G İ R İ Ş

Cebir ve sayılar teorisinde, Q rasyonel sayılar cisminin sonlu genişlemeleri olan sayı cisimleri ve bu cisimlerin ideal sınıfları grubunun mertebesi olarak tanımlanan sınıf sayılarının belirlenmesi en önemli konulardan birisidir.

Dirichlet sınıf sayısı formülü gibi bir takım formüller sınıf sayısının doğrudan hesabını mümkün kılmaktadır. Ancak ideal sınıfları grubu yardımıyla sınıf sayısının belirlenmesi kolay olmadığından bu formüller dışında çeşitli kriterler de elde edilmiştir.

D kare çarpansız bir tamsayı olmak üzere, Q rasyonel sayılar cisminin cebirsel genişlemesi olan $Q(\sqrt{D})$ kuadratik cismi D>0 ise "reel", D<0 ise "imajiner" olarak adlandırılır. İmajiner kuadratik sayı cisimleri için sınıf sayısı 1 problemi 1967 yılında H. M. Stark ve A. Baker tarafından bağımsız olarak çözülerek, bu cisimlerin sonlu sayıda ve $D = -1, -2, -3, -7, -11, -19, -43, -67, -163$ değerlerine karşılık gelen cisimler olduğu belirlenmiştir.

Sınıf sayısı 1 olan reel kuadratik sayı cisimlerinin sayısının sonlu olup olmadığı ise henüz kesinlik kazanmadığından (Gauss Konjektörü), sınıf sayısı 1 problemi reel kuadratik sayı cisimleri için tamamen çözülememiştir. Bu nedenle reel kuadratik sayı cisimlerinde çalışmak daha bir önem kazanmıştır.

Bu cisimlerin sınıf sayısının 1 olması için gerek ve yeter koşulları veren bir takım genel kriterler elde edilmesine rağmen bu kriterlerin Richaut-Degert (R-D) tipinde olmayan cisimlere uygulanması ve bu yolla sınıf sayısı 1 olan cisimlerin tespiti oldukça zor olmaktadır. Aynı zamanda reel kuadratik sayı cisimlerinin sınıf sayısının belirlenmesinde cismin temel birimi de önemli bir rol oynamakta ancak yine R-D tipinden olmayan sayı cisimleri için, temel birimin biçimi belli olmadığından, belirli kriterlerin bu cisimlere uygulanabilmesi de zor

olmaktadır. Bu nedenle son zamanlarda sınıf sayılarının belirlenmesine yönelik çalışmalar "R-D tipinden olmayan reel kuadratik sayı cisimleri " üzerinde yoğunlaşmıştır. Bu çalışmalarda bir çok yöntem kullanılmaktadır. Bu yöntemlerden en sık kullanılan üçü; kuadratik diophantine denklemler, sürekli kesre açılım ve dirichlet sınıf sayısı formülüdür.

Bu çalışmada da, genellikle R-D tipinden olmayan bazı sayı cisimleri ele alınarak, sözü geçen yöntemler yardımıyla sınıf sayısının belirlemeye yönelik kriterlerin elde edilmesi amaçlanmıştır.

I. Bölümde konuyla ilgili ön bilgilere yer verilmiştir.

II. Bölümde reel kuadratik sayı cisminin temel biriminin normunun -1 olması durumunda, 1992 yılında S.-G. Katayama ve 1993 yılında H. Yokoi'nin yaptığı çalışmalar göz önüne alınarak sınıf sayısını herhangi bir tek sayıdan büyük kılan bir "invaryant değer" tanımlanmıştır. Bu invaryant değerden küçük pozitif tamsayılara bağlı olarak sınıf sayısının tek olması için gerek ve yeterli koşullar elde edildikten sonra, bu kriterler ve Y. Kida'nın UBASIC86 programı kullanılarak D nin uygun bir değeri hariç $1 \le u \le 100$ sağlayan ve sınıf sayısı 3 olan 31 tane, sınıf sayısı 5 olan 22 tane reel kuadratik sayı cisminin varlığı gözlenmiştir. Bu çalışma sonunda S. Katayama ve H. Yokoi tarafından ve çeşitli yöntemler sonucunda bulunan cisimler de elde edilmiştir.

III. Bölümde, S.D. Lang, H.Yokoi, I. Yamaguchi ve R.A. Mollin'in diophantine denklemlerin çözülebilirliği ile sınıf sayısı 1 olan çeşitli tipteki reel kuadratik sayı cisimlerini belirlemeye yönelik [12,20,29,36] çalışmaları yardımıyla, $p = [(2n+1)q]^2 \mp 1$ kare çarpansız tamsayısı için $x^2 - py^2 = \mp q$ diophantine denkleminin çözümü irdelenmiş ve bu çözüme bağlı olarak sınıf sayısı 1 olan yegane cismin $Q(\sqrt{3})$ olduğunu belirleyen bir gerek ve yeter koşul elde edilmiştir.

IV. Bölümde ise R-D tipinden olmayan çeşitli tipteki reel kuadratik sayı cisimlerinin $\{1, w_d\}$ tamlık tabanlarının

$$w_d = \begin{cases} \dfrac{1+\sqrt{d}}{2} & , d \equiv 1 \pmod 4 \\ \sqrt{d} & , d \equiv 2,3 \pmod 4 \end{cases}$$

biçiminde tanımlanan, w_d quadratik irrasyonel sayısının sürekli kesre açılımında periyodun 6 olması durumunda, R.A. Mollin [18,21,22,23], K. Tomita [27,28] ve T. Azuhata'nın [2] çalışmaları göz önüne alınarak sürekli kesre açılımın genel biçimi ile temel birimin genel biçimi belirlenmiştir. Ayrıca, temel birimi belirlenen bu katsayılarına bağlı olarak [33,34,35] de tanımlanmış olan invaryant değerleri sıfır ya da sıfırdan farklı kılan gerek ve yeter koşullar elde edilmektedir. Bu çalışmanın sonunda verilen kriterler örneklerle pekiştirilerek sürekli kesre açılımın ve temel birimin belirlenmesindeki pratiklik gözlenmiş ve bu kriterleri sağlayan, sınıf sayısı 1 veya 2 olan cisimler sürekli kesre açılımlarıyla beraber tablolar halinde verilmiştir.

I. BÖLÜM

ÖN BİLGİLER

1.1. TEMEL KAVRAMLAR

1.1.1. Tanım

L ve K, $K \subseteq L$ şartını sağlayan iki cisim ise L cismine K cisminin bir "genişlemesi" denir ve L/K ile gösterilir. L nin K cismi üzerinde vektör uzayı olarak boyutuna "L nin K üzerindeki genişlemesinin derecesi " denir ve $[L:K]$ ile gösterilir. Eğer $[L:K] < \infty$ ise L/K ya "sonlu genişleme", L nin her elemanı K üzerinde cebirsel ise L/K ya "cebirsel genişleme" denir.

1.1.2. Tanım

L/K bir cisim genişlemesi ve α ceb/K olmak üzere $L = K(\alpha)$ biçiminde yazılabilir ise L cismine K cisminin bir "basit genişlemesidir" denir.

1.1.3. Tanım

Q rasyonel sayılar cisminin sonlu bir genişlemesine "cebirsel sayı cismi" denir.

1.1.4. Tanım

L/Q cebirsel bir genişleme olsun. Eğer bir $\alpha \in L$ elemanının Q üzerinde sağladığı polinom katsayıları Z de olan monik bir polinom ise α ya "cebirsel tamsayı" denir. Q nun bir α elemanının cebirsel tamsayı olması için gerek ve yeter koşul $\alpha \in Z$ olmasıdır.

1.1.1. Önerme

L bir cebirsel sayı cismi olsun. Bir $\alpha \in L$ nin Q üzerindeki eşlenikleri $\alpha = \alpha_1, \alpha_2, ..., \alpha_n$ ise,

$$N(\alpha) = \prod_{i=1}^{n} \alpha_i \ , İz(\alpha) = \sum_{i=1}^{n} \alpha_i$$

biçiminde tanımlanan ifadeler sırasıyla, "α nın normu" ve "α nın izi" olarak adlandırılır. Ayrıca, $\alpha, \beta \in L$ için,

$$N(\alpha.\beta) = N(\alpha).N(\beta) \ , \ İz(\alpha + \beta) = İz(\alpha) + İz(\beta)$$

ve $\alpha \in Q$ için

$$N(\alpha) = \alpha^2 \ , \ İz(\alpha) = 2\alpha$$

ifadeleri de sağlanmaktadır.

1.2. KUADRATİK SAYI CİSİMLERİ

1.2.1. Tanım

L/Q cebirsel bir genişleme ve $[L:Q] = 2$ ise L cebirsel sayı cismine "kuadratik sayı cismi" denir.

1.2.1. Önerme

L bir kuadratik sayı cismi ise en az bir d kare çarpansız tamsayısı için $L = Q(\sqrt{d})$ dir.

Kanıt:

$[L:Q] = 2$ ise $L = Q(\alpha)$ biçiminde basit genişlemedir. Yani α katsayıları Q da olan $x^2 + px + q$ biçimindeki asal bir polinomun kökü olduğundan katsayıları Z de olan $ax^2 + bx + c$ polinomunun da bir köküdür. Öyleyse;

$$\alpha = \frac{-b \mp \sqrt{b^2 - 4ac}}{2a}$$

ifadesinde $b^2 - 4ac = k$ alınırsa, $L = Q(\alpha) = Q(\sqrt{k})$ olur. Polinom Q[x] te asal olduğundan k nın tam-kare olmayan en az bir asal çarpanı vardır. Bu çarpana d denilirse, $L = Q(\sqrt{d})$ olur.

1.2.2. Tanım

$K = Q(\sqrt{d})$ kuadratik sayı cismi ise,

$O_K = \{\alpha \in K \mid \alpha \text{ tam} / Z\}$ kümesi toplama ve çarpma işlemine göre bir halkadır. O_K ya K cisminin "tamlık halkası" denir.

$$\alpha \in O_K \Leftrightarrow N(\alpha) \in Z \text{ ve } İz(\alpha) \in Z$$

dir.

1.2.1. Teorem

$K = Q(\sqrt{d})$ bir kuadratik sayı cismi olsun.

$$O_K = \begin{cases} Z + Z\sqrt{d} & , \quad d \equiv 2, 3 \pmod 4 \text{ ise} \\ Z + Z\left(\dfrac{1+\sqrt{d}}{2}\right) & , \quad d \equiv 1 \pmod 4 \text{ ise} \end{cases}$$

biçimindedir.

Kanıt :

$x, y \in Q$ olmak üzere; $\alpha = x + y\sqrt{d}$ olsun. 1.1.1.Önerme ve 1.2.2. Tanımdan $İz(\alpha + \alpha') = 2x \in Z$ dir. Buna göre; $\alpha = 2x + 2y\sqrt{d}$ olarak alındığında, $N(\alpha) = (2x)^2 - (2y)^2 d \in Z$ olur. En az bir k tamsayısı için $(2x)^2 - (2y)^2 d = k$ yazılabildiğinden $(2x)^2 = (2y)^2 d + k \in Z$ dir. d kare çarpansız olduğundan $2y \in Z$ bulunur.

$2x = u$, $2y = v$ olsun. Bu durumda, $x^2 - y^2 d \in Z$ olması $u^2 - v^2 d \equiv 0 \pmod 4$ olmasını gerektirir. Buna göre;

$d \equiv 2, 3 \pmod 4$ ise ,

$u^2 - v^2 d = u^2 + 2v^2 \pmod 4$ veya $u^2 - v^2 d = u^2 + v^2 \equiv 0 \pmod 4$ olacaktır.

Her iki durumda, $u^2 + 2v^2 \equiv 0 \pmod 4$ ve $u^2 + v^2 \equiv 0 \pmod 4$ ifadelerinin u ile v nin ikisinin de çift tamsayılar olması halinde sağlanacağı kolayca görülür. Bu ise x ile y nin birer tamsayı olması gerektiğini gösterir. O halde,

$$O_K \subseteq Z + Z(\sqrt{d})$$

sağlanır.

$d \equiv 1 \pmod 4$ ise $u^2 - dv^2 \equiv u^2 - v^2 \pmod 4$ olur. Bu da, u ile v nin ikisinin birden tek veya çift sayı olduğunu gösterir.

Bu durumda,

$$O_K = \left\{ \frac{u + v\sqrt{d}}{2} \;\middle|\; u \equiv v \pmod 2 \right\}$$

şeklindedir. Diğer yandan,

$$\frac{u + v\sqrt{d}}{2} = \left(\frac{u - v}{2}\right) + v\left(\frac{1 + \sqrt{d}}{2}\right)$$

biçiminde yazılabileceğinden ve $\frac{u - v}{2} \in Z$ olduğundan, $O_K \subseteq Z + Z\left(\frac{1 + \sqrt{d}}{2}\right)$ olacaktır. $N(\sqrt{d}) = -d$, $\text{İz}(\sqrt{d}) = 0$, $N\left(\frac{1 + \sqrt{d}}{2}\right) = \frac{1 - d}{4}$, $\text{İz}\left(\frac{1 + \sqrt{d}}{2}\right) = 1$ ifadeleri birer tamsayı olduğundan, $\sqrt{d}$, $\frac{1 + \sqrt{d}}{2} \in O_K$ olur.

Böylece,

$$Z + Z(\sqrt{d}) \subseteq O_K \;,\; Z + Z\left(\frac{1 + \sqrt{d}}{2}\right) \subseteq O_K$$

olduğu görüleceği için,

$$O_K = Z + Z(\sqrt{d}) \quad \text{ve} \quad O_K = Z + Z\left(\frac{1 + \sqrt{d}}{2}\right)$$

sağlanmış olur.

