SIEVING POLYNOMIAL FOR FACTORIZATION OF NUMBERS OF THE FORM 
\[ n = m^5 + a_4 m^4 + a_3 m^3 + a_2 m^2 + a_1 m + a_0 \]  
FOR \( a_i << m \)

P. ANURADHA KAMESWARI*, G. SURYA KANTHAM

Department of Mathematics, Andhra University, Visakhapatnam - 530003, Andhra Pradesh, India

Copyright © 2019 the author(s). This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract. In the process of factorization of general integers in 1998 Zhang developed a method which can factor integers of the form \( n = m^3 + a_2 m^2 + a_1 m + a_0 \) for \( a_i << m \) by considering \( x = b_2 m^2 + b_1 m + b_0 \) and as in 2002 Eric Landquist[10] generalized the method for numbers of the form \( n = m^5 + a_0 \). In this paper going in the lines of Eric and using solutions of quadratic equation \( ax^2 + bxy + cy^2 = z^2 \) we proposed some parametrization for \( b_i \)'s that are non trivial by considering \( x = b_3 m^3 + b_2 m^2 + b_1 m + b_0 \) and obtained sieving polynomial for factoring of the numbers of the form \( n = m^5 + a_4 m^4 + a_3 m^3 + a_2 m^2 + a_1 m + a_0 \) with \( a_i << m \).

Keywords: factorization; quadratic equation; parametrization; sieving polynomial.

2010 AMS Subject Classification: 94A60, 11T71.

1. INTRODUCTION

In 1998 Zhang Mingzhi developed a method known as Special Quadratic Sieve by combining the ideas of Quadratic Sieve and Number Field Sieve methods. In special quadratic sieve Zhang [15] created a method with small residue for factorization of integers of the form \( n = m^3 + a_2 m^2 + a_1 m + a_0 \) with \( a_i << m \) and it was noticed that for large \( a_i \) the method becomes slower than Quadratic sieve. In 2002 Eric Landquist[9] generalized the method for numbers of the

*Corresponding author
E-mail address: panuradhakameswari@yahoo.in
Received July 31, 2019
form \( n = m^5 + a_0 \). In our paper [1] we proposed a nontrivial parametrization and constructed a sieving polynomial for numbers of the form \( n = m^k + a_0 \) for \( k = 4, 5 \); \( a_0 << m \). In our paper [2] we adapted these ideas to the numbers of the form \( n = m^4 + a_1 m + a_0 \) with \( a_1, a_0 << m \) and gave a sieving polynomial for factorization of \( n = m^4 + a_1 m + a_0 \).

In this paper going in the lines of Eric[10] and using solutions of quadratic equation \( ax^2 + bxy + cy^2 = z^2 \) we proposed some parametrization, that produce non trivial choices for \( b_i \)’s and obtained sieving polynomial for factoring the numbers of the form \( n = m^5 + a_4 m^4 + a_3 m^3 + a_2 m^2 + a_1 m + a_0 \) for \( a_i << m \) by considering \( x = b_3 m^3 + b_2 m^2 + b_1 m + b_0 \) This process is described in section 2 and in section 3 the efficiency of the sieving is discussed, an algorithm is given and an example with procedure is given.

2. **SIEVING POLYNOMIAL VIA PARAMETRIZATION FOR** \( n = m^5 + a_4 m^4 + a_3 m^3 + a_2 m^2 + a_1 m + a_0 \)

The quadratic sieve algorithm for factoring large numbers has several variations. The main idea is to come up with two different integers \( x \) and \( y \), such that \( x^2 \equiv y^2 \pmod{n} \) and \( x \neq y \pmod{n} \). Once such \( x \) and \( y \) are found, there is a chance that \( \gcd(x - y, n) \) and \( \gcd(x + y, n) \) gives non trivial factor of \( n \). In this section we propose to obtain this modular difference of squares for numbers of the form \( n = m^5 + a_4 m^4 + a_3 m^3 + a_2 m^2 + a_1 m + a_0 \) through a sieving polynomial.

