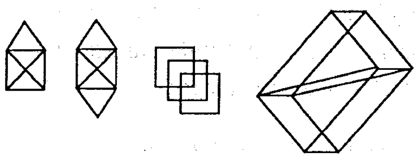
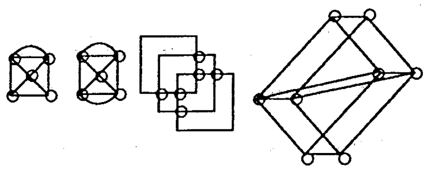
TEOREM: Bağlantılı bir grafın Euler grafı olabilmesi için gerek ve yeter şart bütün düğümlerdeki derecelerin çift olmasıdır.

TEOREM: Bağlantılı bir grafta sadece iki düğüm tek dereceli; diğerleri çift dereceli ise, tek dereceli düğümlerin birinden başlayıp diğerinde bitecek şekilde bir dolaşım vardır.

Bu teoremler yardımı ile düzlemde verilen bir şeklin, kalem kağıttan kaldırılmadan ve çizilen çizgilerin üzerinden gitmeden çizilip, çizilmeyeceği tayin edilebilir. Aşağıda verilen şekilleri ele alalım.

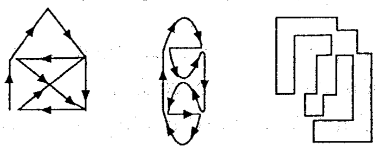


Bu şekillerden hangilerini kalemi kağıttan kaldırmadan ve çizdiğimiz çizgilerden tekrar geçmeden çizebiliriz? Önce bu şekilleri, düğüm ve kirişler daha belirgin olacak şekilde tekrar çiziyoruz.



G_1 G_2 G_3 G_4

G_1–de tek dereceli iki düğüm vardır. Bunların birisinden başlayıp diğerinde duracak şekilde, bu şekil çizilebilir G_2– ve G_3 de bütün düğümler çift dereceli olduğundan, her iki şekilde her hangi bir noktadan başlayıp, yine orda duracak şekilde çizilebilir. G_4 de ise tek dereceli dört düğüm olduğundan bu şekil çizilemez.



Devamı sayı 2'de

ÇİNLİLERİN KALAN TEOREMİ

İSMAİL Ş. GÜLOĞLU

Eski Çin bilgelerinden Yih-Ling (Ölümü 717)'den bize kadar gelebilen problemlerden birinin bugünkü matematik dilimiz ve gösterim tarzımızla ifadesi şudur:

$x \equiv 1 \quad (mod\ 2)$
$x \equiv 2 \quad (mod\ 5)$
$x \equiv 5 \quad (mod\ 6)$
$x \equiv 5 \quad (mod\ 12)$

kongrüans denklemlerinden oluşan sistemin ortak çözümleri kümesini bulunuz!

Yukarıdaki problemde x tamsayısı x≡5 (mod 12) şartını sağlarsa $x \equiv 5$ (mod 6) ve $x \equiv 1$ (mod 2) denklemleri de sağlanmış olacağı için soru

$x \equiv 2$ (mod 5)
$x \equiv 5$ (mod 12)

denklemlerinden oluşan sistemi çözmeğe denktir.

Bu yazımızın konusu olan meşhur Çinlilerin Kalan Teoremi bu sistemin en az bir çözümü olduğunu ifade eder.

Çinlilerin Kalan Teoremi: $m_1, m_2, \ldots, m_k$ *ikişer ikişer aralarında asal pozitif tamsayılar ve* $a_1, a_2, \ldots, a_k$ *herhangi tamsayılar ise*

$x \equiv a_1 \quad (mod\ m_1)$

$x \equiv a_2 \pmod{m_2}$

... ...

$x \equiv a_k \pmod{m_k}$

kongrüans denklemlerinden oluşan sistemin bir ortak çözümü vardır.

Ayrıca x tamsayısı bir çözüm ise y tamsayısının da bir çözüm olması için gerek ve yeter şart $M = m_1 . m_2 . \ldots . m_k$ için

$x \equiv y \pmod{M}$

olmasıdır; özel olarak verilen sistemin $0 < x \leq M$ koşullarına uyan tam bir tane çözümü vardır.

