YAŞAR ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

KARE KALANLAR

Alpaslan SAĞLAM

Tez Danışmanı: Prof. Dr. Rafail ALİZADE

Bornova-İZMİR
2014

Bu tezi okuduğumu ve kapsam ve kalite bakımından yüksek lisans tezi olarak uygunluğunu onaylarım.

Prof. Dr. Rafail ALİZADE (Danışman)

Bu tezi okuduğumu ve kapsam ve kalite bakımından yüksek lisans tezi olarak uygunluğunu onaylarım.

Prof. Dr. Mehmet TERZİLER

Bu tezi okuduğumu ve kapsam ve kalite bakımından yüksek lisans tezi olarak uygunluğunu onaylarım.

Doç. Dr. Engin BÜYÜKAŞIK

Prof. Dr. Behzat GÜRKAN
Enstitü Müdürü

ABSTRACT

QUADRATIC RESIDUES

In this thesis quadratic residues are considered for solving congruences of order two. To investigate whother a given number is a perfect square, Eulerss theorem, Gauss Lemma, Quadratic reciprocity formula and properties of Legendre symbol are used. These results are used for solving mathematical olympiad problems concerning number theory.

Alpaslan SAĞLAM
MSc, Department of Mathemetics
Supervisor: Prof. Dr. Rafail ALİZADE

December 2014, 52 pages

Keywords: Quadratic Congruences, Quadratic Residue, Legendre Symbol, Quadraic Reciprocity.

ÖZET

KARE KALANLAR

Bu tezde ikinci dereceden bir denkliğin çözümü için kare kalanlar kullanılması incelenmiştir. Sayıların değişik mod'larda kare kalan olup olmadığının araştırılması için Euler Kriterinin, Gauss Lemmasının, Karesel Karşılık formülünün ve Legendre sembolünün özelliklerinin kullanılmıştır. Bu sonuçlar sayı teorisi ile ilgili matematik olimpiyat sorularının çözümü için kullanılmıştır.

Alpaslan SAĞLAM
Yüksek Lisans Tezi, Matematik Bölümü
Tez Danışmanı: Prof. Dr. Rafail ALİZADE
Aralık 2014, 52 sayfa

Anahtar sözcükler: İkinci Dereceden Denklemler, Kare Kalan, Legendre Simgesi, Karesel Karşılık.

TEŞEKKÜR

Bu çalışmanın belirlenmesinde ve yürütülmesinde yardımlarını esirgemeyen sayın Prof. Dr. Rafail ALİZADE'ye teşekkürü bir borç bilirim. Aynı zamanda bu çalışmamda beni daima destekleyen sevgili eşim Emel SAĞLAM'a teşekkür ederim.

Alpaslan SAĞLAM

İzmir, 2014

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “Kare Kalanlar” adlı çalışmanın, tarafımdan bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin bibliyografyada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

18.12.2014

Alpaslan SAĞLAM

İÇİNDEKİLER

Sayfa

ABSTRACT iii
ÖZET iv
TEŞEKKÜR v
YEMİN METNİ vi
1 GİRİŞ 1
2 KARE KALANLAR 2
2.1 KARE KALANLAR 2
3 MATEMATİK OLİMPİYATLARI SORULARI VE ÇÖZÜMLERİ 24
3.1 ÖRNEKLER 24
REFERANSLAR 51
ÖZGEÇMİŞ 52

1 GİRİŞ

Bu tezdeki amacımız ikinci dereceden bir denkliğin çözüm yollarını araştırmak ve bu denkliklerin nasıl çözülebildiğini göstermektir. Bu denkliklerin çözümü, ikinci dereceden denklemlerin çözümüne benzer şekilde tam kareye tamamlama yöntemiyle, p bir asal sayı olmak üzere $x^2 \equiv n \pmod{p}$ denkliğinin çözümüne indirgeniyor. Son denkliğin çözümü varsa n'ye mod p' de kare kalan denir. Bu tezde değişik n ve p'ler için n'nin mod p'de kare kalan olup olmadığını araştırdık ve bunun değişik uygulamarını bulduk. Kare kalanların incelenmesinde önemli yer tutan Euler Kriterini, Gauss Lemmasını ve Legendre sembolünün değişik özelliklerini verdik. Bunları ve Karesel Karşılık formülünü kulanarak Legendre sembolünün nasıl hesablanabileceğini gösterdik.

Sayı teorisi ile ilgili matematik olimpiyat sorularının çözümünde kare kalanlar önemli rol oynamaktadır. Tezde böyle sorulara geniş yer verdik. Bu sorulardan bir kısmı verilen sayıların tam kare veya tam küp olup olmaması ile ilgilidir. Bir sayının tam kare (tam küp) olmaması çoğunlukla değişik mod'lar da kare kalanların incelenmesi ile çözülüyor. Bunun dışındaki yöntemlerle de (örneğin iki ardışık tam kare veya tam küp arasına sıkıştırma yöntemi) çözüm örnekleri verdik. Tam kare olan sayının bulunması da genelde çarpanlara ayırma veya yine kare kalanlar yardımıyla eleme yöntemleriyle çözülmektedir. Bunlarla ilgi örnekler de tezde yerini buldu. Değişik ülkelerin matematik olimpiyatlarında çıkmış konuyla ilgili sorulara tezde geniş yer verdik. Tezin matematik olimpiyatlarına çalışacak öğrenciler ve bunları çalıştıracak öğretmenler için faydalı olacağını umuyoruz.

Bu tezin 2. Bölümünde Kare Kalanlarla ilgili tanım, teorem, çözümlü örnekler verilmiştir. 3. Bölümde ise uluslararası ve ulusal matematik olimpiyatlarında çıkmış sorular ve benzer soru tarzlarının çözümleri verilmiştir.

2 KARE KALANLAR

2.1. KARE KALANLAR

$ax^2+bx+c\equiv 0\pmod m$ ikinci dereceden denkliğini çözmek istediğimizi düşünelim. Bu çözümler aynı denkliğin, p asal sayı olmak üzere, mod p'deki çözümlerine bağlıdır. p'nin küçük değerleri için bu denklikler deneme yanılma yöntemiyle kolayca çözülür. Fakat büyük p değerleri için daha gelişmiş yöntemler gereklidir.

p tek asal sayı ve $(a,p)=1$ (a ile p'nin O.B.E.B.'i 1'dir.) olsun. $(4,p)=1$ olduğundan, $(4a,p)=1$ 'dir. Dolayısıyla $x^2+bx+c\equiv 0\pmod p$ denkliğinin çözümü $4ax^2+4abx+4ac\equiv 0\pmod p$ denkliğiyle eşdeğerdir. Son denklikten $(2ax+b)^2\equiv(b^2-4ac)\pmod p$ elde edilir. Bu denkliğin çözümünün olması için y_0, $y^2\equiv(b^2-4ac)\pmod p$ denkliğinin bir çözümü olmak üzere, $(2ax+b)\equiv y_0\pmod p$ denkliğini sağlayan bir x_0 tam sayısını bulunması gerek ve yeterlidir. $(2a,p)=1$ olduğundan son denkliğin $\left[(2ax+b)\equiv y_0\pmod p\right]$ her çözümü vardır. Böylece, $ax^2+bx+c\equiv 0\pmod p$ denkliğinin çözümünün bulunması $y^2\equiv k\pmod p$ şeklinde olan denkliğin çözümünün bulunmasına bağlıdır. $k\not\equiv 0\pmod p$ ise denkliğinin bariz çözümü vardır. $k\not\equiv 0\pmod p$ durumunu incelemeden önce bildiğimiz yöntemleri nasıl kullanabileceğimize bakalım.

$a=b$ ise doğal olarak $a\equiv b\pmod m$'dir. O halde 2. Dereceden denklemleri çözmek için kullanılan alışılmış yöntemleri kullanırız. Sadece, bölme yerine sayının mod m'deki tersi ile çarparız. Öte yandan her zaman k'nın mod m'de karekökünün olup olmadığı varsa bunun bulunması kolay olmayabilir. Yine de bizim bilgilerimiz denkliği çözmek için etkili olabilir.

Örnek 1: Aşağıdaki denkliklerin çözümlerini bulalım. (Sıerpınskı, 1970, 136)

a) $3x^2+6x+5\equiv 0\pmod 7$ **b)** $x^2+6x+2\equiv 0\pmod 7$

c) $7x^2-4x+1\equiv 0\pmod{11}$ **d)** $7x^2-4x+2\equiv 0\pmod{11}$

Çözüm:

a) $3x^2+6x+5\equiv 0\pmod 7$

$15x^2+30x+25\equiv 0$

$x^2+2x+4\equiv 0$

$x^2+2x+1\equiv 4$

$(x+1)^2\equiv 2^2$

$x+1\equiv \mp 2\Rightarrow x\equiv -3,1$ yani $x\equiv 4,1$ olur.

b) $x^2+6x+2\equiv 0\pmod 7$

$x^2+6x+9\equiv 0$

$(x+3)^2\equiv 0\Rightarrow x\equiv -3$ yani $x\equiv 4$ olur.

c) $7x^2-4x+1\equiv 0\pmod{11}$

$56x^2-32x+8\equiv 0$

$x^2+12x+36\equiv 28$

$(x+6)^2\equiv 6$

Karesi 6 olan sayı olmadığından bu dekliğin çözümü yoktur.

d) $7x^2-4x+2\equiv 0\pmod{11}$

$56x^2-32x+16\equiv 0$

$x^2-10x+25\equiv 9$

$(x-5)^2\equiv 3^2$

$x-5\equiv \mp 3\Rightarrow x\equiv 2,8$ olur.

Örnek 2: Aşağıdaki denkliklerin çözümlerini bulalım.

a) $3x^2+6x+5\equiv 0\pmod{49}$ **b)** $3x^2+6x+5\equiv 0\pmod{539}$

Çözüm:

a) Bir önceki örnekten $3x^2+6x+5\equiv 0\pmod 7 \Rightarrow x\equiv 4,1$ dir. Buradan $x\equiv 7k+1$ veya $x\equiv 7k+4$ formundadır.

i. $x\equiv 7k+1$ ise $3(7k+1)^2+6(7k+1)+5\equiv 0\pmod{49}$

$$3(49k^2+14k+1)+42k+6+5\equiv 0\pmod{49}$$

$$3\cdot 49k^2+84k+14\equiv 0\pmod{49}$$

$$84k+14\equiv 0\pmod{49}$$

$$35k\equiv -14\pmod{49}$$

$$k\equiv 1\pmod{49}$$

$x=7k+1=8$ olur.

ii. $x\equiv 7k+4$ ise $3(49k^2+14k+1)+42k+6+5\equiv 0\pmod{49}$

$$3(49k^2+56k+16)+42k+24+5\equiv 0\pmod{49}$$

$$3\cdot 49k^2+210k+77\equiv 0\pmod{49}$$

$$14k+28\equiv 0\pmod{49}$$

$$14k\equiv -28\pmod{49}$$

$$k\equiv -2\pmod{49}$$

$x=7k+4=-10\equiv 39$ olur.

b) $3x^2+6x+5\equiv 0\pmod{539}\Rightarrow 3x^2+6x+5\equiv 0\pmod{11\cdot 49}$

i. a şıkkından $3x^2+6x+5\equiv 0\pmod{49}\Rightarrow x\equiv 8$ veya $x\equiv 39$ dur.

Yani $x=49k+8$ veya $x=49k+39$ formundadır.

ii. $3x^2+6x+5\equiv 0\pmod{11}$

- $x=49k+8\Rightarrow 3\cdot(49k+8)^2+6\cdot(49k+8)+5\equiv 0$

$$3\cdot 49^2\cdot k^2+3\cdot 2\cdot 49k\cdot 8+3\cdot 8^2+6\cdot 49k+6\cdot 8+5\equiv 0$$

$9k^2+6k+3\equiv 0$

$(3k+1)^2\equiv 9$

$3k+1=3$ veya $3k+1=-3$ buradan çözüm yoktur.

- $x=49k+39\Rightarrow 3\cdot(49k+39)^2+6\cdot(49k+39)+5\equiv 0$

$3\cdot 49^2\cdot k^2+3\cdot 2\cdot 49k\cdot 39+3\cdot 39^2+6\cdot 49k+6\cdot 39+5\equiv 0$

$k^2-6k+9\equiv 1$

$k-3=\pm 1\Rightarrow k=4$ veya $k=2$ dir.

Buradan $x=137$ ve $x=235$ çözümdür.

Örnek 3: Aşağıdaki denkliklerin çözümlerini bulalım.

a) $7x^2-4x+2\equiv 0\pmod 7$ **b)** $7x^2-4x+2\equiv 0\pmod{77}$

Çözüm:

a) $7x^2-4x+2\equiv 0\pmod 7$

$-4x+2\equiv 0$

$3x\equiv -2$

$15x\equiv -10$

$x\equiv 4$ olur.

b) $7x^2-4x+2\equiv 0\pmod{77}\Rightarrow 7x^2-4x+2\equiv 0\pmod{7\cdot 11}$ olur. Önceki örneklerden;

$7x^2-4x+2\equiv 0\pmod 7\Rightarrow x\equiv 4,11,18,25,32,39,46,53,60,67,74,...$

$$7x^2-4x+2\equiv 0\pmod{11}\Rightarrow \begin{cases} x\equiv 2,13,24,35,46,57,68,... \\ x\equiv 8,19,30,41,52,63,74,... \end{cases}$$

olduğundan, $x=46$ ve $x=74$ çözümdür.

Örnek 4: Aşağıdaki denkliklerin çözümlerini bulalım.

a) $3x^2+2x\equiv 0\pmod{13}$ **b)** $x^2+9x+4\equiv 0\pmod{13}$

Çözüm:

a) $3x^2+2x\equiv 0\pmod{13}\Rightarrow x(3x+2)\equiv 0\pmod{13}$

- $x\equiv 0$

- $3x+2\equiv 0\pmod{13}$

  $27x+18\equiv 0$

  $x+5\equiv 0$

  $x\equiv 8$

Buradan, $x\equiv 0$ ve $x\equiv 8$ çözümdür.

b) $x^2+9x+4\equiv 0\pmod{13}$

$x^2-4x+4\equiv 0$

$(x-2)^2\equiv 0$

$x\equiv 2$ çözümdür.

Örnek 5: $3x^2+x+3\equiv 0\pmod{17}$ denkliğinin çözümlerini (varsa) bulalım.

Çözüm 1:

$\mod 17$ 'de aşağıdaki denklikleri yazabiliriz.

$3x^2+x+3\equiv 0$

$18x^2+6x+18\equiv 0$

$x^2+6x\equiv -1$

$x^2+6x+9\equiv 8$

$(x+3)^2\equiv 25$

$x+3\equiv \pm 5$ ise $x\equiv -8,2$ veya $x\equiv 2,9$ olur.

Çözüm 2:

Çözüm1'de biz denkliklerin özelliklerini ve tam kareye tamamlama yöntemini kullandık. Fakat 2. dereceden denklemin çözüm formülünü de kullanabilirdik.

$3\cdot 6=18\equiv 1\pmod{17}$ olduğundan, $6^{-1}\equiv 3\pmod{17}$ böylece

$x\equiv 6^{-1}\left(-1\pm\sqrt{1-36}\right)$ ise $x\equiv 3\left(-1\pm\sqrt{-35}\right)$ 'de $\sqrt{-35}$ varsa bulunması gerekir.

