International Research Journal of Mathematics, Engineering and IT
Vol. 3, Issue 12, December 2016 Impact Factor- 5.489
ISSN: (2349-0322)

Website: www.aarf.asia Email : editor@aarf.asia , editoraarf@gmail.com

FACTORIZATION USING SQUARE ROOT OF A SQUARE BINARY QUADRATIC FORM

[1]P Anuradha Kameswari [2]K Vijaya Prasamsa
Department of Mathematics, Andhra University,
Visakhapatnam- 530003, Andhra Pradesh, India.

ABSTRACT

The paper presents a method for factoring a composite integer N based on the composition of binary quadratic forms which depends on the search for ambiguous forms that leads to a non trivial factorization of N. In this method we propose to obtain a square binary quadratic form from a positive definite binary quadratic form and construct an ambiguous form via the square root of a square binary quadratic form.

KEYWORDS: Binary quadratic forms, Square binary quadratic forms, Discriminant, Factorization, Ambiguous forms.

1 Introduction

The theory of binary quadratic forms initiated right from ancient Greeks, developed by Brahma Gupta during seventh century, later by Lagrange, Gauss, Euler, Fermat during seventeenth century, plays a vital role in Computational Number Theory and Cryptography[1]. There are various factorization methods based on binary quadratic forms, Fermat factoring method based on binary quadratic forms representing a composite number N in two different ways by the binary quadratic form $(1,0,1)$ or x^2+y^2 and Mckee method speeds a Fermat algorithm. There are also factorizing methods based on composition of binary quadratic forms like Shank's class group method by Shank's during 1971 with complexity $O(N^{\frac{1}{5}+\varepsilon})$ and Shank's SQUFOF method of complexity $O(N^{\frac{1}{4}+\varepsilon})$ [2] and Schoof's factoring algorithms by Schoof during 1982 with complexity $O(N^{\frac{1}{5}})$. In addition to these, all seive factoring algorithms are based on solutions of the congruence of binary quadratic forms $x^2-y^2\equiv 0(\mathrm{mod}N)$[3]. In [4], we gave a factoring method, factorization via difference of squares using ambiguous forms. In this paper we describe a method based on composition of binary quadratic forms with discriminant $d<0$. This method depends on the search for the ambiguous forms and we consider the positive definite square binary quadratic forms of the form $ax^2+bxy+cy^2$ with a or c square and arrive at the required ambiguous form that leads a non trivial factorization of N. We first give a brief description on basics of binary quadratic forms, composition on binary quadratic forms, ambiguous forms and Shank's class group factorization method.

1.1 Binary Quadratic Forms

A binary quadratic form $f(x,y)$ is a homogeneous polynomial $f(x,y) = ax^2 + bxy + cy^2$ of degree 2 denoted by (a,b,c) where the coefficients a,b and c are fixed integers and the variables x and y are restricted to integers and by square binary quadratic form, we mean a binary quadratic form (a,b,c) where a is a square. A binary quadratic form (a,b,c) is said to be primitive if $\gcd(a,b,c) = 1$ [5].

Definition 1 .1.1 The discriminant of a binary quadratic form $f = (a,b,c)$ denoted as 'd' is defined to be the value $d = b^2 - 4ac$.

Definition 1 .1.2 For $d < 0$, a binary quadratic form $f(x,y)$ is said to be positive definite if $a > 0$ and is negative definite if $a < 0$.

Definition 1 .1.3 For any $n\varepsilon\mathbb{Z}$, n is set to be represented by the binary quadratic form $f(x,y)$, if $n = f(x_0,y_0)$ for some $x_0, y_0\varepsilon\mathbb{Z}$ and if $\gcd(x_0,y_0) = 1$, it is called proper representation.

Definition 1 .1.4 Two binary quadratic forms f and g are equivalent [6] if there exists an integer matrix $M = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ of determinant equal to 1 such that

$$g(x,y) = f(\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix})$$
$$= f(px + qy, rx + sy)$$

Theorem 1.1.5 Equivalence preserves the discriminant $d = b^2 - 4ac$.

Remark 1.1.6 The equivalent relation of quadratic forms on the set of all binary quadratic forms of discriminant d is an equivalence relation and the equivalence classes can be classified by the binary quadratic forms called reduced forms.

