

5. BÖLÜM

KONGRÜANSLAR

Kongrüanslar matematiğin güncel hayatta farkında olmadan yaygın bir şekilde kullandığımız kısımlarından birisidir. Saat 16:00'da Bursa terminalinden Diyarbakır'a hareket edecek otobüse bilet aldığınızı ve Diyarbakır'daki annenizi arayarak seyahatinizi haber verdiğinizi varsayalım. Yolculuğun 18 saat süreceğini biliyorsunuz. O halde matematiksel olarak yapacağınız $16 + 18 = 34$ toplamını hesaplayıp bunu ailenize bildirmek:

- Anne, ben saat 34'de geliyorum!

Tabii ki kongrüanslardan ya da modüler aritmetikten haberi olsun olmasın, hiç kimsenin bu tarz bir ifade kullanmayacağı aşikârdır. Çünkü herkes günün 24 saat olduğunu ve gece yarısından sonra saatlerin 25, 26, ... diye devam etmeyip sıfırlandığını ve hergün yeniden 1, 2, 3, ... diye devam ettiğini bilir. Yani bilerek ya da bilmeyerek 24 modunu kullanır. Hatta bazen öğleden sonraki saatleri de yeniden 1, 2, 3, ... şeklinde başlatırız. Örneğin saat 16:00 yerine öğleden sonra 4:00 ya da kısaca saat 4:00 diyebiliriz. Bu durumda da 12 modundan faydalanırız. 50 gün sonraki doğum gününüzün haftanın hangi gününe geldiğini bulmak istediğinizdeyse haftanın 7 gün olduğunu ve dolayısıyla bugünün 7, 14, 21, 28, ... gün sonrasının bugünle aynı gün olduğunu düşünerek 50'nin içindeki yedileri atarız. Geriye 1 kalır ve biz 50 gün sonrasıyla 1 gün sonrasının, yani yarının, aynı gün olduğunu kullanarak 50 gün sonrasının hangi gün olduğunu kolayca buluruz. Bir başka örnek olarak bugünün 14.08.2006 Pazartesi olduğunu ve seneye bugünün hangi gün olacağını merak ettiniz diyelim. Yani 14.08.2007'nin

haftanın hangi günü olacağını merak ediyorsunuz. 2007 yılının artık yıl olmadığını düşünerek aradığımız günün 365 gün sonrası olduğunu ve 365'ten yedileri atarak bunun 1 gün sonrasıyla aynı gün olacağını, yani 14.08.2007'nin bir Salı günü olacağını buluruz. Bu son iki örnekte de 7 modu kullanılmıştır.

Bu bölümde tamsayılarda denklik (kongrüent olma) kavramını tanımlayacak ve daha sonraki bölümlerde kongrüans denklemlerinin çözümünde ihtiyaç duyacağımız bazı özelliklerini ele alacağız. Fermat'ın küçük teoremini ve Euler'in genelleştirmesini göreceğiz. Bu teoremlerin bazı büyük sayıların verilen bazı sayılara bölümünden elde edilecek kalanları bulmada nasıl kullanılabileceğini belirteceğiz.

5.1. TAM SAYILAR VE MODÜLER ARİTMETİK

5.1.1. Tanım. $m \in \mathbb{Z}$ olmak üzere $a, b \in \mathbb{Z}$ için

$$m \mid (a-b)$$

ise a ve b , m moduna göre denktir (kongrüenttir) denir ve

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

yazılır.

5.1.2. Örnek. $8 \equiv 2 \pmod{2}$, $17 \equiv -3 \pmod{5}$ ve $16 \not\equiv 3 \pmod{4}$ 'dür.

5.1.3. Teorem. a ve b tamsayılarının m ile bölündüğünde aynı kalanı vermeleri için gerek ve yeter şart $a \equiv b \pmod{m}$ olmasıdır.

İspat. $(\Rightarrow)$ a ve b 'nin m ile bölündüklerindeki kalanlar aynı olsun. Yani $a = q'm + r$, $b = qm + r$ ($0 \leq r < m$) olsun. $a - b = (q' - q)m$ olduğundan $m \mid (a - b)$ yani $a \equiv b \pmod{m}$ 'dir.

$(\Leftarrow)$ $a \equiv b \pmod{m}$ olsun. $a = b + km$ olacak şekilde bir $k \in \mathbb{Z}$ vardır. Ayrıca b 'nin m ile bölümünden kalan r ise, yani $b = qm + r$ ($0 \leq r < m$) ise

$$a = (qm + r) + km = (q + k)m + r$$

dir. Yani a 'nın da m ile bölümünden kalan r 'dir.

5.1.4. Uyarı. a ve b 'nin m moduna göre denk olması, a ve b 'nin m ile bölündüğünde aynı kalanı vermesine denktir.

5.1.5. Teorem. Yukarıda tanımlanan " $\equiv$ " bağıntısı bir denklik bağıntısıdır. Bu bağıntı yardımıyla tamsayılar m tane farklı denklik sınıfına ayrılır. Bu denklik sınıflarına m modülüne göre kalan sınıflar denir. Bunların kümesi $\mathbb{Z}_m$ ile gösterilir.

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

ve

$$\begin{aligned}\bar{0} &= \{0 + km; k \in \mathbb{Z}\} \\ \bar{1} &= \{1 + km; k \in \mathbb{Z}\} \\ &\vdots \\ \overline{m-1} &= \{m-1 + km; k \in \mathbb{Z}\}\end{aligned}$$

dir. Genel olarak

$$\bar{r} = \{r + km : k \in \mathbb{Z}\} = \{n : n \equiv r \pmod{m}\}$$

şeklindedir.

5.1.6. Örnek. 4 modundaki kalan sınıfları

$$\begin{aligned}\bar{0} &= \{4k; k \in \mathbb{Z}\} = \{\dots, -8, -4, 0, 4, 8, \dots\} \\ \bar{1} &= \{1 + 4k; k \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, \dots\} \\ \bar{2} &= \{2 + 4k; k \in \mathbb{Z}\} = \{\dots, -6, -2, 2, 6, 10, \dots\} \\ \bar{3} &= \{3 + 4k; k \in \mathbb{Z}\} = \{\dots, -5, -1, 3, 7, 11, \dots\}\end{aligned}$$

dir.

5.1.7. Uyarı. Kalan sınıflar ayrıktır. Yani her tamsayı sadece bir kalan sınıfında bulunur.

Şimdi lineer kongrüansların çözümünde kullanılacak olan bir kavramı tanımlayacağız.

5.1.8. Tanım. m modundaki kalan sınıflarının her birinden bir tek eleman alınmasıyla elde edilen bir kümeye m **modundaki bir tam kalanlar sistemi** denir.

5.1.9. Uyarı. T , m modundaki bir tam kalanlar sistemi ise tam m tane eleman bulundurur. Bu m elemanın iki tanesi seçildiğinde bunlar denk değildir.

5.1.10. Örnek. $\{0,1,\dots,m-1\}$, $\{1,2,\dots,m\}$ ve $\{2,3,\dots,m+1\}$ kümelerinin her biri m modundaki bir tam kalanlar sistemidir.

5.1.11. Örnek. Tam kalanlar sistemindeki elemanların ardışık tamsayılar olması gerekmez. $\{0,1,7,-2,-11\}$ ve $\{0,1,2,3,4\}$ 5 modundaki birer tam kalanlar sistemidirler. $\{0,1,10,15,4\}$ kümesi ise değildir. Benzer şekilde $\{0,1,2,3,4,5\}$ ve $\{6,13,-4,-9,22,35\}$ kümeleri de 6 modundaki iki farklı tam kalanlar sistemidir.

5.1.12. Teorem. (i) T , m modunda bir tam kalanlar sistemi ise $(a,m)=1$ ve $b \in \mathbb{Z}$ olmak üzere

$$T' = \{ax + b \mid x \in T\}$$

kümesi de m modunda bir tam kalanlar sistemidir.

(ii) T , m modunda bir tam kalanlar sistemi ise $(a,m)=d$ ve $b \in \mathbb{Z}$ olmak üzere

$$T' = \{ax + b \mid x \in T\}$$

kümesi m modundaki m tane sayının m/d tanesini bulundurur.

İspat. (i)

(ii)



5.1.13. Örnek. (i) $m = 6$ modunda $T = \{6, 13, -4, -9, 22, 35\}$

kümesi bir tam kalanlar sistemi idi. $a = 5$ ve $b = 13$ alırsak $(5, 6) = 1$ olduğundan $5T + 13 = \{43, 78, -7, -32, 123, 188\}$ kümesi de 6 modunda bir tam kalanlar sistemidir. Gerçekten de $43 \equiv 1 (6)$, $78 \equiv 0 (6)$, $-7 \equiv 5 (6)$, $-32 \equiv 4 (6)$, $123 \equiv 3 (6)$ ve $188 \equiv 2 (6)$ olup her kalan sınıfından birer eleman bulunmaktadır. Aynı modda $a = 4$ ve $b = 13$ alınırsa $4T + 13 = \{37, 65, -3, -23, 101, 153\}$ kümesi bir tam kalanlar sistemi olmayacaktır. Çünkü $(4, 6) = 2$ olup 1'den farklıdır. Gerçekten de $37 \equiv 1 (6)$, $65 \equiv 5 (6)$, $-3 \equiv 3 (6)$, $-23 \equiv 1 (6)$, $101 \equiv 5 (6)$ ve $153 \equiv 3 (6)$ olup sadece 1, 3 ve 5 değerleri elde edilebilmekte, buna karşın 0, 2 ve 4 değerlerine ulaşılamamaktadır.

Dolayısıyla önümüzdeki bölümde daha geniş bir şekilde ele alacağımız gibi $5x + 13 \equiv 2 (6)$ kongrüansının bir çözümü varken, $4x + 13 \equiv 2 (6)$ kongrüansının hiç bir çözümü olmayacaktır. Gerçekten de $5x + 13$, $5T + 13$ kümesinde kalan m modunun tüm değerlerini değerleri alırken $4x + 13$ ise sadece $4T + 13$ kümesinde kalan 1, 3 ve 5 değerlerini alabilecektir (bu değerlerin her birinin 2 farklı x değeri için elde edildiğini unutmayınız!). Dolayısıyla $4x + 13 \equiv 2 (6)$ kongrüansının hiç bir çözümü olmayacaktır.

(ii) $m = 12$ modunda $T = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ bir tam kalanlar sistemidir. $a = 5$ alırsak b ne olursa olsun $(5, 12) = 1$ olduğundan $aT + b$ kümesi bir tam kalanlar sistemi olacaktır. Dolayısıyla c ne olursa olsun $5x \equiv c (12)$ kongrüansının bir çözümü olacaktır. Ancak $a = 8$ alındığında $8T = \{0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88\}$ olup bu kümedeki elemanlar 12 modunda 0, 4 ve 8 sayılarının denklik sınıflarında bulunurlar. Yani 12 modunda $8T$ kümesi $\{0, 4, 8\}$ kümesi halini alır. Bu da 5.1.12. Teoremin (ii) şıkında söylendiği gibi $(8, 12) = 4$ olduğundan $12/4 = 3$ elemandan oluşmaktadır. Bu yüzden örneğin 5, 12 modunda $8T$ kümesinde kalmadığından $8x \equiv 5 (12)$ kongrüansının çözümü olmadığını kolayca söyleyebiliriz.

5.1.14. Teorem. $a \equiv b \pmod{m}$ ve $c \equiv d \pmod{m}$ ise

a) $a \pm c \equiv b \pm d \pmod{m}$

b) $ac \equiv bd \pmod{m}$

c) $ac \equiv bc \pmod{m}$ ve $(c, m) = n$ ise $a \equiv b \pmod{\frac{m}{n}}$ 'dir.

