İki Tamkarenin Toplamı

(Metin Can Aydemir)

Tanım: p bir asal sayı ve n ve α pozitif tamsayı olmak üzere $p^{\alpha}|n$ fakat $p^{\alpha+1} \nmid n$ ise

$$p^{\alpha}||n$$

olarak gösterilir ve "p üzeri α çift böler n" olarak okunur.

Legendre Sembolü: p tek bir asal sayı ve a bir tamsayı olmak üzere,

$$\left(\frac{a}{p}\right) \equiv \begin{cases} 0, p|a \text{ ise} \\ 1, x^2 \equiv a\ (mod p) \text{ olacak şekilde } 0'\text{dan farklı x tamsayısı varsa} \\ -1, x^2 \equiv a\ (mod p) \text{ olacak şekilde } 0'\text{dan farklı x tamsayısı yoksa} \end{cases}$$

olarak tanımlanır.

Özellik 1: $\left(\frac{a}{p}\right)$ Legendre sembolü olmak üzere,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (mod\ p)'\text{dir.}$$

Özellik 2: $\left(\frac{a}{p}\right)$ Legendre sembolü olmak üzere,

$$\left(\frac{a}{p}\right).\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right)'\text{dir.}$$

Özellik 3: $\left(\frac{a}{p}\right)$ Legendre sembolü ve p ile q farklı tek asallar olmak üzere,

$$\left(\frac{q}{p}\right).\left(\frac{p}{q}\right) \equiv (-1)^{\frac{(p-1)(q-1)}{4}}\text{'dir.}$$

Wilson Teoremi: p tek bir asal sayı olmak üzere,

$$(p-1)! \equiv -1 (mod\ p)'\text{dir.}$$

Pisagor Üçlüleri: m, n, c doğal sayı ve m, n aralarında asal olmak üzere $x^2 + y^2 = z^2$ denkleminin doğal sayılardaki çözümleri,

$$(x, y, z) = \big(c.|m^2 - n^2|, 2mnc, c.(m^2 + n^2)\big), \big(2mnc, c.|m^2 - n^2|, c.(m^2 + n^2)\big)$$

formatındadır.

Teorem 1: n, pozitif bir tamsayı olmak üzere, $x^2 + y^2 = n$ denkleminin tamsayılarda çözümü olabilmesi için gerek ve yeterli şart $p \equiv 3(mod\ 4)$ olmak üzere $\forall\ p|n$ için p'nin n'yi bölen en büyük kuvvetinin üssünün çift sayı olmasıdır.

İspat: Bu denklemde x yerine $-x$ yazılsa da denklem değişmeyeceğinden denklemi doğal sayılarda inceleyebiliriz. Önce şart sağlanmazsa denklemin çözümünün olmayacağını gösterelim. Farz edelim ki n'nin öyle bir $4k + 3$ formatında bir p asal böleni var ki a tek sayı olmak üzere $p^a||n$ sağlar. Öyleyse,

$$p|(x^2 + y^2) \Longrightarrow x^2 + y^2 \equiv 0(mod\ p)$$

Eğer x ve y, p'ye bölünmüyorsa,

$$x^2 \equiv -y^2(mod\ p) \Longrightarrow \left(\frac{x}{y}\right)^2 \equiv -1(mod\ p)$$

olur. x ve y, p'ye bölünmediğinden $\left(\frac{x}{y}\right) \equiv b(mod\ p)$ olacak şekilde 0'dan farklı bir b tamsayısı vardır. Dolayısıyla (-1), p modunda karekalandır. $\left(\frac{a}{p}\right)$ Legendre sembolü olmak üzere,

$$\Longrightarrow \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \Longrightarrow p \equiv 1(mod\ 4)$$

olmalı. Bu bir çelişkidir. Dolayısıyla x ve y, p'ye bölünmelidir. $x = p.x_1,\ y = p.y_1$ ve $n = p^2.n_1$ diyelim. Denklem,

$$x_1^2 + y_1^2 = n_1$$

olur. Eğer $a = 1$ ise x_1 ve y_1 tamsayı fakat n_1 tamsayı olmadığından çözümü olmayacaktır.

$a = 2k + 1$ ise yeni denklem ilk denklemin aynısı olduğundan yine x_1 ve y_1, p'ye bölünecektir. Bu işlemi $k + 1$ defa tekrar ettirirsek, n_{k+1} sayısı tamsayı olmayacaktır fakat x_{k+1} ve y_{k+1} tamsayı olur ve

$$x_{k+1}^2 + y_{k+1}^2 = n_{k+1}$$

sağlar. Fakat n_{k+1} tamsayı olmadığından bu çelişkidir. Dolayısıyla kabulumüz yanlıştır. p'nin n'yi bölen en büyük kuvvetinin üssü çift sayı olmalıdır.

