KUADRATİK FORMLAR VE DİOPHANTİNE DENKLEMLERİ

Hatice ALKAN

T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KUADRATİK FORMLAR VE DİOPHANTİNE DENKLEMLERİ

Hatice ALKAN

Doç. Dr. Ahmet TEKCAN
(Danışman)

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

BURSA – 2011

TEZ ONAYI

Hatice ALKAN tarafından hazırlanan "Kuadratik Formlar ve Diophantine Denklemleri" adlı tez çalışması aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Uludağ Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

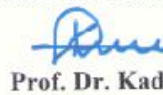
Danışman : Doç. Dr. Ahmet TEKCAN

Başkan :Prof. Dr. Osman BİZİM
Uludağ Üniversitesi,
Fen-Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye :Doç. Dr. Ahmet TEKCAN
Uludağ Üniversitesi,
Fen-Edebiyat Fakültesi,
Matematik Anabilim Dalı

Üye :Doç. Dr. İlhan TAPAN
Uludağ Üniversitesi,
Fen-Edebiyat Fakültesi,
Fizik Anabilim Dalı

Yukarıdaki sonucu onaylarım



Prof. Dr. Kadri ASLAN

Enstitü Müdürü

15.../08/.../2011

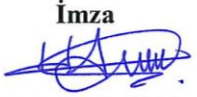
U.Ü. Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

22./07./2011

İmza



Hatice ALKAN

ÖZET

Yüksek Lisans Tezi

KAUDRATİK FORMLAR VE DİOPHANTİNE DENKLEMLERİ

Hatice ALKAN

Uludağ Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Doç. Dr. Ahmet TEKCAN

Bu tezde kuadratik formlar ve Diophantine denklemleri ele alınmış ve bunlar ile ilgili bazı cebirsel özellikler elde edilmiştir.

Bu tez beş bölümden oluşmaktadır. Birinci bölümde çalışma ile ilgili temel tanım ve teoremlere yer verilmiştir.

İkinci bölümde, sonlu cisimler üzerinde tanımlı özel eğriler ele alınmış ve bunlar üzerindeki rasyonel noktaların sayısı sonlu Φ_p cisimlerinde ele alınmıştır.

Üçüncü bölümde, $y^2 - 2yx - 3 = 0$ Diophantine denkleminin tamsayı çözümleri tamsayılarda ve sonlu Φ_p cisminde ele alınmıştır. Daha sonra bu Diophantine denkleminin köklerine bağlı olarak tanımlanan eğri üzerindeki rasyonel noktaların sayısı sonlu Φ_p cisminde belirlenmiştir.

Dördüncü bölümde, kuadratik idealler ve indefinite kuadratik formlar ele alınmıştır. Bu bölümde iki özel kuadratik ideal ele alınmış ve bu ideallerin özellikleri verildikten sonra bu ideallerin çarpımları oluşturulmuştur. Daha sonra bu kuadratik ideallere karşılık gelen indefinite kuadratik formlar ele alınmıştır.

Beşinci bölümde, özel bir tamsayı dizisi verilmiş ve bu dizinin parametrelerine bağlı olarak tanımlanan Pell denkleminin tamsayı çözümleri ve bu çözümlerle ilgili indirgeme bağıntıları elde edilmiştir.

Anahtar Kelimeler: Kuadratik formlar, Kuadratik idealler, Diophantine ve Pell denklemleri, Tamsayı dizileri

2011, vi + 68 sayfa.

ABSTRACT

MSc Thesis

QUADRATIC FORMS AND DIOPHANTINE EQUATIONS

Hatice ALKAN

Uludağ University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Assoc. Prof. Dr. Ahmet TEKCAN

In this thesis, some algebraic properties of binary quadratic forms and Diophantine equations are given.

The thesis consists of five chapters. In the first chapter, the preliminary notations, definitions and theorems which are to be used in later chapters are given.

In the second chapter, the number of rational points on some specific curves is formulated over finite fields Φ_p.

In the third chapter, the integer solutions of Diophantine equation $y^2 - 2yx - 3 = 0$ are considered both over integers and over finite fields Φ_p. Later the number of rational points on curves related to roots of $y^2 - 2yx - 3 = 0$ are determined over Φ_p.

In the fourth chapter, quadratic ideals and indefinite binary quadratic forms are considered. Here two specific kuadratik ideal are considered and derived some properties of them. Later their product is obtained. Finally, some properties of indefinite binary quadratic forms related to these ideals are obtained.

In the last chapter, some properties of a specific integer sequence are given and later integer solutions of a Pell equation related to parameters of this integer sequence are formulated. Also some recurrence relations on this integer sequence are given.

Key words: Quadratic forms, Quadratic ideals, Diophantine and Pell equations, Integers sequences.

2011, vi + 68 pages.

TEŞEKKÜR

Yüksek Lisans tez çalışmam boyunca bilgisiyle ve tecrubesiyle bana her zaman destek olan kıymetli hocam Doç. Dr. Ahmet TEKCAN' a içtenlikle teşekkür ederim.

Tez çalışması ve yazımı konusunda yardımlarını esirgemeyen Arzu ÖZKOÇ' a teşekkür ederim.

İÇİNDEKİLER

SİMGELER DİZİNİ

$F = (a, b, c)$	kuadratik form
$\Delta(F) = b^2 - 4ac$	kuadratik formun determinantı
$M = M(F)$	kuadratik formun matrisi
λ_1, λ_2	kuadratik formun özdeğerleri
$z = z(F)$	kuadratik formun taban noktası
Γ	Modüler grup
$\overline{\Gamma}$	Genişletilmiş modüler grup
gF	F formunun $g \in \overline{\Gamma}$ dönüşümü altındaki resmi
$\wp(\tau; F)$	F formuna karşılık gelen teta serisi
$r(n; F)$	n tamsayısının F formu ile gösterilme sayısı
$F_0 \sim F_1 \sim F_2 \sim \cdots \sim F_{l-1}$	F formunun devri veya has devri
γ	kuadratik irrasyonel
$I_\gamma = [Q, P + \delta]$	kuadratik ideal
$F_\gamma = Q(X + \gamma Y)(X + \bar{\gamma} Y)$	indefinite kuadratik form
$I_{\gamma_0} \sim I_{\gamma_1} \sim I_{\gamma_2} \sim \cdots \sim I_{\gamma_{l-1}}$	I_γ idealinin devri
$[m_0; \overline{m_1, m_2, \cdots, m_{l-1}}]$	γ nın sürekli kesirli açılımı
$ax + by = c$	birinci dereceden Diophantine denklemi
$ax^2 + bxy + cy^2 + dx + ey + f = 0$	ikinci dereceden Diophantine denklemi
$x^2 - dy^2 = \pm N$	Pell denklemi
Φ_p	sonlu cisim
Q_p	ikinci dereceden kalanların kümesi
$\left(\frac{a}{p}\right)$	Legendre sembolü
E_p	özel eğri
$K = \Theta(\sqrt{\Delta})$	kuadratik sayı cismi

ŞEKİL VE TABLOLAR DİZİNİ

1. GİRİŞ

Bu bölümde, tezin sonraki bölümlerinde kullanılacak olan bazı temel kavramlara, teoremlere ve notasyonlara yer verilmiştir.

1.1 Tanım. $a,b,c \in \mathrm{P}$ olmak üzere

$$aX^2 + bXY + cY^2$$

şeklindeki polinomlara kuadratik (ikinci dereceden) form denir ve bu form kısaca katsayılar yardımıyla $F = (a, b, c)$ ile gösterilir. Bu formun determinantı $\Delta(F)$ ile gösterilir ve

$$\Delta(F) = b^2 - 4ac$$

olarak tanımlanır. Üstelik $F = (a, b, c)$ formu için

i) "F tamdır $\Leftrightarrow a,b,c \in \mathrm{Z}$ dir. "

ii) "F pozitif tanımlıdır $\Leftrightarrow \Delta(F) < 0,\ a,c > 0$ dır".

iii) "F indefinitedir $\Leftrightarrow \Delta(F) > 0$ dır".

iv) "F ilkeldir $\Leftrightarrow obeb(a,b,c) = 1$ dir".

Bu formun matrisi $M = M(F)$ ile gösterilir ve

$$M(F) = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

olarak tanımlanır. Bu matrisin izi ve determinantı sırasıyla

$$tr(M(F)) = a + c \quad \text{ve} \quad |M(F)| = ac - \frac{b^2}{4}$$

dür. Üstelik F formu, bu matris yardımıyla

$$F(X,Y) = aX^2 + bXY + cY^2 = [X \quad Y]\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\begin{bmatrix} X \\ Y \end{bmatrix}$$

olarak yeniden ifade edilebilir. Üstelik F nin determinantı matris yardımıyla

$$\Delta(F) = -4\det(M(F))$$

olarak verilebilir.

F formunun özdeğerleri, F nin matrisinin özdeğerleri olarak tanımlanır. Dolayısıyla F nin özdeğerleri

$$|M(F)-\lambda I_2|=0$$

denkleminin kökleridir. Buna göre

$$M(F)-\lambda I_2=\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}-\lambda\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}=\begin{bmatrix} a-\lambda & b/2 \\ b/2 & c-\lambda \end{bmatrix}$$

olup buradan

$$\begin{vmatrix} a-\lambda & b/2 \\ b/2 & c-\lambda \end{vmatrix}=(a-\lambda)(c-\lambda)-\frac{b^2}{4}=0$$

elde edilir. Bu son denklem λ ya göre çözülürse F nin özdeğerleri

$$\lambda_1=\frac{a+c+\sqrt{a^2+b^2+c^2-2ac}}{2} \quad \text{ve} \quad \lambda_2=\frac{a+c-\sqrt{a^2+b^2+c^2-2ac}}{2}$$

olarak bulunur. Bu son denklemde karekök içerisinde gerekli düzenlemeler yapılırsa

$$\begin{aligned} a^2+b^2+c^2-2ac &= a^2+b^2+c^2-4ac+2ac \\ &= b^2-4ac+a^2+c^2+2ac \\ &= b^2-4ac+(a+c)^2 \\ &= \Delta+tr^2(M(F)) \end{aligned}$$

olduğundan F nin özdeğerleri

$$\lambda_1=\frac{tr(M(F))+\sqrt{\Delta+tr^2(M(F))}}{2} \quad \text{ve} \quad \lambda_2=\frac{tr(M(F))-\sqrt{\Delta+tr^2(M(F))}}{2}$$

olarak elde edilir.

Kuadratik formların bir çok cebirsel özelliği (denkliği, indirgenebilirliği, devri, has devri, sağ ve sol komşuları) modüler veya genişletilmiş modüler grup yardımıyla verilir ki bu gruplar aşağıdaki tanımda verilmiştir.

1.2 Tanım. $r,s,t,u \in Z$ olmak üzere

$$z \to \frac{rz+s}{tz+u},\ ru-st=1$$

şeklindeki dönüşümler bileşke işlemine göre bir grup oluştururlar. Bu gruba modüler grup denir ve Γ ile gösterilir. O halde

$$\Gamma = \left\{ \frac{rz+s}{tz+u} :\ r,s,t,u \in \mathrm{Z},\ ru-st=1 \right\}$$

dır. Bu grup PSL$(2,\mathrm{Z})$ ile de gösterilir. $R(z) = -\bar{z}$ dönüşümü sanal eksene göre yansıma dönüşümü olmak üzere $\Gamma \cup R\Gamma$ da bir grup olup bu gruba da genişletilmiş modüler grup denir ve bu grup $\bar{\Gamma}$ ile gösterilir.

Formların bir çok önemli özelliğinin modüler veya genişletilmiş modüler grup yardımıyla verilebileceği belirtilmişti. Bu nedenle ilk olarak bir formun modüler veya genişletilmiş modüler grubun elemanı altındaki resmi verilsin: $F = (a,b,c)$ herhangi bir form ve $g = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in \bar{\Gamma}$ dönüşümü için F nin g altındaki gF resmi

$$gF(X,Y) = (ar^2 + brs + cs^2)X^2 + (2art + bru + bts + 2csu)XY + (at^2 + btu + cu^2)Y^2$$

olarak tanımlanır.

1.3 Uyarı 1. Yukarıdaki tanıma dikkat edilirse gF de ikinci dereceden bir formdur. Üstelik gF formu, F formunda $X \to rX + tY$, $Y \to sX + uY$ değişken değişimi yapılarak elde edilmiştir, yani

$$gF = F(rX + tY, sX + uY)$$

dir.

2. Bu tanıma göre F ile gF aynı özelliklere sahiptirler, yani F pozitif tanımlı, indefinite veya ilkel ise gF de pozitif tanımlı, indefinite veya ilkeldir. Üstelik F ile gF aynı determinantlıdır, yani $\Delta(F) = \Delta(gF)$ dir.

3. gF nin bu şekildeki tanımı genişletilmiş modüler grubun formlar kümesi üzerinde bir grup etkisidir, yani her $g,h \in \bar{\Gamma}$ için $g(hF) = (gh)F$ ve $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} F = F$ dir.

1.4 Tanım. F ve G herhangi iki kuadratik form olsun. Eğer $gF = G$ olacak şekilde en az bir $g \in \overline{\Gamma}$ varsa F ve G formlarına denktir denir. Eğer $\det(g) = 1$ ise bu formlara has denk, $\det(g) = -1$ ise bu formlara has olmayan denk formlar denir.

1.5 Örnek 1. $F = (1, 7, -6)$ ve $G = (2, 7, -3)$ kuadratik formları ve $g = \begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix}$ dönüşümü için

$$\begin{aligned} gF &= F(X + 3Y, X + 4Y) \\ &= (X + 3Y)^2 + 7(X + 3Y)(X + 4Y) - 6(X + 4Y)^2 \\ &= 2X^2 + 7XY - 3Y^2 \\ &= G \end{aligned}$$

dir. Diğer yandan $\det(g) = 1$ olduğundan bu iki form birbirine has denktir.

2. $F = (7, -2, 1)$ ve $G = (1, 0, 6)$ kuadratik formları ve $g = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ dönüşümü için

$$\begin{aligned} gF &= F(Y,\ X + Y) \\ &= 7(Y)^2 - 2(Y)(X + Y) + (X + Y)^2 \\ &= X^2 + 6Y^2 \\ &= G \end{aligned}$$

ve $\det(g) = -1$ olduğundan bu iki form birbirine has olmayan denktir.

1.6 Uyarı. Denk formlar aynı determinantı iken, aynı determinantlı formların denk olması gerekmez. Örneğin $F = (8, -2, 1)$ ve $G = (1, 0, 7)$ kuadratik formları denk olup determinantları -28 dir. Ancak 8 determinantlı F = (1, 4, 2) ve G = (1, 2, -1) formları denk değildir.

1.7 Tanım. $F = (a, b, c)$ pozitif tanımlı formu için

$$|b| \leq a \leq c$$

şartı sağlanıyor ise bu forma indirgenebilirdir denir. F indefinite formu için

$$|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$$

şartı sağlanıyor ise F ye indirgenebilir form denir.

Eğer bir F formu indirgenebilir değilse bu form aşağıdaki indirgeme algoritması kullanılarak indirgenebilir hale getirilebilir.

1.8 Teorem (Buchmann ve Vollmer 2007). $F=(a,b,c)$ pozitif tanımlı formu indirgenebilir olmasın. Bu takdirde $i \geq 0$ için

$$r_i = \left\lfloor \frac{b_i + c_i}{2c_i} \right\rfloor$$

olmak üzere

$$\rho^{i+1}(F) = (c_i, -b_i + 2c_i r_i, c_i r_i^2 - b_i r_i + a_i)$$

tanımlanırsa F nin indirgenmişi $\rho^{i+1}(F)$ dir.

1.9 Örnek. -3 determinantlı $F=(195751,\ 37615,\ 1807)$ pozitif tanımlı formu indirgenebilir değildir. Bu forma yukarıdaki indirgeneme algoritması uygulanırsa aşağıdaki tablo elde edilir:

Tablo 1.1 $F=(195751,\ 37615,\ 1807)$ nin indirgenmişi

i	0	1	2	3	4	5
a_i	195751	1807	301	61	3	1
b_i	37615	-1475	271	-27	3	1
c_i	1807	301	61	3	1	1
r_i	10	-2	2	-4	2	

Bu tabloya göre F nin indirgenmişi $\rho^5(F)=(1,1,1)$ formudur.

1.10 Teorem (Buchmann ve Vollmer 2007). $F=(a,b,c)$ indefinite formu indirgenebilir olmasın. Bu takdirde $i \geq 0$ için

$$r_i = \begin{cases} \operatorname{sgn}(c_i)\left\lfloor \dfrac{b_i}{2\,|c_i|} \right\rfloor & |c_i| \geq \sqrt{\Delta} \\ \operatorname{sgn}(c_i)\left\lfloor \dfrac{b_i + \sqrt{\Delta}}{2\,|c_i|} \right\rfloor & |c_i| < \sqrt{\Delta} \end{cases}$$

olmak üzere F nin indirgenmişi

$$\rho^{i+1}(F) = (c_i, -b_i + 2c_i r_i, c_i r_i^2 - b_i r_i + a_i)$$

dir.

1.11 Örnek. 5 determinantlı $F = (-1360889\,,\ -747003\,,\ -102509\,)$ indefinite formu indirgenebilir değildir. Bu form için aşağıdaki tablo elde edilir:

Tablo 1.2 $F = (-1360889\,,\ -747003\,,\ -102509\,)$ nin indirgenmişi

i	0	1	2	3	4	5	6	7	8	9	10
a_i	-1360889	-10509	-13021	-491	-355	-241	-149	-79	-31	-5	-1
b_i	-747003	-73069	-5057	-835	-585	-379	-217	-99	-25	-5	1
c_i	-102509	-13021	-491	-355	-241	-149	-79	-31	-5	-1	1
r_i	4	3	6	2	2	2	2	2	3	2	2

Bu tabloya göre *F* nin indirgenmişi $\rho^{10}(F) = (-1, 1, 1)$ dir.

Pozitif tanımlı bir $F = (a,b,c)$ formu, verilen bir $z \in \mathrm{Y} = \{z = x + iy : y > 0\}$ karmaşık sayısı için

$$F(X,Y) = a(X + zY)(X + \bar{z}Y)$$

şeklinde yazılabilir. Eğer $z = x + iy$ olarak alınırsa yukarıdaki eşitlik

$$F(X,Y) = a(X + zY)(X + \bar{z}Y) = aX^2 + 2axXY + a\,|\,z\,|^2\,Y^2$$

haline gelir. $2ax = b$ ve $a\,|\,z\,|^2 = c$ denklemlerinden $x = \dfrac{b}{2a}$ ve $y = \dfrac{\sqrt{-\Delta(F)}}{2a}$ elde edilir. y pozitif olduğundan

$$z = \frac{b + i\sqrt{-\Delta(F)}}{2a} \in \mathrm{Y}$$

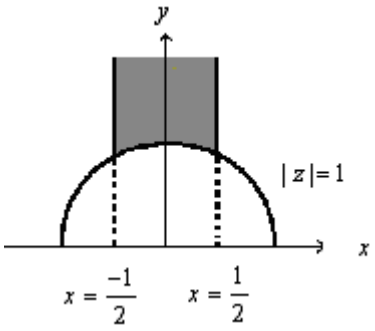
dur. Tersine herhangi bir $z \in \mathrm{Y}$ karmaşık sayısı verildiğinde taban noktası z olan pozitif tanımlı bir form vardır. Gerçekten de $z = x + iy$ için

$$a = \frac{1}{|\,z\,|^2},\ b = \frac{2x}{|\,z\,|^2} \text{ ve } c = 1$$

olarak alınırsa taban noktası z olan $\Delta(F) = \dfrac{-4y^2}{|z|^4} < 0$ determinantlı

$$F = (a, b, c) = \left(\frac{1}{|z|^2}, \frac{2x}{|z|^2}, 1 \right)$$

pozitif tanımlı kuadratik formu elde edilir. Dolayısıyla $\varphi : F \to z(F)$ dönüşümü, sabit determinantlı pozitif tanımlı formlar ile Y nun noktaları arasında birebir bir dönüşümdür. Üstelik pozitif tanımlı F kuadratik formunun indirgenebilir olması, onun taban noktasının modüler grubun temel bölgesinde olması şartına denktir ki bu bölge aşağıdaki gibidir.



Şekil 1.1 Modüler grubun temel bölgesi

1.12 Tanım. Yukarıda elde edilen

$$z = \frac{b + i\sqrt{-\Delta}}{2a}$$

karmaşık sayısına F pozitif tanımlı formun taban noktası denir ve $z = z(F)$ ile gösterilir. F indefinite formunun taban noktası da

$$z = z(F) = \frac{-b + \sqrt{\Delta}}{2a}$$

olarak tanımlanır.