İspat. a) $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ ise $m \mid (a - b)$ ve $m \mid (c - d)$ dir.

Dolayısıyla $m \mid ((a \pm c) - (b \pm d))$ ve böylece de $a \pm c \equiv b \pm d \pmod{m}$ yazılabilir.

b) Verilenler k ve j birer tamsayı olmak üzere $a = b + km$ ve $c = d + jm$ şeklinde yazılabilir. Bu durumda $ac \equiv bd + m(bj + kd + kjm)$ olacağından $ac \equiv bd \pmod{m}$ elde edilir.♣

5.1.14. Sonuç. $a \equiv b \pmod{m}$, $n \in \mathbb{N}$, $c \in \mathbb{Z}$ olmak üzere

i) $a^n \equiv b^n \pmod{m}$

ii) $a \pm c \equiv b \pm c \pmod{m}$

iii) $ac \equiv bc \pmod{m}$ 'dir.

İspat. Tanım kullanılarak kolayca görülür.♣

5.1.13. Teorem ve 5.1.14. Sonuç bize aynı moddaki kongrüansları taraf tarafa toplayıp çıkarabileceğimizi, çarpabileceğimizi göstermektedir. Aynı zamanda bir kongrüansın her iki tarafına bir sayıyı ekleyip çıkarabiliriz, ya da her iki tarafı istediğimiz sayıyla çarpabiliriz. Tek dikkat edilmesi gereken iki tarafı aynı sayı ile bölmektir. Örneğin $6 \cdot 5 \equiv 6 \cdot 7 \pmod{4}$ kongrüansında iki taraftaki 6'ları sadeleştirirsek $5 \equiv 7 \pmod{4}$ kongrüansını elde ederiz ki bu açık bir şekilde yanlıştır.

Bölme yaparken modun değişebilme ihtimali vardır. Teoremin (iii) şıkkı gereği bölme yapıldığında mod küçülebilir. Çünkü mod, mod ile böldüğümüz sayının obebine bölünmelidir. Örneğin $6 \cdot 5 \equiv 6 \cdot 7 \pmod{4}$ kongrüansında her iki taraftaki 6'lar sadeleştirildiğinde modun 6 ile

4'ün obebi olan 2 ye bölünmesi gereklidir. Bu durumda $5 \equiv 7 \pmod{2}$ yani $5 \equiv 7 \pmod{2}$ elde edilir ki bu da doğrudur.

Bu sonuçlardan faydalanarak uygulama alanı çok fazla olan aşağıdaki teoremi elde edebiliriz:

5.1.15. Teorem. $a \equiv b \pmod{m}$ ve $f(x)$ tamsayı katsayılı bir polinom ise

$$P(a) \equiv P(b) \pmod{m}$$

dir.

İspat. $P(x) = a_n x^n + \dots + a_1 x + a_0$ ise

$$P(a) - P(b) = a_n (a^n - b^n) + \dots + a_1 (a - b)$$

ve

$$m \mid (a^n - b^n), \dots, m \mid (a - b)$$

olduğundan sağ taraf ve dolayısıyla da sol taraf m ile bölünür. Böylece $P(a) \equiv P(b) \pmod{m}$ dir.

5.1.16. Örnek. $P(x) = 2x^2 - 3x + 1$ ve $2 \equiv 5 \pmod{3}$ olsun.

$$P(2) = 2 \cdot 2^2 - 3 \cdot 2 + 1 = 3 \text{ ve } P(5) = 2 \cdot 5^2 - 3 \cdot 5 + 1 = 36$$

olup $3 \equiv 36 \pmod{3}$ 'tür.

5.1.17. Teorem. $a \equiv b \pmod{m}$ ise

$$(a, m) = (b, m)$$

dir.

İspat. $a \equiv b \pmod{m}$ ise k bir tamsayı olmak üzere $a = b + km$ şeklinde yazılabilir. $(a, m) = d$ diyelim. $d|a$ ve $d|m$ olduğundan $d|(a - km)$ olup $d|b$ bulunur. Böylece d sayısı b ve m sayılarının bir ortak bölenidir.

İkinci olarak t de b ile m sayılarının bir başka ortak böleni olsun. $t|b$ ve $t|m$ olduğundan $t|(b + km)$ yani $t|a$ olur. $(a, m) = d$ olduğundan $t|a$ ve $t|m$ iken $t|d$ olmalıdır. Böylece $d = (b, m)$ 'dir.

5.1.18. Tanım. $\mathbb{Z}_m$ 'deki "+" ve "." sırasıyla

$$\begin{aligned}\overline{a} + \overline{b} &= \overline{a + b} \\ \overline{a} \cdot \overline{b} &= \overline{a \cdot b}\end{aligned}$$

şeklinde tanımlanır.

5.1.19. Uyarı. Yukarıda tanımlanan "+" ve "." işlemleri iyi tanımlıdır. Yani bu işlemler denklik sınıflarının a ve b temsilcilerine bağlı değildir.

Örneğin $\mathbb{Z}_6$ 'daki "+" ve "." tabloları

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

şeklinde dir.

5.1.20. Tanım. $a \in \mathbb{Z}_m$ ve $(a, m) = 1$ ise $\overline{a}$ elemanına bir asal kalan sınıf denir. Asal kalan sınıfların kümesine m modunun bir indirgenmiş sistemi denir.

5.1.21. Sonuç. m asal ise $\bar{0}$ hariç tüm kalan sınıfları asal kalan sınıflardır.

5.1.22. Teorem. İki asal sınıfın çarpımı yine bir asal sınıftır.

İspat. a ve b , m modunda iki asal kalan sınıfı olsun. Yani $(a,m)=1$ ve $(b,m)=1$ olsun. $(ab,m)=1$ olduğunu göstermek istiyoruz. $(a,m)=1$ olduğundan $ax + my = 1$ olacak şekilde x ve y tamsayıları vardır. Benzer şekilde $(b,m)=1$ olduğundan $bx' + my' = 1$ olacak şekilde x' ve y' tamsayıları vardır. Taraf tarafa çarpma yapılarak

$$(ax + my)(bx' + my') = 1$$

ve böylece

$$abxx' + m(axy' + bxy' + myy') = 1$$

elde edilir. Bu da parantez içi bir tamsayı olduğundan $(ab,m)=1$ olduğu anlamına gelir. Yani iki asal kalan sınıfın çarpımı da bir asal kalan sınıftır. ♣

5.1.23. Teorem. $\bar{I}$, m modunun bir indirgenmiş sistemi ve $(a,m)=1$ ise

$$\bar{I}' = \{ax : x \in \bar{I}\}$$

kümesi de m modunun bir indirgenmiş sistemidir.

İspat. $\bar{I}$, m modunun bir indirgenmiş sistemi olduğundan $\bar{I}$ kümesindeki her bir x elemanı için $(x,m)=1$ olmaktadır. Ayrıca $(a,m)=1$ verildiğinden 5.1.22. Teorem gereği $(ax,m)=1$ olur. Bu da ax elemanlarından oluşan $\bar{I}'$ kümesinin m modunda bir indirgenmiş sistem olduğunu gösterir. ♣

5.1.24. Örnek. 8 modülünün bir indirgenmiş kalanlar sistemi $I = \{1, 3, 5, 7\}$ kümesidir. $a = 3$ alırsak $(3, 8) = 1$ olduğundan $I' = 3I = \{3, 9, 15, 21\}$ olur. Bu da bir indirgenmiş kalanlar sistemidir.

5.2. Fermat ve Euler Teoremleri

Bu kısımda bazı büyük sayıların belirli sayılarla bölümünden kalanları belirlemenin yollarını inceleyeceğiz. Bu problemle ilgili olarak ilk sonucu 1640'lı yıllarda Fermat'ın bölen sayının asal olması durumunda verdiği; daha sonra da 1730'lu yıllarda bu sonucun tüm doğal sayılara Euler tarafından genelleştirildiğini göreceğiz. İlk olarak aşağıdaki iki örneği ele alalım:

5.2.1. Örnek. 2^{30} 'un 15 ile bölümünden kalanı belirleyelim.

$2^4 \equiv 1 \pmod{15}$ olduğundan 5.1.4. Sonuç gereği $(2^4)^7 \equiv 1 \pmod{15}$ yani $2^{28} \equiv 1 \pmod{15}$ bulunur. Ayrıca $2^2 \equiv 4 \pmod{15}$ olduğundan Teorem 5.1.13.(b) gereği $2^{28} \cdot 4 \equiv 1 \cdot 4 \pmod{15}$ ve böylece $2^{30} \equiv 4 \pmod{15}$ bulunur. Bu demektir ki 2^{30} sayısının 15 ile bölümünden kalan 4 tür.

5.2.2. Örnek. 3^{87} 'nin 29 ile bölümünden kalanı bulalım.

$$3^2 \equiv 9 \pmod{29}$$

$$3^3 \equiv -2 \pmod{29}$$

$$3^4 \equiv -6 \pmod{29}$$

$$3^5 \equiv 11 \pmod{29}$$

$$3^6 \equiv 4 \pmod{29}$$

$$3^7 \equiv 12 \pmod{29}$$

$$3^8 \equiv 7 \pmod{29}$$

$$3^9 \equiv -8 \pmod{29}$$

$$3^{10} \equiv 5 \pmod{29}$$

$$3^{11} \equiv 15 \pmod{29}$$

$$3^{12} \equiv 16 \pmod{29}$$

$$3^{13} \equiv -10 \pmod{29}$$

$$3^{14} \equiv 28 \pmod{29}$$

elde edilir. Görüldüğü gibi hedeflenen 1 değerine hala ulaşamadık. 3'ün hangi kuvvetinde 1 elde edileceğini bilebilseydik bunca işleme gerek kalmazdı. Aslında $28 \equiv -1 \pmod{29}$ olduğuna dikkat edersek yukarıda yapılan işlemler kadar daha işlem yapmaktan kaçınmış oluruz. Gerçekten de

$$3^{28} \equiv (3^{14})^2 \equiv (-1)^2 \equiv 1 \pmod{29}$$

olduğundan

$$(3^{28})^3 \cdot 3^3 \equiv 1 \cdot 3^3 = 27 \pmod{29}$$

elde edilebilir. Yani 3^{87} 'nin 29 ile bölümünden kalan 27'dir.

İlk örnekte 2'nin dördüncü kuvvetinde 1 elde ettik ve soruyu kolayca cevaplayabildik. Ancak 5.2.2. Örnekte olduğu gibi bazen verilen sayının kuvvetlerinden 1 olanı bulmak zor olabilir. Bu tür bir durumda aşağıdaki sonuçlar faydalı olacaktır:

5.2.3. Teorem (Fermat'nın küçük teoremi). p asal ve $(a, p) = 1$ ise bu taktirde

$$a^{p-1} \equiv 1 \pmod{p}$$

dir. Denk olarak $a^p \equiv a \pmod{p}$ dir.

İspat. Burada 0, 1, 2, ..., $p-1$ sayıları, p modunda bir tam kalanlar sistemidir. Böylece bir önceki teorem gereği, 0, a , $2a$, ..., $(p-1)a$ sayıları da bir tam kalanlar sistemi olur. Bu iki listeden herhangi birindeki bir eleman mutlaka diğerinde bir tek elemana denktir. 0 dışındaki tüm elemanları karşıtığımızda, 4 gereği

$$a \cdot 2a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}$$

veya denk olarak

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$$

yazabiliriz. Sadeleştirme sonucunda istenen elde edilir. ♣

17. yüzyılda Euler bu teoremi genelleştirmiştir.

5.2.4. Teorem (Euler). $(a, m) = 1$ ise $a^{\varphi(m)} \equiv 1 \pmod{m}$ dir.

İspat.

5.2.5. Teorem (Wilson). p bir asal sayı olmak üzere

$$(p-1)! \equiv -1 \pmod{p}$$

dir.