1.2.1. Sonuç

$K = Q(\sqrt{d})$ cisminin O_K tamlık halkası sonlu üretilmiş bir Z-modüldür ve üreteçleri kümesi;

$d \equiv 2, 3 \pmod 4$ ise $\{1, \sqrt{d}\}$

$d \equiv 1 \pmod 4$ ise $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$

biçimindedir.

1.2.3. Tanım

$K = Q(\sqrt{d})$ kuadratik sayı cismi ise,

$$w = \begin{cases} \sqrt{d} & , d \equiv 2, 3 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & , d \equiv 1 \pmod 4 \end{cases}$$

olmak üzere $\{1, w\}$ ikilisine O_K nın "tamlık tabanı " denir.

1.3. KUADRATİK SAYI CİSİMLERİNİN İDEALLERİ

1.3.1. Tanımlar

A, $K = Q(\sqrt{d})$ cisminin bir alt kümesi olsun. Eğer $A \neq Ø$ kümesi,

i) Her $a,b \in A$ için $a - b \in A$

ii) Her $a \in A$, $c \in O_K$ için $a.c \in A$

iii) $\exists\ 0 \neq \alpha \in O_K$ için $\alpha A \subseteq O_K$

koşullarını sağlıyorsa, A ya K nın bir "kesirsel ideali" denir. Özel olarak, O_K tamlık halkasının bütün idealleri birer kesirsel idealdir. Bu ideallere "tam idealler" denir.

(0) dan farklı kesirsel idealler, ideallerin çarpma işlemi altında bir grup oluştururlar ([25]).

A ile B iki kesirsel ideal olsunlar. $A = (\alpha)B$ olacak biçimde $\exists\, \alpha \in Q(\sqrt{d})$ elemanı varsa, A ile B "denk kesirsel ideallerdir" denir ve $A \sim B$ ile gösterilir.

A ve B, $Q(\sqrt{d})$ nin tam idealleri olsun. Eğer $(\alpha)A = (\beta)B$ olacak biçimde $\alpha, \beta \in O_K$ varsa, A ile B "denk tam ideallerdir" denir.

A bir tam ideal ise $A \cap Z \neq \emptyset$ dır.

O_K tamlık halkası $\{1, w\}$ ile üretilmiş bir Z-modül olduğundan O_K halkasının her tam ideali de sonlu üretilmiş bir Z-modüldür.

A tam ideali r_1, r_2 gibi iki cebirsel tam eleman ile üretildiğinden $\{r_1, r_2\}$ ye A "idealinin tabanı" denir. A ideali bu tabana bağlı olarak,

$$A = \{ar_1 + br_2 \mid a, b \in Z\}$$

biçiminde ifade edilir.

O_K halkası da $O_K = (1, w)$ biçiminde bir idealdir ve O_K ya "birim ideal" denir.

$A = (r_1, r_2)$, $K = Q(\sqrt{d})$ cisminin bir tam ideali olsun. r_1', r_1 in, r_2', r_2 nin eşleniğini göstermek üzere, $A' = (r_1', r_2')$ idealine A idealinin "eşleniği" denir.

1.4. KUADRATİK SAYI CİSİMLERİNİN DİSKRİMİNANTI

1.4.1. Tanım

$K = Q(\sqrt{d})$ cisminin tamlık halkası O_K nın bir tabanı $\{w_1, w_2\} = \{1, w\}$ biçiminde olsun.

$\Delta_{K/Q} = \det(\text{İz}(w_i, w_j))_{i,j=1,2}$ ifadesine O_K tamlık halkasının veya $K = Q(\sqrt{d})$ cisminin "diskriminantı" denir. Ya da G(K/Q), K/Q genişlemesinin Galois grubu olmak üzere diskriminant;

$$\Delta_{K/Q} = \left|\delta_i(w_j)\right|^2 = \left[\det(\delta_i(w_j))\right]^2$$

biçiminde tanımlanır.

1.4.1. Teorem

d kare çarpansız bir tamsayı olmak üzere, $K = Q(\sqrt{d})$ kuadratik sayı cismi veriliyor.

$$\Delta_{K/Q} = \begin{cases} 4d & , \quad d \equiv 2, 3 \pmod 4 \text{ ise} \\ d & , \quad d \equiv 1 \pmod 4 \text{ ise} \end{cases}$$

biçimindedir.

Kanıt:

$d \equiv 2,3 \pmod 4$ ise $Q(\sqrt{d})$ cisminin tamlık halkası O_K nın tabanı $\{1, \sqrt{d}\}$ olduğundan 1.4.1. Tanımdan,

$$\Delta_{K/Q} = \begin{vmatrix} \text{İz}_{K/Q}(1) & \text{İz}_{K/Q}(\sqrt{d}) \\ \text{İz}_{K/Q}(\sqrt{d}) & \text{İz}_{K/Q}((\sqrt{d})^2) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d$$

bulunur.

Benzer biçimde, $d \equiv 1 \pmod 4$ ise $K = Q(\sqrt{d})$ cisminin tamlık halkası O_K nın tabanı $(1, \frac{1+\sqrt{d}}{2})$ olduğundan,

$$\Delta_{K/Q} = \begin{vmatrix} \text{İz}_{K/Q}(1) & \text{İz}_{K/Q}(\frac{1+\sqrt{d}}{2}) \\ \text{İz}_{K/Q}(\frac{1+\sqrt{d}}{2}) & \text{İz}_{K/Q}((\frac{1+\sqrt{d}}{2})^2) \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{vmatrix} = d$$

olarak bulunur.

1.4.2. Tanım

$K = Q(\sqrt{d})$ cisminin bir tam ideali $A = (r_1, r_2)$ olsun. $\delta_A = (r_1.r_2' - r_1'.r_2)^2$ değerine "A idealinin diskriminantı" denir.

1.4.3. Tanım

A, $K = Q(\sqrt{d})$ cisminin bir tam ideali olsun. O_K /A bölüm halkasının eleman sayısına "A idealinin normu" denir ve N(A) = #(O_K /A) biçiminde gösterilir. N(A) daima sonlu bir sayıdır.

1.5. KUADRATİK SAYI CİSİMLERİNDE İDEALLERİN AYRIŞIMI

1.5.1. Tanım

$p \neq 2$ bir asal sayı ve $a \neq 0$ bir tamsayı olsun.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & x^2 \equiv a \pmod{p} \text{ çözümlü ve } (a,p) = 1 \text{ ise} \\ -1, & x^2 \equiv a \pmod{p} \text{ çözümsüz ise} \\ 0, & p \mid a \text{ ise} \end{cases}$$

biçiminde tanımlanan $\left(\frac{*}{*}\right)$ sembolüne "Legendre Sembolü" denir.

1.5.1. Teorem

$p \neq 2$ bir asal sayı ve a, b sıfırdan farklı tamsayılar ise,

i) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

iii) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

iv) $(a,p) = 1 \Rightarrow \left(\frac{a^2}{p}\right) = 1, \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

v) $\left(\frac{1}{p}\right)=1, \quad \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$

vi) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$

koşulları sağlanır ([24]).

1.5.2. Teorem (Gauss Reciprocity Kuralı)

Eğer p ve q farklı tek asal sayılar ise,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

sağlanır ([24]).

1.5.2. Tanım

$\left(\frac{*}{*}\right)$ Legendre sembolü olsun. a pozitif bir tamsayı, b pozitif tek bir tamsayı ve $b=p_1.p_2.....p_n$ (p_i ler asal) biçiminde olmak üzere;

$$\left(\frac{a}{b}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{a}{p_3}\right)...\left(\frac{a}{p_n}\right)$$

ise $\left(\frac{*}{*}\right)$ sembolüne "Jacobi Sembolü" denir.

1.5.3. Tanım

$\left(\frac{*}{*}\right)$ Jacobi sembolü olsun. Eğer

$$\left(\frac{a}{2}\right)=\begin{cases} 1, & a\equiv 1(\mathrm{mod}8) \text{ ise} \\ -1, & a\equiv 5(\mathrm{mod}8) \text{ ise} \\ 0, & a\equiv 0(\mathrm{mod}8) \text{ ise} \\ \text{tanimsiz}, & \text{diger hallerde ise} \end{cases}$$

özelliği ile genişletilmiş ise $\left(\frac{*}{*}\right)$ sembolüne Kronecker Sembolü denir.

1.5.4. Tanım

Δ , $K = Q(\sqrt{d})$ cisminin diskriminantı ve p bir asal sayı olmak üzere,

$$\chi_K(p) = \begin{cases} \left(\frac{\Delta}{p}\right), & p \neq 2,\ p \nmid \Delta \text{ ise} \\ (-1)^{\frac{\Delta^2-1}{8}}, & p = 2,\ 2 \nmid \Delta \text{ ise} \\ 0, & p \mid \Delta \text{ ise} \end{cases}$$

biçiminde tanımlanan χ_K fonksiyonuna K cisminin "Kronecker Karekteri" denir.

1.5.1. Sonuç

$K = Q(\sqrt{d})$ cisminin tamlık halkası O_K olmak üzere, O_K halkasında p tek asal değerinin ayrışımı;

i) $\left(\frac{\Delta}{p}\right) = 1 \Leftrightarrow$ p ayrışır (decomposed)

ii) $\left(\frac{\Delta}{p}\right) = -1 \Leftrightarrow$ p asal kalır (inert)

iii) $\left(\frac{\Delta}{p}\right) = 0 \Leftrightarrow$ p dallanır (ramified)

biçiminde ifade edilir ([5]).

1.5.2.Sonuç

$K = Q(\sqrt{d})$ cisminin tamlık halkası O_K olmak üzere p=2 asalının O_K halkasındaki ayrışımı aşağıdaki biçimde ifade edilir.

i) $\left(\frac{\Delta}{2}\right) = 1 \Leftrightarrow$ 2 ayrışır (decomposed)

ii) $\left(\frac{\Delta}{2}\right) = -1 \Leftrightarrow$ 2 asal kalır (inert)

iii) $\left(\frac{\Delta}{2}\right)=0 \Leftrightarrow$ 2 dallanır (ramified)

1.5.3. Teorem

$K=Q(\sqrt{d})$ kuadratik sayı cismi olsun. Bu durumda,

i) O_K nın (0) dan farklı her asal ideal maksimaldir.

ii) (0) dan farklı her tam ideal, asal ideallerin çarpım biçiminde tek türlü yazılabilir.

iii) (0) dan farklı kesirsel idealler, ideallerin çarpım işlemi altında çarpımsal bir grup oluşturur.

1.5.4. Teorem

p asal bir sayı, $P \subset O_K$, p yi kapsayan asal bir ideal ve $P' = \{\rho' | \rho \in P\} \neq P$ olsun. Diskriminantı Δ olan bir $K=Q(\sqrt{d})$ kuadratik sayı cisminde, bir p asalının ayrışımı;

i) $p \mid \Delta \Leftrightarrow (p)=\rho^2$ ve $N(\rho)=p$

ii) p>2 olsun

$$p \mid \Delta \Rightarrow \begin{cases} (p)=\rho.\rho' \ (\rho \neq \rho') \text{ ve } N(\rho)=N(\rho')=p, & \left(\frac{\Delta}{p}\right)=1 \text{ ise} \\ (p)=\rho \text{ ve } N(\rho)=p^2, & \left(\frac{\Delta}{p}\right)=-1 \text{ ise} \end{cases}$$

iii) p=2

$$p \mid \Delta \Rightarrow \begin{cases} (2)=\rho.\rho' \ (\rho \neq \rho') \text{ ve } N(\rho)=N(\rho')=2, & d \equiv 1 \pmod 8 \text{ ise} \\ (2)=\rho \text{ ve } N(\rho)=4, & d \equiv 5 \pmod 8 \text{ ise} \end{cases}$$

biçimindedir ([3]).

1.6. KUADRATİK SAYI CİSİMLERİNİN TEMEL BİRİMLERİ

1.6.1. Tanım

$K = Q(\sqrt{d})$ cisminin O_K halkasında tersi olan elemanların oluşturduğu gruba cismin "birimler grubu" denir ve U_d ile gösterilir.

1.6.1. Önerme

$\varepsilon \in O_K$ olmak üzere,

$$\varepsilon \in U_d \Leftrightarrow N(\varepsilon) = \mp 1 \text{ olmasıdır.}$$

Kanıt:

$\Rightarrow$ ε birim ise $\varepsilon | 1$ 'dir. Bu durumda $\varepsilon.\varepsilon' = 1$olacak biçimde $\varepsilon' \in O_K$ elemanı vardır. Bu durumda,

$$N(\varepsilon) = N(\varepsilon') = N(1) = 1 \Rightarrow N(\varepsilon).N(\varepsilon') = 1$$

olur. Buradan da $N(\varepsilon)$ nun Z de birim olduğu yani, $N(\varepsilon) = \mp 1$ olduğu görülür. ■

Bu önermeden faydalanarak $K = Q(\sqrt{d})$ kuadratik sayı cisminin birimleri aşağıdaki gibi belirlenir.

$d < 0$ olsun. $d \equiv 2, 3 \pmod 4$ ise $\{1, \sqrt{d}\}$, K cisminin tamlık tabanı olmak üzere, $\alpha \in O_K$ elemanı $x, y \in Z$ için $\alpha = x + y\sqrt{d}$ biçiminde ifade edileceğinden, $\alpha' = x - y\sqrt{d}$ için $N(\alpha) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$ olur. 1.6.1. önermeden $\alpha = x + y\sqrt{d}$ birim olduğundan $x^2 - dy^2 = \mp 1$ denkleminin sonlu sayıdaki çözümleri K imajiner kuadratik sayı cisminin birimlerini verecektir.

