varepsilon = \sqrt{r} N^{\varrho+\beta-\alpha}$
    $e =: \min\{e_s\} := N^{\alpha}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
**end for**
Consider the lattice $\mathcal{L}$ spanned by the matrix $M$ as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix $K$.
**for any** $(M, K)$ **do**
    $J := M^{-1}$
    $Q = JK$.
**end for**
Produce $d_s$, $k$ from $Q$
**for each** triplet $(d_s, k, e_s)$ **do**
    $\phi(N_s) := \frac{e_s d_s - 1}{k}$
    $p_s^{r-1} := \gcd(\phi(N_s), N_s)$.
    $q_s := \frac{N_s}{p_s^r}$
**end for**
**return** the prime factors $(p_s, q_s)$.

**Example 3.3.** *This example gives an illustration of how Theorem 3.4 works on 3 prime power moduli and their corresponding public exponents:*

$N_1 = 230752430767013072249887684293910718837040040071399248283866636915143445411611467379$

$N_2 = 434991743050236060915996189147523264755865914949477613614468188806740952003913552583$

$N_3 = 980914643623371382312729458097187264388503427621447777571718784533143406738292636683$

$e_1 = 629049148810559949841785049761568215700026226807264231457363256802126488638937888039$

$e_2 = 265035571511591897022174737291070924314658140619585199620247165205557379598308572799$

$e_3 = 424302253973827276427319770823031080967261427337097513012296323366084850555293675453.$

*Observe*

$N = \max\{N_1, N_2, N_3\} = 980914643623371382312729458097187264388503427621447777571718784533143406738292636683$

$e = \min\{e_1, e_2, e_3\} = 629049148810559949841785049761568215700026226807264231457363256802126488638937888039$

with $e = \min\{e_1, e_2, e_3\} = N^{\alpha}$ for $\alpha = 0.9857968390$. Taking $t = 3$, $\beta = 0.75$ it gives $\varrho = \frac{t(\alpha-\beta)}{t+1} = 0.1768476292$ and $\varepsilon = 0.00001937850804$.
Applying Theorem 2.4 and using Algorithm 3, we compute

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 287192882900000000000.$$

Consider the lattice $\mathcal{L}$ spanned by the matrix,

$$M = \begin{bmatrix} \mathbf{1} & -[T(X_1)] & -[T(X_2)] & -[T(X_3)] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, it yields the reduced basis with the following matrix

$$K = \begin{bmatrix} -64528041013590 & 22316660983540 & -14660675253070 & -23287047712390 \\ -833898253680997 & -1831141920267418 & -628510813959081 & 1059071291894963 \\ 509570466489060 & -4655727886202360 & -481050100124620 & -5658983802111740 \\ 5843566312885470 & 3758022552321180 & -17342920355447690 & -1610120341214130 \end{bmatrix}$$

Next, from Algorithm 3, we compute $Q = KJ$,

$$Q = \begin{bmatrix} -64528041013590 & -236706501307159 & -105907161352079 & -149177855554037 \\ -833898253680997 & -3058966845644782 & -1368642151792744 & -1927830928699482 \\ 509570466489060 & 1869243826365026 & 836336587427863 & 1178040248091503 \\ 5843566312885470 & 21435799310693196 & 9590799761610551 & 13509331410827634 \end{bmatrix}$$

From the first row of matrix $Q$, it yields the values for $k,\ d_1,\ d_2$ and $d_3$ as follows:

$$k = 64528041013590,\ d_1 = 236706501307159,$$
$$d_2 = 105907161352079,\ d_3 = 149177855554037.$$

Using Algorithm 3, $\phi(N_s) = \frac{e_s d_s - 1}{k}$ for $s = 1, 2, 3$ can be computed as follows,

$$\begin{aligned} \phi(N_1) = {} & 230752430767013072248776543267470057677453472488988696401562070407244760015236527680 \\ \phi(N_2) = {} & 434991743050236060914973940031031094365510983789392873571099791027040771533822542568 \\ \phi(N_3) = {} & 980914643623371382310759325156502208018839297372581980030651478359865012354849827664. \end{aligned}$$

Next, from Algorithm 3, $p_s^{r-1}$ for $s = 1, 2, 3$ and $r = 3$ can be computed as follows,

$$p_1 = 954408180105791988011,\ p_2 = 770755872323270534549,$$
$$p_3 = 994602670246108900363.$$

Finally, from Algorithm 3, $q_s$ for $s = 1, 2, 3$ can be computed as follows,

$$q_1 = 265426222155632917409,\ q_2 = 950015052524020374467,$$
$$q_3 = 996970609016663314889.$$

This shows the factorization of 3 prime power moduli $N_s = p_s^r q_s$ for $s = 1, 2, 3$ and $r = 3$ in polynomial time. Also, one can observe that our work yield $\min(d_1, d_2, d_3) \approx N^{0.1669}$ which is greater than $d \approx N^{0.1319}$, as reported in [14]. This shows that Shehu and Ariffin's attack can not yield the factorization of $t$ prime power moduli in this case.

3.2.3. *The Attack on t Prime Power Moduli $N_s = p_s^r q_s$ Satisfying System of Equation $e_s d - k_s \phi(N_s) = z_s$.*

This section considers another case in which $t$ prime power moduli satisfies equations of the form $e_s d - k_s \phi(N_s) = z_s$ for unknown positive integers $d,\ k_s,$ and $z_s$ for $s = 1, \ldots, t$.
Taking $r \geq 2$, let $N_s = p_s^r q_s,\ s = 1, \ldots, t$. The attack works for $t$ instances $(N_s, e_s)$ when there exists integer $d$ and $t$ integers $k_s$ such that $e_s d - k_s \phi(N_s) = z_s$ is satisfied. The attack shows that $t$ prime factors $p_s$ and $q_s$ of $t$ prime power moduli $N_s = p_s^r q_s$ for $s = 1, ..., t$ can be found efficiently for $N = \max\{N_s\}$ and $d < N^{\varrho},\ k_s < N^{\varrho},\ z_s < N^{\varrho},$ for all $\varrho = \frac{t(1-\beta)}{t+1}$ for $0 < \varrho \leq \frac{1}{2}$ and $o < \beta < 1$. In this case, the instances $(N_s, e_s)$ shared common decryption exponent $d$.

**Theorem 3.5.** *Let $N_s = p_s^r q_s$ be $t$ prime power moduli for $r \geq 2$ where $p_s$ and $q_s$ are prime numbers for $s = 1 \ldots, t$. Let $(e_s, N_s)$ be public key pair and $(d, N_s)$ be private key pair with condition $e_s < \phi(N_s)$ and relation $e_s d \equiv z_s \mod \phi(N_s)$ is satisfied. Let $N = \max\{N_s\}$. If there exists positive integer $d < N^{\varrho}$, $t$ integers $k_s < N^{\varrho}$ and $z_s < N^{\varrho}$, for all $\varrho = \frac{t(1-\beta)}{t+1}$ such that equation $e_s d - k_s \phi(N_s) = z_s$ holds, then prime factors $p_s$ and $q_s$ of $t$ prime power moduli $N_s$ can be successfully recovered in polynomial time for $0 < \varrho \leq \frac{1}{2}$ and $o < \beta < 1$.*

