T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

$x^2 + Dy^2$ BİÇİMİNDE YAZILABİLEN ASAL SAYILAR

YÜKSEK LİSANS TEZİ

Elanur ÇETİNER GÖKTAŞ

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Enstitü Bilim Dalı	**:**	**CEBİR VE SAYILAR TEORİSİ**
Tez Danışmanı	**:**	**Prof. Dr. Refik KESKİN**

Haziran 2022

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

$x^2 + Dy^2$ BİÇİMİNDE YAZILABİLEN ASAL SAYILAR

YÜKSEK LİSANS TEZİ

Elanur ÇETİNER GÖKTAŞ

Enstitü Anabilim Dalı : MATEMATİK

Enstitü Bilim Dalı : CEBİR VE SAYILAR TEORİSİ

Bu tez 21.06.2022 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Elanur ÇETİNER GÖKTAŞ

21/06/2022

TEŞEKKÜR

Tez çalışmamın ve yüksek lisans eğitim hayatımın her aşamasında engin bilgi ve tecrübeleriyle beni yönlendiren, destek olan, yardımlarını ve zamanını hiçbir zaman esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren saygı değer danışman hocam Sayın Prof. Dr. Refik KESKİN'e en içten teşekkürlerimi sunarım.

Ayrıca maddi ve manevi desteğini hiçbir zaman esirgemeyen eşime ve aileme teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

(a,b)	: a ile b'nin en büyük ortak böleni
$\|A\|$	:A kümesinin eleman sayısı
$\det A$	: A matrisinin determinantı
$a\|b$	: a tam sayısı b tam sayısını böler
$a \nmid b$	: a tam sayısı b tam sayısını bölmez
$[\![a]\!]$	: a tam sayısının tam değeri
$\in$	: Elemanıdır
$\notin$	: Elemanı değildir
$\mathbb{Z}_n[x]$	: Katsayıları $\mathbb{Z}_n$'de olan polinomlar halkası
$\left(\frac{a}{p}\right)$	: Legendre sembolü
$\mathbb{Z}_n^*$	: n modülüne göre asal kalanlar sistemi
$\mathbb{Z}^+$	: Pozitif tam sayılar kümesi
$\mathbb{Z}$	: Tam sayılar kümesi
$\|x\|$	: x'in mutlak değeri

ÖZET

Anahtar Kelimeler: Kuadratik rezidü, Legendre sembolü, Kuadratik formlar, Uygun sayılar

Bu çalışma dört bölümden oluşmaktadır. Birinci bölümde temel tanım ve teoremler verilmiştir. İkinci bölüm kuadratik rezidülere ayrılmıştır. Kuadratik rezidü tanımı yapılarak konuyla ilgili teoremler ifade edilmiştir. Üçüncü bölüm çalışmanın ana bölümünü oluşturmaktadır. Bu bölümde bazı D doğal sayıları için $x^2 + Dy^2$ biçiminde yazılabilen asal sayılar karakterize edilmiştir. Ayrıca uygun sayı tanımı verilerek uygun sayılarla ilgili bazı teoremler verilmiştir. Dördüncü bölüm sonuç ve önerilerden oluşmaktadır.

PRIMES OF THE FORM $x^2 + Dy^2$

SUMMARY

Keywords: Quadratic residue, Legendre symbol, Quadratic forms, Convenient numbers

This study consist of four section. In the first section, the main defnitions and theorems are given. Second section is devoted to quadratic residues. By defining quadratic residue, some theorems concerning the subject are given. The third section covers the main subject of the study. In this section, primes of the forms $x^2 + Dy^2$ are characterized for some values of n. Also, some theorems concerning convenient numbers are given. Last section contains results and suggestions.

BÖLÜM 1. GİRİŞ

Bu bölümde sayılar teorisinden iyi bilinen bazı tanımlara ve teoremlere yer verilecektir.

1.1. Bölünebilme

Tanım 1.1. a ve b iki tam sayı ve $a \neq 0$ olsun. Eğer $b = a \cdot c$ olacak biçimde bir c tam sayısı varsa a sayısı b'yi bölüyor veya a, b'nin bir bölenidir ya da a, b'nin bir çarpanıdır denir. a sayısı b'yi bölüyorsa $a|b$, bölmüyorsa bu $a \nmid b$ ile gösterilir.

Bölünebilme tanımı kullanılarak bölünebilme ile ilgili aşağıdaki özellikler kolaylıkla gösterilebilir.

1) $a|b$ ise her c tam sayısı için $a|cb$ dir.
2) $a|b$ ve $b|c$ ise $a|c$ dir.
3) $a|b$ ve $b|a$ ise $a = \pm b$ dir.
4) $a|b$ ise sıfırdan farklı her c tam sayısı için $ac|bc$ dir.
5) $c \neq 0$ ve $ac|bc$ ise $a|b$ dir.
6) $a|b$ ve $c|d$ ise $ac|bd$ dir.
7) $a|b$ ve $a|c$ ise he x, y tam sayısı için $a|bx \mp cy$ dır.

Teorem 1.1. (Bölme Algoritması) $a \neq 0$ olmak üzere a ve b tam sayı çifti için $b = aq + r$, $0 \leq r < |a|$ olacak biçimde q, r tam sayıları vardır ve bu q ve r tek türlü belirlidir.

Tanım 1.2. a ve b iki tam sayı olsun. Eğer bir $d \neq 0$ tam sayısı için $d|a$ ve $d|b$ koşulları sağlanıyor ise d'ye a ve b tam sayılarının bir ortak böleni denir. a ve b aynı anda sıfır olmasın. a ve b'nin pozitif ortak bölenlerinin en büyüğüne bu sayıların en

büyük ortak böleni denir. Bu durum $d = (a, b)$ ile gösterilir. Özellikle $(a, b) = 1$ ise a ve b tam sayılarına aralarında asaldır denir.

Teorem 1.3. d tam sayısı a ve b tam sayılarının en büyük ortak böleni ise $d = ax + by$ olacak şekilde x ve y tam sayıları vardır.

1.2. Kongrüanslar

Tanım 1.4. m bir pozitif tam sayı olsun. Eğer $m|a - b$ ise a ve b sayıları m modülüne göre kongrüenttirler (denktirler) denir. Bu durum $a \equiv b(\mathrm{mod}\, m)$ biçiminde gösterilir.

Teorem 1.5. $m > 0$ olmak üzere $a, b, c, d, m \in \mathbb{Z}$ ve $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$ olsun. Bu takdirde,

i) $a + c \equiv b + d(\mathrm{mod}\, m)$ ve $a - c \equiv b - d(\mathrm{mod}\, m)$,

ii) $ac \equiv bd(\mathrm{mod}\, m)$,

iii) $k \in \mathbb{Z}$ olmak üzere $a + k \equiv b + k(\mathrm{mod}\, m)$ ve $ka \equiv kb(\mathrm{mod}\, m)$

iv) $ax \equiv ay(\mathrm{mod}\, m)$ ve $(a, m) = 1$ ise $x \equiv y(\mathrm{mod}\, m)$

dir.

Tanım 1.6. $m \geq 1$ ve $a_1, a_2, \ldots, a_m$ tam sayıları verilmiş olsun. Eğer

1) $i \neq j$ için $a_i \not\equiv a_j(\mathrm{mod}\, m)$ dir,

2) Her $a \in \mathbb{Z}$ için $a \equiv a_i(\mathrm{mod}\, m)$ olacak şekilde $1 \leq i \leq m$ koşulunu sağlayan en az bir i tamsayısı vardır,

şartları sağlanıyorsa $a_1, a_2, \ldots, a_m$ tamsayılarına m modülüne göre bir tam kalanlar sistemi denir.

Tanım 1.7. Her $m > 0$ tam sayısını, m'yi geçmeyen ve m ile aralarında asal olan tam sayıların sayısına eşleyen fonksiyona Euler'in φ-fonksiyonu denir. Başka bir ifade ile $\varphi(m) = |\{x: (m, x) = 1, 1 \leq x \leq m \; ve \; x \in \mathbb{Z}\}|$ ile tanımlı $\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+$ fonksiyonuna Euler'in φ-fonksiyonu denir.

Örnek: $\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(7) = 6$ dir.

Örnek: p bir asal sayı olmak üzere $\varphi(p) = p - 1$ olduğu kolaylıkla görülebilir.

Tanım 1.8. $m \geq 1$ ve $a_1, a_2, \dots, a_{\varphi(m)}$ tam sayıları verilmiş olsun. Eğer

1) Her $i = 1,2, \dots, \varphi(m)$ için $(a_i, m) = 1$ dir,

2) $i \neq j$ için $a_i \not\equiv a_j (\mathrm{mod}\, m)$ dir,

3) $(a, m) = 1$ koşulunu sağlayan her $a \in \mathbb{Z}$ için $1 \leq i \leq \varphi(m)$ olmak üzere $a \equiv a_i (\mathrm{mod}\, m)$ olacak şekilde bir i tam sayısı vardır,

şartları sağlanıyorsa $a_1, a_2, \dots, a_{\varphi(m)}$ tam sayılarına m modülüne göre bir indirgenmiş kalanlar sistemi denir.

Teorem 1.9. p bir asal sayı ve $p \nmid a$ ise $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ dir.

Teorem 1.10. m bir pozitif tam sayı ve $(a, m) = 1$ ise $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$ dir.

Teorem 1.11 (Güvercin Yuvası ilkesi). m ve n doğal sayılar ve $m > n$ olsun. Eğer m tane nesne n tane kutuya yerleştirilirse bir kutuya en az 2 nesne koyulmalıdır.

İspat: m tane nesne $x_1, x_2, \dots, x_m$ ile n tane kutu da $S_1, S_2, \dots, S_n$ kümeleriyle gösterilirse $x_1, x_2, \dots, x_m$ nesneleri $S_1, S_2, \dots, S_n$ kutularına yerleştirileceğinden

$$S_1 \cup S_2 \cup \dots \cup S_n = \{x_1, x_2, \dots x_m\}$$

olarak yazılabilir. Her kutuya ikiden az nesne yerleştirilirse $1 \leq k \leq n$ için $|S_k| \leq 1$ olacağından

$$m = |S_1 \cup S_2 \cup \dots \cup S_n| \leq |S_1| + |S_2| + \cdots + |S_n| \leq n$$

elde edilir. Bu ise $m > n$ olmasıyla çelişir. Şu halde bir kutuya en az iki nesne yerleştirilmelidir.

Sonuç 1.12. $n > m$ olsun ve $x_1, x_2, \dots, x_n$ tam sayıları verilsin. Bu durumda $m|x_k - x_j$ olacak biçimde $k \neq j$ olan k ve j indisleri vardır.

İspat: $x_1, x_2, \dots, x_n$ tam sayılarının m tam sayısına bölümlerinden elde edilen kalanlar düşünülür ve her tam sayı kalanıyla ilgili kutuya yerleştirilirse $n > m$ olduğundan bu sayılardan en az iki tanesi aynı kutuya yerleştirilmelidir. Yani en az iki tam sayının m tam sayısına bölümünden elde edilen kalanlar aynıdır. Bu tam sayılar x_j ve x_k ise $m|x_k - x_j$ elde edilir.

1.2.1. Bir bilinmeyenli lineer kongrüanslar

Bu kısımda $ax \equiv b(\mathrm{mod}\, m)$ kongrüansının çözümü incelenecektir.

Tanım 1.2.1. $a, b, m \in \mathbb{Z}$ ve $m > 0$ olmak üzere $ax \equiv b(\mathrm{mod}\, m)$ şeklinde verilen kongrüans bağıntısına bir bilinmeyenli bir lineer kongrüans denklemi adı verilir.

Aşağıdaki teorem $ax \equiv b(\mathrm{mod}\, m)$ kongrüansının çözümünün olması için gerekli ve yeterli şartı ifade etmektedir.

Teorem 1.2.2. $ax \equiv b(\mathrm{mod}\, m)$ kongrüansının bir çözümünün olması için gerekli ve yeterli şart $(a, m)|b$ olmasıdır.

İspat: $ax \equiv b(\mathrm{mod}\, m)$ kongrüansının x_1 gibi bir çözümünün olduğunu kabul edelim. Dolayısıyla $ax_1 = b + mk$ olacak biçimde bir k tam sayısı vardır. $\mathrm{g} = (a, m)$ ise $\mathrm{g}|a$ ve $\mathrm{g}|m$ olduğundan $\mathrm{g}|ax_1 - mk$, yani $\mathrm{g}|b$ bulunur. Şimdi de $\mathrm{g}|b$ olsun. Dolayısıyla $b = \mathrm{g}k$ olacak biçimde bir k tam sayısı vardır. $\mathrm{g} = (a, m)$ olduğundan $\mathrm{g} = ax_0 + my_0$ olacak biçimde x_0, y_0 tam sayıları vardır. Buradan $b = \mathrm{g}k = akx_0 + mky_0$ elde edilir. Eğer $x_1 = kx_0$ alınırsa $ax_1 \equiv b(\mathrm{mod}\, m)$ bulunur.

Teorem 1.2.3. $m \geq 1$ olsun. $(a, m) = 1$ ise $ax \equiv b(\mathrm{mod}\, m)$ kongrüansının x_1 gibi bir çözümü vardır ve kongrüansının tüm çözümleri $j \in \mathbb{Z}$ olmak üzere $x = x_1 + jm$ ile

verilir. Özellikle $ar \equiv b(\mathrm{mod}\, m)$ olacak biçimde $0 \leq r \leq m-1$ şartını sağlayan bir r tam sayısı vardır.

İspat: $m = 1$ ise ispat açıktır. $m \geq 2$ olsun. $(a, m) = 1$ olduğundan Teorem 1.10'a göre $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$ yazılabilir. $x_1 = ba^{\varphi(m)-1}$ alınırsa $ax_1 \equiv b(\mathrm{mod}\, m)$ elde edilir. Şimdi x tam sayısı $ax \equiv b(\mathrm{mod}\, m)$ şartını sağlasın. $ax_1 \equiv b(\mathrm{mod}\, m)$ olduğundan $ax \equiv ax_1(\mathrm{mod}\, m)$ elde edilir. $(a, m) = 1$ olduğu kullanılırsa $x \equiv x_1(\mathrm{mod}\, m)$ bulunur. Bu ise $x = x_1 + mk$ olacak biçimde bir k tam sayısının olduğunu gösterir. Diğer yandan $x = x_1 + jm$ ise $x \equiv x_1(\mathrm{mod}\, m)$ olup $ax \equiv b(\mathrm{mod}\, m)$ olduğu görülür. x_1 tam sayısının m tam sayısına bölümünden elde edilen kalan r ise $x \equiv r(\mathrm{mod}\, m)$ olduğundan $ar \equiv b(\mathrm{mod}\, m)$ bulunur.

Teorem 1.2.4. $\mathrm{g} = (a, m)$ ve $\mathrm{g}|b$ olsun. Bu taktirde $\left(\frac{a}{\mathrm{g}}\right)x \equiv \left(\frac{b}{\mathrm{g}}\right)\left(\mathrm{mod}\, \left(\frac{m}{\mathrm{g}}\right)\right)$ kongrüansının çözümleri ile $ax \equiv b(\mathrm{mod}\, m)$ kongrüansının çözümleri aynıdır ve x_1 tam sayısı $\left(\frac{a}{\mathrm{g}}\right)x \equiv \left(\frac{b}{\mathrm{g}}\right)\left(\mathrm{mod}\, \left(\frac{m}{\mathrm{g}}\right)\right)$ kongrüansının bir çözümü ise $ax \equiv b(\mathrm{mod}\, m)$ kongrüansının tüm çözümleri $t \in \mathbb{Z}$ olmak üzere $x = x_1 + (m/\mathrm{g})t$ ile verilir.

İspat: $\mathrm{g} = (a, m)$ ve $\mathrm{g}|b$ olsun. O zaman $ax \equiv b(\mathrm{mod}\, m) \Leftrightarrow m|ax - b \Leftrightarrow (m/\mathrm{g})|(a/\mathrm{g})x - (b/\mathrm{g}) \Leftrightarrow (a/\mathrm{g})x \equiv (b/\mathrm{g})(\mathrm{mod}\, (m/\mathrm{g}))$ olduğu dikkate alınırsa istenen elde edilir.

Teorem 1.2.5. $(a, m) = 1$ olsun. Eğer x_0, y_0 tamsayıları $ax_0 + my_0 = 1$ şartını sağlıyorsa $x_1 = bx_0$ tam sayısı $ax \equiv b(\mathrm{mod}\, m)$ kongrüansının bir çözümüdür.

İspat: $ax_0 + my_0 = 1$ ise $abx_0 + mby_0 = b$ olup $ax_1 + mby_0 = b$ yazılabilir. Bu ise $ax_1 \equiv b(\mathrm{mod}\, m)$ olduğunu gösterir.

Teorem 1.2.6 (Wilson Teoremi). p bir asal sayı ise $(p-1)! \equiv -1(\mathrm{mod}\, p)$ özelliği geçerlidir.

Teorem 1.2.7. p bir asal sayı ve $p > 2$ olsun. Bu durumda, $x^2 \equiv -1(\mathrm{mod}\, p)$ olacak biçimde bir x tam sayısının olması için gerekli ve yeterli şart $p \equiv 1(\mathrm{mod}\, 4)$ olmasıdır.

İspat: Önce $x^2 \equiv -1(\mathrm{mod}\, p)$ olacak biçimde bir x tam sayısı varsa $p \equiv 1(\mathrm{mod}\, 4)$ olduğunu gösterelim. $x^2 \equiv -1(\mathrm{mod}\, p)$ ise $p \nmid x$ olduğu açıktır. Dolayısıyla Teorem 1.9'a göre $x^{p-1} \equiv 1(\mathrm{mod}\, p)$ yazılabilir. $x^2 \equiv -1(\mathrm{mod}\, p)$ olduğundan $(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}(\mathrm{mod}\, p)$, yani $x^{p-1} \equiv (-1)^{\frac{p-1}{2}}(\mathrm{mod}\, p)$ bulunur. Buradan $1 \equiv (-1)^{\frac{p-1}{2}}(\mathrm{mod}\, p)$ olduğu görülür. $p > 2$ olduğundan $(-1)^{\frac{p-1}{2}} = 1$ olmalıdır. Bu ise $(p-1)/2$ tam sayısının çift olmasını gerektirir. $(p-1)/2 = 2k$ olarak yazılırsa $p = 1 + 4k$, yani $p \equiv 1(\mathrm{mod}\, 4)$ elde edilir.