Bu teoremi anlamanızı sağlayacak ve ispatını yapmanızı kolaylaştıracak bir kaç ipucu verelim:

(i) $m_1, m_2, \ldots, m_k$ sayılarının en küçük ortak katı M olduğu için teoremin, çözümün tekliği hakkındaki ikinci kısmının doğruluğu kolayca görülebilir.

(ii) $a_1, a_1+m_1, a_1+2m_1, \ldots, a_1 + (m_2 - 1)m_1$ sayıları m_2 modülüne göre farklı kongrüans sınıflarındadırlar (Niçin?). Şu halde $a_1 + i\, m_1 \equiv a_2 \pmod{m_2}$ olacak şekilde bir için $0, 1, \ldots, m_2$ vardır. $x_1 = a_1 + i\, m_1$ dersek, $x_1, x_1 + m_1m_2, x_1 + 2m_1 m_2, \ldots, x_1 + (m_3-1)m_1m_2$ sayıları m_3 modülüne göre farklı kongrüans sınıflarındadırlar (Niçin?) Şu halde $x_2 = x_1 + j\, m_1m_2 \equiv a_3 \pmod{m_3}$ olacak şekilde j tamsayısı vardır ve

$x_2 \equiv a_3 \pmod{m_3}$

$x_2 \equiv x_1 \equiv a_2 \pmod{m_2}$

$x_2 \equiv x_1 \equiv a_1 \pmod{m_1}$

denklemleri sağlanır. Artık ispatı tamamlamayı okuyucuya bırakabiliriz.

Diğer bir ispat fikri şu gözleme dayanır: Herhangi bir $(a_1, a_2, \ldots, a_k)$ için çözümün varlığı problemi $(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, 0, \ldots 0, 1)$ özel durumlarında çözümün varlığına indirgenebilir, yani her $i = 1, \ldots,$ için

$x_i \equiv 1, \pmod{m_i}$ ve $x_i \equiv 0 \pmod{m_j}$, $j \neq i$

olacak şekilde bir x_i tamsayısı bulunabilirse,

$x = a_1x_1 + a_2x_2 + \ldots + a_k x_k$

sayısı verilen sistemin bir çözümü olur.

Diğer taraftan m_i ve $M_i = \frac{M}{m_i} = m_1m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$ tamsayıları aralarında asal oldukları için $u\, m_i + v\, M_i = 1$ olacak şekilde u ve v tamsayıları vardır. $x_i = v\, .\, M_i$ dersek $x_i \equiv 1 \pmod{m_i}$ ve $x_i \equiv 0 \pmod{m_j}$, $j \neq i$ elde edilir.

Çinlilerin Kalan Teoremi bazı özelliklere sahip uygun tamsayıların ve tamsayı dizilerinin varlığını göstermek için akıllıca kullanılabilir. Zaman zaman olimpiyat soruları arasında da böyle uygulamalara rastlanıyor.

Örnek 1: Her biri uygun bir tam sayının karesine bölünebilen 1000 tane ardışık tamsayı var mıdır?

Bir tamsayının karesine bölünebilme,bir asal sayının karesine bölünebilmeye denk olduğu için problem $p_i^2 \mid (N+i)$, $i = 1, \ldots, 1000$ olacak şekilde p_i asal sayıları ve N tamsayısının bulunup bulunamayacağını sormaktadır.

Sonsuz tane asal sayı olduğu için 1000 tane farklı asal sayı bulabiliriz. Bunları $p_1, p_2, \ldots, p_{1000}$ ile gösterelim ve $m_i = p_i^2$, $i = 1, \ldots, 1000$ diyelim. Aşikâr olarak m_i sayıları ikişer ikişer aralarında asaldırlar ve dolayısı ile Çinlilerin Kalan Teoremine göre

$x \equiv -1 \pmod{m1}$

$x \equiv -2 \pmod{m_2}$

... ...

$x \equiv -1000 \pmod{m_{1000}}$

denklemleri sağlanacak şekilde bir $x = N$ tamsayısı vardır. N+1, N+2, ... , N+1000 ardışık tamsayılarının her biri bir tam sayının karesine bölünür.

30. Uluslararası Matematik Olimpiyatları'nda (1989) şu soru sorulmuştur:

Örnek 2: Her pozitif n tam sayısı için hiç biri uygun bir asal sayının kuvveti olmayan n tane ardışık tamsayının bulunduğunu kanıtlayın.