İspat. Eğer $p = 2$ veya $p = 3$ ise ispat aşıkardır. $p > 3$ olduğunu varsayabiliriz. a sayısı $1, 2, \dots, p-1$ sayılarından biri olsun. $ax \equiv 1 \pmod{p}$ kongrüansını ele alalım. $(a, p) = 1$ 'dir. Bu sebeple eğer x değişkeni $1, 2, \dots, p-1$ değerlerini alırsa, ax ; p modunda 0 dışındaki tüm değerleri alacaktır. Yani kongrüansı sağlayan bir tek x değeri mevcuttur.

$1, 2, \dots, p-1$ sayılarını p modunda çarpımı 1 olan çiftlere ayırabiliriz. Hangi eleman çiftlerinin birbirine eşit iki sayıdan oluştuğunu araştıralım. Diyelim ki bu çift a ve a^{-1} olsun. Bu taktirde çarpımları 1 olduğundan $a^2 \equiv 1 \pmod{p}$ olup $a^2 - 1 \equiv 0 \pmod{p}$ ve buradan

$$p \mid (a-1)(a+1)$$

elde edilir. Bu da $p \mid (a-1)$ veya $p \mid (a+1)$ anlamına gelir. Burada p hem $a-1$ 'i, hem de $a+1$ 'i aynı anda bölemez. Çünkü öyle bir durumda p , bu iki sayının farkı olan 2'yi de bölmek zorunda kalırdı. Böylece $a \equiv 1 \pmod{p}$ veya $a \equiv -1 \pmod{p}$ olurdu. Ancak $1 \leq a \leq p-1$ olduğundan ya $a = 1$ ya da $a = p-1$ olmalıdır. Yani 1 ile $p-1$ arasındaki sayılardan sadece 1 ve $p-1$ 'in tersleri kendileridir. Diğer tüm sayıların kendilerine eşit olmayan birer çarpımsal tersleri mevcuttur.

2, 3, ..., p-2 şeklindeki p-3 adet sayı ile

$$2.3.4. \dots (p-2) \equiv 1 \pmod{p}$$

olacak şekilde (p-3)/2 tane çift elde ederiz. Buradan iki tarafı p-1 ile çarparak (p-1)! $\equiv$ p-1 $\equiv$ -1 (p) elde ederiz.♣

5.2.6. Örnek. p = 11 olsun. O halde

$$\begin{aligned}(p-1)! &= 10! \\ &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10\end{aligned}$$

çarpımında $2 \cdot 6 \equiv 1 \pmod{11}$, $3 \cdot 4 \equiv 1 \pmod{11}$, $5 \cdot 9 \equiv 1 \pmod{11}$ ve $7 \cdot 8 \equiv 1 \pmod{11}$ olduğundan 2 ile 6, 3 ile 4, 5 ile 9 ve 7 ile 8 birbirlerinin çarpıma göre tersleridir. Geriye kalan 1 ve 10 sayılarının tersleri kendileridir. Dolayısıyla

$$\begin{aligned}10! &= 1 \cdot 10 \cdot (3 \cdot 4) \cdot (2 \cdot 6) \cdot (7 \cdot 8) \cdot (5 \cdot 9) \\ &= 1 \cdot 10 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \\ &= 10 \\ &\equiv -1 \pmod{11}\end{aligned}$$

elde edilir.

5.2.7. Sonuç. p, $4m+1$ şeklinde bir asal sayı ise, $n = (2m)!$ olmak üzere $p \mid (n^2+1)$ dir.

$$\begin{array}{ll}\text{İspat.} & -1, -2, \dots, -2m \\ & 4m, 4m-1, \dots, 2m+1\end{array}$$

şeklindeki iki sayı grubunu düşünelim. Alt satırdaki her bir elemanın tam üstünde kalan elemanla farkı p olduğundan bu iki eleman p modunda birbirine denk olur. Böylece

$$4m \cdot (4m-1) \cdot \dots \cdot (2m+1) \equiv (-1) \cdot (-2) \cdot \dots \cdot (-2m) \pmod{p}$$

olur. Buradan da

$$(4m)! \equiv \{(2m)!\}^2 \pmod{p}$$

elde ederiz. $n = (2m)!$ denilirse, Wilson teoremi gereği $(4m)! = (p-1)! \equiv -1 \pmod{p}$ olduğundan $n^2 \equiv -1 \pmod{p}$ sonucu elde edilir.♣

5.2.8. Teorem. p asal olsun. a ve b iki tamsayı ise

$$a^p + b^p \equiv (a+b)^p \pmod{p}$$

dir.

İspat. Fermat'ın küçük teoremi (5.2.3. Teorem) gereği, her c tamsayısı için $c^p \equiv c \pmod{p}$ 'dir. $c = a+b$ olsun. $(a+b)^p \equiv a+b \pmod{p}$ 'dir. Ayrıca $a^p \equiv a$, $b^p \equiv b \pmod{p}$ olduğundan istenen sonuç görülür.♣

5.2.9. Örnek. 5^{38} 'in 13 ile bölümünden kalanı bulalım.

Euler teoremine göre $5^{\varphi(13)} \equiv 1 \pmod{13}$ yani $5^{12} \equiv 1 \pmod{13}$ ve $5^{36} \equiv 1 \pmod{13}$ olur. Sonuçta $5^{38} \equiv 5^{36} \cdot 5^2 \equiv 25 \equiv 12 \pmod{13}$ bulunur.

ALİŞTIRMALAR

1) $(x,6) = 1$ ise,

$$x^2 \equiv 1 \pmod{24}$$

olduğunu gösteriniz.

2) Tam kare olan tüm sayıların son iki basamağını belirleyiniz.

3) Mod 7 de

- a)** hepsi tek
- b)** hepsi çift
- c)** hepsi asal
- d)** hepsi tam kare

olan bir tam kalanlar sistemi bulunabilir mi?

4) 2^{68} sayısı mod 19 da nedir?

5) Her a tamsayısı için $a^{25} - a$ farkının 30 ile bölünebildiğini gösteriniz.

6) Euler Teoreminden faydalanarak

$$f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \quad (5)$$

kongrüansının tüm köklerini belirleyiniz.

7) Wilson Teoremi'ni ispatlayınız:

“Bir n tamsayısının asal olması için gerek ve yeter şart

$$(n-1)! \equiv -1 \pmod{n}$$

olmasıdır.”

8) p bir tek asal sayı olsun.

$$x^2 + 1 \equiv 0 \pmod{p}$$

kongrüansının bir çözümünün olması için gerek ve yeter şartın

$$p \equiv 1 \pmod{4}$$

olması olduğunu gösteriniz.

9) $x^2+1 \equiv 0 \pmod{13}$ kongrüansının çözümlerini araştırınız.

10) $(m,n) = 1$ olsun. x , m modundaki bir indirgenmiş kalanlar sistemindeki tüm değerleri alırken ve y de, n modundaki bir indirgenmiş kalanlar sistemindeki tüm değerleri alırken $nx + my$ toplamının da mn modundaki bir indirgenmiş kalanlar sistemindeki tüm değerleri alacağını gösteriniz.

11) $f(x)$ katsayıları tamsayılar olan bir polinom olsun. Eğer belli bir $n \geq 1$ için $f(x) \equiv 0 \pmod{n}$ kongrüansının hiçbir çözümü yoksa $f(x) = 0$ denkleminin de tamsayı çözümlerinin olmayacağını gösteriniz.

12) $f(x) = x^5 - x^2 + x - 3$ polinomunun tamsayı köklerinin bulunmadığını gösteriniz.

13) Tüm x tamsayıları için $f(x)$ değerleri asal olacak şekilde sabit olmayan tamsayı katsayılı bir $f(x)$ polinomunun mevcut olamayacağını gösteriniz

14) n_i 'ler aralarında asal tamsayılar olmak üzere

$$n = n_1 \dots n_k$$

olsun. $f(x)$ ise katsayıları tamsayılar olan bir polinom olsun. Her bir $i = 1, \dots, k$ için,

$$f(x) \equiv 0 \pmod{n_i}$$

olacak şekilde N_i tane denklik sınıfı bulunsun. Bu durumda Z_n 'de

$$f(x) \equiv 0 \pmod{n}$$

olacak şekilde $N = N_1 \dots N_k$ adet denklik sınıfı bulunduğunu gösteriniz.

15) $x^2 \equiv 1 \pmod{n}$ özelliğindeki $x \in Z_n$ sınıflarının sayısı olan N 'yi belirleyiniz.

16) $x^2 - 1 \equiv 0 \pmod{168}$ kongrüansının kaç tane çözüm sınıfı olduğunu bulunuz.

17) Farklı asalların çarpımı şeklindeki bir sayıya kare içermeyen sayı denilir. Her k doğal sayısı için, hiçbir kare içermeyen sayı olmayan ardışık k tamsayı bulunabileceğini gösteriniz.

18) Polinomlar için Lagrange Teoremi'ni ispat ediniz:

" p asal ve

$$f(x) = a_d x^d + \dots + a_1 x + a_0$$

tamsayı katsayılı bir polinom olsun. Belli bir i için a_i, p modunda sıfıra denk değil ise,

$$f(x) \equiv 0 \pmod{p}$$

kongrüansı, en çok d tane kalan sınıfı tarafından sağlanır.”

19) p bir tek asal sayı ise

$$r = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}$$

rasyonel sayısının (indirgendikten sonra) payının p ile bölünebildiğini gösteriniz. Ayrıca $p > 3$ ise, r nin p ile bölünebildiğini gösteriniz. (Wolsten – Holme teoremi)

20) Z_p den Z_p ye bir f fonksiyonu verilsin. Eğer her bir $x \in Z_p$ için

$$f(x) \equiv g(x) \pmod{p}$$

olacak biçimde tamsayı katsayılı bir $g(x)$ fonksiyonu bulunabiliyorsa f fonksiyonuna bir polinom denilir. İki farklı polinom aynı fonksiyonu tanımlayabilir. (Örneğin, x ve x^p polinomları). Z_p den Z_p ye tam p^p tane polinom olduğunu gösteriniz ve bunun sonucu olarak, Z_p den Z_p ye her bir fonksiyonun bir polinom olması gerektiğini bulunuz.

21) p ve q asal olsun.

$$\Phi_q(x) = 1 + x + x^2 + \dots + x^{q-1}$$

döngüsel polinomunu göz önüne alalım. $p \equiv 1 \pmod{q}$ ise, $\Phi_q(x)$ polinomunun Z_p de $q-1$ kökü olduğunu, $p = q$ iken bir, diğer hallerde hiç köke sahip olmadığını gösteriniz.

$$22) \quad x^{18} + 4x^{14} + 3x + 10 \equiv 0 \pmod{21}$$

kongrüansının tüm köklerini bulunuz.

$$23) \quad ab \equiv 1 \pmod{p}$$

olacak şekilde $a, b \in Z_p$ elemanlarını ikişer ikişer sayarak, p asal iken

$$(p-1)! \equiv -1 \pmod{p}$$

olduğunu gösteriniz.

$$24) \quad p \geq 5 \text{ olsun. } p \text{ nin asal olması için gerek ve yeter şartın}$$

$$6(p-4)! \equiv 1 \pmod{p}$$

olduğunu gösteriniz.

$$25) \quad 31492 \text{ sayısının son iki basamağını hesaplayınız.}$$

26) $(a, 10) = 1$ iken a^{2001} sayısının son üç basamağının a 'nıninkilerle aynı olduğunu gösteriniz.

$$27) \quad ab \equiv 1 \pmod{m}$$

ve a nın m modundaki mertebesi h ise, b nin m modundaki mertebesinin de h olduğunu gösteriniz.

$$28) \quad p \text{ asal sayı olsun. } a_n \not\equiv 0 \pmod{p} \text{ olmak üzere;}$$

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n \equiv 0 \pmod{p}$$

kongrüansının en fazla n tane çözümünün olabileceğini gösteriniz.

