IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 12, Issue 5 Ver. III (Sep. - Oct.2016), PP 19-29
www.iosrjournals.org

Factorization via Difference of Squares using Ambiguous Forms

P Anuradha Kameswari[1] K Vijaya Prasamsa[2] G Surya Kantham[3]
Department of Mathematics, Andhra University,India

Abstract:*In this paper we propose to obtain a factorization via a modular difference of squares , where the squares arise due to binary quadratic forms. To obtain the quadratic forms we adapt Zhang's method of parametrization used in his special quadratic sieve method. A certain linear parametrization in two variables leads to quadratic form in ambiguous forms* $(a,0,c)$ *and* (a,a,c) *with* a *or* c *square. It is shown that there are the solutions of the equation* $au^2+cv^2=z^2$ *and* $au^2+auv+cv^2=z^2$ *leading to non trivial factorization of* n*, via difference of squares.*

Keywords: *Quadratic Forms, Factorization, Ambiguous Forms.*

I. Introduction

There are many attempts to find faster ways to factor composite numbers.The methods like Trial Division, Fermat method, Pollard's p-1 and ρ methods, Continued Fraction method, Elliptic Curve method by Lenstra, Quadratic Sieve and Number Field Sieve method are the known methods to factor a composite number[7]. Quadratic Sieve, was invented by Carl Pomerance in 1981. The quadratic sieve was the fastest known algorithm until the Number Field Sieve was discovered in 1993 and the quadratic sieve is faster than the number field sieve for numbers upto 110 digits long. 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 a non trivial factor of n [8] .

II. Implementing Zhang's Idea Of Parametrization To Obtain A Binary Quadratic Form

In 1998 M.Zhang [1] created a method of making the residues smaller than the quadratic sieve does normally, but only for certain integers n, thus his sieve is called the special quadratic sieve. Now to obtain a binary quadratic form, by implementing Zhang's idea of parametrization, for factoring n, suppose $n = m^3 + a_2 m^2 + a_1 m + a_0$ with $m, a_i \in Z, i = 0,1$ &2and $m = \lfloor n^{\frac{1}{3}} \rfloor$. For $b_i \in Z$,let $x = b_2 m^2 + b_1 m + b_0$ then $x^2 = b_2^2 m^4 + 2b_1 b_2 m^3 + (2b_0 b_2 + b_1^2) m^2 + 2b_0 b_1 m + b_0^2$ with the same conditions on m as in the above equation.we have

$$m^3 \equiv -a_2 m^2 - a_1 m - a_0 (\bmod n)$$

$$m^4 \equiv (a_2^2 - a_1) m^2 + (a_1 a_2 - a_0) m + a_1 a_2 (\bmod n)$$ Then by substitution for m^3 & m^4,

we have $x^2 \equiv c_2 m^2 + c_1 m + c_0 (\bmod n)$ with

$$c_1 = (a_1 a_2 - a_0) b_2^2 - 2a_1 b_1 b_2 + 2b_0 b_1$$

$$c_2 = (a_2^2 - a_1) b_2^2 - 2a_2 b_1 b_2 + b_1^2 + 2b_0 b_2$$

$$c_0 = a_0 a_2 b_2^2 - 2a_0 b_1 b_2 + b_0^2$$

Taking $y = c_2 m^2 + c_1 m + c_0$, Zhang has considered single variable parametrization and double parametrization for b_i's such that $c_2 = 0$ and proposed sieving methods to obtain $y(u,v)$ as a square.In this paper we propose to transform this congruence with certain choices of b_2, b_1, b_0 so that y is a binary quadratic form. A two variable linear parametrization for b_i's is required for this and is given as follows:

For $n = m^3 + a_0; m = \lfloor n^{\frac{1}{3}} \rfloor$ and $b_2 = k_1 u + k_2 v$

$$b_1 = k_3 u + k_4 v$$

$$b_0 = k_5 u + k_6 v \text{、}$$

for $k_i \varepsilon Z ; \forall i = \{1,2,3,4,5,6\}$. Now substituting for b_2, b_1, b_0 , we have

$x^2 = c_2 m^2 + c_1 m + c_0 = y(u,v)$, a binary quadratic form given as

$$y(u,v) = (b_1^2 + 2b_0 b_2)m^2 + (-a_0 b_2^2 + 2b_0 b_1)m - 2a_0 b_1 b_2 + b_0^2$$

$$= [(k_3 u + k_4 v)^2 + 2(k_5 u + k_6 v)(k_1 u + k_2 v)]m^2 \quad + [-a_0 (k_1 u + k_2 v)^2 + 2(k_5 u + k_6 v)(k_3 u + k_4 v)]m$$

$$- 2a_0 (k_3 u + k_4 v)(k_1 u + k_2 v) + (k_5 u + k_6 v)^2$$

$$= (k_3^2 m^2 + 2k_5 k_1 m^2 - a_0 k_1^2 m + 2k_5 k_3 m - 2a_0 k_1 k_3 + k_5^2)u^2$$

$$+ (k_3 k_4 m^2 + k_6 k_1 m^2 + k_5 k_2 m^2 - a_0 k_1 k_2 m + k_6 k_3 m \quad + k_5 k_4 m - a_0 k_3 k_2 - a_0 k_4 k_1 + k_5 k_6) 2uv$$

$$+ (k_4^2 m^2 + 2k_6 k_2 m^2 - a_0 k_2^2 m + 2k_6 k_4 m - 2a_0 k_4 k_2 + k_6^2)v^2$$