Consider the numbers of the form \( n = m^5 + a_4 m^4 + a_3 m^3 + a_2 m^2 + a_1 m + a_0 \) with \( m, a_i \in \mathbb{Z} \) where \( i = 0, 1, 2, 3, 4 \) such that \( a_i << m \) and \( m = \lfloor n^{1/5} \rfloor \). We obtain difference of square \( x^2 \equiv y^2 \pmod{n} \) through several values of a polynomial \( f \) such that \( x^2 \equiv f \pmod{n} \) by taking \( x \) as below:

For \( b_i \in \mathbb{Z} \).

\[
x = b_3 m^3 + b_2 m^2 + b_1 m + b_0
\]

\[
x^2 \equiv f(b_3, b_2, b_1) \pmod{n}
\]

and \( f(b_3, b_2, b_1, b_0) \) is to be made a sieving polynomial with small residues. This leads certain conditions on \( b_0, b_1 \) and \( b_2 \) which can be met through some parameterizations for \( b_0, b_1, b_2, b_3 \).

In this section we propose a non trivial parametrization for \( b_0, b_1, b_2 \) and \( b_3 \) when \( n = m^5 + a_4 m^4 + a_3 m^3 + a_2 m^2 + a_1 m + a_0 \) for \( a_i << m \) for \( i = 0, 1, 2, 3, 4 \) that make \( f \) a sieving polynomial...
with small residue.

Here we describe in the following theorem the process of obtaining a non trivial parametrization for $b_3, b_2, b_1, b_0$ that makes $f(b_3, b_2, b_1, b_0)$ a sieving polynomial.

**Theorem 1.** Let $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$ with $m, a_i \in \mathbb{Z}$ where $i = 0, 1, 2, 3, 4$ such that $a_0 << m$ and $m = \lfloor n^{\frac{1}{5}} \rfloor$ then for $x = b_3m^3 + b_2m^2 + b_1m + b_0$, and $x^2 \equiv f(b_3, b_2, b_1, b_0) \pmod{n}$; then there is a non trivial parametrization for $b_3, b_2, b_1, b_0$ such that $f(b_3, b_2, b_1, b_0)$ is a sieving polynomial of small residue modulo $n$.

**Proof:** Given

(1) \[ n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0 \]

Let

\[ x = b_3m^3 + b_2m^2 + b_1m + b_0 \]

\[ x^2 = b_3^2m^6 + b_2^2m^4 + b_1^2m^2 + b_0^2 + 2b_3b_2m^5 + 2b_3b_1m^4 + 2b_2b_1m^3 + 2b_2b_0m^2 + 2b_1b_0m \]

and as

\[ m^5 \equiv -(a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0) \pmod{n} \]

\[ m^6 \equiv (a_4^2 - a_3)m^4 + (a_3a_4 - a_2)m^3 + (a_2a_4 - a_1)m^2 + (a_1a_4 - a_0)m + a_0a_4 \pmod{n} \]

we have

\[ x^2 \equiv m^4((a_4^2 - a_3)b_3^2 - 2b_3b_2a_4 + b_2^2 + 2b_3b_1) \]

\[ + m^3((a_3a_4 - a_2)b_3^2 - 2b_3b_2a_3 + 2b_3b_0 + 2b_2b_1) \]

\[ + m^2((a_2a_4 - a_1)b_3^2 - 2b_3b_2a_2 + b_1^2 + 2b_2b_0) \]

\[ + m((a_1a_4 - a_0)b_3^2 - 2b_3b_2a_1 + 2b_1b_0) + (a_0a_4b_3^2 - 2b_3b_2a_0 + b_0^2) \pmod{n} \]

\[ \equiv c_4m^4 + c_3m^3 + c_2m^2 + c_1m + c_0 \pmod{n} \]
for

\[ c_4 = (a_2^2 - a_3)b_3^2 - 2b_3b_2a_4 + b_2^2 + 2b_3b_1 \]
\[ c_3 = (a_3a_4 - a_2)b_3^2 - 2b_3b_2a_3 + 2b_3b_0 + 2b_2b_1 \]
\[ c_2 = (a_2a_4 - a_1)b_3^2 - 2b_3b_2a_2 + b_1^2 + 2b_2b_0 \]
\[ c_1 = (a_1a_4 - a_0)b_3^2 - 2b_3b_2a_1 + 2b_1b_0 \]
\[ c_0 = (a_0a_4b_3^2 - 2b_3b_2a_0 + b_0^2) \]

now to obtain a small quadratic residue we need \(c_4m^4 + c_3m^3 + c_2m^2 = 0\), that is

\[ m^4((a_2^2 - a_3)b_3^2 - 2b_3b_2a_4 + b_2^2 + 2b_3b_1) + m^3((a_3a_4 - a_2)b_3^2 - 2b_3b_2a_3 + 2b_3b_0 + 2b_2b_1) + m^2((a_2a_4 - a_1)b_3^2 - 2b_3b_2a_2 + b_1^2 + 2b_2b_0) = 0. \]