29) $x^3+4x+8 \equiv 0 \pmod{15}$ kongrüansını çözünüz.

30) p bir asal sayı ve a nın p modundaki mertebesi 3 olsun. Buna göre

$$1+a+a^2 \equiv 0 \pmod{p}$$

olduğunu ve $1+a$ elemanının mod p de 6. mertebeden olduğunu gösteriniz.

31) p bir tek asal sayı olsun. Bir a tam sayısının p modunda 2. mertebeden olması için gerek ve yeter şartın

$$a \equiv -1 \pmod{p}$$

olduğunu gösteriniz.

32) m modunda a nın mertebesi h ve b nin mertebesi k olsun. $(h,k)=1$ ise, $a.b$ nin mertebesinin $h.k$ olduğunu gösteriniz.

33) a nın p asal modundaki mertebesi h olsun. Eğer h çift ise

$$a^{h/2} \equiv -1 \pmod{p}$$

olduğunu gösteriniz.

34) m modunda a nın mertebesi h ise, $a, a^2, a^3, \dots, a^h$ sayılarından herhangi ikisinin denk olamayacağını gösteriniz.

35) $p, p \equiv 1 \pmod{4}$ özelliğinde bir asal sayı olsun. Eğer bir g tamsayısı p modunda bir ilkel kök ise $-g$ nin de bir ilkel kök olduğunu gösteriniz.

36) a sayısının $f(x) \equiv 0 \pmod{m}$ kongrüansının bir kökü olması için gerek ve yeter şartın

$$f(x) \equiv (x - a)g(x) \pmod{m}$$

olacak şekilde bir $g(x)$ polinomunun bulunması olduğunu gösteriniz.

37) a_0 , mod p de sıfırdan farklı olmak üzere

$$f(x) = a_0x^n + \dots + a_n$$

polinomu için $f(x) \equiv 0 \pmod{p}$ kongrüansının en çok n kökü vardır. Gösteriniz.

38) p asal ve $d \mid (p-1)$ ise

$$x^d \equiv 1 \pmod{p}$$

kongrüansının tam d kökünün olduğunu gösteriniz.

39) Euler Teoreminden faydalananarak her x tamsayısı ve her p asalı için

$$x^{p-1} - 1 \equiv (x-1)(x-2) \dots (x-p+1) \pmod{p}$$

olduğunu gösteriniz.

40) Bir önceki problemde $x = p$ yazılırsa hangi sonuç elde edilir ?

41) Kongrüanslardan faydalananarak 9 ile bölünebilme kuralını elde ediniz.

42) Kongrüanslardan faydalananarak 11 ile bölünebilme için bir kural bulunuz.

43) Eğer

$$f(x) = a_0 \cdot x^n + a_1 \cdot x^{n-1} + \dots + a_n$$

tamsayı katsayılı bir polinomsa ve p, a_0 sayısını bölmeyen bir asal ise

$$f(x) \equiv 0 \pmod{p}$$

kongrüansının p modunda en çok n tane çözümü vardır. Gösteriniz.

44) $28x \equiv 91 \pmod{35}$ kongrüansının çözümünü bulunuz.

45) Euler Teoremini ispatlayınız: “ $(a,n)=1$ ise

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

dir.”

46) $8x \equiv 9 \pmod{24}$ kongrüansının çözüm kümesini bulunuz.

47) $(p-1)!+1$ toplamını bölen en küçük asal sayının p olduğunu gösteriniz.

48) Fermat’ın Küçük Teoremini ispatlayınız: “ $a \in \mathbb{Z}$ ve p , a yı bölmeyen bir asal sayı olsun. a , p modunda sıfıra denk değilse

$$a^{p-1} \equiv 1 \pmod{p}$$

dir.

49) $2^{5^{19}} + 1$ ’in 19 ile bölümünden kalanı bulunuz.

50) 37^{49} sayısının 7 ile bölümünden elde edilen kalanı bulunuz.

51) Fermat Teoremini kullanarak 3^{47} ’nin 23 ile bölümünden kalanı bulunuz.

52) Her n tamsayısı için $n^{33} - n$ sayısının 15 ile bölünebildiğini gösteriniz.

53) $(a,m)=(a-1,m)=1$ ise

$$1 + a + a^2 + \dots + a^{\varphi(m)-1} \equiv 0 \pmod{m}$$

olduğunu gösteriniz.

54) p asal olsun ve a $yı$ bölmesin. $x = a^{p-2} \cdot b$ sayısının $ax \equiv b \pmod{p}$ kongrüansının bir çözümü olduğunu gösteriniz.

55) $p \equiv 1 \pmod{4}$ özelliğinde bir p asalı için

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

olduğunu gösteriniz.

56) Bir önceki sorunun çözümünde verilen (*)'ı kullanarak

a) $x^2 \equiv -1 \pmod{13}$

b) $x^2 \equiv -1 \pmod{17}$

kongrüansları için bir çözüm bulunuz.

57) 17 modunda $16!$ sayısının -1 'e denk olup olmadığını belirleyerek 17'nin bir asal olup olmadığına karar veriniz.

58) n sayısı 5 ile bölünmeyen bir sayı ise 5 modunda n^4 sayısının alacağı değerleri belirleyiniz.

6. BÖLÜM

LİNEER KONGRÜANSLAR VE LİNEER DIOPHANT DENKLEMLERİ İLE İLİŞKİ

Bu bölümde 5. Bölümde tanımladığımız denk (kongrüent) olma kavramından faydalanarak lineer kongrüans denklemlerini inceleyeceğiz. İlk kısımda tek değişkenli lineer kongrüansları ele aldıktan sonra ikinci kısımda bu kongrüansların lineer Diophant denklemleri ile ilişkisi incelenecektir. Son bölümde ise tek değişkenli kongrüanslar için elde edilen sonuçlar iki değişkenli duruma genelleştirilmiş ve daha fazla değişken olması durumunda nasıl genelleştirme yapılabileceği belirtilmiştir.

6.1. Tek Değişkenli Lineer Kongrüanslar

6.1.1. Tanım. a, b tamsayılar ve $m \nmid a$ olmak üzere $ax \equiv b \pmod{m}$ şeklindeki bir ifadeye **tek değişkenli lineer (birinci dereceden) bir kongrüans denklemi** denir.

6.1.2. Uyarı. Eğer $x_1, ax \equiv b \pmod{m}$ lineer kongrüansının bir çözümü ise k bir tamsayı olmak üzere $x_1 + km$ sayısı da bu kongrüansı sağlar. O halde bu tür kongrüanslar için $0 \leq x_1 < m$ olacak şekildeki sayıların çözüm olup olmadığını incelemek yeterlidir.

6.1.3. Örnek. $5x \equiv 2 \pmod{6}$ kongrüansının çözümlerini deneyerek bulalım.

Sadece 0, 1, 2, 3, 4, 5 değerlerini denemek yeterlidir. Bunlardan $x = 4$ 'ün bir çözüm olduğu görülür. O halde tüm çözümler

$$\bar{4} = \{x: x \equiv 4 \pmod{6}\}$$

kümesindeki tamsayılarıdır.

6.1.4. Uyarı. (1) Bazı lineer kongrüansların çözümü olmayabilir. Örneğin $2x \equiv 3 \pmod{4}$ ve $3x \equiv 5 \pmod{12}$ kongrüanslarının çözümleri mevcut değildir. Birincide $2x-3$ her zaman tek bir sayı olduğundan hiç bir zaman 4 ile bölünemez ve kongrüans tanımı gereği hiç bir x değeri için $2x \equiv 3 \pmod{4}$ olamaz.

Bazı kongrüansların ise birden fazla denklik sınıfında kalan çözümleri mevcuttur. Örneğin $2x \equiv 6 \pmod{8}$ kongrüansının çözümleri $\bar{3}$ ve $\bar{7}$ sınıflarındaki tüm tamsayılarıdır.

(2) Mod değişince verilen bir kongrüansın çözümlerinin de değişeceği açıktır.

6.1.5. Tanım. Aynı denklik sınıfında kalan çözümlere **denk çözümler**, farklı sınıflarda kalanlara da **denk olmayan çözümler** denir.

6.1.6. Örnek. Yukarıda $2x \equiv 6 \pmod{8}$ kongrüansının çözümlerinin $\bar{3}$ ve $\bar{7}$ sınıflarındaki tüm tamsayılar olduğunu gördük. Burada 3 ile 11, $\bar{3}$ sınıfında kaldıklarından denk çözümler; 11 ile 15 ise farklı sınıflarda kaldıklarından denk olmayan çözümlerdir.

6.1.7. Teorem. $(a,m) = 1$ ise $ax \equiv b \pmod{m}$ kongrüansının bir tek çözümü vardır.

İspat. T , m modunda bir tam kalanlar sistemi olsun. 5.1.12. Teoremden $b = 0$ alındığında $\{ax: x \in T\}$ kümesinin de $(a,m) = 1$ olduğundan bir tam kalanlar sistemi olacağı görülür. Dolayısıyla verilen bir b tamsayısı için $ax \equiv b \pmod{m}$ olacak şekilde bir tek $b = ax$ ve dolayısıyla bir tek $x \in T$ mevcuttur. ♣

Şimdiye kadar olan kısımda verilen bir lineer kongrüansın çözümünün deneme yoluyla nasıl bulunabileceğini ve hangi durumda bir tek çözüm olacağını belirledik.

6.1.8. Teorem. $(a,m) = 1$ olmak üzere $ax \equiv b \pmod{m}$ lineer kongrüansının çözümü

$$x \equiv a^{\phi(m)-1} \cdot b \pmod{m}$$

şeklindedir.

İspat. Euler teoremine göre $a^{\phi(m)} \equiv 1 \pmod{m}$ 'dir. O halde 5.1.14. Teorem (iii) gereği $a^{\phi(m)} \cdot b \equiv b \pmod{m}$ olur. O halde

$$ax \equiv b \pmod{m}$$

kongrüansında Euler teoreminden faydalanarak

$$ax \equiv a^{\phi(m)} \cdot b \pmod{m}$$

elde edilir. Burada $(a,m) = 1$ olduğundan her iki taraf a 'nın tersi ile çarpılarak

$$x \equiv a^{\phi(m)-1} \cdot b \pmod{m}$$

elde edilir. ♣

6.1.9. Örnek. $3x \equiv 5 \pmod{8}$ kongrüansının çözüm kümesini bulalım. $(3,8) = 1$ olduğundan

$$\begin{aligned} x &\equiv 3^{\phi(8)-1} \cdot 5 \pmod{8} \\ &\equiv 3^{4-1} \cdot 5 \pmod{8} \\ &\equiv 135 \pmod{8} \\ &\equiv 7 \pmod{8} \end{aligned}$$

bulunur.

6.1.10. Teorem. $d = (a,m)$ olmak üzere $ax \equiv b \pmod{m}$ lineer kongrüansının çözümünün olması için gerek ve yeter şart $d|b$

olmasıdır. Bu durumda tam d tane çözüm vardır. Bu çözümler, x_0 bir özel çözüm olmak üzere

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \dots, x_0 + \frac{(d-1)n}{d}$$

şeklinde dir.

İspat. Lineer Diophant denklemleriyle ilişkisinden (Jones, p 47) 6.2 ile birleştir.

a ile modun aralarında asal olmaları durumunda aşağıdaki özel durumu elde ederiz:

6.1.11. Sonuç. $(a, m) = 1$ ise $ax \equiv b \pmod{m}$ lineer kongrüansının bir tek çözümü vardır.

6.1.12. Örnek. $6x \equiv 3 \pmod{21}$ lineer kongrüansının çözüm kümesini bulalım.