*Proof.* Suppose $N_s = p_s^r q_s$ be $t$ prime power moduli, $N = \max\{N_s\}$ and $k_s < N^{\varrho}$ for $r \geq 2$ and $s = 1, \ldots, t$. Then equation $e_s d - k_s \phi(N_s) = z_s$ can be rewritten as:

$$e_s d - k_s (N_s - (N_s - \phi(N_s)) = z_s.$$

Let $\triangle = 2^{\frac{2r+1}{r+1}} N_s^{\frac{r}{r+1}}$

$$e_s d - k_s \left(N_s - \triangle + \triangle - (N_s - \phi(N_s))\right) = z_s$$
$$e_s d - k_s (N_s - \triangle) = z_s - k_s (N_s - \phi(N_S) - \triangle)$$

$$\left| \frac{e_s}{N_s - \triangle} d - k_s \right| = \frac{|z_s - k_s (N_s - \phi(N_S) - \triangle)|}{N_s - \triangle}. \tag{3.2}$$

Since $N = \max\{N_S\}$ and $k_s < N^{\varrho}$, $z_s < N^{\varrho}$ are positive integers. Observe

$$|N_s - \phi(N_S) - \triangle| < N_s^{\beta} < N^{\beta}$$
$$N_s - \triangle > \frac{\sqrt{r+1}}{r} N$$

for $\beta \in (0,1)$. Then plugging the conditions into equation (3.2) yields

$$\begin{aligned}\frac{|z_s - k_s(N_s - \phi(N_S) - \triangle)|}{N_s - \triangle} &\leq \frac{|z_s + k_s(N_s - \phi(N_S) - \triangle)|}{N_s - \triangle} \\ &< \frac{N^{\varrho} + N^{\varrho}(N^{\beta})}{\frac{\sqrt{r+1}}{r}N} \\ &= \frac{r(N^{\varrho} + N^{\varrho+\beta})}{\sqrt{r+1}N} \\ &< \sqrt{2r+1}N^{\varrho+\beta-1}.\end{aligned}$$

Hence,

$$\left|\frac{e_s}{N_s - \triangle}d - k_s\right| < \sqrt{2r+1}N^{\varrho+\beta-1}.$$

We proceed to show the existence of an integer $d$, let $\varepsilon = \sqrt{2r+1}N^{\varrho+\beta-1}$, for $\varrho = \frac{t(1-\beta)}{t+1}$. Then it gives

$$N^{\varrho}\varepsilon^t = N^{\varrho}\left(\sqrt{2r+1}N^{\varrho+\beta-1}\right)^t = \left(\sqrt{2r+1}\right)^t N^{\varrho+\varrho t+\beta t-t} = (2r+1)^{\frac{t}{2}}.$$

Following Theorem 2.4, $(2r+1)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $r, t \geq 2$, then it gives $N^{\varrho}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $d < N^{\varrho}$, then $d < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \ldots, t$, yields

$$\left|\frac{e_s}{N_s - \triangle}d - k_s\right| < \varepsilon.$$

This clearly satisfies the conditions of Theorem 2.4, and proceeds to reveal the private key $d$ and $t$ integers $k_s$ for $s = 1, \ldots, t$. Next, from $e_s d - k_s\phi(N_s) = z_s$, we make the following computations:

$$\begin{aligned}\phi(N_s) &= \frac{e_s d - z_s}{k_s} \\ p_s^{r-1} &= \gcd(\phi(N_s), N_s) \\ q_s &= \frac{N_s}{p_s^r}.\end{aligned}$$

Finally, the prime factors $p_s$ and $q_s$ can be revealed which lead to the factorization of $t$ prime power moduli $N_s = p_s^r q_s$ for $r \geq 2$ and $s = 1, \ldots, t$ in polynomial time. □

Let

$$\begin{aligned}X_1 &= \frac{e_1}{N_1 - 2^{\frac{2r+1}{r+1}}N_1^{\frac{r}{r+1}}}, \; X_2 = \frac{e_2}{N_2 - 2^{\frac{2r+1}{r+1}}N_2^{\frac{r}{r+1}}}, \\ X_3 &= \frac{e_3}{N_3 - 2^{\frac{2r+1}{r+1}}N_3^{\frac{r}{r+1}}}.\end{aligned}$$

Define,

$$T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}].$$

Consider the lattice $\mathcal{L}$ spanned by the matrix,

$$M = \begin{bmatrix} 1 & -[T(X_1)] & -[T(X_2)] & -[T \times X_3] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Taking $r \geq 2$, the matrix $M$ can be used in computing the reduced basis after applying the LLL algorithm.

**Algorithm 4** Theorem 3.5

Initialization: The public key tuple $(N_s, e_s, \varrho, \beta)$ satisfying Theorem 3.5.
Choose $r \geq 2$ and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
**for any** $(r, N, \varrho, \beta)$ **do**
    $\varepsilon := \sqrt{2r+1} N^{\varrho+\beta-1}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
**end for**
Consider the lattice $\mathcal{L}$ spanned by the matrix $M$ as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix $K$.
**for any** $(M, K)$ **do**
    $J := M^{-1}$
    $Q = JK$.
**end for**
Produce $d$, $k_s$ from $Q$
**for each** tuple $(d, k_s, e_s, z_s)$ **do**
    $\phi(N_s) := \frac{e_s d - z_s}{k_s}$
    $p_s^{r-1} := \gcd(\phi(N_s), N_s)$.
    $q_s := \frac{N_s}{p_s^r}$
**end for**
**return** the prime factors $(p_s, q_s)$.

**Example 3.4.** *This example gives an illustration of how Theorem 3.5 works on 3 prime power moduli and their corresponding public exponents:*

$$\begin{aligned}
\textit{Let } N_1 &= 552589083079296395582963537637258987710502984397243532808096725056837793945542263311852509300451 \\
N_2 &= 409009336956200004848526206159753677602922864786417839660443537581155477440303212646889912922681 \\
N_3 &= 185659991588494772190286490085248886795864584720306578938229732631116403569017708089856336697379 \\
e_1 &= 535660672991610223946156685795497788662147614731651359062338800947852331357924924200110870181597 \\
e_2 &= 398146646185722474414615357316831702372730383621128736712077969303212977619132096891312620129374 \\
e_3 &= 209451368450111882047031899410363595522073297167725702489117049064722361040283841327245761880 13.
\end{aligned}$$

*Observe* $N = \max\{N_1, N_2, N_3\}$

$$N = 552589083079296395582963537637258987710502984397243532808096725056837793945542263311852509300451.$$

Using Algorithm 4 for $t = 3$ $r = 3$ and $\beta = 0.75$ gives $\varrho = \frac{t(1-\beta)}{t+1} = 0.1875$ and $\varepsilon = \sqrt{7}N^{\gamma+\beta-1} = 0.000002745673398$.
Applying Theorem 2.4 and using Algorithm 4 for $n = t = 3$, we compute

$$T = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 712622481500000000000000.$$

Consider the lattice $\mathcal{L}$ spanned by the matrix,

$$M = \begin{bmatrix} 1 & -[T(X_1)] & -[T(X_2)] & -[T \times X_3] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, it yields the reduced basis with the following matrix

$$K = \begin{bmatrix} 240575049922396781 & 45168467894653961 & -38707598398094518 & 195092642719432714 \\ -151248559543325924 & -488046878955018644 & 707575095426884472 & 620320224274381944 \\ -574956937086078187 & 491431650385399953 & -786566357699210214 & 209783791280367322 \\ -89655203762229785 & -1063060408191942085 & -430492105618860770 & 168843844246479710 \end{bmatrix}$$

Next, from Algorithm 4, we compute $Q = KJ$,

$$Q = \begin{bmatrix} 240575049922396781 & 233205101389831407 & 234185727874526165 & 27140351020204693 \\ -151248559543325924 & -146615102749620456 & -147231618648953995 & -17063028766409243 \\ -574956937086078187 & -557343294124629361 & -559686920366201207 & -64863472330366436 \\ -89655203762229785 & -86908641981956074 & -87274092461248535 & -10114405885730059 \end{bmatrix}$$