Şimdi p'nin n'yi bölen en büyük kuvvetinin üssü çift sayı ise $x^2 + y^2 = n$ denkleminin çözümünün olduğunu gösterelim. Öncelikle p, $4k + 1$ formatında başka bir asal sayı olmak üzere, $x^2 + y^2 = p$ denkleminin en az bir çözümü olduğunu gösterelim. $r^2 \equiv -1(mod\ p)$ olacak şekilde bir r tamsayısı olduğunu gösterelim. Wilson Teoreminden,

$$(p-1)! \equiv -1(mod\ p)$$

olduğunu biliyoruz. Ayrıca $k \equiv -(p-k)(mod\ p)$ olacağından,

$$(p-1)! \equiv 1.2 \dots \left(\frac{p-1}{2}\right).\left(\frac{p+1}{2}\right) \dots (p-1) \equiv 1.2 \dots \left(\frac{p-1}{2}\right).\left(-\frac{p-1}{2}\right) \dots (-1)$$
$$\equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 (mod\ p)$$

$$\Longrightarrow (p-1)! \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1(mod\ p)$$

olur. Dolayısıyla $r^2 \equiv -1(mod\ p)$ olacak şekilde bir r tamsayısı vardır. Şimdi $f: \{0,1, \dots, [\![\sqrt{p}]\!]\}^2 \to Z^2$ olmak üzere, $f(u,v) = u + vr$ olacak şekilde bir fonksiyon tanımlayalım.

$$[\![\sqrt{p}]\!] + 1 > \sqrt{p} > [\![\sqrt{p}]\!]$$

'dir. f fonksiyonunda $\left([\![\sqrt{p}]\!] + 1\right)^2$ farklı (u,v) çifti seçebiliriz. $\left([\![\sqrt{p}]\!] + 1\right)^2 > p$ olduğundan Güvercin Yuvası İlkesinden $(u_1, v_1) \neq (u_2, v_2)$ fakat $f(u_1, v_1) \equiv f(u_2, v_2)(mod\ p)$ olacak şekilde en az bir $(u_1, v_1), (u_2, v_2)$ vardır. Eğer $u_1 = u_2$ ise

$$f(u_1, v_1) \equiv f(u_2, v_2)(mod\ p) \Longrightarrow u_1 + v_1.r \equiv u_2 + v_2.r(mod\ p) \Longrightarrow v_1.r \equiv v_2.r(mod\ p)$$

$$\Longrightarrow v_1 \equiv v_2(mod\ p)$$

$v_1, v_2 < p$ olduğundan $v_1 = v_2$ olmalı fakat $(u_1, v_1) \neq (u_2, v_2)$ olduğundan bu sağlanamaz. Çelişki.

Benzer şekilde $v_1 = v_2$ olursa da çelişki çıkar.

$$f(u_1, v_1) \equiv f(u_2, v_2)(mod\ p) \Longrightarrow u_1 + v_1.r \equiv u_2 + v_2.r(mod\ p)$$

$$\Longrightarrow (u_1 - u_2) \equiv r.(v_1 - v_2)(mod\ p)$$

olur. $|u_1 - u_2| = a$ ve $|v_1 - v_2| = b$ diyelim. $u_1, u_2, v_1, v_2 \leq [\![\sqrt{p}]\!]$ olduğundan $0 < a, b \leq [\![\sqrt{p}]\!]$ olur.

$$(u_1 - u_2) \equiv r.(v_1 - v_2)(mod\ p) \Longrightarrow a^2 \equiv -b^2(mod\ p) \Longrightarrow a^2 + b^2 \equiv 0(mod\ p)$$

$$a, b \leq [\![\sqrt{p}]\!] \Longrightarrow 0 < a^2 + b^2 \leq 2\left([\![\sqrt{p}]\!]\right)^2 < 2p$$

olduğundan $a^2 + b^2 = p$ olmalı. Dolayısıyla p, $4k+1$ formatında bir asal sayı olmak üzere her p asal sayısı için, $x^2 + y^2 = p$ denkleminin en az bir çözümü vardır.

Şimdi şartı her n tek pozitif tamsayısı için $x^2 + y^2 = n$ denkleminin çözümünün olduğunu gösterelim.

$p_i \equiv 1(mod\ 4)$ ve $q_j \equiv 3(mod\ 4)$ olsun.$(i = \{1,2, \dots, k\}, j = \{1,2, \dots, m\})$

$$n = 2^{\theta}\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right).\left(\prod_{j=1}^{m} q_j^{2\beta_j}\right)$$

olsun. n sayısını bölen en büyük tamkare C^2 olsun. $x = Cx_1,\ y = Cy_1$ şeklinde seçelim. $n = C^2.D$ olsun. Denklemde yerine yazarsak,

$$x_1^2 + y_1^2 = D$$

olur ve burada D kare bölensiz bir sayıdır. $D \neq 1$ ise D'nin asal çarpanlarına ayrılmış hali, $D = r_1.r_2 \ldots r_t$ olsun. D'nin $4k+3$ formatında böleni yoktur. 2 haricindeki tüm asal bölenleri $4k+1$ formatındadır. $2 = 1^2 + 1^2$'dir. Dolayısıyla tüm asal bölenleri iki tamkarenin toplamı olarak yazılabilir.

Herhangi a, b, c, d sayıları için,

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

özdeşliği sağlar. r_1 ve r_2 'nin iki tamkarenin toplamı şeklinde yazılabildiğini biliyoruz. Özdeşlikten dolayısıyla $r_1.r_2$ de iki tamkarenin toplamı şeklinde yazılabilir. Bu işlemi tekrarlayarak D'ye ulaşabiliriz.

$D = 1$ ise n sayısı tamkare demektir. Bu durumda $(x, y) = (\sqrt{n}, 0)$ bir çözüm olur.

Böylece ispatlamış olduk ki n, pozitif bir tamsayı ve $p \equiv 3(mod\ 4)$ olmak üzere $\forall\, p|n$ için p'nin n'yi bölen en büyük kuvvetinin üssü çift sayı ise $x^2 + y^2 = n$ denkleminin tamsayılarda en az bir çözümü vardır.

$x^2 + y^2 = n$ denkleminde (x, y) doğal sayı çözümü ise $(x, -y), (-x, y), (-x, -y)$ çözümleri de tamsayı çözümü olacağından bu kısımdan sonra $x^2 + y^2 = n$ denkleminin çözümleri doğal sayılarda incelenmiştir.