That is

\[ b_1m^2 + 2b_1m(b_3m^2 + b_2m) + b_3^2(a_2^2m^2 - a_3m^2 + a_3a_4m - a_2m + a_2a_4 - a_1) - 2b_2b_3(a_4m^2 + a_3m + a_2) + 2b_3b_0m + 2b_2b_0. \]

Now treating this as a quadratic equation in \(b_1\) we have

\[ b_1 = -(b_3m^2 + b_2m) \pm \sqrt{b_3^2(m^4 - a_2^2m^2 + a_3m^2 - a_3a_4m + a_2m - a_2a_4 + a_1) + 2b_2b_3(m^3 + a_4m^2 + a_3m + a_2) - 2b_3b_0m - 2b_2b_0} \]

Note an integer value for \(b_1\) can be evaluated whenever the term under the square root part is a perfect square. We parameterize the \(b_i\)'s of the term in the square root so that the term under the square root is a perfect square. Note the term in the square root is a quadratic form \(Q(u,v).\) When we parameterize \(b_i\)'s as \(b_i = k_{i_1}u + k_{i_2}v\) for \(i = 0, 2, 3.\) We have for

\[ b_0 = k_0u + k_1v \]
\[ b_2 = k_2u + k_3v \]
\[ b_3 = k_4u + k_5v \]

the term in the square root given as

\[ b_3^2(m^4 - a_2^2m^2 + a_3m^2 - a_3a_4m + a_2m - a_2a_4 + a_1) + 2b_2b_3(m^3 + a_4m^2 + a_3m + a_2) - 2b_3b_0m - 2b_2b_0 \]
\[ = u^2(k_4^2(m^4 - a_2^2m^2 - a_3a_4m + a_3m^2 - a_2a_4 + a_2m + a_1) + 2k_2k_4(a_4m^2 + a_3m + a_2) - 2k_0k_4m - 2k_0k_2) \]
Now by the formulas for the solutions of the equation \( Q(u, v) = z^2 \), as given in the theorem in [1] has solutions whenever \( a \) or \( c \) is a square. In particular for \( a = t^2 \) and if \( \frac{r}{s} \) is the fraction in its lowest terms we have the formulas for \( u, v, z \) given as

\[
\begin{align*}
    u &= \mu s \\
    v &= \mu \left( \frac{r + st}{\lambda} \right) \\
    z &= \mu r
\end{align*}
\]

Now \( Q(u, v) = u^2 (k_4^2 (m^4 - a_3^2 m^2 - a_3 a_4 m + a_3 m^2 - a_2 a_4 + a_2 m + a_1) + 2k_3 k_5 (m^3 + a_4 m^2 + a_3 m + a_2) - 2k_0 k_4 m - 2k_0 k_2) + 2uv(k_4 k_5 (m^4 - a_3^2 m^2 - a_3 a_4 m + a_3 m^2 - a_2 a_4 + a_2 m + a_1) + k_3 k_4 (m^3 + a_4 m^2 + a_3 m + a_2) - k_1 k_4 m - k_1 k_2 - k_0 k_5 m - k_0 k_3) + v^2(k_3^2 (m^4 - a_3^2 m^2 - a_3 a_4 m + a_3 m^2 - a_2 a_4 + a_2 m + a_1) + 2k_3 k_5 (m^3 + a_4 m^2 + a_3 m + a_2) - 2k_1 k_5 m - 2k_1 k_3)
\]

we transform \( Q(u, v) \) as the quadratic form as above by choosing \( k_i \)'s appropriately. In particular for \( k_4 = 0, k_0 = -2k, k_2 = k \) we have

