Available online at http://scik.org
J. Math. Comput. Sci. 9 (2019), No. 6, 784-795
https://doi.org/10.28919/jmcs/4240
ISSN: 1927-5307

SIEVING POLYNOMIAL FOR FACTORIZATION OF NUMBERS OF THE FORM $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$ FOR $a_i << m$

P. ANURADHA KAMESWARI*, G. SURYA KANTHAM

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

Abstract. In the process of factorization of general integers in 1998 Zhang developed a method which can factor integers of the form $n = m^3 + a_2m^2 + a_1m + a_0$ for $a_i << m$ by considering $x = b_2m^2 + b_1m + b_0$ 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 $x = b_3m^3 + b_2m^2 + b_1m + b_0$ and obtained sieving polynomial for factoring of the numbers of the form $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$ 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 $n = m^3 + a_2m^2 + a_1m + a_0$ 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 $n = m^4 + a_1m + a_0$ with $a_1, a_0 << m$ and gave a sieving polynomial for factorization of $n = m^4 + a_1m + a_0$.

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 $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$ for $a_i << m$ by considering $x = b_3m^3 + b_2m^2 + b_1m + b_0$ 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 $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$

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 $x^2 \equiv y^2 (\bmod n)$ and $x \not\equiv y (\bmod n)$. 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 $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$ through a sieving polynomial.

Consider the numbers of the form $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$ with $m,\ a_i \in \mathbb{Z}$ where $i = 0, 1, 2, 3, 4$ such that $a_i << m$ and $m = \lfloor n^{\frac{1}{5}} \rfloor$. We obtain difference of square $x^2 \equiv y^2 (\bmod n)$ through several values of a polynomial f such that $x^2 \equiv f (\bmod n)$ by taking x as below:

For $b_i\ \varepsilon\ \mathbb{Z}$.

$$x = b_3m^3 + b_2m^2 + b_1m + b_0$$

$$x^2 \equiv f(b_3, b_2, b_1)(\bmod n)$$

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 $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$ 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 $m,\ a_i\ \varepsilon\ \mathbb{Z}$ 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 $x^2 \equiv f(b_3, b_2, b_1, b_0)$ $(\bmod n)$; 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

$$n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0 \tag{1}$$

Let

$$x = b_3m^3 + b_2m^2 + b_1m + b_0$$

$$x^2 = b_3^2m^6 + b_2^2m^4 + b_1^2m^2 + b_0^2 + 2b_3b_2m^5 + 2b_3b_1m^4 + 2b_3b_0m^3 + 2b_2b_1m^3 + 2b_2b_0m^2 + 2b_1b_0m$$

and as

$$m^5 \equiv -(a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0)\ (\bmod n)$$

$$m^6 \equiv (a_4^2 - a_3)m^4 + (a_3a_4 - a_2)m^3 + (a_2a_4 - a_1)m^2 + (a_1a_4 - a_0)m + a_0a_4\ (\bmod n)$$

we have

$$\begin{aligned}
x^2 &\equiv m^4((a_4^2 - a_3)b_3^2 - 2b_3b_2a_4 + b_2^2 + 2b_3b_1) \\
&\quad + m^3((a_3a_4 - a_2)b_3^2 - 2b_3b_2a_3 + 2b_3b_0 + 2b_2b_1) \\
&\quad + m^2((a_2a_4 - a_1)b_3^2 - 2b_3b_2a_2 + b_1^2 + 2b_2b_0) \\
&\quad + m((a_1a_4 - a_0)b_3^2 - 2b_3b_2a_1 + 2b_1b_0) + (a_0a_4b_3^2 - 2b_3b_2a_0 + b_0^2)(\bmod n) \\
&\equiv c_4m^4 + c_3m^3 + c_2m^2 + c_1m + c_0(\bmod n)
\end{aligned}$$