Çözüm. $(6, 21) = 3$ ve $3 \mid 3$ olduğundan 3 tane çözüm vardır. $6x \equiv 3 \pmod{21}$ ise öncelikle

$$2x \equiv 1 \pmod{7}$$

alırız. 7 modülündeki kalanlar 0, 1, 2, 3, 4, 5, 6 olduğundan bunlar içinde bir tek $x = 4$ değeri yukarıdaki kongrüansı sağlar. Dolayısıyla 21 modülüne göre

$$\mathcal{C} = \{4 + 7t : t = 0, 1, 2\} = \{4, 11, 18\}$$

dir.

6.1.13. Örnek. $7x \equiv 9 \pmod{21}$ için $(7, 21) = 7 \nmid 9$ olduğundan çözüm yoktur.

6.2. Lineer Kongrüanslar ve Lineer Diophant Denklemleri

Yukarıda gördük ki bir lineer kongrüansın çözümü her zaman olmayabilir. $d = (a,m) \mid b$ ise bir ya da daha fazla çözümün mevcut olacağı da bulduğumuz sonuçlar arasındaydı. Bu bölümde lineer kongrüansların çözümlerinin mevcut olması durumunda bunların nasıl bulunabileceğini göreceğiz. Bunu da lineer Diophant denklemlerinin çözümlerinden faydalanarak gerçekleştireceğiz. Kısacası lineer Diophant denklemleri ile lineer kongrüansların çözümlerini birbirinden faydalanarak bulabileceğimizi göreceğiz.

$ax \equiv c \pmod{b}$ lineer kongrüansının çözümlerinin bulunması $ax + by = c$ lineer Diophant denkleminin çözümlerinin bulunmasına denktir. Hatırlanacağı gibi $ax + by = c$ denkleminin tüm çözümleri, (x_0, y_0) bir özel çözüm ve t bir tamsayı olmak üzere

$$x = x_0 + \frac{b}{d} t, y = y_0 - \frac{a}{d} t$$

şeklindeydi. Yani $ax \equiv c \pmod{b}$ kongrüansının genel çözümü

$$x = x_0 + \frac{b}{d} t$$

şeklindedir.

Tabii ki lineer Diophant denklemlerinin çözümleri (x,y) ikilileri şeklindeken lineer kongrüansların çözümlerinin sadece x şeklinde oluşu aradaki tek farktır.

6.2.1. Örnek. Lineer Diophant denklemleri için ikinci bölümde elde ettiğimiz çözüm yönteminden faydalanarak $21x \equiv 11 \pmod{23}$ lineer kongrüansının çözüm kümesini elde edelim.

$(21,23) = 1 \mid 11$ olup 6.1.7. Teorem gereği çözüm mevcuttur. Bu kongrüansı

$$21x + 23y = 11$$

şeklinde yazarak bir lineer Diophant denklemi elde ederiz. Hatırlanacağı üzere bu denklemi çözebilmek için Euclid algoritması yardımıyla obebi bulmakla işe başlıyorduk:

$$23 = 1 \cdot 21 + 2$$

$$21 = 10 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

olup $(21, 23) = 1$ olduğu elde edilir (tabii sayılar küçük olduğundan obebi yukarıda hiç işlem yapmadan da bulabilmiştik, ama unutmamalıyız ki Euclid algoritmasını kullanmamızın esas amacı tersine giderek obebi katsayıların bir lineer bileşimi olarak ifade etmektir). Tersine gidilerek

$$\begin{aligned} 1 &= 21 - 10 \cdot 2 \\ &= 21 - 10 \cdot (23 - 21) \\ &= 21 \cdot 11 + 23 \cdot (-10) \end{aligned}$$

yazılır. Her iki taraf 11 ile çarpılarak

$$11 = 21 \cdot 121 + 23 \cdot (-110)$$

elde edilir. Yani $21x + 23y = 11$ lineer Diophant denkleminin bir özel çözümünü $x_0 = 121$ ve $y_0 = -110$ olarak belirleriz. O halde genel çözüm t bir tamsayı olmak üzere

$$x = 121 + 23t \text{ ve } y = -110 - 21t$$

olarak bulunur.

6.2.2. Örnek. Lineer kongrüanslar yardımıyla

$$48x + 7y = 17$$

lineer Diophant denkleminin çözümlerini bulalım.

$(48, 7) = 1 \mid 17$ olduğundan 2... Teorem gereği çözüm vardır. İlk olarak bir özel çözüm bulalım.

$$48x \equiv 17 \pmod{7}$$

kongrüansını göz önüne alalım.

$$-x \equiv 3 \pmod{7}$$

ve böylece $x \equiv 4 \pmod{7}$ bulunur. Verilen denklemde $x = 4$ konularak

$$48.4 + 7y = 17$$

ve buradan $y = -25$ bulunur. Böylece $(4, -25)$ ikilisi, $48x + 7y = 17$ 'nin bir özel çözümüdür.

6.3. İki Veya Daha Fazla Değişkenli Lineer Kongrüanslar

Burada sadece 2 değişkenli durumu inceleyeceğiz. Daha fazla değişken olması durumunda da benzer yolla genelleştirme yapılabilir.

$$ax + by \equiv c \pmod{m}$$

şeklindeki bir kongrüansı düşünelim. Eğer bir özel çözüm (x_0, y_0) ise k ve t bir tamsayı olmak üzere $(x_0 + km, y_0 + tm)$ ikilisinin de bir çözüm olacağı açıktır.

6.3.1. Teorem. $ax + by \equiv c \pmod{m}$ lineer kongrüansının çözümünün olması için gerek ve yeter şart $d = (a, b, m)$ olmak üzere $d \mid c$ olmasıdır.

İspat. $ax + by \equiv c \pmod{m}$ kongrüansını $by \equiv c - ax \pmod{m}$ olarak ifade edelim. (Benzer olarak $ax \equiv c - by \pmod{m}$ olarak da ifade edebiliriz). 6.1.8. Teorem gereği bu son ifadenin çözümünün olması için gerek ve yeter şart $(b, m) \mid (c - ax)$ olmasıdır. Denk olarak $ax \equiv c \pmod{(b, m)}$ olmasıdır. Şimdi bu son tek değişkenli kongrüansın çözümünün olması için gerek ve yeter şart $(a, (b, m)) = (a, b, m)$ olduğundan $ax + by \equiv c \pmod{m}$ kongrüansının çözümünün olması için gerek ve yeter şart $d \mid c$ olmasıdır. ♣

6.3.2. Örnek. $3x - 7y \equiv 11 \pmod{13}$ kongrüansının çözüm kümesini bulalım.

$(3, 7, 13) = 1 \mid 11$ olduğundan çözüm vardır. Şimdi

$$3x \equiv 11 + 7y \pmod{13}$$

kongrüansını katsayılarla oynayarak

$$3x \equiv 24 - 6y \pmod{13}$$

haline getirelim. $(3,13) = 1$ olduğundan 3 ile bölme yapılarak

$$x \equiv 8 - 2y \pmod{13}$$

yazılabilir. Dikkat edilirse y 'nin 13 modülüne göre denk olmayan her bir değerine x 'in bir tek değeri karşı gelir. Dolayısıyla

$$\mathcal{C} = \{(8,0), (6,1), (4,2), (2,3), (0,4), (11,5), (9,6), (7,7), (5,8), (3,9), (1,10), (12,11), (10,12)\}$$

olarak elde edilir. x 'in 13 modundaki tüm değerleri aldığına dikkat ediniz.

6.3.3. Uyarı. İlk bakışta y 'ye 0'dan 12'ye kadar değerler verilerek verilen ifadede x değerlerinin bulunabileceği akla gelebilir. Ancak önce x 'i y 'ye bağlı bulmak ve daha sonra bu işlemi yapmak çok daha kolaydır.

6.3.4. Teorem. $(a,m) = 1$ veya $(b,m) = 1$ ise $ax + by \equiv c \pmod{m}$ kongrüansının tam m tane çözümü vardır.

İspat. $(a,m) = 1$ olduğunu kabul edelim. $ax + by \equiv c \pmod{m}$ olduğundan $ax \equiv c - by \pmod{m}$ yazılabilir. Teorem 6.1.5. gereği $(a,m) = 1$ olduğundan bu son kongrüansın bir tek çözümü vardır. Ancak bu her bir y değeri için bir tektir. m modunda y 'nin tam m tane değeri olduğundan (x,y) ikilisinin de m farklı değeri bulunur. ♣

6.3.5. Örnek. 6.3.2. Örnekte $(3,13) = 1$ olduğundan (aynı zamanda $(-7,13)=1$ 'dir) tam 13 tane çözüm bulunduğuna dikkat ediniz.

6.3.6. Örnek. $7x + 8y \equiv 6 \pmod{10}$ kongrüansının çözüm kümesini bulalım.

$(7,8,10) = 1 \mid 6$ olduğundan öncelikle çözümün var olduğunu söyleyebiliriz. Verilen iki değişkenli kongrüansı

$$7x \equiv 6 - 8y \pmod{10}$$

yazarsak ve x değişkenine göre çözmeye çalışırsak ilk olarak

$$-3x \equiv 6 - 18y \pmod{10}$$

elde ederiz. Burada $(-3, 10) = 1$ olduğundan iki tarafı -3 ile bölerek

$$x \equiv -2 + 6y \pmod{10}$$

veya denk olarak

$$x \equiv 8 + 6y \pmod{10}$$

bulunur. Böylece $y = 0, 1, 2, \dots, 9$ alınarak

$$\mathcal{C} = \{(8,0), (4,1), (0,2), (6,3), (2,4), (8,5), (4,6), (0,7), (6,8), (2,9)\}$$

şeklinde tam 10 tane denk olmayan çözüm bulunur.

Burada y 'nin katsayısı olan 8 ile mod olan 10'un obebi 2 olduğundan y 'nin 0'dan 9'a kadar olan değerlerine karşılık x 'in 10 modundaki tüm değerleri alamadığı, ancak $10/2 = 5$ farklı değer aldığı görülür. Bunlar da 0, 2, 4, 6 ve 8'dir.

6.3.7. Örnek. $3x + 4y \equiv 5 \pmod{12}$ kongrüansının çözüm kümesini bulunuz.

$3x \equiv 5 - 4y \pmod{12}$ kongrüansında y değişkenine değerler vererek x değişkeninin değerlerini bulmayı deneriz. $(3, 12) = 3$ olduğundan $5 - 4y$ 'yi her zaman 3 ile bölmek mümkün değildir. O halde y 'nin uygun değerlerini bulmalıyız. Deneme ile ilk değer $y = 2$ olarak bulunur. Böylece

$$3x \equiv -3 \equiv 9 \pmod{12}$$

ve $(3, 12) = 3$ olduğundan

$$x \equiv 3 \pmod{4}$$

bulunur. O halde mod 12'deki x değerleri 3, 7 ve 11'dir. Her bir x değeri için $12/(3,12) = 4$ adet y değeri 2, 5, 8 ve 11 olarak bulunur. O halde çözüm kümesi

$$\mathcal{C} = \{(3,2), (3,5), (3,8), (3,11), (7,2), (7,5), (7,8), (7,11), (11,2), (11,5), (11,8), (11,11)\}$$

şeklinde elde edilir.

ALİŞTIRMALAR

1) a tek ise

$$ax + 3ay \equiv 1 \pmod{2}$$

kongrüansının kaç çözümü olduğunu belirleyiniz.