\[
Q(u, v) = (4k^2)u^2 + uv(2kk_5 (m^3 + a_4 m^2 + a_3 m + a_2 + 2m) - 2kk_1 + 4kk_3) + v^2(k_3^2 (m^4 - a_3^2 m^2 - a_3 a_4 m + a_3 m^2 - a_2 a_4 + a_2 m + a_1) + 2k_3 k_5 (m^3 + a_4 m^2 + a_3 m + a_2) - 2k_1 k_3)
\]

\[
= au^2 + buv + cv^2
\]

\[
= z^2
\]
with

\[ a = (2k)^2 = t^2 \]

\[ b = 2kk_5(m^3 + a_4m^2 + a_3m + a_2 + 2m) - 2kk_1 + 4kk_3 \]

\[ c = k_5^2(m^4 - a_4^2m^2 - a_3a_4m + a_3m^2 - a_2a_4 + a_2m + a_1) + 2k_3k_5(m^3 + a_4m^2 + a_3m + a_2) - 2k_1k_3 \]

Then by the formulas above we have the term under the square root for \( b_1 \) is \( z^2 \), hence is a perfect square. Therefore for appropriate choices of \( k, k_1, k_3, k_5 \) we have non trivial parametrization for \( b_0, b_1, b_2, b_3 \) given as

\[ b_0 = -2ku + k_1v \]
\[ b_1 = -kmu \pm z \]
\[ b_2 = ku + k_3v \]
\[ b_3 = k_5v \]

Now substituting for \( b_2, b_1, b_0 \), we have \( f(b_3, b_2, b_1, b_0) \) given as

\[
\begin{align*}
  f(b_3, b_2, b_1, b_0) &= m((a_1a_4 - a_0)b_3^2 - (2b_3b_2a_1) + (2b_1b_0)) + (a_0a_4b_3^2) - (2b_3b_2a_0) + b_0^2 \\
  &= u^2(4k^2m^2 + 4k^2) + uv(4kk_5m^3 - 2kk_1m^2 + 4kk_3m^2 - 2a_1kk_5m - 2a_0kk_5 - 4kk_1) + v^2(-2k_1k_5m^3 + a_1a_4k_5^2m + a_0a_4k_5^2m - 2a_1k_3k_5m - a_0k_5^2m - 2k_1k_3m^2 - 2a_0k_3k_5 + k_1^2) + 4kmz \pm 2k_1mvz
\end{align*}
\]

Now to make \( f(b_3, b_2, b_1, b_0) = f(u, v) \) a small residue we take \( k_3 = -mk_5 \)

Therefore

\[
\begin{align*}
  f(u, v) &= u^2(4k^2(m^2 + 1)) + v^2(k_5^2(a_1a_4m + a_0a_4 - 2a_1m + a_0m) + k_1^2) - uv(2kk_1m^2 + 2a_1kk_5m + 2a_0kk_5 + 4kk_1) \mp 4zmk_1u \pm 2zmk_1v
\end{align*}
\]
Algorithm:

Step 0: (Initialize) \( n = \text{(number)}, \ m = \left\lfloor n^{\frac{1}{2}} \right\rfloor \)

\( a_4 = \left\lfloor \frac{n-5m}{m^5} \right\rfloor, \ a_3 = \left\lfloor \frac{n-5m-a_4m^4}{m^3} \right\rfloor, \ a_2 = \left\lfloor \frac{n-5m-a_4m^4-a_3m^2}{m} \right\rfloor, \ a_1 = \left\lfloor \frac{n-5m-a_4m^4-a_3m^2-a_2m^2-a_1m}{m} \right\rfloor, \ a_0 = \left\lfloor n - 5m - a_4m^4 - a_3m^3 - a_2m^2 - a_1m \right\rfloor \)

Let \( I = \{x_1, x_2, \cdots, x_r\} \) the set of integers in \( \left[ \left\lfloor -n^{\frac{1}{m}} \right\rfloor, \left\lceil n^{\frac{1}{m}} \right\rceil \right] \)

Step 1: Set

\[ \lambda = n_1 \in I. \]

\[ k = x_1 \in J. \]

\[ k_1 = x_1 \in J. \]

\[ k_5 = x_1 \in J. \]

\( f(b_3, b_2, b_1, b_0) \) is a sieving polynomial with modulo \( n \) for nontrivial parametrization of \( b_i \)'s as above.