for

$$c_4 = (a_4^2 - a_3)b_3^2 - 2b_3b_2a_4 + b_2^2 + 2b_3b_1$$

$$c_3 = (a_3a_4 - a_2)b_3^2 - 2b_3b_2a_3 + 2b_3b_0 + 2b_2b_1$$

$$c_2 = (a_2a_4 - a_1)b_3^2 - 2b_3b_2a_2 + b_1^2 + 2b_2b_0)$$

$$c_1 = (a_1a_4 - a_0)b_3^2 - 2b_3b_2a_1 + 2b_1b_0)$$

$$c_0 = (a_0a_4b_3^2 - 2b_3b_2a_0 + b_0^2)$$

now to obtain a small quadratic residue we need $c_4m^4 + c_3m^3 + c_2m^2 = 0$, that is $m^4((a_4^2 - a_3)b_3^2 - 2b_3b_2a_4 + b_2^2 + 2b_3b_1) + m^3((a_3a_4 - a_2)b_3^2 - 2b_3b_2a_3 + 2b_3b_0 + 2b_2b_1) + m^2((a_2a_4 - a_1)b_3^2 - 2b_3b_2a_2 + b_1^2 + 2b_2b_0) = 0$. That is $b_1m^2 + 2b_1m(b_3m^2 + b_2m) + b_3^2(a_4^2m^2 - a_3m^2 + a_3a_4m - a_2m + a_2a_4 - a_1) - 2b_2b_3(a_4m^2 + a_3m + a_2) + 2b_3b_0m + 2b_2b_0 = 0$. Now treating this as a quadratic equation in b_1 we have

$$b_1 = -(b_3m^2 + b_2m) \pm \sqrt{b_3^2(m^4 - a_4^2m^2 + a_3m^2 - a_3a_4m + a_2m - a_2a_4 + a_1) + 2b_2b_3(m^3 + a_4m^2 + a_3m + a_2) - 2b_3b_0m - 2b_2b_0}$$

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

$$b_3^2(m^4 - a_4^2m^2 + a_3m^2 - a_3a_4m + a_2m - a_2a_4 + a_1) + 2b_2b_3(m^3 + a_4m^2 + a_3m + a_2) - 2b_3b_0m - 2b_2b_0$$

$$= u^2(k_4^2(m^4 - a_4^2m^2 - a_3a_4m + a_3m^2 - a_2a_4 + a_2m + a_1) + 2k_2k_4(a_4m^2 + a_3m + a_2) - 2k_0k_4m - 2k_0k_2)$$

$+2uv(k_4k_5(m^4-a_4^2m^2-a_3a_4m+a_3m^2-a_2a_4+a_2m+a_1)+k_3k_4(m^3+a_4m^2+a_3m+a_2)+k_2k_5(m^3+a_4m^2+a_3m+a_2)-k_1k_4m-k_1k_2-k_0k_5m-k_0k_3)$

$+v^2(k_5^2(m^4-a_4^2m^2-a_3a_4m+a_3m^2-a_2a_4+a_2m+a_1)+2k_3k_5(m^3+a_4m^2+a_3m+a_2)-2k_1k_5m-2k_1k_3)$

$=au^2+buv+cv^2$

$=Q(u,v)$

$=z^2$

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

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

Now $Q(u,v)=u^2(k_4^2(m^4-a_4^2m^2-a_3a_4m+a_3m^2-a_2a_4+a_2m+a_1)+2k_2k_4(a_4m^2+a_3m+a_2)-2k_0k_4m-2k_0k_2)+2uv(k_4k_5(m^4-a_4^2m^2-a_3a_4m+a_3m^2-a_2a_4+a_2m+a_1)+k_3k_4(m^3+a_4m^2+a_3m+a_2)+k_2k_5(m^3+a_4m^2+a_3m+a_2)-k_1k_4m-k_1k_2-k_0k_5m-k_0k_3)+v^2(k_5^2(m^4-a_4^2m^2-a_3a_4m+a_3m^2-a_2a_4+a_2m+a_1)+2k_3k_5(m^3+a_4m^2+a_3m+a_2)-2k_1k_5m-2k_1k_3)$ 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