Teorem 2: p, $4k+1$ formatında bir asal sayı olmak üzere,

i) $x^2 + y^2 = p$ denkleminin doğal sayılarda çözümlerinin sayısı 2'dir.
ii) $x^2 + y^2 = p^2$ denkleminin doğal sayılarda çözümlerinin sayısı 4'dür.

İspat: i) $x = y$ için çözümün olmadığı aşikardır. Genelliği bozmadan $x > y$ olsun. $y = 0$ ise yine çözüm olmaz. Bu denklemi sağlayan en az bir (x, y) çifti olduğunu Teorem 1'den biliyoruz. (x, y) ve (y, x) çiftinden farklı bir (a, b) çözümünün olduğunu kabul edelim. (a, b) çözüm ise (b, a) da çözüm olacağından genelliği bozmadan $b < a < \sqrt{p},\ y < x < \sqrt{p}$ diyebiliriz. $a \equiv b.r(mod\ p)$ olsun.

$a \equiv b.r(mod\ p) \Longrightarrow a^2 \equiv b^2r^2(mod\ p) \Longrightarrow a^2 + b^2 \equiv b^2(1 + r^2) \equiv 0(mod\ p) \Longrightarrow (1 + r^2) \equiv 0(mod\ p)$

Burada $(1 + r^2) \equiv 0(mod\ p)$ olacak şekilde p modunda sadece iki çözüm olacağını göstermeliyiz.

$r^2 \equiv t^2 \equiv -1(mod\ p)$ olsun.

$$(r+t)(r-t) \equiv 0(mod\ p) \Longrightarrow r \equiv t(mod\ p) \text{ veya } r \equiv -t(mod\ p) \text{ olur.}$$

Yani $(1+r^2) \equiv 0(mod\ p)$ olacak şekilde p modunda sadece r ve $-r$ sayıları vardır. Dolayısıyla $x \equiv y.r\ (mod\ p)$ veya $x \equiv -y.r\ (mod\ p)$ olmalıdır.

a) $x \equiv y.r\ (mod\ p)$ ise $(x-a) \equiv (b-y).r\ (mod\ p)$ olur.

$(x-a) \equiv (b-y).r\ (mod\ p) \Longrightarrow (x-a)^2 + (b-y)^2 \equiv 0(mod\ p)$ olur.

$b < a < \sqrt{p},\ y < x < \sqrt{p}$ olduğundan $|x-a|, |b-y| < \sqrt{p} \Longrightarrow 0 < (x-a)^2 + (b-y)^2 < 2p$ olur.

Dolayısıyla $(x-a)^2 + (b-y)^2 = p$ olmalı. İfadeyi açarsak,

$x^2 + a^2 - 2ax + y^2 + b^2 - 2by = 2p - 2ax - 2by = p$ olur. Fakat p tek olduğundan bu sağlanamaz.

b) $x \equiv -y.r(mod\ p)$ ise $(a-x) \equiv (b+y).r(mod\ p)$ olur.

$(x-a) \equiv (b+y).r\ (mod\ p) \Longrightarrow (x-a)^2 + (b+y)^2 \equiv 0(mod\ p)$ olur.

$y < b < a < x < \sqrt{p}$ olduğundan $|x-a| < \sqrt{p}$ ve $(b+y) < 2\sqrt{p} \Longrightarrow 0 < (x-a)^2 + (b+y)^2 < 5p$ olur.

bi) $(x-a)^2 + (b+y)^2 = p$ ise ifadeyi açalım,

$x^2 + a^2 - 2ax + y^2 + b^2 + 2by = 2p - 2ax + 2by = p$ olur. Fakat p tek olduğundan bu sağlanamaz.

bii) $(x-a)^2 + (b+y)^2 = 2p$ ise ifadeyi açalım,

$x^2 + a^2 - 2ax + y^2 + b^2 + 2by = 2p - 2ax + 2by = 2p \Longrightarrow ax = by$ olur fakat $b < a,\ y < x$ kabulumüzden dolayı bu sağlanamaz.

biii) $(x-a)^2 + (b+y)^2 = 3p$ ise ifadeyi açalım.

$x^2 + a^2 - 2ax + y^2 + b^2 + 2by = 2p - 2ax + 2by = 3p$ olur. Fakat p tek olduğundan bu sağlanamaz.

biv) $(x-a)^2 + (b+y)^2 = 4p$ ise ifadeyi açalım,

$x^2 + a^2 - 2ax + y^2 + b^2 + 2by = 2p - 2ax + 2by = 4p \Longrightarrow ax + 2p = by$ olur fakat $b < a,\ y < x$ kabulumüzden dolayı bu sağlanamaz.

Dolayısıyla çözümler (x, y) ve simetriği (y, x) olmak üzere 2 tanedir.

ii) $x^2 + y^2 = z^2$ denkleminin doğal sayılardaki çözümleri Pisagor üçlülerinden dolayı, $m \geq n$ ve $EBOB(m,n) = 1$ olmak üzere,

$(x,y,z) = (c(m^2-n^2), 2mnc, c(m^2+n^2))$ ve $(x,y,z) = (2mnc, c(m^2-n^2), c(m^2+n^2))$ olduğunu biliyoruz. $x^2 + y^2 = p^2$ denkleminin çözümleri için de

$$c(m^2+n^2) = p$$

olmalı. $c = p$ ise $m^2 + n^2 = 1$ olur. Buradan $(m, n) = (1,0)$ bulunur. Yerine yazarsak $(x, y) = (0, p)$ ve $(p, 0)$ çözümleri bulunur. $c = 1$ ise $m^2 + n^2 = p$ olur.Bu denklemin tüm çözümlerinin (a, b) ve (b, a) gibi simetrik iki çözüm olduğunu biliyoruz. Genelliği bozmadan $a > b$ olsun. O halde tüm çözümler;

$$(x, y) = (0, p), (p, 0), (a^2 - b^2, 2ab), (2ab, a^2 - b^2)$$

olur. Dolayısıyla toplam 4 çözüm vardır.