2) Aşağıdaki iki değişkenli kongrüansların çözüm kümelerini bulunuz.

a) $2x + 3y \equiv 5 \pmod{7}$

b) $3x - 2y \equiv 1 \pmod{11}$

c) $5x - 3y \equiv 8 \pmod{17}$

d) $3x - 6y \equiv 5 \pmod{13}$

e) $2x + 8y \equiv 5 \pmod{3}$

f) $3x + 11y \equiv 2 \pmod{7}$

g) $7x + 11y \equiv 3 \pmod{6}$

h) $17x + 11y \equiv 19 \pmod{7}$

3) Aşağıdaki iki değişkenli kongrüansların çözüm kümelerini bulunuz.

a) $3x + 5y \equiv 12 \pmod{15}$

b) $2x - 5y \equiv 6 \pmod{10}$

c) $4x + 7y \equiv 11 \pmod{14}$

d) $6x - 15y \equiv 0 \pmod{12}$

4) Aşağıdaki iki değişkenli kongrüansların çözüm kümelerini bulunuz.

a) $4x + 7y \equiv 5 \pmod{12}$

b) $3x + 7y \equiv 8 \pmod{9}$

c) $4x - 5y \equiv 6 \pmod{12}$

d) $5x - 6y \equiv 7 \pmod{12}$

5) (a,m) , (b,m) veya (c,m) 'den en az biri 1 ise

$$ax + by + cz \equiv d \pmod{m}$$

kongrüansının m^2 tane çözümü olduğunu gösteriniz.

6) $(a,m) = d > 1$ ve $(b,m) = e > 1$ ise

$$ax + by \equiv c \pmod{m}$$

kongrüansının tam m^2/d -e tane çözümü vardır. Bu çözümlerde her bir x değerinden m/d tane, her bir y değerinden ise m/e tane mevcuttur. Aynı zamanda çözüm kümesinde m/e tane farklı x değeri, m/d tane farklı y değeri vardır. Gösteriniz.

Not: a , b , c ve m 'nin hepsi aynı sayı ile bölünebilir haldeyse ilk olarak sadeleştirme yapılmalıdır.

7) Aşağıdaki iki değişkenli kongrüansların çözüm kümelerini bulunuz.

a) $2x + 3y \equiv 5 \pmod{7}$

b) $3x - 2y \equiv 1 \pmod{11}$

c) $5x - 3y \equiv 8 \pmod{17}$

d) $3x - 6y \equiv 5 \pmod{13}$

e) $2x + 8y \equiv 5 \pmod{3}$

f) $3x + 11y \equiv 2 \pmod{7}$

g) $7x + 11y \equiv 3 \pmod{6}$

h) $17x + 11y \equiv 19 \pmod{7}$

8) Aşağıdaki iki değişkenli kongrüansların çözüm kümelerini bulunuz.

a) $3x + 5y \equiv 12 \pmod{5}$

b) $2x - 5y \equiv 6 \pmod{10}$

c) $4x + 7y \equiv 11 \pmod{14}$

d) $6x - 15y \equiv 0 \pmod{12}$

e) $4x + 7y \equiv 5 \pmod{12}$

f) $3x + 7y \equiv 8 \pmod{9}$

g) $4x - 5y \equiv 6 \pmod{12}$

h) $5x - 6y \equiv 7 \pmod{12}$

9) (a,m) , (b,m) veya (c,m) 'den en az biri 1 ise

$$ax + by + cz \equiv d \pmod{m}$$

kongrüansının m^2 tane çözümü vardır. Gösteriniz.

10) Aşağıdaki üç bilinmeyenli kongrüansların çözüm kümelerini bulunuz.

a) $x + 3y + 4z \equiv 1 \pmod{5}$

b) $2x + 4y + 5z \equiv 3 \pmod{5}$

c) $2x + 4y - z \equiv 3 \pmod{5}$

d) $3x - 2y + 4z \equiv 6 \pmod{12}$

e) $3x + 6y + 9z \equiv 11 \pmod{13}$

f) $4x + 6y - 9z \equiv 36 \pmod{37}$

11) Aşağıdaki dört bilinmeyenli kongrüansların çözüm kümelerini bulunuz.

a) $x + 2y + 3z + 4t \equiv 5 \pmod{6}$

b) $x + y + z + t \equiv 1 \pmod{2}$

c) $x + 2y + z + 2t \equiv 3 \pmod{4}$

d) $3x + 2y - 4z + 6t \equiv 5 \pmod{12}$.

12) Z_{11} 'de

$$\begin{aligned}2x + y + z &= 3 \\3x - 5z &= 5 \\2x + 5y - 3z &= 7\end{aligned}$$

sistemi çözünüz.

13) Aşağıda verilen kongrüans sisteminin çözüm kümesini bulunuz.

$$\begin{aligned}2x - 3y &\equiv 1 \quad (4) \\3x - 6y &\equiv 2 \quad (12).\end{aligned}$$

14) $ax + by + cz \equiv d \quad (m)$

lineer kongrüansın çözümünün olması için gerek ve yeter şartları belirleyiniz. Bu kongrüansın çözümü varsa kaç tanedir? Olabilecek durumları açıklayınız.

15) Aşağıdaki kongrüansların çözümlerini ve çözüm sayılarını bulunuz ve sebeplerini açıklayınız.

$$\begin{array}{ll}\mathbf{a)} \quad 2x + 5y - 7z \equiv 4 \quad (3) & \mathbf{b)} \quad 2x + 4y - 5z \equiv 6 \quad (3) \\ \mathbf{c)} \quad 3x + 2y + 5z \equiv 6 \quad (4) & \mathbf{d)} \quad 4x - 2y + 6z \equiv 7 \quad (2).\end{array}$$

16) Z_m 'de

$$\begin{aligned}ax + by &\equiv c \quad (m) \\dx + ey &\equiv f \quad (m)\end{aligned}$$

lineer kongrüans sisteminin çözümünün olması için gerek ve yeter şartları belirleyiniz. Bu sistemin çözümü varsa kaç tanedir? Olabilecek durumları açıklayınız.

17) Aşağıdaki sistemlerin çözümlerini ve çözüm sayılarını bulunuz ve sebeplerini açıklayınız.

$$\mathbf{a)} \quad 2x + 3y \equiv 6 \quad (8) \qquad \mathbf{b)} \quad 3x - 2y \equiv 1 \quad (7)$$

$$5x - 2y \equiv 5 \pmod{8}$$

$$4x - 5y \equiv 4 \pmod{7}$$

$$\text{c) } 3x + 6y \equiv 9 \pmod{4}$$

$$\text{d) } 4x - 6y \equiv 15 \pmod{8}$$

$$5x + 2y \equiv 8 \pmod{4}$$

$$3x - 5y \equiv 7 \pmod{8}$$

18) $a_1x_1 + \dots + a_nx_n \equiv c \pmod{m}$ kongrüansının çözümünün olması için gerek ve yeter şartın $d = (a_1, a_2, \dots, a_n, m)$ olmak üzere $d|c$ olması olduğunu ve bu durumda tam dm^{n-1} tane çözüm olduğunu gösteriniz.

19) $(a, m) = (b, m) = 1$ ise, $ax + by \equiv c \pmod{m}$ kongrüansının tam m tane çözümü olduğunu gösteriniz.

20) $3x + 4y \equiv 5 \pmod{7}$ kongrüansının çözüm kümesini bulunuz.

21) $3x + 5y \equiv 19 \pmod{23}$ kongrüansının çözüm kümesini bulunuz.

22) $2x + 5y \equiv 3 \pmod{7}$ kongrüansının çözüm kümesini bulunuz.

23) $(a, m) = 1$ veya $(b, m) = 1$ ise $ax + by \equiv c \pmod{m}$ kongrüansının m tane çözümü olduğunu gösteriniz.

24) $(a, m) = 1$ ve $(b, m) = e > 1$ ise (veya $(a, m) = d > 1$ ve $(b, m) = 1$ ise)

$$ax \equiv c - by \pmod{m}$$

kongrüansında y 'ye değerler verilerek bulunacak tam m tane çözüm vardır. Bu m çözümde her bir x değerinden tam e tane vardır (Ancak y 'ler farklıdır). Gösteriniz.

25) $3x + 7y \equiv 6 \pmod{15}$ kongrüansının çözüm kümesini bulunuz.

26) $3x + 7y \equiv 8 \pmod{15}$ kongrüansının çözüm kümesini bulunuz.

27) $2x + 7y \equiv 5 \pmod{12}$ kongrüansının çözüm kümesini bulunuz.

28) $3x - 2y \equiv 17 \pmod{15}$ kongrüansının çözüm kümesi nedir?

29) $3x + 4y \equiv 5 \pmod{12}$ kongrüansının çözüm kümesini bulunuz.

30) $5x + 4y \equiv 7 \pmod{10}$ kongrüansının çözüm kümesini bulunuz.

31) $4x - 10y \equiv 7 \pmod{12}$ kongrüansının çözüm kümesi

- a) kaç elemanlıdır?
- b) kaç farklı x değerine sahiptir?
- c) kaç farklı y değerine sahiptir?

32) $6x - 9y \equiv 9 \pmod{18}$ kongrüansının çözüm kümesini bulunuz.

33) $2x + 3y + 4z \equiv 1 \pmod{5}$ kongrüansının çözüm kümesini bulunuz.

34) $x + 2y + 3z \equiv 4 \pmod{5}$ kongrüansının çözüm kümesini bulunuz.

35) $2x + 3y + 5z \equiv 10 \pmod{12}$ üç değişkenli kongrüansının çözüm kümesini bulunuz.

36) $2x + 3y + 4z \equiv 10 \pmod{12}$ üç değişkenli kongrüansının çözüm kümesini bulunuz.

37)
$$\begin{aligned} 4x + 3y &\equiv 3 \pmod{14} \\ 5x + 2y &\equiv 9 \pmod{14} \end{aligned}$$

kongrüans sisteminin çözüm kümesini bulunuz.

38)
$$\begin{aligned} 2x + 5y &\equiv 11 \pmod{13} \\ 3x + 4y &\equiv 6 \pmod{13} \end{aligned}$$

kongrüans sisteminin çözüm kümesini bulunuz.

39) $\mathbb{Z}_{11}$ 'de

$$\begin{aligned} 2x + 3y - z &= 7 \\ 3x - y + 4z &= 5 \\ 4x - 3z &= 7 \end{aligned}$$

denklem sisteminin çözüm kümesini bulunuz.

7. KONGRÜANS SİSTEMLERİ

Bu bölümde sayılar teorisinin en temel konularından birisi olan kongrüans sistemlerini ele alacağız. Çok çeşitli kongrüans sistemleri var olmakla beraber biz burada sadece aynı moda sahip olan iki değişkenli lineer kongrüansların oluşturduğu sistemleri ve bunun sonrasında da farklı modlarda verilmiş olan iki değişkenli lineer kongrüansların oluşturduğu sistemleri ele alacağız.

Kongrüansların aynı modda verilmesi durumunda çözüm yöntemi lineer denklem sistemleriyle tamamen aynıdır. Lineer denklem sistemlerinde kullanılan yerine koyma veya yok etme yöntemleri gibi yöntemlerden herhangi birisi kullanılarak çözüm yapılabilir. Ancak kongrüansların farklı modlarda verilmesi durumunda durum biraz daha karmaşıktır. Bu durumla ilgili en meşhur sonuç Çinlilerin kalanlar teoremi denilen teoremdir. Bu bölümde bu teoremi ve sonuçlarını ele alacağız.

7.1. AYNI MODA SAHİP KONGRÜANSLAR

Bu kısımda aynı modda verilen iki değişkenli iki kongrüansın ortak çözümünü nasıl bulacağımızı bir örnekle göreceğiz. Değişken ve denklem sayısının daha fazla olması durumunda da benzer yöntemlerle çözüm aranabilir.

7.1.1. Örnek: $x + y \equiv 8 \pmod{13}$
 $2x + 3y \equiv 12 \pmod{13}$

kongrüans sistemini çözelim.