For further study we consider only positive definite binary quadratic forms.

Definition 1.1.7 A positive definite quadratic form (a,b,c) is reduced if $|b| \le a \le c$ and in addition, if either $|b| = a$ or $a = c$, then $b \ge 0$ [7].

The following theorem classify the equivalence classes by reduced forms.

Theorem 1.1.8 Every class of primitive positive definite quadratic forms contains a unique reduced form.

1.2 Composition on Binary quadratic forms [8]

Let $\mathcal{C}(d)$ denote the set of equivalence classes of primitive binary quadratic forms of discriminant $d < 0$. We shall use the notation $< a,b,c >$ for the equivalence class containing the form (a,b,c). On the set $\mathcal{C}(d)$ given as $\mathcal{C}(d) = \{< a,b,c > / gcd(a,b,c) = 1 with b^2 - 4ac = d\}$ there is a binary operation '$*$' defined as follows:

for any, $< a_1,b_1,c_1 >, < a_2,b_2,c_2 > \in C(d)$

$$< a_1,b_1,c_1 > * < a_2,b_2,c_2 > = < a_3,b_3,c_3 >$$

where (a_3, b_3, c_3) is a binary quadratic form, obtained from the given quadratic forms (a_1, b_1, c_1) , (a_2, b_2, c_2) as

$$a_3 = \frac{a_1 a_2}{e^2},$$
$$b_3 = x, \text{the unique solution of } x^2 \equiv d(\text{mod}\frac{4a_1 a_2}{e^2}),$$
$$x \equiv b_1(\text{mod}\frac{2a_1}{e}),$$
$$x \equiv b_2(\text{mod}\frac{2a_2}{e})$$
$$c_3 = e^2(\frac{b_3^2 - d}{4a_1 a_2})$$

for $e = \gcd(a_1, a_2, \frac{b_1+b_2}{2})$. In particular, this form (a_3, b_3, c_3) is also represented as $(a_1, b_1, c_1) * (a_2, b_2, c_2)$. With respect to this composition of gauss on $\mathcal{C}(d)$, $\mathcal{C}(d)$ forms an abelian group with $< 1,0, \frac{-d}{4} >$ or $< 1,1, \frac{1-d}{4} >$ as identity accordingly as d even or odd respectively, and for any $< a, b, c >$ in $\mathcal{C}(d)$, $< c, b, a >$ is the inverse.

Definition 1.2.1 The order of the group $\mathcal{C}(d)$ is the number of primitive reduced forms called the class number and is denoted as $h(d)$ [8].

Definition 1.2.2 The set of all classes in $\mathcal{C}(d)$ of order 2 are called the ambiguous classes [9].

Remark 1.2.3 The primitive reduced forms of the ambiguous classes called ambiguous forms are of three types namely $(a, 0, c), (a, a, c)$ and (a, b, a) [10] and are classified by the following lemma.

Lemma 1.2.4 Suppose d is a negative discriminant. If d is even, then the ambiguous forms of discriminant d include the forms $(u, 0, v)$, where $0 < u \leq v$, $\gcd(u, v) = 1$, and $uv = -d/4$. In addition,if $uv = -d/4$, with $\gcd(u, v) = 1$ or 2 and $\frac{1}{2}(u + v)$ odd, we have the forms $\frac{1}{2}(u + v), v - u, \frac{1}{2}(u + v)$ when $\frac{1}{3}v \leq u < v$ and the forms $(2u, 2u, \frac{1}{2}(u + v))$ when $0 < u < \frac{1}{3}v$. If d is odd, then the ambiguous forms of discriminant d are the forms $(\frac{1}{4}(u + v), \frac{1}{2}(v - u), \frac{1}{4}(u + v))$, where $-d = uv$ with $0 < \frac{1}{3}v \leq u \leq v$, $\gcd(u, v) = 1$ and the forms $(u, u, \frac{1}{4}(u + v))$, where $-d = uv$, $0 < u \leq \frac{1}{3}(v)$, $\gcd(u, v) = 1$.