Fakat biz -35 'e 17'nin katlarını ekleyerek $-35\equiv 16\pmod{17}$ ve böylece

$x\equiv 3\left(-1\pm\sqrt{16}\right)\equiv 3(-1\pm 4)\equiv -15,9\equiv 2,9\pmod{17}$

Tabi ki -35 'in $\mod 17$ 'de kökü olmasaydı denkliğinde çözümü

olmayacaktı. Bu bizi aşağıdaki soruya yaklaştırıyor. Verilen bir sayının bir p modunda ne zaman karekökü vardır.

Tanım 2.1.1. p bir tek asal sayı $(n, p)=1$ olsun. $x^2 \equiv n \pmod{p}$ denkliğinin çözümü varsa n'ye $\bmod p$ 'de kare kalan denir.

Tanımdan görüldüğü gibi p moduna göre, kare kalanlar tam olarak p moduna göre karelerdir. Örneğin $\bmod 5$'te 1 ve 4 kare kalandır. $\bmod 7$'de 1, 4 ve 2 kare kalandır. Her tek p asal sayısı ve $(a, p)=1$ için $a^2 \bmod p$'de kare kalandır. (Sıerpınskı, 1970, 134)

Örnek 6: 11 sayısının kare kalanlarını bulalım.

Çözüm: 11 sayısının kare kalanlarını bulmak demek, $0, 1, 2, \ldots, 10$ sayılarının karelerinin $\bmod 11$ e göre kalanlarını bulmak demektir.

$1^2 \equiv 10^2 \equiv 1 \pmod{11}$, $2^2 \equiv 9^2 \equiv 4 \pmod{11}$, $3^2 \equiv 8^2 \equiv 9 \pmod{11}$,

$4^2 \equiv 7^2 \equiv 5 \pmod{11}$, $5^2 \equiv 6^2 \equiv 3 \pmod{11}$ olduğundan kare kalanlar $1, 3, 4, 5, 9$ sayılarıdır. $2, 6, 7, 8, 10$ sayıları kare kalan değildir.

Örnek 7: 13 sayısının kare kalanlarını bulalım.

Çözüm: 13 sayısının kare kalanlarını bulmak demek, $0, 1, 2, 3, \ldots, 12$ sayılarının karelerinin $\bmod 13$ e göre kalanlarını bulmak demektir.

$1^2 \equiv 12^2 \equiv 1 \pmod{13}$, $2^2 \equiv 11^2 \equiv 4 \pmod{13}$, $3^2 \equiv 10^2 \equiv 9 \pmod{13}$,

$4^2 \equiv 9^2 \equiv 3 \pmod{13}$, $5^2 \equiv 8^2 \equiv 12 \pmod{13}$, $6^2 \equiv 7^2 \equiv 10 \pmod{13}$ olduğundan kare kalanlar $1,3,4,9,10,12$ sayılarıdır. $2,5,6,7,8,11$ sayıları kare kalan değildir.

Örnek 8: $x^2 \equiv 3 \pmod{5}$'in çözümü yoktur. Çünkü $\{0, \pm 1, \pm 2\}$ nin çözüm olmadığı söylenebilir. Şu halde $3, \bmod 5$'te bir kare kalan değildir.

Örnek 9: $x^2 \equiv -3 \pmod{7}$' nin çözümleri ± 2 dir. Şu halde $-3, \bmod 7$'de bir kare kalandır.

Teorem 2.1.1: (Euler Kriteri) $p \neq 2$ asal ve $p \nmid a$ olsun. $x^2 \equiv a \pmod{p}$'nin bir çözümü vardır $\Leftrightarrow$ $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ olmasıdır. (Çallıalp, 2009, 59)

Teorem 2.1.2: $p > 2$ bir asal sayı olmak üzere, 1, 2, 3, ... , $p-1$ sayılarından $\frac{p-1}{2}$ tanesi p'nin kare kalanı, $\frac{p-1}{2}$ tanesi de p'nin kare kalanı değildir. (Gürlü, 2009, 156)

İspat: Mod p'ye göre $\{1, 2, 3, \ldots , p-1\}$ kümesinin denklik sınıfı olarak $\left\{\pm 1, \pm 2, \pm 3, \ldots , \pm \frac{p-1}{2}\right\}$ şeklinde yazabiliriz. Bunların karelerini düşünürsek, kare kalanlar, $\left\{1^2, 2^2, 3^2, \ldots , \left(\frac{p-1}{2}\right)^2\right\}$ bulunur. Bunlar birbirinden farklı olup, sayıları da $\frac{p-1}{2}$ dir. Geriye kalanlarda kare kalan değildir.

Örnek 10: S ; $2n+1$ ve $3n+1$ ifadelerinin ikisini birden tam kare yapan $n \in N$ değerlerinin kümesidir. Buna göre, S kümesindeki elemanların ortak bölenlerinin en büyüğü kaçtır? (Gürlü, 2009, 158)

Çözüm:

$a \text{ ve } b \in N$ olmak üzere, $2n+1 = a^2$, $3n+1 = b^2$ şeklinde yazıldığında $3a^2 - 2b^2 = 1 \mod 5$'e göre, kare kalanlar 0, 1 ve 4'tür. Buda ancak $a^2 \equiv b^2 \equiv 1 \pmod{5}$ için gerçekleşir. Buna göre, $2n+1 = a^2 = 5k+1$; $3n+1 = b^2 = 5k' +1$ formundadır ki bu da $5 \mid n$ demektir.

$\mod 8$'e göre kare kalanlar 0, 1 ve 4'tür. Yukarıda olduğu gibi $3a^2 - 2b^2 = 1$ durumu ancak $a^2 \equiv b^2 \equiv 1 \pmod{8}$ için sağlanır. Bu da $2n+1 = a^2 = 8m+1$, $3n+1 = b^2 = 8m' +1$ demektir ki $8 \mid n$ ' dir.

O halde 5 ve 8 sayıları n'yi böler. $2n+1$ ve $3n+1$ ifadelerinin ikisinin birden tam kare olmasını sağlayan n doğal sayılarının en küçüğü 40 olduğuna göre S kümesindeki elemanların O.B.E.B.'i 40'tır.

Örnek 11: $\text{mod}\,11$ 'de kare kalanlar, $\{1, 2^2, 3^2, 4^2, 5^2\}$ yani $\{1,3,4,5,9\}$ olarak bulunur.

Tanım 2.1.2: $p \neq 2$ asal tam sayı olsun,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & eğer\ p \nmid \text{a} \quad ve \quad a\ kare\ kalan\ ise, \\ -1, & eğer\ p \nmid \text{a} \quad ve\ a\ kare\ kalan\ değilse, \\ 0, & eğer\ p \mid \text{a} \quad ise, \end{cases}$$

ile tanımlanır ve $\left(\frac{a}{p}\right)$'ye Legendre Sembolü denir. (Çallıalp, 2009, 60)

Örnek 12: $p \neq 2$ asal tam sayı olsun. Euler Kriterinden

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1; & eğer\ p \equiv 1 \pmod 4\ ise, \\ -1; & eğer\ p \equiv 3 \pmod 4\ ise, \end{cases}$$

olduğu kolayca görülür.

Örnek 13: $p > 2$ bir asal sayı olmak üzere,

$\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)+...+\left(\frac{p-1}{p}\right)=0$ olduğunu gösteriniz?

Çözüm:

Örneğin anlaşılması açısından, durumu $p=5$ için gösterelim. Legendre sembolü olarak $x^2 \equiv a \pmod p$ için çözüm varsa yani a sayısı $\text{mod}\ p$'ye göre kare kalan ise bu durum $\left(\frac{1}{p}\right)=1$ ve kare kalan değil ise $\left(\frac{1}{p}\right)=-1$ şeklinde gösteriliyordu. $\left(\frac{1}{5}\right)+\left(\frac{2}{5}\right)+\left(\frac{3}{5}\right)+\left(\frac{4}{5}\right)=1-1+1-1=0$ demektir. Yani $x^2 \equiv 1 \pmod 5$ için çözüm olduğudan $1,\ \text{mod}\ 5$'e göre kare kalandır.

$x^2 \equiv 2 \pmod 5$ çözüm olmadığından $\left(\frac{2}{5}\right)=-1$ dir. $1^2+2^2+3^2+...+\left(\frac{p-1}{2}\right)^2$ $\text{mod}\ p$'ye göre farklı değerlere denktirler. $\left(\frac{p+1}{2}\right)^2,...,(p-1)^2$ sayıları $\text{mod}\ p$'ye göre biri diğerinin negatifi olan aynı değerlere denktirler. $\frac{p-1}{2}$ tane

kare kalan, $\frac{p-1}{2}$ tane kare kalan olmayan sayı olduğunu biliyoruz. O halde, $\frac{p-1}{2}$ tane 1'in toplamı ile $\frac{p-1}{2}$ tane -1'in toplamı sıfır(0) yapar.

Örnek 14: $p \neq 2$ asal tam sayı ise $\sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = 0$'dır. Çünkü, $1 \leq k \leq p-1$'lerin yarısı için $\left(\frac{k}{p}\right) = +1$, diğer yarısı için, $\left(\frac{k}{p}\right) = -1$ ve hepsinin toplamı da 0 olur.

Legendre Sembolünün şu özellikleri vardır.

Teorem 2.1.3:

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

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

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

iv. $p \nmid c\ ise \left(\frac{ac^2}{p}\right) = \left(\frac{a}{p}\right)$ dir.

İspat:

i. Euler Kriterinden $p \nmid a\ ise \left(\frac{a}{p}\right) = 1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ olduğundan, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ bulunur. $p \mid a\ ise\ a^{\frac{p-1}{2}} \equiv 0 = \left(\frac{a}{p}\right) \pmod{p}$ olduğu açıktır.

ii. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ ve $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \pmod{p}$ denkliklerinden $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ elde edilir.

iii. Eğer $a \equiv b \pmod{p}$ *ise* $x^2 \equiv a \pmod{p}$ *ve* $x^2 \equiv b \pmod{p}$ denklikleri aynıdır. Şu halde $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ elde edilir.

iv. $p \nmid$ c *ise* $x^2 \equiv c^2 \pmod{p}$'nin çözümü var, şu halde $\left(\frac{c^2}{p}\right) = 1$ dir.

Yukarıdaki özelliklerden $\left(\frac{ac^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{c^2}{p}\right) = \left(\frac{a}{p}\right)$ bulunur.

Sonuç 2.1.1: $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ eşitliğinden; iki kare kalanın ve iki kare kalan olmayan sınıfın çarpımının kare kalan ve bir kare kalan ile kare kalan olmayan sınıfın çarpımının da bir kare kalan olmayan sınıfın olduğu anlaşılır.

Sonuç 2.1.2: p tek asal sayı, $n = \prod_{i=1}^{s} m_i$ ve $\forall i$ için $(m_i, p) = 1$ ise $\left(\frac{n}{p}\right) = \prod_{i=1}^{s}\left(\frac{m_i}{p}\right)$ dir.

İspat: $\forall i$ için $(m_i, p) = 1$ olduğunda $(\mathrm{n}, p) = 1$ dir. O halde, Euler Kriterinden $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} = \prod_{i=1}^{s} m_i^{\frac{p-1}{2}} \equiv \prod_{i=1}^{s}\left(\frac{m_i}{p}\right) \pmod{p}$ ve bir k tam sayısı için $\left(\frac{n}{p}\right) - \prod_{i=1}^{s}\left(\frac{m_i}{p}\right) = kp$ Legendre simgesinin tanımından dolayı sol taraf sadece ± 2 veya sıfır(0) olabilir. p tek asal sayı olduğundan bu $k = 0$ durumunda olmak zorunda ve $\left(\frac{n}{p}\right) = \prod_{i=1}^{s}\left(\frac{m_i}{p}\right)$, $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, $\alpha_i \geq 1$ n sayısının asal çarpanlara ayrılışı ise ve p ile n aralarında asal olan tek asal sayı ise son yaptığımız sonuçtan $\left(\frac{n}{p}\right) = \prod_{i=1}^{r}\left(\frac{p_i}{p}\right)^{\alpha_i}$ Böylece n sayısının mod p'de kare kalan olup olmaması n'nin her asal çarpanının mod p'de kare kalan olup olmamasına indirgeniyor.

Tanım 2.1.3: p bir asal tam sayı olmak üzere; $g^0 = 1, g, ..., g^{p-2}$ indirgenmiş (sıfırdan farklı) tam temsilciler sistemi olacak şekilde bir $g \in Z$ varsa g ye modulo p de bir ilkel kök denir.

g nin modulo p de bir ilkel kök olması için gerek ve yeter koşul $g^k \equiv 1 \pmod{p}$ olacak şekilde en küçük pozitif k sayısının $p-1$ olmasıdır.

$g \pmod{p}$ bir ilkel kökse her $p \nmid a$ için $a \equiv g^i \pmod{p}$ olacak şekilde bir $0 \le i < p-1$ bulunabilir. i ye a nın g ye göre indisi denir ve $i = ind\, a$ ile gösterilir. İndisin logaritmaya benzeyen şu özellikleri gösterilebilir.

i. $a \equiv b \pmod{p}$ ise $ind\, a \equiv ind\, b \pmod{p-1}$,

ii. $ind\, ab \equiv ind\, a + ind\, b \pmod{p-1}$,

iii. a nın $\pmod{p}$ tersi $a*$ ise $a* \equiv -ind\, a \pmod{p-1}$.

İndisler yardımı ile $ax \equiv b \pmod{p}$, $(a, p) = 1$ denkliğini çözebiliriz. İndis özelliklerinden $ax \equiv b \pmod{p} \Leftrightarrow ind\, a + ind\, x \equiv ind\, b \pmod{p-1}$ olduğundan a ve b verilince $ind\, x$, dolayısı ile x bulunmuş olur.

$p \neq 2$ asal tam sayı ve g, mod p ilkel kök olsun. Bu takdirde $\{g, g^3, ..., g^{p-2}\}$ kare kalan olmayan sınıflardır. Çünkü, $x^2 \equiv g^k \pmod{p}$'nin çözümü olması için gerek ve yeter koşul $2\, ind\, x \equiv k \pmod{p-1} \Leftrightarrow k$ *çift* olmasıdır.

$\left(\frac{a}{p}\right)$ yi hesaplamak için, $a = \pm p_1^{a_1} \cdots p_r^{a_r}$ şeklinde asal çarpanlara ayrılır ve $\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \left(\frac{p_1^{a_1}}{p}\right) \cdots \left(\frac{p_r^{a_r}}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \left(\frac{p_1}{p}\right)^{a_1} \cdots \left(\frac{p_r}{p}\right)^{a_r}$ eşitliğinden $p \neq q$ asallar olmak üzere; $\left(\frac{p}{q}\right)$ leri bilmek yeterli olacaktır. Bunu hesaplamak için önce Gauss Lemması olarak bilinen şu önermeyi ispatlamalıyız.

Teorem 2.1.4: (Gauss Lemma) $p \neq 2$ asal ve $p \nmid a$ olsun.

$S = \left\{ a, 2a, ..., \frac{p-1}{2} a \right\}$ tam sayılarının her biri $\left[-\frac{p-1}{2}, \frac{p-1}{2} \right]$ aralığındaki tam sayılardan birine $\bmod p$ denktir. v ile bu aralıktaki negatif tam sayılardan birine denk olan S deki tam sayıların sayısını gösterelim. Bu takdirde $\left(\frac{a}{p} \right) = (-1)^v$ dir.