$d \equiv 1 \pmod 4$ ise $(1, \frac{1+\sqrt{d}}{2})$ K nın tamlık tabanı olmak üzere, $\alpha \in O_K$ elemanı $x, y \in Z$ için $\alpha = \frac{x + y\sqrt{d}}{2}$ biçiminde ifade edileceğinden,

$$N(\alpha) = \left(\frac{x + y\sqrt{d}}{2}\right)\left(\frac{x - y\sqrt{d}}{2}\right)$$

bulunur. 1.6.1. Önermeden yararlanarak α birim olduğu için $\frac{x^2 - dy^2}{4} = \mp 1$ bulunur. O halde $x^2 - dy^2 = \mp 4$ denkleminin sonlu sayıdaki çözümü $K = Q(\sqrt{d})$ cisminin birimlerini verecektir.

Bu ifadelere göre imajiner kuadratik sayı cisimlerinin birimleri için aşağıdaki önerme verilebilir.

1.6.2. Önerme

$K = Q(\sqrt{d})$ imajiner kuadratik sayı cismi olsun. i^2 = -1 ve $j = \frac{-1 + \sqrt{3}i}{2}$ olmak üzere,

i) $U_{-1} = \{ \mp 1, \mp i \}$

ii) $U_{-3} = \{ \mp 1, \mp j, \mp j^2 \}$

iii) $d \neq -1, -3$ ise $U_d = \{1, -1\}$

biçimindedir.

1.6.3. Önerme

$K = Q(\sqrt{d})$ reel kuadratik sayı cismi olsun. K cisminin U_d birimler grubu,

$$U_d = \{ \mp \varepsilon_d^s \mid s \in Z \}$$

olacak biçimde bir $\varepsilon_d > 1$ birimi bulunabilir.

1.6.1. Sonuç

s keyfi bir tamsayı olduğu için K cisminin U_d birim grubu sonsuzdur. C sonsuz devirli çarpımsal bir grup olmak üzere, $U_d \cong \{1, -1\} \times C$ dir.

1.6.2. Tanım

$K = Q(\sqrt{d})$ bir reel kuadratik sayı cismi olsun. K cisminin 1 den büyük birimlerinin en küçüğü ε_d ise, ε_d elemanına "temel birim" denir.

1.6.4. Önerme

$K = Q(\sqrt{d})$ reel kuadratik sayı cismi, $x, y \in Z$ için $\eta = \frac{x + y\sqrt{d}}{2} \in K$ ise aşağıdaki ifadeler gerçeklenir.

i) η bir birimdir $\Leftrightarrow x^2 - dy^2 = \mp 4$ olmasıdır. Ayrıca η bir birim ise $\eta > 1 \Leftrightarrow x > 0,\ y > 0$ ır.

ii) $\eta_i = \frac{x_i + y_i\sqrt{d}}{2}$ ($i = 1, 2$ ve $x_i, y_i \in Z$ için) birden büyük birimler ise; $\eta_1 < \eta_2 \Leftrightarrow x_1 < x_2,\ y_1 \le y_2$ 'dir. (Weiss, s.239)

Reel kuadratik sayı cisimlerinde temel birim, $d \equiv 1 \pmod 4$ olması durumunda $x^2 - dy^2 = \mp 4$ ile ifade edilen diophantine denkleminin 1 den büyük en küçük (x_o, y_o) pozitif tamsayı çözümü yardımıyla belirlenebilmektedir.

1.6.3. Tanım

$d = n^2 + r$ kare çarpansız pozitif bir tamsayı $r|4n$ ve $-n < r \le n$ ise $Q(\sqrt{d})$ cismine "Richaut-Degert (R-D) tipinden sayı cismi" denir.

$r = \mp 1, \mp 4$ ise $Q(\sqrt{d})$ cismine "dar (narrow) anlamda", aksi halde, "geniş (extended) anlamda Richaut-Degert (R-D) tipinden reel kuadratik sayı cismi" denir.

Bu cisimlerin temel birimleri, sgnr, r nin işaret fonksiyonu olmak üzere,

$$\varepsilon_d = \begin{cases} n + \sqrt{d} & ,|r| = 1 \text{ ise } (N(\varepsilon_d) = -\text{sgnr}) \\ \dfrac{n + \sqrt{d}}{2} & ,|r| = 4 \text{ ise } (N(\varepsilon_d) = -\text{sgnr}) \\ \dfrac{(2n^2 + r) + 2n\sqrt{d}}{|r|} & ,|r| \neq 1, 4 \text{ ise } (N(\varepsilon_d) = 1) \end{cases}$$

biçiminde belirlenmiştir.

1.7. KUADRATİK SAYI CİSİMLERİNİN SINIF SAYILARI

1.7.1. Tanım

$K = Q(\sqrt{d})$ kuadratik sayı cisminin bütün kesirsel idealleri ideallerin çarpma işlemine göre çarpımsal bir grup oluştururlar. Bu grubu G ile, G nin esas ideallerinin oluşturduğu grubu da E ile gösterelim. G/E bölüm grubu sonlu bir gruptur. G/E bölüm grubuna K cisminin "sınıf grubu" bu grubun eleman sayısına da K cisminin "sınıf sayısı" denir ve h_K ile gösterilir.

Bu nedenle cismin kesirsel idealleri grubu sınıflara ayrılmış olur. Bir sınıfın herhangi iki idealine "denk idealler" denir ve A ~ B biçiminde gösterilir. Ayrıca iki kesirsel idealin denkliği,

$$A \sim B \Leftrightarrow A = (\alpha)B$$

olacak biçimde $\exists\, 0 \neq \alpha \in O_K$ vardır, şeklinde ifade edilir.

Kesirsel ideallerin bir sınıfında tam idealler de vardır. Ayrıca A bir kesirsel ideal ise $\exists 0 \neq \alpha \in O_K$ için $\alpha A \subset O_K$ olduğundan ideal sınıflarının özellikleri ve sınıf sayısı ile ilgili sonuçları elde etmek için yalnızca tam idealleri göz önüne almak yeterlidir.

1.7.2. Tanım

A ve B, $K = Q(\sqrt{d})$ kuadratik sayı cisminin denk ve tam idealleri ise $(\alpha)A = (\beta)B$ olacak biçimde $\exists\, \alpha, \beta \in O_K$ vardır.

Eğer $N(\alpha.\beta) > 0$ ise elde edilen sınıflara "dar anlamda sınıf" denir. Bu sınıftaki ideallerin denkliği $A \approx B$ ile gösterilir. Dar anlamda sınıf sayısı da h_K^+ ile gösterilir.

Eğer $N(\alpha.\beta) > 0$ koşulu gerekli değil ise elde edilen sınıflara "geniş anlamda sınıf" denir ve sınıf sayısı h_K ile gösterilir.

1.7.1. Teorem

$K = Q(\sqrt{d})$ kuadratik sayı cisminin diskriminantı Δ ve temel birimi ε_d olsun. Bu durumda,

i) $\Delta < 0 \Rightarrow h_K^+ = h_K$

ii) $\Delta > 0 \Rightarrow \begin{cases} h_K^+ = h_K & , N(\varepsilon_d) = -1 \text{ için} \\ h_K^+ = 2h_K & , N(\varepsilon_d) = 1 \text{ için} \end{cases}$

koşulları gerçeklenir.

Kanıt:

i) $\Delta < 0$ durumunda her $x = \frac{a + b\sqrt{d}}{2} \in O_K$ için $N(x) = \frac{a^2 - b^2 d}{4} > 0$ olduğundan, her $\alpha, \beta \in O_K$ için $N(\alpha.\beta) > 0$'dır. Bu durumda dar anlamda sınıflar ile geniş anlamda sınıflar aynıdır. Öyleyse $h_K^+ = h_K$ 'dır

ii) $\Delta > 0$ olsun.

$N(\varepsilon_d) = -1$ durumunda, $(\alpha)A = (\beta)B = (\varepsilon_d.\beta)B$ biçiminde yazıldığında $N(\alpha.\beta), N(\alpha\beta\varepsilon_d)$ den biri pozitif olacaktır. Bu durumda dar anlamda sınıflar ile geniş anlamda sınıflar aynı olacaktır. Bu nedenle $h_K^+ = h_K$'dır.

$N(\varepsilon_d) = 1$ durumunda, $\forall \alpha, \beta \in O_K$ için $N(\alpha\beta) > 0$ koşulu her zaman gerçeklenemez. Bu durumda $A \approx B$ veya $A \approx B\sqrt{d}$ den biri gerçeklenir. Bu durumda $h_K^+ = 2h_K$ dır. Yani, geniş anlamda her denklik sınıfı dar anlamda iki denklik sınıfının birleşimidir ([4]).

1.7.2. Teorem

$K = Q(\sqrt{d})$ bir kuadratik sayı cismi, M_K Minkowski Sınırı ve Δ, K cisminin diskriminantı olmak üzere, K cisminin her ideal sınıfında,

$$N(P) \le M_K = \begin{cases} \frac{\sqrt{\Delta}}{2} & d > 0 \text{ ise} \\ \frac{2\sqrt{\Delta}}{\pi} & d < 0 \text{ ise} \end{cases}$$

olacak biçimde bir P tam ideali vardır.

Bir cebirsel sayı cisminin ideal sınıfları sayısı sonludur ([25]).

1.7.2. teoremden faydalanarak Minkowski sınırı yardımıyla bazı sayı cisimlerinin sınıf sayıları belirlenmiştir. Ancak M_K sınırı büyüdükçe bu yöntemle sınıf sayısını hesaplamak da zorlaşmaktadır.

1.7.3. Teorem

Bir sayı cisminin diskriminantı tek bir asal çarpan içeriyorsa, sınıf sayısı tektir ([4]).

1.7.4. Teorem

$K = Q(\sqrt{d})$ cisminin sınıf sayısının 1 olması için gerekli ve yeterli koşul K cisminin O_K tamlık halkasının bir esas ideal bölgesi olmasıdır.

Kanıt:

$:\Rightarrow$ $h_K = 1$ ise $\forall A \subset O_K$ ideali için $A \sim O_K$ dır. Bu durumda $\exists\, 0 \neq \alpha, \beta \in O_K$ için $(\alpha)A = (\beta)O_K = (\beta)$ olur. Bu ise $\exists x \in A$ için $\alpha x = \beta$ olduğunu yani; $x = \frac{\beta}{\alpha} \in A$ olduğunu belirtir ki $A = \left(\frac{\beta}{\alpha}\right)$ esas idealdir.

$\Leftarrow : O_K$ bir esas ideal bölgesi ise $0 \neq \alpha, \beta \in O_K$ olmak üzere her $A = (\alpha)$, $B = (\beta)$ idealleri için;

$(\beta)A = (\alpha)B$ yazılabileceğinden A~B olduğu elde edilir ve böylece $h_K = 1$ dir.

1.7.1. Önerme

A tamlık halkasının bir ideali ve h_K, K cisminin sınıf sayısı ise, A^{h_K} bir esas idealdir ($[26]$).

1.8. BASİT SÜREKLİ KESİRLER

1.8.1. Tanım

$x_o,x_1,...,x_k$ reel sayılar $1\le i\le k$ için $x_i>0$ olsun. Bu sayılar ile belirlenen,

$$< x_o,x_1,...,x_k >= x_o+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+...}}}$$
$$\ddots$$
$$+\cfrac{1}{x_{k-1}+\cfrac{1}{x_k}}$$

kesrine "pozitif sonlu sürekli kesir" denir.

$< x_o,x_1,...,x_k >$ pozitif sonlu sürekli bir kesir olmak üzere, $x_o\in Z$ ve $1\le i\le k$ için $x_i\in Z_+$ ise $< x_o,x_1,...,x_k >$ kesrine "basit sürekli kesir" denir.

Bu kısımda sürekli kesir denilince sadece pozitif, sonlu ve basit olanlar kastedilecektir.

Sonlu bir sürekli kesir aşağıdaki biçimlerde gösterilebilir:

$$< x_o,x_1,...,x_k >,\ < x_o,< x_1,...,x_k >>,\ < x_o,x_1,...,\frac{1}{x_k} >,\ x_o+\frac{1}{< x_1,...,x_k >}.$$

1.8.1.Teorem

(a, b) = 1, $a,b\in Z$ ve $b>0$ olmak üzere $\frac{a}{b}$ biçimindeki bir rasyonel sayı sonlu bir sürekli kesre eşittir. Tersine sonlu sürekli kesrin her değeri bir rasyonel sayıdır.

Kanıt

(a, b) = 1, $a,b\in Z$ ve $b>0$ olmak üzere, $r=\frac{a}{b}$ olsun. a yı b ile Euclide Algoritmasına göre bölersek,

$$a = q_o b + r_o \qquad , 0 < r_o < b$$
$$b = q_1 r_o + r_1 \qquad , 0 < r_1 < r_o$$
$$r_o = q_2 r_1 + r_2 \qquad , 0 < r_2 < r_1 \qquad (\forall i \geq 1 \text{ için } q_i, r_i \in Z^+)$$

.....
$$r_{k-2} = q_k r_{k-1}$$

eşitlikleri elde edilir. Bu eşitlikler kullanılarak,

$$r = \frac{a}{b} =< q_o, q_1, ..., q_n >$$

sonlu sürekli kesri elde edilir. $a < 0$ olabilir. Bu durumda $q_o < 0$ uygun bir biçimde seçilerek $1 \leq i \leq k$ için $q_i \geq 1$ olması sağlanır.

Teoremin tersi, bir merdiven kesrin rasyonel sayı değeri bulunarak elde edilir.

1.8.1. Sonuç

Bir $r = \frac{a}{b}$ rasyonel sayısı,

$$r = \begin{cases} < r >=< r-1, 1 > & ; \ r \in Z \text{ ise} \\ < q_o, q_1, ...q_k >=< q_o, q_1, ..., q_{k-1}, 1 > & ; \ r \notin Z \text{ ise} \end{cases}$$

biçimindedir.