$$\begin{aligned}Q(u,v)&=(4k^2)u^2+uv(2kk_5(m^3+a_4m^2+a_3m+a_2+2m)-2kk_1+4kk_3)\\&\quad+v^2(k_5^2(m^4-a_4^2m^2-a_3a_4m+a_3m^2-a_2a_4+a_2m+a_1)+\\&\quad 2k_3k_5(m^3+a_4m^2+a_3m+a_2)-2k_1k_3)\\&=au^2+buv+cv^2\\&=z^2\end{aligned}$$

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

$$f(b_3, b_2, b_1, b_0) = m((a_1a_4 - a_0)b_3^2 - (2b_3b_2a_1) + (2b_1b_0)) + (a_0a_4b_3^2) - (2b_3b_2a_0) + b_0^2$$

$$= u^2(4k^2m^2 + 4k^2)+$$

$$uv(4kk_5m^3 - 2kk_1m^2 + 4kk_3m^2 - 2a_1kk_5m - 2a_0kk_5 - 4kk_1)+$$

$$v^2(-2k_1k_5m^3 + a_1a_4k_5^2m + a_0a_4k_5^2 - 2a_1k_3k_5m - a_0k_5^2m - 2k_1k_3m^2 -$$

$$2a_0k_3k_5 + k_1^2) \mp 4kmuz \pm 2k_1mvz$$

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

$$f(u, v) = u^2(4k^2(m^2 + 1)) + v^2(k_5^2(a_1a_4m + a_0a_4 - 2a_1m + a_0m) + k_1^2)-$$

$$uv(2kk_1m^2 + 2a_1kk_5m + 2a_0kk_5 + 4kk_1) \mp 4zmku \pm 2zmk_1v$$

$f(b_3, b_2, b_1, b_0)$ 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 $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$

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^{ε} note $f(u, v, k, k_1, k_5)$ is dominated by $n^{\frac{2}{5}+8\varepsilon}$ to keep this below $n^{\frac{1}{2}}$ in order to speed up over quadratic sieve we need to have $n^{\frac{2}{5}+8\varepsilon} < n^{\frac{1}{2}}$, therefore ε is such that $\varepsilon < \frac{1}{80}$, and the sieving interval for $f(\lambda, \mu, k, k_1, k_5)$ is $[\lceil -n^{\frac{1}{80}} \rceil, \lceil n^{\frac{1}{80}} \rceil]$ and sieving can be proceeded by fixing a subset J of list of all integers in the range $I = \{n_i\}_{i=1}^{\nu}$ for n_i integers in the range $[\lceil -n^{\frac{1}{80}} \rceil, \lceil n^{\frac{1}{80}} \rceil]$ 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 $[\lceil -n^{\frac{1}{80}} \rceil, \lceil n^{\frac{1}{80}} \rceil]$ for $q \ni (q\sqrt{m} + p')^2 << m$.

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) $n =$ (number), $m = \lfloor n^{\frac{1}{5}} \rfloor$

$a_4 = \lfloor \frac{n-m^5}{m^4} \rfloor$, $a_3 = \lfloor \frac{n-m^5-a_4m^4}{m^3} \rfloor$, $a_2 = \lfloor \frac{n-m^5-a_4m^4-a_3m^3}{m^2} \rfloor$

$a_1 = \lfloor \frac{n-m^5-a_4m^4-a_3m^3-a_2m^2}{m} \rfloor$, $a_0 = \lfloor n - m^5 - a_4m^4 - a_3m^3 - a_2m^2 - a_1m \rfloor$

Let $I = \{x_1, x_2, \cdots x_r\}$ the set of integers in $[\lceil -n^{\frac{1}{80}} \rceil, \lceil n^{\frac{1}{80}} \rceil]$