Shank's Class Group method of factorization : In this method, the above lemma on ambiguous form is used in implementing factorization method with ambiguous forms. In this method it is noted that each ambiguous form gives a factorization of N, the search for non trivial factorizations is really a search for ambiguous form. Given a negative discriminant d, by using $h(d)$, the class number which is the order of the group $\mathcal{C}(d)$, we have for $h(d) = h = 2^l h_0$, where h_0 is odd, then for $f =< a, b, c > \in C(d)$ and for $F = f^{h_o}$, either $F = I_d$ or one of $F, F^2, F^4, \ldots F^2$ has order 2 in the group and the reduced member of this form of order 2, is an ambiguous form. Hence in this method an ambiguous form is constructed by the knowledge of just h and f.

2 Factorization using square root of a square binary quadratic form

In this section we propose a method to compute ambiguous forms without using the class number $h(d)$ but by finding square root of square binary quadratic forms. In this context we first describe the method of finding a square root of a binary quadratic form.

2.1 Square root of a binary quadratic form

By the definition of composition on $\mathcal{C}(d)$ any class containing a binary quadratic form g is a square root of class containing $g * g$, and as any quadratic form $f \sim g * g$ is also in the same class we consider g as a square root of all such forms f that are equivalent to g^2.In the following theorem we look at possibilities for a square root for a given binary quadratic form.

Theorem 2.1.1 If a primitive binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ represents z^2 with $(x,y) = 1$, then there exists a binary quadratic form g such that $g^2 = (z^2, b', c')$ for some $b', c' \in \mathbb{Z}$ and $f \sim g^2$. In particular, g is a square root of f .

Proof. Let $f(x,y) = ax^2 + bxy + cy^2$ be a square binary quadratic form and let (u,v,z) be a solution of the quadratic equation $f(x,y) = z^2$ with $\gcd(u,v) = 1$. Then there exists integers r,s such that $det\begin{pmatrix} u & r \\ v & s \end{pmatrix} = 1$.

Now for $M = \begin{pmatrix} u & r \\ v & s \end{pmatrix}$, we have $f(M(u,v)) = a'u^2 + b'uv + c'v^2$, where

$$a' = f(u,v) = z^2$$
$$b' = 2aur + b(us + vr) + 2cvs$$
$$c' = f(r,s) = ar^2 + brs + cs^2$$

and by definition of equivalence as $f(x,y) \sim f(M(x,y))$ we have $(a,b,c) \sim (a',b',c') = (z^2, b', c')$. Hence f is equivalent to the square form (z^2, b', c'). We have the class containing f given as $< a,b,c >$ is in $\mathcal{C}(d)$, therefore the class $< a',b',c' >$ is also in $\mathcal{C}(d)$ with

$$< a,b,c > = < a',b',c' > = < z^2,b',c' >$$
$$= < z,b',zc' > * < z,b',zc' > \text{ in } \mathcal{C}(d) \text{ by definition of composition } *.$$

$therefore$, for $(z,b',zc') = g$ as $(z^2,b',c') = g * g = g^2$, we have g is a square root of (z^2,b',c') and the class containing g is a square root of class containing (z^2,b',c') in particular square root of class containing f.

Therefore,we have g is a square root of f .

It is noted that if $f = (a^2,b,c)$, then f is a square form and f has a square root given as (a,b,ac). Now in the following theorem we prove that if f is of the form $f = (a,b,c^2)$ then again f has a square root.

Theorem 2.1.2 If f is a binary quadratic form with a or c square and discriminant $d < 0$, then there is a square form with discriminant d that is equivalent to f.

Proof. Let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form with a or c is a square. Suppose a is a square and if $a = z^2$, for some integer z, then we have $f = (a,b,c) = (z^2,b,c)$ a square form.

Suppose c is a square and if $c = t^2$, for some integer t, a complete set of solutions to the binary quadratic equation $f(x,y) = z^2$ with c as a square can be obtained[12] as follows

Since $c = t^2$ we have

$$ax^2 + bxy + t^2y^2 = z^2$$
$$\Rightarrow x(ax + by) = z^2 - t^2y^2$$
now by setting $\frac{z+ty}{x} = \frac{ax+by}{z-ty} = \lambda(say)$,
we have $z(c - \lambda^2) - a = -y(t\lambda^2 + b\lambda + at)$
then, $z = ly$
$for\ l = \frac{t\lambda^2+b\lambda+at}{\lambda^2-a} = \frac{r}{s}$

where $\frac{r}{s}$ is a fraction in its lowest terms. Then, we have

$$x = \mu\left(\frac{r+ts}{\lambda}\right)$$
$$y = \mu s$$
$$z = \mu r$$

and varying λ and μ a complete set of solutions to the binary quadratic equation $f(x, y) = z^2$ with c as a square is obtained.