Teorem 3: p, $4k + 1$ formatında bir asal sayı ve n pozitif tamsayı olmak üzere, $x^2 + y^2 = p^n$ denkleminin doğal sayılardaki çözüm sayısına A_n diyelim. $A_1 = 2$ ve $A_2 = 4$ olmak üzere,

$$A_n = \frac{(-1)^n + 3}{2} + n \text{'dir.}$$

İspat: x ve y aralarında asal olmak üzere ve $x^2 + y^2 = p^n$ denklemini sağlayan (x, y) çiftlerinin sayısına B_n diyelim. Önce B_n dizisinin terimlerini bulalım. x ve y aralarında asal olduğu için herhangi biri 0 olamaz. Genelliği bozmadan $x > y > 0$ olsun. Şimdi şartı sağlayan (x, y) ve (y, x)'den farklı bir (a, b) ikilisi olamayacağını gösterelim. (a, b) çözüm ise (b, a) da çözüm olacağından genelliği bozmadan $b < a < \sqrt{p^n},\ y < x < \sqrt{p^n}$ diyelim. $a \equiv br(mod\ p^n)$ olsun.

$$a \equiv br(mod\ p^n) \Longrightarrow a^2 \equiv b^2 r^2 (mod\ p^n) \Longrightarrow a^2 + b^2 \equiv b^2(1 + r^2) \equiv 0(mod\ p^n)$$

$$\Longrightarrow r^2 \equiv -1(mod\ p^n)$$

olur. Şimdi bu denklemin p^n modunda sadece 2 çözümü olduğunu gösterelim. r ve $p^n - r$ dışında bir t sayısının da bu denklemi sağladığını farzedelim.

$$r^2 \equiv t^2 \equiv -1(mod\ p^n) \Longrightarrow (r - t)(r + t) \equiv 0(mod\ p^n)$$

$r^2 \equiv t^2 \equiv -1(mod\ p^n)$ olduğundan r ve t, p'ye bölünemez. Dolayısıyla $(r - t)$ ve $(r + t)$ aynı anda p'ye bölünemez. Dolayısıyla $(r - t)$ ve $(r + t)$'den en az biri 0 olmalıdır. Fakat bu r ve $p^n - r$ dışında bir t sayısı seçmemizle çelişir. Dolayısıyla $r^2 \equiv -1(mod\ p^n)$ denklemin p^n modunda sadece 2 çözümü vardır.

Dolayısıyla $x \equiv yr(mod\ p^n)$ veya $x \equiv -yr(mod\ p^n)$ olacaktır. Teorem 2'in i şıkkında yaptığımız ispatta p'nin, tek olmasını, $r^2 \equiv -1(mod\ p)$ denkleminin p modunda 2 çözümü olmasını ve $b < a < \sqrt{p},\ y < x < \sqrt{p}$ kabulunu kullanmıştık. Aynı şartları p^n'de sağladığı için aynı işlemleri p^n 'ye uygulayarak ispatı yapabiliriz.

Dolayısıyla eğer x ve y aralarında asal olmak üzere ve $x^2 + y^2 = p^n$ denklemini sağlayan (x, y) çifti varsa (x, y) ve (y, x) çözümlerinden dolayı $B_n = 2$ olur. Şimdi aralarında asal en az 1 çözümü olduğunu tümevarım ile gösterelim.

$n = 1$ için x ve y aralarında asal olmak zorunda olduğundan doğrudur.

$n = 2$ için denklemin köklerinden $a^2 + b^2 = p$ olmak üzere, $(x, y) = (a^2 - b^2, 2ab)$'yi inceleyelim.

$$EBOB(a, b) = EBOB(a^2 - b^2, 2a) = EBOB(a^2 - b^2, 2b) = EBOB(a^2 - b^2, 2ab) = 1$$

olduğundan $n = 2$ için de doğrudur. Şimdi $n = 1,2, \dots, k-1$ için doğru olduğunu kabul edip $n = k$ için ispatlayalım.

$EBOB(a,b) = EBOB(c,d) = 1$ ve $a^2 + b^2 = p$, $c^2 + d^2 = p^{k-1}$ olsun.

$$p^k = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2$$

olduğunu biliyoruz. $x^2 + y^2 = p^k$ denkleminde $(x,y) = (ac + bd, ad - bc)$ ve $(x,y) = (ad + bc, ac - bd)$ çözümlerinden en az birinin aralarında asal çözümler olduğunu gösterelim. Aksini varsayalım, bu durumda $EBOB$ değeri p^m formatında olması gerekir.

$$EBOB(ac + bd, ad - bc) = EBOB\big(ac + bd, a(ac + bd) - b(ad - bc)\big) = EBOB(ac + bd, cp)$$

$$EBOB(ad + bc, ac - bd) = EBOB\big(ac - bd, b(ad + bc) + a(ac - bd)\big) = EBOB(ac - bd, cp)$$

olur. $EBOB(c,p) = 1$ olduğundan $EBOB(ac + bd, cp) = p$ olmalı. Benzer şekilde $EBOB(ac - bd, cp) = p$ olur. Buradan,

$$ac - bd \equiv ac + bd \equiv 0 (mod\ p) \Longrightarrow ac \equiv bd \equiv 0 (mod\ p)$$

bulunur. Dolayısıyla a, b, c ve d'den birisi p'ye bölünmeli fakat bu kabulumüze aykırıdır. Çelişki

Yani $(x,y) = (ac + bd, ad - bc)$ ve $(x,y) = (ad + bc, ac - bd)$ çözümlerinden en az birinin aralarında asal olması gerekir. Dolayısıyla her n pozitif tamsayısı için $B_n = 2$'dir.