1.13 Uyarı 1. Yukarıda pozitif tanımlı bir F formunun indirgenebilir olma şartının bu formun taban noktasının modüler grubun temel bölgesinde olma şartına denk olduğu görüldü. Benzer şekilde indefinite formların taban noktaları ise yine bu formların

indirgenebilirliklerinde kullanılır. Buna göre "$F=(a,b,c)$ indefinite formunun indirgenebilir olması için gerek ve yeter şart $|z|>1$, $|\bar{z}|<1$ ve $z\cdot\bar{z}<0$ olmasıdır".

2. F_1 ve F_2 indefinite formlarının denklikleri ve bu formların z_1 ve z_2 taban noktaları için Tekcan 2007 aşağıdaki teoremi vermiştir.

1.14 Teorem (Tekcan 2007). F_1 ve F_2 indefinite formları ve bu formların z_1 ve z_2 taban noktaları için

i) "F_1 ve F_2 has denk, yani $\det(g)=1$ için $gF_1=F_2$ dir $\Leftrightarrow (g^{-1})^T z_1=z_2$ dir."

ii) "F_1 ve F_2 has olmayan denk, yani $\det(g)=-1$ için $gF_1=F_2$ dir $\Leftrightarrow (g^{-1})^T z_1=\overline{z_2}$ dir".

1.15 Örnek 1. 73 determinantlı $F_1=(1,7,-6)$ ve $F_2=(4,3,-4)$ formları $g=\begin{bmatrix}7 & 9\\ 10 & 13\end{bmatrix}$ dönüşümü altında birbirine has denktirler. F_1 in taban noktası $z_1=\dfrac{-7+\sqrt{73}}{2}$ ve F_2 nin taban noktası $z_2=\dfrac{-3+\sqrt{73}}{8}$ olup $(g^{-1})^T=\begin{bmatrix}13 & -10\\ -9 & 7\end{bmatrix}$ için

$$(g^{-1})^T z_1=\frac{13\left(\dfrac{-7+\sqrt{73}}{2}\right)-10}{-9\left(\dfrac{-7+\sqrt{73}}{2}\right)+7}=\frac{-3+\sqrt{73}}{8}=z_2$$

dir.

2. 84 determinantlı $F_1=(1,8,-5)$ ve $F_2=(4,6,-3)$ formları $g=\begin{bmatrix}-9 & 1\\ -17 & 2\end{bmatrix}$ dönüşümü altında birbirine has olmayan denktirler. F_1 in taban noktası $z_1=\dfrac{-8+\sqrt{84}}{2}$ ve F_2 nin taban noktası $z_2=\dfrac{-6+\sqrt{84}}{8}$ olup $(g^{-1})^T=\begin{bmatrix}2 & 17\\ -1 & -9\end{bmatrix}$ için

$$(g^{-1})^T z_1 = \frac{2\left(\frac{-8+\sqrt{84}}{2}\right)+17}{-\left(\frac{-8+\sqrt{84}}{2}\right)-9} = \frac{-6-\sqrt{84}}{8} = \overline{z_2}$$

dir.

1.16 Tanım. $F=(a,b,c)$ herhangi bir form ve n bir tamsayı olmak üzere

$$aX^2+bXY+cY^2=n \tag{1.1}$$

denklemini gerçekleyen en az bir (X,Y) tamsayı ikilisi varsa n sayısı F formu ile gösterilebilirdir denir. Eğer F formu ile tüm n tamsayıları gösterilebiliyorsa F ye evrensel form denir.

1.17 Örnek. F = (3, 5, 2) formu evrenseldir. Gerçekten de verilen herhangi bir n tamsayısı için

$$3X^2+5XY+2Y^2=n$$

denkleminin bir çözümü $(X,Y)=(2-n,\ n-3)$ dür.

1.18 Tanım. $F=(a,b,c)$ herhangi bir kuadratik form ve n de pozitif tamsayı olmak üzere bu forma

$$\wp(\tau;F)=1+\sum_{n=1}^{\infty} r(n;F)z^n \tag{1.2}$$

şeklinde bir teta serisi karşılık gelir (Burada $r(n;F)$, (1.1) denklemini sağlayan (X,Y) tamsayı ikililerinin sayısını göstermektedir).

1.19 Örnek. $F=(1,\ 0,\ 6)$ formu ve pozitif n tamsayısı için

$$X^2+6Y^2=n$$

denkleminin

i) $n=1$ için iki tane çözümü vardır ve bu çözümler $\pm(1,0)$ dır.

ii) $n=2,3,5$ için çözümleri yoktur.

iii) $n=4$ için iki tane çözümü vardır ve bu çözümler $\pm(2,0)$ dır.

iv) $n=6$ için iki tane çözümü vardır ve bu çözümler $\pm(0,\,1)$ dir.

Dolayısıyla (1.2) den

$$\wp(\tau;F)=1+\sum_{n=1}^{\infty}r(n;F)z^n=1+2z+2z^4+2z^6+\cdots$$

teta serisi elde edilir.

1.20 Uyarı. F_1 ve F_2 formları denk ise bu formlara karşılık gelen teta serileri aynıdır, yani $\wp(\tau;F_1)=\wp(\tau;F_2)$ dir. Örneğin, $F_1=(4,7,3)$ ve $F_2=(2,\,5,\,3)$ formları denktirler. F_1 formu için

$$4X^2+7XY+3Y^2=n$$

denkleminin

i) $n=1$ için iki tane çözümü vardır ve bu çözümler $\pm(2,\,-3)$ dür.

ii) $n=2$ için dört tane çözümü vardır ve bu çözümler $\pm(1,\,-2),\,\pm(5,\,-7)$ dir.

iii) $n=3$ için dört tane çözümü vardır ve bu çözümler $\pm(0,\,1),\,\pm(8,\,-11)$ dir.

iv) $n=4$ için altı tane çözümü vardır ve bu çözümler $\pm(0,\,1),\,\pm(4,\,-6)$ ve $\pm(11,\,-15)$ dir.

v) $n=5$ için dört tane çözümü vardır ve bu çözümler $\pm(2,\,-1),\,\pm(14,\,-19)$ dur.

Dolayısıyla

$$\wp(\tau;F_1)=1+\sum_{n=1}^{\infty}r(n;F_1)z^n=1+2z+4z^2+4z^3+6z^4+4z^5+\cdots$$

dır. Benzer şekilde F_2 formu için

$$2X^2+5XY+3Y^2=n$$

denkleminin

i) $n=1$ için iki tane çözümü vardır ve bu çözümler $\pm(2,\,-1)$ dir.

ii) $n=2$ için dört tane çözümü vardır ve bu çözümler $\pm(1,\,0),\,\pm(5,\,-3)$ dür.

iii) $n=3$ için dört tane çözümü vardır ve bu çözümler $\pm(0,\,1),\,\pm(8,\,-5)$ dir.

iv) $n=4$ için altı tane çözümü vardır ve bu çözümler $\pm(1,\,-2),\,\pm(4,\,-2)$ ve $\pm(11,\,-7)$ dir.

v) $n=5$ için dört tane çözümü vardır ve bu çözümler $\pm(2,\,-3),\,\pm(14,\,-9)$ dur.

Dolayısıyla

$$\wp(\tau;F_2)=1+\sum_{n=1}^{\infty} r(n;F_2)z^n = 1+2z+4z^2+4z^3+6z^4+4z^5+\cdots$$

dır. Buradan açıkça görülür ki $\wp(\tau;F_1)=\wp(\tau;F_2)$ dir.

Şimdi formların devirleri ve has devirleri ile ilgili aşağıdaki teorem verilebilir.

1.21 Teorem (Buchmann ve Vollmer 2007). $F=(a,b,c)$ indefinite formunun devri, birbirine denk olan formların

$$F_0 \sim F_1 \sim F_2 \sim \cdots \sim F_{l-1}$$

bir dizisi olup bu formlar $i \geq 0$ için

$$s_i = \left\lfloor \frac{b_i+\sqrt{\Delta}}{2\,|\,c_i\,|} \right\rfloor$$

olmak üzere

$$F_{i+1} = (|\,c_i\,|, -b_i+2s_i\,|\,c_i\,|, -a_i-b_is_i-c_is_i^2)$$

şeklindedir. $\tau(F)=(-a,b,-c)$ dönüşümü için F nin has devri, birbirine has denk olan formların bir dizisi olup bu dizi l çift iken

$$F_0 \sim \tau(F_1) \sim F_2 \sim \tau(F_3) \sim \cdots \sim F_{l-2} \sim \tau(F_{l-1})$$

ve l tek iken

$$F_0 \sim \tau(F_1) \sim F_2 \sim \tau(F_3) \sim \cdots \sim \tau(F_{l-2}) \sim F_{l-1} \sim \tau(F_0) \sim F_1 \sim \tau(F_2) \sim \cdots \sim F_{l-2} \sim \tau(F_{l-1})$$

dir.

1.22 Uyarı. $F=(a,b,c)$ indefinite formunun $z(F)=\dfrac{-b+\sqrt{\Delta}}{2a}$ taban noktasının sürekli kesirli açılımı, s_i ler F nin devrindeki sayılar olmak üzere

$$z(F)=[\overline{s_0,s_1,s_2,\cdots,s_{l-1}}]$$

dir.

1.23 Örnek 1. $\Delta = 73$ determinantlı $F = (1, 7, -6)$ formu için yukarıdaki tanımdan aşağıdaki tablo elde edilir:

Tablo 1.3 $F = (1, 7, -6)$ formunun devri

i	0	1	2	3	4	5	6	7	8
a_i	1	6	2	3	4	4	3	2	6
b_i	7	5	7	5	3	5	7	5	7
c_i	-6	-2	-3	-4	-4	-3	-2	-6	-1
s_i	1	3	2	1	1	2	3	1	7

Bu tabloya göre, F nin $z(F) = \dfrac{-7 + \sqrt{73}}{2}$ taban noktasının sürekli kesirli açılımı

$$z(F) = [\overline{1, 3, 2, 1, 1, 2, 3, 1, 7}]$$

olup F nin devri 9 uzunlukludur ve

$$F_0 = (1, 7, -6) \sim F_1 = (6, 5, -2) \sim F_2 = (2, 7, -3) \sim F_3 = (3, 5, -4) \sim F_4 = (4, 3, -4) \sim$$
$$F_5 = (4, 5, -3) \sim F_6 = (3, 7, -2) \sim F_7 = (2, 5, -6) \sim F_8 = (6, 7, -1)$$

şeklindedir. Dolayısıyla has devri 18 uzunluklu olup

$$F_0 = (1, 7, -6) \sim F_1 = (-6, 5, 2) \sim F_2 = (2, 7, -3) \sim F_3 = (-3, 5, 4) \sim F_4 = (4, 3, -4) \sim$$
$$F_5 = (-4, 5, 3) \sim F_6 = (3, 7, -2) \sim F_7 = (-2, 5, 6) \sim F_8 = (6, 7, -1) \sim F_9 = (-1, 7, 6) \sim$$
$$F_{10} = (6, 5, -2) \sim F_{11} = (-2, 7, 3) \sim F_{12} = (3, 5, -4) \sim F_{13} = (-4, 3, 4) \sim F_{14} = (4, 5, -3) \sim$$
$$F_{15} = (-3, 7, 2) \sim F_{16} = (2, 5, -6) \sim F_{17} = (-6, 7, 1)$$

şeklindedir.

2. $\Delta = 84$ determinantlı $F = (1, 8, -5)$ formu için aşağıdaki tablo elde edilir:

Tablo 1.4 $F = (1, 8, -5)$ formunun devri

i	0	1	2	3	4	5
a_i	1	5	4	3	4	5
b_i	8	2	6	6	2	8
c_i	-5	-4	-3	-4	-5	-1
s_i	1	1	2	1	1	8

Bu tabloya göre, $z(F)=\dfrac{-8+\sqrt{84}}{2}=[\overline{1,1,2,1,1,8}]$ dir. Üstelik F nin devri 6 uzunluklu olup

$$F_0=(1,8,-5)\sim F_1=(5,2,-4)\sim F_2=(4,6,-3)\sim F_3=(3,6,-4)\sim$$
$$F_4=(4,2,-5)\sim F_5=(5,8,-1)$$

şeklindedir. Has devri ise 6 uzunluklu olup

$$F_0=(1,8,-5)\sim F_1=(-5,2,\ 4)\sim F_2=(4,6,-3)\sim F_3=(-3,6,\ 4)\sim$$
$$F_4=(4,2,-5)\sim F_5=(-5,8,\ 1)$$

şeklindedir.

1.24 Tanım. $\delta>0$ tam kare olmayan bir sayı olmak üzere

$$\Theta(\delta)=\{x+y\delta : x,y\in\Theta\}$$

kuadratik sayı cismi için $\gamma\in\Theta(\delta)$ elemanı verilsin. Bu takdirde γ elemanı, P ve Q lar

$$Q\mid(P+\delta)(P+\overline{\delta})$$

özelliğindeki tamsayılar olmak üzere $\gamma=\dfrac{P+\delta}{Q}$ şeklinde yazılabilir. Bu sayıya kuadratik irrasyonel denir.

1.25 Teorem (Mollin 1996). Bir γ kuadratik irrasyonel sayısı verildiğinde bu sayıya

$$I_\gamma=[Q,\ P+\delta]$$

kuadratik ideali ve

$$F_\gamma=Q(X+\gamma Y)(X+\overline{\gamma}Y)$$

indefinite kuadratik formu karşılık gelir.

1.26 Uyarı. t, δ nın izi ve n de normu olmak üzere F_γ indefinite formu

$$F_\gamma=Q(X+\gamma Y)(X+\overline{\gamma}Y)=QX^2+(t+2P)XY+\left(\frac{n+tP+P^2}{Q}\right)Y^2$$

haline gelir. Bu formun diskriminantı $\Delta(F)=t^2-4n$ dir.

1.27 Tanım. $I_\gamma = [Q,\ P+\delta]$ kuadratik ideali için $P+\delta > 0$ ve $-Q < P+\overline{\delta} < 0$ şartı sağlanıyorsa bu ideale indirgenebilirdir denir. Eğer $\dfrac{2P}{Q}$ tamsayı ise ideale ambiguous ideal denir.

1.28 Teorem (Mollin 1996). $\gamma = \dfrac{P+\delta}{Q}$ kuadratik irrasyoneli ve $I_\gamma = [Q,\ P+\delta]$ ideali için $i \geq 0$ olmak üzere

$$m_i = \left\lfloor \frac{P_i+\delta}{Q_i} \right\rfloor,\ P_{i+1} = m_i Q_i - P_i \ \text{ ve } \ Q_{i+1} = \frac{\delta^2 - P_{i+1}^2}{Q_i}$$

tanımlansın. Bu takdirde γ nın basit sürekli kesirli açılımı $[m_0; \overline{m_1, m_2, \cdots, m_{l-1}}]$ ve I_γ nın devri $I_{\gamma_0} \sim I_{\gamma_1} \sim I_{\gamma_2} \sim \cdots \sim I_{\gamma_{l-1}}$ şeklindedir.

1.29 Uyarı. $\gamma = \dfrac{P+\delta}{Q}$ kuadratik irrasyonel sayısı için $\gamma > 1$ ve $-1 < \overline{\gamma} < 0$ ise γ nın basit sürekli kesirli açılımı $[0; \overline{m_1, m_2, \cdots, m_{l-1}}] = [\overline{m_1, m_2, \cdots, m_{l-1}}]$ şeklindedir. Bu açılıma saf açılım denir.

1.30 Örnek. $\delta = \sqrt{73}$ için $\gamma = \dfrac{8+\sqrt{73}}{3}$ bir kuadratik irrasyoneldir. Çünkü $3 \mid (64-73)$ dür. $\gamma \cong 5.51 > 1$ ve $\overline{\gamma} \cong -0.18$ olup $-1 < \overline{\gamma} < 0$ dır. Dolayısıyla $I_\gamma = [3,\ 8+\sqrt{73}]$ bir kuadratik ideal olup aşağıdaki tablo elde edilir:

Tablo 1.5 $I_\gamma = [3,\ 8+\sqrt{73}]$ idealinin devri

i	0	1	2	3	4	5	6
P_i	8	7	1	8	8	1	7
Q_i	3	8	9	1	9	8	3
m_i	5	1	1	16	1	1	5

Bu tabloya göre γ nın sürekli kesirli açılımı $[\overline{5, 1, 1, 16, 1, 1, 5}]$ ve I_γ idealinin devri

$$I_{\gamma_0} = [3, 8+\sqrt{73}] \sim I_{\gamma_1} = [8, 7+\sqrt{73}] \sim I_{\gamma_2} = [9, 1+\sqrt{73}] \sim I_{\gamma_3} = [1, 8+\sqrt{73}] \sim$$
$$I_{\gamma_4} = [9, 8+\sqrt{73}] \sim I_{\gamma_5} = [8, 1+\sqrt{73}] \sim I_{\gamma_6} = [3, 7+\sqrt{73}]$$

dir.

1.31 Teorem (Mollin 1996). $D > 0$ tam kare olmayan bir tamsayı olmak üzere $I_1 = [Q_1, P_1 + \sqrt{D}]$ ve $I_2 = [Q_2, P_2 + \sqrt{D}]$ herhangi iki ideal olsun.

$$S = obeb(Q_1, Q_2, P_1 + P_2)$$
$$Q = \frac{Q_1 Q_2}{S^2}$$
$$P \equiv \frac{UQ_2P_1 + VQ_1P_2 + \frac{W}{2}(P_1P_2 + D)}{S} \pmod{2Q}$$

olarak tanımlansın. U, V, W lar $UQ_2 + VQ_1 + \frac{W}{2}(P_1 + P_2) = S$ denklemini sağlayan tamsayılar olmak üzere I_1 ve I_2 nin çarpımı $I = (S)[Q, P + \sqrt{D}]$ idealidir.

1.32 Örnek. $I_1 = [4, 3+\sqrt{21}]$ ve $I_2 = [5, 4+\sqrt{21}]$ idealleri için

$$S = obeb(4, 5, 7) = 1 \text{ ve } Q = \frac{Q_1 Q_2}{S^2} = \frac{(4)(5)}{1} = 20$$

ve

$$P \equiv 15u + 16V + \frac{33W}{2} \pmod{40}$$

dır. Diğer yandan $5U + 4V + \frac{7}{2}W = 1$ denkleminin bir çözümü $(U, V, W) = (-3, 4, 0)$ dır. Dolayısıyla

$$P \equiv 15u + 16V + \frac{33W}{2} \pmod{40}$$
$$\equiv 19 \pmod{40}$$

elde edilir. O halde I_1 ve I_2 ideallerinin çarpımı $I = [20, 19+\sqrt{21}]$ idealidir.

1.33 Tanım. $a, b, c \in Z$ olmak üzere

$$ax + by = c$$

denklemine birinci dereceden Diophantine denklemi denir.

Yukarıdaki denklemin çözümünün olması için gerek ve yeter şart $d = obeb(a,b)$ olmak üzere $d \mid c$ olmasıdır. Eğer (x_0, y_0) bu denklemin bir özel çözümü ise denklemin diğer tüm çözümleri $t \in Z$ için

$$(x, y) = \left(x_0 + \frac{b}{d} t,\ y_0 - \frac{a}{d} t \right)$$

şeklindedir.

1.34 Örnek. $14x + 22y = 50$ Diophantine denklemi için $d = obeb(14, 22) = 2$ ve $2 \mid 50$ olduğundan denklemin çözümleri vardır. $(x_0, y_0) = (2, 1)$ bu denklemin bir özel çözümü olup denklemin diğer tüm çözümleri $t \in Z$ için $(x, y) = (2 + 11t, 1 - 7t)$ şeklindedir.

1.35 Tanım. $a, b, c, d, e, f \in Z$ olmak üzere

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

denklemine ikinci dereceden Diophantine denklemi denir.

Birinci ve ikinci dereceden bu tür denklemler, ilk olarak Yunanlı matematikçi olan Alexandra Diophantus tarafından ele alınmış ve ondan sonra bir çok matematikçi tarafından çalışılmıştır. Günümüzde de bu tür denklemler hala çalışılmaya devam etmektedir (Bu denklemler ile ilgili daha fazla bilgi için Barbeau 2003, Mollin 2008, 2010 ve Nathanson 2000 referanslarına bakılabilir).

1.36 Tanım. $d > 0$ tam kare olmayan bir tamsayı ve $N \in Z$ olmak üzere ikinci tür Diophantine denkleminin özel bir hali olan

$$x^2 - dy^2 = \pm N$$

denklemine Pell denklemi denir. $x^2 - dy^2 = N$ ye pozitif, $x^2 - dy^2 = -N$ ye ise negatif Pell denklemi denir.