Şimdi de $p \equiv 1(\mathrm{mod}\, 4)$, yani $p = 1 + 4n$ olsun. Bu durumda $k = (p-1)/2$ ise k tam sayısının çift tam sayısı ve $k + 1 = \frac{p-1}{2} + 1 = \frac{p+1}{2} = p - \frac{p-1}{2} = p - k$ olduğu görülür. Diğer yandan $1 \le j \le k$ ise $p - j \equiv -j(\mathrm{mod}\, p)$ olduğundan

$$\prod_{j=1}^{k}(p-j) \equiv \prod_{j=1}^{k}(-j)(\mathrm{mod}\, p)$$

yazılabilir. Dolayısıyla

$$(p-1)(p-2)\dots(p-k+1)(p-k) \equiv (-1)(-2)\dots\big(-(k-1)\big)(-k)(\mathrm{mod}\, p)$$

olur. Buradan

$$(p-1)(p-2)(p-3)\dots(p-k+1)(p-k) \equiv (-1)^k k!\,(\mathrm{mod}\, p)$$

bulunur. k tam sayısının çift olduğu kullanılır ve kongrüansının her iki yanı $k!$ ile çarpılırsa

$$k!\,(p-k)(p-k+1)\dots(p-2)(p-1) \equiv (k!)^2(\mathrm{mod}\, p)$$

elde edilir. $p-k=k+1$ olduğu dikkate alınırsa

$$k!\,(k+1)(k+2)\ldots(p-2)(p-1)\equiv(k!)^2(\mathrm{mod}\,p)$$

buradan da $(p-1)!\equiv(k!)^2(\mathrm{mod}\,p)$ bulunur. Wilson Teoremi'ne göre $(p-1)!\equiv-1(\mathrm{mod}\,p)$ dir. Buradan $(k!)^2\equiv-1(\mathrm{mod}\,p)$ bulunur. Dolayısıyla $x=k!$ alınırsa istenen sonuç elde edilir.

Teorem 1.2.8. p bir asal sayı, $p|a^2+b^2$ ve $p\equiv 3(\mathrm{mod}\,4)$ ise $p|a$ ve $p|b$ dir.

İspat: Olmayana Ergi Yöntemiyle: Eğer $p|a$ olduğu gösterilirse $p|a^2+b^2$ olduğundan $p|b^2$, yani $p|b$ elde edilir. Şimdi $p\nmid a$ olduğunu kabul edelim. Dolayısıyla $(p,a)=1$ olup Teorem 1.2.3'e göre $ax\equiv 1(\mathrm{mod}\,p)$ olacak biçimde bir x tam sayısı vardır. Dolayısıyla $a^2x^2\equiv 1(\mathrm{mod}\,p)$ ve $a^2\equiv-b^2(\mathrm{mod}\,p)$ yazılabilir. Buradan da $a^2x^2\equiv-b^2x^2(\mathrm{mod}\,p)$ ve böylece $1\equiv-b^2x^2(\mathrm{mod}\,p)$ bulunur. Bu ise $(bx)^2\equiv-1(\mathrm{mod}\,p)$ olduğunu gösterir. $p>2$ olduğundan önceki teoreme göre $p\equiv 1(\mathrm{mod}\,4)$ olmalıdır. Bu ise hipotezle çelişir. O halde $p|a$ ve böylece $p|b$ elde edilir.

Direkt İspat Yöntemiyle: $p|a^2+b^2$ ise $a^2\equiv-b^2(\mathrm{mod}\,p)$ olur. $p\equiv 3(\mathrm{mod}\,4)$ olduğundan $(p-1)/2$ bir tek tam sayıdır. Böylece $(a^2)^{\frac{p-1}{2}}\equiv-(b^2)^{\frac{p-1}{2}}(\mathrm{mod}\,p)$, yani $a^{p-1}\equiv-b^{p-1}(\mathrm{mod}\,p)$ elde edilir. Ayrıca Teorem 1.9'a göre $a^p\equiv a(\mathrm{mod}\,p)$ ve $b^p\equiv b(\mathrm{mod}\,p)$ yazılabilir. $a^2\equiv-b^2(\mathrm{mod}\,p)$ ve $a^{p-1}\equiv-b^{p-1}(\mathrm{mod}\,p)$ kongrüansları alt alta çarpılırsa $a^{p+1}\equiv b^{p+1}(\mathrm{mod}\,p)$ bulunur. Diğer yandan $a^p\equiv a(\mathrm{mod}\,p)$, $b^p\equiv b(\mathrm{mod}\,p)$ olduğu dikkate alınırsa $a^2\equiv b^2(\mathrm{mod}\,p)$ elde edilir. Böylece $a^2\equiv-b^2(\mathrm{mod}\,p)$ olduğu kullanılırsa $2a^2\equiv 0(\mathrm{mod}\,p)$, yani $p|a$ elde edilir. $p|a^2+b^2$ olduğundan $p|b$ bulunur.

Teorem 1.2.9. $d=(a,b)$ ise $\left(\frac{a}{b},\frac{b}{d}\right)=1$ dir.

Teorem 1.2.10. $a|bc$ ve $(a,b)=1$ ise $a|c$ dir.

BÖLÜM 2. KUADRATİK KONGRÜANSLAR

Tanım 2.1. m pozitif bir tam sayı, $a \in \mathbb{Z}$ ve $(a,m)=1$ olsun. $a^h \equiv 1(mod\ m)$ koşulunu sağlayan en küçük pozitif h tam sayısına a'nın m modülüne göre mertebesi denir.

$a \in \mathbb{Z}$ ve $(a,m)=1$ olsun. a'nın m modülüne göre mertebesi $\varphi(m)$ ise a'ya m modülüne göre bir ilkel kök denir.

Örnek: $3 \equiv 3(mod\ 5)$, $3^2 \equiv 4(mod\ 5)$, $3^3 \equiv 2(mod\ 5)$ ve $3^4 \equiv 1(mod\ 5)$ olduğundan 3'ün 5 modülüne göre mertebesi 4'tür.

Önerme 2.2. $p>2$ asal sayı ise p modülüne göre ilkel kök vardır. Ayrıca g,p modülüne göre bir ilkel kök ise $g, g^2, \dots, g^{p-1}$ sayıları p modülüne göre bir indirgenmiş kalanlar sistemidir [1].

Örnek: Önceki örnekte 3'ün 5 modülüne göre mertebesi 4 olduğunu görmüştük. Ayrıca $\varphi(5)=4$ olduğundan 3 sayısı 5 modülüne göre bir ilkel köktür.

Bu bölümde p asal sayı, $p>2$ ve $p \nmid a$ olmak üzere $x^2 \equiv a(mod\ p)$ kongrüansının çözümünün olup olmadığı araştırılacaktır.

Tanım 2.3. a bir tam sayı ve $(a,m)=1$ olsun. Eğer $x^2 \equiv a(\mathrm{mod}\ m)$ kongrüansının bir çözümü varsa a tam sayısına m modülüne göre bir ikinci dereceden kalan veya karedir denir. Eğer $x^2 \equiv a(\mathrm{mod}\ m)$ kongrüansının çözümü yoksa a tam sayısına m modülüne göre bir kare değildir denir.

$4^2 \equiv 3(\mathrm{mod}\ 13)$ olduğundan 3 tam sayısı 13 modülüne bir karedir.

$7 \equiv 3(\mathrm{mod}\ 4)$ olduğundan Teorem 1.2.7'ye göre $x^2 \equiv -1(\mathrm{mod}\ 7)$ kongrüansının bir çözümü yoktur. O halde -1 sayısı 7 modülüne göre bir kare değildir.

Önerme 2.4. $x^2 \equiv a(\mathrm{mod}\ m)$ olacak biçimde bir x tam sayısı vardır $\Leftrightarrow$ $x_1^2 \equiv a(\mathrm{mod}\ m)$ olacak biçimde $0 \leq x_1 \leq m-1$ şartını sağlayan bir x_1 tam sayısı vardır [1].

İspat: $x^2 \equiv a(\mathrm{mod}\ m)$ olacak biçimde bir x tam sayısı mevcut olsun. Teorem 1.1'e göre $x = mq + x_1,\ 0 \leq x_1 \leq m-1$ olacak şekilde x_1 ve q tam sayıları mevcuttur. Buradan $x \equiv x_1(\mathrm{mod}\ m)$ olduğu dikkate alınırsa $x_1^2 \equiv a(\mathrm{mod} m)$ elde edilir.

Yukarıdaki önermeye göre $x^2 \equiv a(\mathrm{mod}\ m)$ kongrüansının çözümleri varsa bunları m tam sayısından küçük negatif olmayan tam sayılar içinden aramak gereklidir.

$x^2 \equiv 2(\mathrm{mod}\ 5)$ kongrüansının çözümü yoktur. Çünkü x yerine $0,1,2,3,4$ değerleri yazıldığında

$0^2 \not\equiv 2(\mathrm{mod}\ 5)$
$1^2 \not\equiv 2(\mathrm{mod}\ 5)$
$2^2 \not\equiv 2(\mathrm{mod}\ 5)$
$3^2 \not\equiv 2(\mathrm{mod}\ 5)$
$4^2 \not\equiv 2(\mathrm{mod}\ 5)$

olduğu görülür.

Teorem 2.5. p asal sayı, $p > 2$ ve $p \nmid a$ olsun. Bu takdirde,
(1) $x^2 \equiv a(\mathrm{mod}\ p)$ kongrüansının çözümünün olması için gerekli ve yeterli şart $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$ olmasıdır.
(2) $x^2 \equiv a(\mathrm{mod}\ p)$ kongrüansının çözümünün olmaması için gerekli ve yeterli şart $a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\ p)$ olmasıdır.

İspat: (1) $x^2 \equiv a(\mathrm{mod}\, p)$ olacak biçimde bir x tam sayısı mevcut olsun. $p \nmid a$ olduğundan $p \nmid x$ olduğu açıktır. Fermat Teoremi'ne göre $x^{p-1} \equiv 1(\mathrm{mod}\, p)$ yazılabilir. $x^2 \equiv a(\mathrm{mod}\, p)$ olduğundan $x^{p-1} = (x^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}}(\mathrm{mod}\, p)$ olur. Buradan da $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$ elde edilir. Şimdi de $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$ ve g tam sayısı p modülüne göre bir ilkel kök olsun. Bu taktirde Önerme 2.2'ye göre $\mathrm{g}, \mathrm{g}^2, \mathrm{g}^3, \ldots, \mathrm{g}^{p-1}$ tam sayıları p modülüne göre bir indirgenmiş kalanlar sistemidir. Dolayısıyla $a \equiv \mathrm{g}^k(\mathrm{mod}\, p)$ olacak biçimde $1 \leq k \leq p-1$ şartını sağlayan bir k tam sayısı vardır. Buradan $a^{\frac{p-1}{2}} \equiv (\mathrm{g}^k)^{\frac{p-1}{2}}(\mathrm{mod}\, p)$ ve böylece $\mathrm{g}^{k(p-1)/2} \equiv 1(\mathrm{mod}\, p)$ yazılabilir. g tam sayısının p modülüne göre mertebesi $p-1$ olduğundan $(p-1) \mid k(p-1)/2$ elde edilir. Böylece $2|k$ olduğu görülür. $x = \mathrm{g}^{k/2}$ olarak alınırsa $x^2 = \mathrm{g}^k \equiv a(\mathrm{mod}\, p)$ bulunur.

(2) Eğer $a^{(p-1)/2} \equiv -1(\mathrm{mod}\, p)$ ise önceki teoremin (1) özelliğine göre $x^2 \equiv a(\mathrm{mod} p)$ kongrüansının çözümü yoktur. Şimdi $x^2 \equiv a(\mathrm{mod}\, p)$ kongrüansının çözümünün olmadığını kabul edelim. $p \nmid a$ olduğundan Teorem 1.9'a göre $a^{p-1} \equiv 1(\mathrm{mod}\, p)$ dir. Dolayısıyla $p|a^{p-1} - 1$, yani $p|(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1)$ yazılabilir. p asal olduğundan $p|a^{(p-1)/2} - 1$ veya $p|a^{(p-1)/2} + 1$ olur. Eğer $p|a^{(p-1)/2} - 1$ ise $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$ olur ki bu durum (1) özelliğine göre $x^2 \equiv a(\mathrm{mod}\, p)$ kongrüansının çözümünün olmaması ile çelişir. O halde $p|a^{(p-1)/2} + 1$ dir. Bu durumda $a^{(p-1)/2} \equiv -1(\mathrm{mod}\, p)$ olur.

Tanım 2.6. p asal sayı, $p > 2$ ve $p \nmid a$ olsun. $\left(\frac{a}{p}\right)$ sembolünü Legendre kullanmıştır ve $x^2 \equiv a(\mathrm{mod}\, p)$ kongrüansının çözümü varsa $\left(\frac{a}{p}\right) = 1$, $x^2 \equiv a(\mathrm{mod}\, p)$ kongrüansının çözümü yoksa $\left(\frac{a}{p}\right) = -1$ olarak tanımlanır.

Örnek: $3^2 \equiv 2(\mathrm{mod}\, 7)$ olduğundan $\left(\frac{2}{7}\right) = 1$ ve $x^2 \equiv -1(\mathrm{mod}\, 7)$ olacak biçimde x tam sayısı olmadığından $\left(\frac{-1}{7}\right) = -1$ olur.

Teorem 2.7. $p > 2$ bir asal sayı ve $(a, p) = (b, p) = 1$ olsun. Bu takdirde,

(1) $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p)$,

(2) $a \equiv b(\mathrm{mod}\, p)$ ise $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

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

(4) $\left(\frac{1}{p}\right) = \left(\frac{a^2}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$,

(5) $x^2 \equiv a(\mathrm{mod}\, p)$ kongrüansının çözümü vardır $\Leftrightarrow \left(\frac{a}{p}\right) = 1$ ve $x^2 \equiv a(\mathrm{mod}\, p)$ kongrüansının çözümü yoktur $\Leftrightarrow \left(\frac{a}{p}\right) = -1$

ifadeleri doğrudur [1].

İspat: (1) Teorem 2.5 ve $\left(\frac{a}{p}\right)$ Legendre sembolünün tanımı kullanılırsa istenen elde edilir.

(2) $a \equiv b(\mathrm{mod}\, p)$ ise $a^{(p-1)/2} \equiv b^{\frac{p-1}{2}} (\mathrm{mod}\, p)$ yazılabilir. Önceki özelliğe göre $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p)$ ve $b^{(p-1)/2} \equiv \left(\frac{b}{p}\right) (\mathrm{mod}\, p)$ olduğundan $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) (\mathrm{mod}\, p)$ elde edilir. $p > 2$ ve $\left(\frac{a}{p}\right) = \mp 1$, $\left(\frac{b}{p}\right) = \mp 1$ olduğundan $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ elde edilir. Çünkü, eğer $\left(\frac{a}{p}\right) \neq \left(\frac{b}{p}\right)$ ise $\left(\frac{a}{p}\right) - \left(\frac{b}{p}\right) = \mp 2$ olacağından $p|2$ bulunur. Bu durum $p > 2$ olmasına aykırıdır.

(3) $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p)$ ve $b^{(p-1)/2} \equiv \left(\frac{b}{p}\right) (\mathrm{mod}\, p)$ olduğundan $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\mathrm{mod}\, p)$ yazılabilir. $(ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) (\mathrm{mod}\, p)$ olduğundan $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\mathrm{mod}\, p)$ elde edilir. Üstteki duruma benzer şekilde $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ bulunur.

(4) $\left(\frac{1}{p}\right) = \left(\frac{a^2}{p}\right) = 1$ olduğu açıktır. $(-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) (\mathrm{mod}\, p)$ olduğundan $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ elde edilir.

(5) $\left(\frac{a}{p}\right)$ Legendre sembolünün tanımı, Teorem 2.5 ve (1) özelliği kullanıldığında istenilen elde edilir.

Teorem 2.8. (Gauss Lemması) $p > 2$ bir asal sayı ve $p \nmid a$ olsun. Eğer

$$a, 2a, 3a, \dots, \left(\frac{p-1}{2}\right)a$$

tam sayılarının p tam sayısına bölümlerinden elde edilen kalanlardan $p/2$ tam sayısından büyük olanların sayısı n ise $\left(\frac{a}{p}\right) = (-1)^n$ dir [1].

Örnek: $\left(\frac{3}{29}\right)$ değerini hesaplayınız.

Çözüm: $a = 3$, $p = 29$ ve $(p-1)/2 = (29-1)/2 = 14$ olur.

$$3{,}2 \cdot 3{,}3 \cdot 3{,}4 \cdot 3{,}5 \cdot 3{,}6 \cdot 3{,}7 \cdot 3{,}8 \cdot 3{,}9 \cdot 3{,}10 \cdot 3{,}11 \cdot 3{,}12 \cdot 3{,}13 \cdot 3{,}14 \cdot 3$$

tam sayılarının 29 tam sayısına bölümlerinden elde edilen kalanlar sırasıyla 3,6,9,12,15,18,21,24,1,4,7,10,13 tam sayılarıdır. Bunların içinden $29/2$ sayısından büyük olanlar 5 tanedir. Şu halde $\left(\frac{3}{29}\right) = (-1)^5 = -1$ olur.

Teorem 2.9. p asal sayı ve $p > 2$ olsun. Bu taktirde $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ ve a tek tam sayı ve $p \nmid a$ ise

$$t = \sum_{j=1}^{(p-1)/2} [\![ja/p]\!]$$

olmak üzere $\left(\frac{a}{p}\right) = (-1)^t$ formülleri geçerlidir [1].

Örnek: $x^2 \equiv 2(\text{mod } 17)$ kongrüansının çözümünün olup olmadığını gösteriniz.

Çözüm: $\left(\frac{2}{17}\right) = (-1)^{(17^2-1)/8} = (-1)^{\frac{16.18}{8}} = (-1)^{36} = 1$ olduğundan $x^2 \equiv 2(\text{mod } 17)$ kongrüansının çözümü vardır.

Örnek: 2^{53} tam sayısının 103 sayısına bölümünden elde edilen kalanı bulunuz.

Çözüm: $\left(\frac{2}{103}\right) = (-1)^{(103^2-1)/8} = (-1)^{\frac{102\cdot104}{8}} = (-1)^{102\cdot13} = 1$ olduğundan Teorem 2.7'ye göre $2^{(103-1)/2} \equiv 1(\text{mod } 103)$, yani $2^{51} \equiv 1(\text{mod } 103)$ yazılabilir. Buradan $2^{53} \equiv 4(\text{mod } 103)$ elde edilir. Şu halde kalan 4 olur.