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

$$t = (2k)$$
$$b = 2kk_5(m^3 + a_4m^2 + a_3m + a_2) - 2kk_1$$
$$c = k_5^2(-m^4 - 2a_4m^3 - a_4^2m^2 - a_3a_4m - a_3m^2 - a_2a_4 - a_2m + a_1)$$

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

$$u = s\mu$$
$$v = (\frac{r + st}{\lambda})\mu$$
$$z = r\mu$$

compute

$$X^+ = -2ku + k_1v + zm$$
$$X^- = -2ku + k_1v - zm$$

$$F^+ = (m)((a_1a_4 - a_0)b_3^2 - 2b_3b_2a_1 + 2b_1b_0) + a_0a_4b_3^2 - 2b_3b_2a_0 + b_0^2)$$
$$= u^2(4k^2(m^2+1)) + v^2(k_5^2(a_1a_4m + a_0a_4 + 2a_1m + a_0m) + k_1^2) -$$
$$uv(2kk_1m^2 + 2a_1kk_5m + 2a_0kk_5 + 4kk_1) - 4zmku + 2zmk_1v$$
$$F^- = u^2(4k^2(m^2+1)) + v^2(k_5^2(a_1a_4m + a_0a_+2a_1m + a_0m) + k_1^2) -$$
$$uv(2kk_1m^2 + 2a_1kk_5m + 2a_0kk_5 + 4kk_1) + 4zmku - 2zmk_1v$$

print (λ, μ, k, k_1, k_5, X^+, F^+), & (λ, μ, k, k1, 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 $\lambda = n_\nu$ stop else take $\lambda = n_{1_+}$ go to step 1.

Example 1. Factorization of $n = 178499$: Note n is of the form $n = m^5 + a_4m^4 + a_3m^3 + a_2m^2 + a_1m + a_0$ 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 $f(\lambda, \mu, k, k_1, k_5)$ 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 $B \approx L(n)^{\frac{1}{\sqrt{2}}}$, 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 $f(\lambda, \mu, k, k_1, k_5)$. 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 $f(\lambda, \mu, k, k_3, k_5)$ 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

175500	20440	41561	154105	4199	62951	49247	77142	157300	73305	129426	2873	1856	89913	92625	19044
$\downarrow 2$															
87750	10220	41561	154105	4199	62951	49247	38571	78650	73305	64713	2873	928	89913	92625	19044
$\downarrow 2$															
29250	10220	41561	154105	4199	62951	49247	12857	78650	24435	21571	2873	928	29971	30875	3174
$\downarrow 2^2$															
14625	5110	41561	154105	4199	62951	49247	12857	39325	24435	21571	2873	464	29971	30875	3174
$\downarrow 5$															
2925	1022	41561	30821	4199	62951	49247	12857	7865	4887	21571	2873	464	29971	6175	1587
$\downarrow 7$															
2925	146	41561	4403	4199	8993	49247	12857	7865	4887	21571	2873	464	29971	6175	1587
$\downarrow 2^3$															
2925	73	41561	4403	4199	8993	49247	12857	7865	4887	21571	2873	232	29971	6175	1587
$\downarrow 3^2$															
975	73	41561	4403	4199	8993	49247	12857	7865	1629	21571	2873	232	29971	6175	529
$\downarrow 11$															
975	73	41561	4403	4199	8993	4477	12857	715	1629	1961	2873	232	29971	6175	529
$\downarrow 13$															
75	73	3197	4403	323	8993	4477	989	55	1629	1961	221	232	29971	475	529
$\downarrow 2^4$															
75	73	3197	4403	323	8993	4477	989	55	1629	1961	221	116	29971	475	529
$\downarrow 17$															
75	73	3197	259	19	529	4477	989	55	1629	1961	13	116	1763	475	529
$\downarrow 19$															
75	73	3197	259	1	529	4477	989	55	1629	1961	13	116	1763	25	529
$\downarrow 23$															
75	73	139	259	1	23	4477	43	55	1629	1961	13	116	1763	25	23
$\downarrow 5^2$															
15	73	139	259	1	23	4477	43	11	1629	1961	13	116	1763	5	23
$\downarrow 3^3$															
5	73	139	259	1	23	4477	43	11	543	1961	13	116	1763	5	23
$\downarrow 29$															
5	73	139	259	1	23	4477	43	11	543	1961	13	4	1763	5	23
$\downarrow 31$															
5	73	139	259	1	23	4477	43	11	543	1961	13	4	1763	5	23
$\downarrow 2^5$															
5	73	139	259	1	23	4477	43	11	543	1961	13	2	1763	5	23
$\downarrow 37$															
5	73	139	7	1	23	121	43	11	543	53	13	2	1763	5	23
$\downarrow 41$															
5	73	139	7	1	23	121	43	11	543	53	13	2	43	5	23
$\downarrow 43$															
5	73	139	7	1	23	121	1	11	543	53	13	2	1	5	23
$\downarrow 47$															
5	73	139	7	1	23	121	1	11	543	53	13	2	1	5	23
$\downarrow 5^4$				$\downarrow 7^2$	$\downarrow 23^2$	$\downarrow 11^3$		$\downarrow 11^2$	$\downarrow 3^5$		$\downarrow 13^2$	$\downarrow 2^7$	1	$\downarrow 5^4$	$\downarrow 23^2$
1	73	139	1	1	1	1	1	1	181	53	1	1	1	1	1