1.37 Uyarı 1. Yukarıdaki tanımda geçen d tamsayısının tam kare olması durumunda verilen denklem çarpanlara ayrılabilir. Gerçekten de belli bir $t \neq 0$ tamsayısı için $d = t^2$ ise bu denklem $x^2 - dy^2 = \pm N \Leftrightarrow x^2 - t^2 y^2 = \pm N \Leftrightarrow (x - ty)(x + ty) = \pm N$ haline gelir ki N nin $N = k \cdot l$ şeklinde çarpanlara ayrılması durumunda sonlu sayıda durum söz konusu olup bu halde verilen Pell denkleminin sonlu sayıda çözümü vardır veya yoktur. Örneğin $x^2 - 4y^2 = 6$ denklemi için $x^2 - 4y^2 = 6 \Leftrightarrow (x - 2y)(x + 2y) = 6$ olup aşağıdaki durumlar söz konusudur:

Tablo 1.6 $x^2 - 4y^2 = 6$ Pell denklemi

$x - 2y$	$x + 2y$
1	6
2	3
3	2
6	1
-1	-6
-2	-3
-3	-2
-6	-1

Yukarıdaki çarpanların toplamları çift olmadığından verilen denklemin çözümü yoktur. Benzer şekilde $x^2 - 9y^2 = 7$ Pell denklemi için $x^2 - 9y^2 = 7 \Leftrightarrow (x - 3y)(x + 3y) = 7$ olup aşağıdaki durumlar söz konusudur:

Tablo 1.7 $x^2 - 9y^2 = 7$ Pell denklemi

$x - 3y$	$x + 3y$
1	7
7	1
-1	-7
-7	-1

Buna göre denklemin çözümleri sırasıyla $(4, 1), (4, -1), (-4, -1)$ ve $(-4, 1)$ dir.

2. $x^2 - dy^2 = \pm N$ Pell denklemleri ilk olarak İngiliz matematikçi olan John Pell (1611-1685) tarafından 17. yüzyılda ele alınmış ve sonraları Leonhard Euler (1707-1783) tarafından 18. yüzyılda detaylı olarak incelenmiştir. Bu denklemde özel olarak $N = 1$ olarak alınırsa $x^2 - dy^2 = \pm 1$ denklemi elde edilir ki bu denkleme klasik Pell denklemi denir. Bu denklemi sağlayan en küçük pozitif (x_1, y_1) çözümüne denklemin temel çözümü denir. Eğer (x_1, y_1), $x^2 - dy^2 = 1$ pozitif Pell denkleminin temel çözümü ise denklemin diğer tüm çözümleri $n \geq 1$ tamsayısı için

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$$

olmak üzere (x_n, y_n) şeklindedir. Eğer (x_1, y_1), $x^2 - dy^2 = -1$ negatif Pell denklemini temel çözümü ise denklemin diğer tüm çözümleri $n \geq 1$ tamsayısı için

$$x_{2n+1} + y_{2n+1}\sqrt{d} = (x_1 + y_1\sqrt{d})^{2n+1}$$

olmak üzere (x_{2n+1}, y_{2n+1}) şeklindedir. Üstelik $x^2 - dy^2 = \pm 1$ Pell denkleminde $n \to \infty$ için $\frac{x_n}{y_n} \cong \sqrt{d}$ dir.

1.38 Örnek. 1. $x^2 - 6y^2 = 1$ pozitif Pell denkleminin temel çözümü $(x_1, y_1) = (5, 2)$ olup denklemin diğer çözümleri

$$\begin{aligned}
x_2 + y_2\sqrt{6} &= (5 + 2\sqrt{6})^2 = 49 + 20\sqrt{6} \\
x_3 + y_3\sqrt{6} &= (5 + 2\sqrt{6})^3 = 485 + 198\sqrt{6} \\
x_4 + y_4\sqrt{6} &= (5 + 2\sqrt{6})^4 = 4801 + 1960\sqrt{6} \\
x_5 + y_5\sqrt{6} &= (5 + 2\sqrt{6})^5 = 47525 + 19402\sqrt{6} \\
x_6 + y_6\sqrt{6} &= (5 + 2\sqrt{6})^6 = 470449 + 192060\sqrt{6} \\
x_7 + y_7\sqrt{6} &= (5 + 2\sqrt{6})^7 = 4656965 + 1901198\sqrt{6}
\end{aligned}$$

şeklinde devam etmektedir. Burada $\frac{x_7}{y_7} \cong 2.449489743$ ve $\sqrt{6} \cong 2.499489743$ dür.

2. $x^2 - 26y^2 = -1$ negatif Pell denkleminin temel çözümü $(x_1, y_1) = (5, 1)$ olup denklemin diğer çözümleri

$$x_3 + y_3\sqrt{26} = (5+\sqrt{26})^3 = 515 + 101\sqrt{26}$$
$$x_5 + y_5\sqrt{26} = (5+\sqrt{26})^5 = 52525 + 10301\sqrt{26}$$
$$x_7 + y_7\sqrt{26} = (5+\sqrt{26})^7 = 5357035 + 1050601\sqrt{26}$$
$$x_9 + y_9\sqrt{26} = (5+\sqrt{26})^9 = 546365045 + 107151001\sqrt{26}$$
$$x_{11} + y_{11}\sqrt{26} = (5+\sqrt{26})^{11} = 5572387755\ 5 + 1092835150\ 1\sqrt{26}$$

şeklinde devam etmektedir. Burada $\frac{x_{11}}{y_{11}} \cong 5.099019514$ ve $\sqrt{26} \cong 5.099019514$ dür.

2. SONLU CİSİMLER ÜZERİNDE TANIMLI ÖZEL EĞRİLER

Bu bölümde $p \geq 5$ asal sayısına bağlı olarak bir fonksiyon tanımlanacak ve bu fonksiyon ile ilgili bazı cebirsel özellikler verilecektir. Daha sonra bu fonksiyona bağlı olarak tanımlanacak olan eğri üzerindeki rasyonel noktaların sayısı sonlu Φ_p cisminde ele alınacaktır. Bu bölümde elde edilen tüm sonuçlar Tekcan, Alkan ve ark. 2010 dan alınmıştır.

b pozitif tam kare olmayan bir tamsayı ve $p \geq 5$ asal sayısı için

$$f_p(x) = \frac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}}$$

fonksiyonu tanımlansın. Bu takdirde aşağıdaki sonuçlar verilebilir.

2.1 Teorem. $f_p(x)$, derecesi p ve baş katsayısı da $2p+2$ olan bir polinom fonksiyon, yani $f_p(x) \in \mathrm{Z}[x]$ dir. Üstelik

$$f_p(x) = 2\sum_{i=0}^{\frac{p-1}{2}} \binom{p+1}{2i+1} x^{p-2i} b^i$$

dir.

İspat: $p \geq 5$ asal sayısı için Binom formülünden

$$\begin{aligned} f_p(x) &= \frac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}} \\ &= \frac{1}{\sqrt{b}}[(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}] \\ &= 2\left[\binom{p+1}{1} x^p + \binom{p+1}{3} x^{p-2} b + \cdots + \binom{p+1}{p} x b^{\frac{p-1}{2}}\right] \\ &= 2\sum_{i=0}^{\frac{p-1}{2}} \binom{p+1}{2i+1} x^{p-2i} b^i \end{aligned}$$

olduğu görülür.

2.2 Örnek. $5 \le p \le 17$ asal sayıları için

$$f_5(x) = 12x^5 + 40x^3b + 12xb^2$$

$$f_7(x) = 16x^7 + 112x^5b + 112x^3b^2 + 16xb^3$$

$$f_{11}(x) = 24x^{11} + 440x^9b + 1584x^7b^2 + 1584x^5b^3 + 440x^3b^4 + 24xb^5$$

$$f_{13}(x) = 28x^{13} + 728x^{11}b + 4004x^9b^2 + 6864x^7b^3 + 4004x^5b^4 + 728x^3b^5 + 28xb^6$$

$$f_{17}(x) = 36x^{17} + 1632x^{15}b + 17136x^{13}b^2 + 63648x^{11}b^3 + 97240x^9b^4 + 63648x^7b^5 + 17136x^5b^6 + 17136x^5b^6 + 1632x^3b^7 + 36xb^8$$

dir.

2.3 Uyarı. Teorem 2.1 deki $f_p(x)$ nin

$$f_p(x) = 2\sum_{i=0}^{\frac{p-1}{2}} \binom{p+1}{2i+1} x^{p-2i}b^i$$

eşitliği açılırsa

$$f_p = 2(p+1)x^p + \left(\frac{p^3-p}{3}\right)x^{p-2}b + \cdots + 2(p+1)xb^{\frac{p-1}{2}}$$

olduğu görülür. Dolayısıyla $f_p(x)$ polinom fonksiyonu, sonlu Φ_p cisminde dikkate alınırsa aşağıdaki teorem verilebilir.

2.4 Teorem. $f_p(x)$ polinom fonksiyonu için

$$f_p(x) \equiv 2x^p + 2xb^{\frac{p-1}{2}} \pmod{p}$$

dir.

İspat. $f_p(x)$ nin $f_p = 2(p+1)x^p + \left(\frac{p^3-p}{3}\right)x^{p-2}b + \cdots + 2(p+1)xb^{\frac{p-1}{2}}$ açılımına dikkat edilirse bu açılımdaki

$$x^{p-2}b,\ x^{p-4}b^2, \cdots,\ x^3b^{\frac{p-3}{2}}$$

terimlerinin katsayıları p nin bir katını bulundurur. Dolayısıyla da bu katsayılar mod p de sıfıra denk olurlar. O halde $f_p(x) \equiv 2x^p + 2xb^{\frac{p-1}{2}} \pmod{p}$ dir.

2.5 Tanım 1. $m > 1$ tamsayı ve $a \in Z$ sayısı için $x^2 \equiv a \pmod{m}$ denklemini sağlayan en az bir $x \in Z$ varsa a ya mod m ye göre ikinci dereceden kalan denir. İkinci dereceden kalanların kümesi Q_m ile gösterilir.

2. $p > 2$ asal sayısı ve p ile aralarında asal $a \in Z$ sayısı için a nın Legendre sembolü $\left(\frac{a}{p}\right)$ ile gösterilir ve $x^2 \equiv a \pmod{p}$ kongrüansının çözümünün olması halinde 1; $p \mid a$ olması halinde 0 ve $x^2 \equiv a \pmod{p}$ kongrüansının çözümünün olmaması halinde -1 olarak tanımlanır (Mollin 2008).

2.6 Teorem (Fermat' ın Küçük Teoremi). $p > 2$ asal sayısı ve mod p de sıfırdan farklı $a \in Z$ sayısı için

$$a^{p-1} \equiv 1 \pmod{p}$$

dir (Mollin 2008).

2.7 Teorem. $b \in \Phi_p^* = \Phi_p - \{0\}$ bir sabit sayı olmak üzere

$$b^{\frac{p-1}{2}} \equiv \begin{cases} 1 & b \in Q_p \\ p-1 & b \notin Q_p \end{cases} \pmod{p}$$

dir.

İspat. $b \in Q_p$ olsun. Bu takdirde $\left(\frac{b}{p}\right) = 1$ olup yukarıdaki tanım gereği $x^2 \equiv b \pmod{p}$ kongrüansının en az bir çözümü vardır. Şimdi $a \neq 0$ olmak üzere $b = a^2$ olsun. Bu takdirde Fermat' ın küçük teoremi gereği

$$b^{\frac{p-1}{2}} = (a^2)^{\frac{p-1}{2}} = a^{p-1} \equiv 1 \pmod{p}$$

olur. Benzer şekilde $b \notin Q_p$ için $b^{\frac{p-1}{2}} \equiv p-1$ olduğu da gösterilebilir.

2.8 Tanım. $p \geq 5$ asal sayı ve $a, b \in \Phi_p$ olmak üzere

$$y^2 = x^3 + ax + b$$

eşitliğini gerçekleyen tüm (x, y) noktalarının kümesine eliptik eğri denir ve E ile gösterilir. Bu eğrinin diskriminantı $\Delta(E) = -16(4a^3 + 27b^2)$ dir (Silverman 1986).

2.9 Uyarı 1. Yukarıdaki tanımdaki E eliptik eğrisine Weierstrass formu denir.

2. E nin bir eliptik eğri olması için $\Delta(E) \neq 0$, yani $4a^3 + 27b^2 \neq 0$ olmalıdır. Bu şart $x^3 + ax + b$ denkleminin katlı kökünün olmaması demektir. Aksi halde eğri singüler bir eğri belirtir, yani $x^3 + ax + b$ polinomu katlı köke sahiptir.

3. $O = (\infty, \infty)$, sonsuzdaki ideal nokta olmak üzere eğri üzerindeki tüm (x, y) rasyonel noktalarının

$$E(\Phi_p) = \{(x, y) \in \Phi_p \times \Phi_p : y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{O\}$$

kümesi (toplam işlemine göre) bir grup oluşturur. Bu grubun mertebesi $\#E(\Phi_p)$ ile gösterilir ve

$$\#E(\Phi_p) = p + 1 + \sum_{x \in \Phi_p} \left(\frac{x^3 + ax + b}{p} \right)$$

olarak tanımlanır. Örneğin, $p = 7$ ve $a = 2,\ b = 4$ için $E : y^2 = x^3 + 2x + 4$ eliptik eğrisi üzerindeki rasyonel noktaların sayısı

$$\begin{aligned} \#E(\Phi_7) &= 7 + 1 + \sum_{x \in \Phi_7} \left(\frac{x^3 + 2x + 4}{7} \right) \\ &= 8 + \left(\frac{4}{7}\right) + \left(\frac{0}{7}\right) + \left(\frac{2}{7}\right) + \left(\frac{2}{7}\right) + \left(\frac{6}{7}\right) + \left(\frac{6}{7}\right) + \left(\frac{1}{7}\right) \end{aligned}$$

dır. Diğer yandan $Q_7 = \{1, 2, 4\}$ olduğundan

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1,\ \left(\frac{6}{7}\right) = -1 \text{ ve } \left(\frac{0}{7}\right) = 0$$

dır. Dolayısıyla yukarıdaki eşitlikten

$$\#E(\Phi_7) = 10$$

elde edilir (Eliptik eğriler ile ilgili daha fazla bilgi için Washington 2003 ve Silverman 1986 kaynaklarına bakılabilir).

Teorem 2.4 de $f_p(x)$ fonksiyonu için $f_p(x) \equiv 2x^p + 2xb^{\frac{p-1}{2}} \pmod{p}$ olduğu gösterildi. Şimdi bu $f_p(x)$ fonksiyonuna bağlı olarak eğri tanımlanabilir ve bu eğri ile ilgili bağıntılar elde edilebilir. $f_p(x)$ fonksiyonu için eğri

$$E_p : y^2 \equiv f_p(x) \pmod{p}$$

olarak tanımlansın. Bu takdirde

$$E_p : y^2 \equiv 2x^p + 2xb^{\frac{p-1}{2}} \pmod{p}$$

olur. *O* sonsuzdaki ideal nokta olmak üzere (eliptik eğrilerdekine benzer şekilde) bu eğri üzerindeki rasyonel noktaların kümesi

$$E_p(\Phi_p) = \{(x, y) \in \Phi_p \times \Phi_p : y^2 \equiv 2x^p + 2xb^{\frac{p-1}{2}} \pmod{p}\} \cup \{O\}$$

ile gösterilsin. Bu takdirde aşağıdaki teoremler verilebilir.

2.10 Teorem. E_p eğrisi için

$$\# E_p(\Phi_p) = p + 1$$

dir.

İspat. İki hal söz konusudur.

1. Hal: $b \in Q_p$ olsun. Bu takdirde Teorem 2.7 gereği $b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ dir. Dolayısıyla verilen eğri

$$\begin{aligned} E_p : y^2 &\equiv 2x^p + 2xb^{\frac{p-1}{2}} \pmod{p} \\ &\equiv 2x^p + 2x \pmod{p} \end{aligned}$$

haline gelir. Diğer yandan Fermat' ın küçük teoremi gereği $x^p \equiv x \pmod{p}$ olduğundan yukarıdaki eşitlikten

$$E_p : y^2 \equiv 4x \pmod{p}$$

elde edilir. $4 = 2^2$ olduğundan 4 bir kuadratik kalan, yani $4 \in Q_p$ dir. Şimdi $x \in Q_p$ sabit bir nokta olsun. Bu takdirde belli bir $t \neq 0$ için $x \equiv t^2 \pmod{p}$ dir. Dolayısıyla

$$y^2 \equiv 2^2 \cdot t^2 = (2t)^2 \pmod{p} \Leftrightarrow y \equiv \pm 2t \pmod{p}$$

elde edilir. Bu ise kongrüansın farklı iki çözümünün olması demektir. Dolayısıyla E_p eğrisi üzerinde $(t^2,\ 2t)$ ve $(t^2, p-2t)$ şeklinde iki rasyonel nokta vardır. Diğer yandan kuadratik kalanların sayısı $\frac{p-1}{2}$ olduğundan, E_p eğrisi üzerinde $2(\frac{p-1}{2}) = p-1$ tane rasyonel nokta vardır. (0,0) daima E_p üzerindedir. İdeal noktanın da eklenmesiyle eğri üzerinde toplam $p+1$ tane rasyonel nokta olduğu görülür. $x \notin Q_p$ için $y^2 \equiv 4x \pmod{p}$ kongrüansının çözümü olmadığından E_p eğrisi üzerinde rasyonel nokta yoktur.

2. Hal. $b \notin Q_p$ olsun. Bu takdirde $b^{\frac{p-1}{2}} \equiv p-1 \pmod{p}$ ve $x^p \equiv x \pmod{p}$ olduğundan verilen eğri

$$\begin{aligned} E_p : y^2 &\equiv 2x^p + 2xb^{\frac{p-1}{2}} \pmod{p} \\ &\equiv 2x^p + 2x(p-1) \pmod{p} \\ &\equiv 2x + 2x(p-1) \pmod{p} \\ &\equiv 2x(1+p-1) \pmod{p} \\ &\equiv 0 \pmod{p} \end{aligned}$$

haline gelir. $y^2 \equiv 0 \pmod{p}$ kongrüansı, her $x \in \Phi_p$ elemanı için bir çözüme sahip olduğundan E_p eğrisi üzerinde $(0,0),\ (1,0),(2,0),\cdots,(p-1,0)$ rasyonel noktaları vardır. İdeal noktanın da eklenmesiyle E_p de $p+1$ tane rasyonel noktanın olduğu görülür.

E_p eğrisi üzerindeki (x,y) rasyonel noktaların $x-$ve $y-$koordinatlarının toplamları için

$$E_p^x(\Phi_p) = \{x \in \Phi_p : (x,y) \in E_p(\Phi_p)\}$$

ve

$$E_p^y(\Phi_p) = \{y \in \Phi_p : (x,y) \in E_p(\Phi_p)\}$$

kümeleri tanımlansın. Bu kümedeki elemanların toplamları sırasıyla

$$\sum_{[x]} E_p^x(\Phi_p) \quad \text{ve} \quad \sum_{[y]} E_p^y(\Phi_p)$$

ile gösterilsin. Bu takdirde aşağıdaki teorem verilebilir.

2.11 Teorem. E_p eğrisi için

$$\sum_{[x]} E_p^x(\Phi_p) = \begin{cases} \dfrac{p^3 - p}{12} & b \in Q_p \\ \dfrac{p^2 - p}{2} & b \notin Q_p \end{cases}$$

ve

$$\sum_{[y]} E_p^y(\Phi_p) = \begin{cases} \dfrac{p^2 - p}{2} & b \in Q_p \\ 0 & b \notin Q_p \end{cases}$$

dir.

İspat. $U_p = \{1, 2, \cdots, p-1\}$, Φ_p deki birimlerin kümesi olmak üzere bu kümedeki her bir elemanın karesi alınmak suretiyle ikici dereceden kalanların

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

kümesi elde edilir. Q_p deki bu elemanların toplamı

$$\sum_{x \in Q_p} x = \frac{p^3 - p}{24}$$

dür. Şimdi $b \in Q_p$ olsun. Bu takdirde, Teorem 2.10 gereği $x \in Q_p$ için E_p eğrisi üzerinde $(t^2, 2t)$ ve $(t^2, p - 2t)$ gibi iki rasyonel nokta vardır. Q_p de $(p-1)/2$ tane eleman vardır ve bunların her birisi için eğri üzerinde iki rasyonel nokta elde edilir. O halde eğri üzerindeki rasyonel noktaların $x-$ koordinatları toplamı

$$\sum_{[x]} E_p^x(\Phi_p) = 2 \sum_{x \in Q_p} x = \frac{p^3 - p}{12}$$

olur. $b \notin Q_p$ için eğri üzerindeki rasyonel noktalar $(0,0), (1,0), (2,0), \cdots, (p-1, 0)$ olup bu rasyonel noktaların $x-$ koordinatları toplamı

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

olur.

