Journal of Engineering Technology and Applied Sciences, 2018 *e-ISSN:* 2548-0391
Received 10 September 2018, Accepted 24 October 2018 *Vol. 3, No. 3, 165-171*
Published online 26 October 2018 *doi: 10.30931/jetas.473727*

Citation: Nari, K., Özdemir, E., Yaraneri, E., "İkili Kuadratik Formlar ile Çarpanlara Ayırma". Journal of Engineering Technology and Applied Sciences 3 (3) 2018 : 165-171.

İKİLİ KUADRATİK FORMLAR İLE ÇARPANLARA AYIRMA

Kübra Nari[a], Enver Özdemir[a*], Ergün Yaraneri[b]

[a]Bilgi Güvenliği Mühendisliği ve Kriptografi Bölümü, Bilişim Enstitüsü,
İstanbul Teknik Üniversitesi, İstanbul, Türkiye
*nari15@itu.edu.tr, ozdemiren@itu.edu.tr (*Sorumlu Yazar)*

[b]Matematik Bölümü, Fen-Edebiyat Fakültesi,
İstanbul Teknik Üniversitesi, İstanbul, Türkiye
yaraneri@itu.edu.tr

Özet

Bu makalede diskriminantı pozitif olan ikili kuadratik formlar incelenmiştir. Özellikle diskriminantı iki asal sayının çarpımı olan sınıf grubunun etkisiz elemanına ait çevrimin ilginç özellikler taşıdığı gözlemlenmiştir. Bu özelliklerden yararlanarak bir çarpanlara ayırma algoritması tasarlanmış ve özellikle RSA açık anahtarlı şifreleme sisteminin anahtarlarını kırmada etkili olabileceği gösterilmiştir.

Anahtar Kelimler: İkili kuadratik formlar, çarpanlara ayırma

FACTORIZATION WITH BINARY QUADRATIC FORMS

Abstract

In this work we investigated binary quadratic forms that have positive discriminant. Binary quadratic forms of the same discriminant have a equivalence relation among them and this equivalence relationship construct a cycle structure. There exist interesting characteristic specification in the cycle belonging identity element of class group whose the discriminant has just two factors. We designed a factorization algorithm using these features. We show that this method can be effective for breaking the keys of the public key cryptosystem RSA.

Keywords: Binary quadratic forms, factorization

1. Giriş

İlk olarak literatüre Gauss [2] tarafından sunulan ikili kuadratik formların daha sonra birçok matematiksel yapıyla ilişkili olduğu gözlemlenmiştir. Örneğin; ikili kuadratik formların oluşturduğu grup ile aynı diskriminanta sahip derecesi iki olan sayı cisimlerine ait ideal sınıf grubu izomorftur. Bu bağlantı sayı cisimlerine ait birçok sonuca ulaşmada çok yardımcı olmuştur[5]. 20. yüzyılın sonuna doğru kompleks çarpımın da yardımıyla ikili kuadratik formlar hesaplamalı sayılar teorisinde ve kriptografide etkin bir şekilde kullanılmıştır. İlk olarak D. Shanks çarpanlara ayırmada ikili kuadratik formları kullanmıştır[14]. Benzeri bir şekilde bu makalede de geliştirilen metot için ikili kuadratik formlar kullanmıştır.

Herhangi bir sayının asal çarpanlarını bulma sorusuna teorik olarak birçok cevap verilmiş olsa da [3] özellikle 1980'lerin basında sunulan RSA açık anahtarlı kripto algoritmasından sonra pratikte de çok önemli bir hale gelmiştir. Herhangi asal olmayan sayıların çarpanlarına ayrılmasından ziyade sadece iki çarpanı olan sayıların asal çarpanlarını bulmaya yönelik çalışmalara ağırlık verilmiştir. B u konuda yüzlerce çalışma olmasına [3] rağmen günümüzde en çok kullanılan algoritmalar 1980'lerin basında sunulan Sayı Alan Kalburu [6] ve Eliptik Eğri Çarpanlara Ayırma metodudur [11]. Her ne kadar bu metotlar çeşitli sayılar için etkili olmuş olsa da RSA sistemini tehdit eder konumda değildir. Bu çalışmamızda iki tane asal çarpanı olan ve iki asal çarpanı da mod 4'te 3'e denk olan sayılar incelenecektir. Pratikte RSA algoritmasını kullanan sistemlerin büyük bir kısmı böyle sayıları açık anahtar olarak kullanmaktadır. Özetle üzerinde çalışacağımız sayılar aşağıdaki formda olacaktır:

$$n = pq \text{ ve } p, q \equiv 3 \, mod \, 4.$$

Makalenin ilk bölümünde çarpanlara ayırma metodu için kullanacağımız ikili kuadratik formları tanıtacağız. Daha sonra RSA algoritmasını kısaca tanıtacağız, en son bölümde ise algoritmayı sunarak çeşitli analizlere yer vereceğiz.

2. Tanımsız(Indefinite) formlar

Bu bölümde öncelikle tanımsız(indefinite) kuadratik formlardan kısaca bahsedilecek ve bu formlar ile reel kuadratik sayı cisimlerinin ideal sınıf grubu arasındaki bağlantı anlatılacaktır. Sonrasında, tanımsız formların temel olarak kullanıldığı bir çarpanlara ayırma algoritması gösterilecektir. Bu algoritma RSA algoritmasında kullanılan anahtarların (RSA modüllerinin) çarpanlarına ayrılması için tasarlanmıştır.

İkili kuadratik formlar temelde katsayıları tam sayı olan iki değişkenli ve ikinci dereceden fonksiyonlardır.

$$f(x, y) = ax^2 + bxy + cy^2 = (a, b, c)$$

formunda gösterilmektedir ve $ebob(a, b, c) = 1$'dir. Ayrıca tanımlanan f formunun diskriminantı

$$D = b^2 - 4ac$$

şeklinde bulunmaktadır.

Verilen herhangi bir m tamsayısı için, $f(x_0, y_0) = m$ eşitliğini sağlayan x_0, y_0 değerleri bulunabiliyorsa m tamsayısı f formunu temsil eder deriz. Örneğin;

$$m = ax^2 + bxy + cy^2$$

olsun. D değeri diskriminant olmak üzere;

$$4am = (2ax + by)^2 - Dy^2$$

eşitliği elde edilir. Burada açıkça görülebilir ki; $D < 0$ olması durumunda m'in pozitif veya negatif işaretli olma durumu a'nın işaretine bağlıdır. Yani m ve a değerleri aynı işaretlidir. $D > 0$ durumunda ise m degeri pozitif veya negatif işaretli olabilir. Bu sebeple f formu gibi formlar pozitif diskriminantlı tanımsız form olarak adlandırılmaktadır.

f ve f' aşağıdaki şekillerde tanımlanan iki ikili kuadratik form olsun;

$$f(x,y) = ax^2 + bxy + cy^2 = (x,y)\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

ve

$$f'(x,y) = (a',b',c') = a'x^2 + b'xy + c'y^2.$$

Eger 2x2 boyutlarında

$$\begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

eşitliğini sağlayan ve $det(A) = 1$ olmak üzere herhangi bir $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ matrisi bulunabiliyorsa, f ve f' formları birbirine denktir denir.

Bu denklik bağlantısı altında diskriminantı D olan ikili kuadratik formlar, $C(D)$ abelyen grubunu oluşturur. $C(D)$ grubunun mertebesine sınıf numarası(class number) denir ve $h = h(D)$ seklinde gösterilir. Herhangi bir D diskriminantı için sınıf numarası sonlu bir değerdir.

Tanım 2.1. Diskriminant D değerini bölen tek bir s asal sayısı olması durumunda (s, rs, c) seklinde formlar tanımlanabilir ve bu formların oluşturduğu formlara belirsiz(ambiguos) formlar denir.