İspat:

$1 \leq k \neq k' \leq \frac{p-1}{2}$ ise $ka \not\equiv \pm k'a \pmod{p}$ dir. Gerçekten,

$ka \equiv k'a \pmod{p} \Rightarrow k = k'$ çelişkisi ve

$ka \equiv -k'a \pmod{p} \Rightarrow k + k' \equiv 0 \pmod{p}$ $\left(1 \leq k + k' < p \text{ olduğundan} \right)$ çelişkisi bulunurdu. $1 \leq k \leq \frac{p-1}{2}$ için, $r_k \equiv ka \pmod{p}$ ve $-\frac{p-1}{2} \leq r_k \leq \frac{p-1}{2}$ olsun. Şu halde önermede sayacağımız negatif sayılar, $r_1, r_2, ..., r_{\frac{p-1}{2}}$ ler arasında negatif olanlardır. Yukarıda gösterdiğimiz gibi $k \neq k'$ ise $r_k \neq r_{k'}$, yani $|r_k| \neq |r_{k'}|$ dir.

$|r_1|, |r_2|, ..., \left| r_{\frac{p-1}{2}} \right|$ nin sayısı $\frac{p-1}{2}$ ve 1 ile $\frac{p-1}{2}$ arasında birbirinden farklı olduklarına göre bunlar sıraları hariç $1, 2, ..., \frac{p-1}{2}$ den başka bir şey değildirler. Şu halde $r_1 r_2 \cdots r_{\frac{p-1}{2}} = (-1)^v 1 \cdot 2 \cdots \frac{p-1}{2}$ olur. $r_k \equiv ka \pmod{p}$ olduğundan, olur son iki denklikten

$(-1)^v 1 \cdot 2 \cdots \frac{p-1}{2} \equiv a^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdots \frac{p-1}{2} \pmod{p}$ ve $1 \cdot 2 \cdots \frac{p-1}{2}$ ile her iki yanı kısaltarak, Euler kriterinden $(-1)^v \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p} \right) \pmod{p}$ bulunur.

Örnek 15: $p \neq 2$ asal tam sayısı için $\left(\frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}}$ olduğunu, **Örnek 14** de Euler Kriterinden söylemiştik. Şimdi aynı sonucu Gauss Lemmayı kullanarak

gösterelim. $a=-1$ alırsak; $1(-1), 2(-1),..., \frac{p-1}{2}(-1)$ nin hepsi negatif ve $\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$ aralığında olduklarından, $v=\frac{p-1}{2}$ bulunur.

Örnek 16: $p\neq 2$ asal tam sayısı için $\left(\frac{2}{p}\right)$ yi hesaplayalım. $a=2$ alırsak, listemizdeki Sayılardan $1\cdot 2,\ 2\cdot 2, 3\cdot 2, ..., \frac{p-1}{2}\cdot 2$, $\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$ aralığındakilerden birine denk olanların negatiflerini saymak gerekir. Negatif olanlar $\frac{p}{2}\leq 2k\leq p$ arasında olanlardır. Yani $\frac{p}{4}\leq k\leq \frac{p}{2}$ olmalıdır. $p=8m+r$, $0\leq r<8$ koyarsak, p tek olduğundan, $r=1, 3, 5, 7$ olabilir.

Şu halde $2m+\frac{r}{4}\leq k\leq 4m+\frac{r}{2}$ olmalıdır. r için 4 seçeneği ayrı ayrı inceleyelim:

$r=1$ için $2m+\frac{1}{4}\leq k\leq 4m+\frac{1}{2}\Rightarrow k=2m+1, 2m+2, ..., 4m$ olabilir.

Bunların sayısı $v=2m$ dir. Bu halde $p\equiv 1(\mathrm{mod}\,8)$ ise $v=2m$ çift ve $\left(\frac{2}{p}\right)=(-1)^{v}=(-1)^{2m}=+1$ olur.

$r=3$ için $2m+\frac{3}{4}\leq k\leq 4m+\frac{3}{2}\Rightarrow k=2m+1, \ldots, 4m, 4m+1$ olabilir.

Bunların sayısı $v=2m+1$ dir. Bu halde $p\equiv 3(\mathrm{mod}\,8)$ ise $v=2m+1$ tek ve $\left(\frac{2}{p}\right)=(-1)^{v}=(-1)^{2m+1}=-1$ olur.

$r=5$ için $2m+\frac{5}{4}\leq k\leq 4m+\frac{5}{2}\Rightarrow k=2m+2, 2m+3, \ldots, 4m+2$ olabilir.

Bunların sayısı $v=2m+1$ dir. Bu halde $p\equiv 5(\mathrm{mod}\,8)$ ise $v=2m+1$ tek ve $\left(\frac{2}{p}\right)=(-1)^{v}=(-1)^{2m+1}=-1$ olur.

$r=7$ için $2m+\frac{7}{4}\leq k\leq 4m+\frac{7}{2}\Rightarrow k=2m+2, ..., 4m+2, 4m+3$ olabilir.

Bunların sayısı $v=2m+2$ dir. Bu halde $p\equiv 7\pmod 8$ ise $v=2m+2$ çift ve $\left(\frac{2}{p}\right)=(-1)^{v}=(-1)^{2m+2}=+1$ olur.

Böylece sonuç olarak, $\left(\frac{2}{p}\right)=\begin{cases}+1; \text{eğer } p\equiv \pm 1\pmod 8 \text{ ise}\\ -1; \text{eğer } p\equiv \pm 3\pmod 8 \text{ ise}\end{cases}$ bulunur.

$p\equiv \pm 1\pmod 8 \Leftrightarrow \frac{p^2-1}{8}$ çift demek olduğundan, $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ yazabiliriz.

Örnek 17: $p>3$ asal tam sayı için $\left(\frac{3}{p}\right)$ yi hesaplayalım. Gauss Lemmasındaki listemizdeki sayılar 1 ile $\frac{3p}{2}$ arasında;

$1<1\cdot 3, 2\cdot 3, 3\cdot 3, \ldots, \frac{p-1}{2}\cdot 3<\frac{3p}{2}$ olur. Bunları $\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$ arasındaki sayılardan birine modülo p denk yapınca 1 ile $\frac{p}{2}$ arasında olanlar pozitif, $\frac{p}{2}$ ile p arasında olanlar negatif ve p ile $\frac{3p}{2}$ arasında olanlar pozitif olurlar. Şu halde v; $\frac{p}{2}\le 3k\le p$ olan k ların sayısıdır. Buradan $\frac{p}{6}\le k\le \frac{p}{3}$ bulunur. $p=12m+r$, $r=1,5,7,11$ $(p \text{ tek})$ koyarsak, $2m+\frac{r}{6}\le k\le 4m+\frac{r}{3}$ bulunur. $r=1,5,7,11$ için değerleri tabloda gösterelim.

r	k nın aralığı	v	tek-çift	$\left(\frac{3}{p}\right)$
1	$[2m+1, 4m]$	$2m$	çift	+1
5	$[2m+1, 4m+1]$	$2m+1$	tek	-1
7	$[2m+2, 4m+2]$	$2m+1$	tek	-1
11	$[2m+2, 4m+3]$	$2m+2$	çift	+1

sonuç olarak $\left(\frac{3}{p}\right)=+1 \Leftrightarrow p\equiv \pm 1\pmod{12}$ elde edilir.

Not: Son iki örnekte $\left(\frac{a}{p}\right)$ nin modülo $4a$ belirlendiğine dikkat edelim. $p \neq q$ farklı tek sayılar olduğunda, $x^2 \equiv p \pmod{q}$ ile $x^2 \equiv q \pmod{p}$ denliklerinin çözülebildikleri arasında bir ilişki vardır. Bu ilişki Karesel Karşılık (Kuadratik Reciprocity) olarak bilinir. Bu kural Legendre tarafından bulunmuş ve Gauss tarafından ispatlanmıştır.

Teorem 2.1.5:(Karesel Karşılık- Kuadratik Reciprocity) $p \neq q$ tek ve asal tam sayılar ise $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ dir.

Örnek 18: $x^2 \equiv 5 \pmod{41}$ denkliklerinin çözümü var mı? Yani $\left(\frac{5}{41}\right)$ Legendre Sembolünün değerini bulalım. $\left(\frac{5}{41}\right)\left(\frac{41}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{41-1}{2}} = +1$ ve $\left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1$ olduğundan, $\left(\frac{5}{41}\right) = +1$ bulunur. Şu halde verilen denkliğin çözümü vardır.

Örnek 19: $x^2 \equiv 35 \pmod{107}$ denkliklerinin çözümü var mı? Yani $\left(\frac{35}{107}\right) = \left(\frac{5}{107}\right)\left(\frac{7}{107}\right)$ Legendre Sembolünün değerini bulalım.

$\left(\frac{5}{107}\right)\left(\frac{107}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{107-1}{2}} = +1$ ve $\left(\frac{107}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{2}} = -1$, **(Örnek 16)** olduğundan, $\left(\frac{5}{107}\right) = -1$ ve $\left(\frac{7}{107}\right)\left(\frac{107}{7}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{107-1}{2}} = -1$ ve $\left(\frac{107}{7}\right) = \left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = +1$ $\left(107 \equiv 2 \pmod{7}\ ve\ Örnek\, 16\ den\right)$ olduğundan, $\left(\frac{7}{107}\right) = -1$ dir. Şu halde $\left(\frac{35}{107}\right) = \left(\frac{5}{107}\right)\left(\frac{7}{107}\right) = (-1)(-1) = +1$ bulunur.

Örnek 20: $p \neq q$ tek asal tam sayılar olsun.

$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right) \Leftrightarrow p \text{ veya } q \equiv 1 \pmod 4$ Karesel Karşılık Teoreminden,

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$'dir. $p \equiv 1 \pmod 4$ veya $q \equiv 1 \pmod 4$ ise $\frac{p-1}{2}$ ve $\frac{q-1}{2}$ çift olacağından $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=+1$ bulunur.

Tersine $p \not\equiv 1 \pmod 4$ ve $q \not\equiv 1 \pmod 4$ ise $\frac{p-1}{2}$ ve $\frac{q-1}{2}$ nin ikisi de tek olacağından, $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=-1$ bulunur.

$a \neq 0$, p tek asal tam sayı ve $p \nmid a$ ise $a=(-1)^d 2^e \prod_{i=1}^{r} q_i^{e_i}$, $d,e \geq 0$, $e_i \geq 1$ asal çarpanlara ayrılışını yazarak, $\left(\frac{a}{p}\right)$ Legendre Sembolünü kolaylıkla hesaplayabiliriz. Gerçekten; $\left(\frac{a}{p}\right)=\left(\frac{-1}{p}\right)^d\left(\frac{2}{p}\right)^e \prod_{i=1}^{r}\left(\frac{q_i}{p}\right)^{e_i}$ olur. Burada $p \nmid a$ kabul ettiğimizden $q_i \neq p$ dir. Yukarıdaki örneklerde olduğu gibi Karesel Karşılık kullanılarak, $\left(\frac{a}{p}\right)$ hesaplanır.

Örnek 21: $\left(\frac{354}{131}\right)=?$

Çözüm: $354=2\cdot 3\cdot 59$ olduğundan, $\left(\frac{354}{131}\right)=\left(\frac{2}{131}\right)\left(\frac{3}{131}\right)\left(\frac{59}{131}\right)$,

Örnek 16'den $131 \equiv 3 \pmod 8$ olduğundan, $\left(\frac{2}{131}\right)=-1$ dir.

$\left(\frac{3}{131}\right)=\left(\frac{131}{3}\right)\cdot(-1)^{\frac{3-1}{2}\cdot\frac{131-1}{2}}=-\left(\frac{131}{3}\right)=-\left(\frac{2}{3}\right)=-(-1)^{\frac{3^2-1}{8}}=+1$ dir.

$\left(\frac{59}{13}\right)\cdot(-1)^{\frac{13-1}{2}\cdot\frac{59-1}{2}}=\left(\frac{59}{13}\right)=\left(\frac{7}{13}\right)=\left(\frac{13}{7}\right)(-1)^{\frac{7-1}{2}\cdot\frac{13-1}{2}}=\left(\frac{13}{7}\right)=\left(\frac{6}{7}\right)=\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)$

ve $\left(\frac{2}{7}\right)=(-1)^{\frac{7^2-1}{2}}=+1$, $\left(\frac{3}{7}\right)=\left(\frac{7}{3}\right)(-1)^{\frac{7-1}{2}\cdot\frac{3-1}{2}}=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1$ olur. Şu halde, sonuç $\left(\frac{354}{131}\right)=(-1)(+1)(-1)=+1$ olarak bulunur.

Örnek 22: $p \neq q$ tek asal. tam sayılar olsun. $\left(\frac{q}{p}\right)$, sadece p 'nin modülo $4q$ sınıfına bağlıdır. Gerçekten $p' \equiv p \pmod{4q}$, yani $p' = p + 4qk$, $k \in Z$ olsa;

$$\left(\frac{q}{p'}\right) = \left(\frac{p'}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{p+4qk-1}{2}} = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}(-1)^{\frac{q-1}{2}\cdot 2qk} = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} = \left(\frac{q}{p}\right)$$

bulunur.

Şimdi Kare kalan problemini tersinden ele alalım. İlk olarak, -1 hangi $p \neq 2$ asal tam sayıları için kare kalan olur, inceleyelim.

$\left(\frac{-1}{p}\right) = +1 \Leftrightarrow p \equiv 1 \pmod{4}$ olduğunu görmüştük. Şu halde bu problemin cevabı $p \equiv 1 \pmod{4}$ olan asal tam sayılar olur. Yani p asal tam sayısı $\{1, 5, 9, ..., 4n+1, ...\}$ aritmetik dizisinin bir elemanı olmalıdır.

İkinci örnek olarak, 2 hangi $p \neq 2$ asal tam sayıları için kare kalan olur araştıralım. $\left(\frac{2}{p}\right) = +1 \Leftrightarrow p \equiv \pm 1 \pmod{8}$ olduğunu görmüştük. Şu halde cevap $p \equiv \pm 1 \pmod{8}$ olan asal tam sayılarıdır. Yani p asal tam sayısı; $\{1, 9, 17, ..., 8n+1, ...\}$ veya $\{7, 15, ..., 8n-1, ...\}$ aritmetik dizilerinin bir elemanı olmalıdır.

Üçüncü olarak, $q \neq 2$ asal tam sayısı hangi $p \neq 2$ asal tam sayıları için kare kalan olur araştıralım.

Eğer $q = 3$ veya $q = 5$ ise $\left(\frac{3}{11}\right) = \left(\frac{5}{11}\right) = 1$ olduğu gösterilebilir. Eğer $q > 5$ ise $p_0 \neq 2$ asal tam sayısını; $q-1$ in bir tek asal böleni olarak alalım. Eğer bu mümkün değil ise yani $q-1$, 2 nin bir kuvveti ise, o zaman $q-4$ ün bir tek asal böleni olarak alalım. Bu takdirde, $\left(\frac{q}{p_0}\right) = \left(\frac{1}{p_0}\right) = 1$ veya $\left(\frac{q}{p_0}\right) = \left(\frac{4}{p_0}\right) = 1$ olduğundan, q modülo p_0 kare kalan olacak şekilde en az bir p_0 asal tam sayısının varlığı gösterilmiş olur. Şu halde önceki örnekten de anlaşıldığı gibi; $\{p_0, p_0 + 4q, ..., p_0 + 4qk, ...\}$ aritmetik dizisinden

alınan her p asal tam sayısı için $\left(\frac{q}{p}\right)=+1$ olur.