Eğri üzerindeki rasyonel noktaların $y-$ koordinatları için $b \in Q_p$ olsun. Bu takdirde Q_p deki her bir eleman için eğri üzerinde $(t^2,\ 2t)$ ve $(t^2,\ p-2t)$ rasyonel noktaları vardır. Bu noktaların $y-$ koordinatları toplamı p dir. Q_p de $\frac{p-1}{2}$ tane eleman olduğundan eğri üzerindeki tüm rasyonel noktaların $y-$ koordinatları toplamı

$$\sum_{[y]} E_p^y(\Phi_p) = p\left(\frac{p-1}{2}\right) = \frac{p^2-p}{2}$$

olur. $b \notin Q_p$ için, eğri üzerindeki rasyonel noktalar $(0,0),\ (1,0),(2,0),\cdots,(p-1,0)$ olup bu noktaların $y-$ koordinatlarının toplamının 0 olduğu açıktır.

3. $y^2 - 2yx - 3 = 0$ DIOPHANTİNE DENKLEMİ VE BU DENKLEME KARŞILIK GELEN EĞRİ ÜZERİNDEKİ RASYONEL NOKTALAR

Bu bölümde özel bir Diophantine denklemi ele alınacak ve bu denklemin tamsayı çözümleri Z de ve $p \geq 5$ asalı için sonlu Φ_p cisimlerinde ele alınacaktır. Daha sonra ise denklemin köklerine bağlı olarak bir eğri tanımlanacak ve bu eğri üzerindeki rasyonel noktaların sayısı $p \geq 5$ asalı için sonlu Φ_p cisimlerinde belirlenmeye çalışılacaktır. Son olarak bu eğri üzerindeki (x, y) rasyonel noktalarının $x-$ ve $y-$ koordinatları toplamları ile ilgili sonuç verilecektir. Bu bölümde elde edilen tüm sonuçlar Tekcan, Özkoç ve Alkan 2009 dan alınmıştır.

3.1 $y^2 - 2yx - 3 = 0$ Diophantine Denklemi

Bu kısımda

$$D: y^2 - 2yx - 3 = 0$$

Diophantine denkleminin çözümleri tamsayılar kümesinde ve $p \geq 5$ asalı için sonlu Φ_p cisminde ele alınacaktır.

3.1.1 Teorem. *D* Diophantine denkleminin tamsayılarda dört tane çözümü vardır.

İspat. Verilen Diophantine denklemi

$$y^2 - 2yx - 3 = 0 \Leftrightarrow y(y - 2x) = 3$$

haline getirilirse bu denklem için aşağıdaki durumlar söz konusudur:

y	$y-2x$
1	3
3	1
-1	-3
-3	-1

Buradan $(x.y) = \pm(1, 3), \pm(1,-1)$ tamsayı çözümleri elde edilir. O halde denklemin dört tane tamsayı çözümü vardır.

Şimdi verilen Diophantine denkleminin tamsayı çözümleri $p \geq 5$ asalı için sonlu Φ_p cisimlerinde ele alınsın. Eğer verilen Diophantine denklemi Φ_p de düşünülürse

$$D_p : y^2 - 2yx - 3 \equiv 0 \pmod{p}$$

Diophantine denklemi ele edilmiş olur. Bu denklemin tamsayı çözümlerinin kümesi

$$D_p(\Phi_p) = \{(x, y) \in \Phi_p \times \Phi_p : y^2 - 2yx - 3 \equiv 0 \pmod{p}\}$$

ile gösterilirse aşağıdaki teorem verilebilir.

3.1.2 Teorem. D_p Diophantine denklemi için

$$\# D_p(\Phi_p) = p - 1$$

dir.

İspat. $\left(\frac{x}{p}\right)$ Legendre sembolü olmak üzere

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod{12} \\ -1 & p \equiv 5, 11 \pmod{12} \end{cases}$$

ve

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 1, 11 \pmod{12} \\ -1 & p \equiv 5, 7 \pmod{12} \end{cases}$$

olduğu bilinmektedir. Verilen Diophantine denklemi y ye göre çözülmek istenirse verilen her bir $x \in \Phi_p$ için denklemin diskriminantı

$$\Delta \equiv (-2x)^2 - 4(-3) \equiv 4(x^2 + 3) \pmod{p}$$

olur. Dolayısıyla denklemin kökleri

$$y_{1,2} \equiv \frac{2x \pm 2\sqrt{x^2 + 3}}{2} \equiv x \pm \sqrt{x^2 + 3} \pmod{p}$$

olarak elde edilir. Burada iki hal söz konusudur:

1.Hal. $p \equiv 1, 7 \pmod{12}$ olsun. Bu takdirde $\left(\frac{-3}{p}\right) = 1$ dir. Bu ise $x^2 \equiv -3 \pmod{p}$ kongrüansının x_1, x_2 gibi iki tane tamsayı çözümünün olması demektir. x_1 ve x_2 nin bu de-

ğerleri için farklı iki y_1 ve y_2 değerleri elde edilir. Dolayısıyla denkleminin (x_1, y_1) ve (x_2, y_2) gibi iki tamsayı çözümü vardır. Burada yine iki durum söz konusudur:

i) $p \equiv 1 \pmod{12}$ olsun. Bu takdirde $x = 0$ ise $y^2 - 3 = 0 \pmod{p}$ kuadratik kongrüansı için $\left(\frac{3}{p}\right) = 1$ olduğundan bu kongrüansın y_3 ve y_4 gibi iki çözümü vardır. Dolayısıyla denkleminin $(0, y_3)$ ve $(0, y_4)$ gibi iki tamsayı çözümü vardır. x lerin bu değerleri Φ_p den çıkartılarak $H_p = \Phi_p - \{0, x_1, x_2\}$ kümesi dikkate alınsın. Bu takdirde $\# H_p = p - 3$ dür. Üstelik H_p de $x^2 + 3 \equiv t^2 \pmod{p}$ kuadratik kongrüansının çözümü olacak şekilde $\frac{p-5}{2}$ tane x vardır ve bunların her birisi için denklemin $y_{1,2} = x \pm t \pmod{p}$ gibi iki çözümü vardır. Bu ise H_p deki her bir x değeri için denkleminin $2\left(\frac{p-5}{2}\right) = p - 5$ tane tamsayı çözümünün olması demektir. Yukarıda bu denklemin (x_1, y_1), (x_2, y_2), $(0, y_3)$ ve $(0, y_4)$ gibi dört tane daha çözümünün olduğu gösterilmişti. O halde denklemin toplam $p - 5 + 4 = p - 1$ tane tamsayı çözümü vardır.

ii) $p \equiv 7 \pmod{12}$ olsun. Bu takdirde $\left(\frac{3}{p}\right) = -1$ dir. Eğer $x = 0$ ise $y^2 - 3 \equiv 0 \pmod{p}$ kuadratik kongrüansının çözümü yoktur. Bu ise denkleminin $(0, y)$ gibi bir tamsayı çözümünün olmaması demektir. Yukarıda elde edilen x_1, x_2 değerleri Φ_p den çıkartılarak $G_p = \Phi_p - \{x_1, x_2\}$ kümesi oluşturulsun. Bu takdirde $\# G_p = p - 2$ olduğu açıktır. Üstelik G_p de $x^2 + 3 \equiv t^2 \pmod{p}$ kongrüansının çözümü olacak şekilde $\frac{p-3}{2}$ tane x elemanı vardır ve bunların her birisi için $y_{1,2} = x \pm t \pmod{p}$ çözümleri elde edilir. Dolayısıyla her bir $x \in G_p$ için denklemin $2\left(\frac{p-3}{2}\right) = p - 3$ tane tamsayı çözümü vardır. (x_1, y_1) ve (x_2, y_2) de birer çözümü olduğundan denkleminin toplam $p - 3 + 2 = p - 1$ tane tamsayı çözümü vardır.

2. Hal. $p \equiv 5, 11 \pmod{12}$ olsun. $\left(\frac{-3}{p}\right) = -1$ olduğundan $x^2 \equiv -3 \pmod{p}$ kuadratik kongrüansının çözümü yoktur. Burada yine iki durum söz konusudur.

i) $p \equiv 5 (\text{mod}\, 12)$ ise $\left(\frac{3}{p}\right) = -1$ olduğundan $x = 0$ için $y^2 - 3 \equiv 0 (\text{mod}\ p)$ kongrüansının çözümü yoktur. x in bu değeri Φ_p den çıkartılırsa $S_P = \Phi_p - \{0\}$ kümesi elde edilir. Bu takdirde $x^2 + 3 \equiv t^2 (\text{mod}\ p)$ kongrüansının çözümü olacak şekilde S_p de $\frac{p-1}{2}$ tane x değeri vardır ve x in bu değerleri için $y_{1,2} = x \pm t \ (\text{mod}\ p)$ çözümleri elde edilir. Şu halde S_p deki her bir x değeri için iki çözüm olduğundan denklemin $2\left(\frac{p-1}{2}\right) = p - 1$ tane çözümü vardır.

ii) $p \equiv 11 (\text{mod}\, 12)$ ise $\left(\frac{3}{p}\right) = 1$ dir. $x = 0$ ise $y^2 - 3 \equiv 0 (\text{mod}\ p)$ kongrüansının y_1 ve y_2 gibi iki tamsayı çözümü vardır. Bu ise verilen denklemin $(0, y_1)$ ve $(0, y_2)$ gibi iki tamsayı çözümünün olması demektir. x in bu değeri yine Φ_p den çıkartılırsa $L_p = \Phi_p - \{0\}$ kümesi elde edilir. Üstelik bu kümede $x^2 + 3 \equiv t^2 (\text{mod}\ p)$ kongrüansının çözümü olacak şekilde $\frac{p-3}{2}$ tane x değeri vardır ve x in bu değerleri için $y_{1,2} = x \pm t (\text{mod}\ p)$ çözümleri elde edilir. Dolayısıyla denklemin $2\left(\frac{p-3}{2}\right) = p - 3$ tane tamsayı çözümü vardır. $(0, y_1)$ ve $(0, y_2)$ de birer çözüm olduğundan denklemin toplam $p - 3 + 2 = p - 1$ tane tamsayı çözümü vardır.

3.1.3 Örnek. $p = 13,\ 17,\ 19$ ve 23 asalları için D_p Diophantine denkleminin tamsayı çözümlerinin kümesi sırasıyla aşağıdaki gibidir:

$$D_{13}(\Phi_{13}) = \left\{ \begin{matrix} (0,4),\ (0,9),\ (1,3),\ (1,12),\ (3,8),\ (3,11), \\ (6,6),\ (7,7),\ (10,2),\ (10,5),\ (12,1),\ (12,10) \end{matrix} \right\}$$

$$D_{17}(\Phi_{17}) = \left\{ \begin{matrix} (1,3),\ (1,16),\ (4,10),\ (4,15),\ (7,6),\ (7,8),\ (8,4),\ (8,12),\ (9,5), \\ (9,13),\ (10,9),\ (10,11),\ (13,2),\ (13,7),\ (16,1),\ (16,14) \end{matrix} \right\}$$

$$D_{19}(\Phi_{19}) = \left\{ \begin{matrix} (1,3),\ (1,18),\ (2,10),\ (2,13),\ (4,4),\ (5,2),\ (5,8),\ (6,5),\ (6,7),\ (13,12), \\ (13,14),\ (14,11),\ (14,17),\ (15,15),\ (17,6),\ (17,9),\ (18,1),\ (18,16) \end{matrix} \right\}$$

$$D_{23}(\Phi_{23}) = \left\{ \begin{matrix} (0,7),\ (0,16),\ (1,3),\ (1,22),\ (3,12),\ (3,17),\ (6,2),\ (6,10),\ (7,18), \\ (7,19),\ (11,8),\ (11,14),\ (12,9),\ (12,15),\ (16,4),\ (16,5),\ (17,13), \\ (17,21),\ (20,6),\ (20,11),\ (22,1),\ (22,20) \end{matrix} \right\}$$

3.2 Φ_p de Tanımlı Eğri Üzerindeki Rasyonel Noktalar

Bu bölümde bir önceki bölümde ele alınan D_p Diophantine denkleminin köklerine bağlı olarak bir polinom fonksiyon tanımlanacak ve bu fonksiyonun özellikleri verilecektir. Daha sonra bu polinoma bağlı olarak tanımlanacak olan eğri üzerindeki rasyonel noktaların sayıları, Φ_p cisminde belirlenecek ve son olarak elde edilen bu rasyonel noktaların $x-$ve $y-$koordinatları toplamları ile ilgili sonuç verilecektir. D_p Diophantine denkleminin köklerinin $y_1 = x + \sqrt{x^2+3}$ ve $y_2 = x - \sqrt{x^2+3}$ şeklinde olduğu hatırlanırsa, bu kökler yardımıyla $n \geq 1$ tamsayısı için

$$P_n(x) = y_1^n + y_2^n$$

fonksiyonu tanımlansın. Bu takdirde aşağıdaki teorem verilebilir.

3.2.1 Teorem. $P_n(x)$ fonksiyonu, tamsayılar halkasında bir polinom fonksiyondur. Yani her $n \geq 1$ tamsayısı için $P_n(x) \in Z[x]$ dir.

İspat. n çift tamsayı olsun. Bu takdirde Binom formülü gereği

$$\begin{aligned} P_n(x) &= (x+\sqrt{x^2+3})^n + (x-\sqrt{x^2+3})^n \\ &= \sum_{k=0}^{n} \binom{n}{k} (x)^{n-k} (\sqrt{x^2+3})^k + \sum_{k=0}^{n} \binom{n}{k} (x)^{n-k} (-\sqrt{x^2+3})^k \\ &= \left[\begin{matrix} \binom{n}{0} x^n + \binom{n}{1} x^{n-1} (\sqrt{x^2+3})^1 + \binom{n}{2} x^{n-2} (\sqrt{x^2+3})^2 + \cdots + \\ \binom{n}{n-1} x^1 (\sqrt{x^2+3})^{n-1} + \binom{n}{n} (\sqrt{x^2+3})^n \end{matrix} \right] \\ &\quad + \left[\begin{matrix} \binom{n}{0} x^n - \binom{n}{1} x^{n-1} (\sqrt{x^2+3})^1 + \binom{n}{2} x^{n-2} (\sqrt{x^2+3})^2 - \cdots - \\ \binom{n}{n-1} x^1 (\sqrt{x^2+3})^{n-1} + \binom{n}{n} (\sqrt{x^2+3})^n \end{matrix} \right] \end{aligned}$$

$$= 2\left[\binom{n}{0}x^n + \binom{n}{2}x^{n-2}(\sqrt{x^2+3})^2 + \cdots + \binom{n}{n}(\sqrt{x^2+3})^n\right]$$

$$= 2\sum_{i=0}^{\frac{n}{2}}\binom{n}{2i}x^{n-2i}(\sqrt{x^2+3})^{2i}$$

$$= 2\sum_{i=0}^{\frac{n}{2}}\binom{n}{2i}x^{n-2i}(x^2+3)^i$$

elde edilir. Benzer işlemler *n* nin tek olması halinde de yapılırsa

$$P_n(x) = 2\sum_{i=0}^{\frac{n-1}{2}}\binom{n}{2i}x^{n-2i}(x^2+3)^i$$

olduğu görülür. O halde $P_n(x) \in Z[x]$ dir.

Yukarıdaki teoremden aşağıdaki sonuç verilebilir.

3.2.2 Sonuç. $P_n(x)$ polinomu baş katsayısı 2^n olan *n.* dereceden bir polinom fonksiyondur ve $n \geq 1$ için $\left\lfloor \frac{n}{2} \right\rfloor$ terime sahiptir.

Şimdi bu polinom fonksiyon yardımıyla tanımlanacak olan eğri ile ilgili cebirsel özellikler ele alınabilir. $p \geq 5$ asalı için, bu polinom fonksiyonu yardımıyla eğri

$$E_p : y^2 \equiv P_p(x) \pmod{p}$$

olarak tanımlansın. Bu eğri üzerindeki rasyonel noktaların kümesi

$$E_p(\Phi_p) = \{(x, y) \in \Phi_p \times \Phi_p : y^2 \equiv P_p(x) \pmod{p}\}$$

ile gösterilirse aşağıdaki teorem verilebilir.

3.2.3 Teorem. E_p eğrisi için

$$\# E_p(\Phi_p) = p$$

dir.

İspat. Fermat ın küçük teoreminden $a^{p-1} = 1 (\text{mod } p)$ olduğu bilinmektedir. Diğer yandan

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1,7 \ (\text{mod } 8) \\ -1 & p \equiv 3,5 \ (\text{mod } 8) \end{cases}$$

dir. Teorem 3.2.1 e göre $P_n(x)$ polinom fonksiyonunun açık hali

$$P_p(x) = c_2 x^p + c_4 x^{p-2} + c_6 x^{p-4} + \cdots + c_{p-1} x^3 + c_{p+1} x$$

dir. Üstelik Sonuç 3.2.2 gereği $c_2 = 2^p$ olup $c_4, c_6, \cdots, c_{p-1}, c_{p+1}$katsayıları p çarpanı bulundurduklarından bu katsayılar mod p de sıfıra denk olurlar, yani

$$c_4, c_6, \cdots, c_{p-1}, c_{p+1} \equiv 0 (\text{mod } p)$$

dır. $c_2 = 2^p \equiv 2 (\text{mod } p)$ ve $x^p \equiv x (\text{mod } p)$ olduğu dikkate alınırsa yukarıdaki eşitlik

$$E_p : y^2 = P_p(x) \equiv 2x (\text{mod } p)$$

haline gelir. Burada iki hal söz konusudur:

1.Hal. $p \equiv 1,7 (\text{mod } 8)$ olsun. Bu takdirde $\left(\frac{2}{p}\right) = 1$ dir. Buna göre;

i) $\left(\frac{x}{p}\right) = 1$ ise $\left(\frac{2x}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{x}{p}\right) = 1 \cdot 1 = 1$ olduğundan $2x$ bir ikinci dereceden kalan, yani $2x \in Q_p$ dir. Şimdi $t \in \Phi_p$ olmak üzere $2x = t^2$ olsun. Buradan

$$y^2 \equiv 2x (\text{mod } p) \Leftrightarrow y^2 \equiv t^2 (\text{mod } p) \Leftrightarrow y \equiv \pm t (\text{mod } p)$$

olur. Bu $y^2 \equiv 2x (\text{mod } p)$ kongrüansının t ve $p - t$ gibi iki çözümünün olması demektir. O halde her bir $x \in Q_p$ için eğri üzerinde iki rasyonel nokta vardır. $\# Q_p = \frac{p-1}{2}$ olduğundan eğri üzerinde $2\left(\frac{p-1}{2}\right) = p - 1$ tane rasyonel nokta vardır. (0, 0) da eğri üzerinde olduğundan eğri üzerinde toplam p tane rasyonel nokta vardır, yani $\# E_p(\Phi_p) = p$ dir.

ii) $\left(\frac{x}{p}\right)=-1$ ise $\left(\frac{2x}{p}\right)=-1$ olduğundan 2, ikinci dereceden kalan değildir, yani $2x \notin Q_p$ dir. Dolayısıyla $y^2 \equiv 2x \pmod{p}$ kongrüansının çözümü olmadığından E_p eğrisi üzerinde rasyonel nokta yoktur.

2.Hal. $p \equiv 3,5 \pmod 8$ olsun. Bu takdirde $\left(\frac{2}{p}\right)=-1$ dir. Buna göre

i) $\left(\frac{x}{p}\right)=1$ ise $\left(\frac{2x}{p}\right)=-1$ olduğundan $y^2 \equiv 2x \pmod{p}$ kongrüansının çözümü yoktur. Bu ise eğri üzerinde rasyonel noktanın olmaması demektir.

ii) $\left(\frac{x}{p}\right)=-1$ ise $\left(\frac{2x}{p}\right)=1$ olduğundan yukarıdaki durumdan dolayı eğri üzerinde toplam p tane rasyonel nokta vardır.

