ÖKLİD ALGORİTMASI

Cemal Koç *

1. Öklid Algoritması

Daha önceki bir yazımızda (bkz. Cilt 2, Sayı 1, s.17) tamsayılar ve polinomlar için bölme algoritmasını vermiştik. Bu yazımızda bölmenin yinelenmesi ile elde edilen Öklid algoritmasını vereceğiz. Öklid algoritmasının uygulaması olarak en büyük ortak bölenin varlığını ve asal çarpanlara ayırmanın tekliğini göreceğiz. Yazımız boyunca söyleyeceklerimiz hem tamsayılar hem de polinomlar için geçerli olacaktır. Bu ifadeler yerine göre sayılar, yerine göre polinomlar için kullanılacağından yazı içinde sık sık "sayısı (polinomu)" yazılımı yer alacaktır; bu ifadenin tam sayılar için yazıldığını ancak tamsayı sözcüğü yerine polinom sözcüğü konulduğunda da geçerli olduğunu belirtmektedir. $a, b, c, d, r_1, r_2, \ldots$ gibi harflerle hem tamsayılar hem de polinomları göstereceğiz. Şimdi Öklid Algoritmasını verelim:

a ve b iki tamsayı (polinomu) ve $b \neq 0$ olsun. a yı b ye bölmekle elde edilen kalan r_1 ve $r_1 \neq 0$ ise b yi r_1 e bölmekle elde edilen r_2 ve $r_2 \neq 0$ ise r_1 i r_2 ye bölmekle elde edilen kalan r_3 ve $r_3 \neq 0$ olsun. Böylece bir

$$a, b, r_1, r_2, \ldots \qquad (1)$$

dizisi elde edilir. Bu dizi sayılar dizisi ise salt değerce (polinomlar dizisi ise derece olarak) küçüleceğinden sıfıra ulaşmalıdır yani bir yerde kalanlardan biri kendinden sonrakine tam bölünmelidir.

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n + r_{n+1} \\ r_n &= q_{n+2} r_{n+1} \end{aligned} \qquad (2)$$

eşitlikleri elde edilir. Burada sıfırdan farklı son kalan olan r_{n+1} kalanının elde edilişi için yapılan bu ardışık bölme işlemleri topluluğuna *Öklid algoritması* denir.

*ODTÜ Matematik Bölümü öğretim üyesi

Şimdi herkesin aklına gelecek soru "r_{n+1} in önemi ne?" olacaktır. Bir kez r_{n+1} kalanlar dizisinin bütün terimlerini dolayısıyla da a ile b yi böler. (Neden?) Yani r_{n+1}, a ile b nin ortak bölenidir. İkincisi, a ile b nin her ortak böleni r_{n+1}'i böler çünkü (2) eşitliklerine bakarsak

$$d|a, d|b \Rightarrow d|b, d|r_1 \Rightarrow d|r_1,\ d|r_2 \Rightarrow \cdots \Rightarrow d|r_{n-1}, d|r_n \Rightarrow d|r_{n+1}$$

olduğunu görürüz. Demek ki r_{n+1}, a ile b nin öyle bir ortak böleni ki her ortak bölen ile bölünebiliyor. Böyle ortak bölenlere *en büyük ortak bölen* denir.

2. OBEB, OKEK

Biçimsel bir tanım verecek olursak,

Tanım: a, b, c üç tamsayı (polinom) olsun. Eğer

(1) $c \mid a,\ c \mid b$ ve

(2) $d \mid a,\ d \mid b \Rightarrow d \mid c$ ise

c'ye a ile b'nin *en büyük ortak böleni* denir.

Benzer biçimde

(1′) $a \mid c,\ b \mid c$ ve

(2′) $a \mid d,\ b \mid d \Rightarrow c \mid d$ ise

c'ye a ile b'nin *en küçük ortak katı* denir.

