Sadık Eyidoğan

Waring Problemi ve Ramanujan Çember Metodu

#İçerik#

Ram Murty - Intro to Circle Method

1. Waring probleminin özel durumları:
   - → Langrange teoremi
   - → $g(3)$ ve $g(4)$ hakkında kısa bilgiler
2. Waring yapısı
   - → Pillar ve Dickson formülleri
   - → Roth_Ridout Teoremi ve sonucu
   - → ABC sanısı ve sonucu
3. Waring Sanısı
   - → Schnirelmann Yoğunluğu
   - → Linnik'in İspatı
4. Eksponensiyel Toplamlar ve Çember Metodu.

Chapter 1: Waring Problemine Giriş.

Diophantus: Her pozitif tam sayı, en fazla 4 tane tam kare (karesel) sayının toplamı şeklinde yazılabilir mi?

→ Langrange (1770), Diophantus'un sorusunu olumlu olarak cevaplıyor.

→ Edwar Waring: Verilen bir $k \geq 3$ tam sayısı için her pozitif tam sayı belirli sayıda pozitif tam sayıların k-kuvvetinin toplamı şeklinde yazılabilir mi? (Waring Sanısı after the publication of the book "Meditationes Algebraicae. 1787).

Matris Eşitliği Üzerine.

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -(bc+ad) \\ bc-ad & ac-bd \end{bmatrix} \Rightarrow (a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (bc+ad)^2$$

Eğer m ve n iki tam sayının karesi şeklinde yazılabiliyorsa, $m \cdot n$'de iki tam sayının karesi şeklinde yazılabilir.

Teorem 1. $p>2$ asal olmak üz. p iki tam sayının karesinin toplamı şeklinde yazılabilir $\Leftrightarrow$ $p \equiv 1 \pmod 4$.

İspat.

$(\Rightarrow)$ $p>2$ olsun ve $p=a^2+b^2$. $\forall a \in \mathbb{Z}$ için $a^2 \equiv 0,1 \pmod 4$

$$a^2+b^2 \equiv \cancel{0}, 1 \text{ veya } \cancel{2} \pmod 4$$

$$p \equiv 1 \bmod 4$$

$(\Leftarrow)$ **Lemma 2.** $p>2$ asal sayısı için $x^2 \equiv -1 \pmod p$ çözümü mevcut ancak ve ancak $p \equiv 1 \pmod 4$.

Proof. H.W.

Şimdi $p \equiv 1 \pmod 4$ olsun. Lemma 2'den kaynaklı biliyoruz ki $x^2 \equiv -1 \pmod p$ çözümü mevcut. Çözümü $1 \le x \le p-1$ aralığında çözelim. O zaman $p \cdot m = x^2+1$, $\exists m \in \mathbb{N}$ mevcut.

$$p \cdot m = x^2+1 \le (p-1)^2+1 < p^2 \Rightarrow m<p \text{ olmalı}$$

Eğer $F := \{ m \in \mathbb{N} \mid m<p$ ve $m \cdot p$ iki küresel sayının toplamı şeklinde yazılabilir $\}$,

$F \neq \emptyset$.

Diyelim ki F'nin minimum elemanı m_0 olsun.

İddia: $m_0 = 1$

$m_0 > 1$ olsun. $p \cdot m_0 = x_0^2+y_0^2$ yazılır. $x_0 \equiv x_1 \pmod{m_0}$
$(m_0 \in F)$ $\qquad y_0 \equiv y_1 \pmod{m_0}$

Böylelikle $|x_1|, |y_1| \le m_0/2$ olacak şekilde x_1 ve y_1 var.

$x_1 = y_1 = 0$ olamaz. $m_0 \mid x_0$ ve $m_0 \mid y_0$ $\quad m_0^2 \mid x_0^2+y_0^2 = m_0 p \Rightarrow m_0 \mid p$ çelişki.