Örnek: 5^{35} sayısının 67 asal sayısına bölümünden elde edilen kalanı bulunuz.

Çözüm: Önce $\left(\frac{5}{67}\right)$ değerini hesaplayalım.

$$\sum_{j=1}^{(67-1)/2} [\![5j/67]\!] = \sum_{j=1}^{33} [\![5j/67]\!]$$

$$= \sum_{j=1}^{13} [\![5j/67]\!] + \sum_{j=14}^{26} [\![5j/67]\!] + \sum_{j=27}^{33} [\![5j/67]\!]$$

$$= \sum_{j=14}^{26} 1 + \sum_{j=27}^{33} 2$$

$$= 13 + 7.2$$

$$= 27$$

olduğundan Teorem 2.9'a göre $\left(\frac{5}{67}\right) = (-1)^{27} = -1$ olur. Dolayısıyla Teorem 2.7'ye göre $5^{(67-1)/2} \equiv -1(\text{mod } 67)$ yazılabilir. Buradan $5^{33} \equiv -1(\text{mod } 67)$ elde edilir. Dolayısıyla $5^{35} \equiv -25(\text{mod } 67)$, yani $5^{35} \equiv 42(\text{mod } 67)$ bulunur. Dolayısıyla kalan 42 olur.

Teorem 2.10. (İkinci Dereceden İndirgeme Kuralı) p ve q farklı tek asal sayılar iseler $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, yani

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

dir [1].

Örnek: $\left(\frac{-42}{61}\right) = 1$ olduğunu gösteriniz.

Çözüm: $-42 \equiv 19(\text{mod } 61)$ olduğundan $\left(\frac{-42}{61}\right) = \left(\frac{19}{61}\right)$ yazılabilir. Buradan da

$$\left(\frac{19}{61}\right) = (-1)^{\frac{19-1}{2}\cdot\frac{61-1}{2}}\left(\frac{61}{19}\right) = (-1)^{9\cdot 30}\left(\frac{61}{19}\right) = \left(\frac{61}{19}\right) = \left(\frac{4}{19}\right) = \left(\frac{2^2}{19}\right) = 1$$

bulunur.

Teorem 2.11. $p > 2$ olmak üzere p ve q asal sayılar ve $q > p$ olsun. Bu takdirde aşağıdakiler doğrudur.

(1) $p \equiv 1(\text{mod } 4)$ ise $q = 4pk + r, 0 < r < 4p$ olmak üzere $\left(\frac{p}{q}\right) = \left(\frac{r}{p}\right)$ eşitliği vardır.

(2) $p \equiv 3(\text{mod } 4)$ ise $q = 4pk \mp r, 0 < r < 4p$ olacak biçimde bir *r* tam sayısı vardır ve $\left(\frac{p}{q}\right) = \left(\frac{r}{p}\right)$ eşitliği geçerlidir [1].

İspat: (1) $p \equiv 1(\text{mod } 4)$ olsun. Teorem 1.1'e göre $q = 4pk + r, 0 < r < 4p$ olacak biçimde yazılabilir. Böylece $q \equiv r(\text{mod } p)$ olduğu kullanılırsa Teorem 2.7'ye göre $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right)$ elde edilir. Öte yandan $p \equiv 1(\text{mod } 4)$ olduğundan $\frac{p-1}{2}$ bir çift tam sayıdır.

Böylece $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{q}{p}\right) = \left(\frac{r}{p}\right)$ bulunur.

(2) Benzer şekilde Teorem 1.1'e göre $q = 4pk + r_0, 0 < r_0 < 4p$ olacak biçimde yazılabilir. İlk olarak $r_0 \equiv 1(\text{mod } 4)$ olsun. Bu durumda $r = r_0$ olarak alınırsa $r \equiv 1(\text{mod } 4)$ ve $q \equiv r(\text{mod } 4)$ olduğundan $q \equiv 1(\text{mod } 4)$ olur. Böylece $\frac{q-1}{2}$ tam sayısı çifttir. Dolayısıyla

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

elde edilir. Eğer $r_0 \equiv 3(\text{mod } 4)$ ise $r = 4p - r_0$ ve $k_1 = k + 1$ olmak üzere $q = 4pk + r_0 = 4pk + 4p - r = 4p(k+1) - r = 4pk_1 - r$ yazılabilir. Böylece $r \equiv -r_0(\text{mod } 4)$ ve $q \equiv -r(\text{mod } 4)$ olduğundan $q \equiv r_0(\text{mod } 4)$ yani $q \equiv 3(\text{mod } 4)$ elde edilir. Dolayısıyla $(q-1)/2$ tam sayısının tek olduğu kullanılırsa

$$\begin{aligned}\left(\frac{p}{q}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right) = -\left(\frac{q}{p}\right) = -\left(\frac{-r}{p}\right) = -\left(\frac{-1}{p}\right)\left(\frac{r}{p}\right)\\ &= -(-1)^{\frac{p-1}{2}}\left(\frac{r}{p}\right)\\ &= \left(\frac{r}{p}\right)\end{aligned}$$

elde edilir.

Teorem 2.12. $q > 2$ bir asal sayı olsun. Bu takdirde,

(1) $2^{\frac{q-1}{2}} \equiv 1(\text{mod } q) \Leftrightarrow \left(\frac{2}{q}\right) = 1 \Leftrightarrow q \equiv \mp 1(\text{mod } 8)$

(2) $2^{\frac{q-1}{2}} \equiv -1(\text{mod } q) \Leftrightarrow \left(\frac{2}{q}\right) = -1 \Leftrightarrow q \equiv \mp 3(\text{mod } 8)$

özellikleri doğrudur [1].

İspat: (1) $\Leftarrow$) $q \equiv 1(\text{mod } 8)$ ise $q = 1 + 8k$ olacak biçimde bir k tam sayısı vardır. Dolayısıyla $(q^2-1)/8 = \frac{(q-1)(q+1)}{8} = k(8k+2)$ ve böylece $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = 1$ elde edilir. $q \equiv -1(\text{mod } 8)$ ise benzer biçimde $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = 1$ olduğu görülür.

$\Rightarrow$) $\left(\frac{2}{q}\right) = 1$ ise $(-1)^{\frac{q^2-1}{8}} = 1$ olur. Dolayısıyla $(q^2-1)/8$ bir çift tam sayıdır. Bu ise $16|q^2-1$ olduğunu gösterir. q asal sayısı 8 tam sayısına bölünerek $r \in \{1,3,5,7\}$ olmak üzere $q = 8k + r$ biçiminde yazılabilir. Diğer yandan $q^2 - 1 = (8k+r)^2 - 1 = 64k^2 + 16kr + r^2 - 1$ ve $16|q^2-1$ olduğundan $16|r^2-1$ olmalıdır. Bu ise $r = 1$ veya $r = 7$ olduğunu gösterir. Dolayısıyla $q \equiv \mp 1 (\text{mod } 8)$ elde edilir.

(2) özelliğinin ispatı benzer yolla yapılır.

Teorem 2.13. p, q farklı tek asal sayılar ve $p \equiv q (\text{mod } 4a)$ olsun. Bu durumda $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ eşitliği doğrudur [1].

Teorem 2.14. $p > 2$ asal sayısı verilsin. Bu durumda;

(1) $\left(\frac{-2}{p}\right) = 1 \Leftrightarrow p \equiv 1(\text{mod } 8)$ veya $p \equiv 3(\text{mod } 8)$,

(2) $\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv 1(\text{mod } 12)$ veya $p \equiv 11(\text{mod } 12)$,

(3) $\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1(\text{mod } 3)$,

(4) $\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv 1(\text{mod } 5)$ veya $p \equiv 4(\text{mod } 5)$,

(5) $\left(\frac{-7}{p}\right) = 1 \Leftrightarrow p \equiv 1,2,4(\text{mod } 7)$

özellikleri doğrudur [1].

İspat: (1) $\left(\frac{-2}{p}\right) = 1$ olsun. Dolayısıyla

$$1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8} = (-1)^{\frac{p^2+4p-5}{8}}$$

yazılabilir. Bu ise $(p^2+4p-5)/8$ tam sayısının çift tam sayı olduğunu gösterir. Dolayısıyla $p^2 + 4p - 5 = 16k$ olacak biçimde bir k tam sayısı vardır. p asal sayısı 8 sayısına bölünerek $r \in \{1,3,5,7\}$ olmak üzere $p = 8q + r$ biçiminde yazılabilir. Buradan

$$p^2+4p-5=(8q+r)^2+4(8q+r)-5=16(4q^2+qr+2q)+r^2+4r-5$$

elde edilir. Şu halde $16|r^2+4r-5$ olur. Bu ise $r=1$ veya $r=3$ olmasını gerektirir. Yani $p\equiv 1(\text{mod } 8)$ veya $p\equiv 3(\text{mod } 8)$ olur. Tersine $p\equiv 1(\text{mod } 8)$ veya $p\equiv 3(\text{mod } 8)$ ise $\left(\frac{-2}{p}\right)=1$ olduğu benzer biçimde gösterilir.

(2) $\left(\frac{3}{p}\right)=1$ olsun. Dolayısıyla $1=\left(\frac{3}{p}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right)=(-1)^{(p-1)/2}\left(\frac{p}{3}\right)$ yazılabilir. Bu ise $(-1)^{(p-1)/2}$ ile $\left(\frac{p}{3}\right)$ değerinin aynı olduğunu gösterir. $(-1)^{(p-1)/2}=\left(\frac{p}{3}\right)=1$ olsun. Bu durumda $p\equiv 1(\text{mod } 4)$ ve $p\equiv 1(\text{mod } 3)$ olur. Buradan da $p\equiv 1(\text{mod } 12)$ elde edilir. Şimdi de $(-1)^{\frac{p-1}{2}}=\left(\frac{p}{3}\right)=-1$ olsun. Bu durumda da $p\equiv 3(\text{mod } 4)$ ve $p\equiv 2(\text{mod } 3)$ olduğu görülür. Dolayısıyla $p\equiv -1(\text{mod } 4)$ ve $p\equiv -1(\text{mod } 3)$ ve böylece $p\equiv -1(\text{mod } 12)$ elde edilir. Bu ise $p\equiv 11(\text{mod } 12)$ olduğunu gösterir.

Tersine $p\equiv 1(\text{mod } 12)$ veya $p\equiv 11(\text{mod } 12)$ ise $\left(\frac{3}{p}\right)=1$ olduğunu gösterelim. Önce $p\equiv 1(\text{mod } 12)$ olsun. Bu durumda $p\equiv 1(\text{mod } 4)$ ve $p\equiv 1(\text{mod } 3)$ olacaktır. Dolayısıyla $(p-1)/2$ tam sayısının çift olduğu kullanılırsa $\left(\frac{3}{p}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)=\left(\frac{1}{3}\right)=1$ elde edilir. Eğer $p\equiv 11(\text{mod } 12)$ ise benzer ispat yapılır.

(3) Üstteki özellik kullanılarak, bu özelliğin ispatı kolaylıkla yapılabilir.

(4) p asal sayısı $p=5q+r, 0<r<5$ biçiminde yazılabilir. Diğer yandan $\left(\frac{5}{q}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{5}\right)=(-1)^{p-1}\left(\frac{p}{5}\right)=\left(\frac{r}{5}\right)$ olduğu görülür. $\left(\frac{1}{5}\right)=\left(\frac{4}{5}\right)=1$ ve $\left(\frac{2}{5}\right)=\left(\frac{3}{5}\right)=-1$ olduğu dikkate alınırsa istenen elde edilir.

(5) Bu özelliğin ispatı benzer şekilde yapılır.

BÖLÜM 3. $x^2 + Dy^2$ BİÇİMİNDE YAZILABİLEN ASAL SAYILAR

$x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$ biçiminde yazılabilen asal sayılarla Fermat ilgilenmiş ve p asal sayı, $p \equiv 1 (\mathrm{mod}\ 4)$ ise $p = x^2 + y^2$ olacak biçimde x ve y tam sayılarının olduğunu gözlemlemiştir. Fermat, Mersenne'e 1640 yılında yazdığı mektupta aşağıdaki teoremi ifade etmiştir.

Teorem 3.1. p tek asal sayısının $x^2 + y^2$ biçiminde yazılabilmesi için gerekli ve yeterli şart $p \equiv 1 (\mathrm{mod}\ 4)$ olmasıdır. Ayrıca bu yazılıştaki x ve y pozitif tamsayıları tek türlü belirlidir ve x ile y aralarında asaldır.

Bu teoremi Euler ispat etmiştir ve Euler aşağıdaki teoremi bir önceki teoreme eklemiştir.

Teorem 3.2. $n > 1$ tek tam sayı olmak üzere $n = x^2 + y^2$ olacak biçimde tek türlü belirli x ve y pozitif tam sayıları mevcut ve x ile y aralarında asal ise n sayısı asal sayıdır.

Euler bu teoremden hareketle bazı sayıların asal sayı olduğunu görmüştür. Örneğin, $3861317 = 961^2 + 1714^2$ ve $10091401 = 1251^2 + 2920^2$ olduğunu ve bu yazılışların tek türlü olduğunu göstererek 10091401 ve 3861317 sayılarının asal sayı olduğu sonucuna ulaşmıştır. Euler ayrıca $x^2 + 2y^2$, $x^2 + 3y^2$ biçiminde yazılabilen asal sayılarla da ilgilenmiştir. Daha genel olarak a ve b aralarında asal olmak üzere $ax^2 + by^2$ biçiminde yazılabilen doğal sayılarla ilgilenmiştir. Elde ettiği sonuçlar aşağıdaki gibidir. Bu sonuçlar 1763 ve 1774 yıllarında basılmıştır.

Teorem 3.3. (a) p tek asal sayısının $x^2 + 2y^2$ biçiminde yazılabilmesi için gerekli ve yeterli şart $p \equiv 1,3 (\mathrm{mod}\ 8)$ olmasıdır. Ayrıca p'nin $x^2 + 2y^2$ biçimindeki yazılışındaki x ve y pozitif tam sayıları tek türlü belirlidir ve x ile y aralarında asaldır.
(b) Eğer $n > 1$ tek doğal sayısı için tek türlü belirli x ve y doğal sayıları x ile y aralarında asal ve $n = x^2 + 2y^2$ olacak biçimde mevcut ise n sayısı asal sayıdır.

Teorem 3.4. (a) $p > 3$ asal sayısının $x^2 + 3y^2$ biçiminde yazılabilmesi için gerekli ve yeterli şart $p \equiv 1 (\mathrm{mod}\ 3)$ olmasıdır. Ayrıca bu yazılıştaki x ve y pozitif tam sayıları tek türlü belirlidir ve x ile y aralarında asaldır.
(b) $n > 1$ tek doğal sayısı için tek türlü belirli aralarında asal x ve y pozitif tam sayıları $n = x^2 + 3y^2$ olacak biçimde mevcut ise n asaldır.

Bu teoremi kullanarak Euler, $1000003 = 1000^2 + 3 \cdot 1^2 = 16^2 + 3 \cdot 57^2$ olduğunu görerek 1000003 sayısının asal sayı olmadığını görmüştür. Gerçekten $1000003 = 7 \cdot 1429$ dır. Euler Teorem 3.3'ün ispatında sadece $p \equiv 3 (\mathrm{mod}\ 8)$ ise $p = x^2 + 2y^2$ olacak biçimde x ve y tam sayılarının mevcut olduğunu göstermemiştir. Bu kısmı ve Teorem 3.3 ile Teorem 3.4'ün (a) şıklarının ispatını Lagrange 1775 yılında yapmıştır.

Yukarıdaki Teoremlerin b) şıkkındaki ifadeler doğru değildir. Örneğin, $9 = 1^2 + 2 \cdot 2^2$ ve 9'un bu şekilde yazılışı tek türlü olmasına rağmen 9 asal sayı değildir. Ayrıca $25 = 3^2 + 4^2$ olarak tek türlü yazılabilir. Fakat 25 asal sayı değildir. Benzer biçimde $49 = 3 \cdot 4^2 + 1^2$ olup bu yazılış tek türlüdür fakat 49 asal sayı değildir.

Bu konuyla ilgili detaylı bilgi için [2] ve [3] numaralı kaynaklara bakılabilir.

Teorem 3.5 (Thue'nun Lemması). $n > 1$ ve n doğal sayısı bir tam sayının karesi olmasın. Bu durumda a ve b herhangi iki tam sayı ise $|x| < \sqrt{n}, |y| < \sqrt{n}$ ve $ax \equiv by (\mathrm{mod}\ n)$ olacak biçimde ikisi de aynı anda sıfır olmayan x ve y tam sayıları vardır. Özellikle $(a, b) = (b, n) = 1$ ise x ve y tam sayılarının ikisi de sıfırdan farklıdır [1].

İspat: $\sqrt{n}$ tam sayı olmadığından $k < \sqrt{n} < k+1$ olacak şekilde bir k tamsayısı vardır. Dolayısıyla $(k+1)^2 > n$ olur. $0 \leq r \leq k$ ve $0 \leq s \leq k$ olmak üzere $ar + bs$ biçimindeki tam sayıları düşünelim. Bu türdeki tam sayıların sayısı $(k+1)^2$ tanedir. $(k+1)^2 > n$ olduğundan Sonuç 1.12'ye göre $n|(ax_1 + by_1) - (ax_2 + by_2)$ olacak biçimde $(x_1, y_1) \neq (x_2, y_2)$ şartını sağlayan x_1, y_1, x_2, y_2 tam sayıları vardır. $x = x_1 - x_2$ ve $y = y_1 - y_2$ olarak alınırsa $n|ax - by$, yani $ax \equiv by (\mathrm{mod} n)$ olduğu görülür. Ayrıca $0 \leq x_1, y_1, x_2, y_2 \leq k$ olduğu dikkate alınırsa $|x| = |x_1 - x_2| \leq k < \sqrt{n}$ ve $|y| = |y_1 - y_2| \leq k < \sqrt{n}$ yazılabilir. Diğer yandan x ve y tam sayıları aynı anda sıfır olursa $x_1 = x_2$ ve $y_1 = y_2$ olacağından bu $(x_1, y_1) \neq (x_2, y_2)$ olmasıyla çelişir. Şu halde x ve y tam sayıları aynı anda sıfır olamaz. $(a, n) = (b, n) = 1$ ve $x = 0$ ise $by \equiv 0 (\mathrm{mod}\, n)$ ve buradan da $y \equiv 0 (\mathrm{mod}\, n)$ bulunur. Bu ise $y = 0$ olmasını gerektirir. Buradan $x_1 = x_2$ ve $y_1 = y_2$ elde edilir. Bu durum $(x_1, y_1) \neq (x_2, y_2)$ olmasına aykırıdır. Benzer biçimde $y = 0$ ise çelişki elde edilir. Dolayısıyla $(a, n) = (b, n) = 1$ ise $x \neq 0$ ve $y \neq 0$ olur. Bu ise ispatı tamamlar.