Rasyonel sayılar ile sonlu sürekli kesirler arasında birebir eşleme vardır. Her $r \in Q$ için $r =< q_o, q_1, ..., q_k >$ ve $r > 1$ ise $\frac{1}{r} =< 0, q_o, q_1, ..., q_k >$ dir.

Verilen sonlu bir sürekli kesrin rasyonel sayı değerini bulmak, basamak sayısı arttıkça zorlaşır. Bu nedenle ilk birkaç basamak değeri için doğrudan hesaplama yapılarak aşağıdaki rekurans değerleri elde edilir.

$$< q_o >= \frac{q_o}{1}, \quad < q_o, q_1 >= q_o + \frac{1}{q_1} = \frac{q_o . q_1 + 1}{q_1}, \quad < q_o, q_1, q_2 >= \frac{q_o q_1 q_2 + q_o + q_2}{q_1 . q_2 + 1}$$

olduğu göz önüne alındığında, $P_{-2}=0,\ P_{-1}=1,\ Q_{-2}=1,\ Q_{-1}=0$ özel değerleri seçilirse,

$$P_o = q_o = q_o P_{-1} + P_{-2} \quad , \quad P_1 = q_1 q_o + 1 = q_1 P_o + P_{-1}$$

$$Q_o = 1 = q_o Q_{-1} + Q_{-2} \quad , \quad Q_1 = q_1 = q_1 Q_o + Q_{-1}$$

eşitlikleri elde edilir ve $k \geq 0$ için

$$P_k = q_k P_{k-1} + P_{k-2}$$

$$Q_k = q_k Q_{k-1} + Q_{k-2}$$

biçiminde $\{P_k\}$ ve $\{Q_k\}$ tamsayı dizileri elde edilir.

Buradan aşağıdaki sonuçlar söylenebilir.

i) $k \geq 0$ için $Q_k > 0$'dır.

ii) $k > 0$ için $Q_k > 0$ ise $0 < Q_o < Q_1 < .....$'dır.

iii) $Q_k \geq k$'dır.

1.8.2. Teorem

Herhangi bir x pozitif reel sayısı için,

$$< q_o, q_1, ..., q_{k-1}, x >= \frac{xP_{k-1} + P_{k-2}}{xQ_{k-1} + Q_{k-2}}$$

gerçeklenir.

1.8.3. Teorem

i) Eğer her $k \geq 0$ için tamsayısı için $c_k =< q_o, q_1, ..., q_k >$ alınırsa,

$$c_k = < q_o, q_1, ..., q_k >= \frac{P_k}{Q_k} \text{ olacaktır.}$$

ii) Her $k \geq -1$ için,

$$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1} \quad , \qquad c_k - c_{k-1} = \frac{(-1)^{k-1}}{Q_k Q_{k-1}}$$ denklemleri

ve

$P_kQ_{k-2} - P_{k-2}Q_k = (-1)^k q_k$, $c_k - c_{k-2} = \frac{(-1)^k q^k}{Q_k Q_{k-2}}$ eşitlikleri sağlanır.

iii) $\frac{P_k}{Q_k}$ indirgenmiştir ve bu da her $k \geq 0$ için $(P_k, Q_k) = 1$ olmasıdır.

1.9. SONSUZ SÜREKLİ KESİRLER

1.9.1. Tanım

Pozitif sonlu sürekli kesir tanımındaki k değeri sonsuz ise elde edilen sürekli kesre "sonsuz sürekli kesir" denir ve $< q_o, q_1, ... >$ ile gösterilir.

Sonsuz sürekli kesrin ilk k teriminden oluşan sonlu sürekli kesir $c_k = < q_o, q_1, ..., q_k >$ biçiminde olup buna sonsuz sürekli kesrin k. yaklaşımı denir. Eğer k çift ise c_k "çift yaklaşım" k tek ise c_k "tek yaklaşım" olarak adlandırılır.

1.9.1.Teorem

i) Çift yaklaşımlar dizisi düzgün artar.

ii) Çift yaklaşımlar dizisi düzgün azalır.

iii) Tek yaklaşımlar çift yaklaşımlardan büyüktür.

Kanıt

Her k çift sayısı için $c_k - c_{k-1}$ ve $c_k - c_{k-2}$ için 1.8.3 Teoremindeki $P_kQ_{k-2} - P_{k-2}Q_k = (-1)^k q_k$ eşitliğinden $\frac{P_k}{Q_k} = \frac{P_{k-2}}{Q_{k-2}} + \frac{q_k}{Q_k Q_{k-2}}$ ise $c_k = c_{k-2} + \frac{q_k}{Q_k Q_{k-2}}$ bulunur. Her k>0 için Q_k ve q_k değerleri pozitif olduğundan $c_{k-2} < c_k$ elde edilir.

Her $k \geq 1$ tek sayısı için benzer biçimde $c_k = c_{k-2} - \frac{q_k}{Q_k Q_{k-2}}$ bulunur.

Q_k ve q_k değerleri pozitif olduğundan $c_{k-2} > c_k$ olur.

$P_kQ_{k-1} - P_{k-1}Q_k = (-1)^{k-1}$ eşitliği alınırsa, her $j \geq 0$ ve i=2j+1 için

$\frac{P_{2j+1}}{Q_{2j}} - \frac{P_{2j}}{Q_{2j}} = \frac{1}{Q_{2j}Q_{2j+1}}$ ise $c_{2j+1} = c_{2j} + \frac{1}{Q_{2j}Q_{2j+1}}$ ve $c_{2j+1} > c_{2j}$ bulunur.

Bu durumda, her $r,s \geq 0$ için r=s ise $c_{k-2} < c_k$ eşitsizliğinden $c_{2r+1} > c_{2r} > c_{2s}$, r<s ise $c_{k-2} < c_k$ eşitsizliğinden $c_{2r+1} > c_{2s+1} > c_{2s}$ ve $c_{2r+1} > c_{2s}$ eşitsizlikleri elde edilir.

1.9.2.Teorem

$< q_o, q_1, q_2 ... >$ sonsuz sürekli kesri için

i) $\lim_{k\to\infty} c_k$ mevcuttur ve r , s herhangi iki pozitif tamsayı olmak üzere $c_{2r} < \lim_{k\to\infty} c_k < c_{2s+1}$ sağlanır.

ii) $\lim_{k\to\infty} c_k = < q_o, q_1, q_2 ... >$ olur.

iii $\alpha = < q_o, q_1, q_2 ... >$ ise $[\alpha] = q_o$ ve $\alpha = q_o + \frac{1}{< q_o, q_1, ... >}$ dir.

([x] :x elemanının tam değeridir.)

Kanıt

i) 1.91.Teoremden $\{c_{2k}\}$ artan ve herhangi bir tek yaklaşımla üstten sınırlı olduğundan, $\lim_{k\to\infty} c_{2k}$ mevcuttur. Benzer biçimde $\{c_{2k+1}\}$ azalan ve herhangi bir çift yaklaşımla alttan sınırlı olduğundan $\lim_{k\to\infty} c_{2k+1}$ de mevcuttur.

1.9.1. Teoremden $\lim_{k\to\infty} c_{2k+1} = \lim_{k\to\infty} c_{2k} + \lim_{k\to\infty} \frac{1}{Q_k Q_{2k+1}}$ bulunur. $\{Q_k\}$ artan bir dizi ve $Q_k \geq 0$ olduğundan son limit sıfır olacağından $\lim_{k\to\infty} c_{2k+1} = \lim_{k\to\infty} c_{2k}$ elde edilir. Bu da tek ve çift yaklaşımlar dizilerinin limitlerinin aynı olduğunu gösterir. Buradan $\lim_{k\to\infty} c_k = \lim_{k\to\infty} c_{2k} = \lim_{k\to\infty} c_{2k+1}$ sağlanır ve $c_{2r} < \lim_{k\to\infty} c_k < c_{2s+1}$ olacağı açıktır.

ii) ,iii) $c_{2r} < \lim_{k\to\infty} c_k < c_{2s+1}$ eşitsizliğinde r=s=0 alınır ise $q_o < \alpha < q_0 + \frac{1}{q_1}$ elde edilir. $q_1 \geq 1$ olduğundan $q_o < \alpha < q_0 + 1$ ve buradan $[\alpha] = q_o$ bulunur. Ayrıca $c_k = < q_o, q_1, q_2 ... >$ olduğundan

$$\alpha = \lim_{k\to\infty} c_k = q_o + \frac{1}{k \to \infty < q_o, q_1, ... >} = q_o + \frac{1}{< q_o, q_1, ... >}$$

olarak elde edilir.

1.9.3. Teorem

Her sonsuz sürekli kesir bir irrasyonel sayı belirler.

Kanıt:

$\alpha =< q_o, q_1, ... >$ sonsuz sürekli kesri bir rasyonel sayı belirlesin, n sonlu olmak üzere,

$$\alpha =< q_o, q_1, ... >=< p_o, p_1, ..., p_n >$$

olacaktır. Bu ancak ilk n terimin eşit olmasıyla mümkündür.

Bu durumda, $< q_n, q_{n+1}, ... >=< p_n >= p_n \in N^+$ olur ki, bu bir çelişkidir.

1.9.4. Teorem

Her α irrasyonel sayısı bir tek sürekli kesre eşittir ([24]).

Dolayısıyla α irrasyonel sayısı ile sonsuz sürekli kesirler arasında birebir bir eşleme vardır.

$\alpha =< q_o, q_1, ... >$ bir sonsuz sürekli kesir olsun.

$\alpha_k =< q_k, q_{k+1}, ... >$ biçimindeki sonsuz sürekli kesre α kesrinin "k-ıncı tamlayanı" denir.

$q_o \in Z$, $q_1, q_2, ..., q_{k-1} \in Z_+$ ve $\beta =< p_o, p_1, ... >$ 1 den büyük bir irrasyonel sayı ise,

$$< q_o, q_1, ..., q_{k-1}, \beta >=< q_o, q_1, ..., q_{k-1}, p_o, p_1, ... >$$

sağlanır.

1.10. PERİYODİK SÜREKLİ KESİRLER

1.10.1. Tanım

a ile b sıfırdan farklı rasyonel sayılar ve d kare çarpansız bir tamsayı olmak üzere,

$$\alpha = a + b\sqrt{d}$$

sayısına “kuadratik irrasyonel sayı” denir.

1.10.1. Önerme

Her α kuadratik irrasyonel sayısı, d kare çarpansız pozitif tamsayı ve $s \mid d - r^2$, r ve s sıfırdan farklı tamsayılar olmak üzere, $\frac{r+\sqrt{d}}{s}$ biçiminde yazılır.

Kanıt: $\alpha = a + b\sqrt{d}$ şeklinde olsun. r ile s sıfırdan farklı tamsayılar olmak üzere; $\alpha = \frac{u+v\sqrt{d}}{w}$ şeklinde yazılabilir. Karekökün işareti pozitif olacak biçimde,

$$\alpha = \frac{u+\sqrt{v^2 d}}{w} = \frac{u'+\sqrt{d_1}}{w} = \frac{u' \mid w \mid + \sqrt{w^2 d_1}}{w \mid w \mid} = \frac{u_1 + \sqrt{d}}{w_1}$$

yazılışı mümkündür. d_1 ve d tamkare değildir.

Ayrıca, $d - u_1^2 = w^2 d_1 - u'^2 w^2 = (d_1 - u'^2) w^2$ olduğundan $\mp w_1 = w^2 \mid d - u_1^2$ elde edilir. Bu durumda, r=u_1 , $s = w_1$ alınırsa, $\alpha = \frac{r+\sqrt{d}}{s}$ istenen yazılıştır.

1.10.2. Tanım

$\alpha =< q_o, q_1, ... >$ bir irrasyonel sayı olsun. Sonlu bir adımdan sonra q_k lar periyodik olarak eşit değerler alıyorsa bu kesre “periyodik sürekli kesir” denir.

$$\alpha =< q_o, q_1, q_2, ..., \overline{q_{k-1}, q_k, q_{k-1}, ..., q_{k+L-1}} >$$

biçiminde gösterilir ve L sayısına “kesrin periyod uzunluğu” denir.

1.10.1. Teorem

Herhangi bir periyodik sürekli kesir bir quadratik irrasyonel sayıya karşılık gelir, tersine bir quadratik irrasyonel sayının sürekli kesre açılımı periyodiktir ([24]).

1.10.1. Lemma

$\alpha =< q_o, q_1, ... >$ bir kuadratik irrasyonel sayı ve $\alpha = \alpha_o = \dfrac{r_o + \sqrt{d}}{s_o}$, $s \mid d - r^2$, r ve s sıfırdan farklı tamsayılar ise,

$$r_{k+1} = q_k s_k - r_k$$
$$s_{k+1} = \frac{d - r_{k+1}^2}{s_k} \qquad (1.1)$$

rekürans değerleri ve $k \geq 0$ için,

i) r_k ve $s_k \neq 0$ birer tamsayıdır.

ii) $s_k \mid d - r_k^2$ dir.

iii) $\alpha_k = \dfrac{r_k + \sqrt{d}}{s_k}$ dir.

özellikleri kullanılarak $\alpha = \alpha_o = \dfrac{r_o + \sqrt{d}}{s_o}$ kuadratik irrasyonel sayısının sonsuz sürekli kesre açılımı elde edilir.

1.10.2. Lemma

$\alpha = \alpha_o = \dfrac{r_o + \sqrt{d}}{s_o}$ bir kuadratik irrasyonel sayı ve α elemanının eşleniği α' olsun. Eğer $n > 1$ tamsayısı için $\alpha'_{n-1} < 0$ ise,

i) $-1 < \alpha'_n < 0$

ii) $0 < r_n < \sqrt{d}$

iii) $0 < s_n < 2\sqrt{d}$

koşulları gerçeklenir ([24]).