$x^2 + y^2 = p^n$ için, eğer x ve y aralarında asal değilse, $p | EBOB(x,y)$ olur. $x = x_1 p$ ve $y = y_1 p$ diyelim. Denklem,

$$x_1^2 + y_1^2 = p^{n-2}$$

olur. Bu denkleminde çözüm sayısı A_{n-2}'dir. Dolayısıyla her n pozitif tamsayısı için,

$$A_n = A_{n-2} + B_n = A_{n-2} + 2$$

sağlar. Ayrıca $A_1 = 2$ ve $A_2 = 4$ olduğunu Teorem 2'de göstermiştik.

$$A_n - A_{n-2} = A_{n-1} - A_{n-3} = 2 \Longrightarrow A_n - A_{n-1} - A_{n-2} + A_{n-3} = 0$$

olur. Bu dizinin karakteristik denklemini çıkaralım.

$$x^3 - x^2 - x + 1 = (x-1)^2 (x+1) = 0$$

bulunur. Buradan dizinin genel terimi,

$$A_n = A + Bn + C(-1)^n$$

bulunur. $A_1 = 2, A_2 = 4, A_3 = 4$ olduğunu biliyoruz. n yerine sırasıyla 1,2,3 yazarsak,

$$A + B - C = 2$$

$$A + 2B + C = 4$$

$$A + 3B - C = 4$$

denklemlerini elde ederiz bu denklemleri çözersek $A = \frac{3}{2}$, $B = 1$, $C = \frac{1}{2}$ bulunur. Yerine yazarsak genel denklem,

$$A_n = \frac{(-1)^n + 3}{2} + n$$

olur.

Teorem 4: $p_1, p_2, \dots, p_k$ sayıları $4k + 1$ formundaki asal sayılar ve $\alpha_1, \alpha_2, \dots, \alpha_k$ pozitif tamsayılar olmak üzere, $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}$ ise,

$$x^2 + y^2 = n$$

denkleminin aralarında asal çözüm sayısı 2^k'dır.

İspat: Aralarında asal çözüm sayısı S_k olsun. Öncelikle denklemi modüler aritmetik kullanarak düzenleyelim,

$$x^2 + y^2 \equiv 0\ (mod\ n) \implies \left(\frac{x}{y}\right)^2 \equiv -1 (mod\ n)$$

$\frac{x}{y} \equiv r\ (mod\ n)$ diyelim. $r^2 \equiv -1 (mod\ n)$ denkliğinin çözüm sayısına bakalım. r ve n ile aralarında asaldır. t, bu denkliğin bir çözümü olsun.

$$r^2 - t^2 \equiv (r - t)(r + t) \equiv 0\ (mod\ n)$$

olur. n'yi bölen her asal sayı ya $(r - t)$ ya da $(r + t)$ ifadesini bölmelidir. İkisini birden bölemez çünkü bu durumda $(r - t) + (r + t) = 2r$ değerinin de bu asal sayı ile bölünmesi gerekir fakat bu r ve n 'nin aralarında asal olmasıyla çelişir. Asal sayı ikisini birden bölemediğinden asal sayının kuvvetlerini parçalayamayız, yani $i = 1,2, \dots, k$ için

$$\text{ya } \frac{r}{t} \equiv 1 \left(mod\ p_i^{\alpha_i}\right) \text{ ya da } \frac{r}{t} \equiv -1 \left(mod\ p_i^{\alpha_i}\right)$$

olmalıdır. k farklı durumun her biri için 2 seçenek olduğundan toplamda 2^k durum olur. Her durumda Çin kalan teoreminden farklı bir $\frac{r}{t}$ değeri buluruz. Dolayısıyla,

$$r^2 \equiv -1 (mod\ n)$$

denkliğinin t cinsinden çözümleri yazarsak 2^k çözüm bulunur. Şimdi her r çözümü için $\frac{x}{y} \equiv r\ (mod\ n)$ ise ana denklemin doğal sayılarda en fazla bir çözümü olabileceğini gösterelim. n tek olduğundan $x = y$ olamaz ve (x, y) çözüm ise (y, x) de çözüm olacağından $x > y$ kabul edebiliriz. $a > b$, $c > d$ ve $(a, b) \neq (c, d)$ ikilileri için $\frac{a}{b} \equiv \frac{c}{d}\ (mod\ n)$ ve $a^2 + b^2 = c^2 + d^2 = n$ olsun. Genelliği bozmadan $a > c$ olsun, bu durumda $\sqrt{n} > a > c > d > b > 0$ olur. $\frac{a}{b} \equiv \frac{c}{d} \equiv m\ (mod\ n)$ diyelim.

$$a \equiv bm\ (mod\ n)$$

$$c \equiv dm\ (mod\ n)$$

$$\Longrightarrow (a-c) \equiv (b-d)m\ (mod\ n)\ \Longrightarrow (a-c)^2 + (b-d)^2 \equiv 0\ (mod\ n)$$