Aşağıda vereceğimiz teorem Fermat'nın iki kare teoremi olarak bilinir. Bu teoremin ispatı değişik yollardan yapılmıştır. Bununla ilgili olarak [4] numaralı kaynağa bakılabilir. Burada Teorem 3.5 kullanılarak ispat yapılacaktır.

Teorem 3.6. p bir tek asal sayı olsun. $p = a^2 + b^2$ olacak biçimde a ve b tam sayılarının olması için gerekli ve yeterli şart $p \equiv 1 (\mathrm{mod}\ 4)$ olmasıdır [1].

İspat: $p \equiv 1 (\mathrm{mod}\ 4)$ ise Teorem 1.2.7'ye göre $p|r^2 + 1$ olacak biçimde bir r tamsayısı vardır. Teorem 3.5'e göre $1 \cdot x \equiv r \cdot y (\mathrm{mod}\, p)$ olacak biçimde $|x| < \sqrt{p}$ ve $|y| < \sqrt{p}$ şartlarını sağlayan ve ikisi aynı anda sıfır olmayan x, y tamsayıları vardır. Buradan $x^2 + y^2 \equiv r^2 y^2 + y^2 (\mathrm{mod}\, p)$, yani $x^2 + y^2 \equiv (1 + r^2) y^2 (\mathrm{mod}\, p)$ elde edilir. $p|r^2 + 1$ olduğu kullanılırsa $p|x^2 + y^2$ bulunur. Ayrıca x ve y tamsayılarının ikisi de aynı anda sıfır olmadığından $0 < x^2 + y^2 < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p$ yazılabilir. $p|x^2 + y^2$ ve $0 < x^2 + y^2 < 2p$ olduğundan $p = x^2 + y^2$ elde edilir.

Eğer p tek asal sayısı için $p = a^2 + b^2$ olacak biçimde a ve b tam sayıları mevcut ise a ve b tam sayılarının biri çift diğeri tek olmak zorundadır. Aksi halde ikisi de çift veya ikisi de tek ise $2|p$ bulunur. a tek ve b çift tam sayı ise $a^2 \equiv 1(\text{mod } 4)$ ve $b^2 \equiv 0(\text{mod } 4)$ olacağından $p = a^2 + b^2 \equiv 1 + 0(\text{mod } 4)$, yani $p \equiv 1(\text{mod } 4)$ elde edilir.

Önerme 3.7. p, m ve n tam sayılarını bölmeyen bir asal sayı olsun. $p > 2$ ve $p = ma^2 + nb^2$ olacak biçimde a ve b tam sayıları varsa $\left(\frac{m}{p}\right) = \left(\frac{-n}{p}\right)$ dir. Özellikle p, n tam sayısını bölmüyor ve $p = a^2 + nb^2$ ise $\left(\frac{-n}{p}\right) = 1$ dir.

İspat: $p = ma^2 + nb^2$ ise $ma^2 \equiv -nb^2(\text{mod } p)$ ve böylece

$$\left(\frac{m}{p}\right) = \left(\frac{ma^2}{p}\right) = \left(\frac{-nb^2}{p}\right) = \left(\frac{-n}{p}\right)$$

elde edilir.

Aşağıda vereceğimiz 5 teoremin ispatı için [5] numaralı kaynağa bakılabilir. Bu teoremlerin ispatında da Teorem 3.5 kullanılacaktır.

Teorem 3.8. p bir asal sayı olsun. $p = x^2 + 2y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p = 2$ veya $p \equiv 1,3(\text{mod } 8)$ dir.

İspat. $p = 2$ ise $x = 0$ ve $y = 1$ alınır. $p > 2$ ve $p \equiv 1,3(\text{mod } 8)$ ise Teorem 2.14'ün (1) özelliğine göre $\left(\frac{-2}{p}\right) = 1$ olur. Dolayısıyla $u^2 \equiv -2(\text{mod } p)$ olacak biçimde bir u tam sayısı vardır. Teorem 3.5'e göre $x \equiv uy(\text{mod } p)$ ve $0 < |x| < \sqrt{p},\ 0 < |y| < \sqrt{p}$ şartını sağlayan x, y tam sayıları vardır. Böylece $x^2 + 2y^2 \equiv y^2(u^2 + 2)(\text{mod } p)$ elde edilir. Bu ise $p|x^2 + 2y^2$ olduğunu gösterir. $0 < x^2 + 2y^2 < p + 2p = 3p$ olduğundan $x^2 + 2y^2 = p$ veya $x^2 + 2y^2 = 2p$ olur. Eğer $x^2 + 2y^2 = p$ ise ispat biter. Şimdi $x^2 + 2y^2 = 2p$ olsun. Bu durumda x tam sayısı çift olur. $x = 2x_1$ olsun.

Buradan $2p = x^2 + 2y^2 = 4x_1 + 2y^2 = 2(y^2 + 2x_1^2)$ ve böylece $p = y^2 + 2x_1^2$ elde edilir. Tersine $p > 3$ ve $p = x^2 + 2y^2$ olacak biçimde x, y tam sayıları varsa Önerme 3.7'ye göre $\left(\frac{-2}{p}\right) = 1$ dir. Teorem 2.14 dikkate alınırsa $p \equiv 1,3 (\mathrm{mod}\ 8)$ olduğu görülür.

Teorem 3.9. p bir asal sayı olsun. $p = x^2 + 3y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p = 3$ veya $p \equiv 1 (\mathrm{mod}\ 3)$ dir.

İspat: $p = 3$ ise $3 = 0^2 + 3 \cdot 1^2$ dır. Şimdi $p \equiv 1 (\mathrm{mod}\ 3)$ olsun. Bu durumda $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$ olduğu kullanılırsa

$$\begin{aligned}\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right)\\ &= \left(\frac{-1}{p}\right)(-1)^{\frac{p-1}{2}}\left(\frac{1}{3}\right)\\ &= (-1)^{(p-1)/2}(-1)^{(p-1)/2}\\ &= 1\end{aligned}$$

elde edilir. Dolayısıyla $x^2 \equiv -3 (\mathrm{mod}\ p)$ kongrüansının bir çözümü vardır. Bu ise $p \nmid a$ olmak üzere $a^2 + 3 \equiv 0 (\mathrm{mod}\ p)$ olacak biçimde bir a tam sayısının mevcut olduğunu gösterir. Teorem 3.5'e göre, $0 < |x| < \sqrt{p}$ ve $0 < |y| < \sqrt{p}$ olmak üzere $ay \equiv x (\mathrm{mod}\ p)$ olacak biçimde x, y tam sayıları vardır. Buradan $a^2y^2 + 3y^2 \equiv x^2 + 3y^2 (\mathrm{mod}\ p)$ yazılabilir. $a^2 + 3 \equiv 0 (\mathrm{mod}\ p)$ olduğu kullanılırsa $x^2 + 3y^2 \equiv 0 (\mathrm{mod}\ p)$ elde edilir. $0 < x^2 < p$ ve $0 < y^2 < p$ olduğundan $0 < x^2 + 3y^2 < p + 3p = 4p$ bulunur. $p | x^2 + 3y^2$ olduğundan $x^2 + 3y^2 = pk$ olacak biçimde k doğal sayısı vardır ve k doğal sayısı 1,2,3 değerlerini alabilir. $k = 1$ ise $x^2 + 3y^2 = p$ olur. $k = 2$ ise x ve y tam sayılarının ikisi de çifttir veya ikisi de tektir. Her iki durumda da $4 | 2p$ elde edilir. Bu ise mümkün değildir. $k = 3$ ise $x^2 + 3y^2 = 3p$ olacağından $3 | x$ olur. $x = 3z$ olsun. Bu durumda $3p = x^2 + 3y^2 = 9z^2 + 3y^2 = 3(y^2 + 3z^2)$, yani $p = y^2 + 3z^2$ elde edilir. Bu ise ispatı tamamlar. Eğer $p > 3$ ve $x^2 + 3y^2 = p$ olacak biçimde x, y tam sayıları varsa Önerme 3.7'ye ve Teorem 2.14'e göre $p \equiv 1 (\mathrm{mod}\ 3)$ olduğunu görmek kolaydır.

Teorem 3.10. p bir asal sayı olsun. $p = x^2 + 7y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p = 7$ veya $p \equiv 1,2,4 (\text{mod } 7)$ dir.

İspat: $p = 7$ ise $x = 0$ ve $y = 1$ alınır. Şimdi $p > 7$ ve $p \equiv 1,2,4(\text{mod } 7)$ olsun. Teorem 2.14'ün (5) özelliğine göre $\left(\frac{-7}{p}\right) = 1$ olur. Bu ise $w^2 \equiv -7(\text{mod } p)$ olacak biçimde bir w tam sayısının mevcut olduğunu gösterir. Teorem 3.5'e göre $x \equiv wy(\text{mod } p)$ olacak biçimde $0 < |x| < \sqrt{p}$, $0 < |y| < \sqrt{p}$ şartlarını sağlayan x, y tam sayıları vardır. Böylece $x^2 + 7y^2 \equiv (w^2y^2 + 7y^2) \equiv y^2(w^2 + 7)(\text{mod } p)$, yani $p|x^2 + 7y^2$ elde edilir. $0 < x^2 + 7y^2 < p + 7p = 8p$ olduğundan $x^2 + 7y^2 = kp$ olacak biçimde $k \in \{1,2,3,4,5,6,7\}$ mevcuttur. Eğer $x^2 + 7y^2 = p$ veya $x^2 + 7y^2 = 7p$ ise ispat açıktır. $x^2 + 7y^2 = 4p$ ise x ve y tam sayılarından ikisi birden tek veya ikisi birden çift olmalıdır. x ve y tam sayılarının ikisi de tek ise $x^2 \equiv 1(\text{mod } 8)$, $y^2 \equiv 1(\text{mod } 8)$ olacağından $x^2 + 7y^2 = 8(\text{mod } 8)$, yani $8|x^2 + 7y^2$ bulunur. Bu ise $8|4p$ olmasını gerektirir. Bu mümkün değildir. Şu halde x ve y tam sayılarının ikisi de çift tam sayıdır. $x = 2a, y = 2b$ olsun. $4p = x^2 + 7y^2 = 4(a^2 + 7b^2)$ ve buradan da $p = a^2 + 7b^2$ bulunur. Diğer yandan $x^2 + 7y^2 = 2p$ ise x ve y aynı anda tek olamaz Çünkü bu durumda $8|x^2 + 7y^2$, yani $8|2p$ olur. Bu ise mümkün değildir. Dolayısıyla x ve y aynı anda çift olmalıdır. Bu durumda da $2|p$ bulunur. Şu halde $x^2 + 7y^2 = 2p$ olamaz. Eğer $x^2 + 7y^2 = 5p$ ise $x^2 \equiv -7y^2(\text{mod } 5)$ olup $1 = \left(\frac{x^2}{5}\right) = \left(\frac{-7y^2}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right) = 1 \cdot (-1) = -1$ elde edilir. Bu ise bir çelişkidir. Benzer biçimde $x^2 + 7y^2 = 3p$ olamayacağı da gösterilebilir. Çünkü $x^2 + 7y^2 = 3p$ ise $1 = \left(\frac{x^2}{3}\right) = \left(\frac{-7y^2}{3}\right) = \left(\frac{2}{3}\right) = \left(\frac{-1}{3}\right) = -1$ olur. Bu ise bir çelişkidir. $x^2 + 7y^2 = 6p$ olamayacağı benzer yolla gösterilir. $p > 7$ ve $p = x^2 + 7y^2$ olacak biçimde x ve y tam sayıları varsa Önerme 3.7'ye ve Teorem 2.14'e göre $p \equiv 1,2,4(\text{mod } 7)$ olduğunu görmek kolaydır.

Teorem 3.11. p bir asal sayı olsun. $p = 2x^2 + 3y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p = 2,3$ veya $p \equiv 5,11(\text{mod } 24)$ dir.

İspat: $p = 2$ ise $x = 1,\ y = 0$ ve $p = 3$ ise $x = 0,\ y = 1$ alınırsa istenilen elde edilir. Eğer $p \equiv 5,11(\text{mod}24)$ ise $\left(\frac{2}{p}\right) = \left(\frac{-3}{p}\right) = -1$ olduğunu görmek kolaydır. c tam sayısını $\left(\frac{c}{p}\right) = -1$ olacak biçimde seçelim. $\left(\frac{2}{p}\right) = \left(\frac{-3}{p}\right) = -1$ olduğundan $\left(\frac{2c}{p}\right) = \left(\frac{-3c}{p}\right) = 1$ olur. Dolayısıyla $r^2 \equiv 2c(\text{mod}\, p)$ ve $s^2 \equiv -3c(\text{mod}\, p)$ olacak biçimde r ve s tam sayıları vardır. Ayrıca $(x, y) \neq (0,0)$ olmak üzere $|x| < \sqrt{p}$, $|y| < \sqrt{p}$ ve $rx \equiv sy(\text{mod}\, p)$ olacak biçimde x ve y tam sayıları vardır. Böylece $2cx^2 + 3cy^2 \equiv r^2x^2 - s^2y^2(\text{mod}\, p)$ ve buradan da $2cx^2 + 3cy^2 \equiv (rx - sy)(rx + sy)(\text{mod}\, p)$ elde edilir. $p|rx - sy$ olduğundan $p|2cx^2 + 3cy^2$ bulunur. $p \nmid c$ olduğu kullanılırsa $p|2x^2 + 3y^2$ bulunur. $0 < 2x^2 + 3y^2 < 2p + 3p = 5p$ olduğu dikkate alınırsa $2x^2 + 3y^2 = p,\ 2x^2 + 3y^2 = 2p,\ 2x^2 + 3y^2 = 3p$ veya $2x^2 + 3y^2 = 4p$ olduğu görülür. $2x^2 + 3y^2 = p$ ise ispat biter. $2x^2 + 3y^2 = 2p$ veya $2x^2 + 3y^2 = 3p$ olamayacağı $p \equiv 5,11(\text{mod}\ 24)$ olduğu kullanılarak gösterilebilir. Şu halde $2x^2 + 3y^2 = 4p$ olur. Bu durumda da y tam sayısının çift ve dolayısıyla x tam sayısının da çift olduğu görülür. $x = 2a, y = 2b$ olsun. Buradan $4p = 2x^2 + 3y^2 = 4(2a^2 + 3b^2)$ ve dolayısıyla $p = 2a^2 + 3b^2$ elde edilir. $p > 3$ ve $p = 2x^2 + 3y^2$ olacak biçimde x ve y tam sayıları varsa Önerme 3.7'ye ve Teorem 2.14'e göre $p \equiv 5,11(\text{mod}\ 24)$ olduğu gösterilebilir.

Teorem 3.12. p bir asal sayı olsun. $p = x^2 + 5y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p = 5$ veya $p \equiv 1,9(\text{mod}\ 20)$ dir.

İspat: $\Rightarrow$) $p > 5$ ve $p = x^2 + 5y^2$ olacak biçimde x ve y tam sayıları mevcut olsun. Önerme.3.7'ye göre $\left(\frac{-5}{p}\right) = 1$ yazılabilir. Eğer $p \equiv 3(\text{mod}4)$ ise

$$1 = \left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = -\left(\frac{5}{p}\right) = -\left(\frac{p}{5}\right)$$

bulunur. Bu ise $\left(\frac{p}{5}\right) = -1$ olduğunu gösterir. Buradan da $p \equiv \mp 3(\text{mod}\ 5)$ elde edilir. Böylece $p = x^2 + 5y^2$ olduğu kullanılırsa $x^2 \equiv \mp 3(\text{mod}\, 5)$ yazılabilir. Bu ise $\left(\frac{\mp 3}{5}\right) = 1$ olmasını gerektirir. Bu olamaz. Çünkü basit bir hesaplamayla

$\left(\frac{3}{5}\right) = \left(\frac{-3}{5}\right) = -1$ olduğu görülebilir. Şu halde $p \equiv 3(\text{mod } 4)$ olamaz. Dolayısıyla $p \equiv 1(\text{mod } 4)$ olur. Eğer $p \equiv 1(\text{mod } 4)$ ise

$$1 = \left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{5}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}} = \left(\frac{p}{5}\right)$$

olur. Bu ise $p \equiv 1,4(\text{mod } 5)$ olmasını gerektirir. $p \equiv 1(\text{mod } 5)$ ise $p \equiv 1(\text{mod } 4)$ olduğundan $p \equiv 1(\text{mod } 20)$ elde edilir. Eğer $p \equiv 4(\text{mod } 5)$ ve $p \equiv 1(\text{mod } 4)$ ise $p \equiv 9(\text{mod } 5)$ ve $p \equiv 9(\text{mod } 4)$ olduğu kullanılarak $p \equiv 9(\text{mod } 20)$ elde edilir.

$\Leftarrow$) $p \equiv 1,9(\text{mod } 20)$ ise $p \equiv 1(\text{mod } 4)$ ve $p \equiv \mp 1(\text{mod } 5)$ olduğu kullanılarak

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{\mp 1}{5}\right) = 1$$

elde edilir. Dolayısıyla $a^2 \equiv -5(\text{mod } p)$ olacak biçimde a tam sayısı vardır. Teorem 3.5'e göre, $0 < |x| < \sqrt{p}$ ve $0 < |y| < \sqrt{p}$ olmak üzere $ax \equiv y(\text{mod } p)$ olacak biçimde x ve y tam sayıları vardır. Buradan $p|5x^2 + y^2$ elde edilir. Ayrıca $x^2 + 5y^2 < p + 5p = 6p$ olduğundan $x^2 + 5y^2 = pk$ ise $1 \leq k \leq 5$ olur. Eğer $k = 2$ ise x ve y tam sayıları aynı anda tektir veya aynı anda çifttir. Eğer x ve y tam sayıları tek tam sayı ise $2p = 5x^2 + y^2 \equiv 5 \cdot 1 + 1 \equiv 6(\text{mod } 8)$ olur. Bu ise $p \equiv 3(\text{mod } 4)$ olmasını gerektirir. Bu da $p \equiv 1(\text{mod } 4)$ olmasıyla çelişir. Eğer x ve y tam sayıları aynı anda çift ise $4|2p$ olduğu görülür. Bu olamaz. Şu halde $k = 2$ olamaz. Benzer biçimde $k = 4$ olamayacağı gösterilebilir. $k = 3$ ise $3p = 5x^2 + y^2$ olur. $p \equiv 1(\text{mod } 4)$ olduğundan $5x^2 + y^2 = 3p \equiv 3(\text{mod } 4)$, yani $x^2 + y^2 \equiv 3(\text{mod } 4)$ elde edilir. Bu olamaz. Şu halde $k = 1$ veya $k = 5$ olabilir. $k = 1$ ise ispat biter. $k = 5$ ise $5p = 5x^2 + y^2$ olur. Buradan $5|y$ bulunur. Böylece $p = x^2 + 5(y/5)^2$ elde edilir.