Note $y(u,v)$ is a binary quadratic form in u , v and we have for $x = x(u,v)$

$$(x(u,v))^2 \equiv y(u,v) (\bmod n)$$

Therefore for a factorization via difference of squares in the next section , we look for the cases when $y(u,v)$ is a square.

III. Factorization Via Difference Of Squares Using Ambiguous Forms

A Binary Quadratic form in x,y given by $Ax^2 + Bxy + Cy^2$ is represented as (A, B, C) [9][10] and the forms $(A,0,C)$ and (A, A, C) are called Ambiguous Forms. In this factorization via differnce of squares our main aim is to express $y(u,v)$ as a square, for this, the Binary Quadratic form $y(u,v)$ obtained above is first transformed as an ambiguous form in u, v as $(a,0,c)$ and (a,a,c) with a or c is a square and then we consider the equations

$$y(u,v) = au^2 + cv^2 = z^2 \text{ and}$$

$$y(u,v) = au^2 + auv + cv^2 = z^2$$

Note the two equations are of the form $ax^2 + bxy + cy^2 = z^2$ with a or c is a square and by the study of solution to this equation in [12],History of the Theory of Numbers, a complete solution for the equation is given by E.So's as follows:

Consider the equation $au^2 + buv + cv^2 = z^2$ such that a or c is a square.Suppose a is a square, let $a = t^2$, for some $t \in z$,then we have

$$t^2 u^2 + buv + cv^2 = z^2$$

$$\Rightarrow v(bu + cv) = z^2 - t^2 u^2$$

By setting $\dfrac{z + tu}{v} = \dfrac{bu + cv}{z - tu} = \lambda (say)$

we have

$$z + tu = v\lambda$$

$$\Rightarrow cz + ctu = cv\lambda$$

$$\Rightarrow cz + ctu = [\lambda(z - tu) - bu]\lambda$$

$$\Rightarrow z(c - \lambda^2) = -u(tc + t\lambda^2 + b\lambda)$$

$$\Rightarrow \frac{z}{u} = \frac{t\lambda^2 + b\lambda + tc}{\lambda^2 - c}$$

$$\Rightarrow z = lu \text{ for}$$

$$l = \frac{t\lambda^2 + b\lambda + tc}{\lambda^2 - c} = \frac{r}{s}$$

where $\frac{r}{s}$ is a fraction in its lowest terms. Hence, we have $u = \mu s, z = \mu r, v = \mu\left(\frac{r+ts}{\lambda}\right)$

and varying λ *and* μ we have solutions for $au^2 + cv^2 = z^2$ *and* $au^2 + auv + cv^2 = z^2$ with a or c is a square and of all the solutions we consider solutions which give non-trivial factorization i.e., we look at solutions (u, v, z) of the equations

$y(u,v) = au^2 + cv^2 = z^2$ and

$$y(u,v) = au^2 + auv + cv^2 = z^2$$

that lead to the difference of squares $(x(u,v))^2 \equiv z^2 (\bmod n)$ and the $gcd(x-z,n), \gcd(x+z,n)$ gives a non trivial factor for n.

Now in the next two sections we describe the cases of transforming the binary quadratic form $y(u,v)$ as an ambiguous form by appropriate choices for b_0, b_1, b_2 and we show that there exists solutions (u,v,z) leading to non trivial factorization.

1.1 Transformation of $y(u,v)$ as ambiguous form $(a,0,c)$ where a or c is a square

We obtained the binary quadratic form $y(u,v)$ by substituting the linear double parametrization for b_0, b_1, b_2 as $k_i u + k_j v$ for $i = 1,3,5$ and $j = 2,4,6$. In this section we propose the following choices of $k_{i'}s$ and $k_{j'}s$ to obtain such $(a,0,c)$ form where a or c is a square. We consider the pairs $(k_1,k_2);(k_3,k_4);(k_5,k_6)$ corresponding to b_2, b_1, b_0 respectively and propose the choices for $k_{i'}s$ and $k_{j'}s$ according to the following cases:

Case i:

$(0,k_2);(0,k_4);(k_5,0)$ *with* $k_2 = 1; k_4 = -m; k_5 = a_0 m$

In this case we have $b_2 = v;\ b_1 = -mv;\ b_0 = a_0 mu$, substituting in x and y we have

$$y(u,v) = (a_0^2 m^2)u^2 + (m^4 + a_0 m)v^2$$

$$x(u,v) = a_0 mu$$

Note $y(u,v)$ is an ambiguous form $(a,0,c)$ with $a = a_0^2 m^2$, a square.