Tanım 2.2. Diskriminantı D olan tanımsız bir (a,b,c) formunu ele alalım. Eğer bu form aşağıdaki koşulları sağlıyorsa indirgenmiş(reduced) form olarak adlandırılmaktadır.

$$\begin{gathered} 0 < b < \sqrt{D} \\ \sqrt{D} - b < 2|a| < \sqrt{D} + b \end{gathered} \qquad (1)$$

Yukarı tanım bize herhangi bir D diskriminant için sonlu sayıda indirgenmiş formun olduğunu göstermektedir. Ayrıca aynı diskriminant değerine sahip bir $f = (a,b,c)$ tanımlı formu için bu forma denk indirgenmiş bir form bulunur. Negatif diskriminantlar için her sınıfta sadece bir indirgenmiş form vardır. Ancak pozitif diskriminant değerli tanımsız formlarda bu durum farklıdır. Her sınıf birden fazla indirgenmiş forma sahip olabilir. Bu durumda, iki indirgenmiş formun aynı sınıfta olup olmadığına karar veren başka bir tanımlama daha mevcuttur.

Tanım 2.3. $f = (a, b, c)$ ve $f' = (c, b', c')$ iki indirgenmiş form olmak üzere

$$b + b' \equiv 0 \, mod \, 2c$$

denkliğinin sağlanması durumunda f' formu f'nin komsusudur(adjacent) denir.

Verilen indirgenmiş f formunun sağ komsusu f' ve sol komsusu (x', b'', a) olan essiz(unique) bir indirgenmiş formu bulunmaktadır ve bu komsu formlar aşağıdaki matris dönüşümü altında birbirine denktir.

$$\begin{pmatrix} 0 & -1 \\ 1 & \dfrac{b + b'}{2c} \end{pmatrix} \tag{2}$$

İspatları [2] 'de sunulmuş olan bu iki sonuç, verilen formların indirgenmiş olup olmadığına karar vermekte bize yardımcı olmaktadır.

Hatırlatma 2.4. (1) İndirgenmiş formların kümesi komsu formların oluşturduğu çevrimsel(cycle) yapı içerisinde bölünmüş bir şekilde bulunabilir.
(2) İki indirgenmiş form ancak ve ancak aynı çevrimde(cycle) ise birbirine denktir.

İspat. İspatlar için [2]'de Proposition 3.4 ve Theorem 3.5 'e bakınız.

Bu hatırlatma sonucunda sunu söyleyebiliriz ki; verilen diskriminant D değeri için sonlu sayıda indirgenmiş form var ise, indirgenmiş bir formun sürekli aynı yöndeki komsu formlarını bulmaya devam ettiğimizde son ulaşacağımız form yine en bastaki indirgenmiş form olacaktır.

3. RSA şifreleme sistemi

RSA şifreleme sistemi günümüzde güvenli iletişimde kullanılan açık anahtarlı bir şifreleme metodudur. Kısaca anlatmak gerekirse; Bob ve Alice isimli iki kişinin internet üzerinde haberleşmek istediğini düşünelim. m mesajı tam sayı olmak üzere Bob, m mesajını Alice'e göndermek istiyor. Bu durumda, Bob m mesajını şifrelemek için Alice'nin açık anahtarını(public key) kullanarak c şifreli metnini elde edecektir. Böylece, Alice c mesajını yalnızca kendi gizli anahtarını kullanarak deşifre ederek m mesajını okuyabilecektir.

Alice'nin açık anahtarı n ve e olmak üzere iki tam sayıdan oluşmaktadır. n tamsayı değeri, p ve q belirli koşulları sağlayan yaklaşık aynı büyüklükte iki asal sayı olmak üzere $n = pq$ seklinde tanımlanır. Ayrıca e değeri $ebob(e, (p - 1)(q - 1)) = 1$ koşulunu sağlamalıdır. Bu durumda, c şifreli metin aşağıdaki şekilde hesaplanmaktadır:

$$c \equiv m^e \, mod \, n.$$

p ve q değerlerini bilen Alice, aşağıdaki denkliği kullanarak d değerini hesaplar;

$$ed \equiv 1 \, mod \, (p - 1)(q - 1)$$

ve sonrasında

$$m \equiv c^d \equiv m^{ed} \, mod \, n$$

denkliğiyle m mesajını elde etmis olur.