3. Efficiency of Sieving with \( f(u, v, k, k_1, k_5) \)

For the polynomial \( f(u, v, k, k_1, k_5) \) as sieving polynomial with \( u = u(\lambda, \mu), v = v(\lambda, \mu) \) if all the parameters \( \lambda, \mu, k, k_1, k_5 \) are of order \( n^\varepsilon \) note \( f(u, v, k, k_1, k_5) \) is dominated by \( n^{\frac{5}{2}+8\varepsilon} \) to keep this below \( n^{\frac{1}{2}} \) in order to speed up over quadratic sieve we need to have \( n^{\frac{5}{2}+8\varepsilon} < n^{\frac{1}{2}} \), therefore \( \varepsilon \) is such that \( \varepsilon < \frac{1}{80} \), and the sieving interval for \( f(\lambda, \mu, k, k_1, k_5) \) is \( \left[ \left\lfloor -n^{\frac{1}{m}} \right\rfloor, \left\lceil n^{\frac{1}{m}} \right\rceil \right] \) and sieving can be proceeded by fixing a subset \( J \) of list of all integers in the range \( I = \{n_i\}_{i=1}^y \) for \( n_i \) integers in the range \( \left[ \left\lfloor -n^{\frac{1}{m}} \right\rfloor, \left\lceil n^{\frac{1}{m}} \right\rceil \right] \) and evaluating \( f(\lambda, \mu, k, k_1, k_5) \) for integer values of \( \lambda, \mu \in I \) and \( k, k_1, k_5 \in J \). Note that if the sieving polynomial does not yield non trivial factorization in the sieving interval then the sieving polynomial may be used with the parameters \( p \) replaced by \( q\sqrt{m} + p' \) for \( p' \) varying in \( \left[ \left\lfloor -n^{\frac{1}{m}} \right\rfloor, \left\lceil n^{\frac{1}{m}} \right\rceil \right] \) for \( q \geq (q\sqrt{m} + p')^2 < m. \)

An algorithm to evaluate \( f(\lambda, \mu, k, k_1, k_5), x(\lambda, \mu, k, k_1, k_5) \) is given in the following:

Algorithm:

Step 0: (Initialize) \( n = \text{(number)}, \ m = \left\lfloor n^{\frac{1}{2}} \right\rfloor \)

\( a_4 = \left\lfloor \frac{n-5m}{m^5} \right\rfloor, \ a_3 = \left\lfloor \frac{n-5m-a_4m^4}{m^3} \right\rfloor, \ a_2 = \left\lfloor \frac{n-5m-a_4m^4-a_3m^2}{m} \right\rfloor, \ a_1 = \left\lfloor \frac{n-5m-a_4m^4-a_3m^2-a_2m^2-a_1m}{m} \right\rfloor, \ a_0 = \left\lfloor n - 5m - a_4m^4 - a_3m^3 - a_2m^2 - a_1m \right\rfloor \)

Let \( I = \{x_1, x_2, \cdots, x_r\} \) the set of integers in \( \left[ \left\lfloor -n^{\frac{1}{m}} \right\rfloor, \left\lceil n^{\frac{1}{m}} \right\rceil \right] \)

Step 1: Set

\[ \lambda = n_1 \in I. \]

\[ k = x_1 \in J. \]

\[ k_1 = x_1 \in J. \]

\[ k_5 = x_1 \in J. \]
step 2: Compute

\[ t = (2k) \]
\[ b = 2kk5(m^3 + a_4m^2 + a_3m + a_2) - 2kk_1 \]
\[ c = k_5^2(-m^4 - 2a_4m^3 - a_3^2m^2 - a_3a_4m - a_3m^2 - a_2a_4 - a_2m + a_1) \]

and evaluate

\[ r = \lambda^2 t + b\lambda + ct \]
\[ s = \lambda^2 - c \]

and compute the fraction \( \frac{r}{s} \) in its lowest terms.