Bu kongrüanslardan ilki -2 ile çarpılırsa

$$\begin{aligned} -2x - 2y &\equiv -16 \pmod{13} \\ 2x + 3y &\equiv 12 \pmod{13} \end{aligned}$$

ve taraf tarafa toplama yapılırsa $y \equiv -4 \equiv 9 \pmod{13}$ olur. Bu değer verilen iki kongrüanstan herhangi birisinde yerine yazılırsa, örneğin ilk kongrüanstan $9 + x \equiv 8 \pmod{13}$ ve böylece $x \equiv -1 \equiv 12 \pmod{13}$ çözümü bulunur. O halde çözüm ikilisi $(x, y) = (\overline{12}, \overline{9})$ olarak bulunur.

7.1.2. Uyarı: Aynı moda sahip kongrüansların sisteminin çözümünde lineer denklem sistemlerinin çözümüne benzer yol izlenir.

7.2. FARKLI MODLARA SAHİP KONGRÜANSLAR

Bu kısımda farklı modlardaki kongrüanslardan oluşan kongrüans sistemlerinin çözüm yöntemlerini ve bununla ilgili olarak ta Çinlilerin kalanlar teoremini ele alacağız.

7.2.1. Örnek: $x \equiv 3 \pmod{6}$
 $x \equiv 11 \pmod{15}$

kongrüans sistemini çözelim.

$x \equiv 3 \pmod{6}$ olduğundan a bir tamsayı olmak üzere $x = 3 + 6a$ ve $x \equiv 11 \pmod{15}$ olduğundan b bir tamsayı olmak üzere $x = 11 + 15b$ yazılabilir. Sistemin çözümünün olması için a ve b sayılarının

$$3 + 6a = 11 + 15b$$

olacak şekilde, denk olarak ta

$$6a - 15b = 8$$

lineer Diophant denklemini sağlayacak şekilde bulunabilmesi gerekir. Ancak $(6,15) = 3 \nmid 8$ olduğundan bu denklem çözülemez.

Şimdi de aşağıdaki kongrüans sistemini ele alalım.

$$\begin{aligned} \mathbf{7.2.2. \text{Örnek:}} \quad x &\equiv 3 \quad (4) \\ x &\equiv 5 \quad (7) \end{aligned}$$

kongrüans sistemini çözelim. Bu kongrüans sistemi örneğin dörder dörder sayıldığında 3; yedişer yedişer sayıldığında 5 kalan bir ceviz torbasındaki cevizlerin kaç tane olduğunu bulma probleminin çözümünde kullanılabilir.

$x \equiv 3 \pmod{4}$ kongrüansından a bir tamsayı olmak üzere $x = 3 + 4a$ ve benzer olarak $x \equiv 5 \pmod{7}$ kongrüansından da b bir tamsayı olmak üzere $x = 5 + 7b$ yazılabilir. O halde $3 + 4a = 5 + 7b$ ve denk olarak

$$4a - 7b = 2$$

lineer Diophant denklemini sağlanmalıdır. Burada $(4,7) = 1/2$ olduğundan çözüm vardır. Çözümü elde edebilmek için 2. Bölümde gördüğümüz gibi önce katsayıların obebini Euclid algoritmasını kullanarak bulmalı ve sonra da 2'yi bu katsayıların lineer birleşimi olarak ifade ederek bir özel çözüm elde etmeliyiz.

$$\begin{aligned} 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

olduğundan tersine gidilerek

$$\begin{aligned} 1 &= 4 - 3 = 4 - (7 - 4 \cdot 1) \\ 1 &= 4 \cdot (2) - 7 \cdot (1) \end{aligned}$$

ve böylece

$$2 = 4 \cdot (4) - 7 \cdot (2)$$

eşitliği elde edilir. Yani $a = 4$ ve $b = 2$ bulunur. Bu değerler yukarıdaki eşitliklerden birisinde yerine konularak

$$x = 3 + 4 \cdot 4 = 19$$

bulunur. Yani torbada 19 ceviz vardır. Aslında torbada 19 değil de 47, 75, 103, 131, 159, ... ceviz de olsaydı bu soru aynı kongrüanslar yardımıyla çözüldü. Yani bu kongrüans sisteminin bir çok çözümü mevcuttur. Ancak bu yöntemde x 'in hangi modda bulunacağı elde edilemez. Bu yüzden ikinci bir yöntem izlenir.

$x \equiv 3 \pmod{4}$ kongrüansından yukarıdaki gibi a bir tamsayı olmak üzere $x = 3 + 4a$ olarak yazılır. Bu değer diğer kongrüansta x yerine yazılırsa

$$3 + 4a \equiv 5 \pmod{7}$$

tek değişkenli lineer kongrüansı elde edilir. Bu kongrüansın $4a \equiv 2 \pmod{7}$ veya denk olarak $4a \equiv 16 \pmod{7}$ şeklinde yazılmasıyla $(4, 7) = 1$ olduğundan $a \equiv 4 \pmod{7}$ elde edilir. Bunu da b bir tamsayı olmak üzere $a = 4 + 7b$ şeklinde yazabiliriz. Dolayısıyla

$$\begin{aligned} x &= 3 + 4a \\ &= 3 + 4(4 + 7b) \\ &= 19 + 28b \end{aligned}$$

ve denk olarak

$$x \equiv 19 \pmod{28}$$

çözümü bulunur.

7.2.3. Sonuç. Farklı modüle sahip olan kongrüansların bir sisteminin çözümünde yerine koyan metodu kullanılır. Çıkan sonuç, modüllerin çarpımı ile elde edilen modüldedir. Ancak bu modüller aralarında asalken doğrudur. Genelde ise aşağıdaki sonuç doğrudur.

$$\begin{aligned} \mathbf{7.2.4. Teorem.} \quad &x \equiv a \pmod{m} \\ &x \equiv b \pmod{n} \end{aligned}$$

sisteminin çözümünün olması için gerek ve yeter şart $a \equiv b \pmod{(m,n)}$ olmasıdır. Eğer bir çözüm varsa bu çözüm $[m, n]$ modundadır.

İspat: İlk kongrüanstan k bir tamsayı olmak üzere $x = a + mk$ yazar ve bunu ikinci kongrüansta yerine koyarsak

$$a + mk \equiv b \pmod{n}$$

kongrüansı ve denk olarak ta

$$mk \equiv b - a \pmod{n}$$

tek değişkenli lineer kongrüansı elde edilir. Bu kongrüansın çözümünün olması için gerek ve yeter şart $(m,n)|(b - a)$ olması yani $a \equiv b \pmod{(m,n)}$ olmasıdır.

İkinci olarak bu sistemin çözümünün mevcut olduğunu varsayalım.

İlk kongrüanstan k bir tamsayı olmak üzere, $x = a + mk$ yazarız. Bu değer ikinci kongrüansta yerine konulduğunda

$$a + mk \equiv b \pmod{n}$$

veya denk olarak, $mk \equiv b - a \pmod{n}$ kongrüansı elde edilir. Bu son kongrüansın k_0 çözümü ise $\frac{n}{(m,n)}$ modundadır. Bu çözüm t bir

tamsayı olmak üzere $k = k_0 + \frac{n}{(m,n)}t$ şeklindedir. Bu yukarıdaki $x = a + mk$ eşitliğinde yerine konularak

$$\begin{aligned} x &= a + m(k_0 + \frac{n}{(m,n)}t) \\ &= a + mk_0 + \frac{mn}{(m,n)}t \end{aligned}$$

şeklinde düşünülebilir. Yani çözüm istenildiği gibi $\frac{mn}{(m,n)} = [m,n]$ modundadır.

7.2.5. Örnek. $x \equiv 3 \pmod{14}$

$$x \equiv 7 \pmod{16}$$

kongrüans sisteminin çözüm kümesini bulalım.

$(14,16) = 2$ ve $3 \equiv 7 \pmod{2}$ olduğundan 7.2.4. Teorem gereği sistemin bir çözümü vardır. $x \equiv 3 \pmod{14}$ kongrüansından a bir tamsayı olmak üzere $x = 3 + 14a$ yazılabilir. Bu değer ikinci kongrüansa yerine konulduğunda

$$3 + 14a \equiv 7 \pmod{16}$$

ve denk olarak

$$14a \equiv 4 \pmod{16}$$

kongrüansı elde edilir. Buradan 14 yerine -2 yazılarak

$$-2a \equiv 4 \pmod{16}$$

kongrüansına ulaşırız. $(2,16) = 2$ olduğundan $a \equiv -2 \pmod{8}$ ve denk olarak da $a \equiv 6 \pmod{8}$ bulunur. Son olarak b bir tamsayı olmak üzere $a = 6 + 8b$ yazıldığında

$$\begin{aligned} x &= 3 + 14a \\ &= 3 + 14(6+8b) \\ &= 87 + 112b \end{aligned}$$

ve böylece $x \equiv 87 \pmod{112}$ elde edilir. Burada $112 = [14,16]$ olduğuna dikkat ediniz.

Şimdi geçmiş binlerce yıl öncesine dayanan ve bu türlü kongrüans sistemlerinin çözümünde kullanılan bir sonucu göreceğiz. Bu sonucun burada göreceğimiz şekli problemin en basit şekli olan modların aralarında asal olduğu ve başkatsayıların 1 olduğu duruma aittir. Daha genel durumlar, alıştırılmalarda ele alınmıştır.

7.2.6. Teorem (Çinlilerin Kalanlar Teoremi). $1 \leq i < j \leq n$ için $(m_i, m_j) = 1$ ise

$$x \equiv a_1 \pmod{m_1}$$

$$\begin{aligned}x &\equiv a_2 \pmod{m_2} \\&\vdots \\x &\equiv a_n \pmod{m_n}\end{aligned}$$

lineer kongrüans sisteminin $m = \prod_{i=1}^n m_i$ modunda bir tek çözümü vardır.

İspat. $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, ..., $x \equiv a_n \pmod{m_n}$ sisteminin çözümünün olması için alınacak her kongrüans çiftinin çözümünün olması gerekeceğinden herhangi iki i ve j indeksi için

$$x \equiv a_i \pmod{m_i} \text{ ve } x \equiv a_j \pmod{m_j}$$

kongrüanslarının bir çözümünün olması gerekir. 7.2.4. Teorem gereği bu iki kongrüanslı sistemin çözümü

$$(m_i, m_j) \mid (a_j - a_i)$$

iken vardır. O halde her i, j indeks çifti için $(m_i, m_j) \mid (a_j - a_i)$ oluyorsa $x \equiv a_i \pmod{m_i}$ sisteminin çözümü olacaktır. Ancak $1 \leq i < j \leq n$ için $(m_i, m_j) = 1$ verildiğinden ve $1 \mid (a_j - a_i)$ olacağından sistemin çözümü mevcuttur.