$\sqrt{n} > a > c > d > b > 0$ olduğundan $\sqrt{n} > |a-c| > 0$ ve $\sqrt{n} > |b-d| > 0$ olur. Buradan,

$$2n > (a-c)^2 + (b-d)^2 > 0 \Longrightarrow (a-c)^2 + (b-d)^2 = n$$

olur. Bu denklemi açarsak $a^2 + b^2 + c^2 + d^2 - 2ac - 2bd = 2n - 2ac - 2bd = n$ bulunur fakat denklemin sol tarafı çiftken sağ tarafı tek olduğundan çelişki olur. Dolayısıyla $r^2 \equiv -1(mod\ n)$ olan her r için ana denklemin en fazla 1 çözümü olabilir. $r^2 \equiv -1(mod\ n)$ denkliğinin 2^k çözümü olduğundan ana denklemin aralarında asal çözüm sayısı en fazla 2^k olabilir. Yani $S_k \leq 2^k$ 'dır.

Şimdi de tümevarım kullanarak $S_k \geq 2^k$ olduğunu gösterelim. n sayısının $4t+1$ formunda tek asal çarpanı varsa aralarında asal çözüm sayısının 2 olduğunu göstermiştik, $k-1$ asal çarpanı için doğru olsun ve k asal çarpan için ispatlayalım. $x^2 + y^2 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{k-1}^{\alpha_{k-1}}$ denkleminin aralarında asal çözümlerinin sayısına s diyelim ve çözümler $(a_1, b_1), (a_2, b_2), \dots, (a_s, b_s)$ olsun. $x^2 + y^2 = p_k^{\alpha_k}$ denkleminin aralarında asal çözümleri (a, b) ve (b, a) olsun. $i = 1,2, \dots, s$ için

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = (a_i^2 + b_i^2)(a^2 + b^2) = (a_i a + b_i b)^2 + (a_i b - b_i a)^2 = (a_i a - b_i b)^2 + (a_i b + b_i a)^2$$

olur. Bu $(a_i a + b_i b, a_i b - b_i a), (a_i a - b_i b, a_i b + b_i a)$ çözümlerinin aralarında asal olduğunu gösterelim, Eğer değillerse karelerinin toplamı $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ olduğundan $EBOB$'ları $p_1, p_2, \dots, p_k$ asal sayılarından en az birine bölünür. Bölündüğü asal sayılardan biri p_k ise

$$EBOB((a_i a + b_i b)\,, (a_i b - b_i a)) = EBOB\big((a_i a + b_i b)\,, b_i(a_i a + b_i b) + a_i(a_i b - b_i a)\big)$$

$$= EBOB((a_i a + b_i b), b(a_i^2 + b_i^2))$$

olur. $a_i^2 + b_i^2$ ile b değerleri p_k ile aralarında asal olduğundan $EBOB$, p_k'ya bölünemez. Başka bir asala bölünsün, bu asala p diyelim. p, $a_i^2 + b_i^2$ ifadesini böler.

$$EBOB((a_i a + b_i b)\,, (a_i b - b_i a)) = EBOB\big((a_i a + b_i b)\,, a(a_i a + b_i b) + b(a_i b - b_i a)\big)$$

$$= EBOB((a_i a + b_i b), a_i(a^2 + b^2))$$

olur. Benzer şekilde $a^2 + b^2$ ve a_i, p ile aralarında asal olduğundan p, $EBOB$'u bölemez, dolayısıyla $((a_i a + b_i b)\,, (a_i b - b_i a))$ ikilisi aralarında asaldır. Benzer şekilde $((a_i a - b_i b)\,, (a_i b + b_i a))$ ikilisinin de aralarında asal olduğu bulunabilir.

Eğer hiçbir farklı $i = 1,2, \dots, s$ değeri için $(a_i a + b_i b, a_i b - b_i a), (a_i a - b_i b, a_i b + b_i a)$ ve permütasyonları çakışmıyorsa $S_k \geq 2s = 2S_{k-1} \geq 2^k$ olacaktır. Şimdi bunu göstermeliyiz. n tek sayı olduğundan $(x, y) = (y, x)$ olamayacağını biliyoruz, dolayısıyla bu durumları incelemeye gerek yok.

$j \in \{1,2, \dots, s\}$ ve $i \neq j$ olan bir j için,

i) $(a_i a + b_i b, a_i b - b_i a) = (a_i a - b_i b, a_i b + b_i a)$ ise $bb_i = 0$ bulunur fakat bunun olamayacağını biliyoruz. Çelişki.

ii) $(a_i a + b_i b, a_i b - b_i a) = (a_i b + b_i a, a_i a - b_i b)$ ise

$$a_i b - b_i a = a_i a - b_i b \implies b(a_i + b_i) = a(a_i + b_i) \implies a = b$$

bulunur. Çelişki.

iii) $(a_i a + b_i b, a_i b - b_i a) = (a_j a + b_j b, a_j b - b_j a)$ ise

$$a_i a + b_i b = a_j a + b_j b \implies \frac{a}{b} = \frac{b_j - b_i}{a_i - a_j}$$

$$a_i b - b_i a = a_j b - b_j a \implies \frac{a}{b} = \frac{a_i - a_j}{b_i - b_j}$$

İki denklemi birleştirirsek $\frac{a}{b} = -\frac{b}{a}$ bulunur. Çelişki.

Benzer şekilde diğer durumlardan da çelişki bulunur.