Case ii:

$(0,k_2);(k_3,0);(0,k_6)$ *with* $k_2 = m; k_3 = m; k_6 = a_0$

In this case we have $b_2 = mv;\ b_1 = mu;\ b_0 = a_0 v$

$$y(u,v) = (m^4)u^2 + (a_0 m^3 + a_0^2)v^2$$

$$x(u,v) = m^3 v + m^2 u + a_0 v$$

Note $y(u,v)$ is an ambiguous form $(a,0,c)$ with $a = m^4$, a square.

Case iii:

$(0,k_2);(k_3,0);(k_5,0)$ *with* $k_2 = a_0 m; k_3 = m^2; k_5 = a_0$

In this case we have $b_2 = a_0 mv;\ b_1 = m^2 u;\ b_0 = a_0 u$

$$y(u,v) = (m^3 + a_0)^2 u^2 + (-a_0^3 m^3)v^2$$

$$x(u,v) = a_0 m^3 v + m^3 u + a_0 u$$

Note $y(u,v)$ is an ambiguous form $(a,0,c)$ with $a = m^3 + a_0{}^2$, a square.

Case iv:

$(k_1,0);(0,k_4);(k_5,0)$ *with* $k_1 = m; k_4 = a_0 m; k_5 = a_0$

In this case we have $b_2 = mu;\ b_1 = a_0 mv;\ b_0 = a_0 u$

$$y(u,v)=(a_0m^3+a_0^2)u^2+(m^4a_0^2)v^2$$

$$x(u,v)=m^3u+a_0m^2v+a_0u$$

Note $y(u,v)$ is an ambiguous form $(a,0,c)$ with $c=m^4a_0^2$, is a square.

Case v:

$(k_1,0);(k_3,0);(0,k_6)\ with\ k_1=-a_o;k_3=a_0m;k_6=m$

In this case we have $b_2=-a_0u;\ b_1=a_0mu;\ b_0=mv$

$$y(u,v)=(a_0^2m^4+a_0^3m)u^+(m^2)v^2$$

$$x(u,v)=mv$$

Note $y(u,v)$ is an ambiguous form $(a,0,c)$ with $c=m^2$, a square.

Case vi:

$(k_1,0);(0,k_4);(0,k_6)\ with\ k_1=a_0m;k_4=m^2;k_6=a_0$

In this case we have $b_2=a_0mu;\ b_1=m^2v;\ b_0=a_0v$

$$y(u,v)=(-a_0^3m^3)u^2+(m^3+a_0)^2v^2$$

$$x(u,v)=a_0m^3u+m^3v+a_0v$$

Note $y(u,v)$ is an ambiguous form $(a,0,c)$ with $c=(m^3+a_0)^2$, a square.

Note: The binary quadratic form $y(u,v)$ in each of the above cases is transformed into $(a,0,c)$, an ambiguous form with a or c is a square.So considering the equation $au^2+cv^2=z^2$ for corresponding a,c in each of the above cases from solution (u,v,z), we have a difference of squares $(x(u,v))^2\equiv z^2 \bmod n$ leading to a factor of n where $x(b_2,b_1,b_0)=x(u,v)$ for each choice of b_2,b_1,b_0.

1.2 Transformation of $y(u,v)$ as ambiguous form (a,a,c) where a or c is a square

We propose the following choices of $k_{i'}s$ and $k_{j'}s$ to obtain such (a,a,c) form where a or c is a square.

Case (i):

$(0,k_2);(0,k_4);(k_5,0)$ with $k_2=a_0;k_4=-2a_0m;k_5=-2a_0m^2$

In this case we have $b_2=a_0v,b_1=-2a_0mv,b_0=-2a_0m^2u$

$$y(u,v)=(4a_0^2m^4)u^2+4a_0^2m^4uv+(4a_0^2m^4+3a_0^3m)v^2$$

$$x(u,v)=-a_0m^2v-2a_0m^2u$$

Note $y(u,v)$ is an ambiguous form (a,a,c) with $a=4a_0^2m^4$, a square.

Case (ii):

$(0,k_2);(k_3,0);(0,k_6)$ with $k_2=-m^2;k_3=4a_0;k_6=a_0m$

In this case we have $b_2=-m^2v;\ b_1=4a_0u;\ b_0=a_0mv$

$$y(u,v)=(16a_0^2m^2)u^2+16a_0^2m^2uv+(-3a_0m^5+a_0^2m^2)v^2$$

$$x(u,v)=-m^4v+4a_0mu+a_0mv$$

Note $y(u,v)$ is an ambiguous form (a,a,c) with $a=16a_0^2m^2$, a square.