From the first row of matrix $Q$, it yields the values for $k$, $d_1$, $d_2$ and $d_3$ as follows:

$$d = 240575049922396781,\ k_1 = 233205101389831407,$$
$$k_2 = 234185727874526165,\ k_3 = 27140351020204693.$$

Using Algorithm 4, $\phi(N_s) = \frac{e_s d - z_s}{k_s}$ for $s = 1, 2, 3$ can be computed as follows, where $z_1, z_2, z_3$ are :

$$z_1 = 12594844191468409,\ z_2 = 7690976311642434,\ z_3 = 18446004731332273$$
$$\phi(N_1) = 552589083079296395582961635823819347184701123613286126361334990579765661347407538020846597914464$$
$$\phi(N_2) = 409009336956200004848524825976621275030379645558289047131769573374160014405441556077741716001204$$
$$\phi(N_3) = 185659991588494772190285551403327968148144196253737749368311956715037950804743239281977597971160.$$

Next, from Algorithm 4, $p_s^{r-1}$ for $s = 1, 2, 3$ and $r = 3$ can be computed as follows,

$$p_1 = 112105281561818170503691307,\ p_2 = 988706976202053289655339,$$
$$p_3 = 901538558587875149528599.$$

Finally, from Algorithm 4, $q_s$ for $s = 1, 2, 3$ can be computed as follows,

$$q_1 = 392214892049653107897457,\ q_2 = 423185157151460671796099,$$
$$q_3 = 253375960517480945644421.$$

This shows the factorization of 3 prime power moduli $N_s = p_s^r q_s$ simultaneously for $r \geq 2$ and $s = 1, \ldots, t$. From our result, one can also observe that our work yields $d \approx N^{0.18154}$. The equation $e_s d - k_s \phi(N_s) = z_s$ is a generalization of equation $e_i d - k_i \phi(N_i) = 1$, as reported in [14].

3.2.4. *The Attack on t Prime Power Moduli $N_s = p_s^r q_s$ Satisfying System of Equation $e_s d_s - k\phi(N_s) = z_s$.*

This section presents another cryptanalysis attack in which $t$ prime power moduli $N_s = p_s^r q_s$ satisfies equations of the form $e_s d_s - k\phi(N_s) = z_s$ for unknown positive integers $d_s,\ k,$ and $z_s$ for $s = 1, \ldots, t$ and $r \geq 2$ which can be simultaneously factored in polynomial time. In this case, every pair of the instances $(N_s, e_s)$ has its own unique decryption exponent $d_s$.

**Theorem 3.6.** *Let $N_s = p_s^r q_s$ be $t$ prime power moduli where $p_s$ and $q_s$ are prime numbers for $s = 1, \ldots, t$ and $t \geq 3$. Let $(e_s, N_s)$ be public key pair and $(d_s, N_s)$ be private key pair with $e_s < \phi(N_s)$ and relation $e_s d_s \equiv z_s \mod \phi(N_s)$ is satisfied. Let $e = \min\{e_s\} = N^\alpha$ be public exponent. If there exists positive $t$ integers $d_s < N^\varrho$, integer $k < N^\varrho$ and $t$ integers $z_s < N^\varrho$, for all $\varrho = \frac{t(\alpha-\beta)}{t+1}$ such that equation $e_s d_s - k\phi(N_s) = z_s$ holds, then prime factors $p_s$ and $q_s$ of $t$ prime power moduli $N_s = p_s^r q_s$ for $N_s$ and $r \geq 2$ can be successfully recovered in polynomial time for $0 < \varrho \leq \frac{1}{2}$, $0 < \beta < 1$ and $\beta < \alpha < 1$.*

*Proof.* Suppose $N_s = p_s^r q_s$ be $t$ prime power moduli and $e = \min\{e_s\} = N^\alpha$ be public exponent for $s = 1, \ldots t$ and suppose that $d_s < N^\varrho$, for $r \geq 2$ and $t \geq 3$. Then equation $e_s d_s - k\phi(N_s) = z_s$ can be rewritten as

$$e_s d_s - k(N_s - (N_s - \phi(N_s))) = z_s.$$

Let $\triangle = 2^{\frac{2r+1}{r+1}} N_s^{\frac{r}{r+1}}$

$$e_s d_s - k(N_s - \triangle + \triangle - (N_s - \phi(N_s))) = z_s$$
$$e_s d_s - k\left(N_s - \triangle\right) = z_s - k(N_s - \phi(N_s) - \triangle)$$
$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| = \frac{|z_s - k(N_s - \phi(N_s) - \triangle)|}{e_s}.$$

Since $N = \max\{N_s\}$ and $d_s < N^\varrho$, $k < N^\varrho$, $z_s < N^\varrho$. Observe

$$|N_s - \phi(N_s) - \triangle| < N_s^\beta < N^\beta$$

for $\beta \in (0, 1)$. Also since $e = \min\{e_s\} = N^\alpha$, for $s = 1, \ldots t$ then it gives

$$\begin{aligned}\frac{|z_s - k(N_s - \phi(N_s) - \triangle)|}{e_s} \leq & \frac{|z_s + k(N_s - \phi(N_s) - \triangle)|}{e_s} \\ & < \frac{N^{\varrho} + N^{\varrho}(N^{\beta})}{N^{\alpha}} \\ & = \frac{N^{\varrho} + N^{\varrho+\beta}}{N^{\alpha}} \\ & < \sqrt{r+2}N^{\varrho+\beta-\alpha}.\end{aligned}$$

Hence,

$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| < \sqrt{r+2}N^{\varrho+\beta-\alpha}.$$

We proceed to show the existence of integer $k$ and $t$ integers $d_s$. Let $\varepsilon = \sqrt{r+2}N^{\varrho+\beta-\alpha}$ and $\varrho = \frac{t(\alpha-\beta)}{t+1}$. Then it gives

$$N^{\varrho}\varepsilon^t = N^{\varrho}\left(\sqrt{r+2}N^{\varrho+\beta-\alpha}\right)^t = (\sqrt{r+2})^t N^{\varrho+\beta t-\alpha t} = (r+2)^{\frac{t}{2}}.$$

Following Theorem 2.4, $(r+2)^{\frac{t}{2}} < 2^{\frac{t(t-3)}{4}} \cdot 3^t$ for $r, t \geq 2$, then $N^{\varrho}\varepsilon^t < 2^{\frac{t(t-3)}{4}} \cdot 3^t$. It follows that if $k < N^{\varrho}$ then $k < 2^{\frac{t(t-3)}{4}} \cdot 3^t \cdot \varepsilon^{-t}$ for $s = 1, \ldots, t$, yields

$$\left| k\frac{(N_s - \triangle)}{e_s} - d_s \right| < \varepsilon.$$

This clearly satisfies the conditions of Theorem 2.4, and proceeds to reveal the private keys $t$ integers $d_s$ and $k$ for $s = 1, \ldots, t$. Next, from $e_s d_s - k\phi(N_s) = z_s$ we make the following computations:

$$\begin{aligned}\phi(N_s) &= \frac{e_s d_s - z_s}{k} \\ p_s^{r-1} &= \gcd(\phi(N_s), N_s) \\ q_s &= \frac{N_s}{p_s^r}.\end{aligned}$$

Finally, the prime factors $p_s$ and $q_s$ can be revealed which lead to the factorization of $t$ prime power moduli $N_s$ for $s = 1, \cdots, t$ in polynomial time. □