1.10.3. Tanım

Bir sürekli kesrin periyod dışında kalan elemanı yoksa bu kesre "pürperiyodik (tamamen periyodik) kesir" denir.

1.10.4. Tanım

α bir kuadratik irrasyonel sayı ve α', α nın eşleniği olsun. Eğer $\alpha > 1$, $-1 < \alpha' < 0$ ise α ya "indirgenmiş kuadratik irrasyonel sayı" denir.

1.10.2. Teorem

Bir α kuadratik irrasyonel sayısının sonsuz sürekli kesrinin pür-periyodik olması için gerek ve yeter koşul α nın indirgenmiş olmasıdır ([24]).

1.10.3. Teorem

d kare çarpansız bir tamsayı olsun. α kuadratik irrasyonel sayısının sonsuz sürekli kesre açılımı;

$$\alpha = \sqrt{d} \text{ ise, } < q_o, \overline{q_1,...,2q_o} >$$

$$\alpha = \frac{1+\sqrt{d}}{2} \text{ ise, } (\alpha \geq 7 \text{ için}) \quad < q_o, \overline{q_1,...,2q_o - 1} >$$

biçimindedir (Hasse [5]).

1.10.5. Tanım

$\alpha = a + b\sqrt{d}$ kuadratik irrasyonel sayı olsun. $d \equiv 1 \pmod 4$ ise $\Delta = d$, $d \equiv 2, 3 \pmod 4$ ise $\Delta = 4d$ biçimindeki $\Delta > 0$ sayısına "α nın diskriminantı" denir.

1.10.6. Tanım

ξ, η reel sayıları için $ad - bc = \mp 1$ $(a,b,c,d \in Z)$ olmak üzere $\xi = \frac{a\eta + b}{c\eta + d}$ sağlanıyor ise ξ ve η ya "denk sayılar denir" ve $\xi \sim \eta$ ile gösterilir.

i) ξ ve η gibi iki irrasyonel sayının denk olması için gerek ve yeter şart bunların sürekli kesre açılımlarının sonlu adımlardan sonra tamamen aynı olmasıdır ([14]).

ii) Bütün irrasyonel sayılar birbirine denktir ([24]).

iii) Denk kuadratik irrasyonel sayıların diskriminantı eşittir.

iv) Her kuadratik irrasyonel sayı ayrı diskriminanta sahip bir indirgenmiş kuadratik irrasyonel sayıya denktir.

v) ξ ve η indirgenmiş iki irrasyonel sayı olsun. Aşağıdaki denk koşullardan biri sağlanır ise $\xi \sim \eta$ dır.

a) $\xi = \dfrac{a\eta + b}{c\eta + d}$, $\quad ad - bc = \mp 1 \; (a,b,c,d \in Z)$

b) $\xi =< q_o, q_1, ..., q_{m-1}, \eta >$, $\; q_i \in Z_+ \qquad i=0,.....m-1$

c) $\eta =< p_o, p_1, ..., p_{n-1}, \xi >$, $\; p_i \in Z_+ \qquad i=0,.....n-1$

II. BÖLÜM

TEMEL BİRİMİNİN NORMUNUN -1 OLMASI DURUMUNDA SINIF SAYISI TEK SAYI OLAN REEL KUADRATİK SAYI CİSİMLERİNİN İNVARYANT DEĞERLER YARDIMIYLA BELİRLENMESİ

Temel birimin normuna bağlı olarak, belirli tipteki reel kuadratik sayı cisimlerinin sınıf sayılarının belirlenmesi için, R. A. Mollin - H. C. Williams, S. Katayama, H. Yokoi, H. Taya - N. Terai, H. K. Kim, M, - G. Leu – T. Ono çeşitli yöntemler geliştirmişlerdir. 1990 yılında Shin-Ichi Katayama ve Shigeru Katayama dirichlet sınıf sayısı formülünü kullanarak temel birimin normu -1 olup sınıf sayısı 1, 3 ya da 5 olan reel kuadratik sayı cisimlerini belirlemişlerdir ([8]). 1998 yılında F. Karaali ve H. İşcan temel birimin normunun +1 olması durumunda $1 \le u \le 100$ için invaryant değerler yardımıyla sınıf sayısı 1 veya 2 olan reel kuadratik sayı cisimlerini belirlemişlerdir ([7]).

Bu bölümde, D kare çarpansız bir tamsayı, $\varepsilon_D = \frac{t + u\sqrt{D}}{2} > 1$, $Q(\sqrt{D})$ reel kuadratik sayı cisminin temel birimi olmak üzere, temel birimin normunun -1 olması durumunda $1 \le u \le 100$ için D nin uygun bir değeri hariç sınıf sayısı tek sayı olan reel kuadratik sayı cisimlerinin belirlenmesi amaçlanmıştır.

Burada $N(\varepsilon_D) = -1$ olan reel kuadratik sayı cismi $k = Q(\sqrt{D})$, k cisminin sınıf sayısı h_k, diskriminantı d_k, kronecker karakteri χ_k ile gösterilecektir.

Ayrıca, $N : Q(\sqrt{D}) \to Q$ norm fonksiyonu, [x] ile de herhangi bir x elemanının tam değeri gösterilmektedir.

2.1. Önerme

D kare çarpansız pozitif bir tamsayı olsun. Eğer, $t^2 - Du^2 = -4$ denklemi çözülebilir ise, p_i ve q_j ler mod 4 e göre 1 e denk asal sayılar, e_j ler pozitif tamsayılar ve δ_1, δ_2, 0 yada 1 olmak üzere, D ve u;

$$D = 2^{\delta_1} \prod_i p_i \,, \quad u = 2^{\delta_2} \prod_j q_j^{e_j}$$

biçiminde asal çarpanlara ayrılır. Ayrıca $D \equiv 2 \pmod 4$ ise $t \equiv 0 \pmod 2$, $u \equiv 0 \pmod 2$ dir.

Kanıt:

$t^2 - Du^2 = -4$ Pell Denklemi çözülebilir ise $t^2 \equiv -4 \pmod{Du^2}$'dir. p, Du^2 nin herhangi bir asal çarpanı olmak üzere $t^2 \equiv -4 \pmod p$ elde edilir. Buradan $1 = \left(\frac{-4}{p}\right) = (-1)^{\frac{p-1}{2}}$ olduğu kullanılarak $p \equiv 1 \pmod 4$ bulunur. Eğer $u \equiv 0 \pmod 4$ sağlanırsa $t^2 - Du^2 = -4$ denkleminden $t \equiv 0 \pmod 2$ olur. $u = 4u_o$, $t = 2t_o$ olarak alındığında $t_o^2 - 4u_o^2 = 1$ elde edilir. Bu durumda $t_o^2 \equiv -1 \pmod 4$ olur. Bu bir çelişki olduğundan $u \equiv 0 \pmod 2$ olmalıdır.

2.2. Önerme

$k = Q(\sqrt{D})$ cismi için $N(\varepsilon_D) = -1$ iken, sınıf sayısı h_k tek sayı ise p, $p \equiv 1 \pmod 4$ sağlayan bir asal olmak üzere, D = p dir.

Kanıt:

$N(\varepsilon_D) = -1$ olduğundan kuadratik sayı cisimlerinin cins teoreminden h_k^+, k nın dar anlamda sınıf sayısı h_k^* bir cinsteki sınıfların sayısı ve t, D nin farklı asal çarpanlarının sayısı olmak üzere, [5] den $h_k = h_k^+ = 2^{t-1} h_k^*$ sağlanır.

h_k tek sayı olduğundan $2^{t-1}=0$ olmalıdır. Bu t=1 olması sonucunu vereceğinden $\exists$ p asalı için D = p bulunur. 2.1. Önermeden $p \equiv 1 \bmod(4)$ olacağı açıktır.

2.1. Lemma

D kare çarpansız bir tamsayı ve $N(\varepsilon_D) = -1$ olmak üzere,

$$V_D = \left\{ v \mid \ 0 \le v < u^2, \ \ v^2 \equiv -4 \ (\mathrm{mod} u^2) \ \right\}$$

$$(V,W)_D = \left\{ (v,w) \mid v \in V_D, \ v^2 + 4 = w.u^2 \ \right\}$$

biçiminde iki küme tanımlansın. Herhangi bir D için,

$$t = u^2 n + v$$

$$D = u^2 n^2 + 2vn + w$$

olacak biçimde tek şekilde tanımlanan $n \in N_o = N \cup \{0\}$ ve $(v,w) \in (V,W)_D$ değerleri vardır. Özel olarak u > 2 ise $0 \le w < v < u^2$ ve $\left[\frac{D}{t} \right] = n$ dir ([31]).

Kanıt:

$\boldsymbol{D}_- = \left\{ \ D \in \boldsymbol{D} \mid \ N(\varepsilon_D) = -1 \right\}$ temel biriminin normu -1 olan tüm $Q(\sqrt{D})$ cisimlerini belirleyen kare çarpansız tamsayılarının kümesini göstersin.

Herhangi bir $D \in \boldsymbol{D}_-$ için $\left[\frac{t}{u^2} \right] = n$ ve $t = u^2 n + v$ alınırsa, bu durumda n ve v sayıları $n \in N_o$, $0 \le v < u^2$ olacak biçimde tek şekilde tanımlanır. Buradan,

$$Du^2 = t^2 + 4 = (u^2 n + v)^2 + 4 = u^4 n^2 + 2u^2 nv + v^2 + 4$$

ve

$$v^2 + 4 \equiv 0 \ (\mathrm{mod} u^2)$$

bulunur. Bu da $v \in V_D$ olduğunu gösterir. $v^2 + 4 = wu^2$ alınırsa, w da tek şekilde tanımlanmış olacağından $(v,w) \in (V,W)_D$ olacaktır. Ayrıca,

$Du^2 = t^2 + 4 = (u^2 n + v)^2 + 4 = u^4 n^2 + 2u^2 nv + v^2 + 4$ ve $v^2 + 4 \equiv 0 \ (\mathrm{mod} u^2)$

ifadelerinden $D = u^2n^2 + 2nv + \frac{v^2+4}{u^2} = u^2n^2 + 2nv + w$ elde edilir.

u > 2 durumunda, $0 \le v < u^2$ eşitsizliğinden $w.u^2 = v^2 + 4 < u^4 + 4$ olacağından $w \le u^2$ olduğu görülür. $w = u^2$ alınırsa, $v^2 + 4 = wu^2$ ifadesinden $u^4 - v^2 = 4$, $(u^2 - v)(u^2 + v) = 4$ olur. Bu ise u > 2 durumuyla çelişir. Öyleyse $0 \le w < u^2$ olmalıdır. $g(x) = -x^2 + u^2x - 4$ polinomu göz önüne alınırsa,

$$g(1) = -1 + u^2 - 4 = u^2 - 5 > 0$$

ve

$$g(w) = -w^2 + u^2w - 4, \quad g(w) = v^2 - w^2 > 0 \text{ , } w^2 < v^2, \ w < v$$

bulunur. O halde,

$$0 \le w < v < u^2$$

eşitsizliği gerçeklenir.

Sonuç olarak, $t = u^2n + v$ ve $D = u^2n^2 + 2vn + w$ olduğu kullanılarak

$$D = u^2n^2 + vn + vn + w = tn + vn + w$$

olarak yazılabilir. Buradan

$$\left[\frac{D}{t}\right] = \left[\frac{tn + vn + w}{t}\right] = \left[n + \frac{vn + w}{t}\right]$$

bulunur. $w + vn > 0$ ve

$$t - (vn + w) = t - vn - w = u^2n + v - vn - w = n(u^2 - v) + v - w > 0$$

olduğundan,

$$\left[\frac{D}{t}\right] = n$$

elde edilir.

2.2. Lemma (Tatuzawa)

$0 < \alpha < \frac{1}{2}$ sağlayan herhangi bir α gerçel sayısı için d_k, $d_k \ge \max\{ e^{1/\alpha}, e^{11.2} \}$ sağlayan bir pozitif tamsayı ve χ_d, modülü d_k olan esas olmayan primitif bir karakter olsun. Bu durumda χ_d karakterine karşılık gelen

$L(s,\chi_d)$ L-fonksiyonunun s = 1 noktasındaki değeri için, d_k nın uygun bir değeri hariç,

$$L(1,\chi_d) > 0{,}655\left(\frac{\alpha}{d_k{}^{\alpha}}\right)$$

eşitsizliği sağlanır ([27]).

2.3. Önerme

D kare çarpansız bir tamsayı olmak üzere $Q(\sqrt{D})$ cisminin temel biriminin normu $N(\varepsilon_D) = -1$ ise $t < \varepsilon_D < u\sqrt{D}$ ve $u \neq 2$ ise $\varepsilon_D < D$ sağlanır.

Kanıt:

$\varepsilon_D = \frac{t + u\sqrt{D}}{2} > 1$ temel biriminin normu $N(\varepsilon_D) = -1$ ise $t^2 - Du^2 = -4$ dir.

Bu durumda, $t^2 = Du^2 - 4 \Rightarrow t = \sqrt{Du^2 - 4} < u\sqrt{D}$ olur ve buradan

$$\varepsilon_D = \frac{t + u\sqrt{D}}{2} < \frac{u\sqrt{D} + u\sqrt{D}}{2} = u\sqrt{D}$$ eşitsizliği gerçeklenir.

u = 1 için ;

$$t^2 - Du^2 = t^2 - D = -4 \Rightarrow t^2 = D - 4$$
$$\Rightarrow t^2 < D$$
$$\Rightarrow t < \sqrt{D}$$

olur. Bu durumda, $\frac{t}{u^2} = t < \sqrt{D}$ olduğundan $\frac{t}{u^2} \geq 1$ olarak elde edilir.