Tanım 3.13. A, B ve C birer tam sayı olmak üzere $q(x, y) = Ax^2 + Bxy + Cy^2$ iki değişkenli polinomuna bir ikinci dereceden iki değişkenli form (binary quadratic form) veya kısaca iki değişkenli form denir. Eğer $q(u, v) = Au^2 + Buv + Cv^2 = m$ olan u

ve v tam sayıları varsa m tam sayısı $q(x,y)$ tarafından temsil edilir denir. Eğer ayrıca u ile v aralarında asal ise m'ye $q(x,y)$ tarafından ilkel biçimde temsil edilir denir.

Tanım 3.14. Eğer $q(x,y)=0$ iken $(x,y)=0$ elde ediliyorsa $q(x,y)$'ye yön bağımlı (anisotropic) iki değişkenli form denir. Eğer $q(x,y)\geq 0$ ve $q(x,y)=0$ iken $(x,y)=0$ elde ediliyorsa $q(x,y)$ ye pozitif tanımlıdır denir. Ayrıca A,B,C tamsayıları aralarında asal ise $q(x,y)$ ye iki değişkenli ilkel form denir [6,7].

Tanım 3.15. p,q,r,s tam sayıları $ps-qr=\mp 1$ şartını sağlamak üzere $Q'(x,y)=Q(px+ry,qx+sy)$ olacak biçimde mevcut ise $Q(x,y)$ ve $Q'(x,y)$ iki değişkenli formlarına denktirler denir.

Tanım 3.16. $q(x,y)=Ax^2+Bxy+Cy^2$ iki değişkenli formunda $\Delta=B^2-4AC$ değerine iki değişkenli formun diskriminantı denir.

Önerme 3.17. Denk iki değişkenli formların diskriminantları eşittir [1].

İspat. $f(x,y)=ax^2+bxy+cy^2$ iki değişkenli formu için $M_f=\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ olarak tanımlansın. Bu durumda $f(x,y)=\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ olarak yazılabilir ve f'nin diskriminantı $-4\det M_f$ olur. Şimdi $Q(x,y)$ ve $Q'(x,y)$ denk iki değişkenli formlar olsunlar. Bu durumda $Q(x,y)=Ax^2+Bxy+Cy^2$ ve $ps-qr=\mp 1$ olmak üzere $Q'(x,y)=Q(px+ry,qx+sy)$ dir. Ayrıca $Q(x,y)=\begin{pmatrix} x & y \end{pmatrix}\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ olup $Q(x,y)$'nin diskriminantı $B^2-4AC=-4\det M_Q$ dır. Öte yandan $P=\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ olmak üzere

$$Q'(x,y)=Q(px+ry,qx+sy)=\begin{pmatrix} px+ry & qx+sy \end{pmatrix}\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}\begin{pmatrix} px+ry \\ qx+sy \end{pmatrix}$$

$$= (x \quad y)\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = (x \quad y)PM_QP^T\begin{pmatrix} x \\ y \end{pmatrix}$$

olarak yazılabilir. $Q'(x,y)$ nin diskriminantı

$$\begin{aligned} -4\det\left(PM_QP^T\right) &= -4\left(\det P \det M_Q \det P^T\right) \\ &= -4(\det P)^2 \det M_Q \\ &= -4\det M_Q \\ &= B^2 - 4AC \end{aligned}$$

olarak elde edilir.

Önerme 3.18. n sayısı $Q(x,y) = Ax^2 + Bxy + Cy^2$ iki değişkenli formu tarafından ilkel biçimde temsil edilsin. Bu durumda $\Delta = B^2 - 4AC$, n modülüne göre bir karedir [6].

İspat. $n = Q(p,q)$ ve $(p,q) = 1$ şartını sağlayan p ve q tam sayıları mevcut olsun. O zaman $ps - qr = 1$ olan r ve s tam sayıları mevcuttur.

$$\begin{aligned} Q'(x,y) &= Q(px + ry, qx + sy) \\ &= A(px + ry)^2 + B(px + ry)(qx + sy) + C(qx + sy)^2 \\ &= x^2(Ap^2 + Bpq + Cq^2) + (2prA + (ps + qr)B + 2qsC)xy + \\ &(Ar^2 + Brs + Cs^2)y^2 \\ &= x^2n + (2prA + (ps + qr)B + 2qsC)xy + Q(r,s)y^2 \end{aligned}$$

olsun. O zaman Q' ve Q iki değişkenli denk formlardır. Önerme 3.17'ye göre Q' ve Q iki değişkenli formlarının diskriminantları eşit olduğundan

$$B^2 - 4AC = (2prA + (ps + qr)B + 2qsC)^2 - 4nQ(r,s)$$

olup

$$B^2 - 4AC \equiv (2prA + (ps + qr)B + 2qsC)^2 (\text{mod } n)$$

olur. Yani $B^2 - 4AC$, n modülüne göre karedir.

Teorem 3.19. c ve d pozitif tam sayılar ve p asal sayı olsun. Eğer $p = cx^2 + dy^2$ olacak biçimde x ve y pozitif tam sayıları varsa x ve y tek türlü belirlidir [1].

İspat. $p = cx^2 + dy^2, p = cu^2 + dv^2$ olacak biçimde x, y, u, v pozitif tam sayıları mevcut olsun. $p = cx^2 + dy^2$ ve $p = cu^2 + dv^2$ olduğundan $d = \frac{p-cx^2}{y^2}$ ve $d = \frac{p-cu^2}{v^2}$ dir. O halde $\frac{p-cx^2}{y^2} = \frac{p-cu^2}{v^2}$ ve buradan da $pv^2 - cx^2v^2 = py^2 - cu^2y^2$ elde edilir. Dolayısıyla $p(y^2 - v^2) = c(u^2y^2 - v^2x^2)$ dir. Böylece $p|c(u^2y^2 - v^2x^2)$ dır. $0 < c < p$ olduğundan $p \nmid c$ dir. O halde $p|u^2y^2 - v^2x^2$ elde edilir. Dolayısıyla $p|uy - vx$ veya $p|uy + vx$ dir. $p|uy - vx$ olsun. $p^2 = (cxu + dyv)^2 + cd(uy - vx)^2$ olduğundan $cd = 1$ ve $uy - vx = 0$ olmalıdır. Buradan $u = x, y = v$ elde edilir. Çünkü burada $(x, y) = (u, v) = 1$ dir. Eğer $p|uy + vx$ ise $p^2 = (cxu - dyv)^2 + cd(uy + vx)^2$ olduğundan bu durumda da $cd = 1$ ve $cxu - dyv = 0$ olmalıdır. Yani $xu - yv = 0$ ve böylece $x = v$, $y = u$ elde edilir. Sonuç olarak ya $x = u$, $y = v$ ya da $x = v$, $y = u$ olur. Yani p'nin yazılışındaki x ve y ler tek türlü belirlidir.

Önerme 3.20. $Q(x, y) = Ax^2 + Bxy + Cy^2$ primitif(ilkel) yön bağımlı iki değişkenli form olsun. $\Delta = B^2 - 4AC$ ve p tek asal sayı olsun. Eğer p asal sayısı için $\left(\frac{\Delta}{p}\right) = -1$ ise

1) $p|Q(x, y)$ olduğunda $p|x$ ve $p|y$ dir.

2) Eğer $(x, y) \neq (0,0)$ ise $\gamma_p\big(Q(x, y)\big)$ çifttir. Burada $\gamma_p(Q(x, y))$, $p^t|Q(x, y)$ şartını sağlayan en büyük pozitif t tam sayısını göstermektedir [6,7].

İspat. 1) $p|Q(x, y)$ ise $p|4AQ(x, y)$, yani $p|4A(Ax^2 + Bxy + Cy^2)$ dir. O halde $p|(2Ax + By)^2 - (B^2 - 4AC)y^2$ dir. Bu ise $(2Ax + By)^2 \equiv (B^2 - 4AC)y^2 (\text{mod } p)$ olduğunu gösterir. Dolayısıyla $(2Ax + By)^2 = \Delta y^2 (\text{mod } p)$ dir. $p \nmid y$ olsun. $p \nmid \Delta$ olduğundan $p \nmid 2Ax + By$ dir. Bu durumda $\left(\frac{\Delta y^2}{p}\right) = 1$ dir. Bu ise

$\left(\frac{\Delta}{p}\right) = 1$ olmasını gerektirir. Bu olamaz çünkü $\left(\frac{\Delta}{p}\right) = -1$ dir. O halde $p|y$ dir. Benzer yolla $p|4C(Cy^2 + Bxy + Ax^2)$ olduğu kullanılırsa $p|(2Cy + Bx)^2 - (B^2 - 4AC)x^2$ elde edilir. Buradan da benzer yolla $p|x$ bulunur. Şu halde $p|x$ ve $p|y$ dir.

2) Tersine $\gamma_p\big(Q(x,y)\big)$ tek olsun. O zaman $Q(x,y) = p^{2k+1}b,\ p \nmid b$ olacak şekilde $k \geq 0$ ve b tamsayıları olurdu. 1) şıkkına göre $p|x$ ve $p|y$ olacağından $x = p^{\alpha}t, y = p^{\beta}s, p \nmid t, p \nmid s$ olacak biçimde t ve s tam sayıları vardır. $\alpha \leq \beta$ olsun. $Ax^2 + Bxy + Cy^2 = Q(x,y) = p^{2k+1}b$ olduğundan $p^{2k+1}b = Ap^{2\alpha}t^2 + Bp^{\alpha}tp^{\beta}s + Cp^{2\beta}s^2 = p^{2\alpha}(At^2 + Bp^{\beta-\alpha}ts + Cp^{2\beta-2\alpha}s^2)$ olur. $p \nmid b$ olduğundan $2\alpha > 2k+1$ olamaz. O halde $2\alpha < 2k+1$ dir. Bu durumda $p^{2k+1-2\alpha}b = At^2 + Bp^{\beta-\alpha}ts + p^{2\beta-2\alpha}Cs^2$ olur. $\beta = \alpha$ ise $p^{2k+1-2\alpha}b = At^2 + Bts + Cs^2$ olur. Bu ise $p|s$ ve $p|t$ olmasını gerektirir. Şu halde $\alpha < \beta$ dır. O zaman $p|(At^2 + Bp^{\beta-\alpha}ts + Cp^{2\beta-2\alpha}s^2)$ olduğundan $p|At^2$ elde edilir. $p \nmid t$ olduğu kullanılırsa $p|A$ bulunur. Bu durumda $\Delta = B^2 - 4AC \equiv B^2 (\mathrm{mod}\, p)$ olur. Bu ise $\left(\frac{\Delta}{p}\right) = 1$ olmasını gerektirir. Bu olamaz çünkü $\left(\frac{\Delta}{p}\right) = -1$ dir. Şu halde $\gamma_p(Q(x,y))$ çift olmak zorundadır.

Sonuç 3.21. Eğer p asal sayısı için $\left(\frac{-\mathrm{D}}{p}\right) = -1$ ve $p|x^2 + Dy^2$ ise $p|x$ ve $p|y$ dir.

Teorem 3.22. m ve n tam sayılar olsun. mn sayısı $Q(x,y) = ax^2 + bxy + cy^2$ tarafından ilkel olarak temsil edilirse m sayısı da $q(x,y) = Ax^2 + Bxy + Cy^2$ tarafından ilkel olarak temsil edilir ve $b^2 - 4ac = B^2 - 4AC$ dir [1].

İspat. $mn = ax^2 + bxy + cy^2$ olan x ve y tam sayıları mevcut olsun. $r = (n,y)$ alınırsa $n = ru, y = rv$ ve $(u,v) = 1$ olacak biçimde u ve v tam sayıları vardır. O zaman $mru = ax^2 + bxrv + cr^2v^2$ olur. Buradan $r|ax^2$ olduğu görülür. $(x,y) = 1$ olduğundan $(x,r) = 1$ olur. Dolayısıyla $r|a$ dır. $a = rs$ olsun. $mru = ax^2 + bxrv + r^2v^2$ eşitliğinin her iki yanını r ile bölersek $mu = sx^2 + bxv + crv^2$ buluruz. $(u,v) = 1$ olduğundan $x = up + vq$ olacak biçimde u ve v tam sayıları vardır. x in bu değeri $mu = sx^2 + bxv + crv^2$ denkleminde yerine yazılırsa

$$mu = s(up + vq)^2 + b(up + vq)v + crv^2$$
$$= (sq^2 + bq + cr)v^2 + (2suq + bu)vp + su^2p^2$$

elde edilir. Buradan $u|(sq^2 + bq + cr)$ olduğu görülür. Çünkü $(u, v) = 1$ dir. $A = \frac{sq^2+bq+cr}{u}$, $B = 2sq + b$, $C = su$ alınırsa $m = Av^2 + Bvp + Cp^2$ elde edilir. $(x, y) = 1$, $y = rv$ ve $x = up + vq$ olduğundan $(v, p) = 1$ olduğu görülür. Ayrıca $4AC - B^2 = 4\left(\frac{sq^2+bq+cr}{u}\right)su - (2qs + b)^2 = 4s(sq^2 + bq + cr) - (2sq + b)^2 = 4scr - b^2 = 4ac - b^2$ dir. O halde $m = Av^2 + Bvp + Cp^2$ ve $B^2 - 4AC = b^2 - 4ac$ dir.

Teorem 3.23. $q(x, y) = Ax^2 + Bxy + Cy^2$ yön bağımlı iki değişkenli form olsun. $q(x, y)$'nin diskriminantı $\Delta = B^2 - 4AC$ olsun. $(n, 2AC) = 1$ olmak üzere Δ sayısı mod n'ye göre bir kare olsun. Bu durumda $Ab^2 + Bb + C = \ell n$ olacak biçimde b ve ℓ tam sayıları vardır. Ayrıca $(b, n) = 1$ dir [6,7].

İspat. $\mathbb{Z}_n[x]$ de $P(x) = \bar{A}x^2 + \bar{B}x + \bar{C}$ polinomunu ele alalım. $\Delta \equiv a^2 (\mathrm{mod}\, n)$ olan $a \in \mathbb{Z}$ olduğundan $\bar{\Delta} = \bar{a}^2$ dir. $\bar{a}^2 = \bar{\Delta} = \overline{B^2 - 4AC} = \bar{B}^2 - \bar{4}\bar{A}\bar{C}$ olduğundan $P(x)$ polinomunun köklerinden ikisi $\frac{-\bar{B}\mp\sqrt{\bar{\Delta}}}{\overline{2A}}$ ile bulunabilir. Burada $\frac{1}{\overline{2A}}$, $\overline{2A}$ nın mod n'ye göre tersidir. Dolayısıyla kökler $\frac{-\bar{B}\mp\bar{a}}{\overline{2A}}$ olup $\bar{b} \in \mathbb{Z}_n$, $\bar{A}\bar{b}^2 + \bar{B}\bar{b} + \bar{C} = \bar{0}$ olacak biçimde vardır. Bu ise $Ab^2 + Bb + C = \ell n$ olacak biçimde ℓ ve b tam sayılarının olduğunu gösterir. $(b, n) = 1$ dir. Çünkü p asal sayısı için $p|b$ ve $p|n$ ise $p|C$ olacağından bu durum $(n, C) = 1$ olmasına aykırıdır. Şu halde $(b, n) = 1$ dir.

Teorem 3.24. $q(x, y) = Ax^2 + Bxy + Cy^2$ iki değişkenli formu verilsin. Eğer $n > 0$, $(n, 2AC) = 1$ ve $\Delta = B^2 - 4AC$ sayısı mod n'ye göre bir kare ve n tam kare değilse $x, y \in \mathbb{Z}$ tam sayıları $0 < |x| < \sqrt{n}$, $0 < |y| < \sqrt{n}$ ve $q(x, y) = kn$ olacak biçimde vardır. Ayrıca $0 < |k| < |A| + |B| + |C|$ dir [6].

İspat. Teorem 3.23'e göre $Ab^2 + Bb + C = kn$ olan b ve k tam sayıları $(b, n) = 1$ olacak biçimde vardır. $(b, n) = 1$ olduğundan Teorem 3.5'e göre

$x \equiv by(\text{mod } n), 0 < |x| < \sqrt{n}\,, 0 < |y| < \sqrt{n}$ olacak biçimde x ve y tamsayıları mevcuttur. Bu durumda $q(x,y) = Ax^2 + Bxy + Cy^2 \equiv Ab^2y^2 + Bby^2 + Cy^2 \equiv y^2(Ab^2 + Bb + C) \equiv 0(\text{mod } n)$ olur. O halde $q(x,y) = kn$ olan k tam sayısı vardır. $kn = q(x,y)$ olduğundan $k = \frac{q(x,y)}{n}$ olup buradan

$$
\begin{aligned}
|k| &= \frac{|q(x,y)|}{n} = \frac{|Ax^2 + Bxy + Cy^2|}{n} \\
&< \frac{|A||x|^2 + |B||x||y| + |C||y|^2}{n} \\
&< \frac{|A|n + |B|n + |C|n}{n} \\
&= |A| + |B| + |C|
\end{aligned}
$$

elde edilir.

Sonuç 3.25. a) n pozitif tam sayısı $(n, 2AC) = 1$ olacak biçimde verilsin. Ayrıca $-AC$ sayısı mod n'ye göre bir kare olsun. O zaman $Ax^2 + Cy^2 = kn$ ve $|k| < |A| + |C|$ olacak biçimde x, y, k tam sayıları mevcuttur.
b) n pozitif tam sayısı $(n, 2D) = 1$ olacak biçimde verilsin. Ayrıca $-D$ sayısı mod n'ye göre bir kare olsun. Bu durumda $x^2 + Dy^2 = kn$ ve $|k| < 1 + |D|$ olacak biçimde x, y, k tam sayıları mevcuttur.

Teorem 3.26. (Vinogradov'un Lemması) a, b, n pozitif tam sayılar ve $n > 1$ olsun. Ayrıca $(ab, n) = 1$ olsun. $\alpha > 0$ reel sayısı verilsin. Bu durumda hepsi sıfır olmayan x, y tam sayıları $ax \equiv by(\text{mod } n)$ ve $|x| < \alpha, |y| \leq \frac{n}{\alpha}$ olacak biçimde vardır [7].