Let

$$X_1 = \frac{(N_1 - 2^{\frac{2r+1}{r+1}} N_1^{\frac{r}{r+1}}) + 1}{e_1},\ X_2 = \frac{(N_2 - 2^{\frac{2r+1}{r+1}} N_2^{\frac{r}{r+1}}) + 1}{e_2},\ X_3 = \frac{(N_3 - 2^{\frac{2r+1}{r+1}} N_3^{\frac{r}{r+1}}) + 1}{e_3}.$$

Define,

$$T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}].$$

Consider the lattice $\mathcal{L}$ spanned by the matrix,

$$M = \begin{bmatrix} \mathbf{1} & -[T(X_1)] & -[T(X_2)] & -[T(X_3)] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Taking $r \geq 2$, the matrix $M$ can be used in computing the reduced basis after applying the LLL algorithm

**Algorithm 5** Theorem 3.6

Initialization: The public key tuple $(N_s, e_s, \alpha, \beta, \varrho)$ satisfying Theorem 3.6.
Choose $r \geq 2$ and $N = \max\{N_s\}$ for $s = 1, \ldots, t$.
**for any** $(r, N, \alpha, \beta, \varrho)$ **do**
    $\varepsilon = \sqrt{r+2} N^{\varrho+\beta-\alpha}$
    $e =: \min\{e_s\} := N^{\alpha}$
    $T = [3^{t+1} \times 2^{\frac{(t+1)(t-4)}{4}} \times \varepsilon^{-t-1}]$ for $t \geq 2$.
**end for**
Consider the lattice $\mathcal{L}$ spanned by the matrix $M$ as stated above.
Applying the LLL algorithm to $\mathcal{L}$ yields the reduced basis matrix $K$.
**for any** $(M, K)$ **do**
    $J := M^{-1}$
    $Q = JK$.
**end for**
Produce $d_s$, $k$ from $Q$
**for each** triplet $(d_s, k, e_s, z_s)$ **do**
    $\phi(N_s) := \frac{e_s d_s - z_s}{k}$
    $p_s^{r-1} := \gcd(\phi(N_s), N_s)$.
    $q_s := \frac{N_s}{p_s^r}$
**end for**
**return** the prime factors $(p_s, q_s)$.

**Example 3.5.** *This example gives an illustration of how Theorem 3.6 works on 3 prime power moduli and their corresponding public exponents:*

$$N_1 = 118206700499027973555226065271614027133355822416165333781707131772561895107920252379$$

$$N_2 = 153187267586393370493787125781781250360337971520690436340144738974644921936384902153$$

$$N_3 = 924899290347826697102573577323286044355305745566432529788292084959590562885708269169$$

$$e_1 = 944721701896524093348103370244093137009660979547777813024924191503242413565332231 23$$

$$e_2 = 925995466598943224506439532320239713941284965387703819238402532258026161689224667 97$$

$$e_3 = 629828696197243558343755829089787763417070253274519076605922408153811221100854704887.$$

*Observe*

$$N = \max\{N_1, N_2, N_3\} = 924899290347826697102573577323286044355305745566432529782928420849595905628857082691 69$$

$$e = \min\{e_1, e_2, e_3\} = 925995466598943224506439532320239713941284965387703819238402532258026161689224667 97$$

with $e = \min\{e_1, e_2, e_3\} = N^{\alpha}$ for $\alpha = 0.9880965575$. Taking $t = 3$, $\beta = 0.75$ it gives $\varrho = \frac{t(\alpha-\beta)}{t+1} = 0.1785724181$,$\varepsilon = 0.00002246340004$ .
Applying Theorem 2.4 and using Algorithm 5, we compute

$$C = [3^{t+1} \cdot 2^{\frac{(t+1)(t-4)}{4}} \cdot \varepsilon^{-t-1}] = 159057099200000000000.$$

Consider the lattice $\mathcal{L}$ spanned by the matrix,

$$M = \begin{bmatrix} \mathbf{1} & -[T(X_1)] & -[T(X_2)] & -[T(X_3)] \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{bmatrix}$$

Therefore, by applying the LLL algorithm to $\mathcal{L}$, it yields the reduced basis with the following matrix

$$K = \begin{bmatrix} -192479622515690 & -477895645520 & -115255751942450 & 123625906116600 \\ 300578256728925 & 1229934560231400 & -602650460625375 & 38597963550500 \\ -1282731106006613 & 354397216043096 & -475121843615865 & -2396325179490180 \\ 1337229767906843 & -1481780789001256 & -3446686105094985 & -1015254431182020 \end{bmatrix}$$

Next, from Algorithm 5, we compute $Q = KJ$,

$$Q = \begin{bmatrix} -192479622515690 & -240836862805235 & -318418701848887 & -282655057392665 \\ 300578256728925 & 376093445279694 & 497246082783771 & 441397189459762 \\ -1282731106006613 & -1604995538518056 & -2122019818292808 & -1883682177099557 \\ 1337229767906843 & 1673186064806441 & 2212176859064010 & 1963713103001738 \end{bmatrix}$$

From the first row of matrix $Q$, it yields the values for $k$, $d_1$, $d_2$ and $d_3$ as follows:

$$k = 192479622515690, d_1 = 240836862805235,$$
$$d_2 = 318418701848887,\ d_3 = 282655057392665.$$

Using Algorithm 5, $\phi(N_s) = \frac{e_s d_s - z_s}{k}$ for $s = 1, 2, 3$ can be computed as follows, where $z_1, z_2, z_3$ are :

$$z_1 = 125587188015385, z_2 = 213104320451339, z_3 = 223377252772855$$

$$\begin{aligned} \phi(N_1) &= 11820670049902797355481221322408897920442751821218512043829912018031086126906939320 8 \\ \phi(N_2) &= 15318726758639337049331746232391674144929515448559432423497865399547577916624799544 0 \\ \phi(N_3) &= 92489929034782669710021054527475913748082630652189351887545856298944763886324402490 0. \end{aligned}$$

Next, from Algorithm 5, $p_s^{r-1}$ for $s = 1, 2, 3$ and $r = 3$ can be computed as follows,

$$p_1 = 601114833736581054997,\ p_2 = 601114833736581054997,$$
$$p_3 = 1161433282369002470551.$$

Finally, from Algorithm 5, $q_s$ for $s = 1, 2, 3$ can be computed as follows,

$$q_1 = 544214062088679626023,\ q_2 = 718297824560170977461,$$
$$q_3 = 590352823628934085319.$$

This shows the factorization of 3 prime power moduli $N_s = p_s^r q_s$ simultaneously for $r \geq 2$ and $s = 1, \ldots, t$. From our result, one can also observe that our work yields $\min(d_1, d_2, d_3) \approx N^{0.1712}$. The equation $e_s d_s - k\phi(N_s) = z_s$ is a generalization of equation $e_i d_i - k\phi(N_i) = 1$, as reported in [14].

## 4. Conclusion

In this paper, we developed new technique that led to the successful factorization of prime power modulus $N = p^r q$ for $r \geq 2$ via good approximation of $\phi(N)$. The paper also showed that using $N - \left\lceil 2^{\frac{2r+1}{r+1}} N^{\frac{r}{r+1}} \right\rceil$ as good approximation of $\phi(N)$ led to the extension of the bound to susceptible decryption exponent. The paper also presented four cryptanalysis attacks that successfully factored $t$ prime power moduli $N_s = p_s^r q_s$ for $s = 1, \ldots, t$ using generalized key equations of the form $e_s d - k_s\phi(N_s) = 1$, $e_s d_s - k\phi(N_s) = 1$, $e_s d - k_s\phi(N_s) = z_s$ and $e_s d_s - k\phi(N_s) = z_s$ . It has improved susceptible decryption exponent bounds of [14] from $d \approx N^{0.1857}$ to $d \approx N^{0.1863}$ and from $\min\{d_i\} \approx N^{0.1319}$ to $\min\{d_s\} \approx N^{0.1669}$. From these results, the paper generalized key equations of [14] from $e_i d - k_\phi(N_i) = 1$ to $e_s d - k_s\phi(N_s) = z_s$ and also from $e_i d_i - k\phi(N_i) = 1$ to $e_s d_s - k\phi(N_s) = z_s$.