Günümüzde bilinmektedir ki, RSA şifreleme sistemini kırmanın tek yolu verilen n açık anahtarının çarpanlarına ayrılmasıdır. Bundan dolayı n'i çarpanlarına ayırabilecek güçlü bir yöntem bulmak önemini korumaktadır.

Bu aşamada sunu belirtmeliyiz ki, RSA modülleri çoğunda çarpanlar mod 4'te 3'e denk olmaktadır. Bununla ilgili detaylı bilgi için [1]'e bakılabilir. Bu asamadan sonra, n'in çarpanları p ve q degerlerinin mod 4'te 3'e denk olduğu kabul edilecektir.

Önerme 3.1. $n = pq$ olsun. c, c' tamsayı olmak üzere (p, p, c) ve (q, q, c') asal formların, diskriminantı n olan ikili kuadratik formların oluşturduğu gruptaki mertebeleri 1'dir.

İspat. $\mathbb{Q}(\sqrt{n})$ bir reel kuadratik cisim olsun. Diskriminantı n olan ikili kuadratik form sınıflarının $C(n)$ grubu, $\mathbb{Q}(\sqrt{n})$ cisminin sınıf grubuna (narrow) izomorfiktir. (p, p, c) asal formu $\mathbb{Q}(\sqrt{n})$ cisminin sınıf grubuda p'nin üzerindeki ideale karsılık gelir. $\mathbb{Q}(\sqrt{n})$ cisminin ideal sınıf sayısının tek sayı olduğu bilinmektedir. Aynı zamanda p'nin üstündeki idealin $\mathbb{Q}(\sqrt{n})$ cismine ait tamsayı halkasında karesi 1'e esittir. Dolayısıyla bu idealin mertebesi ya 1 ya da 2'dir. İdeal sınıf sayısı tek olduğu için mertebe 1 olmak zorundadır. Aynı argüman (q, q, c') formu içinde geçerlidir.

Lemma 3.2. $n = pq$ olmak üzere $p < q$ olduğunu kabul edelim. Bu durumda herhangi k ve c' tamsayıları için (p, kp, c') formu $C(n)$ üzerinde indirgenmiştir.

İspat. $C(n)$ grubunun diskriminantının n oldugunu ve p'nin n'i böldüğünü biliyoruz. Bu durumda aşağıdaki eşitlikten

$$p^2 - 4pc = n = pq$$

c hesaplanarak $C(n)$ grubunda (p, p, c) seklinde bir belirsiz form elde edilir. Eğer (p, p, c) formununa

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

matrisini uygularsak;

$$\begin{pmatrix} p & 3p/2 \\ 3p/2 & c'' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} p & p/2 \\ p/2 & c \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

olmak üzere $c \in \mathbb{Z}$ değeri için $(p, 3p, c'')$ şeklinde denk bir form elde edilmiş olur. Böylece, A matrisini aynı şekilde yeterince sayıda uygularsak k ve c' tam sayıları için indirgenmiş (p, kp, c') formunu elde ederiz.

Lemma 3.2 ve Önerme 3.1 birlikte ele alındığında söyleyebiliriz ki; $\rho = (p, kp, c)$ formu elde edilir ve (p, kp, c) formunun $C(n)$ grubunun birim elemanı ile aynı çevrim(cycle) üzerinde olduğu görülür. Bu durumda n'nin bir çarpanı olarak p elde edilmiş olur. Bu sonuca istinaden aşağıda RSA modülü n üzerinde etkili olan bir algoritmanın adımlarını tanımlayacağız.

Algoritma 1. Girdi: $n = pq$ ve $p, q \equiv 3 \, mod \, 4$ olmak üzere, bir RSA modülü n seçilir.