Öklid algoritması bize a ile b nin r_{n+1} gibi bir en büyük ortak böleninin varlığını gösteriyor. Peki, bu en büyük ortak bölen en azından bir anlamda tek mi? c_1 ve c_2, a ile b nin en büyük ortak bölenleri ise c_1 bölen, c_2 en büyük ortak bölen alınarak $c_1|c_2$, c_2 bölen, c_1 en büyük ortak bölen alınarak $c_2|c_1$ olduğu görülür yani $c_2 = c_1 c_1', c_1 = c_2 c_2'$ ve dolayısıyla $c_2 = (c_2 c_2')c_1'$ çıkar. Demek ki $c_2' c_1' = 1$ olur, yani tamsayılarda $c_2 = \mp c_1$, polinomlarda $c_2 = c_1$ (sıfırdan farklı bir sabit) olmaktadır. a ve b gibi iki tamsayının pozitif en büyük ortak bölenine (iki polinomun yalın

(başkatsayısı 1 olan) en büyük ortak bölenine) *ortak bölenlerin en büyüğü* (OBEB) denir ve (a,b) ile gösterilir. Görüldüğü gibi yukardaki adlandırmada her ne kadar "en büyük" nitelemesi varsa da tanımın büyüklük sıralaması ile ilgisi yoktur. Yaptığımız tartışmadan *OBEB'in varlığını ve tekliğini* söyleyebiliyoruz.

Yukarıdaki (2) eşitliklerinde herbir kalanı kendinden önce gelen türünden yazar arka arkaya yerine koymalar yaparsak,

$$\left.\begin{array}{rcl} r_{n+1} &=& r_{n-1} - q_{n+1}r_n \\ r_n &=& r_{n-2} + q_n r_{n-1} \\ r_{n-1} &=& r_{n-3} + q_{n-1}r_{n-2} \\ &\vdots& \end{array}\right\} \Rightarrow$$

$$\begin{aligned} r_{n+1} &= r_{n-1} + q_{n+1}r_n \\ &= r_{n-1} + q_{n+1}(r_{n-2} + q_n r_{n-1}) \\ &= \cdots \end{aligned}$$

Sonuçta da

$$r_{n+1} = a_1 a + b_1 a$$

olacak biçimde a_1 ve b_1 öğeleri buluruz. Gerekirse r_{n+1}'i tersinir bir öğe ile çarparak hem OBEB'in varlığını hem de

$$(a,b) = a^*a + b^*b \qquad (3)$$

yazılabileceğini görmüş oluyoruz.

Örnekler. 1) 67367 ile 51813 sayılarının OBEBini ve

$$(67367, 51813) = a^*67367 + b^*51813$$

eşitliğini sağlayan iki a^*, b^* sayısı bulunuz. Kolaylık olsun diye işlemleri şu çizelge yardımıyla yapalım:

Bölüm		1	3	3	51
B-B *	67367	51813	15554	5151	101
	51813	46662	15453	5151	
Kalan	15554	5151	101	0	

* Bölünen-Bölen

Böylece son sıfırdan farklı kalan olarak 101 buluruz. Demek ki OBEB 101 dir. Ayrıca

$$\begin{aligned} 101 &= 15554 - 3 \cdot 5151 \\ 5151 &= 51813 - 3 \cdot 15554 \\ 15554 &= 67367 - 51813 \end{aligned}$$

eşitliklerinden

$$\begin{aligned} 101 &= 15554 - 3(51813 - 3 \cdot 15554) \\ &= 10 \cdot 15554 - 3 \cdot 51813 \\ &= 10 \cdot (67367 - 51813) - 3 \cdot 51813 \\ &= 10 \cdot 67367 - 13 \cdot 51813 \end{aligned}$$

bulunur. Demek ki $a^* = 10$, $b^* = -13$ alınabilir.

2) $2x^3 + 3x^2 - 3x - 2$ ve $-x^3 - 2x^2 + x + 2$ polinomlarının ortak bölenlerinin en büyüğünü bulup bunu

$$a^*(2x^3 + 3x^2 - 3x - 2) + b^*(-x^3 - 2x^2 + x + 2)$$

biçiminde yazınız.