## References


[1] A. Rivest, R. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM 21 **2** (1978) 120–126. .

[2] M. K. Dubey, N. Ratan, R. Verma, N. Saxena, *Cryptanalytic attacks and countermeasures on RSA*, in: P. K. (2014), In Proceedings of the Third International Conference on Soft Computing for Problem Solving, Springer, (2014), 10–18. .

[3] T. Fujioka, A. Okamoto, S. Miyaguchi, ESIGN, *An effient digital signature implementation for smart cards*, Advances in Cryptology EUROCRYPT 91, Lecture Notes in Computer Science, Springer, (1991), 446–457.

[4] T. Okamoto, S. Uchiyama, *A new public-key cryptosystem as secure as factoring*, in: Advances in Cryptology EUROCRYPT'98, Lecture Notes in Computer Science, Springer, (1998), 308–318.

[5] T. Takagi, *Fast RSA-type cryptosystem modulo $p^k q$*, in: Advances in Cryptology CRYPTO '98. CRYPTO 1998, Lecture Notes in Computer Science, Springer, (1998), 318–326.

[6] A. May, *Secret exponent attacks on RSA-type schemes with moduli $N = p^r q$*, in: Public Key Cryptography-PKC 2004, Springer, (2004), 218–230.

[7] S. Sarkar, *Small secret exponent attack on RSA variant with modulus $N = p^2 q$*, in: Proceedings International Workshop on Coding and Cryptography-WCC2013 Norway and INRIA, (2013), 215–222.

[8] R. Lu, Y. Zhang, D. Lin, *New results on solving linear equations modulo unknown divisors and its applications*, IACR Cryptology eprint **1** (2014) 343–354.

[9] S. Sarkar, *Revisiting prime power RSA*, Discrete Applied Mathematics **203**(C) (2016) 127–133.

[10] K. Itoh, K. Kunihiro, K. Kurosawa, *Small secret key attack on a variant of RSA (due to takagi)*, in: CT-RSA 2008, in:LNCS, (2008), 387–406.

[11] J. Blomer, A. May, *A generalized Wiener attack on RSA*, in: International Workshop on Public Key Cryptography, Springer, (2004), 1-13.

[12] J. Hinek, *On the security of some variants of RSA*, Phd thesis, Universiti Waterloo, Ontario, Canada (2007).

[13] A. Nitaj, M. Ariffin, D. Nassr, H. Bahig, *New Attacks on the RSA cryptosystem*, in: Progress in Cryptology AFRICACRYPT 2014. Lecture Notes in Computer Science, **8469**, Springer, (2014), 178-198.

[14] S. Shehu, M.R.K Ariffin, *New attacks on prime power RSA $N = p^r q$ using good approximation of $\phi(N)$*, Malaysian Journal of Mathematical Sciences special issues:The 5th International Cryptology and Information Security Conference(New Ideas in ) **11**(S) (2017) 121–138.

[15] H. Lenstra, A.K. Lenstra, L. Lovsz, *Factoring polynomials with rational coefficients*, Mathematische Annalen (1982) 513–534.

[16] A. Nitaj, *Diophantine and lattice cryptanalysis of the RSA cryptosystem*, in: Artificial Intelligence, Evolutionary Computing and Metaheuristics, Springer, (2013), 139-168.

[17] X. Wang, X. G., M. Wang, X. Meng, Mathematical Foundations of Public Key Cryptography, CRC Press, Boca Rating London New York, 2016.

Saidu Isah Abubakar,
Department of Mathematics, Sokoto State University , Sokoto, :+2348069191131, Orcid number:0000-0002-0201-0064
*Email address*: siabubakar82@gmail.com

Zaid Ibrahi,
Department of Mathematics, Sokoto State University, Sokoto ,+2348035780166: Orcid number:0000-0002-0251-6495
*Email address*: malamzaid2@gmail.com

Sadiq Shehu,
Department of Mathematics, Sokoto State University , Sokoto, +2348066284440: Orcid number:0000-0001-5908-7452
*Email address*: sadiqshehuzezi@gmail.com

Ahmad Rufai,
Department of Mathematics, Sokoto State University , Sokoto, +2347068272590: Orcid number:0000-0003-3223-9924
*Email address*: rufaiahmad35@yahoo.com

Proceedings of International Mathematical Sciences
ISSN:2717-6355, URL:https://dergipark.org.tr/tr/pub/pims
Volume II Issue 2 (2020), Pages 129-135. Doi: 10.47086/pims.778024

# A NOTE ON THE STABILITY OF SOLUTION FOR ELLIPTIC-SCHRÖDINGER TYPE NONLOCAL BOUNDARY VALUE PROBLEM

YILDIRIM OZDEMIR* AND MECRA ESER**
*DUZCE UNIVERSITY, KONURALP CAMPUSS, FACULTY OF ARTS AND SCIENCES, DUZCE, TURKEY. ORCID NUMBER:0000-0003-2767-522X
**DUZCE UNIVERSITY, DUZCE, TURKEY. ORCID NUMBER:0000-0002-2779-7190

Abstract. In the present article, a problem for an elliptic-Schrödinger equation with nonlocal boundary value condition is considered. The stability estimates are established for the solution of elliptic-Schrödinger problem. A theorem for stability of the solution of this problem and a conclusion section is presented.

## 1. introduction

In the present paper, the nonlocal boundary-value problem (NBVP)

$$\begin{cases} -\dfrac{d^2u(t)}{dt^2} + Au(t) = g(t)\,(0 \le t \le 1), \\ i\dfrac{du(t)}{dt} - Au(t) = f(t)\,(-1 \le t \le 0), \\ u(1) = u(-1) + \varphi \end{cases} \tag{1.1}$$

for differential equations of elliptic-Schrödinger type in a Hilbert space $H$ with self-adjoint positive definite operator $A$ is considered.

In the literature it is known that various NBVPs for the elliptic-Schrödinger equations can be reduced to the problem (1.1).

Whenever the following conditions are satisfied an abstract function $u(t)$ is called a solution of the problem (1.1):

i. $u(t)$ is twice continuously differentiable on the interval $(0, 1]$ and continuously differentiable on the segment $[-1, 1]$. The derivative at the endpoints of the segment are understood as the appropriate unilateral derivatives.

2020 *Mathematics Subject Classification.* 2010 MSC: 65L10, 34B10, 65M12.
*Key words and phrases.* partial differential equation; nonlocal boundary value problem; stability.

Submitted on August 07th, 2020. Published on 12.30.2020. Communicated by Sahin Uyaver.

ii. The element $u(t)$ belongs to $D(A)$ for all $t \in [-1,1]$, and the function $Au(t)$ is continuous on the segment $[-1,1]$.
iii. $u(t)$ satisfies the equations and nonlocal boundary condition (1.1).

There are also different type of works on elliptic and Schrödinger equations (see, for example, [13, 14, 15, 16] and references given therein).

Many scientists have been studied the methods of solutions of NBVPs for partial differential equations (PDEs) and PDEs of mixed type extensively (see, [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12] and references given therein).

## 2. The main theorem on stability

In the present section the stability estimates for elliptic-Schrödinger equations are obtained.