Bu durumda $\exists m_1 \in \mathbb{N}$ var ki $x_1^2+y_1^2 = m_0 m_1$ sağlanır ve $m_1 \le m_0/2$.

$$\left(x_1^2+y_1^2 \leq \frac{m_0^2}{4} + \frac{m_0^2}{4} = \frac{m_0}{2} = m_0 \frac{m_0}{2}\right)$$

Böylece, $p.m_0$ ve $m_0 m_1$' in durumlarından

$$(p.m_0)(m_0 m_1) = (x_0^2+y_0^2)(x_1^2+y_1^2)$$
$$= (x_0 x_1 + y_0 y_1)^2 + (x_1 y_0 - x_0 y_1)^2 \quad \text{Lemma 1.2.}$$

$$x_0 x + y_0 y_1 \equiv x_0^2 + y_0^2 \equiv 0 \pmod{m_0}$$
$$x_1 y_0 - x_0 y_1 \equiv 0 \pmod{m_0}$$

Burada şunu söyleyebiliriz $p\, m_1 = \underbrace{\left(\frac{x_0 x_1 + y_0 y_1}{m_0}\right)^2}_{\in \mathbb{Z}} + \underbrace{\left(\frac{x_1 y_0 - x_0 y_1}{m_0}\right)^2}_{\in \mathbb{Z}}$

yani $m_1 \in \mathcal{F}$ olur bu ise m_0'ın minimal oluşuyla çakışır. Burada $p \equiv 1 \pmod 4$ iki karesel sayının toplamı şeklinde yazılabilir.

Langrange Teoremi. Her pozitif tam sayı 4 tane karesel sayının toplamı şeklinde yazılır.

$$\begin{bmatrix} a & -\bar{b} \\ b & \bar{a} \end{bmatrix}\begin{bmatrix} c & -\bar{d} \\ d & \bar{c} \end{bmatrix} = \begin{bmatrix} ac-\bar{b}d & -\overline{(bc+\bar{a}d)} \\ bc+\bar{a}d & \overline{(ac-\bar{b}d)} \end{bmatrix}$$

"Quaternion"

matris eşitliğinden

$$(a,b,c,d \in \mathbb{C}) \quad (|a|^2+|b|^2)(|c|^2+|d|^2) = |ac-\bar{b}d|^2 + |bc+\bar{a}d|^2$$

elde edilir.

Bu eşitlikten eğer m ve n iki tam sayısı, 4 tane karesel sayının toplamı şeklinde yazılabiliyorsa $m.n$ de yazılabilir sonucu çıkar.

Lemma 3. $p>2$ asal sayısı için öyle bir $0 \leq x,y \leq \frac{p-1}{2}$ tam sayıları vardır ki $x^2+y^2+1 \equiv 0 \pmod p$. (Lemmalar ilk 5 chapterında inceleniyor)

Langrange Teoremi İspatı. (1770)

$$\mathcal{F} = \{ m \in \mathbb{N} : m < p \text{ ve } pm \text{ dört karesel sayının toplamı şeklinde yazılsın} \}$$

Lemma 1.3 kullanarak $x^2+y^2+1 = p.m$ olduğunu biliyoruz.

$\left(0 \leq x,y \leq \frac{p-1}{2}\right)$ değerleri mevcut olduğundan $\mathcal{F} \neq \emptyset$, $\mathcal{F}$'nin minimum eleman m_0 olsun.

$m_0 > 1$ olsun. $m_0 \in F$ oldugundan $m_0 p = x^2+y^2+z^2+w^2$ seklinde yazılabilir. O zaman

- x, y, z, w her biri cift olamaz.

$$\frac{m_0}{4} \cdot p = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2 + \left(\frac{w}{2}\right)^2$$ olacagından m_0'nın minimalliği ile celişir.

- x, y, z, w her biri tek olamaz.

$$\frac{m_0}{4} \cdot p = \underbrace{\left(\frac{x+y}{2}\right)^2}_{\in \mathbb{Z}} + \underbrace{\left(\frac{x-y}{2}\right)^2}_{\in \mathbb{Z}} + \underbrace{\left(\frac{z+w}{2}\right)^2}_{\in \mathbb{Z}} + \underbrace{\left(\frac{z-w}{2}\right)^2}_{\in \mathbb{Z}} \quad \text{↯} \ (m_0 \text{ minimalliği ile})$$

- Benzer düşünce ile x, y, z, w'nın iki tek ikisi cift olamaz.
- O halde x, y, z, w'nın 3'ü tek veya 1'i tek olmalı. Bu durumda $p \cdot m_0$ tek olur.

Modüler aritmetik özelliginden dolayı

$|x_0|, |y_0|, |z_0|, |w_0| < m_0/2$ degerleri var ki $x \equiv x_0$, $y \equiv y_0$, $z \equiv z_0$ ve $w \equiv w_0 \pmod{m_0}$. Buradan

$$x^2+y^2+z^2+w^2 \equiv x_0^2+y_0^2+z_0^2+w_0^2 \pmod{m_0}$$

Böylece $x^2+y^2+z^2+w^2 = m_0 \cdot m_1$ olacak sekilde $m_1 \in \mathbb{N}$ mevcut. Ve

$|x_0|, |y_0|, |z_0|, |w_0| < \frac{m_0}{2}$ oldugundan

$m_0 m_1 = x_0^2 + y_0^2 + z_0^2 + w_0^2 \leq m_0^2 = m_0 m_0 \Rightarrow m_1 < m_0$ olur. $m_1 = m_0$ olamaz.