(1) $C(n)$'in birim elemanı $(1, 1, (n-1)/4)$ formunun indirgenmis formu hesaplanır, bu indirgenmiş form $I = (1, b, c)$ olsun.
(2) (2) matris dönüşümü kullanılarak (p, kp, c') formu elde edilene kadar I formunun komşu formları hesaplanmaya devam edilir.

(p, kp, c') formunu ifade eden k ve c' değerlerinin bulunduğunu ve bu formun I birim elemanıyla aynı çevrim(cycle) içerisinde olduğunu gösterdik. Bu durumda I birim elemanından başlayıp sağ veya sola doğru komşu elemanları bulmaya devam edersek (p, kp, c') formu ile karşılaşmış oluruz. Bu forma ulaşma hızı I birim elemanının içinde bulunduğu çevrimin(cycle) eleman sayısına bağlıdır. $\mathbb{Q}(\sqrt{n})$ cisminin sınıf numarası h her zaman $\sqrt{n}$'den küçük olacaktır ve benzer şekilde diskriminant n için indirgenmiş form sayısı $\sqrt{n}$'den daha az sayıda olacaktır. Sınıf numarasının daha büyük bir değer olması durumunda birim elemanın bulunduğu çevrim kısa olur ve n'in bir çarpanına daha hızlı ulasılır. Öte yandan, eger h sınıf numarası küçük bir sayı ancak I birim elemanının bulunduğu çevrimin boyutu büyükse algoritma etkili bir şekilde çalışmayacaktır. Genel olarak, birim elemanın bulunduğu çevrimin boyutu küçükse, algoritma polinom zamanlı bir şekilde n'nin çarpanını bulabilecektir.

Teşekkür

Bu çalışma İstanbul Teknik Üniversitesi Araştırmacı Yetiştirme Programı (İTÜ-AYP) tarafından, İTÜ-AYP-2016-9 proje numarası ile desteklenmiştir.

Kaynaklar

[1] D. Boneh, Twenty Years of Attacks on the RSA Cryptosystem, Notices of AMS, 1999.
[2] D. A. Buell, Binary Quadratic Froms (Classical Theory and Modern Computations), Springer- Verlag, 1989.
[3] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, 2000.
[4] H. Cohen, H. W. Lenstra, Heuristics on class groups of number fields, Number Theory, Noordwijkerhout 1983, LN in Math. 1068, Springer-Verlag, (1984):33-62.
[5] D. A. Cox, "Primes of the form $x^2 + ny^2$ - Fermat, class field theory, and complex multiplication," John Wiley & Sons, New York, 1989.
[6] R. Crandall, C. Pomerance, Prime numbers: a computational perspective, Springer, New York, 2001.
[7] H. Davenport, H. Heilbronn, On the Density of Discriminants of Cubic Fields II, Proc. lloy. Soc. Lond. A 322 (1971): 405-420.
[8] G. Degert, Uber die bestimmung der grundeinheit gewisser reell-quadratischen zahlkorper. Abh. Math. Sem. Univ. Hamburg, 22 (1958):92-97.
[9] D. Goldfeld, Gauss' class number problem for imaginary quadratic fields, Bulletin of the AMS Volume 13,(1985):23-37.
[10] P. Hartung, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3. J. Number Theory 6 (1974):276-278.

[11] H. W. Lenstra, Jr., Factoring integers with elliptic curves, Ann. of Math. 126 (1987): 649–673.
[12] C. Richaud, Sur la resolution des equations $x^2 - Ay^2 = \pm 1$. Atti. Acad. Pontif. Nuovi Lincei (1866):177-182.
[13] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems. Commun. of the ACM, 21(1978):120-126.
[14] D. Shanks, Class number, a theory of factorization, and genera, Proc. Symp. in Pure Maths.20, A.M.S., Providence, R.I., (1969): 415-440.
[15] D. Shanks, On Gauss and composition I and II, Number Theory and Applications, R. Mollin (ed.), Kluwer Academic Publishers, (1989):263-204.
[16] L.C. Washington, Introduction to Cyclotomic Fields, 2nd edition, Springer, 1996.