Teorem 3.27. n pozitif tam sayı ve n tam kare olmasın. Ayrıca $(n, 2AC) = 1$ ve $\Delta = B^2 - 4AC$ sayısı mod n'ye göre bir kare olsun. Bu durumda $q(x,y) = Ax^2 + Bxy + Cy^2$ yön bağımlı iki değişkenli form olmak üzere $q(x,y) = kn$ olacak biçimde x, y, k tam sayıları vardır ve $|k| < |B| + 2\sqrt{|A||C|}$ dir [7].

İspat. x ve y'nin rolünü değiştirerek $|A| \leq |C|$ kabul edebiliriz. Teorem 3.23'e göre b ve k tam sayıları $(b, n) = 1$ olmak üzere $Ab^2 + Bb + C = kn$ olacak biçimde vardır.

Teorem 3.26'yı $a = 1,\ \alpha = \left|\frac{C}{A}\right|^{\frac{1}{4}}\sqrt{n}$ alarak uygulayalım. Bu durumda x, y tam sayıları ikisi birden sıfır olmayacak, $x \equiv by(\mathrm{mod}\, n)$ ve $0 < |x| < \alpha = \left|\frac{C}{A}\right|^{\frac{1}{4}}\sqrt{n}, 0 < |y| < \alpha = \left|\frac{A}{C}\right|^{\frac{1}{4}}\sqrt{n}$ şartını sağlayacak biçimde vardır. Buradan $q(x,y) = Ax^2 + Bxy + Cy^2 \equiv y^2(Ab^2 + Bb + C) \equiv 0(\mathrm{mod}\, n)$ elde edilir. O halde $q(x,y) = kn$ olan k tam sayısı vardır.

$$\begin{aligned} 0 < |q(x,y)| &= |Ax^2 + Bxy + Cy^2| \\ &\leq |A||x|^2 + |B||x||y| + |C||y|^2 \\ &< \left(|B| + 2\sqrt{|A||C|}\right)n \end{aligned}$$

elde edilir. O halde $|k| = \left|\frac{q(x,y)}{n}\right| < |B| + 2\sqrt{|A||C|}$ dir.

Sonuç 3.28. n tam kare olmayan bir pozitif tam sayı ve $-AC, \mathrm{mod}\, n$'ye göre bir kare olsun. Ayrıca $(n, 2AC) = 1$ olsun. Bu durumda $Ax^2 + Cy^2 = kn, |k| < 2\sqrt{|A||C|}$ olacak biçimde x ve y tam sayıları vardır.

Sonuç 3.29. D kare olmayan pozitif tam sayı ve n pozitif tam sayısı karesiz olsun. Ayrıca $(n, 2D) = 1$ ve $-D$ sayısı $\mathrm{mod}\, n$'ye göre bir kare olsun. O zaman x, y, k tam sayıları $x^2 + Dy^2 = kn, 0 < |k| < 2\sqrt{D}$ olacak biçimde vardır.

Aşağıdaki teoremlerin ispatı Sonuç 3.25 kullanılarak yapılabilir. Fakat Sonuç 3.29 ispatlarda kısalık sağlayacaktır.

Teorem 3.30. $p > 6$ olsun. $p = x^2 + 6y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow \left(\frac{-6}{p}\right) = 1$ ve $p \equiv \mp 1(\mathrm{mod}\, 8)$ dir.

İspat. $\Rightarrow$) $p = x^2 + 6y^2$ olacak biçimde x ve y tam sayıları mevcut olsun. O zaman x tektir. $p = x^2 + 6y^2$ olduğundan $x^2 \equiv -6y^2(\mathrm{mod}\, p)$ yazılabilir. Açık olarak $p \nmid x$

ve $p \nmid y$ dir. Böylece $1 = \left(\frac{x^2}{p}\right) = \left(\frac{-6y^2}{p}\right) = \left(\frac{-6}{p}\right)$ elde edilir. Ayrıca $p = x^2 + 6y^2$ olduğu ve $x^2 \equiv 1(\text{mod } 8), y^2 \equiv 0,1,4(\text{mod } 8)$ olduğu dikkate alınırsa $p \equiv \mp 1(\text{mod } 8)$ elde edilir.

$\Leftarrow$) $\left(\frac{-6}{p}\right) = 1$ ve $p \equiv \mp 1(\text{mod } 8)$ olsun. O zaman $x^2 \equiv -6(\text{mod } p)$ olan x tam sayısı vardır. Dolayısıyla -6 sayısı p modülüne göre bir karedir. Sonuç 3.29'a göre $x^2 + 6y^2 = kp$ ve $0 < |k| < 2\sqrt{6}$ olacak biçimde x, y ve k tam sayıları vardır. $k > 0$ olduğundan $1 \leq k \leq 4$ olur. Dolayısıyla $k = 1,2,3,4$ olabilir. $\left(\frac{-6}{p}\right) = 1$ olduğundan $1 = \left(\frac{-6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-3}{p}\right) = \left(\frac{-3}{p}\right)$ dir. Çünkü $p \equiv \mp 1(\text{mod } 8)$ olduğundan $\left(\frac{2}{p}\right) = 1$ dir. $\left(\frac{-3}{p}\right) = 1$ olduğundan Teorem 2.14'ün (3) özelliğine göre göre $p \equiv 1(\text{mod } 3)$ elde edilir. O halde $kp \equiv k(\text{mod } 3)$ olur.

Diğer yandan $x^2 + 6y^2 \equiv 0,1(\text{mod } 3)$ olduğu kullanılırsa $k \equiv kp = x^2 + 6y^2 \equiv 0,1(\text{mod } 3)$ elde edilir. Bu ise $k \equiv 1,3,4$ olmasını gerektirir. $k = 4$ ise $4p = x^2 + 6y^2$ olur. O zaman x çift olmalıdır. $x = 2t$ olsun. Buradan $4p = 4t^2 + 6y^2$ ve böylece $2p = 2t^2 + 3y^2$ elde edilir. O halde y çifttir. $y = 2r$ olsun. $2p = 2t^2 + 3 \cdot 4r^2$ ve buradan $p = k^2 + 6r^2$ elde edilir. $k = 1$ ise zaten istenen elde edilir. $k = 3$ olsun. Bu durumda $3p = x^2 + 6y^2$ ve böylece $3|x$ olur. $x = 3a$ olsun. O zaman $3p = 9a^2 + 6y^2 \Rightarrow p = 3a^2 + 2y^2$ elde edilir. Bu ise $p \equiv 2y^2(\text{mod } 3)$ olması demektir. Bu olamaz. Çünkü $p \equiv 1(\text{mod } 3)$ tür. Şu halde $k = 1$ veya $k = 4$ olabilir ve bu durumda da $p = x^2 + 6y^2$ olan x ve y tam sayılarının olduğu görülür.

Teorem 3.31. $p > 5$ olsun. $p = x^2 + 10y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow \left(\frac{p}{5}\right) = 1$ ve $\left(\frac{-10}{p}\right) = 1$ dir.

İspat: $\Longrightarrow$) $p = x^2 + 10y^2$ olacak biçimde x ve y tam sayıları mevcut olsun. O zaman Önerme 3.7'ye göre $\left(\frac{-10}{p}\right) = 1$ dir. Ayrıca $p = x^2 + 5y^2$ olduğundan $5 \nmid x$ olur. O

zaman $x^2 \equiv 1,4(\text{mod } 5)$ dır. Buradan $p = x^2 + 5y^2 \equiv x^2 \equiv 1,4(\text{mod } 5)$ elde edilir. Teorem 2.14'ün (4) özelliğinden dolayı $\left(\frac{p}{5}\right) = 1$ dir.

$\Longleftarrow$) $\left(\frac{p}{5}\right) = 1$ ve $\left(\frac{-10}{p}\right) = 1$ olsun. $\left(\frac{-10}{p}\right) = 1$ olduğundan $x^2 \equiv -10(\text{mod } p)$ olan x tam sayısı vardır. Dolayısıyla -10 sayısı mod p'ye göre bir karedir. Sonuç 3.29'a göre $p = x^2 + 10y^2,\ 0 < k < 2\sqrt{10}$ olacak biçimde x, y ve k tam sayıları vardır. Buradan $1 \leq k \leq 6$ olduğu görülür. $k = 1$ ise $p = x^2 + 10y^2$ olur. $k = 2$ olsun. O zaman $2p = x^2 + 10y^2$ olur. Dolayısıyla $5 \nmid x$ ve x çift olur. $x = 2a$ olsun. Bu durumda $p = 2a^2 + 5y^2 \equiv 2a^2 \equiv 2,3(\text{mod } 5)$ olur. Bu olamaz. Çünkü $\left(\frac{p}{5}\right) = 1$ olduğundan Teorem 2.14'ün (4) özelliğine göre $p \equiv 1,4(\text{mod } 5)$ olmalıdır. $\left(\frac{-10}{3}\right) = \left(\frac{-1}{3}\right) = -1$ olduğundan $k = 3,6$ olamayacağı Sonuç 3.21'den görülür. $k = 5$ olsun. O zaman $5p = x^2 + 10y^2$ olup $5|x$ elde edilir. $x = 5a$ olsun. Bu durumda $p = 5a^2 + 2y^2 \equiv 2y^2(\text{mod } 5)$ elde edilir. Ayrıca $5 \nmid y$ olduğu görülür. O halde $y^2 \equiv 1,4(\text{mod } 5)$ olur. Dolayısıyla $p \equiv 2,3(\text{mod } 5)$ dir. Bu olamaz. Çünkü $\left(\frac{p}{5}\right) = 1$ dir. $k = 4$ olsun. O zaman $4p = x^2 + 10y^2$ olduğu dikkate alınırsa x'in çift sayı olduğu görülür. $x = 2a$ olsun. O zaman $4p = 4a^2 + 10y^2$ ve böylece y çift olur. $y = 2b$ olsun. Bu durumda $4p = 4a^2 + 40b^2$, yani $p = a^2 + 10b^2$ olur.

Teorem 3.32. p asal ve $p > 6$ olsun. $p = x^2 + 12y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p \equiv 1(\text{mod } 3)$ ve $p \equiv 1(\text{mod } 4)$ dir.

İspat: $\Longrightarrow$) $p > 6, p$ asal ve $p = x^2 + 12y^2$ ise $p \equiv 1(\text{mod } 3)$ ve $p \equiv 1(\text{mod } 4)$ olduğu açıktır.

$\Longleftarrow$) $p \equiv 1(\text{mod } 3)$ ve $p \equiv 1(\text{mod } 4)$ olsun. Bu durumda $\left(\frac{12}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) \equiv \left(\frac{1}{3}\right) = 1$ olur. Dolayısıyla -12 sayısı mod p'ye göre bir karedir. Sonuç 3.29'a göre $x^2 + 12y^2 = kp, 1 \leq k \leq 2\sqrt{12}$ şartını sağlayan x, y, k tam sayıları vardır. O zaman $1 \leq k \leq 6$ dır. $k = 1$ ise $x^2 + 12y^2 = p$ olur. $k = 2$ olsun. Bu durumda x çift olur. $x = 2a$ olsun. $2p = x^2 + 12y^2 = 4a +$

$12y^2$ ve böylece $p = 2a^2 + 3y^2$ yazılabilir.. Burada $3 \nmid a$ olduğu görülür. O zaman $p = 2a^2 + 3y^2 \equiv 2 (\text{mod } 3)$ elde edilir. Bu olamaz çünkü $p \equiv 1 (\text{mod } 3)$ dir. $k = 3$ olsun. O zaman $3p = x^2 + 12y^2$ olduğundan $x = 3a$ olan $a \in \mathbb{Z}$ vardır. Buradan $p = 3a^2 + 4y^2$ elde edilir ve bu bize a'nın tek tam sayı olduğunu gösterir. O zaman $p \equiv 3 (\text{mod } 4)$ olduğu görülür. Bu $p \equiv 1 (\text{mod } 4)$ olmasına aykırıdır. $k = 4$ olsun. Bu durumda $4p = x^2 + 12y^2$ den x'in çift sayı olduğu ve $p = \left(\frac{x}{2}\right)^2 + 3y^2$ olduğu görülür. Eğer y tekse $\frac{x}{2}$ de çift olacağından $p \equiv 3 (\text{mod } 4)$ olur. Bu olamaz o halde y çift sayıdır. O zaman $p = \left(\frac{x}{2}\right)^2 + 12\left(\frac{y}{2}\right)^2$ elde edilir. $\left(\frac{-12}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{2}{5}\right) = -1$ olduğundan Sonuç 3.21'e göre $k = 5$ olamayacağı görülür. $k = 6$ olsun. O zaman $6p = x^2 + 12y^2$ ve böylece $6|x$ olduğu görülür. $x = 6a$ olsun. O zaman $p = 6a^2 + 2y^2$ olur. Bu olamaz çünkü p tek asal sayıdır.

Teorem 3.33. $p > 13$ olsun. $p = x^2 + 13y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p \equiv 1 (\text{mod } 4)$ ve $\left(\frac{p}{13}\right) = 1$ dir [6,7].

İspat: $\Longrightarrow$) $p = x^2 + 13y^2$ olan x ve y tam sayıları varsa Önerme 3.7'ye göre $\left(\frac{-13}{p}\right) = 1$ dir. Ayrıca $p = x^2 + 13y^2 \equiv x^2 + y^2 \equiv 1 (\text{mod } 4)$ olur. $1 = \left(\frac{-13}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{13}{p}\right) = \left(\frac{13}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{13-1}{2}}\left(\frac{p}{13}\right) = \left(\frac{p}{13}\right)$ olur. Yani $\left(\frac{p}{13}\right) = 1$ dir.

$\Longleftarrow$) $p \equiv 1 (\text{mod } 4)$ ve $\left(\frac{p}{13}\right) = 1$ olsun. O zaman $\left(\frac{-13}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{13}{p}\right) = \left(\frac{13}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{13-1}{2}}\left(\frac{p}{13}\right) = \left(\frac{p}{13}\right) = 1$ olduğundan Sonuç 3.29'a göre $x^2 + 13y^2 = kp$ olan $0 < k < 2\sqrt{13}$ şartını sağlayan x, y, k tam sayıları vardır. Buradan $1 \leq k \leq 7$ elde edilir. $k = 3$ veya $k = 5$ ise $\left(\frac{-13}{3}\right) = -\left(\frac{13}{3}\right) = -1$ ve $\left(\frac{-13}{5}\right) = \left(\frac{13}{5}\right) = \left(\frac{2}{5}\right) = -1$ olduğundan Sonuç 3.21'e göre $k|x$ ve $k|y$ olur. O zaman $k^2|x^2 + 13y^2$, yani $k^2|kp$ ve buradan $k|p$ elde edilir. Bu olamaz çünkü $p > 13$ tür. Eğer $k = 2$ ise $2p = x^2 + 13y^2 \equiv x^2 (\text{mod } 13)$ buradan $\left(\frac{2}{13}\right)\left(\frac{p}{13}\right) = 1$ elde edilir. Ayrıca $\left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = (-1)^{21} = -1$ olduğundan $\left(\frac{p}{13}\right) = -1$ olarak bulunur. Bu olamaz. Çünkü

$\left(\frac{p}{13}\right) = 1$ dir. Şimdi $k = 4$ olsun. Bu durumda $4p = x^2 + 13y^2$ olup buradan $4|x^2 + y^2$ elde edilir. Bu ise x ve y'nin aynı anda çift olmasını gerektirir. O halde $x = 2a, y = 2b$ alınırsa $4p = x^2 + 13y^2 = 4a^2 + 13 \cdot 4b^2$ ve buradan da $p = a^2 + 13b^2$ bulunur. Eğer $k = 1$ ise zaten $p = x^2 + 13y^2$ elde edilir. Diğer yandan $\left(\frac{-13}{3}\right) = \left(\frac{\mathbf{-13}}{\mathbf{7}}\right) = -1$ olduğundan $k = 6,7$ olamayacağı Sonuç 3.21'den görülür.

Teorem 3.34. $p > 15$ olsun. $p = x^2 + 15y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow \left(\frac{-3}{p}\right) = \left(\frac{5}{p}\right) = 1$ dir [6,7].

İspat: $\Longrightarrow$) $p > 15$ ve $p = x^2 + 15y^2$ olan x ve y tam sayıları mevcut olsun. Bu durumda Önerme 3.7'ye göre $\left(\frac{-15}{p}\right) = 1$ dir. Bu ise $\left(\frac{-3}{p}\right)\left(\frac{5}{p}\right) = 1$ olduğunu gösterir. $p = x^2 + 15y^2$ olduğundan $3 \nmid x$ olur ve böylece $p \equiv 1 (\mathrm{mod}\ 3)$ bulunur. Şu halde $\left(\frac{p}{3}\right) = 1$ dir. O zaman $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = 1$ olur. $1 = \left(\frac{-3}{p}\right)\left(\frac{5}{p}\right)$ olduğu kullanılırsa $\left(\frac{5}{p}\right) = 1$ elde edilir.

$\Longleftarrow$) $\left(\frac{-3}{p}\right) = \left(\frac{5}{p}\right) = 1$ olsun. O zaman $\left(\frac{-15}{p}\right) = 1$ dir. Dolayısıyla $-15, \mathrm{mod}\ p$'ye göre bir karedir. Sonuç 3.29'a göre $x^2 + 15y^2 = kp, 1 \leq k \leq 2\sqrt{15}$ olacak biçimde x, y, k tam sayıları vardır. Bu durumda $1 \leq k \leq 7$ dir. $k = 1$ ise $p = x^2 + 15y^2$ olur. $k = 2$ olsun. O zaman $2p = x^2 + 15y^2$ olduğundan x ve y aynı anda tek olmalıdır. Bu durumda $2p \equiv 1 + 15 \equiv 0 (\mathrm{mod}\ 8)$ olur. Bu ise olamaz. $k = 3$ olsun. $3p = x^2 + 15y^2$ olduğundan $3|x$ olur. $x = 3a$ olsun. O zaman $p = 3a^2 + 5y^2$ olur ve $3 \nmid y$ olduğu görülür. O zaman $p \equiv 5y^2 \equiv 5 \equiv 2 (\mathrm{mod}\ 3)$ olur. Bu $\left(\frac{-3}{p}\right) = 1$ olmasına aykırıdır. $k = 4$ olsun. O zaman $4p = x^2 + 15y^2$ olduğundan x ve y aynı anda tek tam sayı olamaz. O halde x ve y çifttir. Buradan $p = \left(\frac{x}{2}\right)^2 + 15\left(\frac{y}{2}\right)^2$ elde edilir. $k = 5$ olsun. Bu durumda $5p = x^2 + 15y^2$ olduğundan $5|x$ olur. $x = 5a$ olsun. O zaman $p = 5a^2 + 3y^2$ elde edilir ve $3 \nmid a$ olduğu görülür. Buradan $p \equiv 2 (\mathrm{mod}\ 3)$ elde edilir. Bu ise $\left(\frac{-3}{p}\right) = 1$ olmasına aykırıdır. $k = 6$ olsun. O zaman $6p = x^2 +$

$15y^2$ olup $3|x$ olduğu görülür. $x = 3a$ olsun. Buradan $2p = 3a^2 + 5y^2$ elde edilir. Bunun olamayacağı a ve y'nin çift veya tek olma durumları incelendiğinde görülür. $\left(\frac{-15}{7}\right) = \left(\frac{-1}{7}\right) = -1$ olduğundan $k = 7$ olamayacağı Sonuç 3.21 den görülür.