**Theorem 2.1.** *Suppose that $\varphi \in D(A)$ and $f(0), g(0) \in H$. Let $f(t)$ be continuously differentiable and $g(t)$ be twice continuously differentiable functions on $[-1,0]$ and $[0,1]$, respectively. Then, there is a unique solution of the problem (1.1) and the following stability inequalities hold:*

$$\max_{-1\le t\le 1}\|u(t)\|_H \le M\left[\|\varphi\|_H + \max_{-1\le t\le 0}\|f(t)\|_H + \max_{0\le t\le 1}\left\|A^{-1/2}g(t)\right\|_H\right] \tag{2.1}$$

$$\max_{-1\le t\le 1}\left\|\frac{du(t)}{dt}\right\|_H + \max_{-1\le t\le 1}\left\|A^{1/2}u(t)\right\|_H \tag{2.2}$$

$$\le M\left[\left\|A^{1/2}\varphi\right\|_H + \max_{-1\le t\le 0}\left\|A^{1/2}f(t)\right\|_H + \max_{0\le t\le 1}\|g(t)\|_H\right]$$

$$\max_{-1\le t\le 0}\left\|\frac{du(t)}{dt}\right\|_H + \max_{0\le t\le 1}\left\|\frac{d^2u(t)}{dt^2}\right\|_H + \max_{-1\le t\le 1}\|Au(t)\|_H \tag{2.3}$$

$$\le M\left[\|A\varphi\|_H + \|g(0)\|_H + \|f(0)\|_H + \max_{0\le t\le 1}\|g'(t)\|_H + \max_{-1\le t\le 0}\|f'(t)\|\right],$$

*where $M$ is independent of not only $f(t)$, $t \in [-1,0]$ but also $g(t)$, $t \in [0,1]$ and $\varphi$.*

**Proof.** First of all, we will obtain a formula for the solution of problem (1.1). It is known that there are unique solutions of the initial value problems

$$-\frac{d^2u(t)}{dt^2} + Au(t) = g(t), (0 \le t \le 1), u(0) = u_0, u(1) = u_1, \tag{2.4}$$

and

$$i\frac{du(t)}{dt} - Au(t) = f(t), (-1 \le t \le 0), u(0) = u_0 \tag{2.5}$$

that is,

$$u(t) = e^{-tA}u_0 - i\int_0^t e^{-i(t-s)A}f(s)\,ds, -1 \le t \le 0 \tag{2.6}$$

and

$$u(t) = \left(I - e^{-2A^{1/2}}\right)^{-1}\left[\left(e^{-tA^{1/2}} - e^{-(-t+2)A^{1/2}}\right)u_0 + \left(e^{-(1-t)A^{1/2}} - e^{-(t+1)A^{1/2}}\right)u_1\right] + \left(I - e^{-2A^{1/2}}\right)^{-1}\left(e^{-(1-t)A^{1/2}} - e^{-(t+1)A^{1/2}}\right) \tag{2.7}$$

$$\times \int_0^1 A^{-1/2} 2^{-1} \left( e^{-(1-s)A^{1/2}} - e^{-(s+1)A^{1/2}} \right) g(s) ds$$

$$- \int_0^1 A^{-1/2} 2^{-1} \left( e^{-(t+s)A^{1/2}} - e^{-|t-s|A^{1/2}} \right) g(s) ds, 0 \leq t \leq 1,$$

respectively. Using formulas (2.6), (2.7) and nonlocal boundary condition

$$u(1) = u(-1) + \varphi,$$

we get

$$u(t) = \left( I - e^{-2A^{1/2}} \right)^{-1} \left[ \left( e^{-tA^{1/2}} - e^{-(-t+2)A^{1/2}} \right) u_0 \right. \tag{2.8}$$

$$\left. + \left( e^{-(1-t)A^{1/2}} - e^{-(t+1)A^{1/2}} \right) \left( e^{iA} u_0 - i \int_0^{-1} e^{i(1+s)A} f(s) ds + \varphi \right) \right]$$

$$+ \left( I - e^{-2A^{1/2}} \right)^{-1} \left( e^{-(1-t)A^{1/2}} - e^{-(t+1)A^{1/2}} \right)$$

$$\times \frac{1}{2} \int_0^1 \left( e^{-(1-s)A^{1/2}} - e^{-(s+1)A^{1/2}} \right) A^{-1/2} g(s) ds$$

$$- \frac{1}{2} \int_0^1 \left( e^{-(t+s)A^{1/2}} - e^{-|t-s|A^{1/2}} \right) A^{-1/2} g(s) ds, 0 \leq t \leq 1.$$

Now, using the following

$$u'(0^+) = \frac{1}{i} \left[ Au(0) + f(0) \right],$$

we obtain the operator equation

$$\left\{ \left( I - e^{-2A^{1/2}} \right) + i \left( I + e^{-2A^{1/2}} \right) A^{-1/2} - 2iA^{-1/2} e^{-\left( A^{1/2} - iA \right)} \right\} u_0$$

$$= i \left\{ \left[ -2A^{-1/2} e^{-A^{1/2}} \left( i \int_0^{-1} e^{iA(-1+s)} f(s) ds + \varphi \right) \right] \right.$$

$$+ A^{-1} e^{-A^{1/2}} \int_0^1 \left( e^{-(1-s)A^{1/2}} - e^{-(s+1)A^{1/2}} \right) g(s) ds$$

$$\left. + i \left( I - e^{-2A^{1/2}} \right) A^{-1} f(0) + A^{-1} \left( I - e^{-2A^{1/2}} \right) \int_0^1 e^{-sA^{1/2}} g(s) ds \right\}.$$

Here, the operator

$$\left( I - e^{-2A^{1/2}} \right) + iA^{-1/2} \left( I + e^{-2A^{1/2}} \right) - 2iA^{-1/2} e^{-\left( A^{1/2} - iA \right)}$$

has an inverse,

$$T = \left[ \left( I - e^{-2A^{1/2}} \right) + iA^{-1/2} \left( I + e^{-2A^{1/2}} \right) - 2iA^{-1/2} e^{-\left( A^{1/2} - iA \right)} \right]^{-1}$$

and

$$\left\| A^{-1/2} T \right\|_{H \to H} \leq M \tag{2.9}$$

holds.

It is needed to obtain a formula for $u(0)$ for the solution of problem (1.1). To do this we must show that $T$ is a bounded operator. Let $A^{1/2} = B$. Since

$$A^{-1/2} T = \left[ \left( A^{1/2} - A^{1/2} e^{-2A^{1/2}} \right) + i \left( I + e^{-2A^{1/2}} \right) - 2ie^{-\left( A^{1/2} - iA \right)} \right]^{-1}$$

$$= \left[ \left( B - Be^{-2B} \right) + i \left( I + e^{-2B} \right) - 2ie^{-\left( B - iB^2 \right)} \right]^{-1}$$

we have that

$$\left\| A^{-1/2} T \right\|_{H \to H} \leq \sup_{\delta \leq \mu < \infty} \frac{1}{\mu - \mu e^{-2\mu} + i \left( 1 + e^{-2\mu} \right) - 2ie^{-\mu} e^{-i\mu^2}}.$$

Using Euler formula, we get

$$\beta(\mu) = \mu - \mu e^{-2\mu} + 2e^{-\mu} \sin \mu^2 + i \left( I + e^{-2\mu} - 2e^{-\mu} \cos \mu^2 \right).$$