$u > 2$ için 2.1.Lemma'dan $0 \leq w < u^2$ ve $t = u^2 n + v$ olduğu kullanılarak $\frac{t}{u^2} = n + \frac{v}{u^2}$ yazılır. $n \neq 0$ olduğundan $\frac{t}{u^2} - n = \frac{v}{u^2} < 1$ olur. Buradan da $\frac{t}{u^2} > 1$ olduğu görülür.

$t^2 - Du^2 = -4$ denklemi $\frac{t^2}{u^2} = D - \frac{4}{u^2} = (D - \frac{2}{u})(D + \frac{2}{u})$ biçiminde yazılırsa,

$$D > t.\frac{t}{u^2} > D - \frac{1}{2} \qquad (2.1)$$

eşitsizliği elde edilir. u=1 için $\frac{t}{u^2} \geq 1$, $u > 2$ için $\frac{t}{u^2} > 1$ ve (2.1) eşitsizliğinden $t < D$ bulunur. Ayrıca $u \neq 2$ durumunda $t^2 + 4 = Du^2$ ifadesinde t<D alınırsa $Du^2 < D^2 + 4$, $Du^2 < D^2$ buradan da $u\sqrt{D} < D$ elde edilir. Sonuç olarak, $t < \varepsilon_D < u\sqrt{D}$ ve $u\sqrt{D} < D$ olduğundan $\varepsilon_D < D$ eşitsizliği gerçekleşmiş olur.

2.3. Lemma (Davenport-Ankeny-Hasse-Ichimura)

$D > 1$ kare çarpansız rasyonel bir tamsayı ve $\varepsilon_D = \frac{t + u\sqrt{D}}{2} > 1$, $Q(\sqrt{D})$ cisminin temel birimi olsun. $m > 1$ doğal sayısı için,

$$x^2 - Dy^2 = \mp 4m$$

diophantine denkleminin en az bir aşikar olmayan çözümü varsa,

$$m \geq \begin{cases} \frac{t}{u^2} & , N(\varepsilon_D) = -1 \\ \frac{t-2}{u^2} & , N(\varepsilon_D) = 1 \end{cases}$$

sağlanır ([20]).

2.4. Önerme

m tek, pozitif bir tamsayı olmak üzere, sabit bir u elemanı için, $h_k > m$ olacak biçimde bir c gerçel sayısı ve temel birimin u değerine bağlı $n \geq v(u)$ olduğunda $h_k > m$ sağlayan bir $v(u)$ gerçel sayısı vardır. (D nin uygun bir değeri hariç)

Kanıt:

Dirichlet sınıf sayısı formülünden, $y \geq 11{,}2$ gerçel sayısı ve $d_k \geq e^y$ sağlayan d_k nın uygun bir değeri hariç, $L(1, \chi_k) > \frac{0{,}655}{y} d_k^{-1/y}$ olduğundan,

$$h_k = \frac{\sqrt{d_k}}{2\log\varepsilon_D}.L(1,\chi_k) > \frac{0{,}655\sqrt{d}_k.d_k^{-1/y}}{2y\log\varepsilon_D}$$

eşitsizliği elde edilir.

$N(\varepsilon_D) = -1$ durumunda, $\varepsilon_D < u\sqrt{D}$ ve $D \equiv 1 \pmod 4$ iken, $D = d_k$ olduğu kullanılarak,

$$h_k > \frac{0{,}655.d_k^{1/2-1/y}}{y(2\log u + \log d_k)}$$

eşitsizliği elde edilir. Özellikle $d_k = e^y$ için

$f(\log u, y) = \frac{0{,}655.e^{y-2/2}}{2y\log u + y^2}$ olarak ele alındığında $y \geq 11.2$ için $f(\log u, y)$ fonksiyonunun monoton artan bir fonksiyon olduğu görülür.

$f(\log u, c) = \frac{0{,}655.e^{\frac{c}{2}-1}}{2c\log u + c^2} \geq m$ eşitsizliğinden c gerçel sayısının alacağı en küçük ve en büyük değerler ;

$1 \leq u \leq 100$ olmak üzere,

$$h_k > f(\log u, c) = \frac{0{,}655.e^{\frac{c}{2}-1}}{c(2\log 1 + c)} = \frac{0{,}655.e^{\frac{c}{2}-1}}{c^2} \geq m \qquad (2.2)$$

$$h_k > f(\log u, c) = \frac{0{,}655.e^{\frac{c}{2}-1}}{c(2\log 100 + c)} = \frac{0{,}655.e^{\frac{c}{2}-1}}{9{,}21c + c^2} \geq m \qquad (2.3)$$

eşitsizliklerinden bulunur. Aynı zamanda,

$t^2 - Du^2 = -4$ ifadesinden $t = \sqrt{Du^2 - 4}$ bulunacağından $\frac{t}{u^2} = \frac{\sqrt{Du^2 - 4}}{u^2}$

elde edilir. Buradan $e^c \leq D = d_K = u^2 + 2vn + w$ olduğu kullanılarak

$$\frac{t}{u^2} \geq \frac{\sqrt{u^2 e^c - 4}}{u^2} \qquad (2.4)$$

eşitsizliğine ulaşılır. (2.3) den

$$\frac{0,655.e^{\frac{c}{2}}}{e(9,21c+c^2)} \geq m \Rightarrow \sqrt{e^c} \geq \frac{m(9,21c+c^2)}{0,24}$$

$$\Rightarrow e^c \geq \frac{m^2(9,21c+c^2)^2}{0,0576}$$

eşitsizliği elde edilir.

Bu eşitsizlik kullanılarak,

$$\frac{t}{u^2} \geq \frac{\sqrt{u^2e^c-4}}{u^2} \geq \sqrt{\frac{\frac{u^2(9,21c+c^2)^2m^2}{0,0576}-4}{u^4}}$$

$$= \sqrt{\frac{(9,21c+c^2)^2m^2}{(0,0576)u^2}-\frac{4}{u^4}} \qquad (2.5)$$

olduğu görülür. (2.4) ve (2.5) eşitsizliklerinden

$$\frac{t}{u^2} = \sqrt{\frac{(9,21c+c^2)^2m^2}{(0,0576)u^2}-\frac{4}{u^4}}$$

elde edilir. $v(u)=\frac{t}{u^2}$ olarak alınırsa, $v(u)$ invaryant değeri

$$v(u)=\sqrt{\frac{(9,21c+c^2)^2m^2}{(0,0576)u^2}-\frac{4}{u^4}}$$

olacaktır.

Buradan, $n \geq v(u)$ sağlayan n değerleri için $h_k > m$ olduğu sonucuna ulaşılır.

O halde $n \geq v(u)$ olan n değerleri için $h_k > m$ (m: tek sayı) olduğundan $0 \leq n < v(u) = \sqrt{\frac{(9,21c+c^2)^2m^2}{(0,0576)u^2}-\frac{4}{u^4}}$ invaryant değeri için $D = u^2n^2+2vn+w$ olmak üzere, $K = Q(\sqrt{D})$ cisimlerinin sınıf sayısı tek sayı olabilir.

2.4. Lemma

$D>1$ kare çarpansız bir tamsayı ve $q\neq 2$ bir asal olsun. Bu durumda aşağıdaki koşullar denktir,

i) e, $x^2-Dy^2=\mp 4q^e$ denklemi en az bir tam çözüme sahip olacak biçimdeki en küçük tamsayıdır.

ii) $\left(\frac{D}{q}\right)=1$ dir ve e doğal sayısı $Q(\sqrt{D})$ nin ideal sınıf grubunda q nun q_1, q_2 $(q_1\neq q_2)$ asal çarpanlarının mertebesidir ([20]).

2.5. Lemma

$D>1$ kare çarpansız bir tamsayı, q, $\left(\frac{D}{q}\right)=1$ olan bir tek asal ve e, $Q(\sqrt{D})$ cisminin ideal sınıf grubunda q nun q_i $(i=1,2)$ asal çarpanlarının mertebesi olsun. Bu durumda $x^2-Dy^2=\mp 4q^e$ Diophantine denklemi en az bir tam çözüme sahiptir.

Kanıt:

$\left(\frac{D}{q}\right)=1$ olduğundan $q=q_1.q_2$ biçiminde asal çarpanlarına ayrılır. $q_1=q$, $q^e=(w)$ ve $w=\frac{x+y\sqrt{D}}{2}$ biçiminde alındığında,

$$q^e=N(q)^e=\left|\frac{x^2-Dy^2}{4}\right|$$

olduğu görülür ve böylece $x^2-Dy^2=\mp 4q^e$ denklemi bir tam çözüme sahiptir.

2.5. Önerme

$k=Q(\sqrt{D})$ reel kuadratik sayı cisminin sınıf sayısı $h_k=m$ gibi bir tek sayı ise ve q $\left(\frac{D}{q}\right)=1$ sağlayan bir tek asal ise $q^m\geq n$ dir.

Kanıt:

$\left(\frac{D}{q}\right)=1$ olduğundan $x^2-Dy^2=\mp 4q^e$ Diophantine denkleminin aşikar olmayan en az bir tam çözümü vardır. $\left(\frac{D}{q}\right)=1$ olduğundan $q=q_1.q_2$ biçiminde asal çarpanlarına ayrılır.

$q_1=q,\ \ q^e=(w)$ ve $w=\frac{x+y\sqrt{D}}{2}$ biçiminde alındığında,

$$q^e=N(q)^e=\left|\frac{x^2-Dy^2}{4}\right|$$

olduğu görülür. Buradan $x^2-Dy^2=\mp 4q^e$ denkleminin bir çözüme sahip olduğu çıkar. $N(\varepsilon_D)=-1$ olduğundan 2.3. Lemmadan $q^e\geq\frac{t}{u^2}$ olur. $q^{h_k}\geq q^e$ olduğuna göre $q^{h_k}\geq\frac{t}{u^2}$ yazılır. u = 1 ise t = n olur ve $h_k=m$ den $q^m\geq\frac{t}{u^2}=n$ sağlanır. u=2 için t=4n dir ve $q^m\geq\frac{t}{u^2}=\frac{4n}{4}=n$ eşitsizliği de sağlanır. $u>2$ için $t=u^2n+v$ ve $0\leq w<v<u^2$ olduğu kullanılarak $q^m\geq\frac{t}{u^2}=\frac{u^2n+v}{u^2}=n+\frac{v}{u^2}$ olur. $\frac{v}{u^2}\leq 0$ olduğundan $q^m\geq n$ eşitsizliği elde edilir.

2.1. Teorem

$N(\varepsilon_D)=-1$ durumunda $1\leq u\leq 100$ için $h_k=3$ olan D nin uygun bir değeri hariç, 31 tane $k=Q(\sqrt{D})$ reel kuadratik sayı cismi vardır.

Kanıt:

2.2. Önermede verilen yöntemler m tek sayısı olarak m=3 alındığında, $n\geq v(u)$ olan n değerleri için $h_k>3$ olacağından $h_k>f(\log u,c)\geq 3$ eşitsizliğinden $c\geq 16.18007$ olduğu kullanılarak,

$$v(u) \geq \frac{\sqrt{u^2 e^c - 4}}{u^2} \geq \frac{\sqrt{u^2 e^{16.18007} - 4}}{u^2} = \sqrt{\frac{e^{16.18.007}}{u^2} - \frac{4}{u^4}}$$

ifadesinden $v(u) = \sqrt{\frac{(3261)^2}{u^2} - \frac{4}{u^4}}$ alınabilir. Öyleyse,

$$0 \leq n < v(u) = \sqrt{\frac{(3261)^2}{u^2} - \frac{4}{u^4}}$$

eşitsizliğini sağlayan n değerleri için $D = u^2 n^2 + 2vn + w$ olmak üzere, $k = Q(\sqrt{D})$ reel kuadratik sayı cisminin sınıf sayısı $h_k = 3$ olabilir.

Buna göre**;** $h_k = 3$ ise,

i) $p \equiv 1 \pmod 4$ olmak üzere, D **=** p asaldır.

ii) $\left(\frac{D}{q}\right) = 1$ olan bir q tek asal değeri için $q^3 \geq n$'dir. (2.5.Önermenin kanıtına benzer olarak elde edilir.)

iii) $0 \leq n < v(u) = \sqrt{\frac{(3261)^2}{u^2} - \frac{4}{u^4}}$

koşulları sağlandığından bu biçimdeki D değerleri bu kısmın sonunda verilmiş olan bilgisayar programı ve Y. Kida'nın UBASIC86 [10] programı kullanılarak tespit edildikten sonra $1 \leq u \leq 100$ sağlayan u değerleri için D nin uygun bir değeri hariç $h_k = 3$ sağlayan 31 tane reel kuadratik sayı cismi elde edilmiştir. Bu teoremi sağlayan u, v, w, n ve D değerleri 2.1.Tablo ile verilmektedir.

$N(\varepsilon_D) = -1$ durumunda sınıf sayısı $h_k = 3$ olan bu cisimler arasında H.Yokoi'nin [31], S-I, S-G Katayama'nın [8,9] çalışmalarında belirlediği cisimlerde bulunmaktadır. Bunlar2.1.Tabloda sırasıyla *, ● ve ▲ sembolleriyle belirtilmiştir. Tabloda, hiçbir sembolle belirtilmeyen cisimler literatürde rastlamadığımız bu yöntemle elde edilmiş yeni cisimlerdir. Ancak bunlar başka bir yöntemle önceden belirlenmiş de olabilir.