Case(iii):

$(0,k_2);(k_3,0);(k_5,0)$ with $k_2=a_0;k_3=0;k_5=2a_0m^2$

In this case we have $b_2=a_0v,b_1=0,b_0=2a_0m^2u$

$$y(u,v)=4a_0^2m^4u^2+4a_0^2m^4uv-a_0^3mv^2$$

$$x(u,v)=a_0m^2v+2a_0m^2u$$

Note $y(u,v)$ is an ambiguous form (a,a,c) with $a=4a_0^2m^4$, a square.

Case (iv):

$(k_1,0);(0,k_4);(k_5,0)$ with $k_1=2;k_4=m;k_5=0$

In this case we have $b_2=2u, b_1=mv, b_0=0$

$$y(u,v)=-4a_0mu^2-4a_0muv+m^4v^2$$

$$x(u,v)=m^2(2u+v)$$

Note $y(u,v)$ is an ambiguous form (a,a,c) with $c=m^4$,a square.

Case (v):

$(k_1,0);(k_3,0);(0,k_6)$ with $k_1=2m;k_3=0;k_6=-a_0$

In this case we have $b_2=2mu, b_1=0, b_0=-a_0v$

$$y(u,v)=-4a_0m^3u^2-4a_0m^3uv+a_0^2v^2$$

$$x(u,v)=2m^3u-a_0v$$

Note $y(u,v)$ is an ambiguous form (a,a,c) with $c=a_0^2$, a square.

Case (vi):

$(k_1,0);(0,k_4);(0,k_6)$ with $k_1=2m;k_4=2m^2;k_6=a_0$

In this case we have $b_2=2um, b_1=2m^2v, b_0=a_0v$

$$y(u,v)=(-4a_0m^3)u^2+(-4a_0m^3)uv+(4m^6+a_0^2+4a_0m^3)v^2$$

$$x(u,v)=2m^3u+2m^3v+a_0v$$

Note $y(u,v)$ is an ambiguous form (a,a,c) with $c=(2m^3+a_0)^2$ is a square.

Note: The binary quadratic form $y(u,v)$ in each of the above cases is transformed into (a,a,c), an ambiguous form with a or c is a square.So considering the equation $au^2+auv+cv^2=z^2$ for corresponding a,c in each of the above cases from solution (u,v,z), we have a difference of squares $(x(u,v))^2 \equiv z^2 \bmod n$ leading to a factor of n where $x(b_2,b_1,b_0)=x(u,v)$ for each choice of b_2,b_1,b_0.

IV. Table

A list of choices of $k_{i'}s$ and $k_{j'}s$ which transformed $y(u,v)$ into ambiguous forms is shown in the following table :

S.No	Cases	$(a,0,c)$	(a,a,c)
(i)	$(0,k_2);(0,k_4);(k_5,0)$	$k_2=1;k_4=-m;k_5=a_0m$ $y(u,v)=a_0^2m^2u^2+a_0(m^4+a_0m)v^2$ $a=a_0^2m^2$ is a square	$k_2=a_0;k_4=-2a_0m;k_5=-2a_0m^2$ $y(u,v)=(4a_0^2m^4)u^2+4a_0^2m^4uv$ $+(4a_0^2m^4+3a_0^3m)v^2A$ $a=4a_0^2m^4$ is a square
(ii)	$(0,k_2);(k_3,0);(0,k_6)$	$k_2=m;k_3=m;k_6=a_0$ $y(u,v)=m^4u^2+a_0(m^3+a_0)v^2$ $a=m^4$ is a square	$k_2=-m^2;k_3=4a_0;k_6=a_0m$ $y(u,v)=16a_0^2m^2u^2+16a_0^2m^2uv+$ $(-3a_0m^5+a_0^2m^2)v^2$ $a=16a_0^2m^2$ is a square
(iii)	$(0,k_2);(k_3,0);(k_5,0,)$	$k_2=a_0m;k_3=m^2;k_5=a_0$ $y(u,v)=(m^3+a_0)^2u^2+(-a_0^3m^3)v^2$ $a=(m^3+a_0)^2$ is a square	$k_2=a_0;k_3=0;k_5=2a_0m^2$ $y(u,v)=4a_0^2m^4u^2+4a_0^2m^4uv-a_0^3mv^2$ $a=4a_0^2m^4$ is a square