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 2: List of X, F for primes in B

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

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$(X_1 \cdot X_3 \cdot X_7 \cdot X_9 \cdot X_{12})^2 \equiv F_1 \cdot F_3 \cdot F_7 \cdot F_9 \cdot F_{12} (\bmod n)$. That is $(113423 \cdot 86868 \cdot 82312 \cdot 11380 \cdot 42401)^2 \equiv (2^2 \cdot 3^2 \cdot 5^4 \cdot 11 \cdot 13^3 \cdot 17 \cdot 19)^2$ 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 $n = m^5 + a_4 m^4 + a_3 m^3 + a_2 m^2 + a_1 m + a_0$ are obtained by considering $x = b_3 m^3 + b_2 m^2 + b_1 m + b_0$ and giving non trivial parametrization for b_i's through the solutions of quadratic equation $ax^2 +$

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

Conflict of Interests

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

REFERENCES

[1] P. Anuradha Kameswari, G. Suryakantham, Sieving polynomials for factorization of numbers of the form $n = m^k + a_0$ for $k = 4,5$, Int. J. Appl. Eng. Res. 14 (4) (2019), 908 - 916.

[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.

[3] Tom M.Apostol, Introduction to Analytic number theory Springer Verlag, New York, 1989.

[4] Baker, A., A Comprehensive Course in Number Theory, Cambridge University Press, 2012.

[5] D. Burton, Elementary Number Theor Sixth ed, Mc Graw Hill, New York, 2007.

[6] Dickson Leonard Eugene, History of the Theory of Numbers, Volume II, Chelsea Publishing Company, 1919.

[7] Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman, An Introduction to Mathematical Cryptography, Springer, 2008.

[8] Hardy GH., Wright EM., An introduction to the theory of numbers, Oxford University Press, 1979.

[9] Neal Koblitz, A course in number theory and cryptography, Springer Science & Business Media, 1994.

[10] Landquist, E., An implementation of Zhang's Special Quadratic Sieve and Possible Extension, Math 488 (2002), 1-18.

[11] I. Niven, H. S. Zuckerman, and H.L. Montgomery, An Introduction to the Theory of Numbers, Fifth Edition, John Wiley & Sons, New York, 1991.

[12] Crandall, R. and Pomerance, C., Prime Numbers: A Computational Perspective, Springer Science & Business Media, 2005.

[13] Riesel,H., Prime Numbers and Computer Methods for Factorization, Revised and corrected second printing, Birkh*ä*user Inc, 1987.

[14] Landquist, E., Possible ways to extend Zhang's Special Quadratic Sieve, June 4, 2003.

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