Ve önerilen çözüm şu idi: $N = [(n+1)!]^2 + 1$ diyelim. Elbette her $j \in \{1, 2, \dots, n\}$ için $1+j$ sayısı $N+j$ nin bir bölenidir. Uygun bir j için $N+j$ bir p asal sayısının kuvveti olsa $1+j = p^r$ ve $N+j = p^s$ olacak şekilde r ve s pozitif tamsayıları bulunur. $r < s$ dir. $N+j = (1+j) + ((n+1)!)^2$ ve $p^{r+1} | [(n+1)!]^2$ olduğunda $p^{r+1} | (1+j)$ elde ederiz ki bu mümkün değildir. Şu halde $N+1, N+2, \dots, N+n$ ardışık tamsayıları istenen koşulu sağlayan bir dizi oluştururlar.

Çinlilerin Kalan Teoremi'nden istifade ile şöyle bir çözüm de verebiliriz:

Bir tamsayının bir asal sayının kuvveti olmaması demek en az iki farklı asal böleni bulunması demektir. 2n tane farklı asal sayı alalım. Bunları $p_1, p_2, p_3, \dots, p_{2n}$ ile gösterelim ve

$$m_i = p_{2i-1}\, p_{2i}, \qquad i = 1, 2, \dots, n$$

diyelim. m_i sayıları ikişer ikişer aralarında asaldırlar. Çinlilerin Kalan Teoremi'nden

$$\begin{aligned} N &\equiv -1 \pmod{m_1} \\ N &\equiv -2 \pmod{m_2} \\ &\dots \\ N &\equiv -n \pmod{m_n} \end{aligned}$$

olacak şekilde bir N (pozitif) tam sayısının bulunduğunu biliyoruz. $N+1, N+2, \dots, N+n$ istenen özelliklere sahip bir dizi olur.

Bu yazıyı, konuyu ne kadar kavradığınızı anlamanıza ve uygulamadaki becerinizi tanımanız ve geliştirmenize vesile olacak alıştırma ve problemlerle tamamlayalım.

Alıştırma 1.

$$\begin{aligned} 2x &\equiv 3 \pmod{5} \\ 3x &\equiv 4 \pmod{7} \\ 5x &\equiv 2 \pmod{11} \end{aligned}$$

sistemini sağlayan en küçük pozitif tamsayıyı bulunuz. Bu örnekten hareketle Çinlilerin Kalan Teoreminin daha genel olarak nasıl ifade ve ispat edilebileceğini düşününüz.

Alıştırma 2. m ve n pozitif tamsayılar, d ve e sırasıyla bunların en büyük ortak böleni ve en küçük ortak katı olsun. a ve b tamsayılar olmak üzere

$$x \equiv a \pmod{m} \text{ ve } x \equiv b \pmod{n}$$

denklemlerinin bir ortak çözümünün bulunması için gerek ve yeter şart

$$a \equiv b \pmod{d}$$

olmasıdır. Eğer bir çözüm varsa, $0 < x \le e$ koşulunu sağlayan tam bir tane çözüm vardır.

İspatlayın.

Problem 1. Her n pozitif tam sayısı için ardışık öyle n tane tamsayının bulunabileceğini gösterin ki bunların her biri için onu bölüp diğerlerini bölmeyen bir tamsayı bulunsun.

Problem 2. n ve d pozitif tamsayılar olsun. Ardışık terimleri arasındaki fark 2d ve uzunluğu n olan ve tek sayılardan oluşan öyle bir $a_1, a_2, \dots, a_n$ aritmetik dizisi var mıdır ki, her $j \in \{1, 2, \dots, n\}$ için bu dizinin j-inci terimi a_j'yi bölen, diğer terimleri bölmeyen j tane asal sayı bulunsun.

İşte size zor bir problem:

Problem 3. Uygun n pozitif tamsayısı için 2^n+1 sayısının asal olduğunu biliyoruz ($n = 1, 2, 4$). Acaba k pozitif bir tamsayı olmak üzere $(k \cdot 2^n+1)_{n\in\mathbb{N}}$ dizisinin terimleri arasında muhakkak en az bir asal sayı bulunur mu? Başka bir deyişle $(k \cdot 2^n+1)_{n\in\mathbb{N}}$ dizisinin hiç bir terimi asal sayı olmayacak şekilde bir k tamsayısı var mıdır?

İyi çalışmalar!