2.1.Tablo

u	v	w	n	D	
1	0	4	15	229	* ●
1	1	5	14		
1	0	4	27	733	*●
1	1	5	26		
1	0	4	35	1229	*●
1	1	5	34		
1	0	4	37	1373	*●
1	1	5	36		
1	0	4	47	2213	*●
1	1	5	46		
1	0	4	67	4493	*●
1	1	5	66		
1	0	4	73	5333	●
1	1	5	72		
1	0	4	97	9413	*●
1	1	5	96		
2	0	1	8	257	*●
2	4	5	7		
2	0	1	27	2917	*●
2	4	5	26		
2	0	1	37	5477	●
2	4	5	36		
2	0	1	47	8837	●
2	4	5	46		
5	11	5	26	17477	
5	14	8	13	4597	*
5	14	8	15	6053	
5	14	8	23	13877	
10	36	13	4	1901	*▲
10	36	13	10	10733	
10	64	41	9	9293	▲
13	140	116	5	5741	
25	261	109	4	12197	▲
29	82	8	3	8069	▲
34	76	5	2	4933	*▲
58	1600	761	0	761	
50	2136	1825	1	8597	▲
65	1661	653	2	24197	▲
65	3689	3221	0	3221	*▲
65	3689	3221	2	34877	▲
73	3777	2677	0	2677	*▲
82	5968	5297	0	5297	▲
82	5968	5297	1	23957	▲

$(h_k = 3,\ N(\varepsilon_D) = -1)$

2.2. Teorem

$N(\varepsilon_D) = -1$ durumunda $1 \le u \le 100$ için $h_k = 5$ olan, D nin uygun bir değeri hariç 23 tane $k = Q(\sqrt{D})$ reel kuadratik sayı cismi vardır.

Kanıt:

2.1 Teoreminin kanıtına benzer olarak 2.3.Önermede $m = 5$ alındığında, $n \ge v(u)$ olan n değerleri için $k = Q(\sqrt{D})$ olacağından $h_k > f(\log u, c) \ge 5$ eşitsizliğinden $c \ge 17.5201$ olduğu kullanılarak,

$$v(u) \ge \frac{\sqrt{u^2 e^c - 4}}{u^2} \ge \frac{\sqrt{u^2 e^{17.5201} - 4}}{u^2}$$

ifadesinden, $v(u)$, $v(u) = \sqrt{\frac{(6374)^2}{u^2} - \frac{4}{u^4}}$ olarak alınabilir. O halde $0 \le n \le v(u)$ eşitsizliğini sağlayan n değerleri için $D = u^2 n^2 + 2vn + w$ olmak üzere $k = Q(\sqrt{D})$ reel kuadratik sayı cisminin sınıf sayısı $h_k = 5$ olabilir.

Buna göre, $h_k = 5$ ise,

i) $p \equiv 1 \pmod 4$ asal olmak üzere, D = p dir.

ii) $\left(\frac{D}{q}\right) = 1$ olan bir q tek asal değeri için $q^5 \ge n$ dir. (2.5. Önermenin kanıtına benzer olarak elde edilir.)

iii) $0 \le n < v(u) = \sqrt{\frac{(6374)^2}{u^2} - \frac{4}{u^4}}$

koşulları sağlandığından bu biçimdeki D değerleri aynı bilgisayar programında katsayılar değiştirilmek suretiyle tespit edilmiş ve $1 \le u \le 100$ sağlayan u değerleri için D nin uygun bir değeri hariç 23 tane reel kuadratik sayı cismi elde edilmiştir. Bu teoremi gerçekleyen u, v, w, n ve D değerleri 2.2.Tablo ile verilmektedir.

$N(\varepsilon_D) = -1$ olmak üzere, sınıf sayısı $h_k = 5$ olan cisimleri belirledikten sonra bunların içinde H.Yokoi'nin [31], S-I, S-G Katayama'nın [8] ve [9]

çalışmalarındaki cisimlerin de aynen elde edildiği gözlenmiştir. Bunlar 2.2.Tabloda *, ● ve ▲ sembolleriyle belirtilmiştir. Aynen $h_k = 3$ probleminde olduğu gibi, hiçbir sembolle belirtilmemiş olan cisimler bu çalışma sonucunda belirlenmiş cisimler olup, literatürde gözlemediğimiz ancak önceden belirlenme ihtimalinin de olabileceği yeni cisimlerdir.

2.2.Tablo

u	v	w	n	D	
1	0	4	33	1093	*●
1	0	4	57	3253	*●
1	0	4	85	7229	●
1	0	4	103	10613	●
1	0	4	115	13229	●
1	0	4	137	18773	●
1	0	4	167	27893	●
1	0	4	193	37253	●
2	0	1	10	401	*●
2	0	1	33	4357	*●
2	0	1	55	12101	●
2	0	1	73	21317	●
2	0	1	103	42437	●
5	11	5	18	8501	
5	11	5	32	26309	
5	11	5	54	74093	
13	29	5	12	25037	
26	140	29	8	45533	▲
58	1600	761	3	40637	▲
61	1364	500	1	6949	▲
65	536	68	5	111053	▲
85	2236	692	3	79133	▲
97	1305	181	2	43037	▲

$(h_k = 5, N(\varepsilon_D) = -1)$

III. BÖLÜM

$p=[(2n+1)q]^2\mp 1$ İÇİN $x^2-py^2=\mp q$ DENKLEMİNİN ÇÖZÜLEBİLİRLİĞİ VE $K=Q(\sqrt{p})$ CİSMİNİN SINIF SAYISI

$K=Q(\sqrt{p})$ reel kuadratik sayı cismi h_K, K cisminin sınıf sayısı olsun. Ankeny, Chowla, Hasse $p=(2nq)^2+1$ asalı için (q: asal, n> 1), $h_K>1$ olduğunu kanıtlamışlardır ([1]). S.-D.Lang, $p=[(2n+1)q]^2+4$ asalı için (q: tek asal, $n\geq 1$) $h_K>1$ olacağını kanıtlamıştır ([12]). 1983 yılında Yokoi $p=[(2n+1)q]^2\mp 2$ asalı ve q tek asalı için $x^2-py^2=\mp q$ diophantine denkleminin çözümüne bağlı olarak $K=Q(\sqrt{p})$ cisminin sınıf sayısını veren bazı kriterler elde etmiştir ([37]).

Bu bölümde, Yokoi'nin bu çalışmasından ve yukarıdaki çalışmalardan faydalanılarak, $n\geq 0$ ve q tamsayılar olmak üzere $p=[(2n+1)q]^2\mp 1$ kare çarpansız tamsayı için $x^2-py^2=\mp q$ denkleminin çözülebilirliği incelenerek elde edilen kriterler yardımıyla $K=Q(\sqrt{p})$ cisminin sınıf sayısının 1 olması için bir teorem verilecektir.

3.1. Tanım

D>1 kare-çarpansız tamsayısı ve m>1 tamsayısı için $m=s^2$ ve $x_o\equiv y_o\equiv 0 \pmod{s}$ ise (x_o,y_o) a $x^2-Dy^2\equiv\mp 4m$ diophantine denkleminin "aşikar tam çözümü" denir. Denklemin bu çözümünden farklı çözümleri "aşikar olmayan tam çözümler" olarak adlandırılır.

3.1. Teorem

p ve q farklı tek asallar olsun. Bu durumda $x^2 - py^2 = \mp q$ diophantine denkleminin tamsayılarda en az bir çözümünün olması için gerek ve yeter koşul q nun $Q(\sqrt{p})$ cisminde $q = q.q'$ ($q \neq q'$, $Nq = Nq' = q$, $q = (w)$, $q' = (w')$) biçiminde esas asal ideallere ayrışmasıdır. Burada $w, w' \in Q(\sqrt{p})$ dir

Kanıt:

Yokoi'nin [37] çalışmasından yararlanılarak yapılacaktır. $x^2 - py^2 = \mp q$ denkleminin tamsayılarda bir (u,v) çözümü varsa, $u^2 - pv^2 = \mp q$ ifadesinden $u^2 \equiv pv^2 \pmod{q}$ sağlanır. Buradan $\left(\frac{pv^2}{q}\right) = \left(\frac{p}{q}\right) = 1$ elde edilir. Kuadratik cisimlerdeki parçalanma kurallarından q, $Q(\sqrt{p})$ de tamamen parçalanır. Bu parçalanış;

$$\mp q = (u + v\sqrt{p})(u - v\sqrt{p})$$

biçimindedir. Burada

$$q = (u + v\sqrt{p}) \quad \text{ve} \quad q' = (u - v\sqrt{p})$$

$Q(\sqrt{p})$ cisminde birinci dereceden esas asal ideallerdir. Ayrıca $Nq = q.q' = q$ eşitliği sağlanır.

Tersine, q, $Q(\sqrt{p})$ cisminde q ve q' gibi esas ideallere ayrışıyorsa, $w = u + v\sqrt{p}$, $w' = u - v\sqrt{p}$ olacak biçimde u, v rasyonel tamsayıları vardır. $w, w' \in Q(\sqrt{p})$ olmak üzere, $q = (w)$ ve $q' = (w')$ olacaktır. Böylece,

$$q = q.q' = Nq = |N(w)| = |u^2 - pv^2|$$

eşitliğinden $x^2 - py^2 = \mp q$ denkleminin tamsayılarda en az bir çözüme sahip olduğu görülür.

3.1. Lemma

ℓ, m pozitif tamsayılar ve m tamkare olmasın. Bu durumda $m \geq 2\ell$ olmadıkça $u^2 - (\ell^2 + 1)v^2 = \mp m$ denkleminin tamsayılarda çözümü yoktur ([12]).

3.1. Önerme

p kare çarpansız bir tamsayı ve q, $p = [(2n+1)q]^2 - 1$ $(n \geq 0)$ sağlayan bir çift tamsayı olsun. Bu durumda, $x^2 - py^2 = \mp q$ denkleminin en az bir çözüme sahip olması için gerek ve yeter koşul p = 3 olmasıdır.

Kanıt:

$p = [(2n+1)q]^2 - 1$ kare çarpansız tamsayısı için, q, bir tek tamsayı ise $p \equiv 0 \pmod 4$ olacağından bu p nin seçimiyle çelişir. q bir çift tamsayı ise $p \equiv 3 \pmod 4$ olur. Özel olarak, p asal bir sayı ise, $\ell = (2n+1)q$ alındığında, $p = \ell^2 - 1 = (\ell - 1)(\ell + 1)$ olur. p asal olduğundan, $\ell - 1 = 1$, $\ell + 1 = p$ ifadelerinden $p = 3$ ve $\ell = 2$ bulunur. Bu da $q = 2$ olmasıdır.

$p = [(2n+1)q]^2 - 1$ kare çarpansız tamsayısı ve q çift tamsayısı için $x^2 - py^2 = q$ denklemini gözönüne alarak, tamsayılarda bir en küçük $(x,y) = (u,v)$ çözümünün varolduğunu varsayalım. Bu durumda, $u^2 - pv^2 = q$ olacaktır.

$q > v^2$ ise;

$q = u^2 - \ell^2 v^2 + v^2$ ifadesinden $q - v^2 = (u - \ell v)(u + \ell v) > 0$ olur. $a = u - \ell v$, $b = u + \ell v$ pozitif tamsayılardır. Bu tamsayılar kullanılarak elde edilen $\ell = \dfrac{b-a}{2v}$, $q = ab + v^2$ ifadeleri ve $(a-1)(b+1) = ab + a - b - 1 \geq 0$, $ab - 1 \geq b - a$ eşitsizliğinden,

$$\leq \frac{1}{2v}(ab-1-2vab-2v^3)$$

$$\leq -\frac{1}{2v}((2v^3+1)+(2v-1)ab)<0$$

bulunur. Bu da çelişkidir.

$q \leq v^2$ durumunda, $Q(\sqrt{p})$ nin temel birimi $\varepsilon = \ell + \sqrt{\ell^2-1}$ in normu $1= N(\varepsilon) = N(\ell+\sqrt{\ell^2-1}) = 1$, $q = N(u - v\sqrt{\ell^2-1}) = u^2 - pv^2$ ile çarpıldığında,

$$q = N((\ell u - v\sqrt{\ell^2-1}) + u\sqrt{\ell^2-1} - v(\ell^2-1))$$

$$q = (\ell u - v\sqrt{\ell^2-1})^2 - (u-\ell v)^2(\ell^2-1)$$

elde edilir.

v nin minimal seçiminden $|u-\ell v| \geq v$ olacağından $u-\ell v \geq v$ yada $\ell v - u \geq v$ olur.

$u-\ell v \geq v$ ise $u \geq (\ell+1)v$ olduğu kullanılarak,

$$q = u^2 - (\ell^2-1)v^2 \geq (\ell+1)^2 v^2 - (\ell^2-1)v^2 = (2\ell+2)v^2$$

$q \geq (2\ell+2)v^2$ eşitsizliği elde edilir ki bu $q \leq v^2$ seçimiyle çelişir.

$\ell v - u \geq v$ iken $(\ell-1)v \geq u$ olacağından,

$$q = u^2 - (\ell^2-1)v^2 \leq (\ell-1)^2 v^2 - (\ell^2-1)v^2 = (2-2\ell)v^2 = -2v^2(\ell-1) < 0$$

bulunur. $\ell \geq 1$ için $q \leq -2v^2(2\ell-1)$ eşitsizliği de $q \leq v^2$ ile çelişir. O halde $x^2 - py^2 = q$ denkleminin tamsayılarda çözümü yoktur.

$x^2 - py^2 = -q$ denklemi alınarak tamsayılardaki en küçük çözümünün $(x,y) = (u,v)$ olduğu varsayılırsa, $u^2 - pv^2 = -q$ olur. Burada $v=1$ ise $u^2 - (\ell^2-1)v^2 = u^2 - \ell^2 + 1 = -q$ iken $u^2 - \ell^2 = -q-1$ bulunur. q en küçük çift tamsayı olarak yani; $q=2$ alındığında, $u^2 - \ell^2 = -3 \Rightarrow (u-\ell)(u+\ell) = -3$ olur. $u+\ell = 3$, $u-\ell = -1$ eşitliklerinden $u=1$, $\ell = 2$ ve $p=3$ bulunur. Bu da önermenin ifadesindeki uygun durumdur.