3.2.4 Örnek. $p=17$ ve $p=19$ asalları için E_p üzerindeki rasyonel noktaların kümesi sırasıyla

$$E_p(\Phi_{17}) = \begin{Bmatrix} (0,0),\ (1,\pm 6),\ (2,\pm 2),\ (4,\pm 5),\ (8,\pm 4),\ (9,\pm 1),(13,\pm 3), \\ (15,\pm 8),\ (16,\pm 7) \end{Bmatrix}$$

$$E_p(\Phi_{19}) = \begin{Bmatrix} (0,0),\ (2,\pm 2),\ (3,\pm 5),\ (8,\pm 4),\ (10,\pm 1),\ (12,\pm 9),\ (13,\pm 8), \\ (14,\pm 3),\ (15,\pm 7),\ (18,\pm 6) \end{Bmatrix}$$

dır.

Şimdi eğri üzerindeki rasyonel noktaların $x-$ve $y-$koordinatları toplamları ele alınabilir. Bunun için

$$E_p{}^x(\Phi_p) = \{x \in \Phi_p : (x,y) \in E_p(\Phi_p)\} \text{ ve } E_p{}^y(\Phi_p) = \{y \in \Phi_p : (x,y) \in E_p(\Phi_p)\}$$

kümeleri tanımlansın ve bu kümelerdeki elemanların toplamları

$$\sum_{[x]} E_p^x(\Phi_p) \quad \text{ve} \quad \sum_{[y]} E_p^y(\Phi_p)$$

ile gösterilsin. Bu takdirde aşağıdaki teorem verilebilir.

3.2.5 Teorem. E_p üzerindeki rasyonel noktaların $x-$ve $y-$koordinatları toplamları için

$$\sum_{[x]} E_p^x(\Phi_p) = \frac{1}{12}\begin{cases} p^3 - p & p \equiv 1,7 \pmod 8 \\ -p^3 + 12p^2 - 11p & p \equiv 3,5 \pmod 8 \end{cases}$$

ve

$$\sum_{[y]} E_p^y(\Phi_p) = \frac{1}{2}\begin{cases} p^2 - p & p \equiv 1,7 \pmod 8, x \in Q_p \\ 0 & p \equiv 1,7 \pmod 8, x \notin Q_p \\ 0 & p \equiv 3,5 \pmod 8, x \in Q_p \\ p^2 - p & p \equiv 3,5 \pmod 8, x \notin Q_p \end{cases}$$

dir.

İspat: $U_p = \{1, 2, \cdots, p-1\}$ birimlerin kümesi için

$$\sum_{x \in U_p} x = \frac{p^2 - p}{2}$$

dır. Bu kümedeki her bir elemanın karelerinin alınmasıyla ikinci dereceden kalanların kümesi yani Q_p kümesi elde edilmiş olur. Bir önceki bölümde, Q_p deki elemanların toplamının

$$\sum_{x \in Q_p} x = \frac{p^3 - p}{24}$$

olduğu gösterilmişti. Şimdi $p \equiv 1,7 \pmod 8$ olsun. Bu takdirde bir önceki teorem gereği her bir $x \in Q_p$ için $2x$ bir ikinci dereceden kalan olup eğri üzerinde (x,t) ve $(x, p-t)$ gibi iki tane rasyonel nokta vardır. Bu rasyonel noktaların $x-$koordinatlarının toplamı $2x$ dir. Dolayısıyla eğri üzerindeki tüm (x, y) rasyonel noktaların $x-$koordinatlarının toplamı

$$\sum_{[x]} E_p^x(\Phi_p) = 2\sum_{x \in Q_p} x = \frac{p^3 - p}{12}$$

dır. $p \equiv 3,5 \pmod 8$ için her bir $x \in (U_p - Q_p)$ için $2x$ bir ikinci dereceden kalan olup bu x ler için eğri üzerinde (x,t) ve $(x, p-t)$ rasyonel noktaları vardır ve bu rasyonel noktaların $x-$koordinatları toplamı $2x$ dir. Dolayısıyla eğri üzerindeki tüm rasyonel noktaların $x-$koordinatları toplamı

$$\sum_{[x]} E_p^x(\Phi_p) = 2\left(\sum_{x \in U_p} x - \sum_{x \in Q_p} x \right) = \frac{-p^3 + 12p^2 - 11p}{12}$$

olur.

Noktaların $y-$koordinatları toplamı için $p \equiv 1,7 \pmod 8$ ve $x \in Q_p$ ise $2x$ ikinci dereceden bir kalan olup $y^2 \equiv 2x \pmod p$ kongrüansının t ve $p-t$ gibi iki çözümü vardır. Dolayısıyla eğri üzerinde iki rasyonel nokta olup bu rasyonel noktaların $y-$koordinatları toplamı p dir. $\#Q_p = (p-1)/2$ olduğundan $y-$lerin toplamı $\frac{p^2-p}{2}$ dir. $x \notin Q_p$ için $2x \notin Q_p$ olduğundan $y^2 \equiv 2x \pmod p$ kongrüansının çözümü yoktur. Dolayısıyla eğri üzerinde rasyonel nokta olmadığından bu toplam 0 dır. $p \equiv 3,5 \pmod 8$ ve $x \in Q_p$ için $2x \notin Q_p$ olduğundan $y^2 \equiv 2x \pmod p$ kongrüansının çözümü yoktur. Dolayısıyla eğri üzerinde rasyonel nokta olmadığından bu toplam 0 dır. $x \notin Q_p$ ise $2x$ bir ikinci dereceden kalan olup $y^2 \equiv 2x \pmod p$ kongrüansının t ve $p-t$ gibi iki çözümü vardır. Bu ise eğri üzerinde iki rasyonel nokta olması demektir. Bu rasyonel noktaların $y-$koordinatları toplamı p olup eğri üzerindeki tüm rasyonel noktaların $y-$koordinatlarının toplamı $p\left(\frac{p-1}{2}\right) = \frac{p^2-p}{2}$ olur.

4. KUADRATİK İDEALLER VE İNDEFİNİTE KUADRATİK FORMLAR

Bu bölümde kuadratik idealler ve indefinite kuadratik formlar ele alınacak bu iki kavram arasındaki ilişki verilecektir. Ayrıca bu bölümde iki farklı kuadratik ideal ele alınıp bu ideallerin özellikleri verildikten sonra bu ideallerin çarpımları ele alınacaktır. Bu bölümde son olarak bu ideallere karşılık gelen indefinite kuadratik formlar ele alınacak ve bu formların bazı cebirsel özellikleri verilecektir.

Mollin 2006, Quadratics isimli kitabında geniş bir şekilde kuadratik idealleri ele almıştır. $D \neq 1$ pozitif tam kare olmayan bir tamsayı olmak üzere *r* sayısı, $D \equiv 1 (\text{mod } 4)$ iken $r = 2$, diğer hallerinde $r = 1$ olarak tanımlansın. Bu takdirde $K = \Theta(\sqrt{\Delta})$, $\Delta = \frac{4D}{r^2}$ determinantlı bir kuadratik sayı cismidir. Bu sayı cisminin tamsayılar halkası O_Δ ile gösterilirse

$$O_\Delta = \{\alpha x + \beta y \mid x, y \in Z\}$$

olur. Bu takdirde her bir $w_\Delta \in O_\Delta$ elemanı $x, y \in Z$ ve $\alpha, \beta \in O_\Delta$ olmak üzere

$$w_\Delta = \alpha x + \beta y$$

şeklinde yazılabilir. Buradaki α, β ikilisine *K* için bir tam baz denir ve $I = [\alpha, \beta]$ ile gösterilir. $a, b, c \in Z$ ve $w_\Delta \in O_\Delta$ elemanı için $I = [a, b + cw_\Delta]$ olarak tanımlanırsa aşağıdaki teorem verilebilir.

4.1 Teorem (Mollin 2006). $I = [a, b + cw_\Delta]$ bir idealdir $\Leftrightarrow$ $c \mid b$, $c \mid a$ ve $ac \mid N(b + cw_\Delta)$ dir.

Giriş bölümünde kuadratik irrasyonellerden ve kuadratik ideallerden bahsedilmişti. Hatırlanacağı üzere izi $t = \delta + \overline{\delta}$ ve normu $n = \delta\overline{\delta}$ olan bir δ irrasyoneli verildiğinde $Q \mid (\delta + P)(\overline{\delta} + P)$ özelliğinde öyle *P* ve *Q* tamsayıları vardır ki $\gamma = \frac{P + \delta}{Q} \in \Theta(\delta)$ bir kuadratik irrasyonel olup bu kuadratik irrasyonele bir I_γ ideali ve $\Delta = t^2 - 4n$ determinantlı bir F_γ indefinite kuadratik formu karşılık gelir.

4.1 Kuadratik İdealler ve Bu İdeallerin Çarpımı

Bu bölümde iki özel kuadratik ideal ele alınacak ve bu ideallerin bazı özellikleri verildikten sonra bu iki idealin çarpımı elde edilecektir. $k \geq 2$ tamsayı olmak üzere

$$I_1 = [k,\ k-1+\sqrt{k^2+k+1}] \text{ ve } I_2 = [k+1,\ k+\sqrt{k^2+k+1}]$$

idealleri ele alınsın. Bu takdirde aşağıdaki sonuçlar verilebilir ki bunlar Tekcan, Özkoç ve Alkan 2010 dan alınmıştır.

4.1.1 Teorem. I_1 ve I_2 idealleri için

i) I_1 ideali her $k \geq 2$ tamsayısı için indirgenebilirdir.

ii) I_1 ideali ambiguoustur $\Leftrightarrow k = 2$ dir.

iii) $t \geq 1$ tamsayısı için $k = 3t+1$ formunda ise γ_1 kuadratik irrasyonelinin sürekli kesirli açılımı $\gamma_1 = [\overline{1,\ 1,\ 6t+2,\ 1,\ 1,\ 2t}]$ şeklinde olup I_1 in devri

$$I_1^0 = [3t+1,\ 3t+\sqrt{9t^2+9t+3}] \sim I_1^1 = [3t+2,\ 1+\sqrt{9t^2+9t+3}] \sim$$
$$I_1^2 = [1, 3t+1+\sqrt{9t^2+9t+3}] \sim I_1^3 = [3t+2,\ 3t+1+\sqrt{9t^2+9t+3}] \sim$$
$$I_1^4 = [3t+1,\ 1+\sqrt{9t^2+9t+3}] \sim I_1^5 = [3,\ 3t+\sqrt{9t^2+9t+3}]$$

dir.

iv) I_2 ideali her $k \geq 2$ tamsayısı için indirgenebilirdir.

v) I_2 ideali her $k \geq 2$ tamsayısı için ambiguous değildir.

vi) $t \geq 1$ tamsayısı için $k = 3t+1$ formunda ise γ_2 kuadratik irrasyonelinin sürekli kesirli açılımı $\gamma_2 = [\overline{1,\ 1,\ 2t,\ 1,\ 1,\ 6t+2}]$ şeklinde olup I_2 nin devri

$$I_2^0 = [3t+2,\ 3t+1+\sqrt{9t^2+9t+3}] \sim I_2^1 = [3t+1,\ 1+\sqrt{9t^2+9t+3}] \sim$$
$$I_2^2 = [3, 3t+\sqrt{9t^2+9t+3}] \sim I_2^3 = [3t+1,\ 3t+\sqrt{9t^2+9t+3}] \sim$$
$$I_2^4 = [3t+2,\ 1+\sqrt{9t^2+9t+3}] \sim I_2^5 = [1,\ 3t+1+\sqrt{9t^2+9t+3}]$$

dir.

İspat. i) $k \geq 2$ olduğundan $k^2+k+1>1$ olup buradan

$$k^2+k+1>1 \Leftrightarrow k^2+k+1>k^2+(k-1)^2-2k(k-1)$$
$$\Leftrightarrow D>Q_1^2+P_1^2-2P_1Q_1$$
$$\Leftrightarrow P_1+\sqrt{D}>Q_1$$

elde edilir. Diğer yandan

$$k^2+1<3k+k^2+1 \Leftrightarrow (k-1)^2<k^2+k+1 \Leftrightarrow P_1-\sqrt{D}<0$$

ve

$$4k^2-4k+1>k^2+k+1 \Leftrightarrow (k-1)^2+k^2+2k(k-1)>k^2+k+1$$
$$\Leftrightarrow P_1^2+Q_1^2+2P_1Q_1>D \Leftrightarrow P_1-\sqrt{D}>-Q_1$$

dir. O halde

$$P_1+\sqrt{D}>Q_1 \text{ ve } -Q_1<P_1-\sqrt{D}<0$$

olduğundan I_1 indirgenebilirdir.

ii) I_1 idealinin ambiguous olması için gerek ve yeter şart tanımdan dolayı $\frac{2P_1}{Q_1}$ in tamsayı olmasıdır. O halde $\frac{2P_1}{Q_1} \in Z \Leftrightarrow \frac{2k-2}{k}=2-\frac{2}{k} \in Z \Leftrightarrow k=2$ dir.

iii) $t \geq 1$ tamsayısı için $k=3t+1$ olsun. Bu takdirde aşağıdaki tablo elde edilir:

Tablo 4.1.1 I_1 idealinin devri

i	0	1	2	3	4	5
P_i	$3t$	1	$3t+1$	$3t+1$	1	$3t$
Q_i	$3t+1$	$3t+2$	1	$3t+2$	$3t+1$	3
m_i	1	1	$6t+2$	1	1	$2t$

Bu tabloya göre γ_1 in sürekli kesirli açılımı $\gamma_1=\overline{[1,\ 1,\ 6t+2,\ 1,\ 1,\ 2t]}$ ve I_1 idealinin devri

$$I_1^0=[3t+1,\ 3t+\sqrt{9t^2+9t+3}] \sim I_1^1=[3t+2,\ 1+\sqrt{9t^2+9t+3}] \sim$$
$$I_1^2=[1, 3t+1+\sqrt{9t^2+9t+3}] \sim I_1^3=[3t+2,\ 3t+1+\sqrt{9t^2+9t+3}] \sim$$

$$I_1^4 = [3t+1,\ 1+\sqrt{9t^2+9t+3}] \sim I_1^5 = [3,\ 3t+\sqrt{9t^2+9t+3}]$$

şeklindedir.

iv) $k \geq 2$ olduğundan $k^2+k>0$ olup buradan $k^2+k+1>1$ olur. Buradan

$$\begin{aligned} k^2+k+1 > 2k^2-2k^2+2k-2k+1 &\Leftrightarrow k^2+k+1>(k+1)^2+k^2-2k(k+1) \\ &\Leftrightarrow D > Q_2^2+P_2^2-2P_2Q_2 \\ &\Leftrightarrow P_2+\sqrt{D}>Q_2 \end{aligned}$$

elde edilir. Diğer yandan

$$k^2 < k^2+k+1 \Leftrightarrow P_2^2 < D \Leftrightarrow P_2-\sqrt{D}<0$$

ve

$$\begin{aligned} 3k^2+3k>0 &\Leftrightarrow k^2+k^2+2k+1+2k^2+2k>k^2+k+1 \\ &\Leftrightarrow k^2+(k+1)^2+2k(k+1)>k^2+k+1 \\ &\Leftrightarrow P_2^2+Q_2^2+2P_2Q_2>D \\ &\Leftrightarrow P_2-\sqrt{D}>-Q_2 \end{aligned}$$

olduğundan $P_2+\sqrt{D}>Q_2$ ve $-Q_2<P_2-\sqrt{D}<0$ olur. O halde I_2 indirgenebilirdir.

v) $\dfrac{2P_2}{Q_2}=\dfrac{2k}{k+1}=2-\dfrac{2}{k+1}$ hiçbir zaman tamsayı olmadığından I_2 ambiguous değildir.

vi) $t \geq 1$ tamsayısı için $k=3t+1$ olsun. Bu takdirde aşağıdaki tablo elde edilir:

Tablo 4.1.2 I_2 idealinin devri

i	0	1	2	3	4	5
P_i	$3t+1$	1	$3t$	$3t$	1	$3t+1$
Q_i	$3t+2$	$3t+1$	3	$3t+1$	$3t+2$	1
m_i	1	1	$2t$	1	1	$6t+2$

Bu tabloya göre $\gamma_2 = \overline{[1,\ 1,\ 2t,\ 1,\ 1,\ 6t+2]}$ olup I_2 nin devri

$$I_2^0 = [3t+2,\ 3t+1+\sqrt{9t^2+9t+3}] \sim I_2^1 = [3t+1,\ 1+\sqrt{9t^2+9t+3}] \sim$$

$$I_2^2 = [3,\ 3t+\sqrt{9t^2+9t+3}] \sim I_2^3 = [3t+1,\ 3t+\sqrt{9t^2+9t+3}] \sim$$

$$I_2^4 = [3t+2,\ 1+\sqrt{9t^2+9t+3}] \sim I_2^5 = [1,\ 3t+1+\sqrt{9t^2+9t+3}]$$

dir.

4.1.2 Sonuç. I_1^2 ve I_1^5, I_1 idealinin devrinde, I_2^2 ve I_2^5 ise I_2 idealinin devrindeki ambiguous ideallerdir.

Şimdi yukarıda ele alınan I_1 ve I_2 ideallerinin çarpımları ele alınabilir.

4.1.3 Teorem. I_1 ve I_2 ideallerinin çarpımı

$$I = [k^2+k,\ k^2+k-1+\sqrt{k^2+k+1}]$$

idealidir.

İspat. Giriş bölümünde verilen iki idealinin çarpımı tanımlanmıştı. Bu tanıma göre I_1 ve I_2 idealleri için

$$S = obeb(k, k+1, 2k-1) = 1 \quad \text{ve} \quad Q = \frac{Q_1 Q_2}{S^2} = k^2+k$$

dır. O halde

$$\begin{aligned} P &\equiv \frac{1}{S}\left[UQ_2P_1 + VQ_1P_2 + \frac{W}{2}(P_1P_2 + D)\right] \pmod{2Q} \\ &\equiv \left[U(k+1)(k-1) + V(k)(k) + \frac{W}{2}(k^2 - k + k^2 + k + 1)\right] \pmod{2(k^2+k)} \\ &\equiv \left[U(k^2-1) + Vk^2 + \frac{W}{2}(2k^2+1)\right] \pmod{2(k^2+k)} \end{aligned}$$

olur. Burada *U, V* ve *W* lar

$$U(k+1) + V(k) + \frac{W}{2}(2k-1) = 1$$

denklemini gerçekleyen tamsayılar olup bu denklemin çözümü $(U,V,W) = (1-k,\ k,\ 0)$ dır. O halde yukarıdaki eşitlik

$$P \equiv k^2+k-1 \pmod{(2k^2+k)} = k^2+k-1$$

olur. Dolayısıyla I_1 ve I_2 ideallerinin çarpımı $I = [k^2+k,\ k^2+k-1+\sqrt{k^2+k+1}]$ dır.

4.1.4 Örnek. $t=5$ için

$$\gamma_1=\frac{15+\sqrt{273}}{16}=[\overline{1,\ 1,\ 32,\ 1,\ 1,\ 10}]$$

olup $I_1=[16,15+\sqrt{273}]$ idealinin devri

$$I_1^0=[16,15+\sqrt{273}]\sim I_1^1=[17,1+\sqrt{273}]\sim\ I_1^2=[1,16+\sqrt{273}]\sim$$
$$I_1^3=[17,16+\sqrt{273}]\sim I_1^4=[16,1+\sqrt{273}]\sim I_1^5=[3,15+\sqrt{273}]$$

dir. Benzer şekilde

$$\gamma_2=\frac{16+\sqrt{273}}{17}=[\overline{1,\ 1,\ 10,\ 1,\ 1,\ 32}]$$

olup $I_2=[17,16+\sqrt{273}]$ idealinin devri

$$I_2^0=[17,16+\sqrt{273}]\sim I_2^1=[16,1+\sqrt{273}]\sim I_2^2=[3,15+\sqrt{273}]\sim$$
$$I_2^3=[16,15+\sqrt{273}]\sim I_2^4=[17,1+\sqrt{273}]\sim I_2^5=[1,16+\sqrt{273}]$$

dir. Üstelik I_1 ve I_2 ideallerinin çarpımı $I=[272,271+\sqrt{273}]$ idealidir.

4.1.5 Teorem. I çarpım ideali her $k\geq 2$ tamsayısı için indirgenemezdir ve ambiguous değildir.

İspat. $k\geq 2$ olduğundan

$$k^4+2k^3-2k^2-3k>0$$

dır. Buradan

$$\begin{aligned} k^4+2k^3-2k^2-3k>0 \quad &\Leftrightarrow \quad k^4+2k^3-k^2-2k+1>k^2+k+1 \\ &\Leftrightarrow \quad k^2+k-1>\sqrt{k^2+k+1} \\ &\Leftrightarrow \quad P>\sqrt{D} \\ &\Leftrightarrow \quad P-\sqrt{D}>0 \end{aligned}$$

elde edilir ki bu indirgenebilirlik tanımı ile çelişir. O halde I indirgenemezdir. Diğer yandan

$$\frac{2P}{Q}=\frac{2(k^2+k-1)}{k^2+k}=2-\frac{2}{k^2+k}\notin Z$$

olduğundan I ambiguous değildir.