(iv)	$(k_1,0);(0,k_4);(k_5,0)$	$k_1=m;k_4=a_0m;k_5=a_0$ $y(u,v)=(a_0m^3+a_0^2)u^2+m^4a_0^2v^2$ $c=m^4a_0^{\ 2}$ is a square	$k_1=2;k_4=m;k_5=0$ $y(u,v)=-4a_0mu^2-4a_0muv+m^4v^2$ $c=m^4$ is a square
(v)	$(k_1,0);(k_3,0);(0,k_6,)$	$k_1=-a_0;k_3=a_0m;k_6=m$ $y(u,v)=(a_0^2m^4+a_0^3m)u^2+m^2v^2$ $c=m^2$ is a square	$k_1=2m;k_3=0;k_6=-a_0$ $y(u,v)=-4a_0m^3u^2-4a_0m^3uv+a_0^2v^2$ $c=a_0^2$ is a square
(vi)	$(k_1,0);(0,k_4,);(0,k_6)$	$k_1=a_0m;k_4=m^2;k_6=a_0$ $y(u,v)=(-a_0^3m^3)u^2+(m^3+a_0)^2v$ $c=(m^3+a_0)^2$ is a square	$k_1=2m;k_4=2m^2;k_6=a_0$ $y(u,v)=(-4a_0m^3)u^2+(-4a_0m^3)uv$ $+(4m^6+a_0^2+4a_0m^3)v^2$ $c=(2m^3+a_0)^2$ is a square

In the following theorem we show that there exists solution (u,v,z) in each of the above cases leading to non trivial factorization.

Theorem: Let n be a composite number and for $n=m^3+a_0$ where $m=\lfloor n^{\frac{1}{3}}\rfloor$, if $x=b_2m^2+b_1m+b_0$ then in the congruence $x^2\equiv c_2m^2+c_1m+c_0$, the linear parametrizationsfor $b_{i'}s$ as $b_2=k_1u+k_2v$, $b_1=k_3u+k_4v$, $b_0=k_5u+k_6v$ transform $c_2m^2+c_1m+c_0$ as $y(u,v)$, a binary quadratic form in u,v and further $y(u,v)$ can be transformed into ambiguous forms as $(a,0,c)$ or (a,a,c) where a or c is a square for suitable linear parametrizations of $b_{i'}s$ such that in each of these linear parameterizations the equation $au^2+buv+cv^2=z^2$ with a or c is a square and $b=0$ or $b=a$ has a solution (u,v,z) leading to a non-trivial factorization of n via the difference of squares $(x(u,v))^2\equiv z^2(\mathrm{mod}\,n)$.

Proof In section II it is seen that a two variable linear parametrizations for $b_{i'}s$ i.e., $b_2=k_1u+k_2v$, $b_1=k_3u+k_4v$, $b_0=k_5u+k_6v$ for $k_i\varepsilon Z;\forall i=1,2,3,4,5,6$ has tranformed $c_2m^2+c_1m+c_0$ into $y(u,v)$, a binary quadratic form in u,v. In section III it is described how the proposedchoices for $k_{i'}s$ and $k_{j'}s$ further transform into $y(u,v)$ into ambiguous forms as $(a,0,c)$ or (a,a,c) where a or c is a square in the sections 3.1 and 3.2 respectively.Now it remains to prove the existence of solution (u,v,z) to the equation $au^2+buv+cv^2=z^2$ with a or c is a square and $b=0$ or $b=a$ leading to a non trivial factorization of n .

Consider the equation $y(u,v)=au^2+buv+cv^2=z^2 with a=t^2$ By setting

$$\frac{z+tu}{v}=\frac{bu+cv}{z-tu}=\lambda(say),$$

we have a complete set of solutions from the ratio

$$\frac{z}{u}=\frac{\lambda^2t+b\lambda+ct}{\lambda^2-c}$$

now for $b=0$ we have $\frac{z}{u}=\frac{\lambda^2t+ct}{\lambda^2-c}$

or $\frac{z}{tu}=\frac{\lambda^2+c}{\lambda^2-c}=\frac{r}{s}(say),$

where $\frac{r}{s}$ is a fraction in its lowest terms.Now we get a complete set of solutions given as

$$tu = \mu s,\ z = \mu r,\ \ v = \mu\left(\frac{r+s}{\lambda}\right).$$

Now for each of the cases above by varying λ and μ and substituting these values in the difference of squares $(x(u,v))^2 = z^2 (\operatorname{mod} n)$, we seein the following that there are solutions (u,v,z) with $\gcd(x(u,v)-z,n)$ or $\gcd(x(u,v)+z,n)$ greater than 1 and not equal to n,thus leading to non trivial factorization of n.

In case(i) we have

$$y(u,v) = (a_0^2 m^2)u^2 + (m^4 + a_0 m)v^2$$

$x(u,v) = a_0 mu$ with $a = t^2 = a_0^2 m^2$ and $c = mn$.

Nowvarying λ over prmes,in particular for $\lambda = p$, a square free prime factor of n, note

$x \pm z = tu \pm z = \mu s \pm \mu r = \mu(s \pm r) = s \pm r$; $\mu = 1$ with

$\gcd(x - z, n) = \gcd(-2c/p, n) = \gcd(mn/p, n) and \gcd(x + z, n) = \gcd(\lambda^2, n) = \gcd(p^2, n) = p$

,

the solution (u,v,z) leads to a non trivial factorization of $n.$ Therefore note that varying λ over prmes $p \le n$ for μ =1each choice of $\lambda = p$, either leads to a non-trivial factorization or a quadratic residue mod n which helps in sieving the prime choices for $\lambda = p$.