Then from the set of solutions,we have for a solution (x, y, z) with $\gcd(x, y) = 1$, as f properly represents z^2 by above theorem(3) we have $f = (a, b, c) \sim (z^2, b', c')$, a square form equivalent and (z, b', zc') is a square root of f.

For example note for $f = (6,3,4)$ a binary quadratic form with $c = 4 = 2^2 = t^2$, we have the solution of the binary equation $f(x, y) = z^2$, given as $x = 7, y = -5, z = 17$, $for\ \lambda = 1\ and\ \mu = 1$ in the formulas above and $f(7, -5) = 289 = 17^2 = z^2$. Then for $g^2 = (z^2, b', c') = (289, 245, 52) \sim f$ implies $g = (z, b', zc') = (17, 245, 884)$ is a square root of f.

2.2 Implementing Factorization with square root of a square binary quadratic form

In this method we propose to obtain a square binary quadratic form from a positive definite binary quadratic form and construct an ambiguous form via the square root of a square binary quadratic form to implement the factorization of a composite number $N = pq$ for p, q primes.

Theorem 2.2.1 If f is a square binary quadratic form with discriminant $d < 0$ then there is an ambiguous form $g^{o(f)}$ where $(o(f)$ is the order of the class containing f, in $\mathcal{C}(d)$, leading to factorization of a composite number $N = pq$ for some binary quadratic form g.

Proof. Let (a, b, c) be a binary quadratic form with discriminant d for some integers a, b, c.By the above theorem if the form (a, b, c) is such that a or c is a square, then we have a square binary quadratic form f. Now first note in any case we can obtain a square form $f \in \mathcal{C}$ for some class $\mathcal{C}$ in $\mathcal{C}(d)$ for if (a, b, c) for some integers a, b, c is such that

Case(1): (a, b, c) is not primitive i.e., $\gcd(a, b, c) = t > 1$, then the form $g = (t^2, b, \left(\frac{a}{t}\right)\left(\frac{c}{t}\right))$ is of discriminant $b^2 - 4 \cdot t^2 \cdot \frac{ac}{t^2} = b^2 - 4ac = d$ and g is a square form of discriminant d.

Case(2): If (a, b, c) is primitive, then $\gcd(a, b, c) = 1$ and we have two sub cases

$(i)\gcd(a, c) \neq 1$
$(ii)\gcd(a, c) = 1$

case(i): If $\gcd(a, c) \neq 1$ then for $\gcd(a, c) = t > 1$, we have $g = (t^2, b, \left(\frac{a}{t}\right)\left(\frac{c}{t}\right))$ is a square

form of discriminant d.
case(ii): If $\gcd(a,c)=1$, then for $\gcd(a,b)=1$ we have $f*f=(a,b,c)*(a,b,c)=(a^2,b,\frac{b^2-d}{4a^2})$ is a square form of discriminant d and for $\gcd(a,b)\neq 1$ if $\gcd(a,b)=t>1$, we take g = $(a^{'},b,ct)$ with $a'=\frac{a}{t}$ then we have $f*f=(a',b,ct)*(a',b,ct)=(a'^2,b,\frac{b^2-d}{4a'^2})$ is a square form of discriminant d.

Now for implementation of factorization with ambigous form take $f=(a^2,b,c)$, a primitive square binary quadratic form such that $<f>\notin c_0$ in $\mathcal{C}(d)$. Then for $f=(a^2,b,c)=(a,b,ac)*(a,b,ac)=g*g$, we have $g=(a,b,ac)$ is a square root of f. Now if order of the class containing the form f is denoted as $o(f)$, then $(g^{o(f)})^2=g^{2o(f)}=(\sqrt{f})^{2o(f)}=f^{o(f)}=I_d$. Therefore the reduced form of $g^{o(f)}$ is an ambiguous form. Now using this ambiguous form, we implement factorization on a composite number given as $N=pq$ for p,q distinct odd prime factors accordingly as $N\equiv 3(\mathrm{mod}4)$ or $N\equiv 1(\mathrm{mod}4)$.