4.2 İndefinite Kuadratik Formlar

Bu bölümde bir önceki bölümde ele alınan kuadratik ideallere karşılık gelen indefinite formlar ele alınacak ve bu formların bazı özellikleri verilecektir. Giriş bölümünde kuadratik irrasyoneller, kuadratik idealler ve indefinite formlar arasındaki ilişki verilmişti. Bu ilişkiye göre $\gamma = \frac{P+\sqrt{D}}{Q}$ kuadratik irrasyoneli için $I_\gamma = [Q, P+\sqrt{D}]$ bir kuadratik ideal ve $F_\gamma = (Q,\ 2P,\ \frac{P^2-D}{Q})$ da $4D$ determinantlı bir indefinite formdur. Dolayısıyla $I_1 = [k,\ k-1+\sqrt{k^2+k+1}]$ ve $I_2 = [k+1,\ k+\sqrt{k^2+k+1}]$ ideallerine karşılık gelen indefinite formlar sırasıyla

$$F_{I_1} = (k,\ 2k-2,\ -3) \text{ ve } F_{I_2} = (k+1,\ 2k,\ -1)$$

dır. Bu takdirde aşağıdaki teorem verilebilir.

4.2.1 Teorem. F_{I_1} ve F_{I_2} indefinite formları için

i) Her $k \geq 2$ tamsayısı için F_{I_1} indirgenebilir ve ambiguoustur.

ii) $t \geq 1$ tamsayısı için $k = 3t+1$ ise F_{I_1} in devri

$$F_{I_1^0} = (3t+1, 6t, -3) \sim F_{I_1^1} = (3, 6t, -3t-1) \sim F_{I_1^2} = (3t+1, 2, -3t-2) \sim$$

$$F_{I_1^3} = (3t+2, 6t+2, -1) \sim F_{I_1^4} = (1, 6t+2, -3t-2) \sim F_{I_1^5} = (3t+2, 2, -3t-1)$$

dir.

iii) Her $k \geq 2$ tamsayısı için F_{I_2} indirgenebilir ve ambiguoustur.

iv) $t \geq 1$ tamsayısı için $k = 3t+1$ ise F_{I_2} nin devri

$$F_{I_2^0} = (3t+2, 6t+2, -1) \sim F_{I_2^1} = (1, 6t+2, -3t-2) \sim F_{I_2^2} = (3t+2, 2, -3t-1) \sim$$

$$F_{I_2^3} = (3t+1, 6t, -3) \sim F_{I_2^4} = (3, 6t, -3t-1) \sim F_{I_2^5} = (3t+1, 2, -3t-2)$$

dir.

İspat. i) $k > 0$ olduğundan

$$4k+4 > -8k+4 \Leftrightarrow 4k^2+4k+4 > 4k^2-8k+4$$

$$\Leftrightarrow \sqrt{4k^2+4k+4} > 2k-2$$
$$\Leftrightarrow \sqrt{\Delta} > b_1$$

dır. Üstelik $k \geq 2$ olduğundan $4k+4>0$ dır. Buradan

$$4k+4>0 \Leftrightarrow 4k^2+4k+4>4k^2 \Leftrightarrow \sqrt{4k^2+4k+4}>2k$$

olur, yani $\sqrt{4k^2+4k+4}-2k>0$ dir. Diğer yandan $3k-5>0$ olduğunda

$$4k(3k-5)>0 \quad \Leftrightarrow \quad 12k^2-20k+4>4$$
$$\Leftrightarrow \quad 16k^2-20k+4>4k^2+4$$
$$\Leftrightarrow \quad b_1 > \left|\sqrt{\Delta}-2|a_1|\right|$$

olur. Buradan $\left|\sqrt{\Delta}-2|a_1|\right| < b_1 < \sqrt{\Delta}$ elde edilir. O halde F_{I_1} indirgenebilirdir.

$g=[p;q;u;v] \in \overline{\Gamma}$ elemanı ve $F_{I_1}=(k,\ 2k-2,\ -3)$ indefinite formu için

$$kp^2+(2k-2)pq-3q^2=k$$
$$2kpu+(2k-2)pv+(2k-2)uq-6qv=2k-2$$
$$ku^2+(2k-2)uv-3v^2=-3$$

denklem sisteminin bir çözümü, $p=1,\ q=0,\ u=0,\ v=-1$ dir. $\det g=-1$ olduğundan F_{I_1} kendisine has olmayan denk ve böylece ambiguoustur.

ii) $t \geq 1$ tamsayısı için $k=3t+1$ ise F_{I_1} formu için aşağıdaki tablo elde edilir:

Tablo 4.2.1 F_{I_1} formunun devri

i	0	1	2	3	4	5
i	$3t+1$	3	$3t+1$	$3t+2$	1	$3t+2$
b_i	$6t$	$6t$	2	$6t+2$	$6t+2$	2
c_i	-3	$-3t-1$	$-3t-2$	-1	$-3t-2$	$-3t-1$
s_i	$2t$	1	1	$6t+2$	1	1

Bu tabloya göre F_{I_1} indefinite formunun devri

$$F_{I_1^0}=(3t+1,6t,-3) \sim F_{I_1^1}=(3,6t,-3t-1) \sim F_{I_1^2}=(3t+1,2,-3t-2) \sim$$

$$F_{I_1^3} = (3t+2, 6t+2, -1) \sim F_{I_1^4} = (1, 6t+2, -3t-2) \sim F_{I_1^5} = (3t+2, 2, -3t-1)$$

dir.

iii) i) dekine benzer şekilde gösterilebilir.

iv) $t \geq 1$ tamsayısı için $k = 3t+1$ ise F_{I_2} formu için aşağıdaki tablo elde edilir:

Tablo 4.2.2 F_{I_2} formunun devri

i	0	1	2	3	4	5
i	$3t+2$	1	$3t+2$	$3t+1$	3	$3t+1$
b_i	$6t+2$	$6t+2$	2	$6t$	$6t$	2
c_i	-1	$-3t-2$	$-3t-1$	-3	$-3t-1$	$-3t-2$
s_i	$6t+2$	1	1	$2t$	1	1

Bu tabloya göre F_{I_2} nin devri

$$F_{I_2^0} = (3t+2, 6t+2, -1) \sim F_{I_2^1} = (1, 6t+2, -3t-2) \sim F_{I_2^2} = (3t+2, 2, -3t-1) \sim$$

$$F_{I_2^3} = (3t+1, 6t, -3) \sim F_{I_2^4} = (3, 6t, -3t-1) \sim F_{I_2^5} = (3t+1, 2, -3t-2)$$

dir.

4.2.2 Örnek. $t = 5$ olsun. Bu takdirde $k = 16$ olup $F_{I_1} = (16,\ 30,\ -3)$ formunun devri

$$F_{I_1^0} = (16,\ 30,\ -3) \sim F_{I_1^1} = (3, 30,\ -16) \sim F_{I_1^2} = (16,\ 2,\ -17) \sim$$

$$F_{I_1^3} = (17,\ 32,\ -1) \sim F_{I_1^4} = (1, 32,\ -17) \sim F_{I_1^5} = (17,\ 2,\ -16)$$

ve $F_{I_2} = (17,\ 32,\ -1)$ formunun devri ise

$$F_{I_2^0} = (17,\ 32,\ -1) \sim F_{I_2^1} = (1, 32,\ -17) \sim F_{I_2^2} = (17,\ 2,\ -16) \sim$$

$$F_{I_2^3} = (16,\ 30,\ -3) \sim F_{I_2^4} = (3, 30,\ -16) \sim F_{I_2^5} = (16,\ 2,\ -17)$$

dir.

4.2.3 Sonuç. Eğer $t \geq 1$ tamsayısı için $k = 3t+1$ ise F_{I_1} ve F_{I_2} indefinite formlarının devrindeki tüm formlar ambiguoustur.

$I = [k^2 + k, k^2 + k - 1 + \sqrt{k^2 + k + 1}]$ çarpım idealine karşılık gelen indefinite form

$$F_I = (k^2 + k,\ 2k^2 + 2k - 2,\ k^2 + k - 3)$$

olup bu form ile ilgili aşağıdaki teorem verilebilir.

4.2.4 Teorem. F_I indefinite formu indirgenemez, fakat ambiguoustur.

İspat. $k \geq 2$ olduğundan $k^3 + 2k^2 - 2k - 3 > 0$ dır. Buradan

$$\begin{aligned} 4k(k^3 + 2k^2 - 2k - 3) > 0 &\Leftrightarrow 4k^4 + 8k^3 - 8k^2 - 12k + (4k^2 + 4k + 4) > 4k^2 + 4k + 4 \\ &\Leftrightarrow 4k^4 + 8k^3 - 4k^2 - 8k + 4 > 4k^2 + 4k + 4 \\ &\Leftrightarrow 4(k^2 + k - 1)^2 > 4k^2 + 4k + 4 \\ &\Leftrightarrow 2(k^2 + k - 1) > \sqrt{4k^2 + 4k + 4} \\ &\Leftrightarrow b > \sqrt{\Delta} \end{aligned}$$

elde edilir. O halde F_I indirgenebilir değildir.

$g = [p; q; u; v] \in \overline{\Gamma}$ dönüşümü için

$$\begin{aligned} (k^2 + k)p^2 + 2(k^2 + k - 1)pq + (k^2 + k - 3)q^2 &= k^2 + k \\ 2(k^2 + k)pu + 2(k^2 + k - 1)(pv + uq) + 2(k^2 + k - 3)qv &= 2k^2 + 2k - 2 \\ (k^2 + k)u^2 + 2(k^2 + k - 1)uv + (k^2 + k - 3)v^2 &= k^2 + k - 3 \end{aligned}$$

sisteminin bir çözümü $p = 3$, $q = -2$, $u = 4$ ve $v = -3$ dür. $\det g = -1$ olduğundan F_I kendisine has olmayan denk ve böylece ambiguoustur.

5. ÖZEL TAMSAYI DİZİSİ VE PELL DENKLEMİ

Tamsayı dizileri sayılar teorisinde çok eski bir konu olup hala da günümüzde geçerliliğini koruyan bir konudur. En çok bilinen tamsayı dizisi, meşhur Fibonacci tamsayı dizisidir ki bu dizi ilk kez bir İtalyan matematikçi olan Leonardo Fibonacci, (1170-1250) tarafından ele alınmıştır. Aslında bu sayı dizisi 6. yüzyıldan itibaren Hintli matematikçiler tarafından bilinmesine rağmen Avrupa' da 13. yüzyılda Fibonacci tarafından ele alınmıştır. Bu sayı dizisi, $F_0 = 0, F_1 = 1$ ve tüm $n \geq 2$ için

$$F_n = F_{n-1} + F_{n-2}$$

indirgeme bağıntısı ile verilen bir sayı dizidir, yani dizinin terimi kendisinden önce gelen ilk iki terimin toplamı olarak tanımlanmaktadır. Buna göre dizinin ilk birkaç terimi

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377 , 610, 987, 1597, ⋯

şeklindedir. Bu sayı dizisinin karakteristik denklemi $x^2 - x - 1 = 0$ olup bu denklemin kökleri

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{ve} \quad \beta = \frac{1-\sqrt{5}}{2}$$

dir. Bu köklerden α olanı, altın orana karşılık gelmektedir ve yaklaşık değeri 1,618 dir. Üstelik $n \geq 2$ için $\lim_{n\to\infty} \frac{F_n}{F_{n-1}} = \alpha$ dır. Fibonacci sayıları Binet formülü olarak ta bilinen

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

formülü ile verilebilir. Fibonacci sayıları ile ilgili yüzlerce bağıntı bulunmakta olup bu bağıntılardan bazıları aşağıdaki gibidir:

$$\sum_{i=1}^{n} F_i = F_n + F_{n-1} - 1$$

$$\sum_{i=1}^{n} F_{2i} = F_{2n+1} - 1$$

$$\sum_{i=1}^{n} F_{2i-1} = F_{2n}$$

$$\sum_{i=0}^{n} \binom{n}{i} F_i = F_{2n}$$

$$\sum_{i=0}^{n} \binom{n}{i} 2^i F_i = F_{3n}$$

Ayrıca dizinin terimleri arasında

$$F_{2n} = F_{n+1}^2 - F_{n-1}^2 = F_n(F_{n+1} + F_{n-1}) = F_n(F_n + 2F_{n-1})$$
$$F_{2n+1} = F_{n+1}^2 + F_n^2$$
$$F_{3n} = F_{n+1}^3 + F_n^3 - F_{n-1}^3$$
$$F_{n+2}^2 - F_{n+1}^2 = F_n F_{n+3}$$
$$F_n^2 = F_{n-1}^2 + 3F_{n-2}^2 + 2F_{n-2}F_{n-3}$$
$$F_{n+1}^2 = 4F_n F_{n-1} + F_{n-2}^2$$
$$F_n^2 + F_{n-1}^2 = F_{2n-1}$$
$$F_{n+1}F_m + F_n F_{m-1} = F_{m+n}$$
$$F_{2n} = 3F_{2n-2} - F_{2n-4}$$
$$F_{2n+1} = 3F_{2n-1} - F_{2n-3}$$
$$F_{-n} = (-1)^{n+1}F_n$$

şeklinde indirgeme bağıntıları vardır. Diğer önemli bir tamsayı dizisi Lucas tamsayı dizisi olup bu dizi de ilk olarak bir Fransız matematikçi olan François Édouard Anatole Lucas (1842–1891) tarafından ele alınmıştır. Bu sayı dizisi, Fibonacci sayı dizisine benzemekle birlikte başlangıç değerleri farklı olan bir sayı dizisidir ve $L_0 = 2, L_1 = 1$ ve tüm $n \geq 2$ için $L_n = L_{n-1} + L_{n-2}$ şeklinde tanımlanmaktadır. Bu dizinin ilk birkaç terimi

2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, ⋯

dir. Bu dizinin karakteristik denklemi ve bu denklemin kökleri Fibonacci sayı dizisi ile aynı olup dizinin *n*. terimi $L_n = \alpha^n + \beta^n$ Binet formülü ile verilebilir.

Fibonacci ve Lucas sayıları arasında bir çok cebirsel bağıntı olup bunlardan bazıları:

$$F_{m+n} = \frac{F_m L_n + L_m F_n}{2},\ L_n^2 - 5F_n^2 = 4(-1)^n,\ L_n = F_{n-1} + F_{n+1} \text{ ve } F_{2n} = F_n L_n$$

şeklindedir. Başka bir tamsayı dizisi Pell tamsayı dizisi olup bu dizi de ilk olarak bir İngiliz matematikçi olan John Pell (1611 –1685) tarafından çalışılmıştır. Başlangıç değerleri Fibonacci sayı dizisine benzemekle birlikte, dizinin genel terimindeki katsayı farkı yüzünden bu dizisinden farklıdır ve $P_0 = 0, P_1 = 1$ ve $n \geq 2$ için $P_n = 2P_{n-1} + P_{n-2}$ şeklinde tanımlanan bir tamsayı dizisidir. Bu dizinini ilk birkaç terimi

0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, ⋯

şeklindedir. Bu dizinin karakteristik denklemi $x^2 - 2x - 1 = 0$ olup bu denklemin kökleri $x_{1,2} = 1 \pm \sqrt{2}$ dir. Dolayısıyla dizinin herhangi bir *n*.terimi Binet formülünden

$$P_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}$$

elde edilebilir. Bu sayı dizilerinden başka, Pell-Lucas, Jacobsthal ve Pell-Jacobsthal sayı dizileri de en önemli sayı dizileridir.

Bu sayı dizilerinin daha genel hali şu şekildedir: P ve Q, $P^2 - 4Q \neq 0$ özelliğinde iki tamsayı olmak üzere bu iki parametreye bağlı ve

$$U_0 = 0, U_1 = 1 \quad \text{ve} \quad V_0 = 2, V_1 = P$$

başlangıç değerleri verilen tamsayı dizileri $n \geq 2$ için

$$U_n = U_n(P,Q) = PU_{n-1} - QU_{n-2}$$

ve

$$V_n = V_n(P,Q) = PV_{n-1} - QV_{n-2}$$

şeklindedir. Bu dizilerinin karakteristik denklemi $x^2 - Px + Q = 0$ olup bu denklemin kökleri

$$x_{1,2} = \frac{P \pm \sqrt{P^2 - 4Q}}{2}$$

dir. Dolayısıyla dizilerin *n*. terimi Binet formülü gereği

$$U_n = \frac{x_1^n - x_2^n}{x_1 - x_2} \quad \text{ve} \quad V_n = x_1^n + x_2^n$$

dir. Bu tamsayı dizileri için aşağıdaki tablo elde edilir:

Tablo 5.1 Tamsayı Dizileri

P	Q	U_n	V_n
1	-1	Fibonacci sayı dizisi	Lucas sayı dizisi
2	-1	Pell sayı dizisi	Pell-Lucas sayı dizisi
1	-2	Jacobsthal sayı dizisi	Pell-Jacobsthal sayı dizisi

Bu U_n ve V_n tamsayı dizileri için

$$M = \begin{bmatrix} P & -Q \\ 1 & 0 \end{bmatrix}$$

matrisi tanımlanırsa

$$\begin{bmatrix} U_n \\ U_{n-1} \end{bmatrix} = M^{n-1}\begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{ve} \quad \begin{bmatrix} V_n \\ V_{n-1} \end{bmatrix} = M^{n-1}\begin{bmatrix} P \\ 2 \end{bmatrix}$$

olur. Üstelik $D = P^2 - 4Q$ için bu iki tamsayı dizisi

$$V_n^2 - DU_n^2 = 4Q^n$$
$$U_{n+1}^2 - PU_{n+1}U_n + QU_n^2 = Q^n$$
$$DU_n = V_{n+1} - QV_{n-1}$$
$$V_n = U_{n+1} - QU_{n-1}$$

indirgeme bağıntılarını,

$$U_{m+n} = U_m V_n - Q^n U_{m-n}$$
$$V_{m+n} = V_m V_n - Q^n V_{m-n} = DU_m U_n + Q^n V_{m-n}$$
$$2U_{m+n} = U_m V_n + U_n V_m$$
$$2Q^n U_{m-n} = U_m V_n - U_n V_m$$

toplamsal bağıntılarını ve

$$U_{2n} = U_n V_n$$
$$V_{2n} = V_n^2 - 2Q^n$$
$$U_{3n} = U_n(V_n^2 - Q^n) = U_n(DU_n^2 + 3Q^n)$$
$$V_{3n} = V_n(V_n^2 - 3Q^n)$$

çarpımsal bağıntılarını gerçekler (Daha fazla bilgi için Mollin 2008, 2009 ve Ribenboim 2000 e bakılabilir).

5.1 Özel Tamsayı Dizisi

Bu bölümde Tekcan, Özkoç ve ark. 2011 in $U_n = PU_{n-1} - QU_{n-2}$ tamsayı dizisine benzer şekilde tanımladıkları tamsayı dizisi ile ilgili elde ettiği sonuçlar verilecektir.

5.1.1 Teorem $P, Q \in Z^+$ için her bir $p \equiv 1 (\text{mod } 4)$ asal sayısı $P^2 - 4Q$ formunda yazılabilir.

İspat. $p \equiv 1 (\text{mod } 4)$ asal sayı ise $k \in Z^+$ için $p = 1 + 4k$ olup

$$p = P^2 - 4Q$$

denkleminin bir çözümü $(P,Q)=(2k+1,\ k^2)$ dir. O halde her bir $p\equiv 1(\text{mod } 4)$ asalı P^2-4Q formunda yazılabilir.

$p\geq 5$, $p\equiv 1(\text{mod } 4)$ özelliğinde bir asal sayı olsun. Bu takdirde *P* ve *Q* yukarıdaki gibi olmak üzere Tekcan, Özkoç ve ark. 2011, $A_{k,n}$ tamsayı dizisini, $A_{k,0}=0$, $A_{k,1}=1$ ve tüm $n\geq 2$ için

$$A_{k,n}=PA_{k,n-1}-QA_{k,n-2}=(2k+1)A_{k,n-1}-k^2A_{k,n-2}$$

olarak tanımlamışlardır. Bu eşitliğin karakteristik denklemi $x^2-Px+Q=0$ olup denklemin kökleri

$$\alpha=\frac{2k+1+\sqrt{p}}{2} \quad \text{ve} \quad \beta=\frac{2k+1-\sqrt{p}}{2}$$

dir. Dolayısıyla Binet formülü gereği her $n\geq 1$ için $A_{k,n}=\dfrac{\alpha^n-\beta^n}{\alpha-\beta}$ dir.