Teorem 2.1.6:(Aritmetik Diziler için Dirichlet Teoremi)

$0<a\le k$ ve $(a,k)=1$ olmak üzere, her $\{a,a+k,a+2k,...,a+mk,...\}$ aritmetik dizisinde sonsuz asal sayı vardır. Böylece şu sonucu ifade edebiliriz.

Teorem 2.1.7: $q\neq 2$ asal tam sayı olmak üzere, –1, 2 veya q modülo p de kare kalan olacak şekilde sonsuz asal p tam sayısı vardır.

$p\neq q$ tek asal tam sayıları için $\left(\frac{q}{p}\right)$ yi daha açık şekilde ifade edelim.

Teorem 2.1.8: $p\neq q$ tek asal tam sayılar olsun.

$$\left(\frac{q}{p}\right)=+1\Leftrightarrow p\equiv \pm 1^2,\pm 3^2,...,(q-2)^2 \pmod{4q}$$

İspat: Eğer $p\equiv(2a+1)^2 \pmod{4q}$ ise $p\equiv 1 \pmod 4$ ve Karesel Karşılık Teoreminden $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=1$ olur. Eğer $p\equiv -(2a+1)^2 \pmod{4q}$ ise $p\equiv -1 \pmod 4$ ve

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

olur.

Tersine $\left(\frac{q}{p}\right)=1$ olsun. Karesel Karşılık ve Euler Kriterinden

$\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)$ her iki yanı $\left(\frac{p}{q}\right)$ ile çarparak; $1=\left(\frac{p(-1)^{\frac{p-1}{2}}}{q}\right)$

bulunur. Şu halde, $x^2\equiv p(-1)^{\frac{p-1}{2}} \pmod q$'nin bir çözümü var ve x veya $q-x$ den biri tektir. Genelliği bozmadan x in tek olduğunu kabul edebiliriz. Şu halde $x^2\equiv 1 \pmod 4$ olur.

Eğer $p \equiv 1 \pmod 4$ ise $(-1)^{\frac{p-1}{2}} = 1$ olduğundan, $x^2 \equiv p \pmod q$ dir. Diğer taraftan, $x^2 \equiv 1 \pmod 4$ ve $p \equiv 1 \pmod 4$ den $x^2 \equiv p \pmod 4$ bulunur. Şu halde önceki denklikle beraber $x^2 \equiv p \pmod{4q}$ elde edilir.

Eğer $p \equiv -1 \pmod 4$ ise $(-1)^{\frac{p-1}{2}} = -1$ olduğundan, $x^2 \equiv -p \pmod q$ dur. Diğer taraftan, $x^2 \equiv 1 \pmod 4$ ve $p \equiv -1 \pmod 4$ den $x^2 \equiv -p \pmod 4$ olur. Şu halde $x^2 \equiv -p \pmod{4q}$ elde edilir.

Örnek 23: $\left(\frac{3}{p}\right)$ yi önceki örneklerde hesaplamıştık. Şimdi yukarıdaki teoremi kullanarak hesaplayalım. $q = 3$ alırsak $4q = 12$ olur.

$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{12}$ bulunur. (Çünkü $q - 2 = 1$)

Örnek 24: $\left(\frac{5}{p}\right) = 1 \Leftrightarrow p = \pm 1 \; veya \; \pm 3^2 \pmod{20}$ olmalıdır. Bu da $p \equiv \pm 1 \pmod 5$ demektir.

Örnek 25: $\left(\frac{11}{p}\right) = 1 \Leftrightarrow p = \pm 1, \pm 3^2, \pm 5^2, \pm 7^2, \pm 9^2 \pmod{44}$ olmasıdır. Kareler mod 44 de hesaplanırsa p asal tam sayısı $p \equiv \pm 1, \pm 5, \pm 9, \pm 25, \pm 37 \pmod{44}$ olmalıdır.

Teorem 2.1.9: (Wilson Teoremi)

Herhangi bir p asal sayısı için $(p-1)! \equiv -1 \pmod p$ dir.

İspat: $p = 2$ için $1! \equiv -1 \pmod 2$ doğrudur. $p > 2$ olması durumunda $1 \le a \le p-1$ bağıntısını sağlayan her bir a sayısının a ile p aralarında asal olacağından modülo p ye göre tersi vardır. 1 ve $p-1$ sayılarının tersi de kendileridir. Böylece, $2 \cdot 3 \cdot ... \cdot (p-3) \cdot (p-2) \equiv 1 \pmod p$ (Çarpımdaki sayılar ikişerli olarak birbirleriyle eşleşip p modunda 1 olurlar.) olur. Son denkliğin

her iki tarafını 1 ve $p-1$ ile çarptığımızda,

$1\cdot 2\cdot 3\cdot ...\cdot (p-3)\cdot (p-2)\cdot (p-1)\equiv p-1(\text{mod } p)$ denkliği elde edilir. Bu da $(p-1)!\equiv -1(\text{mod } p)$ demektir.

Bu teoremin karşıtı da doğrudur. Şimdi bu teoremin karşıtını verelim.

Teorem 2.1.10: $(n-1)!\equiv -1(\text{mod } n)$ ise n asaldır.

İspat: Farzedelim n bileşik bir sayı olsun. Bu durumda, $n=a\cdot b$ için $1<a<n$ $1<b<n$ olacak şekilde a ve b sayıları vardır. $a<n$ olduğundan $a\mid (n-1)!$ dir. Çünkü a sayısı $1,2,3,...,n-1$ sayılarından biridir. $(n-1)!\equiv -1(\text{mod } n)$ olduğundan, $n\mid (n-1)!+1$ dir. $n\mid (n-1)!+1\cdot n$ ise $a\mid (n-1)!+1$ dir. $a\mid (n-1)!$ durumunun ikisi birden gerçekleşmesi $a=1$ demektir. Bu da $1<a<n$ durumu ile çelişir.

Teorem 2.1.11: Bir tam sayının tam kare olması için gerek ve yeter şart her p asal tam sayısı için modülo p kare kalan olmasıdır.

İspat: Eğer $a=b^2$, $b\in Z$ ise her p asal tam sayısı için $a\equiv b^2(\text{mod } p)$ olur. Tersine, a nın tam kare olmadığını kabul edelim. Şu halde ya $a<0$ ya da $p_i\,(i=1,2,...,r)$ ler farklı asal tam sayılar, $r\geq 1$ ve $i<r$ ise $p_i\neq 2$ olmak üzere $a=m^2p_1\cdots p_r$ şeklindedir.

1. hal:

$a>0$ olsun. $\left(\frac{a}{p}\right)=-1$ olacak şekilde bir p asal tam sayısının bulunduğunu gösterelim.

Önce q tek bir asal tam sayı ise $u\equiv 1(\text{mod } 4)$, $q\nmid u$ ve $\left(\frac{u}{q}\right)=-1$ olacak şekilde bir $u\in Z$ bulunduğunu gösterelim. **Teorem 2.1.8'**den u yu modülo $4q$; sayıları $\frac{q-1}{2}$ tane olan $1^2,3^2,...,(q-2)^2$ nin $(u\equiv 1(\text{mod } 4)$ *aldığımızdan pozitif kareler*$)$ pozitif en küçük temsilcileri q elemanlı $\{1,5,9,...,4q-3\}$ kümesinin elemanları dışında seçmeliyiz. Burada

tek sayıların karesinin, $\text{mod}\,\text{ülo}\,4$,1'in sınıfında olacağını hatırlatalım. Ayrıca $q \equiv 1 \pmod 4$ ise u olarak q yu , $q \equiv -1 \pmod 4$ ise $3q$ yu da alamayız. Şu halde q elemandan, $q - \frac{q-1}{2} - 1 = \frac{q-1}{2} \geq 1$, yani en az bir eleman kalacağı anlaşılır. p_r tek olduğundan, $q = p_r$ alabiliriz. Eğer $p_r = 2$ ise $u = 5$ alabiliriz.

Çin Kalan Teoremine göre;
$$\begin{aligned} x &\equiv 1 \pmod{p_1} \\ &\cdots\cdots\cdots\cdots \\ x &\equiv 1 \pmod{p_{r-1}} \\ x &\equiv u \pmod{4p_r} \end{aligned}$$

sağlayan bir $x \in Z$ bulunur. Dirichlet Teoreminden $p \equiv x \pmod{4p_1 \cdots p_r}$ olacak şekilde bir p asal tam sayısı da vardır. Bu takdirde

$$\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_r}{p}\right) = \left(\frac{p}{p_1}\right)(-1)^{\frac{p_1-1}{2}\cdot\frac{p-1}{2}} \cdots \left(\frac{p}{p_{r-1}}\right)(-1)^{\frac{p_{r-1}-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p_r}{p}\right) = -1$$

bulunur. Çünkü her $i = 1, 2, ..., r-1$ için, $p \equiv x \equiv 1 \pmod{p_i}$ ve $p \equiv x \equiv 1 \pmod 4$ dir. Ayrıca $p_r = 2$ olduğunda, $p \equiv 5 \pmod 8$ olduğundan, $\left(\frac{2}{p}\right) = -1$; p_r tek iken, $p \equiv u \pmod{p_r}$ olduğundan,

$$\left(\frac{p_r}{p}\right) = \left(\frac{p}{p_r}\right)(-1)^{\frac{p_r-1}{2}\cdot\frac{p-1}{2}} = \left(\frac{u}{p_r}\right) = -1 \text{ dir.}$$

2. hal:

$a < 0$ olsun. $a = -m^2$ ise p asal tam sayısının $p \equiv -1 \pmod 4$ $(\text{örneğin } p = 3)$ alırsak, $\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right) = -1$ olur.

Eğer $a = -m^2 p_1 \cdots p_r$, p_i ler farklı asal tam sayılar, $r \geq 1$ ise p asal tam sayısının $p \equiv 1 \pmod 4$ olacak şekilde alırsak, 1. halden;

$$\left(\frac{-a}{p}\right) = -1 \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-a}{p}\right) = -1 \text{ bulunur.}$$

Şimdiye kadar, $x^2 \equiv a \pmod n$ denkliğinin çözümünün olup olmadığını araştırdık. Fakat çözümü olması halinde çözümleri nasıl bulacağız? Yukarıdaki yöntemler çözümü bulmamıza yaramıyor. Modül büyüdükçe bu iş daha da

zorlaşır. Bununla birlikte $p \equiv 3 \pmod 4$ veya $p \equiv 5 \pmod 8$ olduğunda, $x^2 \equiv a \pmod p$'nin çözümlerini bulmak için bir yöntem verelim.

i. $p \equiv 3 \pmod 4$ asal tam sayı ve $x^2 \equiv a \pmod p$ nin bir çözümü mevcut olsun. Yani $\left(\frac{a}{p}\right) = 1$ ve $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) = 1 \pmod p$ olsun.

Bu taktirde $a^{\frac{p-1}{2}} \equiv 1 \pmod p \Rightarrow a^{\frac{p+1}{2}} \equiv \left(a^{\frac{p+1}{4}}\right)^2 \equiv a \pmod p$

olduğundan, $x = a^{\frac{p+1}{4}}$ verilen denkliğinin bir çözümüdür.

ii. $p \equiv 5 \pmod 8$ asal tam sayı ve $x^2 \equiv a \pmod p$ nin bir çözümü mevcut olsun. Önce Wilson Teoremini kullanarak, $x^2 \equiv -1 \pmod p$'nin bir çözümünü bulalım:

$$-1 \equiv (\mathrm{p}-1)! \equiv 1 \cdot 2 \cdots \frac{p-1}{2}\left(p - \frac{p-1}{2}\right) \cdots (p-1)(p-2) \pmod p$$

$$\equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \equiv \left(\frac{p-1}{2}!\right)^2 \pmod p$$ olduğundan, $x = \frac{p-1}{2}!$ bir çözümdür. Şimdi $\left(\frac{a}{p}\right) = 1$ alalım. Euler Kriterinden,

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) = 1 \pmod p$ olduğundan, $a^{\frac{p-1}{4}} \equiv 1 \pmod p$ veya

$a^{\frac{p-1}{4}} \equiv -1 \pmod p$ olur. Birincisinden, $a^{\frac{p+3}{4}} \equiv \left(a^{\frac{p+3}{8}}\right)^2 \equiv a \pmod p$ ve

ikincisinden, $a^{\frac{p+3}{4}} \equiv \left(a^{\frac{p+3}{8}}\right)^2 \equiv -a \pmod p$ yani

$\left[a^{\frac{p+3}{8}}\left(\frac{p-1}{2}\right)!\right]^2 \equiv a \pmod p$ bulunur.

Şu halde çözümler, $x = \pm a^{\frac{p+3}{8}}$ veya $x = \pm a^{\frac{p+3}{8}} . \left(\frac{p-1}{2}\right)!$ olarak bulunur.

3 MATEMATİK OLİMPİYATLARI SORULARI VE ÇÖZÜMLERİ

Bir sayının karesinin değişik modüllerde alabileceği değerler aşağıdaki gibidir.

$a = x^2 = 0,1,4,5,6,9 \pmod{10}$

$x^2 = 0,1 \pmod 3$

$x^2 = 0,1 \pmod 4$

$x^2 = 0,1,4 \pmod 5$

$x^2 = 0,1,2,4 \pmod 7$

$x^2 = 0,1,4 \pmod 8$

$x^2 = 0,1,4,7 \pmod 9$

Bunun dışında bir sayının tam kare olmadığını göstermek için tam karelerin aşağıdaki özellikleri kullanılır.

$p \mid x^2 \Rightarrow p \mid x \Rightarrow p^2 \mid x^2$

$n^2 < a < (n+1)^2 \Rightarrow a \neq x^2$

$a.b = x^2$, $(a,b) = 1$ ve $a = y^2$, $b = z^2$ (Alizade, 2013)

3.1. ÖRNEKLER

1) Bir 1000 basamaklı sayıda bir tanesi dışında tüm basamaklar 5'tir. Bu sayının hiçbir tam sayının karesi olamayacağını kanıtlayınız?

Çözüm:

- 55x...55

şeklinde olamaz 5 ile bitiyorsa 25 ile bitmek zorunda.

- $555...x5 \equiv 5 \pmod 8$

şeklinde olamaz mod 8 de kare kalanlar 0,1 ve 4 tür.

- $555...5\,\mathrm{x}$, $\mathrm{x} = \not{0}, 1, 4, \not{5}, 6, 9$

$555...51 \equiv 3 \pmod 4$ olamaz mod 4' te kare kalanlar 0 ve1' dir.

$555...59 \equiv 3 \pmod 4$ olamaz mod 4' te kare kalanlar 0 ve1' dir.

$555...54 \equiv 2 \pmod 4$ olamaz mod 4' te kare kalanlar 0 ve1' dir.

$555...56 \equiv 2 \pmod 4$ burada $3 \mid 555...56$, $9 \nmid 555...56$

2) $n > 1$ olmak üzere, $p = p_1 \cdot p_2 \cdot p_3 \cdots p_n$ ilk n asal sayının çarpımı olsun. $p-1$ ve $p+1$ sayılarının hiçbirinin tam kare olmadığını gösteriniz?