İkinci olarak çözümün hangi modda bulunacağını belirleyelim. İlk iki kongrüansla işe başlayalım. 7.2.4. Teoreme göre ilk iki kongrüansın ortak çözümü $[m_1, m_2]$ modundadır. Bu şekilde devam edilerek sistemin $[m_1, m_2, \dots, m_n]$ modunda bir tek çözümünün olduğu görülür. Ancak m_i sayıları aralarında asal olduklarından $[m_1, m_2, \dots, m_n] = m_1 m_2 \dots m_n$ olduğu açıktır. Yani bu n kongrüanstan oluşan sistemin çözümü modların çarpımıyla elde edilen moddadır. ♣

İkinci ispat. Bir tek kongrüans varsa çözüm aşikârdır. Varsayalım ki n 'den daha az sayıda kongrüans içeren yukarıdaki tipte her sistemin çözümü olsun. $1 \leq i < j \leq n$ için, $(m_i, m_j) = 1$ olacak şekildeki m_i 'ler için

$$x \equiv a_i \pmod{m_i}$$

kongrüans sistemini ele alalım. Bu n kongrüanstan son $n-1$ tanesi varsayım gereği çözülebilirdir. Çözüm olarak ta, $M = m_2 m_3 \dots m_n$ modunda bir kongrüans elde edilir. Yani n kongrüanstan oluşan sistem, iki kongrüanstan oluşan

$$x \equiv a_1 \pmod{m_1} \text{ ve } x \equiv A \pmod{M}$$

gibi bir sisteme dönüşür. y bir tamsayı olmak üzere

$$x \equiv a_1 + m_1 y$$

yazılırsa

$$a_1 + m_1 y \equiv A \pmod{M}$$

veya

$$m_1 y \equiv A - a_1 \pmod{M}$$

elde edilir. $(m_1, M) = 1$ olduğundan, bu son kongrüansın mod M 'de bir tek çözümü vardır. Bu çözüm $y \equiv A' \pmod{M}$ ise, z bir tamsayı olmak üzere

$$y \equiv A' + Mz,$$

yazılabileceğinden

$$\begin{aligned} x &= a_1 + m_1(A' + Mz) \\ &= (a_1 + m_1 A') + m_1 Mz \end{aligned}$$

ve denk olarak

$$x \equiv a_1 + m_1 A' \pmod{m_1 M}$$

veya

$$x \equiv a_1 + m_1 A' \pmod{m_1 m_2 \dots m_n}$$

şeklinde çözümün tekliği elde edilir. ♣

7.2.7. Örnek. $x \equiv 6 \pmod{17}$

$$x \equiv 4 \pmod{11}$$

$$x \equiv 5 \pmod{6}$$

kongrüans sisteminin çözüm kümesini bulalım.

$(17,11) = (17,6) = (11,6) = 1$ olduğundan sistemin çözümü vardır.

$x \equiv 6 \pmod{17}$ kongrüansını a bir tamsayı olmak üzere $x = 6 + 17a$ şeklinde yazabiliriz. Bu değeri ikinci kongrüansta yerine yazarak

$$6 + 17a \equiv 4 \pmod{11}$$

kongrüansını ve denk olarak

$$17a \equiv -2 \pmod{11}$$

kongrüansını elde ederiz. Gerekli katsayı ayarlamalarından sonra bu kongrüansı

$$6a \equiv 9 \pmod{11}$$

şekline dönüştürürüz ve bunu da

$$-5a \equiv 20 \pmod{11}$$

olarak yazabiliriz. $(5,11) = 1$ olduğundan bu kongrüansın çözümü $a \equiv -4 \pmod{11}$ ya da $a \equiv 7 \pmod{11}$ şeklinde bulunur. b bir tamsayı olmak üzere $a = 7 + 11b$ olarak yazalım ve bu yukarıda yerine konulduğunda

$$\begin{aligned} x &= 6 + 17 \cdot (7 + 11b) \\ &= 125 + 187b \end{aligned}$$

olarak bulunur. Şimdi de bu değer üçüncü kongrüansta yerine konularak

$$125 + 187b \equiv 5 \pmod{6}$$

veya denk olarak

$$b \equiv 0 \pmod{6}$$

elde edilir. c bir tamsayı olmak üzere $b = 6c$ yazılarak

$$\begin{aligned} x &= 125 + 187 \cdot (6c) \\ &= 125 + 1122c \end{aligned}$$

ve sonuç olarak

$$x \equiv 125 \pmod{1122} \text{ bulunur.}$$

7.2.8. Örnek. $x \equiv 8 \pmod{5}$

$$x \equiv 5 \pmod{3}$$

$$x \equiv 11 \pmod{7}$$

$$x \equiv 2 \pmod{4}$$

kongrüanslarının ortak çözümünü bulalım.

$(5,3) = (5,7) = (5,4) = (3,7) = (3,4) = (7,4) = 1$ olduğundan çözüm vardır. İlk kongrüanstan a bir tamsayı olmak üzere

$$x = 8 + 5a$$

yazılır ve ikinci kongrüansta yerine yazılırsa

$$8 + 5a \equiv 5 \pmod{3}$$

ve denk olarak

$$2a \equiv 2 \pmod{3}$$

bulunur. $(2,3) = 1$ olduğundan $a \equiv 1 \pmod{3}$ bulunur. b bir tamsayı olmak üzere $a = 1 + 3b$ yazılırsa x değeri

$$\begin{aligned} x &= 8 + 5(1 + 3b) \\ &= 13 + 15b \end{aligned}$$

olarak elde edilir. Bu değer üçüncü kongrüansta yerine konulduğunda

$$8 + 15b \equiv 11 \pmod{7}$$

ve böylece de $b \equiv 3 \pmod{7}$ elde edilir. c bir tamsayı olmak üzere

$$b = 3 + 7c$$

yazılarak yukarıda yerine konulursa

$$\begin{aligned} x &= 8 + 15b \\ &= 8 + 15 \cdot (3 + 7c) \\ &= 53 + 105c \end{aligned}$$

elde edilir. x 'in bu değeri son kongrüansta yerine konularak

$$53 + 105c \equiv 2 \pmod{4}$$

ve buradan

$$c \equiv 1 \pmod{4}$$

elde edilir. d bir tamsayı olmak üzere

$$c = 1 + 4d$$

yazılarak

$$\begin{aligned} x &= 53 + 105(1 + 4d) \\ &= 158 + 420d \end{aligned}$$

ve denk olarak

$$x \equiv 158 \pmod{420}$$

sonucuna ulaşılır.

ALIŞTIRMALAR

1) $m + n = 7$ ise

$$x \equiv a \pmod{m}$$

$$x \equiv 2a \pmod{n}$$

sisteminin çözümü var mıdır?

2)

$$x \equiv a \pmod{m}$$

$$x \equiv a \pmod{mn}$$

sisteminin çözümünün

$$x \equiv a \pmod{mn}$$

olduğunu gösteriniz.

3)

$$x \equiv a \pmod{m}$$

$$x \equiv a \pmod{n}$$

sisteminin çözümünün $x \equiv a \pmod{[m,n]}$ olduğunu gösteriniz.

4)

$$x \equiv a \pmod{m_1}$$

$$x \equiv a \pmod{m_2}$$

$$x \equiv a \pmod{m_3}$$

kongrüans sisteminin çözümünün $x \equiv a \pmod{[m_1, m_2, m_3]}$ olduğunu gösteriniz.

5)

$$x \equiv 2 \pmod{3}$$

$$x \equiv 2 \pmod{4}$$

$$x \equiv 2 \pmod{6}$$

kongrüans sisteminin çözümünü bulunuz.

$$\begin{array}{ll} 6) & x \equiv 1 \quad (2) \\ & x \equiv 1 \quad (3) \\ & x \equiv 1 \quad (4) \end{array}$$

kongrüans sisteminin çözümü nedir?

7) Bir torba ceviz 7'şer 7'şer, 9'ar 9'ar ve 11'er 11'er sayılınca hep 2 ceviz kalıyor. Torbada 1.000 ile 1.500 arasında ceviz olduğu bilindiğine göre kaç ceviz vardır?

8) Çinlilerin kalan teoremini ispat ediniz:

“ $m_1, m_2, \dots, m_n$ ikişer ikişer asal olmak üzere

$$\begin{array}{ll} x \equiv a_1 & (m_1) \\ x \equiv a_2 & (m_2) \\ \vdots & \\ x \equiv a_n & (m_n) \end{array}$$

lineer kongrüans sisteminin $m_1 m_2 \dots m_n$ modunda bir tek çözümü vardır.”

9) Çinlilerin kalan teoreminin aşağıdaki farklı halini ispatlayınız:

“ $m_1, \dots, m_s$ ikişer ikişer asal olan tamsayılar olsun.

$$M = m_1 \dots m_s$$

diyelim. Her bir i için $(a_i, m_i) = 1$ olacak şekilde $a_1, \dots, a_s$ tam sayılarını alalım. Bu durumda

$$\begin{array}{ll} a_1 x \equiv b_1 & (m_1) \\ \vdots & \\ a_s x \equiv b_s & (m_s) \end{array}$$

sisteminin M modunda bir tek çözümü vardır. ”

$$\begin{array}{ll}
 10) & a_1x \equiv b_1 \quad (m_1) \\
 & a_2x \equiv b_2 \quad (m_2) \\
 & \vdots \\
 & a_nx \equiv b_n \quad (m_n)
 \end{array}$$

kongrüans sisteminin $[m_1, m_2, \dots, m_n]$ modunda bir tek çözümü vardır. Gösteriniz. (bu Çinlilerin kalan teoreminin genel hali olarak bilinir)

$$\begin{array}{ll}
 11) & x \equiv 2 \quad (3) \\
 & x \equiv 3 \quad (5) \\
 & x \equiv 2 \quad (7)
 \end{array}$$

sistemi Çinlilerin kalan teoreminden faydalanarak çözünüz.

12) Her bir n değeri için her biri 1'den büyük bir tam kareye bölünebilen n ardışık sayının varlığını gösteriniz.

13) 50 kişiyi geçmeyen bir sınıfta, Sayılar Teorisi dersini alan öğrenciler Çinlilerin kalan teoremini çalışmak üzere eşit gruplara bölünmeye çalışıyorlar. Üçerli gruplara bölünmek istediklerinde 2 öğrenci, dörderli gruplara bölünmek istediklerinde 1 öğrenci artıyor. Beşerli gruplar yapabilmeleri için öğretim üyesinin de bir grupta yer alması gerekiyor. Sınıfta kaç kişi vardır ?

$$\begin{array}{ll}
 14) & x \equiv 1 \quad (2) \\
 & x \equiv 2 \quad (3) \\
 & x \equiv 3 \quad (4)
 \end{array}$$

kongrüans sistemi sağlayan x değeri için, $100 < x < 110$ olduğu bilindiğine göre x nedir?

$$\begin{array}{ll}
 15) & x \equiv 3 \quad (5) \\
 & x \equiv 2 \quad (6) \\
 & x \equiv 1 \quad (15)
 \end{array}$$

kongrüans sisteminin çözümü nedir?

$$\begin{array}{ll}
 16) & x \equiv 2 \quad (3) \\
 & x \equiv 3 \quad (6)
 \end{array}$$

kongrüans sisteminin çözümü nedir?

$$\begin{array}{ll} 17) & x \equiv 1 \quad (2) \\ & x \equiv 3 \quad (4) \\ & x \equiv 3 \quad (6) \end{array}$$

kongrüans sisteminin çözümü nedir?

$$\begin{array}{ll} 18) & x \equiv 1 \quad (3) \\ & x \equiv 5 \quad (8) \\ & x \equiv 11 \quad (17) \end{array}$$

kongrüans sisteminin çözümü nedir?

$$\begin{array}{ll} 19) & x \equiv 1 \quad (2) \\ & x \equiv 2 \quad (3) \\ & x \equiv 3 \quad (5) \\ & x \equiv 5 \quad (7) \end{array}$$

kongrüans sisteminin çözümü nedir?

20) $m = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ birleşik bir sayı olsun. $ax \equiv b \pmod{m}$ kongrüansının çözümlerinin, modları aralarında asal olan asal kuvvetler olan $ax \equiv b \pmod{p_i^{e_i}}$ kongrüanslarının ortak çözümüyle aynı olduğunu gösteriniz.

$$21) \quad 3x \equiv 11 \pmod{2.275}$$

kongrüansını daha küçük modlara sahip kongrüansların bir sistemine dönüştürerek çözünüz.

$$\begin{array}{ll} 22) & x^2 \equiv 1 \quad (3) \\ & x \equiv 2 \quad (4) \end{array}$$

kongrüans sisteminin genel çözümünü bulunuz.