Olsaydı, $m_0^2 \mid m_1$ ve $p = x^2+y^2+z^2+w^2 \Rightarrow m_0 \mid p$ ↯

O halde, $1 \leq m_1 \leq m_0$ olmalı. Bu durumda $(m_0 m_1)(m_0 p)$ degerine bakalım

$$m_0^2 (m_1 p) = (m_0 m_1)(m_0 p) = (x_0^2+y_0^2+z_0^2+w_0^2)(x^2+y^2+z^2+w^2)$$
$$= x_2^2 + y_2^2 + z_2 + w_2^2 \quad (\text{matris gözleminden})$$

Buradan $m_0 \mid x_2, y_2, z_2, w_2$ oldukları gösterilir ise

$$m_1 p = \left(\frac{x_2}{m_0}\right)^2 + \left(\frac{y_2}{m_0}\right)^2 + \left(\frac{z_2}{m_0}\right)^2 + \left(\frac{w_2}{m_0}\right)^2 \Rightarrow m_1 \in F \text{ olup}$$

m_0'ın minimalliği ile çelişir.

Sonuç: Langrange Teoremi

Waring Sanısı.

$k \geq 2$ doğal sayısı verilsin. Bu durumda öyle bir $g \in \mathbb{N}$ var mı ki her doğal sayı g tane negatif olmayan tam sayının k. kuvvetinin toplamı şeklinde, $n = x_1^k + x_2^k + \cdots + x_g^k \quad (x_i \in \mathbb{Z})$ yazılsın.

$k \geq 2$ değeri için minimum g değerini $g(k)$ olarak tanımlayalım. Langrange teoreminden $g(2) = 4$ olduğunu biliyoruz. Waring sanısı üzerinde düşünecek olursak:

1) $\forall k \geq 2$ için sonlu bir $g(k)$ değeri var mı?

2) Mevcut ise $g(k)$'yı veren formül mevcut mu?

3) $g(k)$ üzerine alt sınır ve üst sınır belirleyebilir miyiz?

* (1909) Arthur Wiefeich tarafından $g(3) = 9$ olduğu gösteriliyor. Wieferich ispatındaki eksiklik 3 yıl sonra Kimpner tarafından gideriliyor.

(Waring Problems on Cubes / Keila Leonard, 2024).

İspat. $N > 6^{10}$ olsun. Bu durumda

$$\begin{aligned} N &= a^3 + b^3 + 6^k q = a^3 + b^3 + 6^k(6\,8^{2k} + r) \\ &= a^3 + b^3 + 6^k(6\,8^{2k} + d^3 + 6m) \\ &= a^3 + b^3 + (2^k d)^3 + 6^k(6 \cdot 8^{2k} + 6m) \\ &= a^3 + b^3 + c^3 + 6A(A^2 + m) \qquad (A = 8^k,\ A^2 > m) \end{aligned}$$

şeklinde yazılır.

Lemma 1. A ve m negatif olmayan tam sayılar olup $m \leq A^2$ ve m üç sayının karesinin toplamı şeklinde yazılsın. Bu durumda $6A(A^2+m)$ sayısı 6 tane sayının kübünün toplamı şeklinde yazılır.

Minkowski → g(2) ve θ

İspat. $m = m_1^2 + m_2^2 + m_3^2$ olsun.

$$
\begin{aligned}
6A(A^2+m) &= 6A(A^2+m_1^2+m_2^2+m_3^2) \\
&= 6A^3 + 6Am_1^2 + 6Am_2^2 + 6Am_3^2 \\
&= \sum_{i=1}^{3} 2A(A^2+3m_i^2) \\
&= \sum_{i=1}^{3} (2A^3 + 6Am_i^2 + m_i^3 - m_i^3 + 3A^2m_i - 3A^2m_i) \\
&= \sum_{i=1}^{3} (A+m_i)^3 - (A m_i)^3
\end{aligned}
$$

$\Rightarrow$ 6 tane sayının kübünün toplamı şeklinde yazılır.