Taking absolute value of $\beta(\mu)$, we obtain

$$|\beta(\mu)| = \sqrt{\begin{array}{l} \mu^2 + \mu^2 e^{-4\mu} + 4e^{-2\mu} \sin^2 \mu^2 - 2\mu^2 e^{-2\mu} + 4\mu e^{-\mu} \sin \mu^2 - 4\mu e^{-3\mu} \sin \mu^2 \\ +1 + e^{-4\mu} + 4e^{-2\mu} \cos^2 \mu^2 + 2e^{-2\mu} - 4e^{-\mu} \cos \mu^2 - 4e^{-3\mu} \cos \mu^2 \end{array}}$$

or

$$|\beta(\mu)| = \sqrt{\begin{array}{l} 1 + \mu^2 + \left( 1 + \mu^2 \right) e^{-\mu} + 4e^{-2\mu} + 2 \left( 1 - \mu^2 \right) e^{-2\mu} \\ +4\sqrt{1+\mu^2} e^{-\mu} \left[ \mu \left( \sqrt{1+\mu^2} \right)^{-1} \sin \mu^2 - \left( \sqrt{1+\mu^2} \right)^{-1} \cos \mu^2 \right] \\ -4\sqrt{1+\mu^2} e^{-3\mu} \left[ \mu \left( \sqrt{1+\mu^2} \right)^{-1} \sin \mu^2 + \left( \sqrt{1+\mu^2} \right)^{-1} \cos \mu^2 \right] \end{array}}.$$

Choosing $\frac{\mu}{\sqrt{1+\mu^2}} = \sin \alpha$ and $\frac{1}{\sqrt{1+\mu^2}} = \cos \alpha$, we can write

$$|\beta(\mu)| = \sqrt{\begin{array}{l} \left( 1 + \mu^2 \right) + \left( 1 + \mu^2 \right) e^{-4\mu} + 4e^{-2\mu} + 2 \left( 1 - \mu^2 \right) e^{-2\mu} \\ -4\sqrt{1+\mu^2} e^{-\mu} \cos \left( \mu^2 + \alpha \right) - 4\sqrt{1+\mu^2} e^{-3\mu} \cos \left( \mu^2 - \alpha \right) \end{array}}$$

$$\geq \sqrt{1 + \mu^2 + \left( 1 + \mu^2 \right) e^{-4\mu} + 2 \left( 1 - \mu^2 \right) e^{-2\mu} 4\sqrt{1+\mu^2} e^{-\mu} - 4\sqrt{1+\mu^2} e^{-3\mu}}.$$

Now, let

$$\psi(\mu) = \mu^2 + \left( 1 + \mu^2 \right) e^{-4\mu} + 2 \left( 1 - \mu^2 \right) e^{-2\mu} 4\sqrt{1+\mu^2} e^{-\mu} - 4\sqrt{1+\mu^2} e^{-3\mu}.$$

Hence, it is enough to prove the inequality $\psi(\mu) > 0$ for $\mu \geq \delta$. It is seen that for sufficiently large $\delta$ the inequality holds. Therefore,

$$\left\| A^{-1/2} T \right\|_{H \to H} \leq 1.$$

This means that $A^{-1/2} T$ is bounded. So,

$$u(0) = A^{-1/2} T \left( I - e^{-2A^{1/2}} \right) \left\{ i \int_0^1 A^{-1/2} e^{-sA^{1/2}} g(s)\, ds - A^{-1/2} f(0) \right\} \quad (2.10)$$

$$+ T e^{-A^{1/2}} A^{-1/2} \left\{ 2 \int_0^{-1} e^{iA(-1+s)} f(s)\, ds - 2i\varphi + i \int_0^1 \right.$$

$$\left. \times \left( e^{-(1-s)A^{1/2}} - e^{-(s+1)A^{1/2}} \right) A^{-1/2} g(s)\, ds \right\}.$$

Finally, we have formulas (2.6), (2.8) and (2.10) for the solution of the nonlocal boundary value problem (1.1).

Now, proofs of estimates (2.1), (2.2) and (2.3) will be given. Firstly, we consider (2.1). Using formula (2.10), we get

$$\|u(0)\|_H \leq \left\| A^{-1/2} T \right\|_{H \to H} \left\| I - e^{-2A^{1/2}} \right\|_{H \to H} \quad (2.11)$$

$$\times\left\{|i|\int_0^1\left\|e^{-sA^{1/2}}\right\|_{H\to H}\left\|A^{-1/2}g(s)\right\|_H ds+\left\|A^{-1/2}\right\|_{H\to H}\|f(0)\|_H\right\}$$
$$+\left\|e^{-A^{1/2}}\right\|_{H\to H}\left\|A^{-1/2}T\right\|_{H\to H}\left\{2\int_0^{-1}\left\|e^{iA(-1+s)}\right\|_{H\to H}\|f(s)\|_H ds+2|i|\,\|\varphi\|_H\right.$$
$$\left.+|i|\int_0^1\left(\left\|e^{-(1-s)A^{1/2}}\right\|_{H\to H}+\left\|e^{-(s+1)A^{1/2}}\right\|_{H\to H}\right)\left\|A^{-1/2}g(s)\right\|_H ds\right\}$$

or

$$\|u(0)\|_H\le M\left[\|\varphi\|_H+\max_{-1\le t\le 0}\|f(t)\|_H+\max_{0\le t\le 1}\left\|A^{-1/2}g(t)\right\|_H\right]. \tag{2.12}$$

Then, using formulas (2.6) and (2.8), we obtain for $-1\le t\le 0$

$$\|u(t)\|_H\le M\left[\|\varphi\|_H+\max_{-1\le t\le 0}\|f(t)\|_H+\max_{0\le t\le 1}\left\|A^{-1/2}g(t)\right\|_H\right] \tag{2.13}$$

and for $0\le t\le 1$

$$\|u(t)\|_H\le M\left[\|u(0)\|_H+\max_{-1\le t\le 0}\|f(t)\|_H+\|\varphi\|_H+\max_{0\le t\le 1}\left\|A^{-1/2}g(t)\right\|_H\right]. \tag{2.14}$$

Therefore, using estimates (2.12), (2.13) and (2.14), we complete proof of inequality (2.1).

Secondly, the proof of the estimate (2.2) will be obtained. Applying $A^{1/2}$ to (2.10) and taking the norm of it, we can write

$$\left\|A^{1/2}u(0)\right\|_H\le M\left[\left\|A^{1/2}\varphi\right\|_H+\max_{-1\le t\le 0}\left\|A^{1/2}f(t)\right\|_H+\max_{0\le t\le 1}\|g(t)\|_H\right]. \tag{2.15}$$

After that, applying $A^{1/2}$ to (2.6) and (2.8) and taking norm of them, we obtain

$$\left\|A^{1/2}u(t)\right\|_H\le\left\|A^{1/2}u(0)\right\|_H+\max_{-1\le t\le 0}\left\|A^{1/2}f(t)\right\|_H,\ -1\le t\le 0 \tag{2.16}$$

and

$$\left\|A^{1/2}u(t)\right\|_H\le M\left[\left\|A^{1/2}u(0)\right\|_H+\max_{-1\le t\le 0}\left\|A^{1/2}f(t)\right\|_H\right. \tag{2.17}$$
$$\left.+\left\|A^{1/2}\varphi\right\|_H+\max_{0\le t\le 1}\|g(t)\|_H\right],\ 0\le t\le 1.$$

Combining estimates (2.15), (2.16) and (2.17), we obtain (2.2).