Dolayısıyla hiçbir farklı $i = 1,2, \dots, s$ değeri için $(a_i a + b_i b, a_i b - b_i a), (a_i a - b_i b, a_i b + b_i a)$ ve permütasyonları çakışmaz. Bu durumda $S_k \geq 2^k$ olur. Hem $S_k \geq 2^k$ hem de $S_k \leq 2^k$ olduğundan $S_k = 2^k$ olmalıdır. Böylece $x^2 + y^2 = n$ denkleminin aralarında asal çözüm sayısının 2^k olduğunu göstermiş oluruz.

Teorem 5: $p_1, p_2, \dots, p_k$, $4t + 1$ formunda farklı asal sayılar ve $\alpha_1, \alpha_2, \dots, \alpha_k$ pozitif tam sayı olsun.

$$x^2 + y^2 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

denkleminin doğal sayılarda çözüm sayısı,

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1) + \frac{1-(-1)^{(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}\text{'dir.}$$

İspat: $\alpha_1, \alpha_2, \dots, \alpha_k$ sayılarını tekler ve çiftler olarak ayıralım. Tek olanlar, $m_1, m_2, \dots, m_t$ ve çift olanlar $n_1, n_2, \dots, n_s$ olsun. Burada $t + s = k$ 'dır. $EBOB(x, y) = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ olsun. $x = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} x_1$ ve $y = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} y_1$ yazarsak $EBOB(x_1, y_1) = 1$ ve

$$x_1^2 + y_1^2 = p_1^{\alpha_1 - 2\beta_1} p_2^{\alpha_2 - 2\beta_2} \dots p_k^{\alpha_k - 2\beta_k}$$

olur. $i = 1,2, \dots, k$ için

$$\frac{\alpha_i}{2} \geq \beta_i \geq 0\text{'dır.}$$

β_i değerlerinin hepsi $\frac{\alpha_i}{2} > \beta_i \geq 0$ aralığında olduğunda k farklı asal bölen olacağından her durumda 2^k çözüm olur. β_i, bu aralıkta $\left[\left[\frac{\alpha_i+1}{2}\right]\right]$ farklı değer alır. Dolayısıyla bu durumdan,

$$2^k\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]=2^k\left(\prod_{i=1}^{t}\left[\!\left[\frac{m_i+1}{2}\right]\!\right]\right)\left(\prod_{j=1}^{s}\left[\!\left[\frac{n_j+1}{2}\right]\!\right]\right)=\left(\prod_{i=1}^{t}(m_i+1)\right)\left(\prod_{j=1}^{s}n_j\right)$$

çözüm gelir. Eğer α_i'lerden hiçbiri çift değilse başka bir durum olmayacağından tüm durum bu olacaktır ve bu ifadeyi düzenlersek,

$$2^k\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]=\left(\prod_{i=1}^{k}(\alpha_i+1)\right)=\left(\prod_{i=1}^{k}(\alpha_i+1)\right)+\frac{1-(-1)^{\left(\prod_{i=1}^{k}(\alpha_i+1)\right)}}{2}$$

olur. Eğer α_i'lerden en az biri çiftse fakat hepsi birden çift değil ise, sırasıyla çift kuvvetleri ele alırsak, çözüm sayısı,

$$2^k\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]+\left(\frac{2^{k-1}\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]}{\left[\!\left[\frac{n_1+1}{2}\right]\!\right]}+\frac{2^{k-1}\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]}{\left[\!\left[\frac{n_2+1}{2}\right]\!\right]}+\cdots+\frac{2^{k-1}\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]}{\left[\!\left[\frac{n_s+1}{2}\right]\!\right]}\right)$$

$$+\left(\frac{2^{k-2}\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]}{\left[\!\left[\frac{n_1+1}{2}\right]\!\right]\left[\!\left[\frac{n_2+1}{2}\right]\!\right]}+\frac{2^{k-2}\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]}{\left[\!\left[\frac{n_1+1}{2}\right]\!\right]\left[\!\left[\frac{n_3+1}{2}\right]\!\right]}+\cdots+\frac{2^{k-2}\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]}{\left[\!\left[\frac{n_{s-1}+1}{2}\right]\!\right]\left[\!\left[\frac{n_s+1}{2}\right]\!\right]}\right)+\cdots$$

$$+\frac{2^{k-s}\prod_{i=1}^{k}\left[\!\left[\frac{\alpha_i+1}{2}\right]\!\right]}{\left[\!\left[\frac{n_1+1}{2}\right]\!\right]\left[\!\left[\frac{n_2+1}{2}\right]\!\right]\ldots\left[\!\left[\frac{n_s+1}{2}\right]\!\right]}$$

$$=\left(\prod_{i=1}^{t}(m_i+1)\right)\left(\prod_{j=1}^{s}n_j\right)\left(1+\frac{1}{n_1}+\frac{1}{n_2}+\cdots+\frac{1}{n_1n_2\ldots n_s}\right)$$

$$=\left(\prod_{i=1}^{t}(m_i+1)\right)\left(\prod_{j=1}^{s}n_j\right)\left(1+\frac{1}{n_1}\right)\left(1+\frac{1}{n_2}\right)\ldots\left(1+\frac{1}{n_s}\right)$$

$$=\left(\prod_{i=1}^{t}(m_i+1)\right)\left(\prod_{j=1}^{s}(n_j+1)\right)=\prod_{i=1}^{k}(\alpha_i+1)=\left(\prod_{i=1}^{k}(\alpha_i+1)\right)+\frac{1-(-1)^{\left(\prod_{i=1}^{k}(\alpha_i+1)\right)}}{2}$$