In the case when $N\equiv 3(\mathrm{mod}4)$, we have $d=-N$ and the reduced form of $g^{o(f)}$ is of the form $(\frac{1}{4}(u+v),\frac{1}{2}(v-u),\frac{1}{4}(u+v))$, $0<\frac{1}{3}v\leq u\leq v$ or $(u,u,\frac{1}{4}(u+v))$, $0<u\leq\frac{1}{3}(v)$ with $d=-uv$ and $\gcd(u,v)=1$ i.e., $uv=-d=N$ thus factoring N as uv.

In the case when $N\equiv 1(\mathrm{mod}4)$, for any $f\neq(2,2,\frac{1+N}{2})$, we have $d=-4N$ and the reduced form of $g^{o(f)}$ is of the form $(\frac{1}{2}(u+v),(v-u),\frac{1}{2}(u+v))$, $0<\frac{1}{3}v\leq u\leq v$ or $(2u,2u,\frac{1}{2}(u+v))$, $0<u\leq\frac{1}{3}(v)$, with $\frac{-d}{4}=-uv$ and $\gcd(u,v)=1$ i.e., $uv=\frac{-d}{4}=N$ thus factoring N as uv in this case as well.[11]

Note if $g^{o(f)}$ is an ambiguous form equivalent to identity or (2,2, (N+1)/2) (in the case when $N\equiv 1(\mathrm{mod}4)$), the ambiguous form leads to trivial factorization. So if such ambiguous is not obtained then we go for another choice of square form f.

Example 2.2.2 : To find factors of N = 41347:

For N = 41347 since $N\equiv 3(\mathrm{mod}4)$, we have for $d=-N=-413477$. The group $\mathcal{C}(d)$ is with the identity class as $<1,1,10337>$. Take $f=(49,3,211)$ a square binary quadratic form with $a=7^2=z^2$, then by above theorem 2.1.2 we have $f=(49,3,211)=(7,3,1477)*(7,3,1477)$ with $g=(7,3,1477)$ the square root of f. By above theorem 2.2.1, as $g^{o(f)}$ is an ambiguous form we proceed to compute g^m, using the composition and reduction process as given in the below algorithm for m = 1,2.... . We have

$g^2=f=$ (49,3,211), $g^3=g^2*g=<49,3,211>*<7,3,1477>=<343,199,59>$.

The reduced form of g^3 is (59,37, 181). So on repeating the process, at 12^{th} iteration, we have $g^{13}=<581,-445,103>$ with its reduced form equal to (103,33,103), an ambiguous form of the type (a,b,a). Now by implementing the lemma we have the factorization of given N by cosidering (103,33,103) as the form $(\frac{1}{4}(u+v),\frac{1}{2}(v-u),\frac{1}{4}(u+v)$, for $-d=uv$ then

we have $u = 173$ and $v = 239$, with N = $-d = uv = 173 \cdot 239$.

2.3 Algorithm to find the ambiguous form

Step1: Start
Step2: Input the values of $a,\ b,\ c$ such that $a = t^2$ where t is a positive integer.
Step3: Calculate discriminant $d = b^2 - 4ac$
Step4:
If $d \equiv 0(mod4)$, then compute $I_d = (1,0,\frac{-d}{4})$
Else
{
If $d \equiv 1(mod)4$, then compute $I_d = (1,1,\frac{(1-d)}{4})$
}
Step5: Find the reduced form of (a,b,c) as below and verify whether the result $\neq I_d$ otherwise go to step 1.
Step6: Let the input of reduction process be (a_r,b_r,c_r) =(t,b,tc)
Step7: [Reduction process]
while$(a_r > c_r$ or $abs(b_r) > a_r$ or $(a_r == c_r$ and $b_r < 0)$ or $(b_r == -a_r$ and $a_r < c_r))$
If$(a_r > c_r$ or $(a_r == c_r$ and $b_r < 0))$ then $(a_r,b_r,c_r) = (c_r,-b_r,a_r)$
If$(abs(b_r) > a_r$ or $(b_r == -a_r$ and $a_r < c_r))$ then
Compute $m = \frac{b_r}{2a_r}$ and b'_r as below