	-2	$x+1$
$2x^3 + 3x^2 - 3x - 2$	$-x^3 - 2x^2 + x + 2$	$-x^2 - x + 2$
$2x^3 + 4x^2 - 2x - 4$	$-x^3 - 2x^2 + x + 2$	
$-x^2 - x + 2$	0	

Demek ki son kalan $-x^2 - x + 2$'dir. Yalınlaştırmak için bunu -1 ile çarparsak $OBEB = x^2 + x - 2$ elde ederiz. Ayrıca

$$\begin{aligned} -x^2 - x + 2 &= 2x^3 + 3x^2 - 3x - 2 \\ &\quad +(-2)(-x^3 - 2x^2 + x + 2) \end{aligned}$$

den $a^* = 1$ ve $b^* = -2$ alınabileceği görülür.

Alıştırma. Herhangi üç a, b, c tamsayısı (polinomu) verildiğinde $b \neq 0$ ise $((a,b),c) = (a,(b,c))$ olacağını ve bu ortak değerin a, b, c nin bir ortak böleni olduğunu ve a, b, c nin her ortak böleninin katı olduğunu gösteriniz. (Bundan dolayı bu öğeye a, b, c nin OBEBi denir ve (a,b,c) ile gösterilir. Aynı sonuç daha fazla sayıdaki tamsayı ya da polinom için yinelenebilir.)

Yukarıda elde ettiğimiz (3) bağıntısı sayılar kuramının en temel bağıntılarından biridir. Özellikle bu bağıntıya dayanan ve şimdi kanıtlayacağımız şu önerme her yerde kullanılmaktadır:

a ile b sayılarının (polinomlarının) aralarında asal olması için gerek ve yeter koşul

$$aa^* + bb^* = 1 \qquad (4)$$

olacak biçimde a^* ve b^* sayılarının (polinomlarının) bulunmasıdır.

a ile b aralarında asal demek $(a,b) = 1$ demek olduğu için önermenin bir yönü (3) bağıntısının doğrudan sonucudur. Öbür yönünü görmek için ise $a^*a + b^*b = 1$ olduğunu varsayalım. Eğer a ile b nin bir c ortak böleni bulunsaydı

$$c|a, \quad c|b \Rightarrow c|1$$

olurdu ve dolayısıyla $c = \mp 1$ çıkardı. Bu ise $(a,b) = 1$ yani a ile b aralarında asal demektir.

Örnek 1. Ardışık sayılar aralarında asaldır:

$$(n+1)-n=1.$$

Örnek 2. $x^5+3x^4-x^2+x+1$ ve x^5+3x^4-1 polinomlarının OBEB'i nedir?

Bunu bulmak için

$$x^5+3x^4-1-(x^5+3x^4-x^2+x+1)=x^2-x-2$$

eşitliğinden yararlanalım. Bu iki polinomun her ortak böleni x^2-x-2 nin de bölenidir. Yani yalın ortak bölen adayları

$$x,\ x+1,\ x-2,\ x^2-x-2$$

dir. $x=-1$ ve $x=2$ için x^5+3x^4-1 in değeri 0 olmadığından $x+1$ ile $x-2$ ortak bölen olamaz öyleyse verilen polinomlar aralarında asaldır.

Örnek 3. Eğer $P(x)$ ve $Q(x)$ aralarında asal polinomlarsa, x in her m tamdeğeri için $P(m)$ ve $Q(m)$ sayıları aralarında asaldır. Çünkü, $P(x)$ ile $Q(x)$ aralarında asal olduğundan

$$P^*(x)P(x)+Q^*(x)Q(x)=1$$

olacak biçimde $P^*(x)$ ve $Q^*(x)$ polinomları bulunabilir oysa bu bize

$$P^*(m)P(m)+Q^*(m)Q(m)=1$$

eşitliğini verir bu ise $P(m)$ ile $Q(m)$ nin aralarında asal olduğunu gösterir.

Alıştırma. (UMO 1959) Hiçbir n doğal sayısı için $\frac{21n+4}{14n+3}$ kesrinin kısaltılamayacağını gösteriniz.