step 3: For \( \mu = \) multiple of \( \lambda \in I \)

compute

\[ u = s\mu \]
\[ v = \left( \frac{r + st}{\lambda} \right)\mu \]
\[ z = r\mu \]

compute

\[ X^+ = -2ku + k_1v + zm \]
\[ X^- = -2ku + k_1v - zm \]

\[ F^+ = (m)((a_1a_4 - a_0)b_3^2 - 2b_3b_2a_1 + 2b_1b_0) + a_0a_4b_3^2 - 2b_3b_2a_0 + b_0^2) \]
\[ = u^2(4k^2(m^2 + 1)) + v^2(k_5^2(a_1a_4m + a_0a_4 + 2a_1m + a_0m) + k_1^2) - uv(2kk_1m^2 + 2a_1kk_5m + 2a_0kk_5 + 4kk_1) - 4zmk_1u + 2zmk_1v \]

\[ F^- = u^2(4k^2(m^2 + 1)) + v^2(k_5^2(a_1a_4m + a_0a_4 + 2a_1m + a_0m) + k_1^2) - uv(2kk_1m^2 + 2a_1kk_5m + 2a_0kk_5 + 4kk_1) + 4zmk_1u - 2zmk_1v \]
print \((λ, \mu, k, k_1, k_5, X^+, F^+), & (λ, \mu, k, k_1, k_5, X^-, F^-)\)

**step 4:** Go to step 5 if \(k_5 = x_r\) else take \(k_5 = x_{1+}\) go to step 1

**step 5:** Go to step 6 if \(k_1 = x_r\) else take \(k_1 = x_{1+}\) go to step 1.

**step 6:** Go to step 7 if \(k = x_r\) else take \(k = x_{1+}\) go to step 1.

**step 7:** If \(λ = n_v\) stop else take \(λ = n_{1+}\) go to step 1.

**Example 1.** Factorization of \(n = 178499\): Note \(n\) is of the form 
\[n = m^5 + a_4 m^4 + a_3 m^3 + a_2 m^2 + a_1 m + a_0\] for \(m = \lfloor (n^{1/5}) \rfloor = 12,\ a_4 = 1,\ a_3 = 2,\ a_2 = 1,\ a_1 = 2\) and \(a_0 = 2\), now using the sieving polynomial given by above theorem (1) we compute the values of \(f(λ, \mu, k, k_1, k_5)\) for \(I = \{-2, -1, 2\} \subseteq [-2, 2]\) using the above algorithm and use the list of the values in the sieving for factorization.

Now for factorization we need a factor base \(B \approx L(n)^{1/2}\), where \(L(n) = e^{\sqrt{(\ln(n) \ln(\ln(n)))}}\) as in [7] in order to have a reasonable chance of factoring \(n\), using the factor base \(B\) we obtain \(F\) from the list of \(f(λ, \mu, k, k_1, k_5)\). For finding such \(F\) we go through the process of the sieve of Eratosthenes as given below:

For \(n = 178499, B = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}\)

\(I = \{-2, -1, 2\}\) and for the initial list of \(f(λ, \mu, k, k_3, k_5)\) given as

\[175500, 20440, 76176, 134800, 41561, 154105, 4199, 62951, 49247, 77142, 157300, 73305, 129426, 154105, 2873, 1856, 89913, 92625, 19044\]

The sieving with primes through \(B\), is as in the following table:
Table 1: Sieving $n = 178499$ with prime powers for primes in B