Teorem 3.35. p asal sayı ve $p > 21$ olsun. $p = x^2 + 21y^2$ olacak biçimde x ve y tam sayıları vardır$\Leftrightarrow p \equiv 1(\text{mod } 4)$, $\left(\frac{3}{p}\right) = \left(\frac{7}{p}\right) = 1$ dir [6,7].

İspat: $\Longrightarrow$) $p = x^2 + 21y^2$ olacak biçimde x ve y tam sayıları varsa kolay bir hesaplamayla $p \equiv 1(\text{mod } 4)$ olduğu görülür. $p = x^2 + 21y^2$ olduğundan $3 \nmid x$ olur ve bu durumda $p \equiv 1(\text{mod } 3)$ bulunur. O halde $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = 1$ olur. Ayrıca Önerme 3.7'ye göre $\left(\frac{-21}{p}\right) = 1$ dir. O halde $\left(\frac{3}{p}\right)\left(\frac{-7}{p}\right) = 1$ ve buradan $\left(\frac{-7}{p}\right) = 1$ ve böylece $p \equiv 1(\text{mod } 4)$ olduğu kullanılırsa $\left(\frac{7}{p}\right) = 1$ elde edilir.

$\Longleftarrow$) $p \equiv 1(\text{mod } 4)$, $\left(\frac{3}{p}\right) = \left(\frac{7}{p}\right) = 1$ olsun. Bu durumda $\left(\frac{-21}{p}\right) = 1$ olduğu görülür. O halde -21 sayısı mod p'ye göre bir karedir. Sonuç 3.29'a göre $x^2 + 21y^2 = kp$, $1 \leq k \leq 2\sqrt{21}$ olacak biçimde x, y, k tam sayıları vardır. Buradan $1 \leq k \leq 9$ olduğu görülür. $k = 1$ ise $p = x^2 + 21y^2$ dir. $k = 2$ olsun. O zaman $2p = x^2 + 21y^2$ olur. Dolayısıyla x ve y aynı anda çift olamaz. O halde x ve y aynı anda tek olur. $2p = x^2 + 21y^2 \equiv 1 + 21 \equiv 22(\text{mod } 8)$ ve buradan $p \equiv 3(\text{mod } 4)$ bulunur. Bu durum $p \equiv 1(\text{mod } 4)$ olmasına aykırıdır. $k = 3$ olsun. O zaman $3|x$ dir. $x = 3a$ olsun. $3p = 9a^2 + 21y^2$ den $p = 3a^2 + 7y^2$ elde edilir. Buradan da $7 \nmid a$ olduğu görülür. O zaman $p \equiv 3a^2(\text{mod } 7)$ elde edilir. Dolayısıyla $\left(\frac{p}{7}\right) = \left(\frac{3}{7}\right) = \left(\frac{-4}{7}\right) = \left(\frac{-1}{7}\right) = -1$ dır. Bu $\left(\frac{7}{p}\right) = 1$ olmasına aykırıdır. $k = 4$ olsun. O zaman $4p = x^2 + 21y^2$ olur. Eğer x ve y aynı anda tek ise $4p \equiv 22(\text{mod } 8)$ olur. Bu ise olamaz. O zaman x ve y aynı anda çifttir. Buradan $p = \left(\frac{x}{2}\right)^2 + 21\left(\frac{y}{2}\right)^2$ elde edilir. $k = 5$ olsun. Bu durumda $5p = x^2 + 21y^2$ olur. $3 \nmid x$ dir. Dolayısıyla $5p \equiv 1(\text{mod } 3)$ yani $p \equiv 2(\text{mod } 3)$ bulunur. Bu $\left(\frac{3}{p}\right) = 1$ olmasına aykırıdır. $k = 6$ olsun. $6p = x^2 + 21y^2$ olduğundan

$3|x$ olur. $x = 3a$ alınırsa $2p = 3a^2 + 7b^2$ elde edilir ve $3 \nmid b$ olduğu görülür. Dolayısıyla $2p \equiv 7 \equiv 1(\text{mod } 3)$ tür. Bu ise $p \equiv 2(\text{mod } 3)$ olmasını gerektirir. Bu olamaz. Çünkü $\left(\frac{3}{p}\right) = 1$ ve $p \equiv 1(\text{mod } 4)$ tür. $k = 7$ olsun. O zaman $7p = x^2 + 21y^2$ olup buradan $7|x$ elde edilir. $x = 7a$ olsun. Dolayısıyla $p = 7a^2 + 3y^2$ bulunur. Bu ise $7 \nmid y$ ve $p \equiv 3y^2(\text{mod } 7)$ olmasını gerektirir. O zaman $\left(\frac{p}{7}\right) = \left(\frac{3}{7}\right) = -1$ olur. Bu yine $\left(\frac{7}{p}\right) = 1$ olmasına aykırıdır. $k = 8$ ise $8p = x^2 + 21y^2$ olacağından x ve y aynı anda çift olmalıdır. Bu durumda $2p = \left(\frac{x}{2}\right)^2 + 21\left(\frac{y}{2}\right)^2$ olmasını gerektirir. Benzer yolla bunun olmayacağı gösterilir. $k = 9$ ise $3|x$ ve $3|y$ olduğu görülür. O zaman $9p = x^2 + 21y^2$ den $p = \left(\frac{x}{3}\right)^2 + 21\left(\frac{y}{3}\right)^2$ bulunur.

Teorem 3.36. $p > 22$ olsun. $p = x^2 + 22y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p \equiv \mp 1(\text{mod } 8)$ ve $\left(\frac{p}{11}\right) = 1$ dir [6,7].

İspat: $\Longrightarrow$) $p = x^2 + 22y^2$ olan x ve y tam sayıları mevcut olsun. O zaman Önerme 3.7'ye göre $\left(\frac{-22}{p}\right) = 1$ dir. $p = x^2 + 22y^2$ olduğundan $p = x^2 + 22y^2 \equiv x^2 - 2y^2(\text{mod } 8)$ olur. Eğer y çift x tek ise $p \equiv x^2 - 2y^2 \equiv 1(\text{mod } 8)$ olur. Eğer y tek ise $p \equiv x^2 - 2y^2 \equiv x^2 - 2(\text{mod } 8)$ olur. Bu durumda x'in tek olduğu görülür. O zaman $p \equiv -1(\text{mod } 8)$ elde edilir. Dolayısıyla $p \equiv \mp 1(\text{mod } 8)$ dir. $1 = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{11}{p}\right)$ ve $\left(\frac{2}{p}\right) = 1$ olduğu kullanılırsa

$$1 = \left(\frac{-1}{p}\right)\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{11-1}{2}}\left(\frac{p}{11}\right) = \left(\frac{p}{11}\right)$$

elde edilir. Yani $\left(\frac{p}{11}\right) = 1$ dir.

$\Longleftarrow$) $p \equiv \mp 1(\text{mod } 8)$ ve $\left(\frac{p}{11}\right) = 1$ olsun. Kolay bir hesaplamayla $\left(\frac{-22}{p}\right) = 1$ olduğu görülür. O zaman $-22 \bmod p$'ye göre bir karedir. Sonuç 3.29'a göre $x^2 + 22y^2 = kp$, $0 < k < 2\sqrt{22}$ olacak biçimde x, y, k tam sayıları vardır. Bu durumda $1 \leq k \leq 9$

elde edilir. $k=1$ ise $p=x^2+22y^2$ olur. $\left(\frac{-22}{3}\right)=\left(\frac{-1}{3}\right)=-1$, $\left(\frac{-22}{5}\right)=\left(\frac{-2}{5}\right)=\left(\frac{2}{5}\right)=1$, $\left(\frac{-22}{7}\right)=\left(\frac{-1}{7}\right)=-1$ olduğundan Sonuç 3.21'e göre k'nın 3,5,7 değerlerini alamayacağı görülür. Şimdi $k=2$ olsun. O zaman $2p=x^2+22y^2$ olup bu durumda x çift olur. $x=2a$ olsun. Buradan $2p=4a^2+22y^2$ ve böylece $p=2a^2+11y^2$ elde edilir. Dolayısıyla y tek tam sayıdır. Buradan $p=2a^2+11y^2\equiv 2a^2+3(\text{mod } 8)$ elde edilir. $p\equiv \mp 1(\text{mod } 8)$ olduğundan $2a^2+3\equiv 1,-1(\text{mod } 8)$, yani $2a^2\equiv -2,4(\text{mod } 8)$ ve dolayısıyla $a^2\equiv -1,2(\text{mod } 4)$ olur. Bu olamaz çünkü herhangi bir x tam sayısı için $x^2\equiv 0,1(\text{mod } 4)$ tür. Şimdi $k=4$ olsun. Bu durumda $4p=x^2+22y^2$ olduğundan x çift tam sayı olur. $x=2a$ olsun. O zaman $2p=2a^2+11y^2$ elde edilir ve bu y'nin de çift tam sayı olduğunu gösterir. $y=2b$ olsun. Buradan $p=a^2+22b^2$ elde edilir. $k=6$ olsun. Bu durumda $3|x^2+22y^2$ dir. $\left(\frac{-22}{3}\right)=\left(\frac{-1}{3}\right)=-1$ olduğundan Sonuç 3.21'e göre $3|x$ ve $3|y$ ve buradan $9|x^2+22y^2$, yani $9|6p$ elde edilir. Bu olamaz. Eğer $k=9$ ise benzer biçimde $3|x$ ve $3|y$ ve buradan $9p=x^2+22y^2$ ve böylece $p=\left(\frac{x}{3}\right)^2+22\left(\frac{y}{3}\right)^2$ elde edilir. $k=8$ olamayacağı benzer yollarla gösterilir.

Teorem 3.37. $p>33$ ve p asal sayı olsun. $p=x^2+33y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p\equiv 1(\text{mod } 4)$ ve $\left(\frac{3}{p}\right)=\left(\frac{11}{p}\right)=1$ dir [6,7].

İspat: $\Longrightarrow$) $p=x^2+33y^2$ ise $p\equiv x^2+y^2(\text{mod } 4)$ olup x ve y den biri çift biri tek olacağından $p\equiv 1(\text{mod } 4)$ bulunur. Önerme 3.7'ye göre $\left(\frac{-33}{p}\right)=1$ olup buradan $\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{11}{p}\right)=1$ yani $\left(\frac{3}{p}\right)\left(\frac{11}{p}\right)=1$ elde edilir. Diğer yandan $3\nmid x$ olduğundan $p\equiv 1(\text{mod } 3)$ ve buradan da $\left(\frac{3}{p}\right)=1$ olduğu görülür. Buradan da $\left(\frac{11}{p}\right)=1$ elde edilir.

$\Longleftarrow$) $p\equiv 1(\text{mod } 4)$, $\left(\frac{3}{p}\right)=\left(\frac{11}{p}\right)=1$ ise $\left(\frac{-33}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)\left(\frac{11}{p}\right)=1$ elde edilir. O zaman -33 sayısı mod p'ye göre bir karedir. Sonuç 3.29'a göre $x^2+33y^2=kp$, $1\le k\le 2\sqrt{33}$ olacak biçimde x,y,k tam sayıları vardır. Burada $1\le k\le 11$ olduğu görülür. $k=1$ ise $p=x^2+33y^2$ dir. $\left(\frac{-33}{5}\right)=\left(\frac{2}{5}\right)=-1$ olduğundan $k=5$

ve $k = 10$ olamayacağı Sonuç 3.21'den görülür. $k = 2$ ise $2p = x^2 + 33y^2$ olup bu durumda $3 \nmid x$ ve $2p \equiv 1(\text{mod } 3)$ olduğu görülür. O zaman $p \equiv 2(\text{mod } 3)$ olur. Bu olamaz. Çünkü $\left(\frac{3}{p}\right) = 1$ ve $p \equiv 1(\text{mod } 4)$ tür. $k = 3$ olsun. O zaman $3|x$ ve buradan $x = 3a$ alınırsa $3p = 9a^2 + 3 \cdot 11y^2$ elde edilir. Dolayısıyla $p = 3a^2 + 11y^2$ dir. Bu durumda da $3 \nmid y$ olup buradan $p \equiv 11 \equiv -1(\text{mod } 3)$ bulunur. Bu yine olamaz. $k = 4$ olsun. $4p = x^2 + 33y^2 \equiv x^2 + y^2(\text{mod } 8)$ olduğundan x ve y aynı anda tek olamaz. O halde x ve y çifttir. Bu ise $p = \left(\frac{x}{2}\right)^2 + 33\left(\frac{y}{2}\right)^2$ olduğunu gösterir. $k = 6$ olsun. O zaman $6p = x^2 + 33y^2$ den $3|x$ bulunur. $x = 3a$ olsun. Böylece $2p = 3a^2 + 11y^2$ elde edilir. Buradan $11 \nmid a$ ve $2p \equiv 3a^2(\text{mod } 11)$bulunur. Bu $\left(\frac{2}{11}\right)\left(\frac{p}{11}\right) = \left(\frac{3}{11}\right)$ olduğunu gösterir. O halde $\left(\frac{p}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{-5}{11}\right) = -\left(\frac{5}{11}\right) = -1$ dir. Bu olamaz. Çünkü $p \equiv 1(\text{mod } 4)$ ve $\left(\frac{11}{p}\right) = 1$ dır. $k = 7$ olsun. O zaman $7p = x^2 + 33y^2$ ve $11 \nmid x$ dir. Dolayısıyla $7p \equiv x^2(\text{mod } 11)$ dir. O halde $\left(\frac{7p}{11}\right) = 1$ dir. Bu ise $\left(\frac{7}{11}\right)\left(\frac{p}{11}\right) = 1$ yani $(-1)\left(\frac{p}{11}\right) = 1$ olduğunu gösterir. Buradan $\left(\frac{p}{11}\right) = -1$ olduğu görülür. Bu olamaz. Çünkü $p \equiv 1(\text{mod } 4)$ ve $\left(\frac{11}{p}\right) = 1$ dir.

Teorem 3.38. $p > 37$ olsun. $p = x^2 + 37y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p \equiv 1(\text{mod } 4)$ ve $\left(\frac{p}{37}\right) = 1$ dir [6,7].

İspat: $\Longrightarrow$) $p = x^2 + 37y^2$ olacak biçimde x ve y tam sayıları mevcut olsun. Bu durumda $p = x^2 + 37y^2 \equiv x^2 + y^2 \equiv 1(\text{mod } 4)$ olur. Çünkü burada x ve y tam sayılarından biri tek diğeri çift tam sayıdır. Ayrıca Önerme 3.7'ye göre $\left(\frac{-37}{p}\right) = 1$ dir. Şu halde

$$\left(\frac{p}{37}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{37-1}{2}}\left(\frac{37}{p}\right) = \left(\frac{37}{p}\right) = \left(\frac{-37}{p}\right) = 1$$

elde edilir.

$\Longleftarrow$) $\left(\frac{p}{37}\right)=1$ ve $p\equiv 1(\mathrm{mod}\,4)$ olsun. Bu durumda $\left(\frac{-37}{p}\right)=1$ olduğunu görmek kolaydır. O zaman $x^2\equiv -37(\mathrm{mod}\,p)$ olacak biçimde bir x tam sayısı vardır. Dolayısıyla -37 sayısı $\mathrm{mod}\,p$'ye göre bir karedir. Sonuç 3.29'a göre $x^2+37y^2=kp\,, 0<k<2\sqrt{37}$ olacak biçimde x,y,k tam sayıları vardır. Buradan $1\leq k\leq 12$ elde edilir.

$$\left(\frac{-37}{3}\right)=\left(\frac{-1}{3}\right)=-1\,,$$
$$\left(\frac{-37}{5}\right)=\left(\frac{2}{5}\right)=-1\,,$$
$$\left(\frac{-37}{7}\right)=\left(\frac{-2}{7}\right)=\left(\frac{5}{7}\right)=\left(\frac{7}{5}\right)=\left(\frac{2}{5}\right)=-1$$

olduğundan $k=3,5,7,11$ değerlerinin olamayacağı Sonuç 3.21 kullanılarak gösterilir. Eğer $k=1$ ise $p=x^2+37y^2$ olur. $k=2$ olsun. O zaman $2p=x^2+37y^2$ olduğundan x ve y tek olmalıdır. Bu durumda $2p=x^2+37y^2\equiv 1+37=38\equiv -2(\mathrm{mod}\,8)$ ve buradan $p\equiv -1(\mathrm{mod}\,4)$ olur. Bu durum $p\equiv 1(\mathrm{mod}\,4)$ olmasına aykırıdır. $k=4$ olsun. O zaman $4p=x^2+37y^2$ olduğundan x ve y aynı anda tek veya aynı anda çift olmalıdır. x ve y tek olsun. O zaman $4p=x^2+37y^2\equiv 1+37\equiv 2(\mathrm{mod}\,4)$ olur. Bu olamaz. O halde x ve y çift olur. Bu durumda $4p=x^2+37y^2$ olduğundan $p=\left(\frac{x}{2}\right)^2+37\left(\frac{y}{2}\right)^2$ elde edilir. $\left(\frac{-37}{3}\right)=\left(\frac{-1}{3}\right)=-1$, $\left(\frac{-37}{5}\right)=\left(\frac{2}{5}\right)=-1$, $\left(\frac{-37}{7}\right)=\left(\frac{5}{7}\right)=\left(\frac{7}{5}\right)=\left(\frac{2}{5}\right)=-1$ ve $\left(\frac{-37}{11}\right)=\left(\frac{-4}{11}\right)=\left(\frac{-1}{11}\right)=-1$ olduğundan $k=6,7,10,11,12$ olamayacağı Sonuç 3.21 kullanılarak gösterilebilir. $k=8$ olsun. O zaman $8p=x^2+37y^2$ olur. Burada da x ve y'nin aynı anda çift veya aynı anda tek olduğu görülür. x ve y tek ise $8p=x^2+37y^2\equiv 1+37\equiv -2(\mathrm{mod}\,8)$ olur. Bu olamaz. x ve y çiftse $x=2a\,, y=2b$ yazılarak $8p=4a^2+37\cdot 4b^2$ yani $2p=a^2+37b^2$ elde edilir. Bunun olamayacağı yukarıda gösterildi. $k=9$ ise $3|x$ ve $3|y$ olacağından $p=\left(\frac{x}{3}\right)^2+37\left(\frac{y}{3}\right)^2$ elde edilir.