3. Asal Çarpanlara Ayırma

Şimdi de (4) bağıntısından yararlanarak her sayı ve polinomun esas itibariyle tek türlü olarak asalların çarpımıyla oluşturulabileceğini görelim. Anımsayacak olursak (bkz. Matematik Dünyası, Cilt 3, Sayı 3, s.1) asal sayılar tam iki tane pozitif tam böleni bulunan pozitif sayılar ve asal polinomlarsa tam iki tane yalın (monik) böleni bulunan yalın polinomlardı.

Şimdi göstermek istediğimiz ve ilkokul sıralarında bile kullandığımız sonucu ifade edelim:

Her a pozitif tamsayısı (yalın polinomu)

$$a=p_1^{s_1}p_2^{s_2}\cdots p_m^{s_m}$$

biçiminde tek türlü olarak asal çarpanlara ayrılabilir. Bu çarpanlamanın varlığını görmek için asal çarpanlara ayrılamayan sayılarını (polinomların) varlığını düşünelim. Bunların en küçüğü (en küçük dereceli lerinden biri) k olsun. $k=1$ ya da $k=p$ (asal) olamaz (neden?), öyleyse k nın gerçek bölenleri vardır: $k=qr;\ 1<q<k,\ 1<r<k$ $(0<der(q)<der(k)\ 0<der(r)<der(k))$ k nın seçiliş biçimi nedeniyle bundan küçük olan q ve r asal çarpanlara ayrılabilir:

$$q=p_1^{e_1}\cdots p_m^{e_m},\quad r=p_1^{f_1}\cdots p_m^{f_m}$$

bu ise

$$k=qr=p_1^{e_1+f_1}\cdots p_m^{e_m+f_m}$$

olması demektir. Sonuç k nın seçilişi ile çeliştiği için seçilen biçimde bir k sayısı dolayısıyla da asal çarpanlara ayrılamayan pozitif tamsayı bulunamaz.

Çarpanlamanın tekliğine gelince, p_i ve q_j ler asal olmak üzere

$$a=p_1^{e_1}\cdots p_m^{e_m}=q_1^{f_1}\cdots q_t^{f_t};$$

eşitliğinden $m=t, p_1=q_1,\ldots,p_m=q_m$ sonucuna ulaşmamız gerekiyor. Bunun için ise yukarda belirttiğimiz (4) bağıntısına gerek duyuyoruz. Şöyle ki, p asal $p|rs, p\nmid r$ ise $(p,r)=1$ demektir ve dolayısıyla

$$1=p^*p+r^*r\Rightarrow s=p^*ps+r^*rs\Rightarrow p|s$$

çıkar. Demekki bir asal bir çarpımı bölerse çarpanlardan en az birini böler, bu ise $p_1^{e_1}\cdots p_m^{e_m}=q_1^{t_1}\cdots q_t^{f_t}$ eşitliğinden arka arkaya uygulamalarla p_i lerle q_i lerin sıralama dışında aynı olacakları sonucunu verecektir. Ayrıntıları düşünmeyi okura bırakıyoruz.

Asal çarpanlara ayrılma özelliği tam sayıların ana özelliğidir. Bu özellik bilindikten sonra ele alınamayacak problem yoktur denilebilir. Asal çarpanlara ayırmanın yararlarından biri bölenleri belirlemektir. Gerçekten

$$a=p_1^{s_1}\cdots p_m^{s_m}$$

nin pozitif (yalın) bölenlerinin

$$a=p_1^{t_1}\cdots p_m^{t_m}\quad(0\le t_1\le s_1,\ldots,0\le t_m\le s_m)$$

biçiminde belirlenebileceğini ve bu bölenlerin $(s_1+1)\cdots(s_m+1)$ tane olduğunu hemen söyleyebiliriz. Bundan yararlanılarak

$$a=p_1^{s_1}\cdots p_m^{s_m},\ b=p_1^{t_1}\cdots p_m^{t_m},\ (0\le s_i,\ 0\le t_i)$$

ile belirli a ve b için en büyük ortak bölen ve en küçük ortak katı sırasıyla

$$\begin{aligned}(a,b) &= p_1^{k_1}\cdots p_m^{k_m};\ k_i = kuc(s_i,t_i)\\ [a,b] &= p_1^{b_1}\cdots p_m^{b_m};\ b_i = buy(s_i,t_i)\end{aligned}$$

biçiminde belirtebiliriz. Böylece en küçük ortak katın varlığını da görmüş oluyoruz. Buradan hemen

$$ab = [a,b](a,b)$$

eşitliğini de yazabiliriz.