In case(ii), the same argument as above may be repeated since we have

$$y(u,v) = (m^4)u^2 + (a_0 m^3 + a_0^2)v^2$$

$x(u,v) = m^2 u + nv$ with $a = t^2 = m^4$ and $c = a_0 n$

Now varying λ over prmes as above we have ,

$x \pm z = tu + nv \pm z = \mu s \pm \mu r + nv = \mu(s \pm r) + nv = s \pm r + nv$; $\mu = 1$ with

$\gcd(x - z, n) = \gcd(-2c/p + nv, n) = \gcd(a_0 n/p + nv, n) and$

$\gcd(x + z, n) = \gcd(\lambda^2 + nv, n) = \gcd(p^2 + nv, n) = p,$ the solution (u,v,z) leads to a non trivial factorization of nandas $x - z = \mu(s - r) + nv = -2c/p + nv$ for c as above, and for $\lambda = p, \mu = 1,$ the solution (u,v,z) leads to a non-trivial factorization for n.

In case(iii), we have

$$y(u,v) = (m^3 + a_0)^2 u^2 + (-a_0^3 m^3)v^2$$

$x(u,v) = a_0 m^3 v + m^3 u + a_0 u$ with $a = t^2 = n^2$ and $c = -a_0^3 m^3$

In this particular case where $a = n^2$, $y(u,v)$ may be written as

$$y(u,v) = (m^3 + a_0)^2 u^2 + (-a_0^3 m^3)v^2$$

$$= (a_0 nu^2 + a_0^4 v^2) + m^3 nu^2 - a_0^3 nv^2$$

$$= y_1(u,v) + m^3 nu^2 - a_0^3 nv^2$$

The solution (u,v,z) for $y_1(u,v) = z^2$ may be obtained asin case (ii) by interchanging u and v and note this solution leads to non trivial factorization in this case as well for $\lambda = p$ for suitable value $\mu = t$ .For case(iv),case(v) and case(vi) , the same argument as in case(ii), case(i) and case(iii) respectively may be repeated by interchanging u and v.

Now note for the (a,a,c) form in each of the cases above can be considered as $(a,0,c)$ forms again as follows.

In case(i) we have

$$y(u,v) = (4a_0^2 m^4)u^2 + (4a_0^2 m^4)uv + (4a_0^2 m^4 + 3a_0^3 m)v^2$$

$$y(w,v) = (a_0^2 m^4)w^2 + (3a_0^2 mn)v^2 \quad for \quad w = 2u + v$$

$$x(w,v) = -a_0 m^2 w$$

This is same as in case(i) of $(a,0,c)$ form and by the same argument as in case(i) there is a solution (w,v,z)

leading to non-trivial factorization of n.

In case(ii)

$$y(u,v)=(4a_0m)^2u^2+(4a_0m)^2uv+(-3a_0m^5+a_0^2m^2)v^2$$
$$y(w,v)=(2a_0m)^2w^2-(3a_0m^2n)v^2 \quad for w=2u+v$$
$$x(w,v)=2a_0mw-mnv$$

This is same as in case(ii) form of $(a,0,c)$ and by the same argument as in case(ii) there is a solution (w,v,z) leading to non-trivial factorization of n.

In case(iii)

$$y(u,v)=(4a_0^2m^4)u^2+(4a_0^2m^4)uv-(a_0^3m)v^2$$
$$y(w,v)=(a_0m^2)^2w^2-(ma_0^2n)v^2 \quad for w=2u+v$$
$$x(w,v)=(a_0m^2)w$$

This is same as in case(i) form of $(a,0,c)$ and by the same argument as in case(i) there is a solution (w,v,z) leading to non-trivial factorization of n.

In case(iv)

$$y(u,v)=-4a_0mu^2-4a_0muv+m^4v^2$$
$$y(w,v)=m^4w^2+mnv^2-mnw^2 \quad for w=2u+v$$
$$x(w,v)=m^2w$$

Now taking $y_1(w,v)=m^4w^2+mnv^2$, we have

$$(x(w,v))^2\equiv y_1(w,v)-mnw^2 (\mathrm{mod}\, n)$$

≡≡≡

The solution (w,v,z) for $y_1(w,v)=z^2$ may be obtained as in case(ii) and note this solution leads to non-trivial factorization for a suitable value of μ.