<table>
<thead>
<tr>
<th>175500</th>
<th>20440</th>
<th>41561</th>
<th>154105</th>
<th>4199</th>
<th>62951</th>
<th>49247</th>
<th>77142</th>
<th>157300</th>
<th>73305</th>
<th>129426</th>
<th>2873</th>
<th>1856</th>
<th>89913</th>
<th>92625</th>
<th>19044</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\downarrow^2$</td>
<td>87750</td>
<td>10220</td>
<td>41561</td>
<td>154105</td>
<td>4199</td>
<td>62951</td>
<td>49247</td>
<td>38571</td>
<td>78650</td>
<td>73305</td>
<td>64713</td>
<td>2873</td>
<td>928</td>
<td>89913</td>
<td>92625</td>
</tr>
<tr>
<td>$\downarrow^2$</td>
<td>29250</td>
<td>10220</td>
<td>41561</td>
<td>154105</td>
<td>4199</td>
<td>62951</td>
<td>49247</td>
<td>12857</td>
<td>78650</td>
<td>24435</td>
<td>21571</td>
<td>2873</td>
<td>928</td>
<td>29971</td>
<td>30875</td>
</tr>
<tr>
<td>$\downarrow^5$</td>
<td>14625</td>
<td>5110</td>
<td>41561</td>
<td>154105</td>
<td>4199</td>
<td>62951</td>
<td>49247</td>
<td>12857</td>
<td>39325</td>
<td>24435</td>
<td>21571</td>
<td>2873</td>
<td>464</td>
<td>29971</td>
<td>30875</td>
</tr>
<tr>
<td>$\downarrow^5$</td>
<td>2925</td>
<td>1022</td>
<td>41561</td>
<td>30821</td>
<td>4199</td>
<td>62951</td>
<td>49247</td>
<td>12857</td>
<td>38571</td>
<td>78650</td>
<td>24435</td>
<td>21571</td>
<td>2873</td>
<td>464</td>
<td>29971</td>
</tr>
<tr>
<td>$\downarrow^7$</td>
<td>146</td>
<td>41561</td>
<td>4403</td>
<td>323</td>
<td>8993</td>
<td>4477</td>
<td>989</td>
<td>55</td>
<td>1629</td>
<td>1961</td>
<td>221</td>
<td>232</td>
<td>29971</td>
<td>475</td>
<td>529</td>
</tr>
<tr>
<td>$\downarrow^{3^2}$</td>
<td>75</td>
<td>3197</td>
<td>4403</td>
<td>323</td>
<td>8993</td>
<td>4477</td>
<td>989</td>
<td>55</td>
<td>1629</td>
<td>1961</td>
<td>221</td>
<td>116</td>
<td>29971</td>
<td>475</td>
<td>529</td>
</tr>
<tr>
<td>$\downarrow^{17}$</td>
<td>75</td>
<td>3197</td>
<td>259</td>
<td>19</td>
<td>529</td>
<td>4477</td>
<td>989</td>
<td>55</td>
<td>1629</td>
<td>1961</td>
<td>13</td>
<td>116</td>
<td>1763</td>
<td>475</td>
<td>529</td>
</tr>
<tr>
<td>$\downarrow^{11}$</td>
<td>75</td>
<td>3197</td>
<td>259</td>
<td>1</td>
<td>529</td>
<td>4477</td>
<td>989</td>
<td>55</td>
<td>1629</td>
<td>1961</td>
<td>13</td>
<td>116</td>
<td>1763</td>
<td>25</td>
<td>529</td>
</tr>
<tr>
<td>$\downarrow^{23}$</td>
<td>75</td>
<td>3197</td>
<td>259</td>
<td>1</td>
<td>23</td>
<td>4477</td>
<td>43</td>
<td>55</td>
<td>1629</td>
<td>1961</td>
<td>13</td>
<td>116</td>
<td>1763</td>
<td>25</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{5^2}$</td>
<td>15</td>
<td>3197</td>
<td>259</td>
<td>1</td>
<td>23</td>
<td>4477</td>
<td>43</td>
<td>11</td>
<td>1629</td>
<td>1961</td>
<td>13</td>
<td>116</td>
<td>1763</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{3^3}$</td>
<td>5</td>
<td>3197</td>
<td>259</td>
<td>1</td>
<td>23</td>
<td>4477</td>
<td>43</td>
<td>11</td>
<td>543</td>
<td>1961</td>
<td>13</td>
<td>116</td>
<td>1763</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{29}$</td>
<td>5</td>
<td>3197</td>
<td>259</td>
<td>1</td>
<td>23</td>
<td>4477</td>
<td>43</td>
<td>11</td>
<td>543</td>
<td>1961</td>
<td>13</td>
<td>4</td>
<td>1763</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{31}$</td>
<td>5</td>
<td>3197</td>
<td>259</td>
<td>1</td>
<td>23</td>
<td>4477</td>
<td>43</td>
<td>11</td>
<td>543</td>
<td>1961</td>
<td>13</td>
<td>4</td>
<td>1763</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{25}$</td>
<td>5</td>
<td>3197</td>
<td>259</td>
<td>1</td>
<td>23</td>
<td>4477</td>
<td>43</td>
<td>11</td>
<td>543</td>
<td>1961</td>
<td>13</td>
<td>2</td>
<td>1763</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{37}$</td>
<td>5</td>
<td>3197</td>
<td>7</td>
<td>1</td>
<td>23</td>
<td>4477</td>
<td>43</td>
<td>11</td>
<td>543</td>
<td>53</td>
<td>13</td>
<td>2</td>
<td>1763</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{41}$</td>
<td>5</td>
<td>3197</td>
<td>7</td>
<td>1</td>
<td>23</td>
<td>121</td>
<td>43</td>
<td>11</td>
<td>543</td>
<td>53</td>
<td>13</td>
<td>2</td>
<td>43</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{43}$</td>
<td>5</td>
<td>3197</td>
<td>7</td>
<td>1</td>
<td>23</td>
<td>121</td>
<td>1</td>
<td>11</td>
<td>543</td>
<td>53</td>
<td>13</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{47}$</td>
<td>5</td>
<td>3197</td>
<td>7</td>
<td>1</td>
<td>23</td>
<td>121</td>
<td>1</td>
<td>11</td>
<td>543</td>
<td>53</td>
<td>13</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>$\downarrow^{5^4}$</td>
<td>1</td>
<td>73</td>
<td>139</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>181</td>
<td>53</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Through the sieving of Eratosthenes procedure we obtain B-smooth numbers as those $F$ with the values $f(\lambda, \mu, k, k_3, k_5)$ that are reduced to 1, while factoring with primes in B. The list of
prime factors of the B-smooth numbers and their indices, are given in the following table.