Bir alıştırma ve bir problem çözümü ile yazımıza son veriyoruz. Alıştırmada verilen dost sayı çiftleri MS826 ve 301 yılları arasında yaşamış bulunan Harranlı Tabit Bin Kurra tarafından elde edilmiş. Çok sonraları Fermat ve Descartes tarafından yeniden bulunmuş ve 1747'de de Euler tarafından incelenmişlerdir.

Alıştırma. m ve n gibi iki doğal sayıdan birinin öz bölenleri toplamı diğer sayıya eşit oluyorsa bu sayı çiftine *dost sayılar* denir.

1) 284 ve 220 sayılarının dost sayılar olduğunu gösteriniz.

2) $p = 3\cdot 2^{n-1}-1$, $q = 3\cdot 2^n - 1$ ve $r = 9\cdot 2^{n-1}-1$ asal sayılarsa $M = 2^n pq$ ve $N = 2^n r$ sayılarının dost sayılar olacağını gösteriniz. $n \le 4$ için buradan elde edilebilecek dost sayıları belirtiniz.

Problem. (1991 Amerikan Matematik Olimpiyadı) Bir ABC üçgeninde A açısı B açısının iki katı, C açısı geniş açı ve a,b,c kenar uzunlukları tamsayılardır. Mümkün olan en küçük çevreyi belirleyip kanıtını yapınız.

Çözüm. Çevresi en küçük olan ABC üçgenini gözönüne alalım. A daki iç açıortayın BC yi kestiği nokta N olsun. Açıortay bağıntısından

$$\frac{|NB|}{C} = \frac{|NC|}{b} = \frac{|NB|+|NC|}{b+c} = \frac{a}{b+c}$$

elde edileceği için $|NC| = \frac{ab}{b+c}$ çıkar.

Oysa ANC ve BAC üçgenleri benzer olacağından

$$\frac{|NC|}{b} = \frac{b}{a} \text{ yanı } \frac{a}{b+c} = \frac{b}{a}$$

Sonuçta da $a^2 = b(b+c)$ elde edilir. Burada b ile $b+c$ aralarında asal olmalıdır. Değilse b ile c nin 1 den farklı bir d ortak böleni bulunurdu, bu ortak bölen a yı da bölerdi. Kenarları $\frac{a}{d}, \frac{b}{d}, \frac{c}{d}$ olan üçgense hem ABC ye benzer hem de daha küçük çevreli olurdu. Bu ise ABC nin seçilişine uymaz. Böylece aralarında asal b ve $b+c$ sayılarının tam kare olduklarını çıkarıyoruz:

$$b = m^2,\ b+c = n^2,\ a = mn;\ (m,n\in\mathbb{Z}^+)$$

ABC 'nin üçgen olma koşulu $c < a+b$ eşitsizliğini; $\hat{C}$ açısının geniş açı olması koşulu da $c^2 > a^2+b^2$ eşitsizliğini veriyor. Bu eşitsizlikleri m ve n türünden yazdığımızda

$$\sqrt{3} < \frac{n}{m} < 2$$

elde ediyoruz. Bu eşitsizlikler $m = 1,2$ ya da 3 olduğunda hiçbir n için sağlanmazlar. Buna göre $m \ge 4$ ve $n^2 \ge 3m^2 \ge 48$ yani $n \ge 7$ olmalıdır; dolayısıyla da

$$a+b+c = mn+n^2 \ge 4.7+7^2 = 77$$

olmalıdır. Oysa $m = 4, n = 7$ alınarak elde edilen $a = 28, b = 16, c = 33$ kenar uzunluklarına sahip üçgen çevresi 77 olan ve problemin koşullarını sağlayan bir üçgendir. Öyleyse bu üçgen istenen üçgendir.

KAYNAKÇA

[1] B.L. van der Waerden: *A History of Algebra*, Springer-Verlag, Berlin, 1985.