In case(v) we have

$$y(u,v)=-4a_0m^3u^2-4a_0m^3uv+a_0^2v^2$$
$$y(w,v)=a_0^2w^2+a_0nv^2-a_0nw^2 \text{ for } w=2u+v$$
$$x(w,v)=m^3w-nv$$

Now taking $y_1(w,v)=a_0^2w^2+a_0nv^2$, we have

$$(x(w,v))^2\equiv y_1(w,v)-a_0nw^2 (\mathrm{mod}\, n)$$

The solution (w,v,z) for $y_1(w,v)=z^2$ may be obtained as in case(i) and note this solution leads to non-trivial factorization for a suitable value of μ.

In case(vi) we have

$$y(u,v)=(-4a_0m^3)u^2+(-4a_0m^3)uv+(2m^3+a_0)^2v^2$$
$$y(w,v)=-a_0m^3w^2+n^2v^2+3m^3nv^2 \text{ for } w=2u+v$$
$$x(w,v)=m^3w+nv$$

Now taking $y_1(w,v)=-a_0m^3w^2+n^2v^2$, we have

$$(x(w,v))^2\equiv y_1(w,v)+3m^3nv^2 (\mathrm{mod}\, n)$$

The solution (w,v,z) for $y_1(w,v)=z^2$ may be obtained as in case(iii) and note this solution leads to non-trivial factorization for a suitable value of μ.

Example 1: In this example we give the factorization for $n = 3961$ by transforming into an ambiguous form $(a,0,c)$:We have for $n = 3961, m = 15, a_0 = 586$ then considering case(ii) for $(a,0,c)$ form we take $k_1 = k_4 = k_5 = 0; k_6 = 586; k_2 = 15 = k_3$ then

$$y(u,v) = m^4u^2 + a_0nv^2$$

$$= 50625u^2 + 2321146v^2 = au^2 + cv^2$$

note

$$a = 50625 \text{ is a square } i.e., a = t^2 \text{ for } t = 225$$

Now we have a solution (u,v,z) for the equation $y(u,v) = 50625u^2 + 2321146v^2 = z^2$ by using the formulas described above for $\lambda = 17, \mu = 1$, we have

$$\frac{z}{tu} = \frac{\lambda^2 + c}{\lambda^2 - c}$$

$$= \frac{136555}{-136521} = \frac{r}{s}$$

Hence

$$tu = \mu s \Rightarrow tu = -136521,$$

$$z = \mu r = 136555,$$

$$v = \frac{\mu(r+s)}{\lambda} = 2$$

Then, $y(u,v) = 136555^2$ and $x(u,v) = m^2u + nv = -128599$

Therefore $x^2 \equiv y(\bmod n)$

$$\Rightarrow x^2 \equiv z^2(\bmod n)$$

$$\Rightarrow (-128599)^2 \equiv 136555^2(\bmod 3961)$$

And $gcd(x - z, n) = gcd(-265154, 3961) = 233$

Therefore $3961 = 233 \cdot 17$.

Example 2: In this example we give the factorization for $n = 3961$ by transforming into an ambiguous form (a,a,c) :

We have for $n = 3961, m = 15, a_0 = 586$

then considering case(i) for (a,a,c) form we take

$$k_1 = k_3 = k_6 = 0; k_2 = a_0; k_4 = -2a_0m; k_5 = -2a_0m^2$$

$$y(u,v) = 4a_0^2m^4u^2 + 4a_0^2m^4uv + (4a_0^2m^4 + 3a_0^3m)v^2$$

This can be transformed into $(a,0,c)$ form in w, v as

$$y(w,v) = a_0^2m^4w^2 + 3a_0^2mnv^2 = aw^2 + cv^2$$

note

$$a = 1738442250 \quad 0$$

is a square i.e., $a = t^2 \; for t = 131850$

Now we have a solution (w, v, z) for the equation $y(w,v) = 17384422500w^2 + 61208620020v^2 = z^2$ by using the formulas described above.

for $\lambda = 17, \mu = 1$, we have

$$\frac{z}{tw} = \frac{\lambda^2 + +c}{\lambda^2 - c}$$

$$= \frac{3600507077}{-3600507043} = \frac{r}{s}$$

Hence

$$tw = \mu s \Rightarrow tw = -3600507043,$$

$$z = \mu r = 3600507077,$$

$$v = \frac{\mu(r+s)}{\lambda} = 2$$

Then,

$$y(w,v) = 3600507077^2 and x(w,v) = -a_0 m^2 w = -tw = 3600507043$$

Therefore $x^2 \equiv y (\bmod n)$

$$\Rightarrow x^2 \equiv z^2 (\bmod n)$$

$$\Rightarrow 3600507043^2 \equiv 3600507077^2 (\bmod 3961)$$

And $gcd(x+z, n) = gcd(7201014120, 3961) = 233$

Therefore $3961 = 17 \cdot 233$

Example 3: In this example we give the factorization for $n = 3961$ by transforming into an ambiguous form $(a,0,c)$ for a=n^2:

We have for

$$n = 3961, m = 15, a_0 = 586$$

Then considering case(iii) for $(a,0,c)$ form we take

$$(0, k_2); (k_3, 0); (k_5, 0) \; with \; k_2 = a_0 m; k_3 = m^2; k_5 = a_0$$

$$y(u,v) = (m^3 + a_0)^2 u^2 + (-a_0^3 m^3) v^2$$

$$= (a_0 n u^2 + a_0^4 v^2) + m^3 n u^2 - a_0^3 n v^2$$

$$= y_1(u,v) + m^3 n u^2 - a_0^3 n v^2$$

Then considering case(iv) for $(a,0,c)$ form we have a solution (u, v, z) for the equation $y_1(u,v) = a_0 n u^2 + a_0^4 v^2 = 12306u^2 + 117920812800v^2 = z^2$ by using the formulas described above

for a=12306 , c=117920812800 , t= $a_0^{\;2} = 343396$ and

for $\lambda = 17, \mu = t = 343396$, we have

$$\frac{z}{tv} = \frac{\lambda^2 + c}{\lambda^2 - c}$$

$$= \frac{12595}{-12017} = \frac{r}{s}$$

Hence

$$tv = \mu s \Rightarrow tv = -4126589732,$$

$$z = \mu r = 4325072620,$$

$$v = \frac{\mu(r+s)}{\lambda} = 11675464$$

Then,

$$y(u,v) = 4325072620^2 \, and x(u,v) = nu + a_0 m^3 v = 22479891150$$

Therefore $x^2 \equiv y(\bmod n)$

$$\Rightarrow x^2 \equiv y_1 + m^3 nu^2 - a_0^3 nv^2 (\bmod n)$$

$$\Rightarrow x^2 \equiv z^2 (\bmod n)$$

$$\Rightarrow (22479891150)^2 \equiv 4325072620^2 (\bmod 3961)$$

Thersefore

$$gcd(x - z, n) = gcd(18154818530, 3961) = 17, and$$

$$gcd(x + z, n) = gcd(26804963770, 3961) = 233$$

Therefore $3961 = 233 \cdot 17$

V. Conclusion

The factorization via difference of squares proposed in this paper using binary quadratic forms is obtained by certain linear parametrization of two variables . We proposed 6 cases of linear parametrization for $(a,0,c)$ form and 6 cases of linear parametrization for (a,a,c) form. We proved a theorem that in each of these cases there are solutions of the equations $au^2 + cv^2 = z^2$ and $au^2 + auv + cv^2 = z^2$ leading to non-trivial factorization for n. It is seen that the solutions obtained either leads to a non trivial factorization or a quadratic residue mod n which helps in sieving the prime choices for $\lambda = p$ .The solutions depend on varying λ over primes and a solution leading to nontrivial factorization may be obtained in at least p steps for p being square free prime factor of n. In particular for $n = pq$ with $p < q$, the nontrivial factorization of n can be obtained in steps less than $\sqrt{n}$.

References

Journal Papers:

[1]. M. Zhang, *Factorization of the Numbers of the form* $m^3 + c_2 m^2 + c_1 m + c_0$, 1998, Springer-Verlag, London, UK, ISBN 3-540-64657-4.
[2]. Seth Viren Neel, *Binary Quadratic Form and The Ideal Class Group*.
[3]. D.H. Lehmer and E. Lehmer, *A New Factorization Technique Using Quadratic Forms*.
[4]. Benzamin Bakker, *Lecture Notes: Quadratic Forms*.
[5]. Eric Landqusit, *An implementation of Zhang's Special Quadratic Sieve and Possible Extension*, Math 488: Integer Factorization, Dec 20, 2002.
[6]. Eric Landqusit, *Possible ways to extend Zhang's Special Quadratic Sieve*, June 4, 2003.

Books:

[7]. Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, 1985, Birkh $\ddot{a}$ user Inc, ISBN 0-8176-3291-3.
[8]. Tom M. Apostol, *Introduction to Analytic Number Theory* Springer-Verlag, New York Inc, 1989, ISBN 978-81-85015-12-5.
[9]. Ivan Niven, Herbert S.Zuckerman, Hugh L.Montgomery, *An Introduction to The Theory of Numbers*, Fifth Edition, John Wiley and Sons, Inc., 2008, ISBN:978-81-265-1811-1.
[10]. Alan Baker, *A Coprehensive Course in Number Theory*, cambridge university press,2012,ISBN 978-1-107-01901-0.
[11]. Richard Crandall, Carl Pomerance,*Prime Numbers: A Computational Perspective*, Springer Science + Business MediaInc., 2005,ISBN-10: 0-387-25282-7.
[12]. Leonard Eugene Dickson, *History of the Theory of Numbers*, Volume II, Chelsea Publishing Company, 1919, ISBN 0-8284-0086-5.
[13]. Neil Koblitz, *A course in Number Theory and Cryptography*, second edition, 1994, Springer-Verlag, New York Inc, ISBN 0-387-94293-9.