<table>
<thead>
<tr>
<th>X</th>
<th>F</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
</tr>
</thead>
<tbody>
<tr>
<td>113423</td>
<td>175500</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>96070</td>
<td>154105</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>86868</td>
<td>4199</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>58596</td>
<td>62951</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>31682</td>
<td>49247</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>58856</td>
<td>77142</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>82312</td>
<td>157300</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>2</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>178361</td>
<td>19044</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>11380</td>
<td>92625</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>27018</td>
<td>8913</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>98609</td>
<td>1856</td>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>42401</td>
<td>2873</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

We now look for relations modulo 2 between the rows of the above table. That we have from the first, third, seventh, ninth and last row contain $F_1 = 175500$, $F_3 = 4199$, $F_7 = 157300$, $F_9 = 92625$ and $F_{12} = 2873$ with prime factors 2, 3, 5, 11, 13, 17, 19 in B of even index. Now finding the corresponding $X_1, X_3, X_7, X_9, X_{12}$ we have for $X_1 = 113423$, $X_3 = 86868$, $X_7 = 82312$, $X_9 = 11380$, $X_{12} = 42401$. This leads to the congruence $(X_1 \cdot X_3 \cdot X_7 \cdot X_9 \cdot X_{12})^2 \equiv F_1 \cdot F_3 \cdot F_7 \cdot F_9 \cdot F_{12}(\mod n)$. That is $(113423 \cdot 86868 \cdot 82312 \cdot 11380 \cdot 42401)^2 \equiv (2^6 \cdot 3^2 \cdot 5^4 \cdot 11 \cdot 13^3 \cdot 17 \cdot 19)^2$ Thus $(6035)^2 \equiv (116947)^2$. Then we find a nontrivial factor of 178499 by combining the gcd(6035 + 116947, 178499) = 103.

4. Conclusion

In this paper sieving polynomials for factorization of the numbers of the form $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$ are obtained by considering $x = b_3m^3 + b_2m^2 + b_1m + b_0$ and giving non trivial parametrization for $b_i$’s through the solutions of quadratic equation $ax^2 +$
SIEVING POLYNOMIAL FOR FACTORIZATION...

\[
by + cy^2 = z^2 \text{ for } a \text{ or } c \text{ is a square. This process of arriving to a sieving polynomial of small residue for } n = m^5 + a_3m^3 + a_2m^2 + a_1m + a_0 \text{ is described. An algorithm for evaluating the values of sieving polynomials is given and the sieving process leading to factorization of } n \text{ is described in an example.}
\]

**Conflict of Interests**

The author(s) declare that there is no conflict of interests.

**REFERENCES**


[2] P. Anuradha Kameswari, G. Suryakantham, Sieving polynomials for factorization of numbers of the form \( n = m^4 + a_1m + a_0 \), J. Computer Math. Sci. in Press.


[15] Mingzhi, Zhang., Factorization of the Numbers of the form \( m^3 + c_2m^2 + c_1m + c_0 \), Springer-Verlag, London, 1998.