Sonuç olarak $g(3) = 9$. □

↑ $g(4) \leq 20$.

* (1986) (Balasubramanian ve ark.) → Deshouillers ve Dress $g(4) = 19$ olduğunu göstermek için Ramanujan çember methodu ve Vinogradov yaklaşımlarını kullanarak ispatlıyorlar.

$N < 10^{357}$, bilgisayar yardımı ile

$N > 10^{357}$, H.L. çember metodu + Vinogradov yaklaşımı

Theorem 2. $g(4) \leq 53$.

İspat.

$$
\begin{aligned}
(a^2+b^2+c^2+d^2) &= a^4+b^4+c^4+d^4+2a^2b^2+2a^2c^2+2a^2d^2+2b^2c^2 \\
&\quad + 2b^2d^2 + 2c^2d^2
\end{aligned}
$$

$$(a+b)^4 + (a-b)^4 = 2a^4 + 12a^2b^2 + 2b^4$$

$$
\begin{aligned}
6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(a+c)^4+(a-c)^4+(a+d)^4+(a-d)^4 + \\
&\quad + (b+c)^4 + (b-c)^4 + (b+d)^4 + (b-d)^4 + (c+d)^4 + (c-d)^4
\end{aligned}
$$

elde edilir. Bu durumda Langrange teoremini kullanarak $\forall x \in \mathbb{N}$ için $6x^2$ sayısının $\left(6x^2 = 6(a_x^2+b_x^2+c_x^2+d_x^2)^2\right)$ 12 tane sayının 4. kuvvet lerinin toplamı şeklinde yazılır.

Keyfi $n \geq 1$ doğal sayısı verilsin

$$n = 6b + r \quad , \quad 0 \leq r \leq 5$$

b için Langrange teoremi kullanılırsa

$$
\begin{aligned}
n &= 6 \cdot (x_b^2 + y_b^2 + z_b^2 + w_b^2) + r \\
&= \underbrace{6x_b^2 + 6y_b^2}_{\text{12 tane sayının dördüncü kuvvetinin toplamı}} + 6z_b^2 + 6w_b^2 + r
\end{aligned}
$$

$\Rightarrow g(4) \leq 53$ olduğu elde edilir.

n üzerinde biraz çalışırsa $g(4) \leq 50$ gösterilir.

k	1	2	3	4	6	7
	4	9	19	37	73	143

Waring Sanısı Genellemesi

Yeterince büyük her $n \gg$ tam sayı değeri belirli sayıda pozitif tam sayıların k. kuvvetlerinin toplamı şeklinde yazılabilir mi?

$k \geq 1$ için belirli sayıların minimumuna $G(k)$ diyelim. $G(k)$ fonksiyonuna neler söylenebilir?

Bilinen $G(k)$ değerleri:

k	2	3	4	5	6	7
$G(k)$	4	$4 \leq G(3) \leq 7$ öngörü $= 4$?	16	$6 \leq G(5) \leq 17$	$9 \leq G(6) \leq 24$	$8 \leq G(7) \leq 33$

Ayrıca, $\frac{g(k)}{G(k)}$ 'da bilinmiyor. Nasıl davranır? $G(k)$ üzerine üst sınırlar:

$G(k) \leq (k-2)2^{k-1}+5$ (Hardy–Littlewood)

$\leq 3 2 (k \log k)^2$
$\leq k(3\log k + 11)$ } Vinogradov

$\leq 2k(\log k + 2\log\log k + O(\log\log\log k))$ Vinogradov

$\leq 2k(\log k + \log\log k + O(1))$ Vaughan

Best $\leq k(\log k + \log\log k + O(1))$ Wooley

J.A Euler Sanısı (1772) $\forall k \geq 2$ için $g(k) = 2^k + \lfloor (\frac{3}{2})^k \rfloor - 2$ sağlanır.

J.A Euler, bu sanıyı $g(k)$ için alt sınır verme çabasıyla üretiliyor.

$3^k > 2^k q - 1$ eşitsizliğini sağlayan maksimum q değeri

$2^k \lfloor (\frac{3}{2})^k \rfloor - 1 < 2^k (\frac{3}{2})^k - 1 = 3^k - 1 < 3^k$

$q = \lfloor (\frac{3}{2})^k \rfloor$ olarak alalım.

$n = 2^k(q-1) + 2^k - 1 = \underbrace{(2^k + 2^k + \cdots + 2^k)}_{q-1} + \underbrace{(1+1+\cdots+1)}_{2^k-1}$