olur. Eğer $s=k$ ise, yani tüm kuvvetler çift ise $x^2+y^2=1$ denkleminin çözüm sayısı 2^0 değil, 2 olduğundan çözüm sayısı elde ettiğimiz formülden 1 fazladır. Dolayısıyla bu durumda toplam çözüm sayısı,

$$\left(\prod_{i=1}^{t}(m_i+1)\right)\left(\prod_{j=1}^{s}(n_j+1)\right)+1=\left(\prod_{i=1}^{k}(\alpha_i+1)\right)+1=\left(\prod_{i=1}^{k}(\alpha_i+1)\right)+\frac{1-(-1)^{\left(\prod_{i=1}^{k}(\alpha_i+1)\right)}}{2}$$

olur. Yani her durumda toplam çözüm sayısı,

$\left(\prod_{i=1}^{k}(\alpha_i+1)\right)+\frac{1-(-1)^{\left(\prod_{i=1}^{k}(\alpha_i+1)\right)}}{2}$'dir.

Teorem 6: $p_1, p_2, \dots, p_k$, $4t+1$ formunda farklı asal sayılar ve $a, \alpha_1, \alpha_2, \dots, \alpha_k$ pozitif tam sayı olsun.

$$x^2+y^2=2^a p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

denkleminin doğal sayılarda çözüm sayısı,

$$(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)+\frac{1-(-1)^{(a+1)(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}$$'dir.

İspat: $n=2^a p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ olsun. $a \geq 2$ için $4|n$ olur. $x^2+y^2 \equiv 0\ (mod\ 4)$ olması için x ve y çift olmalıdır. $x=2x_1$ ve $y=2y_1$ dersek,

$$x_1^2+y_1^2=2^{a-2} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

olur. Benzer şekilde ilerlersek a çift ise bu işlemi $\frac{a}{2}$ defa uygularsak,

$$x_{\frac{a}{2}}^2+y_{\frac{a}{2}}^2=p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

olur. Bu denklemin Teorem 5'den $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)+\frac{1-(-1)^{(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}$ çözümü vardır. a çift olduğundan,

$$\frac{1-(-1)^{(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}=\frac{1-(-1)^{(a+1)(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}$$

olacaktır. Dolayısıyla çözüm sayısı

$$(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)+\frac{1-(-1)^{(a+1)(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}$$

olur. Eğer a tek ve $\alpha_1, \alpha_2, \dots, \alpha_k$ sayılarının hepsi birden çift değilse, $a=2k+1$ için, çözümün başında x ve y'nin çift olmasında uyguladığımız işlemi k defa uygularsak,

$$x_k^2+y_k^2=2p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

olur. Bu denklemde genelliği bozmadan $x_k > y_k$ için (x_k, y_k) ikilisinin birisi tek, diğeri çift olamayacağından,

$$x_k=e+f$$

$$y_k=e-f$$

olacak şekilde $e>f$ doğal sayıları vardır. Denklemde yerine yazarsak,

$$e^2+f^2=p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

bulunur. Bu denklemin tüm çözümlerini çözüm sayısının

$$(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)+\frac{1-(-1)^{(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}$$

olduğunu gösterdiğimizden $x_k^2+y_k^2=2p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ denkleminin çözüm sayısı da

$$(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)+\frac{1-(-1)^{(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}$$

olur. $\alpha_1,\alpha_2,\dots,\alpha_k$ sayılarının hepsi birden çift olmadığından

$$\frac{1-(-1)^{(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}=\frac{1-(-1)^{(a+1)(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}=0$$

olacaktır. Dolayısıyla çözüm sayısı

$$(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)+\frac{1-(-1)^{(a+1)(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}\text{,dir.}$$

Eğer a tek ve $\alpha_1,\alpha_2,\dots,\alpha_k$ sayılarının hepsi birden çift ise bir önceki durumun aynısını yaparsak sadece $(x_k,y_k)=\left(\sqrt{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}},\sqrt{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}}\right)$ durumunda simetriği kendisi olacağından bir çözüm azalacaktır, bu durumda da $\alpha_1,\alpha_2,\dots,\alpha_k$ sayılarının hepsi birden çift olduğundan

$$\frac{1-(-1)^{(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}-1=\frac{1-(-1)^{(a+1)(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}=0$$

olacağından çözüm sayısı

$$(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)+\frac{1-(-1)^{(a+1)(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}$$

olacaktır. Tüm durumlarda çözüm sayısı aynı olduğundan, çözüm sayısı

$$(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)+\frac{1-(-1)^{(a+1)(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)}}{2}$$

olacaktır.

Kaynakça

Bates, M. (tarih yok). *Primes of the form x2+ny2.*

Cox, D. A. (1989). *Primes of the Form x2+ny2: Fermat, Class Field Theory, and Complex Multiplication.* New York: Wiley-Interscience Publication.

Hagedorn, T. R. (tarih yok). *Primes Of The Form x2 + ny2 And The Geometry Of (Convenient) Numbers*

B. Spearman, K. S. Williams, Representing Primes by Binary Quadratic Forms, American Mathematical Monthly, 99(5) (1992), pp. 423-426

I. Stewart, D. Tall, Algebraic Number Theory and Fermat's Last Theorem, 3rd Ed., A.K. Peters, Natick, MA 2001.

A. Weil, Number Theory: An Approach Through History, Birkha¨user, Boston, Basel, and Stuttgart, 1984.

P.J. Weinberger, Exponents of the class groups of complex quadratic fields, Acta Arith. 22 (1973), pp. 117–124..