5.1.2 Teorem. $A_{k,n}$ dizisinin ilk $n-$terim toplamı

$$\sum_{i=1}^{n}A_{k,n}=\frac{A_{k,n+1}-k^2A_{k,n}-1}{2k-k^2}$$

dir.

İspat. $A_{k,n}=PA_{k,n-1}-QA_{k,n-2}=(2k+1)A_{k,n-1}-k^2A_{k,n-2}$ dizisi için

$$A_{k,n+2}=(2k+1)A_{k,n+1}-k^2A_{k,n}=2kA_{k,n+1}+A_{k,n+1}-k^2A_{k,n}$$

olduğundan $A_{k,n+2}-A_{k,n+1}=2kA_{k,n+1}-k^2A_{k,n}$ elde edilir. Bu son eşitlikte *n* yerine 0 dan *n* ye kadar değerler verilirse ve denklem taraf tarafa toplanırsa

$$A_{k,n+2}-A_{k,1}=(2k-k^2)(A_{k,1}+A_{k,2}+\cdots+A_{k,n})+2kA_{k,n+1}-k^2A_{k,0}$$

elde edilir. $A_{k,0}=0$ ve $A_{k,1}=1$ olduğundan bu son eşitlik

$$A_{k,n+2}-1=(2k-k^2)(A_{k,1}+A_{k,2}+\cdots+A_{k,n})+2kA_{k,n+1}$$

haline gelir. Buradan

$$A_{k,1} + A_{k,2} + \cdots + A_{k,n} = \frac{A_{k,n+2} - 2kA_{k,n+1} - 1}{2k - k^2}$$

olur. Bu son eşitlikte $A_{k,n+2} \to (2k+1)A_{k,n+1} - k^2 A_{k,n}$ değişken değişimi yapılırsa istenilen sonuç görülür.

5.1.3 Teorem. $A_{k,n}$ dizisi her $n \geq 2$ tamsayısı için

$$A_{k,2n} = (2k^2 + 4k + 1)A_{k,2n-2} - k^4 A_{k,2n-4}$$

$$A_{k,2n+1} = (2k^2 + 4k + 1)A_{k,2n-1} - k^4 A_{k,2n-3}$$

indirgeme bağıntılarını gerçekler.

İspat. $A_{k,2n} = (2k+1)A_{k,2n-1} - k^2 A_{k,2n-2}$ olduğu hatırlanırsa

$$\begin{aligned}
A_{k,2n} &= (2k+1)A_{k,2n-1} - k^2 A_{k,2n-2} \\
&= (2k+1)[(2k+1)A_{k,2n-2} - k^2 A_{k,2n-3}] - k^2 A_{k,2n-2} \\
&= A_{k,2n-2}[(2k+1)^2 k^2] - k^2(2k+1)A_{k,2n-3} \\
&= A_{k,2n-2}[(2k+1)^2 - k^2] - k^2(2k+1)[(2k+1)A_{k,2n-4} - k^2 A_{k,2n-5}] \\
&= A_{k,2n-2}[(2k+1)^2 - k^2] - k^2(2k+1)^2 A_{k,2n-4} + k^4(2k+1)A_{k,2n-5} \\
&= A_{k,2n-2}[(2k+1)^2 - k^2] - k^2 A_{k,2n-2} + k^2 A_{k,2n-2} - k^2(2k+1)^2 A_{k,2n-4} \\
&\quad + k^4(2k+1)A_{k,2n-5} \\
&= A_{k,2n-2}[(2k+1)^2 - 2k^2] + k^2[(2k+1)A_{k,2n-3} - k^2 A_{k,2n-4}] - k^2(2k+1)^2 A_{k,2n-4} \\
&\quad + k^4(2k+1)A_{k,2n-5} \\
&= A_{k,2n-2}[(2k+1)^2 - 2k^2] + k^2(2k+1)A_{k,2n-3} - k^4 A_{k,2n-4} - k^2(2k+1)^2 A_{k,2n-4} \\
&\quad + k^4(2k+1)A_{k,2n-5} \\
&= A_{k,2n-2}[(2k+1)^2 - 2k^2] + A_{k,2n-4}[k^2(2k+1)^2 - k^4 - k^2(2k+1)^2] \\
&\quad + A_{k,2n-5}[-k^4(2k+1) + k^2(2k+1)] \\
&= A_{k,2n-2}[(2k+1)^2 - 2k^2] - k^4 A_{k,2n-4}
\end{aligned}$$

elde edilir. Diğer ifade de benzer şekilde gösterilebilir.

5.1.4 Teorem. $A_{k,n}$ dizisi için

$$A_{k,n}=\frac{1}{2^{n-1}}\begin{cases}\sum_{i=1}^{\frac{n-2}{2}}\binom{n}{2i+1}(2k+1)^{n-(2i+1)}(4k+1)^{i} & n\ çift\ iken\\ \sum_{i=1}^{\frac{n-1}{2}}\binom{n}{2i+1}(2k+1)^{n-(2i+1)}(4k+1)^{i} & n\ tek\ iken\end{cases}$$

ve

$$A_{k,n}=\begin{cases}\sum_{i=0}^{\frac{n-2}{2}}\binom{n-1-i}{i}(-1)^{i}(2k+1)^{n-(2i+1)}k^{2i} & n\ çift\ iken\\ \sum_{i=0}^{\frac{n-1}{2}}\binom{n-1-i}{i}(-1)^{i}(2k+1)^{n-(2i+1)}k^{2i} & n\ tek\ iken\end{cases}$$

dir.

İspat. Binet formülünden görülür.

5.1.5 Teorem. Her $n\geq 1$ tamsayısı için

$$\alpha^{n}+\beta^{n}=\begin{cases}A_{k,n+1}-k^{2}A_{k,n-1}\\ 2A_{k,n+1}-(2k+1)A_{k,n}\\ (2k+1)A_{k,n}-2k^{2}A_{k,n-1}\end{cases}$$

dir.

İspat. $A_{k,n+1}=(2k+1)A_{k,n}-k^{2}A_{k,n-1}$ olduğu dikkate alınırsa

$$\begin{aligned}A_{k,n+1}-k^{2}A_{k,n-1}&=[(2k+1)A_{k,n}-k^{2}A_{k,n-1}]-2k^{2}A_{k,n-1}\\ &=(2k+1)A_{k,n}-2k^{2}A_{k,n-1}\\ &=(2k+1)\left(\frac{\alpha^{n}-\beta^{n}}{\alpha-\beta}\right)-2k^{2}\left(\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}\right)\\ &=\frac{2k+1}{\sqrt{4k+1}}(\alpha^{n}-\beta^{n})-\frac{2k^{2}}{\sqrt{4k+1}}\left(\frac{\alpha^{n}}{\alpha}-\frac{\beta^{n}}{\beta}\right)\\ &=\alpha^{n}+\beta^{n}\end{aligned}$$

elde edilir. Diğerleri de benzer şekilde gösterilebilir.

Şimdi $P = 2k+1$ ve $Q = k^2$ sayıları için

$$M = \frac{P - 2Q + \sqrt{D}}{2\sqrt{D}},\ N = P - Q - 1,\ H = \frac{P + 2 + \sqrt{D}}{2\sqrt{D}},\ L = \frac{2Q - P + \sqrt{D}}{2Q\sqrt{D}},$$

$$K = \frac{PQ + 4P + 8Q - 2 + (3Q + 2P)\sqrt{D}}{2\sqrt{D}}$$

sayıları tanımlansın. Bu takdirde aşağıdaki teorem verilebilir.

5.1.6 Teorem. $A_{k,n}$ dizisi için

i. $\sum_{i=1}^{n} A_{k,n} = \frac{1}{N}[M\alpha^n - \overline{M}\beta^n - 1]$ dir.

ii. $n \geq 0$ için $A_{k,n} + A_{k,n+1} = H\alpha^n - \overline{H}\beta^n$ dır.

iii. $n \geq 2$ için $A_{k,n+1} + A_{k,n-1} = K\alpha^{n-2} - \overline{K}\beta^{n-2}$ dir.

iv. $n \geq 1$ için $A_{k,n} - A_{k,n-1} = L\alpha^n - \overline{L}\beta^n$ dir.

İspat. i. $A_{k,k+1} - k^2 A_{k,n-1} = \alpha^n + \beta^n$ eşitliğinde $n \to n+1$ değişken değişimi yapılırsa

$$\begin{aligned}\alpha^{n+1} + \beta^{n+1} &= A_{k,n+2} - k^2 A_{k,n} = (2k+1)A_{k,n+1} - 2k^2 A_{k,n} \\ &= (A_{k,n+1} - k^2 A_{k,n}) + 2kA_{k,n+1} - k^2 A_{k,n}\end{aligned}$$

olur. Buradan

$$\begin{aligned}A_{k,n+1} - k^2 A_{k,n} &= \alpha^{n+1} + \beta^{n+1} - 2kA_{k,n+1} + k^2 A_{k,n} \\ &= \alpha^{n+1} + \beta^{n+1} - 2k\left(\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta}\right) + k^2\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right) \\ &= \alpha^n\left(\alpha - \frac{2k\alpha}{\sqrt{4k+1}} + \frac{k^2}{\sqrt{4k+1}}\right) + \beta^n\left(\beta + \frac{2k\beta}{\sqrt{4k+1}} - \frac{k^2}{\sqrt{4k+1}}\right) \\ &= \alpha^n\left(\frac{2k+1-2k^2+\sqrt{4k+1}}{2\sqrt{4k+1}}\right) - \beta^n\left(\frac{2k+1-2k^2-\sqrt{4k+1}}{2\sqrt{4k+1}}\right) \\ &= \alpha^n\left(\frac{P - 2Q + \sqrt{D}}{2\sqrt{D}}\right) - \beta^n\left(\frac{P - 2Q - \sqrt{D}}{2\sqrt{D}}\right) \\ &= M\alpha^n + \overline{M}\beta^n\end{aligned}$$

elde edilir. Buna göre Teorem 5.1.2 den istenilen sonuç görülür.

ii. $A_{k,n+1} = (2k+1)A_{k,n} - k^2 A_{k,n-1}$ olup buradan

$$A_{k,n+1} - (2k+1)A_{k,n} = -k^2 A_{k,n-1} \Leftrightarrow A_{k,n+1} - 2kA_{k,n} - 2A_{k,n} + A_{k,n} = -k^2 A_{k,n-1}$$

$$\Leftrightarrow A_{k,n+1} + A_{k,n} - (2k+2)A_{k,n} = -k^2 A_{k,n-1}$$

$$\Leftrightarrow A_{k,n+1} + A_{k,n} = (2k+2)A_{k,n} - k^2 A_{k,n-1}$$

$$\Leftrightarrow A_{k,n+1} + A_{k,n} = (2k+2)\left(\frac{\alpha^n - \beta^n}{\sqrt{D}}\right) + k^2\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\sqrt{D}}\right)$$

$$\Leftrightarrow A_{k,n+1} + A_{k,n} = \left(\frac{2k+3+\sqrt{D}}{2\sqrt{D}}\right)\alpha^n + \left(\frac{2k+3-\sqrt{D}}{2\sqrt{D}}\right)\beta^n$$

$$\Leftrightarrow A_{k,n+1} + A_{k,n} = \left(\frac{P+2+\sqrt{D}}{2\sqrt{D}}\right)\alpha^n + \left(\frac{P+2-\sqrt{D}}{2\sqrt{D}}\right)\beta^n$$

$$\Leftrightarrow A_{k,n+1} + A_{k,n} = H\alpha^n + \overline{H}\beta^n$$

elde edilir. Diğerleri de benzer şekilde gösterilebilir.

$A_{k,n}$ tamsayı dizisi için

$$M(A_{k,n}) = \begin{bmatrix} 2k+1 & -k^2 \\ 1 & 0 \end{bmatrix} \quad \text{ve} \quad W(A_{k,n}) = \begin{bmatrix} 2k+1 & 1 \\ 1 & 0 \end{bmatrix}$$

matrisleri tanımlanırsa

$$\begin{bmatrix} A_{k,n} \\ A_{k,n-1} \end{bmatrix} = M(A_{k,n})^{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

olduğu açıktır. *W* matrisi için aşağıdaki teorem verilebilir.

5.1.7 Teorem. $A_{k,n}$ dizisi verilsin. Bu takdirde her $n \geq 1$ tamsayısı için

$$\begin{bmatrix} A_{k,n+1} & A_{k,n} \\ A_{k,n} & A_{k,n-1} \end{bmatrix} = M(A_{k,n})^{n-1} W(A_{k,n})$$

dir.

İspat. $n = 1$ için

$$\begin{bmatrix} A_{k,2} & A_{k,1} \\ A_{k,1} & A_{k,0} \end{bmatrix} = W(A_{k,n}) = \begin{bmatrix} A_{k,2} & A_{k,1} \\ A_{k,1} & A_{k,0} \end{bmatrix}$$

olup eşitlik doğrudur. Kabul edilsin ki eşitlik $n-1$ için doğrudur. Bu takdirde

$$\begin{bmatrix} A_{k,n+1} & A_{k,n} \\ A_{k,n} & A_{k,n-1} \end{bmatrix} = M(A_{k,n})^{n-1} W(A_{k,n})$$

$$= M(A_{k,n}) \begin{bmatrix} A_{k,n} & A_{k,n-1} \\ A_{k,n-1} & A_{k,n-2} \end{bmatrix}$$

$$= \begin{bmatrix} (2k+1)A_{k,n} - k^2 A_{k,n-1} & (2k+1)A_{k,n-1} - k^2 A_{k,n-2} \\ A_{k,n} & A_{k,n-1} \end{bmatrix}$$

olduğundan eşitlik her n için doğrudur.

5.1.8 Sonuç. $A_{k,n}$ dizisi verilsin. Buna göre $n \geq 1$ için $A_{k,n-1}A_{k,n+1} - A_{k,n}^2 = (-1)^n$ dir ve $n \geq 0$ için $A_{k,n+1}^2 - (2n+1)A_{k,n+1}A_{k,n} + k^2 A_{k,n}^2 = (-1)^{n+1} k^2$ dir.

Hatırlanacağı üzere a,b,c,d sayılarının çapraz oranı

$$[a,b;c,d] = \frac{(a-b)(c-d)}{(b-c)(d-a)}$$

olarak tanımlanmaktadır. Şimdi ardışık $A_{k,n}, A_{k,n+1}, A_{k,n+2}$ ve $A_{k,n+3}$ terimlerinin çapraz oranlarının limitleri ile ilgili olarak aşağıdaki teorem verilebilir.

5.1.9 Teorem. $A_{k,n}, A_{k,n+1}, A_{k,n+2}$ ve $A_{k,n+3}$ terimleri için

$$R = 2k^2 + 12k + 4,\ S = 4k + 4,\ T = 12k^3 + 23k^2 + 34k + 13 \text{ ve } U = 5k^2 + 16k + 11$$

olmak üzere

$$\lim_{n\to\infty} [A_{k,n}, A_{k,n+1}; A_{k,n+2}, A_{k,n+3}] = \begin{cases} \dfrac{-1}{4} & p = 5 \ \textit{iken} \\ \dfrac{-R - S\sqrt{p}}{T + U\sqrt{p}} & p > 5 \ \textit{iken} \end{cases}$$

dir.

İspat. $p = 5$ için $k = 1$ olup $A_{1,n} = 3A_{1,n-1} - A_{1,n-2}$ dir. Dolayısıyla

$$A_{1,n+2} = 3A_{1,n+1} - A_{1,n}$$
$$A_{1,n+3} = 3A_{1,n+2} - A_{1,n+1} = 3[3A_{1,n+1} - A_{1,n}] - A_{1,n+1} = 83A_{1,n+1} - 3A_{1,n}$$

olup çapraz oran tanımından

$$[A_{1,n}, A_{1,n+1}; A_{1,n+2}, A_{1,n+3}] = \frac{(A_{1,n} - A_{1,n+1})(A_{1,n+2} - A_{1,n+3})}{(A_{1,n+1} - A_{1,n+2})(A_{1,n+3} - A_{1,n})}$$

$$= \frac{(A_{1,n} - A_{1,n+1})[(3A_{1,n+1} - A_{1,n}) - (8A_{1,n+1} - 3A_{1,n})]}{[A_{1,n+1} - (3A_{1,n+1} - A_{1,n})][(8A_{1,n+1} - 3A_{1,n}) - A_{1,n}]}$$

$$= \frac{(A_{1,n} - A_{1,n+1})(-5A_{1,n+1} + 2A_{1,n})}{4(-2A_{1,n+1} + A_{1,n})(A_{1,n+1} - A_{1,n})}$$

olur. Diğer yandan

$$A_{1,n+1} = \frac{\left(\frac{3+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{3-\sqrt{5}}{2}\right)^{n+1}}{\sqrt{5}} \text{ ve } A_{1,n} = \frac{\left(\frac{3+\sqrt{5}}{2}\right)^{n} - \left(\frac{3-\sqrt{5}}{2}\right)^{n}}{\sqrt{5}}$$

olduğu hatırlanır ve her iki tarafının limiti alınırsa

$$\lim_{n\to\infty}[A_{1,n}, A_{1,n+1}; A_{1,n+2}, A_{1,n+3}] = \frac{-1}{4}$$

elde edilir.

$p \geq 7$ için $A_{k,n}, A_{k,n+1}, A_{k,n+2}$ ve $A_{k,n+3}$ ardışık dört tamsayının çapraz oranı

$$[A_{k,n}, A_{k,n+1}; A_{k,n+2}, A_{k,n+3}] = \frac{(A_{k,n} - A_{k,n+1})(A_{k,n+2} - A_{k,n+3})}{(A_{k,n+1} - A_{k,n+2})(A_{k,n+3} - A_{k,n})}$$

dır. Diğer yandan $A_{k,n} = (2k+1)A_{k,n-1} - k^2 A_{k,n-2}$ olduğundan

$$A_{k,n+2} = (2k+1)A_{k,n+1} - k^2 A_{k,n}$$

$$A_{k,n+3} = (2k+1)A_{k,n+2} - k^2 A_{k,n+1} = (3k^2 + 4k + 1)A_{k,n+1} - (2k^3 + k^2)A_{k,n}$$

$$A_{k,n+2} - A_{k,n+3} = (-3k^2 - 2k)A_{k,n+1} - 2k^3 A_{k,n}$$

$$A_{k,n+3} - A_{k,n} = (3k^2 + 4k + 1)A_{k,n+1} - (2k^3 + k^2 + 1)A_{k,n}$$

bulunur. O halde yukarıdaki eşitlik

$$[A_{k,n}, A_{k,n+1}; A_{k,n+2}, A_{k,n+3}]$$

$$= \frac{(A_{k,n} - A_{k,n+1})[(-3k^2 - 2k)A_{k,n+1} + 2k^3 A_{k,n}]}{[-2A_{k,n+1} + k^2 A_{k,n}][(3k^2 + 4k + 1)A_{k,n+1} - (2k^3 + k^2 + 1)A_{k,n}]}$$

$$= \frac{(A_{k,n} - A_{k,n+1})[(-3k - 2)A_{k,n+1} + 2k^2 A_{k,n}]}{(-2A_{k,n+1} + kA_{k,n})[(3k^2 + 4k + 1)A_{k,n+1} - (2k^3 + k^2 + 1)A_{k,n}]}$$

$$= \frac{(A_{k,n} - A_{k,n+1})[(-3k - 2)A_{k,n+1} + 2k^2 A_{k,n}]}{(k+1)(-2A_{k,n+1} + kA_{k,n})[(3k + 1)A_{k,n+1} - (2k^2 + k + 1)A_{k,n}]}$$

haline gelir. $A_{k,n+1}=\dfrac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}$ ve $A_{k,n}=\dfrac{\alpha^{n}-\beta^{n}}{\alpha-\beta}$ olduğu dikkate alınır ve yukarıdaki eşitliğin limiti alınırsa istenilen sonuç görülür.