Çözüm:

- $p = p_1 \cdot p_2 \cdot p_3 \cdots p_n \equiv 0 \pmod 3$ $(p_1 = 2, p_2 = 3, p_3 = 5)$

$p-1 \equiv 2 \pmod 3 \Rightarrow p-1 \neq x^2$

- $p = p_1 \cdot p_2 \cdot p_3 \cdots p_n \equiv 2 \pmod 4$ $(p_1 = 2, p_2 = 3, p_3 = 5)$

$p+1 \equiv 3 \pmod 4 \Rightarrow p+1 \neq x^2$

3) $n > 11$ tam sayıları için $n^2 - 19n + 89$ sayısının tam kare olmadığını gösteriniz? (Alizade, 2013)

Çözüm:

$n^2 - 19n + 89 = x^2$

$4n^2 - 76n + 356 = 4x^2$

$(2n-19)^2 - (2x)^2 = 5$

$(2n-19-2x)(2n-19+2x) = 5$

- $\left.\begin{matrix} 2n-19-2x=1 \\ 2n-19+2x=5 \end{matrix}\right\} \Rightarrow 4n = 44 \Rightarrow n = 11$
- $\left.\begin{matrix} 2n-19-2x=-1 \\ 2n-19+2x=-5 \end{matrix}\right\} \Rightarrow 4n = 32 \Rightarrow n = 8$
- $\left.\begin{matrix} 2n-19-2x=5 \\ 2n-19+2x=1 \end{matrix}\right\} \Rightarrow 4n = 44 \Rightarrow n = 11$
- $\left.\begin{matrix} 2n-19-2x=-5 \\ 2n-19+2x=-1 \end{matrix}\right\} \Rightarrow 4n = 32 \Rightarrow n = 8$

4) n tam sayı olmak üzere, $49n+14$ şeklinde yazılabilen bir sayı bir tam sayının karesi olabilir mi?

Çözüm:

$$7 \mid 49n+14 = 7(7n+2)$$

$$7^2 \nmid 49n+14$$

oluğundan bir tam sayının karesi olamaz.

5) $3n^2+3n+7$ sayısının tam küp olmasını sağlayan kaç n pozitif tamsayı vardır?

Çözüm:

$$a^3 \equiv \mp 0,1 \pmod 7$$

$$a^3 \equiv \mp 0,1 \pmod 9$$

$$A = 3n^2+3n+7$$

$$n = 3k \Rightarrow 27k^2+9k+7 \equiv 7 \pmod 9$$

$$n = 3k+1 \Rightarrow 27k^2+18k+3+9k+3+7 = 27k^2+27k+13 \equiv 4 \pmod 9$$

$$n = 3k-1 \Rightarrow 27k^2-18k+3+9k-3+7 = 27k^2-9k+7 \equiv 7 \pmod 9$$

7, 4, 7 mod 9'a göre tam küp olamaz.

$$x^3 \not\equiv 4,7 \pmod 9$$

6) $5p\left(2^{p+1}-1\right)$ sayısını tam kare yapan kaç p asal sayısı vardır?

Çözüm:

$$p \mid 5p\left(2^{p+1}-1\right) \Rightarrow p^2 \mid 5p\left(2^{p+1}-1\right)$$

$$p = 5 \Rightarrow 5 \cdot 5\left(2^{5+1}-1\right) = 25 \cdot 63 \neq x^2$$

$$p \neq 5 \Rightarrow p \mid \left(2^{p+1}-1\right) \Rightarrow 2^{p+1} \equiv 1 \pmod p \quad \left(2^{p-1} \equiv 1 \pmod p \; Fermat\, teoremi\right)$$

$$1 \equiv 2^{p+1} \equiv 2^{p-1} \cdot 2^2 \equiv 4 \pmod p$$

$$p = 3 \Rightarrow 5 \cdot 3\left(2^4-1\right) = 15^2$$

7) 2^n+65 sayısının, bir tam sayının karesine eşit olmasını sağlayan en büyük n tam sayısı kaçtır?

Çözüm:

$2^n + 65 \equiv 1,4 \pmod 5 \Rightarrow n = 2k$ olmalı.

$2^{2k} + 65 = x^2 \Rightarrow \left(x - 2^k\right)\left(x + 2^k\right) = 65$

$$\left.\begin{matrix}\left(x - 2^k\right) = 1 \\ \left(x + 2^k\right) = 65\end{matrix}\right\} \Rightarrow x = 33, k = 5 \; ve \; n = 10$$

$$\left.\begin{matrix}\left(x - 2^k\right) = 5 \\ \left(x + 2^k\right) = 13\end{matrix}\right\} \Rightarrow x = 9, k = 2 \; ve \; n = 4$$

8) $2n+1 \, ve \, 3n+1$ sayıları tam kare ise, $5n+3$ sayısının asal olmayacağını gösteriniz? (n pozitif tam sayıdır)

Çözüm:

$2n+1 = a^2 \; ; 3n+1 = b^2 \Rightarrow 5n+3$ asal değil

$5n+3 = 4\left(2n+1\right) - \left(3n+1\right) = 4a^2 - b^2 = \left(2a-b\right)\left(2a+b\right)$

$5n+3$ ün asal olduğunu varsayarsak

$2a - b = 1, \; 2a + b = 5n + 3$

$2a + b = 5n + 3 = a^2 + b^2 + 1$

$\left(a-1\right)^2 = b - b^2 \le 0 \Rightarrow a = 1 \, ve \, n = 0$

9) $\dfrac{2^{p-1}-1}{p}$ sayısının tam kare olmasını sağlayan kaç p asal sayısı vardır?

Çözüm:

$$\frac{2^{p-1}-1}{p} = a^2, \; \left.\begin{matrix}a^2 = n.m \\ \left(n,m\right) = 1\end{matrix}\right\} \Rightarrow n = b^2, \; m = c^2$$

$$p \neq 2 \Rightarrow p - 1 = 2m \; , \; \frac{\left(2^m - 1\right)\left(2^m + 1\right)}{p} = a^2$$

a) $\dfrac{2^m - 1}{p} = b^2, \; 2^m + 1 = c^2 \Rightarrow \left(c-1\right)\left(c+1\right) = 2^m \Rightarrow c = 3 \Rightarrow m = 3, \; p = 7$

sağlar.

b) $2^m - 1 = b^2 \; ; \dfrac{2^m + 1}{p} = c^2$

$m \geq 2$ *ise* $2^m - 1 \equiv 3 \pmod 4 \Rightarrow 2^m - 1 \neq b^2$

$m = 1$ *alalım* $\Rightarrow p = 3 \Rightarrow \dfrac{2^2 - 1}{3} = 1^2$, $p = 3$ *sağlar.*

10) a *ve* b tam sayıları için $a^2 + b^2$ sayısı 7'ye bölünüyorsa, a *ve* b sayılarının her ikisinin7'ye bölündüğünü kanıtlayınız?

Çözüm:

$x^2 \in \{0,1,2,4\} \pmod 7$

$a^2 + b^2 \equiv 0 \pmod 7 \Rightarrow a^2 \equiv b^2 \equiv 0 \pmod 7 \Rightarrow 7 \mid a$ *ve* $7 \mid b$

0 0

1 1

2 2

4 4

11) Aşağıdaki n tam sayılarından hangisi için $x^2 \equiv -1 \pmod n$ denkliğini sağlayan en az bir x tam sayısı vardır?

a) 97 **b)** 98 **c)** 99 **d)** 100 **e)** Hiçbiri

Çözüm:

$x^2 \equiv -1 \pmod n$ (p asal) denkleminin çözümü tam olarak $p \equiv 1 \pmod 4$ durumunda vardır.

$$\left.\begin{array}{l} x^4 \equiv 1 \pmod p \\ x^{p-1} \equiv 1 \pmod p \end{array}\right\} \Rightarrow (p-1,4) = \begin{cases} 1 \\ 2 \\ 4 \end{cases}$$

$x^{(p-1,4)} \equiv 1 \pmod p$, $x^2 \equiv 1 \pmod p$, $4 \mid p-1$

$d = 4u + (p-1)v \Rightarrow x^d = \left(x^4\right)^u \cdot \left(x^{p-1}\right)^v \equiv 1, \left[\left(x^4\right)^u \equiv 1, \left(x^{p-1}\right)^v \equiv 1\right]$

$x = 97$ sağlar.

$x^2 \equiv -1 \pmod{98} \Rightarrow x^2 \equiv -1 \pmod 7 \equiv 3 \pmod 4$ çelişki

$x^2 \equiv -1 \pmod{99} \Rightarrow x^2 \equiv -1 \pmod{11} \equiv 3 \pmod 4$ çelişki

$x^2 \equiv -1 \pmod{100} \Rightarrow x^2 \equiv -1 \pmod 4$ çelişki

12) Üç tam sayının karelerinin 8'e bölünmesinden elde edilen kalanın 7 olmayacağını kanıtlayınız?

Çözüm:

x	x^2	
0	0	$(\mathrm{mod}\,8)$
1	1	$(\mathrm{mod}\,8)$
2	4	$(\mathrm{mod}\,8)$
3	1	$(\mathrm{mod}\,8)$
4	0	$(\mathrm{mod}\,8)$
5	1	$(\mathrm{mod}\,8)$
6	4	$(\mathrm{mod}\,8)$
7	1	$(\mathrm{mod}\,8)$

$x^2 \in \{0,1,4(\mathrm{mod}\,8)\}$

$x^2 + y^2 + z^2 \in \{0,1,2,3,4,5,6\}$

13) Asal çarpanlarına ayrıldığında tüm asal çarpanlarının kuvvetleri tek sayı olan pozitif tam sayıların oluşturduğu küme, en çok kaç ardışık tam sayı içerir?

Çözüm:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	1		2		1		3		1		2		1		4		1		2

$a^2 = 2^2 \ldots$

21, 22, 23, 24, 25

29, 30, 31, 32, 33, 34, 35

en fazla 7 tane olur.

14) Dört basamaklı $aabb$ sayısı bir tam karedir. Bu sayıyı bulunuz?

Çözüm:

$aabb = x^2 \Rightarrow 1100a + 11b = x^2 \Rightarrow 11(100a + b) = x^2$

$100a + b \equiv a + b \equiv 0(\mathrm{mod}\,11)$

$a + b = 11$

$\downarrow \quad \downarrow$

$2 \quad 9 \quad \rightarrow \quad 2299 \equiv 3 \pmod 4$ *tam kare olamaz*

$3 \quad 8 \quad \rightarrow \quad 3388 \equiv 3 \pmod 5$ *tam kare olamaz*

$4 \quad 7 \quad \rightarrow \quad 4477 \equiv 2 \pmod 5$ *tam kare olamaz*

$5 \quad 6 \quad \rightarrow \quad 5566 \equiv 2 \pmod 4$ *tam kare olamaz*

$6 \quad 5 \quad \rightarrow \quad 6655 \equiv 3 \pmod 4$ *tam kare olamaz*

$7 \quad 4 \quad \rightarrow \quad 7744$

$8 \quad 3 \quad \rightarrow \quad 8833 \equiv 3 \pmod 5$ *tam kare olamaz*

$9 \quad 2 \quad \rightarrow \quad 9922 \equiv 2 \pmod 4$ *tam kare olamaz*

$7744 = 11^2.8^2 = 88^2 \qquad (a = 7 \; ve \; b = 4 \; olur)$

15) Bir tam sayının karesinin basamakları toplamı 2003 olabilir mi?

Çözüm:

A rakamlar toplamı $2003 \Rightarrow A = 3k + 2$

$A \equiv 2 \pmod 3 \Rightarrow A$ tam kare olamaz.

16) Bir tam sayının karesinin basamakları toplamı 2004 olabilir mi?

Çözüm:

A rakamlar toplamı $2004 \Rightarrow A = 3k$

$A \equiv 0 \pmod 3$

$A \equiv 6 \pmod 9 \Rightarrow A$ tam kare olamaz.

17) Beş ardışık pozitif tam sayının kareleri toplamının tam kare olmayacağını gösteriniz?

Çözüm:

$a = (n-2)^2 + (n-1)^2 + (n)^2 + (n+1)^2 + (n+2)^2 = 5n^2 + 10 = 5(n^2 + 2)$

$a = x^2 \Rightarrow n^2 + 2 \equiv 0 \pmod 5$

$n^2 \equiv 3 \pmod 5$ çelişki a tam kare olamaz.

18) $x^2 + (x+1)^2 + (x+2)^2 = y^2$ denkleminin x, y tam sayı olacak şekilde kaç tane (x, y) çözüm takımı vardır?

Çözüm:

$3x^2+6x+5=y^2$

$y^2=2\pmod 3$ olduğundan çelişki vardır çözüm yoktur.

19) Pozitif tam bölenlerinin sayısı tek sayı olan her pozitif tam sayının bir tam sayının karesine eşit olduğunu gösteriniz?

Çözüm:

$=p_1^{k_1}\cdots p_m^{k_m}$

$(k_1+1)\cdots(k_m+1)$ tek

$k_1+1,...,k_m+1$ tek

$k_1,...,k_m$ çift

$n=\left(p_1^{\frac{k_1}{2}}\cdots p_m^{\frac{k_m}{2}}\right)^2$ olduğundan tam karedir.

20) İki tek sayının kareleri toplamı bir tam sayının karesine eşit olabilir mi?

Çözüm:

$2m+1+2k+1\equiv 2\pmod 4$ çelişki olamaz.

21) *aaabbb* şeklindeki bir altı basamaklı sayı tam kare olabilir mi?

Çözüm:

$x^2=aaabbb=111000\cdot a+111\cdot b=111(1000a+b)$

$x^2=3\cdot 37(1000a+b)$

$a+b=111k$ olamaz?

22) x *ve* y tam sayılar olmak üzere x^2+y^2 toplamı 3'e bölünüyorsa ve $100<x,y<200$ ise (x,y) ikilisi kaç değişik değer alabilir?

Çözüm:

$x^2+y^2\equiv 0\pmod 3\Rightarrow x^2\equiv y^2\equiv 0\pmod 3\Rightarrow 3\mid x\,,\,3\mid y$

$100<x,y<200\Rightarrow x,y\in\{102,105,108,...,198\}$

x *ve* y 33 değer alabilir bu yüzden (x, y) çözümlerinin sayısı $33 \cdot 33 = 1089$ dur.

23) Tam sayı katsayılı ikinci dereceden bir polinomun diskriminantı 23, 24, 25, 28, 33 sayılarından hangisine eşit olamaz?

Çözüm:

$\Delta = b^2 - 4ac \equiv b^2 \pmod 4$

$23 \equiv 3 \pmod 4$ olduğundan $\Delta \neq 23$

24) $\sqrt{17p + 625}$ sayısının bir tam sayı olmasını sağlayan en büyük p asal sayısı nedir?

Çözüm:

$x^2 = 17p + 625 \Rightarrow 17p = x^2 - 625 \Rightarrow 17p = (x-25)(x+25)$

$17p$	$=$	$(x-25)$	$\cdot$	$(x+25)$		
		1		$17p$	$\Rightarrow$	$p = 3$
		p		17	$\Rightarrow$	$x < 0$ *olamaz*
		17		p	$\Rightarrow$	$x = 42$ $p = 67$

25) $2p^4 - 7p^2 + 1$ sayısının bir tam sayı olmasını sağlayan en büyük p asal sayısı nedir?

Çözüm:

- $p = 3$ *ise* $2p^4 - 7p^2 + 1 = 100 = 10^2$
- $p \neq 3$ *ise* $p^2 \equiv 1 \pmod 3$

  $2p^4 - 7p^2 + 1 \equiv 2 \cdot 1 - 7 \cdot 1 + 1 \equiv 2 \pmod 3$

  $2p^4 - 7p^2 + 1$

tam kare olamaz $p \neq 3$ için.