Thirdly, the proof of the estimate (2.3) will be obtained. Using formula (2.6) and integration by parts, we get for $-1\le t\le 0$

$$u(t)=e^{-tA}u_0-A^{-1}\left\{\left[f(t)-e^{-itA}f(0)\right]-\int_0^t e^{-i(t-s)}f'(s)\,ds\right\}. \tag{2.18}$$

Using formula (2.8) and integration by parts, we get for $0\le t\le 1$

$$u(t)=\left(I-e^{-2A^{1/2}}\right)^{-1}\left[\left(e^{-tA^{1/2}}-e^{-(-t+2)A^{1/2}}\right)u_0\right. \tag{2.19}$$
$$+\left(e^{-(1-t)A^{1/2}}-e^{-(t+1)A^{1/2}}\right)$$
$$\left.\times\left(e^{iA}u_0-A^{-1}\left\{\left[f(-1)-e^{iA}f(0)\right]-\int_0^{-1}e^{i(1+s)A}f'(s)\,ds+\varphi\right\}\right)\right]$$

$$+\left(I-e^{-2A^{1/2}}\right)^{-1}\left(e^{-(1-t)A^{1/2}}-e^{-(t+1)A^{1/2}}\right)$$
$$\times\frac{1}{2}A^{-1}\left\{\left(I-e^{-2A^{1/2}}\right)g(1)-\int_0^1\left(e^{-(1-s)A^{1/2}}-e^{-(s+1)A^{1/2}}\right)g'(s)\,ds\right\}$$
$$-\frac{1}{2}A^{-1}\left\{\left[e^{-(1+t)A^{1/2}}-e^{-|1-t|A^{1/2}}\right]g(1)\right.$$
$$\left.-\int_0^1\left(e^{-(t+s)A^{1/2}}-e^{-|t-s|A^{1/2}}\right)g'(s)\,ds\right\}.$$

Lastly, using (2.10) and integration by parts, we get

$$u(0)=A^{-1/2}T\left(I-e^{-2A^{1/2}}\right) \tag{2.20}$$
$$\times\left\{-iA^{-1}\left[\left(e^{-A^{1/2}}g(1)-g(0)\right)-\int_0^1 e^{-sA^{1/2}}g'(s)\,ds\right]-A^{-1/2}f(0)\right\}$$
$$+A^{-1/2}Te^{-A^{1/2}}\left\{2A^{-1}\left[\left(e^{-2iA}f(-1)-e^{-iA}f(0)\right)-\int_0^{-1}e^{iA(-1+s)}f'(s)\,ds\right]-2i\varphi\right.$$
$$\left.+\frac{iA^{-1}}{2}\left[\left(I-e^{-2A^{1/2}}\right)g(1)-\int_0^1\left(e^{-(1-s)A^{1/2}}-e^{-(s+1)A^{1/2}}\right)g'(s)\,ds\right]\right\}.$$

Here, we can write

$$g(1)=g(0)+\int_0^1 g'(s)\,ds\quad\text{and}\quad f(-1)=f(0)+\int_{-1}^0 f'(s)\,ds.$$

Now, applying the operator $A$ to formulas (2.18), (2.19), (2.20) and taking their norm, we obtain

$$\|Au(0)\|_H\le M\left[\|A\varphi\|_H+\|g(0)\|_H+\|f(0)\|_H+\max_{0\le t\le 1}\|g'(t)\|_H\right. \tag{2.21}$$
$$\left.+\max_{-1\le t\le 0}\|f'(t)\|_H\right],$$
$$\|Au(t)\|_H\le M\left[\|Au_0\|_H+\|f(0)\|_H+\max_{-1\le t\le 0}\|f'(t)\|_H\right],-1\le t\le 0, \tag{2.22}$$
$$\|Au(t)\|_H\le M\left[\|Au_0\|_H+\|\varphi\|_H+\|g(0)\|_H+\|f(0)\|_H\right. \tag{2.23}$$
$$\left.+\max_{0\le t\le 1}\|g'(t)\|_H+\max_{-1\le t\le 0}\|f'(t)\|_H\right],0\le t\le 1.$$

Combining estimates (2.21), (2.22) and (2.23), we obtain inequality (2.3). This completes the proof of the main theorem.

## 3. Conclusion

In conclusion, the stability estimates for the solution of problem (1.1) for the elliptic-Schrödinger equation are established. Note that some results of this paper, without proof, were presented in [17, 18].

**Acknowledgments.** The author would like to sincerely thank Prof. Dr. Hüseyin ÇAKALLI and Prof. Dr. Allaberen ASHYRALYEV for his valuable supports.

## References


[1] M. S. Salahitdinov, Equations of Mixed-Composite Type, FAN, Tashkent, Uzbekistan, 1974.

[2] T. D. Drjuev, Boundary Value Problems for Equations of Mixed and Mixed-Composite Types, FAN, Tashkent, Uzbekistan, 1979.

[3] M. G. Karatopraklieva, *A nonlocal boundary value problem for an equation of mixed type*, Diff. Urav., **27** (1991), 68-79, in Russian.

[4] D. Bazarov and H. Soltanov, Some Local and Nonlocal Boundary Value Problems for Equations of Mixed and Mixed-Composite Types, Ylym, Ashgabat, Turkmenistan, 1995.

[5] S. N. Glazatov, Sobolev Inst. of Math. SB RAS, Preprint no: 46, 26p (1998).

[6] A. Ashyralyev, and Y. Ozdemir, *On nonlocal boundary value problems hyperbolic-parabolic equations* Taiwan. J. Math., **4** (2007), 1075-1089.

[7] A. Ashyralyev, and O. Gercek, *Nonlocal boundary value problems of elliptic-parabolic differential and difference equations*, Discrete. Dyn. Nat. Soc., **2008** (2008), 1-16.

[8] A. Ashyralyev, and A. Sirma, *Nonlocal boundary value problems for Shrödinger equations*, Comput. Math. Appl., **55** (2008), 392-407.

[9] A. Ashyralyev, and B. Hicdurmaz, *A note on the fractional Schrödinger differential equatios*, Kybernetes, **40** (2011), 736-750.

[10] A. Ashyralyev and O. Yıldırım, *On multipoint nonlocal boundary value problems for hyperbolic differential and difference equations*, Taiwan. J. Math., **14** (2010), 165-194.

[11] Y. Ozdemir, and M. Kucukunal, *A note on nonlocal boundary value problems for hyperbolic Schrödinger equations*, Abstr. Appl. Anal., **2012** (2012), 1-12.

[12] A. Ashyralyev, and O. Yıldırım, *A note on the second order accuracy stable difference schemes for the nonlocal boundary value hyperbolic problem*, Abstr. Appl. Anal., **2012** (2012), 1-29.

[13] P. Quittner and P. Souplet, *Optimal Lioville-type theorems for noncooperative elliptic Schrödinger systems and equations*, Comm. Math. Phys., **311** (2012), 1-19.

[14] B. Liu and L. Ma, *Symmetry results for eliiptic Schrödinger systems on half spaces*, J. Math. Anal. Appl., **401** (2013), 259-268.

[15] N. Godet and N. Tzvetkov, *Strichartz estimates for the periodic non-elliptic Schrödinger equation*, **350** (2012), 995-958.

[16] P. Souplet, *Lioville-type theorems for ellitic Schrödinger systems associated with copositive matrices*, Networks & Heterogeneous Media, **7** (2012), 697-988.

[17] Y. Ozdemir and M. Eser, *Numerical solution of the elliptic-Schrödinger equation with the Dirichlet and Neumann condition*, AIP Conf. Proc., **1611** (2014), 410-414.

[18] Y. Ozdemir and M. Eser, *On nonlocal boundary value problems for elliptic-Schrödinger equations*, AIP Conf. Proc., **1676** (2015).



Yildirim Ozdemir,
Duzce University, Konuralp Campuss, Faculty of Arts and Sciences, Duzce, Turkey. Phone: +(90) 544 686 5722, Orcid number:0000-0003-2767-522X
*Email address*: yozdemir28@gmail.com

Mecra Eser,
Duzce University, Duzce, Turkey. Orcid number:0000-0002-2779-7190