5.1.10 Örnek. $p=5$ için $k=1$ olup $P=3$ ve $Q=1$ dir. O halde $A_{1,n}=3A_{1,n-1}-A_{1,n-2}$ dır. Bu dizinin ilk birkaç terimi

$$0,1,\ 3,\ 8,\ 21,\ 55,\ 144,\ 377,\ 987,\ 2584,\ 6765,\ 17711,\ 46368,\ \cdots$$

dir. $n=9$ için

$$A_{1,9}=2584\ ,\ A_{1,10}=6765\ ,\ A_{1,11}=17711\ \text{ ve }\ A_{1,12}=46368$$

dir. O halde

$$\lim_{n\to\infty}[A_{1,9},A_{1,10};A_{1,11},A_{1,12}]=\frac{(-4181)(-28657)}{(-10946)(43784)}=\frac{119814917}{-479259664}\cong -0,25$$

bulunur. Dolayısıyla

$$[A_{1,9},A_{1,10};A_{1,11},A_{1,12}]\to\frac{-1}{4}$$

dür. $p=13$ için $k=3$ olup $P=7$ ve $Q=9$ dur. Buna göre $A_{3,n}=7A_{3,n-1}-9A_{3,n-2}$ için

$$0,1,\ 7,\ 40,\ 117,\ 217,\ 1159,\ 6160,\ 32689,\ 173383,\ 919480,\ 4875913,\ 25856071,$$
$$137109280,\ 727060321,\ \cdots$$

dir. $n=10$ için

$$A_{3,10}=4875913\ ,A_{3,11}=25856071\ ,A_{3,12}=137109280\ \text{ ve }\ A_{3,13}=727060321$$

olup

$$\lim_{n\to\infty}[A_{3,10},A_{3,11};A_{3,12},A_{3,13}]=\frac{1237726605\ 2444478}{-8034533287\ 9765272}\cong -0,15405$$

bulunur. Diğer yandan $p=13$ ve $k=3$ için $R=58,S=16,T=376$ ve $U=104$ olup

$$\frac{-R-S\sqrt{p}}{T+U\sqrt{p}}=\frac{-58-16\sqrt{13}}{376+104\sqrt{13}}=\frac{-176+16\sqrt{13}}{768}\cong -0,15405$$

dır. O halde

$$[A_{3,10},A_{3,11};A_{3,12},A_{3,13}]\to\frac{-R-S\sqrt{p}}{T+U\sqrt{p}}$$

dir.

Yukarıdaki teoremden aşağıdaki sonuç verilebilir.

5.1.11 Sonuç. Ardışık $A_{k,n}, A_{k,n+1}, A_{k,n+2}$ ve $A_{k,n+3}$ tamsayıları için

$$\lim_{n\to\infty}[A_{k,n}, A_{k,n+1}; A_{k,n+3}, A_{k,n+2}] = \frac{-T-U\sqrt{p}}{R+S\sqrt{p}}$$

$$\lim_{n\to\infty}[A_{k,n}, A_{k,n+2}; A_{k,n+3}, A_{k,n+1}] = \frac{T+U\sqrt{p}}{(R+T)+(U+S)\sqrt{p}}$$

$$\lim_{n\to\infty}[A_{k,n}, A_{k,n+2}; A_{k,n+1}, A_{k,n+3}] = \frac{(R+T)+(U+S)\sqrt{p}}{T+U\sqrt{p}}$$

$$\lim_{n\to\infty}[A_{k,n}, A_{k,n+3}; A_{k,n+2}, A_{k,n+1}] = \frac{R+S\sqrt{p}}{(R+T)+(U+S)\sqrt{p}}$$

$$\lim_{n\to\infty}[A_{k,n}, A_{k,n+3}; A_{k,n+1}, A_{k,n+2}] = \frac{T+U\sqrt{p}}{(R+T)+(U+S)\sqrt{p}}$$

dir.

5.2 Pell Denklemi

Bu bölümde bir önceki bölümde elde edilen tamsayı dizisinin parametrelerine bağlı olarak tanımlanacak olan Pell denklemi ve bu denklemin tamsayı çözümleri ele alınacak ve bu çözümlerle ilgili indirgeme bağıntıları verilecektir. Bu bölümdeki elde edilen tüm sonuçlar, Tekcan, Özkoç ve ark. 2010 dan alınmıştır.

Hatırlanacağı üzere bir önceki bölümdeki tamsayı dizisinin parametreleri $P = 2k+1$ ve $Q = k^2$ idi. Bu P ve Q parametrelerine bağlı olarak Pell denklemi

$$x^2 - Py^2 = Q$$

olarak tanımlansın. $p = 5$ için $k = 1$ olup $P = 3,\ Q = 1$ olduğundan $x^2 - 3y^2 = 1$ klasik Pell denklemi elde edilir. $p \geq 7$ için ise elde edilen Pell denklemleri klasik Pell denklemi değildir. Dolayısıyla $x^2 - Py^2 = Q$ Pell denkleminin çözümleri iki kısımda ele alınacaktır.

5.2.1 Teorem. $p = 5$ olsun. Bu takdirde $x^2 - 3y^2 = 1$ klasik Pell denklemi için

i) $\sqrt{3}$ ün sürekli kesirli açılımı $\sqrt{3} = [1;\overline{1, 2}]$ dir.

ii) Denklemin temel çözümü $(x_1, y_1) = (2, 1)$ dir.

iii) Denklemin tüm çözümleri $n \geq 1$ için

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

olmak üzere (x_n, y_n) şeklindedir.

iv) Denklemin (x_n, y_n) çözümleri $n \geq 2$ için $x_n = 2x_{n-1} + 3y_{n-1}$ ve $y_n = x_{n-1} + 2y_{n-1}$ bağıntısını ve $n \geq 4$ için $x_n = 3(x_{n-1} + x_{n-2}) - x_{n-3}$ ve $y_n = 3(y_{n-1} + y_{n-2}) - y_{n-3}$ bağıntısını gerçekler.

v) Denklemin (x_n, y_n) çözümleri $n \geq 2$ için

$$\frac{x_n}{y_n} = [1;\underbrace{1, 2, \cdots, 1, 2}_{n-2 \text{ tane}}, 1, 3]$$

kesirli açılımı yardımıyla da verilebilir.

İspat. i) $\sqrt{3}$ ün sürekli kesirli açılımı için

$$\sqrt{3} = 1 + (\sqrt{3} - 1) = 1 + \frac{1}{\frac{1}{\sqrt{3}-1}} = 1 + \frac{1}{\frac{\sqrt{3}+1}{2}} = 1 + \frac{1}{1 + \frac{\sqrt{3}-1}{2}}$$

$$= 1 + \frac{1}{1 + \frac{2}{\sqrt{3}-1}} = 1 + \frac{1}{1 + \frac{1}{\sqrt{3}+1}} = 1 + \frac{1}{1 + \frac{1}{2 + (\sqrt{3}-1)}}$$

olduğundan $\sqrt{3} = [1;\overline{1, 2}]$ dir.

ii) $(x_1, y_1) = (2, 1)$ denklemin temel çözümüdür, çünkü $2^2 - 3 \cdot 1^2 = 1$ dir.

iii) İspat tümevarım ile yapılmak istenirse, $n = 1$ için

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

olup bu temel çözüm olduğundan denklemin bir çözümüdür. Kabul edilsin ki denklem $n - 1$ için gerçeklenir, yani $x_{n-1}^2 - 3y_{n-1}^2 = 1$ dir. Bu takdirde

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} = \begin{bmatrix} 2x_{n-1} + 3y_{n-1} \\ x_{n-1} + 2y_{n-1} \end{bmatrix}$$

olup buradan

$$x_n^2 - 3y_n^2 = (2x_{n-1} + 3y_{n-1})^2 - 3(x_{n-1} + 2y_{n-1})^2 = x_{n-1}^2 - 3y_{n-1}^2 = 1$$

elde edilir. O halde (x_n, y_n) de denklemin bir çözümüdür.

iv) Yukarıdaki eşitlikten

$$x_n = 2x_{n-1} + 3y_{n-1} \text{ ve } y_n = x_{n-1} + 2y_{n-1}$$

olduğu görülür. Diğer bağıntılar da tümevarımla gösterilebilir.

5.2.2 Örnek. $x^2 - 3y^2 = 1$ Pell denkleminin tamsayı çözümleri aşağıdaki gibidir:

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^2 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} x_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^3 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 26 \\ 15 \end{bmatrix}$$

$$\begin{bmatrix} x_4 \\ y_4 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^4 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 97 \\ 56 \end{bmatrix}$$

$$\begin{bmatrix} x_5 \\ y_5 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^5 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 362 \\ 209 \end{bmatrix}$$

$$\begin{bmatrix} x_6 \\ y_6 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}^6 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1351 \\ 780 \end{bmatrix}$$

Üstelik

$$\frac{7}{4} = [1;1,3], \quad \frac{26}{15} = [1;\ 1,2,1,3], \quad \frac{97}{56} = [1;1,2,1,2,1,3],$$

$$\frac{362}{209} = [1;1,2,1,2,1,2,1,3] \text{ ve } \frac{1351}{780} = [1;1,2,1,2,1,2,1,2,1,3]$$

dür.

Şimdi $p > 5$ için $x^2 - Py^2 = Q$ Pell denklemi ele alınabilir.

5.2.3 Teorem. $p > 5$ asal sayısı için $x^2 - Py^2 = Q$ Pell denklemi verilsin. Bu takdirde

i) Denklemin temel çözümü $(x_1, y_1) = (k+1, 1)$ dir.

ii) $\sqrt{P}$ nin sürekli kesirli açılımı

$$\sqrt{P} = \begin{cases} [t; \overline{2t}] & p = 2t^2 + 1 \\ [t; \overline{t, 2t}] & p = 2t^2 + 3 \\ [t-1; \overline{1, t-2, 1, 2t-2}] & p = 2t^2 - 5 \end{cases}$$

dır.

iii) $n \geq 1$ için

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} k+1 & 2k+1 \\ 1 & k+1 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

olmak üzere $\{(x_n, y_n)\}$ dizisi tanımlansın. Bu takdirde $x_n^2 - Py_n^2 = Q^n$ dir.

iv) Denklemin (x_n, y_n) çözümleri $n \geq 2$ için

$$x_n = (k+1)x_{n-1} + (2k+1)y_{n-1} \text{ ve } y_n = x_{n-1} + (k+1)y_{n-1}$$

bağıntısını gerçekler.

İspat. $P = 2k+1,\ Q = k^2$ olduğu hatırlanırsa

i) $(x_1, y_1) = (k+1, 1)$ denklemin temel çözümüdür. Çünkü $(k+1)^2 - (2k+1)1^2 = k^2$ dir.

ii) $p = 2t^2 + 1$ olsun. Bu takdirde $k = \dfrac{t^2}{2}$ olup $P = 2k+1 = t^2+1$ dir. O halde

$$\sqrt{t^2+1} = t + (\sqrt{t^2+1} - t) = t + \frac{1}{\dfrac{1}{\sqrt{t^2+1}-t}} = t + \frac{1}{\dfrac{\sqrt{t^2+1}+t}{1}} = t + \frac{1}{2t + (\sqrt{t^2+1} - t)}$$

olduğundan $\sqrt{P} = [t; \overline{2t}]$ dir. p nin diğer iki değeri için $\sqrt{P}$ nin sürekli kesirli açılımı benzer şekilde gösterilebilir.

iii) Tümevarım ile yapılmak istenirse $n = 1$ için

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} k+1 & 2k+1 \\ 1 & k+1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} k+1 \\ 1 \end{bmatrix}$$

olup bu temel çözüm olduğundan denklemin bir çözümüdür. Kabul edilsin ki denklem $n-1$ için gerçeklenir, yani $x_{n-1}^2 - Py_{n-1}^2 = Q^{n-1}$ dir. Bu takdirde

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} k+1 & 2k+1 \\ 1 & k+1 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$= \begin{bmatrix} k+1 & 2k+1 \\ 1 & k+1 \end{bmatrix} \begin{bmatrix} k+1 & 2k+1 \\ 1 & k+1 \end{bmatrix}^{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$= \begin{bmatrix} k+1 & 2k+1 \\ 1 & k+1 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix}$$
$$= \begin{bmatrix} (k+1)x_{n-1} + (2k+1)y_{n-1} \\ x_{n-1} + (k+1)y_{n-1} \end{bmatrix}$$

olup buradan

$$x_n^2 - Py_n^2 = [(k+1)x_{n-1} + (2k+1)y_{n-1}]^2 - (2k+1)[x_{n-1} + (k+1)y_{n-1}]^2 = k^{2n} = Q^n$$

olduğundan (x_n, y_n) de denklemin bir çözümüdür.

5.2.4 Örnek 1. $t = 6$ için $p = 73$ olup $k = 18$ dir. Dolayısıyla $x^2 - 37y^2 = 324$ Pell denklemi elde edilmiş olur. $\sqrt{37} = [6; \overline{12}]$ dir. Üstelik $(x_1, y_1) = (19, 1)$ denklemin temel çözümü olup diğer bazı çözümleri

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} 19 & 37 \\ 1 & 19 \end{bmatrix}^2 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 398 \\ 38 \end{bmatrix}$$
$$\begin{bmatrix} x_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} 19 & 37 \\ 1 & 19 \end{bmatrix}^3 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 8968 \\ 1120 \end{bmatrix}$$
$$\begin{bmatrix} x_4 \\ y_4 \end{bmatrix} = \begin{bmatrix} 19 & 37 \\ 1 & 19 \end{bmatrix}^4 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 211832 \\ 30243 \end{bmatrix}$$
$$\begin{bmatrix} x_5 \\ y_5 \end{bmatrix} = \begin{bmatrix} 19 & 37 \\ 1 & 19 \end{bmatrix}^5 \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 5143984 \\ 786544 \end{bmatrix}$$

dir. Tüm çözümleri için $x_n^2 - 37y_n^2 = 324^n$ dir.

2. $t = 23$ için $p = 1061$ olup $k = 265$ dir. Dolayısıyla $x^2 - 531y^2 = 70225$ Pell denklemi elde edilir. $\sqrt{531} = [23; \overline{23, 46}]$ dir. Üstelik $(x_1, y_1) = (265, 1)$ denklemin temel çözümü olup $n \geq 1$ için

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 265 & 531 \\ 1 & 265 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

olmak üzere $x_n^2 - 531y_n^2 = 70225^n$ dir.

3. $t = 9$ için $p = 157$ olup $k = 39$ dir. Dolayısıyla $x^2 - 79y^2 = 1521$ Pell denklemi elde edilir. $\sqrt{79} = [8;\overline{1, 7, 1, 16}]$ dır. $(x_1, y_1) = (40, 1)$ bu denklemin temel çözümü olup $n \geq 1$ için

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 40 & 79 \\ 1 & 40 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

olmak üzere $x_n^2 - 79y_n^2 = 1521^n$ dir.

$x^2 - Py^2 = Q$ Pell denkleminin tamsayı çözümleri $p \geq 5$ asalı için Φ_p de ele alınırsa denklemin tamsayı çözümlerinin

$$D_p = \{(x, y) \in \Phi_p \times \Phi_p : x^2 - Py^2 \equiv Q (\text{mod } p)\}$$

kümesi için aşağıdaki teorem verilebilir.

5.2.5 Teorem. $x^2 - Py^2 = Q$ Pell denklemi için

$$\# D_p = \begin{cases} p+1 & p \equiv 5 (\text{mod } 8) \\ p-1 & p \equiv 1 (\text{mod } 8) \end{cases}$$

dir.

İspat: $p \equiv 5 (\text{mod } 8)$ olsun. $y = 0$ ise $x^2 \equiv k^2 (\text{mod } p)$ nin $x = k$ ve $x = p - k$ gibi farklı iki çözümü vardır. Bu ise verilen denklemin $(k, 0)$ ve $(p-k, 0)$ gibi iki tamsayı çözümünün olması demektir. Eğer $x = 0$ ise $-(2k+1)y^2 \equiv k^2 (\text{mod } p)$ kongrüansının çözümü olmadığından denklemin tamsayı çözümü yoktur. $S_p = \Phi_p - \{k, p-k\}$ tanımlansın. Bu takdirde $\frac{x^2 - Q}{P}$ tam kare olacak şekilde S_p de $\frac{p-1}{2}$ tane eleman vardır. $u \neq 0$ için $\frac{x^2 - Q}{P} = u^2$ denilirse $y^2 \equiv u^2 (\text{mod } p)$ nin $y = u$ ve $y = p - u$ gibi farklı iki çözümü vardır. Bu ise verilen denklemin (x, u) ve $(x, p-u)$ gibi iki çözümünün olması

demektir. Dolayısıyla verilen denklemin toplam $2\left(\frac{p-1}{2}\right) = p-1$ tane tamsayı çözümü vardır. $(k,0)$ ve $(p-k,0)$ da bu denklemin birer çözümü olduğundan denklemin $p+1$ tane tamsayı çözümü vardır. Benzer şekilde $p \equiv 1 (\text{mod } 8)$ iken denklemin $p-1$ tane tamsayı çözümünün olduğu gösterilebilir.

KAYNAKLAR

Buchmann, J., Vollmer, U. 2007. Binary Quadratic Forms: An Algorithmic Approach. Springer-Verlag, Berlin, Heidelberg.

Flath, D.E. 1989. Introduction to Number Theory. Wiley.

Mollin, R.A. 1996. Quadratics. CRS Press, Boca Raton, New York, London, Tokyo.

Mollin, R.A. 2008. Fundamental Number Theory with Appl. Chapman & Hall/ CRC.

Mollin, R.A. 2009. Advanced Number Theory with Applications. CRC Press, Taylor and Francis Group, Boca Raton, London, New York.

Nathanson, M.B. 2000. Elementary Methods in Number Theory. Springer.

Ribenboim, P. 2000. My Numbers, My Friends, Popular Lectures on Number Theory, Springer-Verlag, New York, Inc.

Silverman, J.H. 1986. The Arithmetic of Elliptic Curves. Springer-Verlag.

Tekcan, A., Özkoç, A., Alkan, H. 2009. The Diophantine Equation $y^2 - 2yx - 3 = 0$ and Corresponding Curves over Φ_p . *Int. Jour.l of Comp. and Math.Sci.* 3(6): 260-263.

Tekcan, A., Özkoç, A., Alkan, H. 2010. On Cycles and Products of Ideals and Corresponding Indefinite Quadratic Forms. *Comp. Ren. Mat. Math. Rep*. 32(2): 40-51.

Tekcan, A., Özkoç, A., Kocapınar, C., Alkan, H. 2010. The Diophantine Equation $x^2 - Py^2 = Q$. *Int. Journal of Comp. and Math.Sci.* 4(2): 59-62.

Tekcan, A., Alkan, H., Özkoç, A., Çetin, E., Cangül, İ.N. 2010. Rational Points on Curves over Finite Fields. *Antarctica Journal of Mathematics* **7**(4): 431-437.

Tekcan, A., Özkoç, A., Çetin, E., Alkan, H., Cangül, İ.N. 2011. Quadratic Forms, Elliptic Curves and Integer Sequence. *Acta Universitatis Apulensis* 25: 9-30.

Washington, L.C. 2003. Elliptic Curves, Number Theory and Cryptography. Chapmann & Hall / CRC.

ÖZGEÇMİŞ

Adı Soyadı: Hatice ALKAN

Doğum Yeri ve Tarihi: Aydın, 28.04.1988

Yabancı Dil: İngilizce

Eğitim Durumu (Kurum ve Yıl):

Lise: Çine Lisesi

Lisans: Uludağ Üniversitesi

Yüksek Lisans: Uludağ Üniversitesi

Çalıştığı Kurumlar ve Yıl:

2008-2009 Özel Grup Dershanesi

2009-2010 Birey Dershanesi

2010-2011 Mudanya Zafer Dershanesi (Halen çalışmakta)

İletişim: haticealkan988_@hotmail.com

Yayınları:

[1] **Tekcan, A., Özkoç, A., Alkan, H.** *The Diophantine Equation* $y^2 - 2yx - 3 = 0$ *and Corresponding Curves over* Φ_p. Int. Jour. of Comp. and Math.Sci. **3**(6)(2009), 260-263.

[2] **Tekcan, A., Özkoç, A., Alkan, H.** *On Cycles and Products of Ideals and Corresponding Indefinite Quadratic Forms.* Comp. Ren. Mat. Math. Rep. **32**(2)(2010), 40-51.

[3] **Tekcan, A., Özkoç, A., Kocapınar, C., Alkan, H**. *The Diophantine Equation* $x^2 - Py^2 = Q$. Int. Jour. of Comp. and Math.Sci. **4**(2)(2010), 59-62.

[4] **Tekcan, A., Alkan, H., Özkoç, A., Çetin, E., Cangül, İ.N**. *Rational Points on Curves over Finite Fields*. Antarctica Journal of Mathematics **7**(4)(2010), 431-437.

[5] **Tekcan, A., Özkoç, A., Çetin, E., Alkan, H., Cangül, İ.N.** *Quadratic Forms, Elliptic Curves and Integer Sequence*. Acta Universitatis Apulensis **25**(2011), 9-30.