26) $p > 5$ bir asal sayı ise $p^2 \equiv 1 \pmod{30}$ veya $p^2 \equiv 19 \pmod{30}$ olduğunu gösteriniz?

Çözüm:

- $\left.\begin{array}{l} p^2 \equiv 1 \pmod 2 \\ p^2 \equiv 1 \pmod 3 \end{array}\right\} \Rightarrow p^2 \equiv 1 \pmod 6$

  $p^2 \equiv 1 \pmod 5 \Rightarrow p^2 \equiv 1 \pmod{30}$

- $p^2 \equiv 4 \pmod 5$

  $\left.\begin{array}{l} p^2 \equiv 1 \pmod 6 \\ p^2 \equiv 4 \pmod 5 \end{array}\right\} \Rightarrow \begin{array}{l} 1,7,13,19 \\ 4,9,14,19 \end{array} \Rightarrow p^2 \equiv 19 \pmod{30}$

27) $x^3 - 13y^3 = 1453$ eşitliğini sağlayan (x, y) tam sayı sıralı ikililerinin sayısı kaçtır?

Çözüm:

$x^3 - 13y^3 = 1453 \qquad a^3 \in \{0,1,6 \pmod 7\}$

x^3	+	y^3	≡	4 $\pmod 7$
0		0		
1		1		
6		6		

Buradaki kombinasyonların hiçbiri 4'ü vermez. Bu nedenle çözüm yoktur.

28) $39p + 1$ sayısını tam kare yapan kaç p asal sayısı vardır?

Çözüm:

$x^2 = 39p + 1 \Rightarrow 39p = x^2 - 1 \Rightarrow 39p = (x-1)(x+1)$

$(x-1)$	·	$(x+1)$	=	$3 \cdot 13 \cdot p$
3		$13p$		*olamaz*
13		$3p$		$p = 5$
$3p$		13		*olamaz*
1		$3 \cdot 13 \cdot p$		*olamaz*
39		p		$p = 41$
p		39		$p = 37$

$p = 5,\ p = 37\ ve\ p = 41$ sağlar.

29) İki basamaklı bir sayının bunun ters yazılımı ile toplamı bir tam sayının karesine eşittir. Bu özelliğe sahip olan tüm iki basamaklı sayıları bulunuz?

Çözüm:

$ab+ba=11(a+b)$

a	+	b	=	11
↓		↓		
2		9		
3		8		
4		7		
5		6		
6		5		
7		4		
8		3		
9		2		

Bu şekilde 8 tane iki basamaklı sayı vardır.

30) m'nin aşağıdaki değerlerinden hangisi için $3x^2+4y^2+5z^2=m$ eşitliğini sağlayan (x,y,z) üçlüsü yoktur?

a) 2007 **b)** 20008 **c)** 2009 **d)** 2010 **e)** 2011

Çözüm:

m	=	$3x^2$	+	$5z^2$	≡	$0,1,3(\mathrm{mod}\,4) \Rightarrow m \not\equiv 2(\mathrm{mod}\,4)$
		↓		↓		
		0		0		
		1		1		

2 kalanını vermemesi gerekir. Bu sebeple 2010 olamaz.

31) Bir dizi $a_1=1$ ve $\forall n\geq 1$ için $a_{n+1}=a_1^{\,2}+a_2^{\,2}+a_3^{\,2}+...+a_n^{\,2}+n$ ile tanımlanıyor bu dizinin kaç terimi tam karedir?

Çözüm:

$a_{n+1}=a_1^{\,2}+a_2^{\,2}+a_3^{\,2}+...+a_n^{\,2}+n$

$n\to n-1,\ a_n=a_1^{\,2}+a_2^{\,2}+a_3^{\,2}+...+a_{n-1}^{\,2}+n$

$a_n^{\,2}<a_{n+1}=a_1^{\,2}+a_2^{\,2}+a_3^{\,2}+...+a_n^{\,2}+n<(a_n+1)^2$ eşitsizliğinin doğruluğunu inceleyelim

$$= a_n{}^2 + a_1{}^2 + a_2{}^2 + a_3{}^2 + ... + a_{n-1}{}^2 + n$$

$$= a_n{}^2 + a_n + 1$$

$$< a_n{}^2 + 2a_n + 1 = (a_n + 1)^2$$

$\forall n \geq 1$ için

$a_1{}^2 < a_2 < (a_1 + 1)^2$

$a_2{}^2 < a_3 < (a_2 + 1)^2$

$a_2, a_3, ...$ tam kare olamazlar ise $a_1 = 1$ sadece 1 tam kare var.

32) $7 \cdot 2^n + 1$sayısının tam kare olmasını sağlayan kaç n pozitif tam sayısı vardır?

Çözüm:

$7 \cdot 2^n + 1 = m^2 \Rightarrow 7 \cdot 2^n = (m-1) \cdot (m+1)$

I. $\left.\begin{matrix} m-1 = 2^k \\ m+1 = 7 \cdot 2^l \end{matrix}\right\} \Rightarrow 2 = 7 \cdot 2^l - 2^k \Rightarrow 2 + 2^k = 7 \cdot 2^l$

- $l \geq 2$, $k > l \Rightarrow 2 \equiv 0 (\mathrm{mod}\, 4)$ olamaz.
- $l = 0 \Rightarrow 2 + 2^k = 7$ olamaz.
- $l = 1 \Rightarrow 2 + 2^k = 14$ olamaz.

II. $\left.\begin{matrix} m-1 = 7 \cdot 2^k \\ m+1 = 2^l \end{matrix}\right\} \Rightarrow 2 = 2^l - 7 \cdot 2^k \Rightarrow 7 \cdot 2^k + 2 = 2^l$

- $k \geq 2 \Rightarrow l > k \Rightarrow 2 \equiv 0 (\mathrm{mod}\, 4)$ olamaz.
- $k = 0 \Rightarrow 7 + 2 = 2^l$ olamaz.
- $k = 1 \Rightarrow 16 = 2^l \Rightarrow l = 4$ buradan $k = 1, l = 4, \mathrm{m} = 15, \mathrm{n} = 5$

33) $5^p + 4p^4$ sayısını tam kare yapan tüm p asal sayılarını bulunuz?

Çözüm:

- $p = 5 \Rightarrow 5^5 + 4 \cdot 5^4 = 5^4 (5 + 4) = 5^4 \cdot 3^2$ tam karedir
- $p \neq 5 \Rightarrow 5^p + 4 \cdot \mathrm{p}^4 = a^2 \Rightarrow 5^p = a^2 - 4 \cdot \mathrm{p}^4 \Rightarrow 5^p = (a - 2p^2)(a + 2p^2)$

$$\left.\begin{aligned} a-2p^2 &= 5^k \\ a+2p^2 &= 5^{p-k} \end{aligned}\right\} \Rightarrow 4p^2 = 5^{p-k} - 5^k \quad ,$$

- $k \neq 0$ ise mod 5'te $0 \equiv 5-1 \pmod{p} \Rightarrow 0 \equiv 4 \pmod{p} \Rightarrow p = 2$ çelişki.
- $k = 0$ ise $4p^2 = 5^p - 1$ mod p 'de

  $0 \equiv 5-1 \pmod{p} \Rightarrow 0 \equiv 4 \pmod{p} \Rightarrow p = 2$ dir.

  $5^2 + 4 \cdot 2^4 = 25 + 64 = 89$

34) p asal sayısı için $n(n+p)$ hangi n değerleri için tam karedir?

Çözüm:

$$\left.\begin{aligned} d \mid n \\ d \mid n+p \end{aligned}\right\} \Rightarrow d \mid p \text{ ise } d = 1 \text{ veya } d = p$$

- $d = p$ ise $n = pk$

$pk(pk+p) = m^2 \Rightarrow pk \cdot p(k+1) = m^2 \Rightarrow p^2 \cdot k(k+1) = m^2$ olamaz çünkü ardışık iki sayı tam kare değildir.

- $d = 1$ ise $n = m^2, n+p = s^2 \Rightarrow p = s^2 - m^2 \Rightarrow p = (s-m)(s+m)$

$$\left.\begin{aligned} s+m &= p \\ s-m &= 1 \end{aligned}\right\} \Rightarrow 2s = p+1 \text{ ise } p \text{ tek olmalıdır.}$$

$s = \frac{p+1}{2}$ *ve* $m = \frac{p-1}{2}$ bir tane değer alabilir.

35) $(2p)^n + 1$ sayısını tam küp yapan pozitif tam n ve asal $p \geq 5$ sayılarını bulunuz.

Çözüm:

$(2p)^n + 1 = a^3$ olsun. $(2p)^n = a^3 - 1 = (a-1)(a^2+a+1)$, a^2+a+1 tek sayıdır.

($2^n \| a-1$ ifadesinin anlamı $\frac{a-1}{2^n}$ tam sayıdır ama $\frac{a-1}{2^{n+1}}$ tam sayı değildir.)

$a-1 = 2^n p^k \Rightarrow a = 2^n p^k + 1 \quad (k \geq 0)$

$(2p)^n = (a-1)\left[(a-1)^2 + 3(a-1) + 3\right]$

$2^n p^n = 2^n p^k \left[2^{2n} p^{2k} + 3.2^n p^k + 3 \right]$ $(k < n)$ olmalıdır.

1.durum: $k > 0$ ise $p \mid 3$ olmalıdır ise çelişki elde edilir.

2.durum: $k = 0$ olduğunda

$p^n = 4^n + 3 \cdot 2^n + 3$

$n = 1 için\ p = 13$

$n = 2\ için\ p^2 = 16 + 12 + 3 = 31$ olamaz

$n = 3 için\ p^3 = 64 + 24 + 3 = 91$ olamaz

$n > 3 için\ p^n = 4^n + 3.2^n + 3 < 5^n \Rightarrow p < 5$ olur.

$n = 1 için\ p = 13$ olur buda tek çözümdür.

36) (a_n) pozitif tam sayılar dizisinde $a_{n+1} = a_n{}^3 + 1999$ dur. Bu dizinin terimleri arasında en fazla kaç tane tam kare olabilir?

Çözüm:

$\mod 7$ de tam küpler $\{-1, 0, 1\}$ dir.

$1999 \equiv 4 (\mod 7)$

$a_{n+1} = a_n{}^3 + 1999 \equiv \{-1, 0, 1\} + 4 = \{3, 4, 5\}$

$a_{n+1} = m^2 \in \{0, 1, 2, 4\}$

$a_n \equiv 0 (\mod 7)$

$a_{n+1} \equiv 4 (\mod 7)$

$a_{n+2} \equiv (a_{n+1})^3 + 4 \equiv 5 (\mod 7)$

$a_{n+3} \equiv (a_{n+2})^3 + 4 \equiv 5^3 + 4 \equiv (-2)^3 + 4 \equiv 3 (\mod 7)$

$a_{n+4} \equiv (a_{n+3})^3 + 4 \equiv 3^3 + 4 \equiv 3 (\mod 7)$

şu ana kadar sadece iki çözüm olabilir.

$a_n = x^2$, $a_{n+1} = y^2$ olsun.

$y^2 = (x^2)^3 + 1999 = x^6 + 1999$

$(y - x^3)(y + x^3) = 1999$

$$\left.\begin{array}{l} y-x^3=1999 \\ y+x^3=1 \end{array}\right\} \Rightarrow y=1000\,,\ x^3=999$$

$y=1000 \Rightarrow$ iki tane tam kare olamaz. İlk terimi tam kare seçersek bir tane olur.

37) 6^n+2^m+2 sayısını tam kare yapan n,m pozitif tam sayılarını bulunuz?

Çözüm:

- $n,m\geq 2$ ise $6^n+2^m+2\equiv 2\pmod 4$ olduğundan tam kare değil.
- $n=1 ve\, m=1$ ise $6+2+2=10$ tam kare olamaz.
- m ve n den bir tanesi 1 diğeri ≥ 2 olsun.

1.durum:

$n=1$ olsun $2^m+8=t^2$

- $m=2$ ise $2^2+8=t^2$ olamaz.
- $m\geq 3$ ise $2^3\left(2^{m-3}+1\right)=t^2$ eşitliğinde $2^{m-3}+1$ çift olmalıdır. $m=3$ sağlar. $n=1$, $m=3$ çözüm olur.

2.durum:

$m=1$ olsun $6^n+4=t^2$ ise $(-1)^n+4=t^2\pmod 7 \Rightarrow 3\, veya\, 5=t^2\pmod 7$

$\bmod 7$ de tam kareler 0,1,2 ve 4 olduğundan çözüm kümesi boş kümedir.

sadece $n=1$, $m=3$ çözüm olur.

38) $n(n+173)$ sayısı tam kare olacak şekilde kaç n tane pozitif tam sayısı vardır?

Çözüm:

$n(n+173)=a^2$

$(n,n+173)=(n,173)=1\vee 173$

- $(n,173)=1\Rightarrow \left.\begin{array}{l} n=x^2 \\ n+173=y^2 \end{array}\right\} \Rightarrow y^2-x^2=173$

$(y-x)(y+x)=173\Rightarrow y=87\,,\ x=86$

- $(n,173)=173\Rightarrow n=173k\Rightarrow 173k.(173k+173)$

$173k(173k+173)=173^2k(k+1)=a^2$

$k=0 \Rightarrow n=0$ çözüm yoktur.

39) n bir tam sayı olmak üzere, $p^2=n^3+1$ eşitliğini sağlayan kaç tane p asal sayısı vardır?

a) 1 **b)** 2 **c)** 3 **d)** 4 **e)** Hiçbiri

Çözüm:

$$n^3+1=\underset{\downarrow}{(n+1)}\cdot\underset{\downarrow}{\left(n^2-n+1\right)}=p^2$$

1	p^2	$\Rightarrow$	$n=0$ *p asal değil.*
p	p	$\Rightarrow$	$n+1=n^2-n+1 \Rightarrow n=2 \Rightarrow p=3$
p^2	1	$\Rightarrow$	$n^2-n=0$, $n=0$, $n=1$

40) $p+q=(p-q)^3$ eşitliğini sağlayan tüm p,q asal sayılarını bulunuz?

Çözüm1:

$p+q=p^3-3p^2q+3pq^2-q^3$

$\mathrm{mod}\,3$'de $p+q=p-q$

$p+q=p-q$

$p+q=p-q \Rightarrow 2q=0 \Rightarrow q\equiv 0(\mathrm{mod}\,3) \Rightarrow q=3$

$p+q=(p-q)^3 \Rightarrow p+3=p^3-9p^2+27p-27$

$\Rightarrow p^3-9p^2+26p=0 \Rightarrow p\left(p^2+p+1\right)\equiv 0(\mathrm{mod}\,5)$

buradan $p=5$ olur.

Çözüm2:

$p-q=p+p+q-q\equiv 2p(\mathrm{mod}\,p+p) \Rightarrow 0\equiv(2p)^3\equiv 8p^3(\mathrm{mod}\,p+p)$

$p+q\,|\,8p^3$; $\left(p^3,p+q\right)=1$

$p+q\,|\,8 \Rightarrow p+q=8 \Rightarrow p=5$, $q=3$ olur.

41) 100'den küçük kaç asal sayı ardışık pozitif tam sayıların karelerini toplamı olarak yazılabilir?