$q = 2,\ v > 1$ ve $q > 2,\ v \geq q$ durumlarında $Q(\sqrt{p})$ nin temel biriminin normu, $-q = N(u - v\sqrt{\ell^2 - 1}) = u^2 - pv^2$ ile çarpıldığında v nin minimal seçimi ile, $|\ell v - u| \geq v$ elde edilir. $\ell v - u \geq v$ iken $(\ell - 1)v \geq u$ olduğu kullanılarak,

$$\begin{aligned} -q = u^2 - (\ell^2 - 1)v^2 &\leq (\ell - 1)^2 v^2 - (\ell^2 - 1)v^2 \\ &= 2v^2(1 - \ell) \\ &= -2v^2(\ell - 1) \end{aligned}$$

bulunur. Buradan, $q \geq 2v^2(\ell - 1)$ olur. Bu ise her iki durumla da çelişir.

$u - \ell v \geq v$ iken $u \geq v(\ell + 1)$ olduğu kullanılarak,

$$-q = u^2 - (\ell^2 - 1)v^2 \geq (\ell + 1)^2 v^2 - (\ell^2 - 1)v^2 = v^2(2\ell + 2)$$

eşitsizliği elde edilir. Bu da bir çelişkidir.

q>2 , v<q olsun.

$-q = u^2 - (\ell^2 - 1)v^2 = u^2 - \ell^2 v^2 + v^2 \Rightarrow q + v^2 = (\ell v - u)(\ell v + u) > 0$ ve $\ell v - u = a$, $\ell v + u = b$ pozitif tamsayılardır. Bu ifadelerden $\ell = \frac{a+b}{2v}$, $q = ab - v^2$ sağlanır. $a \geq 1, b \geq 1$ iken $ab + 1 \leq a + b$ olduğunu kullanılarak;

$$\begin{aligned} 0 \leq 2nq = \ell - q = \frac{a+b}{2v} - ab + v^2 &= \frac{1}{2v}(a + b - 2vab + 2v^3) \\ &\leq \frac{1}{2v}(ab + 1 - 2vab + 2v^3) \\ &= \frac{1}{2v}((2v^3 + 1) - (2v - 1)ab) \end{aligned}$$

elde edilir.

Buradan da $ab \leq \frac{2v^3 + 1}{2v - 1}$ eşitsizliği gerçeklenir ve

$$q = ab - v^2 \le \frac{2v^3+1}{2v-1} - v^2 = \frac{v^2+1}{2v-1} = \frac{v}{2} + \frac{v+2}{2(2v-1)}$$

bulunur.

Eğer v=1 yada v=2 ise $q \le \frac{5}{3}$ olur. Bu ise bir çelişkidir. v>2 olması durumunda $0 \le \frac{v+2}{2v-1} \le 1$ eşitsizliğinden $2q = v + \frac{v+2}{2v-1} \le v+1$ yani, $q \le \frac{v+1}{2}$ olur ki bu da q>v olması ile çelişir.

O halde $x^2 - py^2 = \mp q$ denkleminin q = 2 ve p = 3 durumunun dışında tamsayılarda bir çözümü yoktur.

3.2. Önerme

p kare çarpansız bir tamsayı, $n \ge 0$ olmak üzere, q, $p = [(2n+1)q]^2 + 1$ sağlayan pozitif bir tamsayı olsun. Bu durumda $x^2 - py^2 = \mp q$ denkleminin tamsayılarda bir (x,y)=(u,v) çözümü varsa, $q \le v^2$ sağlanır.

Kanıt:

$p = [(2n+1)q]^2 + 1$ kare-çarpansız tamsayısı için eğer, q bir tek tamsayı ise $p \equiv 2 (\mathrm{mod}\, 4)$, q çift tamsayı ise $p \equiv 1 (\mathrm{mod}\, 4)$ olacaktır.

$x^2 - py^2 = \mp q$ denkleminin çözümü için, $q \ne a^2$ $(\forall a \in Z^+)$ alınırsa, 3.1. Lemmadan $q \ge 2(2n+1)q$ çelişkisi ortaya çıkar. Bu durumda denklemin aşikar olmayan tam çözümünün olmadığı açıktır. Öyleyse, $q = a^2$ olması durumunda çözüm aranabilir.

$p = [(2n+1)q]^2 + 1$ kare-çarpansız tamsayısında $\ell = (2n+1)q$ alınırsa, $p = \ell^2 + 1$ olur.

Öncelikle, $x^2 - py^2 = q$ denkleminin tamsayılarda en az bir $(x,y) = (u,v)$ çözümünün olduğu varsayılırsa, $u^2 - pv^2 = q$ elde edilir.

$q > v^2$ ise;

$q = u^2 - (\ell^2 + 1)v^2 = u^2 - \ell^2 v^2 - v^2 \Rightarrow q + v^2 = (u - \ell v)(u + \ell v) > 0$ ve $u - \ell v = a$, $u + \ell v = b$ pozitif tamsayılardır. Bu ifadelerden $\ell = \frac{b-a}{2v}$, $q = ab - v^2$ sağlanır. $b - a \le ab - 1$ olduğunu kullanarak;

$$0 \le 2nq = \ell - q = \frac{b-a}{2v} - ab + v^2 = \frac{1}{2v}(b - a - 2vab + 2v^3)$$

$$\le \frac{1}{2v}(ab - 1 - 2vab + 2v^3)$$

$$= \frac{1}{2v}((2v^3 - 1) - (2v - 1)ab)$$

bulunur.

Buradan da $ab \le \frac{2v^3 - 1}{2v - 1}$ eşitsizliği gerçeklenir.

$q = ab - v^2 \le \frac{2v^3 - 1}{2v - 1} - v^2 = \frac{v}{2} + \frac{v - 2}{2(v - 1)} \le \frac{v + 1}{2}$ eşitsizliğinden

$q \le \frac{v+1}{2}$ çıkar, bu da $q > v^2$ seçimiyle çelişir.

$q \le v^2$ durumunda $Q(\sqrt{p})$ nin temel birimi ε nun normu, $N(\varepsilon) = N(\ell + \sqrt{\ell^2 + 1}) = -1$ ifadesinin karesi, $q = N(u - v\sqrt{\ell^2 + 1})$ ile çarpılırsa,

$$q = N(u - v\sqrt{\ell^2 + 1}).N(2\ell^2 + 1 + 2\ell\sqrt{\ell^2 + 1})$$

$$= (u^2 + 2u\ell^2 - 2\ell v(\ell^2 + 1))^2 - (2\ell^2 v - 2u\ell - v)^2(\ell^2 + 1)$$

eşitliği elde edilir. v nin minimal seçiminden,

$$\left| 2\ell^2 v - 2u\ell - v \right| \ge v$$

dir. Buradan,

$2\ell^2 v - 2u\ell - v \ge 0$ ise $2\ell^2 v - 2u\ell - v \ge v$

ya da

$2\ell^2 v - 2u\ell - v < 0$ ise $2u\ell + v - 2\ell^2 v \ge v$

yazılabilir.

$$2\ell^2 v - 2u\ell - v \geq v \quad \text{ise} \quad u\ell \leq v(\ell^2 - 1)$$

olur. Buradan

$$q = u^2 - (\ell^2+1)v^2 \;\Rightarrow\; \ell^2 q = \ell^2 u^2 - (\ell^2+1)v^2 \leq v^2(\ell^2-1)^2 - (\ell^2+1)v^2\ell^2$$
$$= v^2(1-3\ell^2)$$

bulunur.

$\ell \geq 1$ iken $1-3\ell^2 < 0$ olur ki bu bir çelişkidir.

$2u\ell + v - 2\ell^2 v \geq v$ ise $u \geq \ell v$ olur. Buradan,

$$q = u^2 - (\ell^2+1)v^2 \;\geq\; \ell^2 v^2 - (\ell^2+1)v^2 = -v^2$$

yani, $q \geq -v^2$ eşitsizliği elde edilir. Bu eşitsizlik ise tüm q ve v değerleri için doğrudur.

Şimdi de $x^2 - py^2 = -q$ denklemi alınarak tamsayılarda en az bir $(x,y) = (u,v)$ çözümüne sahip olduğu varsayıldığında;

$q > v^2$ durumunda,

$$-q = u^2 - (\ell^2+1)v^2 \;\Rightarrow\; q - v^2 = \ell^2 v^2 - u^2 = (\ell v - u)(\ell v + u) > 0$$

sağlanır. Burada $a = \ell v - u > 0,\ b = \ell v + u > 0$ rasyonel tamsayılardır. a ile b ifadelerinden $\ell = \dfrac{b+a}{2v}$, $q = ab + v^2$ ve $a + b \leq ab + 1$ olduğu kullanılarak,

$$0 \leq 2nq = \ell - q = -\frac{1}{2v^2}((2v^3 - 1) + (2v-1)ab) < 0$$

bulunur ki bu da çelişkidir.

$q = v^2$ alınırsa, 3.1.Tanımdan $u \equiv v \equiv 0 \pmod{v}$ olacağından $x^2 - py^2 = \mp q$ denkleminin aşikar bir tam çözümü vardır.

$q < v^2$ durumunda,

$$N(\ell + \sqrt{\ell^2+1}) = N(\varepsilon) = -1$$

normunun karesi ile

$$N(u + v\sqrt{\ell^2+1}) = -q$$

normu çarpıldığında,

$$-q = (u + 2u\ell^2 - 2\ell v(\ell^2 + 1))^2 - (2\ell^2 v - 2u\ell - v)^2(\ell^2 + 1)$$

bulunur.

v nin minimal seçiminden, $\left|2\ell^2 v - 2u\ell - v\right| \geq v$ dir.

$2\ell^2 v - 2u\ell - v \geq v$ ise $u\ell \leq v(\ell^2 - 1)$ ve buradan $-\ell^2 q \leq v^2(1 - 3\ell^2)$ ya da $\ell^2 q \geq v^2(3\ell^2 - 1)$ sağlanır. $\ell \geq 1$ durumunda $q \geq 2v^2$ eşitsizliği elde edilir. Bu da $q < v^2$ seçimiyle çelişir. Eğer $-2\ell^2 v + 2u\ell + v \geq v$ ise $u \geq \ell v$ olur ve $-q = u^2 - (\ell^2 + 1)v^2 \geq -v^2$ eşitsizliğinden $q \leq v^2$ olur ki bu da varsayılan durumdur. Öyleyse, $p = [(2n+1)q]^2 + 1$ kare çarpansız tamsayısı için $q \leq v^2$ durumunda $x^2 - py^2 = \mp q$ deklemi tamsayılarda bir çözüme sahip olabilir.

3.1.Sonuç

$p = [(2n+1)q]^2 + 1$ kare çarpansız tamsayısı için $x^2 - py^2 = \mp q$ denkleminin $q \leq v^2$ olmadıkça tamsayılarda çözümü yoktur.

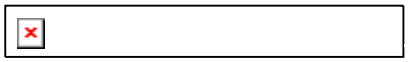
3.2. Teorem

i) $p = [(2n+1)q]^2 - 1$ $(n \geq 0)$ kare çarpansız bir tamsayı ve q=2 ise p=3 dışında $Q(\sqrt{p})$ reel kuadratik sayı cisminin sınıf sayısı $h_K > 1$ dir.

ii) $p = [(2n+1)q]^2 + 1$, $(n \geq 0)$ kare çarpansız tamsayı ve q, $q \equiv 1 (\mathrm{mod}\, 4)$ sağlayan bir tek asal olsun. Bu durumda, $Q(\sqrt{p})$ cisminin sınıf sayısı $h_K > 1$ dir.

Kanıt

i) $p = [(2n+1)q]^2 - 1$ kare çarpansız tamsayısı ve q=2 için $p \equiv 3 (\mathrm{mod}\, 4)$ olacağı açıktır. Böylece q=2 tamsayısı $Q(\sqrt{p})$ cisminde dallanır. Bu durumda $h_K = 1$ olduğu varsayıldığında, $\pm 2 = u^2 - pv^2$ olacak biçimde u ile v rasyonel tamsayıları vardır. p nin seçiminden,



(u,v)

$x^2 - py^2 = \mp q$ $(x,y) = (u,v)$

$h_K = 1$ $h_K > 1$

ii) $p = [(2n+1)q]^2 + 1$ den $p \equiv 1 \pmod{q}$ olur. Buradan $q \equiv 1 \pmod{4}$ asalı için $\left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1$ sağlanır. Bu ise q nun $Q(\sqrt{p})$ cisminde ω ve ω' gibi esas divizörlere ayrışmasıdır. Böylece onun normu,

$$\Re(\omega) = q$$

dur.

$h_K = 1$ olduğu varsayılsın. Böylece ω esas divizörü,

$$\omega \cong w = u + v\sqrt{p} \quad (u, v \in Z)$$

olarak yazıldığında,

$$\Re(\omega) = |N(w)| = \left|N(u + v\sqrt{p})\right|$$

eşitliğinden $u^2 - pv^2 = \mp q$ elde edilir. Bu da $x^2 - py^2 = \mp q$ denkleminin tamsayılarda bir (x,y) = (u,v) çözümünün olmasıdır. Bu ise hem 3.1. Lemmadan $q \geq 2(2n+1)q$ çelişkisini ortaya çıkardığından hem de 3.1. Önermedeki $q \leq v^2$ olması halinde bir tamsayı çözümünün varolabilceği durumu ile çelişeceğinden $h_K > 1$ dir.