Teorem 3.39. p asal ve $p>29$ olsun. $p=x^2+58y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p\equiv 1,3(\mathrm{mod}\,8)$ ve $\left(\frac{p}{29}\right)=1$ dir [6,7].

İspat: $\Longrightarrow$) $p = x^2 + 58y^2$ ise x tek tam sayıdır ve y'nin durumuna göre $p \equiv 1,3 (\mathrm{mod}\ 8)$ elde edilir. Diğer yandan Önerme 3.7'ye göre $\left(\frac{-58}{p}\right) = 1$ dir. Bu durumda kolay bir hesaplamayla $\left(\frac{p}{29}\right) = 1$ olduğu görülür.

$\Longleftarrow$) $\left(\frac{p}{29}\right) = 1$ ve $p \equiv 1,3 (\mathrm{mod}\ 8)$ olsun. Bu durumda Teorem 2.14'e göre $\left(\frac{-2}{p}\right) = 1$ dir. Basit bir hesaplamayla $\left(\frac{-58}{p}\right) = 1$ olduğu görülür. Bu durumda $-58, \mathrm{mod}\ p$'ye göre bir karedir. Dolayısıyla Sonuç 3.29'a göre $x^2 + 58y^2 = kp\ , 1 \leq k \leq 2\sqrt{58}$ olacak biçimde x, y, k tam sayıları vardır. Ayrıca $1 \leq k \leq 15$ olduğu görülür. Diğer yandan

$\left(\frac{-58}{3}\right) = \left(\frac{-1}{3}\right) = -1\ ,$
$\left(\frac{-58}{5}\right) = \left(\frac{2}{5}\right) = -1,$
$\left(\frac{-58}{7}\right) = \left(\frac{-2}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{2}{7}\right) = -1,$
$\left(\frac{-58}{11}\right) = \left(\frac{-3}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{3}{11}\right) = (-1)(-1)\left(\frac{11}{3}\right) = \left(\frac{-1}{3}\right) = -1$

ve

$\left(\frac{-58}{13}\right) = \left(\frac{-6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{13}{7}\right) = \left(\frac{-1}{7}\right) = -1$

olduğundan $k = 3,5,6,7,10,11,12,13,14,15$ olamayacağı Sonuç 3.21 kullanılarak gösterilebilir. $k = 1$ ise $x^2 + 58y^2 = p$ olur. $k = 2$ olsun. $2p = x^2 + 58y^2$ olur. O halde x çifttir. $x = 2a$ olsun. Buradan $p = 2a^2 + 29y^2$ elde edilir. O halde y tek tam sayı olur. Bu durumda $p \equiv 2a^2 + 29 (\mathrm{mod}\ 8)$ ve dolayısıyla $p \equiv -3, -1 (\mathrm{mod}\ 8)$ elde edilir. Bu olamaz. $k = 4$ olsun. O zaman $4p = x^2 + 58y^2$ olup x ve y çift olur. Böylece $p = \left(\frac{x}{2}\right)^2 + 58\left(\frac{y}{2}\right)^2$ olur. $k = 8$ olsun. $8p = x^2 + 58y^2$ olur ve bu durumda x ve y çift olur. $x = 2a\ , y = 2b$ olsun. $8p = 4a^2 + 58 \cdot 4b^2$ yani $2p = a^2 + 58b^2$ elde edilir. O halde a çift olur. $a = 2c$ olsun. $p = 2c^2 + 29b^2$ ve böylece

$p \equiv -3, -1 (\text{mod } 8)$ elde edilir. Bu olamaz. $k = 9$ ise $3|x$ ve $3|y$ olacağından $p = \left(\frac{x}{3}\right)^2 + 58\left(\frac{y}{3}\right)^2$ elde edilir.

Teorem 3.40. p asal ve $p > 190$ olsun. $p = x^2 + 190y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p \equiv 1,7(\text{mod } 8)$ ve $\left(\frac{p}{5}\right) = \left(\frac{p}{19}\right) = 1$ dir [7].

Teorem 3.41. p asal ve $p > 253$ olsun. $p = x^2 + 253y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p \equiv 1(\text{mod } 4)$ ve $\left(\frac{p}{11}\right) = \left(\frac{p}{23}\right) = 1$ dir [7].

Teorem 3.42. p asal ve $p > 385$ olsun. $p = x^2 + 385y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p \equiv 1(\text{mod } 4)$ ve $\left(\frac{p}{5}\right) = \left(\frac{p}{7}\right) = \left(\frac{p}{11}\right) = 1$ dir [7].

Teorem 3.43. p asal ve $p > 1365$ olsun. $p = x^2 + 1365y^2$ olan x ve y tam sayıları vardır $\Leftrightarrow p \equiv 1(\text{mod } 4)$ ve $\left(\frac{p}{3}\right) = \left(\frac{p}{5}\right) = \left(\frac{p}{7}\right) = \left(\frac{p}{13}\right) = 1$ dir [7].

Tanım 3.44. D doğal sayısı verilsin. n doğal sayısı için aralarında asal tek türlü belirli x ve y doğal sayıları $n = x^2 + Dy^2$ olacak biçimde mevcut olduğunda $n = tp$, $n = 2tp$ veya $n = t2^s$ olacak biçimde s doğal sayısı, $p > 2$ asal sayısı ve $t|D$ olan t doğal sayısı mevcut ise D'ye uygun(convenient-idoneal) sayı denir [2].

Teorem 3.45. 1 ,2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848 sayıları uygun sayılardır [2].

Euler bu teoremin ispatını aşağıdaki teoremdeki kriteri uygulayarak yapmıştır.

Teorem 3.46. $D > 1$ sayısı uygun sayıdır $\Leftrightarrow$ x ve D aralarında asal olmak üzere $n = x^2 + D < 4D$ olarak yazılan n sayısı ya asaldır ya da bir asalın iki katıdır veya bir asalın karesidir veya n sayısı $s \geq 1$ olmak üzere 2^s biçimindedir [2].

Euler 1848'den büyük başka uygun sayı olmadığını, önce 3000 sonra 10000 sayılarına kadar olan sayılarla hesaplama yaparak ileri sürmüştür.

Teorem 3.47. D pozitif bir tam sayı olsun. Bu durumda aşağıdakiler denktir.

1) Aralarında asal N ve a pozitif tam sayıları şu şartı sağlayacak biçimde vardır: $p \equiv a(\text{mod } N)$ ve p asal ise $p = x^2 + Dy^2$ olacak biçimde x ve y tam sayıları vardır.

2) $p \equiv 1(\text{mod } 4D)$ şartını sağlayan her p asal sayısı için $p = x^2 + Dy^2$ olacak biçimde x ve y tam sayıları vardır.

3) $m = 4D$ olmak üzere $S \subset \mathbb{Z}_m^*$ alt kümesi şu şartı sağlayacak biçimde vardır: p asal ve $p \nmid D$ ise $p = x^2 + Dy^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p \equiv s(\text{mod } m)$ olan bir $s \in S$ vardır.

4) D sayısı bilinen 65 uygun sayıdan biridir. Ayrıca en fazla iki tane daha D değeri vardır ve bu D değerleri 10^8 den küçük değildir [7].

Teorem 3.48. D bilinen uygun sayılardan birini göstersin. Bu durumda p asal sayısı için $p = x^2 + Dy^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p = D$ dir veya aşağıdaki 6 maddenin hepsi sağlanır.

a) $\left(\frac{-D}{p}\right) = 1$ dir.

b) q tek asal sayı ve $q|D$ ise $\left(\frac{p}{q}\right) = 1$ dir.

c) Eğer $D \equiv 0(\text{mod } 8)$ ise $p \equiv 1(\text{mod } 8)$ dir.

d) Eğer $D \equiv 1,4,5(\text{mod } 8)$ ise $p \equiv 1(\text{mod } 4)$ tür.

e) Eğer $D \equiv 2(\text{mod } 8)$ ise $p \equiv 1,3(\text{mod } 8)$ dir.

f) Eğer $D \equiv 6(\text{mod } 8)$ ise $p \equiv 1,7(\text{mod } 8)$ dir [7].

Euler ayrıca aşağıdaki teoremi vermiştir.

Teorem 3.49. 1) D uygun sayı ve $D = t^2$ ise $t = 1,2,3,4,5$ dır.

2) D uygun sayı ve $D \equiv 3(mod\ 4)$ ise $4D$ de uygun sayıdır.

3) D uygun sayı ve $D \equiv 4(\text{mod } 8)$ ise $4D$ de uygun sayıdır.

4) Eğer k^2D uygun sayı ise D de uygun sayıdır.

5) D uygun sayı ve $D \equiv 2(\text{mod } 3)$ ise $9D$ de uygun sayıdır.

6) $D > 1$ uygun sayı ve $D \equiv 1(\mathrm{mod}\ 4)$ ise $4D$ de uygun sayı değildir.

7) D uygun sayı ve $D \equiv 2(\mathrm{mod}\ 4)$ ise $4D$ de uygun sayıdır.

8) D uygun sayı ve $D \equiv 8(\mathrm{mod}\ 16)$ ise $4D$ uygun sayı değildir.

9) D uygun sayı ve $D \equiv 16(\mathrm{mod}\ 32)$ ise $4D$ uygun sayı değildir.

10) D uygun sayı ve $D + a^2 = p^2 < 4D$ olan p asal sayısı varsa $4D$ uygun sayı değildir [2].

Euler' in bu teoremin 4), 6), 8) ve 9) numaralı maddelerinin ispatı tam açık değildir.

Grube [8] numaralı kaynakta, 1877 yılında bu teoremin tam bir ispatını vermiştir.

Uygun sayılarla ilgili daha ayrıntılı bilgi için [2] numaralı kaynağa bakılabilir.

Uygun sayılarla ilgili aşağıdaki teorem verilebilir.

Teorem 3.50. D bir uygun sayıdır $\Leftrightarrow$ $D = ab + bc + ca$ olacak biçimde $0 < a < b < c$ şartını sağlayan a, b, c tam sayıları yoktur [9].

Chowla [10], uygun sayıların sonlu tane olduğunu göstermiştir [11].

Weinberger [12], eğer genelleştirilmiş Riemann hipotezi doğru ise 65 tane uygun sayının olduğunu ispatlamıştır. Eğer genelleştirilmiş Riemann hipotezi doğru değilse en az iki tane daha uygun sayının olduğunu göstermiştir. Bunun için [13] numaralı kaynaktaki Corollary 23'e bakılabilir [14]. Genelleştirilmiş Riemann hipotezi için [15] numaralı kaynağa bakılabilir.

Uygun sayılarla ilgili en güncel makale olan Kani'nin [13] numaralı çalışmasından aşağıdakiler verilebilir.

Önerme 3.51. Eğer D uygun sayı ve $D \equiv 3(\mathrm{mod}\ 4)$ ise $D = 3,7,15$ tir [13].

Teorem 3.52. D uygun sayı ve $t^2 | D,\ t > 0$ ise $t = 1,2,3,4,5$ tir. Ayrıca,

(a) D uygun sayı ve $9|D$ ise $D = 9,18,45,72$ dir.

(b) D uygun sayı ve $25|D$ ise $D = 25$ dir.

(c) D uygun sayı ve $4|D$ ve $\frac{D}{4}$ tek sayı ise $D = 4,12,28,60$ dır.

(d) D uygun sayı ve $16|D$ ise $D = 16,48,112,240$ dır [13].

Önerme 3.53. $D > 288$ ve D uygun sayı ise $D \not\equiv 3(\text{mod } 4)$ tür. Eğer $D \equiv 1,2(\text{mod } 4)$ ve D uygun sayı ise D karesizdir. Ayrıca $D \equiv 0(\text{mod } 4)$ ise $m = \frac{D}{4}$ karesiz uygun sayıdır ve $m \equiv 2(\text{mod } 4)$ tür [13].

Önerme 3.54. D uygun sayı ve $p < \sqrt{D},\ p \nmid n$ ise $\left(\frac{-D}{p}\right) = -1$ dir [13].

Önerme 3.55. $D \equiv 2,4,6(\text{mod } 8)$ olsun. D uygun sayıdır $\Leftrightarrow p > 2$, $p \nmid D$ ve $\left(\frac{-D}{p}\right) = -1$ şartını sağlayan p asal sayısı için $Dt^2 = k(p-k)$ olacak biçimde k ve t pozitif tam sayıları vardır [13].

Önerme 3.56. $D \geq 1$ olsun. D uygun sayıdır $\Leftrightarrow x^2 + Dy^2$ biçiminde yazılabilen p asal sayıları bir m modülüne göre kongrüans bağıntıları ile ifade edilebilir [13].

Teorem 3.57. $p > 14$ asal sayısı verilsin. $1 \leq j \leq k$ için $(a_j, m) = 1$ şartını sağlayan $a_1, a_2, \dots, a_k$ ve m pozitif tam sayıları "$p = x^2 + 14y^2$ olacak biçimde x ve y tam sayıları vardır $\Leftrightarrow p \equiv a_1, a_2, \dots, a_k(\text{mod m})$ dir" önermesini sağlayacak biçimde yoktur [16].

Bu teorem bir önceki teoreme göre 14 sayısının uygun sayı olmadığını gösterir.

Uygun sayılar ile ilgili daha fazla bilgi için [13] numaralı kaynağa bakılabilir.

BÖLÜM 4. SONUÇLAR VE ÖNERİLER

Bu çalışmada, D doğal sayısının bazı değerleri için $p = x^2 + Dy^2$ biçiminde yazılabilen p asal sayılarının sağlaması gerektiği şartlar tespit edilmiştir. Burada ele alınan D doğal sayıları, uygun sayı olarak adlandırılan sayılardır. Bilinen uygun sayıların en büyüğü 1848 ve en küçüğü 1 dir. Çalışmanın konusu iki değişkenli formlarla ilgili olmasına rağmen iki değişkenli formlar bu çalışmada ayrıntılı olarak ele alınmamıştır. İki değişkenli formlar ve özellikle $q(x, y) = Ax^2 + Bxy + Cy^2$ iki değişkenli formu tarafından temsil edilen asal sayılarla ilgili araştırma yapmak isteyenlere [17], [18] ve [19] numaralı kaynakları tavsiye edebiliriz.

KAYNAKLAR

[1] Redmond, D., Number Theory, Marcel Dekker, 1996.

[2] Feri, G., Leonhard Euler's Convenient Numbers, Math. Intelligencer, 7 (1985), 3: 55-59, 64.

[3] Steing, J., On Euler's idoneal Numbers, Elemente Der Mathematik, 21: 73-88, 1960.

[4] Elsholtz, C. A., Combinatorial Approach to Sums of Two Square and Related Problems, Additive Number Theory, Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson, Springer Verlag, 115-140, 2010.

[5] Nagell, T., Introduction to Number Theory, Chelsa Publishing, Second Edition, 1964.

[6] Clark, Pete L. Thue-Vinogradov and Integers of the Form $x^2 + Dy^2$, http://alpha.math.uga.edu/~pete/thuelemmav6.pdf, Erişim Tarihi: 01.11.2021.

[7] Clark, Pete L., Thue's Lemma and Idoneal Quadratic Forms, https://sciencedocbox.com/116200895-Physics/Thue-s-lemma-and-idoneal-quadratic-forms.html, Erişim Tarihi: 01.11.2021.

[8] Grube, F., Ueber einige Eulersche Sätze aus der Theroie der quadratischen Formen. Zeitschrift für Mathematik und Physik 19: 492-519, 1874.

[9] Halter-Koch, F., Quadratic Irrationals: An Indtroduction to Classical Number Theory, Chapman and Hall, 2013.

[10] Chowla, S., An extension of Heilbronn's class-number theorem Quart. Math., 5: 304-307, 1934.

[11] Slone, N.J.A, The On-Line Encyclopedia Of Integer Sequences, http://oeis.org/A000926. Erişim Tarihi: 02.02.2022.

[12] Weinberger, P. J., Exponents of the class groups of complex quadratic fields, Acta Arith. 22: 117-124, 1973.

[13] Kani, E., Idoneal Numbers and Some Genaralizotions, Ann. Sci. Math. Québec, 35(2): 197-227, 2011.

[14] Brandhost, S., Sonel,S., and Veniani, D. C., Idoneal Genera and K3 Surface Covering an Enriques Surface, arXiV: 2003. 08914V6, 7 Jan 2022, Erişim Tarihi: 02.02. 2022.

[15] Agélas, L., Generalized Riemann Hypotesis, http://hal.archives-ouvertes.fr/hal-00747680V3, Erişim Tarihi: 02.02.2022.

[16] Blair, K., Spearmen and Kenneth S. Williams, Representing Primes by Binary Quadratic Forms, The American Mathematical Montly, 99(5): 423-426, 1992.

[17] Niven, I., Zuckerman, H. S., Hugh, M., An Introduction to the theory of numbers, Fifth edition, John Wiley and Sons, 1991.

[18] Cox, D. Primes of the Form $x^2 + ny^2$, John Wiley and Sons, 1989.

[19] Clark, P. L., Geometry of Numbers with Applications to Number Theory, alpha.math.uga.edu/~pete/geometryofnumbers.pdf, Erişim Tarihi: 02.02. 2022.

ÖZGEÇMİŞ

Adı Soyadı **:** Elanur Çetiner Göktaş

ÖĞRENİM DURUMU

Derece	**Eğitim Birimi**	**Mezuniyet Yılı**
Yüksek Lisans	Sakarya Üniversitesi / Fen Bilimleri Enstitüsü / Matematik Bölümü	Devam ediyor
Lisans	Sakarya Üniversitesi / Fen-Edebiyat Fakültesi / Matematik Bölümü	2017
Lise	Adapazarı Anadolu İmam Hatip Lisesi	2012

YABANCI DİL

İngilizce