Çözüm:

1, 4, 9, 16, 25, 36, 49, 64, 81

- Ardışık iki tam kare toplamı şeklinde olan asal sayılar
  1+4=5, 4+9=13, 16+25=41, 25+36=61
- Ardışık üç tam kare toplamı şeklinde olan asal sayılar 4+9+16=29
- Ardışık dört tam kare olamaz çünkü ikisi çift ikisi tek olduğundan toplam çift olur.

42) $4xy-x-y=z^2$ denkleminin pozitif tam sayı köklerinin bulunmadığını gösteriniz?

Bilgi: $a\in Z$ *ve* $a\equiv 3(\bmod 4)$ ise p tek asal sayı $p=4k+3\vee p=4k+1$

a'nın , $p=4k+3$ şeklinde bir asal böleni vardır.

$a=p_1^{k_1}...p_n^{k_n}\equiv 3(\bmod 4)$

Hepsi $p=4k+1$ olsaydı ifade sağlanmazdı en az bir tanesi $p=4k+3$ tür.

Çözüm: $16xy-4x-4y=4z^2\Rightarrow\quad (4x-1)(4y-1)=4z^2+1$

$4x-1$'in $p=4k+3$ şeklinde bir asal böleni vardır.

$4z^2+1\equiv 0(\bmod p)\Rightarrow 4z^2\equiv -1(\bmod p)\Rightarrow (2z)^2\equiv -1(\bmod p)...(1)$

$$\left.\begin{array}{l}(2z)^2\equiv 1(\bmod p)\\ (2z)^{p-1}\equiv 1(\bmod p)\end{array}\right\}\Rightarrow (2z)^{(4,p-1)}\equiv 1(\bmod p)\Rightarrow p-1=4k+2$$

$\Rightarrow (4,4k+2)=2\Rightarrow (2z)^2\equiv 1(\bmod p)...(2)$

(1) ve (2) den çelişki elde edilir. Bu sebeple çözüm yoktur.

43) m,n pozitif tam sayılar olmak üzere, $2001m^2+m=2002n^2+n$ eşitliği sağlandığına göre, $m-n$ sayısının bir tam kare olduğunu gösteriniz?

Çözüm:

$2001m^2+m=2002n^2+n$

$2001m^2-2001n^2+m-n=n^2$

$2001(m-n)(m+n)+(m-n)=n^2$

$(m-n)(2001m+2001n+1)=n^2$

olur. Son eşitliğe göre, eğer $p\mid m-n$ oluyorsa $p\mid 2001m+2001n+1$ olmalıdır.

Ayrıca, $(2001m+2001n+1)-2001(m-n)=4002n+1$ sayısını da bölmelidir.

Fakat, $p \mid n$ olduğundan, $p \nmid 4002n+1$ olacaktır. O halde,

$(2001m+2001n+1)$ ve $(m-n)$ sayıları aralarında asal olmalı ve her biri bir tam kare olmalıdır. Yani, $(m-n)$ bir tam kare olur.

44) 11 tane 1 ile başlayan 20 basamaklı bir sayının tam kare olmayacağını ispatlayınız. (Özdemir, 2012, 295)

Çözüm:

$111...11 \cdot 10^9 \le n < 111...11 \cdot 10^9 + 10^9$ olduğundan

$(10^{11}-1) \cdot 10^9 \le 9n < (10^{11}-1) \cdot 10^9 + 9 \cdot 10^9$ olur. Eşitsizliğin sol tarafına göre,

$(10^{10}-1)^2 < 10^{20} - 10^9 \le 9n < 10^2 + 8 \cdot 10^9 < (10^{10}+1)^2$

olduğundan, $9n, (10^{10}-1)^2$ ile $(10^{10}+1)^2$ arasındaki tek tam kare olan 10^{20} olabilir. Fakat, 10^{20} sayısı 9'a bölünemeyeceğinden, 11 tane 1 ile başlayan 20 basamaklı bir tam kare olamaz.

45) x, y pozitif tam sayılar olmak üzere, $2x^2+x=3y^2+y$ ise, $x-y$, $2x+2y+1$, $3x+3y+1$ ifadeleri tam karedir ispatlayınız.

Çözüm:

$2x^2+x=3y^2+y$ denklemini $x^2=(x-y)(3x+3y+1)$ ve

$y^2=(x-y)(2x+2y+1)$ biçiminde yazabiliriz.

$OBEB(3(x+y)+1, 2(x+y)+1)=1$ olduğundan, $OBEB(x^2, y^2)=x-y$ olmalıdır. $OBEB(x^2, y^2)=(OBEB(x, y))^2$ olduğundan, $2x+2y+1$ ve $3x+3y+1$ ifadeleri de tam kare olmalıdır.

46) $a, b, c \in Z^+$ olmak üzere, $\frac{1}{a}+\frac{1}{b}=\frac{1}{c}$ ve $OBEB(a, c)=1$ eşitliği sağlandığına göre, $a+b$, $a-c$ ve $b-c$'nin üçünün de tam kare olduğunu gösteriniz.

Çözüm:

$\frac{1}{b}=\frac{a-c}{a\cdot c}$ yazalım. Öklid algoritmasına göre,

$OBEB(a,c)=OBEB(a,\text{a}-c)=OBEB(\text{c},\text{a}-c)=1$ olduğundan $\frac{1}{b}=\frac{a-c}{a\cdot c}$ eşitliğindeki kesirler en sade haldedirler. O halde, $a-c=1$ ve $a.c=b$ olmalıdır. Buna göre, $a+b=a+a.c=a(c+1)=a^2$ ve

$b-c=a.c-c=c(a-1)=c^2$ olduğu görülür.

47) $OBEB(a,\text{b},c)=1$ ve $a^2b^2+b^2c^2+c^2a^2$ sayısı tam kare olacak biçimde sonsuz sayıda (a,b,c) pozitif tam sayı üçlüsü bulunduğunu ispatlayınız.

Çözüm:

x bir tek sayı ve $(x,y)=1$ olmak üzere, $a=x^2,b=2y^2\ ve\ c=xy$ diyelim. x tek ve x ile y aralarında asal olduğundan, $OBEB(a,\text{b},c)=1$'dir.

$a^2b^2+b^2c^2+c^2a^2=x^4y^4+4x^2y^6+x^6y^2$

$a^2b^2+b^2c^2+c^2a^2=x^2y^2\left(4x^2y^2+4y^4+x^4\right)$

$a^2b^2+b^2c^2+c^2a^2=x^2y^2\left(x^2+2y^2\right)^2$

olduğundan, $OBEB(a,\text{b},c)=1$ ve $a^2b^2+b^2c^2+c^2a^2$ sayısı tam kare olacak biçimde $a,b\ ve\ c$ üçlüleri x ve y'ye bağlı olarak sonsuz sayıda seçilebilir. Yani, sonsuz sayıda (a,b,c) üçlüsü vardır.

48) Herhangi 9 tanesinin toplamı tam kare olan 10 farklı tam sayı var mıdır? (Rusya 1999)

Çözüm:

$a_1,a_2,a_3,...,a_{10}$ istenen şekildeki 10 farklı tam sayı olsun. Bu sayıların tamamının toplamı S ise, $i=1,2,3,...,10$ için $S-a_i=k_i^2$ olacak şekilde bir k_i olmasını istiyoruz. $i=1,2,3,...,10$ için tüm eşitlikleri toplarsak,

$10S-(a_1+a_2+a_3+...+a_{10})=k_1{}^2+k_2{}^2+k_3{}^2+...+k_{10}{}^2$ veya

$9S=k_1{}^2+k_2{}^2+k_3{}^2+...+k_{10}{}^2$ elde edilir. Bu eşitliğe göre,

$k_1^2 + k_2^2 + k_3^2 + ... + k_{10}^2$ toplamı 9'a bölünebilmelidir. Örneğin; $k_i = 3i$ alınabilir. Böylece,

$$k_1^2 + k_2^2 + k_3^2 + ... + k_{10}^2 = 9\left(1^2 + 2^2 + 3^2 + ... + 10^2\right) = 9 \cdot \frac{10 \cdot 11 \cdot 21}{6} = 9 \cdot 385$$

olur. $a_i = S - \left(S - a_i\right) = \frac{k_1^2 + k_2^2 + k_3^2 + ... + k_{10}^2}{9} - k_i^2$ eşitliğini kullanarak ,

$a_i = 385 - k_i^2$ eşitliğinden, 376, 349, 304, 241, 160, 61, -56, -191, -344, -515 sayılarının istenen şekilde olduğu görülür.

49) n pozitif tam sayısı için, $n^3 + 7n - 133$ ifadesi pozitif bir tam sayının küpü oluyorsa, n sayısına "iyi sayı" diyelim. Tüm iyi sayıların toplamını bulunuz? (USC. Math. Contest)

Çözüm:

$n^3 + 7n - 133 = m^3$ diyelim

- $n = m$ olması durumunda, $7n = 133$ denkleminden $n = 19$ bulunur.
- $m \geq n + 1$ olsun. Bu durumda,

  $n^3 + 7n - 133 = m^3 \geq \left(n + 1\right)^3 = n^3 + 3n^2 + 3n + 1$ eşitsizliğinden,

  $3n^2 - 4n + 134 \leq 0$ elde edilir ki, bu eşitsizliğin n pozitif tam sayıları için çözümü yoktur.
- $m \leq n - 1$ olduğunu kabul edelim. Bu durumda

  $n^3 + 7n - 133 = m^3 \leq \left(n - 1\right)^3 = n^3 - 3n^2 + 3n - 1$ eşitsizliğinden,

  $3n^2 + 4n - 132 \leq 0$ olur. Bu eşitsizliğe göre, $n \leq 6$ olması gerekir. Böylece kontrol edilirse, $6^3 + 7 \cdot 6 - 133 = 5^3$ ve $5^3 + 7 \cdot 5 - 133 = 3^3$ olduğundan 5 ve 6 sayılarının "iyi" sayı olduğu görülür. $n \leq 4$ için, $n^3 + 7n - 133$ ifadesi negatiftir ve pozitif bir sayının küpü olamaz. O halde, iyi sayıların toplamı $5 + 6 + 19 = 30$ olarak bulunur.

50) $n^2 - 19n + 99$ sayısı tam kare olacak şekilde tüm n pozitif tam sayılarının toplamını bulunuz. (AIME 1999)

Çözüm:

$m \in Z^+$ için, $n^2 - 19n + 99 = m^2$ olsun. Buna göre, $n^2 - 19n + 99 - m^2 = 0$

denkleminden $n_{1,2}=\dfrac{19\pm\sqrt{361-4\left(99-m^2\right)}}{2}$ olur. Bu ifadenin bir tam sayı olması $k\in Z^+$ için $361-4\left(99-m^2\right)=4m^2-35=k^2$ durumunda mümkündür. Buradan, $\left(2m-k\right)\cdot\left(2m+k\right)=35$ olduğundan

$$\left.\begin{matrix}2m-k=1\\2m+k=35\end{matrix}\right\} \text{ veya } \left.\begin{matrix}2m-k=5\\2m+k=7\end{matrix}\right\}$$

denklem sistemleri elde edilir. Birinci denklemden $k=17$, ikinci denklemden $k=1$ bulunur. Böylece $n\in\{1,18,10,9\}$ olabilir.

51) $n^2+2009n$ sayısı tam kare olacak şekilde en büyük n pozitif tam sayısı kaçtır? (Özdemir, 2012, 297)

Çözüm:

$n^2+2009n=\left(n+k\right)^2=n^2+2nk+k^2$ eşitliğinden $n=\dfrac{k^2}{2009-2k}$ elde edilir.

Bu eşitliğe göre,

$k<1005$ olmalıdır. k'yı en büyük seçelim ki, n en büyük olsun. Buna göre,

$k=1004$ seçilirse $n=\dfrac{1004^2}{2009-2\cdot1004}=1004^2$ elde edilir.

52) n^4+n^3+1 ifadesi tam kare olacak şekilde tüm n pozitif tam sayılarını bulunuz?

Çözüm:

$\left(n^2\right)^2=n^4<n^4+n^3+1$ olduğundan, bir $k\in Z^+$ için

$n^4+n^3+1=\left(n^2+k\right)^2=k^2+n^4+2kn^2$

yazılabilir. Buradan, $\left(n-2k\right)n^2=k^2-1\qquad(*)$ elde edilir. $k^2-1\geq0$'dır. O halde, $n^2>0$ ve $\left(n-2k\right)n^2>0$ olduğundan, $n>2k$ olur. Ayrıca, $(*)$ eşitliğine göre, n^2 sayısı k^2-1 sayısını bölmelidir. Bundan dolayı, $n^2\leq k^2-1$ veya $k=1$ olabilir. Şimdi, k'nın sadece 1 olabileceğini gösterelim. Bunun için, olmayana ergi yöntemini kullanacağız. Kabul edelim ki, $k>1$ olsun. Buna göre, $k^2>k^2-1\geq n^2$ eşitsizliğinden $k\geq n$ elde edilir. Fakat, bu $n>2k$ olması

ile çelişir. O halde, $k=1$ ve dolayısıyla da $n=2$ olmalıdır. $2^4+2^3+1=25$ sayı istenen şekildeki tam karedir.

53) n^2+n ve n^3+2n^2 ifadelerinin ikisi de tam sayı olacak şekilde kaç tane rasyonel olmayan n reel sayısı vardır?

Çözüm:

$n^2+n=a$ ve $n^3+2n^2=b$ ifadeleri tam sayı olsun. Bu durumda, n sayısı, $n^2+n-a=0$ ve $n^3+2n^2-b=0$ denklemlerinin köküdür. Polinomlarda bölme işlemi ile, $n^3+2n^2-b=\left(n^2+n-a\right)(n+1)+(a-1)n+(a-b)$ yazılabilir. Bu eşitliğe göre, n sayısı $(a-1)n+(a-b)=0$ denkleminin de bir köküdür. Eğer, $a\neq 1$ ise $n=\dfrac{(b-a)}{(a-1)}$ olur ki, n bir rasyonel sayı olur. Bunu istemiyoruz. O halde, $a=1$ ve dolayısıyla da $b=1$ olmalıdır. $n^2+n=1$ eşitliğine göre, $n=\dfrac{-1\pm\sqrt{5}}{2}$ olur. O halde, istenen şekilde iki tane n değeri vardır.

54) m ve n sayıları her ikisi de pozitif ya da negatif olan birbirinden farklı sayılar olmak üzere, m^2+4n ve n^2+4m sayılarının her ikisi de tam kare olacak şekilde kaç tane (m,n) tam sayı ikilisi vardır? (Asya Pasifik M.O.)

Çözüm:

i. $m,n>0$ olsun. Bu durumda, $k\in Z^+$ için, $m^2+4n=(m+2k)^2$ olmalıdır. Buradan, $n=km+k^2>m$ olur. Benzer şekilde, $m>n$ olur. Bu bir çelişkidir. Dolayısıyla, m ve n ikisi birden pozitif olamaz.

ii. $m,n<0$ olsun,. Bu durumda, $m=-M$ ve $n=-N$ yazalım. Bu durumda, $M,N>0$ olur $M\geq N$ kabul edebiliriz. M^2-4N tam karedir ve $k\in Z$ için,

$M^2-4N=(M-2k)^2$ yazılabilir. Buradan sırasıyla,

$M^2-4N=(M-2k)^2$

$M^2-4N=M^2-4Mk+4k^2$

$-4N=-4Mk+4k^2$

$$N = Mk - k^2$$

olur. O halde, $M > N$ kabul edebiliriz. Buna göre,

$M > N = Mk - k^2 = k(M-k) > 0$ eşitsizliğinden, $0 < M-k$ ve

$M < \frac{k^2}{k-1} = k+1+\frac{1}{k-1} \le k+2$ elde edilir. Böylece $0 < M-k < 2$

eşitsizliğinden, $M-k=1$, $M=k+1$ ve $N=k$ elde edilir. Sonuç olarak,

$M^2 - 4N = (k+1)^2 - 4k = (k-1)^2$ ve $N^2 - 4M = k^2 - 4k - 4 = (k-2)^2 - 8 = z^2$

olacaktır.