$L1: b'_r = b_r - 2a_r m,$ (1)
$If abs(b'_r) <= a_r)$ then $b_r = b'_r$ (2)
Else Repeat the steps from L1 by incrementing m by 1 (3)
Compute $c_r = \frac{b_r^2 - d}{4a_r}$ (4)

Return (a_r,b_r,c_r)
Step8: with the obtained reduced form (a_r,b_r,c_r) find the composition as below.
Step9:[Composition process]
Let (a_1,b_1,c_1) and (a_2,b_2,c_2) be two primitive quadratic forms such that

$$d = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$$

For the first iteration $a_1 = a_2 = t, b_1 = b_2 = b, c_1 = c_2 = tc$
For the next iterations $a_1 = a_r, b_1 = b_r, c_1 = c_r$ where a_r,b_r,c_r output of reduced form obtained from step 10 a_2,b_2,c_2 is same as first iteration.
We compute a_3,b_3,c_3 such that
$< a_1,b_1,c_1 > * < a_2,b_2,c_2 > = < a_3,b_3,c_3 >$ as follows
Evaluate

$$e = \gcd(a_1,a_2,(b_1+b_2)/2)$$
$$a_3 = \frac{(a_1a_2)}{e^2}$$

b_3 is an integer solution that satisfies

$$b_3^2 \equiv d(mod(\frac{4a_1a_2}{e^2}))$$

$$b_3 \equiv b_1 (mod 2a_1/e)$$

$$b_3 \equiv b_2 (mod 2a_2/e)$$

$$c_3 = \frac{(b_3^2 - d)}{4a_3}$$

Step10: Go to step 7 and let the input of reduction process be $a_r = a_3, b_r = b_3, c_r = c_3$.
Step11: Repeat step 9 by inputting the reduced form (a_r, b_r, c_r) obtained from step 7 until $b_r == 0$ or $a_r == b_r$ or $a_r == c_r$ which results to an ambiguous form.
Step12: Stop

3. Conclusion:

In Shank's Class Group Factorization Method, the factorization method is based on composition of binary quadratic forms and computation of class number $h(d)$. In the method proposed by us, the factorization is based on finding the square root of square binary quadratic form and depends on the order of the class containing the square form. The complexity is based on composition and reduction algorithms of binary quadratic forms. For any form (a, b, c) the reduction depends on $a \leq \sqrt{d}/3$ and hence the complexity is $O(\sqrt{d})$. The advantage of the proposed method is that it does not depend on the computation of the class number $h(d)$.

References

Journal Papers

[2] D.J.Guan, *Introduction to the Shank's SQUFOF Integer Factoring Algorithm*, May 26, 2010.

[1] Dr P.Anuradha Kameswari, *Factorization via difference of squares using ambiguous forms*, IOSR-JM, 2016

[2] Benzamin Bakker, *Lecture Notes: Quadratic Forms*.

Chapters In Books

[3] Larry J.Gerstein, *Basic Quadratic Forms, Graduate studies in Mathematics, vol 90, American Mathematical Society Providence*, Rhode Island, ISBN:978-0-8218-4465-6.

[4] Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, 1985, Birkhäuser Inc, ISBN 0-8176-3291-3.

[5]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.

[6]Alan Baker, *A Coprehensive Course in Number Theory*, cambridge university press,2012,ISBN 978-1-107-01901-0.

[7]Franz Lemmermeyer, *Binary Quadratic Forms, An Elementary Approach to the Arithmetic of Elliptic and Hyper Elliptic Curves*,Nov 8, 2010.

[8] Rick L.Shepherd, *Binary Quadratic Forms and Genus Theory*, 2013 , The University of North Caarolina at Greesboro.

[9]Richard Crandall, *Carl Pomerance,Prime Numbers: A Computational Perspective, Springer Science + Business MediaInc.*, 2005,ISBN-10: 0-387-25282-7.

[10]D.Shank, *Class Number, A Theory of Factorization and Genera*, Proc. Symposium of Pure Mathematics, vol.20, American Mathematical Society, 1969.

[11] Leonard Eugene Dickson, *History of the Theory of Numbers, Volume II, Chelsea Publishing Company*, 1919, ISBN 0-8284-0086-5.