İkinci ifadenin sağlanabilmesi için, $(k-2-z)(k-2+z) = 2^3$ eşitliğine göre,

$k=5$ ve $z=1$ bulunur. Böylece $M=6$ ve $N=5$ olur. O halde, $(-6,-5)$ ve simetriden $(-5,-6)$ bir çözüm olur. O halde sadece 2 çözüm vardır.

55) $10x^3 + 20y^3 + 8xyz = 1999z^3$ denkleminin tam sayılarda kaç tane çözümü vardır? (Municipal 1999)

Çözüm:

$(x,y,z) = (0,0,0)$ denklemin bir çözümüdür. Şimdi denklemin başka çözümü olup olmadığını arayalım. Denklem homojen olduğundan, $OBEB(x,y,z) = 1$ kabul edebiliriz. Çünkü, $OBEB(x,y,z) = d > 1$ olursa, $x_1 = x \mid d$, $y_1 = y \mid d$ ve $z_1 = z \mid d$ yazılarak, $OBEB(x_1, y_1, z_1) = 1$ bulunacaktır. Denklemin sol tarafı 2'ye bölündüğünden, sağ tarafı da bölünmelidir. O halde, $z = 2z_1$, $z_1 \in Z$ olacağından $10x^3 + 20y^3 + 16xyz_1 = 1999 \cdot 8 \cdot z_1^3$ yani

$5x^3 + 10y^3 + 8xyz_1 = 1999 \cdot 4 \cdot z_1^3$ elde edilir. Benzer düşünceyle, $x = 2x_1$ olmalıdır. Buna göre,

$5 \cdot 4 \cdot x_1^3 + 5y^3 + 8x_1yz_1 = 1999 \cdot 4 \cdot z_1^3$ olur. Bu düşünceyle, $y = 2y_1$ olmalıdır. Buna göre sırasıyla,

$5 \cdot 4 \cdot x_1^3 + 5 \cdot 8 \cdot y_1^3 + 16x_1y_1z_1 = 1999 \cdot 2 \cdot z_1^3$

$5 \cdot 2 \cdot x_1^3 + 5 \cdot 4 \cdot y_1^3 + 8x_1y_1z_1 = 1999 \cdot z_1^3$

$10 \cdot x_1^3 + 20 \cdot y_1^3 + 8x_1y_1z_1 = 1999 \cdot z_1^3$

elde edilir. Buna göre, $OBEB(x,y,z) = 2$ çelişkisi elde edilir. O halde

denklemin tek tam sayı çözümü $(0,0,0)$ bulunur.

56) $a<b<c$ olmak üzere, $(a+b+c)^2=a^3+b^3+c^3$ denklemini sağlayan tüm (a,b,c) pozitif tam sayı üçlülerini bulunuz?

Çözüm:

$0<a<b<c$ olduğundan, $b\le c-1$, $a\le c-2$ yazılabilir. Bu durumda $a+b+c\le 3c-3$ olur. O halde, $a^3+b^3+c^3=(a+b+c)^2\le(3c-3)^2=9(c-1)^2$ olacaktır. Buradan da, $a^3+b^3\le 9(c-1)^2-c^3$ (*) elde edilir. a^3+b^3 pozitif olduğundan, $9(c-1)^2-c^3>0$ olmalıdır. Bunun için $c\le 6$ olmalıdır. Böylece, $3\le c\le 6$ elde edilir. c sayısının bu değerleri için, sırasıyla $9(c-1)^2-c^3$ ifadesi 9, 17, 19, 9 değerlerini alabilir. (*) eşitsizliğine göre, $3^3=27$ olduğundan, b sayısının 3'ten küçük olması gerekir. Buna göre, $a<b<c$ olduğuda göz önüne alınarak, $a=1$ ve $b=2$ olması gerektiği görülür. Böylece, $(3+c)^2=1^3+2^3+c^3$ eşitliğinden, $6c+c^2=c^3$ olur. Buradan, $c=3$ elde edilir.

57) $5n^2=36a^2+18b^2+6c^2$ denklemini sağlayan kaç tane (a,b,c,n) tam sayı dörtlüsü vardır? (Asya Pasifik M.O. 1989)

Çözüm:

Eşitliğin sağ tarafı 3'e bölünmektedir. O halde n sayısı da 3'e bölünmelidir. Yani $n=3k$, $k\in Z$ olmalıdır. Buna göre, $5\cdot 9k^2=36a^2+18b^2+6c^2$ eşitliğinden, $15k^2=12a^2+6b^2+2c^2$ olur. Benzer mantıkla, $c=3e$, $e\in Z$ olmalıdır. Buradan $5k^2-4a^2=2b^2+6e^2$ elde edilir. Bu denklemin bir çözümü (m,a,b,e) olsun. Öyle ki en küçük m sayısını alalım. Yani, denklemi sağlayan dörtlüler içinde m sayısının en küçük olanını alarak çözümü yapalım.

Şimdi bu denklemin çözümü için $\mathrm{mod}16$'da kalanları inceleyelim. Bir sayının karesi $\mathrm{mod}16$'da çift ise 0 veya 4, tek ise 1 veya 9 kalanını verir. Buna göre, her bir terimi inceleyelim.

i. k 'nın bir çift tam sayı olması gerektiği açıktır. Çünkü eşitliğin sağ tara fındaki her terim 2'ye bölünür. O halde, $5k^2 \equiv 0,4 \pmod{16}$ olur.

ii. $4a^2 \equiv 0$ *veya* $4 \pmod{16}$'dır.

iii. $2b^2 \equiv 0,2$ *veya* $8 \pmod{16}$'dır.

iv. $6e^2 \equiv 0,6$ *veya* $8 \pmod{16}$'dır.

Buna göre, $2b^2 + 6e^2 \equiv 0,2,6,8,10$ *veya* $14 \pmod{16}$,

$2k^2 - 4a^2 \equiv 0,4$ *veya* $12 \pmod{16}$ olduğundan, $2b^2 + 6e^2 \equiv 5k^2 - 4a^2$ denkliğinin sağlanması sadece her iki taraf sıfıra denk iken mümkündür. $2b^2 + 6e^2 \equiv 0 \pmod{16}$ ise b ve e çift sayılar olması gerekir. Diğer taraftan, a sayısı tek sayı olmalıdır. Aksi durumda, m,a,b,e sayılarının hepsi çift sayılar olur ve $\left(\frac{m}{2},\frac{a}{2},\frac{b}{2},\frac{e}{2}\right)$ dörtlüsü de denklemin bir çözümüdür. Denklemi sağlayan en küçük m sayısını almamıza rağmen, $\frac{m}{2} < m$ olacak şekilde bir çözüm bulmuş olduk. Yani a sayısı çift olmamalıdır. Buna göre, $b = 2b_1$, $e = 2e_1$ *ve* $k = 2k_1$ diyelim. $8b_1^2 + 24e_1^2 \equiv 20k_1^2 - 4a^2$ denkliğinden, $2b_1^2 + 6e_1^2 \equiv 5k_1^2 - a^2$ elde edilir. a tek sayı olduğundan, $5k_1^2 - a^2 \equiv 4,12 \pmod{16}$ olabilir. Fakat

$2b_1^2 + 6e_1^2 \equiv 0,2,6,8,10$ *veya* $14 \pmod{16}$

olabileceğinden denklemin $(0,0,0,0)$'dan başka çözümü yoktur.

58) $(m-n)^2 = \frac{4mn}{m+n-1}$ deklemini sağlayan $0 < m+n < 100$ olacak şekilde kaç tane (m,n) tam sayı çifti vardır? (Estonya M.O. 1999)

Çözüm:

$(m-n)^2 \cdot (m+n-1) = 4mn$ eşitliği düzenlenirse, sırasıyla

$2mn - m^2 + m^3 - n^2 + n^3 - mn^2 - m^2n = 4mn$

$m^3 + n^3 - mn^2 - m^2n = 2mn + n^2 + m^2$

$m(m^2 - n^2) - n(m^2 - n^2) = (m+n)^2$

$(m^2-n^2)(m-n)=(m+n)^2$

$(m-n)^2(m+n)=(m+n)^2$

elde edilir. Buna göre, $m+n=0$ veya $(m-n)^2=m+n$ bulunur. $m+n=0$ ise $n=-m$ ve tüm $m\in Z$ için $(m,-m)$ ikilileri bir çözümdür. Fakat $m+n=0$ olacağından istenen koşulumuz sağlanmaz. $(m-n)^2=m+n$ eşitliğinden, $m-n=a$ ve $m+n=a^2$ olur. Bu eşitlikler toplanırsa, $2m=a(a+1)$ ve buradan da, $m=\frac{a(a+1)}{2}$ ve $n=\frac{a(a-1)}{2}$ bulunur. Böylece, $a\in Z$ için, $\left(\frac{a(a+1)}{2},\frac{a(a-1)}{2}\right)$ ikilileri bir çözümdür. Buradan, $m+n=a^2$ eşitliğine göre, $0<a^2<100$ olmalıdır. Bu durumda $a=\pm1,\pm2,\pm3,\pm4,\pm5,\pm6,\pm7,\pm8$ *veya* ±9 olur. Diğer taraftan verilen denklemde paydanın sıfır olmayacağı göz önüne alınırsa, $m+n\neq1$ olmayacağından, $a=\pm1$ olmalıdır. Böylece istenen şekilde $2\cdot8=16$ tam sayı çifti vardır.

59) n bir pozitif tam sayı olmak üzere, $2+2\sqrt{28n^2+1}=m$ denklemini sağlayan m tam sayılarından kaç tanesi tam kare değildir?

a) 4 **b)** 1 **c)** 0 **d)** sonsuz sayıda **e)** 3

Çözüm:

$2+2\sqrt{28n^2+1}=m$ ifadesinde, kareköklü ifade yalnız bırakılıp kare alınırsa, $4.(28n^2+1)=m^2-4m+4$ olur. Bu eşitliğe göre, çift olmalıdır. $m=2k$, $k\in Z$ diyelim. $(28n^2+1)=k^2-2k+1$ denkleminden, $28n^2=k.(k-2)$ olur. Bu denklemde, sol taraf çift olduğundan, sağ tarafın çift olması k 'nın çift olmasıyla mümkündür. O halde, $k=2u$, $u\in Z$ diyelim. Yerine yazıp sadeleştirirsek, $7n^2=u.(u-1)$ olur. u ve $u-1$ aralarında asal olduğundan, iki durum mümkündür.

i. $u=7x^2$, $u-1=y^2$ olursa, $7x^2-y^2=1$ elde edilir. Bu denklemi $\bmod 7$ de düşünürsek, $y^2\equiv-1(\bmod 7)$ olmalıdır. Fakat, bu mümkün değildir.

ii. $u=x^2$, $u-1=7y^2$ olursa, $x^2-7y^2=1$ elde edilir. Bu durumda denklemin çözümü vardır. Bu durumda, $k=2x^2$ olduğundan, $m=4x^2=(2x)^2$ elde edilir. O halde, denklemi sağlayan m tam sayılarından tamamı tam karedir.

60) $S(\text{n})$, ilk n pozitif tam sayının toplamını göstersin. Buna göre, eğer n ve $S(\text{n})$ sayılarının her ikisi de bir tam kare ise n sayısına fantastik sayı diyelim. Örneğin, 49 sayısı fantastik bir sayıdır çünkü, $49=7^2$ ve $S(49)=1+2+3+...+49=1225=35^2$ sayıları tam karedir. 49 sayısından büyük başka bir fantastik sayı bulunuz?

Çözüm:

$n=k^2$ olsun $S(\text{n})=\dfrac{n.(n+1)}{2}=\dfrac{k^2.\left(k^2+1\right)}{2}$ sayısının tam kare olmasını istiyoruz. k^2 bir tam kare olduğundan, $\dfrac{k^2+1}{2}$ sayısının tam kare olması yeterlidir. O halde, $\dfrac{k^2+1}{2}=m^2$, $m\in Z$ olsun. Bu durumda,

$k^2-2m^2=\left(k+m\sqrt{2}\right)\cdot\left(k-m\sqrt{2}\right)=-1$ olmalıdır. Bu eşitliği $(k,m)=(7,5)$ sağlar. Yani, soruda verilen örnek sağlanır. Bu eşitliği,

$\left(3+2\sqrt{2}\right)\cdot\left(3-2\sqrt{2}\right)=1$ ile çarpalım. Bu çarpıma P dersek

$$P=\left(7+5\sqrt{2}\right)\cdot\left(7-5\sqrt{2}\right)\cdot\left(3+2\sqrt{2}\right)\cdot\left(3-2\sqrt{2}\right)$$

$$P=\left(7+5\sqrt{2}\right)\cdot\left(3+2\sqrt{2}\right)\cdot\left(7-5\sqrt{2}\right)\cdot\left(3-2\sqrt{2}\right)$$

$$P=\left(41+29\sqrt{2}\right)\cdot\left(41-29\sqrt{2}\right)$$

$$P=41^2-2\cdot29^2=-1$$

olduğundan, $(k,m)=(41,29)$ sayı çifti de, $k^2-2m^2=-1$ eşitliğini sağlar. Böylece $n=41^2=1681$ sayısı da bir fantastik sayıdır.

REFERANSLAR

[1] Alizade,R., Ders Notları, Yaşar Üniversitesi, İzmir 2013.

[2] Çallıalp,F., Sayıların Teorisi, Birsen Yayınevi, İstanbul 2009.

[3] Gürlü,Ö., Sayılar Teorisine Giriş, Çağlayan A.Ş., İzmir 2009

[4] Özdemir,M., Sayılar Teorisine, Altın Nokta Yayınevi, İzmir 2012

[5] Karakaş,H.İ., Aliyev,i., Sayılar Teorisinde İlginç Olimpiyat Problemleri ve Çözümleri, Tübitak 1998.

[6] Sıerpınskı, W., 250 Problems ın Elementary Number Theory, Elsevıer, New York 1970.

WEB KAYNAKLARI

[1] http://www.tubitak.gov.tr/tr/olimpiyatlar/io-matematik-olimpiyatlari/

[2] http://www.tubitak.gov.tr/tr/olimpiyatlar/ulusal-bilim-olimpiyatlari/

[2] http://www.mathlinks.ro/Forum/

[3] http://www. artofproblemsolving.com/Forum/

ÖZGEÇMİŞ

1975 yılında Kars Sarıkamışta'ta doğan yazar, ilk ve orta öğrenimini Ardahan Göle'de tamamladı. 1993 yılında Dumlupınar Üniversitesi Matematik Bölümün'nde yüksek öğrenimine devam etti. 1998 yılında mezun olup 1999 yılında Milli Eğitim Bakanlığı'nda öğretmenlik yapmaya başladı. Halen Çiğli Mehpare Yağcı Anadolu İmam Hatip Lisesi'nde Matematik öğretmeni olarak görev yapmaktadır. Evli ve iki çocuk babasıdır.