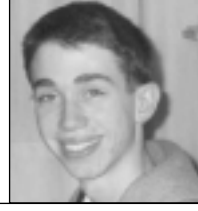




Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (1)

Euler φ fonksiyonu

E. Mehmet Kırıl* / luzumi_86@yahoo.com



Yazımıza iki kolay anlaşılır soruyla başlayalım:

Soru 1. $x/180$ şeklinde yazılan 1'den küçük kaç pozitif ve sadeleşmeyen kesir vardır?

Soru 2. 15'le ortak böleni olmayan 15'ten küçük pozitif doğal sayıların toplamı kaçtır?

Bu tür soruları yanıtlamak için "Euler φ fonksiyonu" adı verilen bir fonksiyondan yararlanılır. Sayılar kuramının en önemli fonksiyonlarından biri olan Euler φ fonksiyonu şöyle tanımlanır: $\varphi(n)$, n 'den küçüğeşit ve n 'yle aralarında asal (yani n 'yle en büyük ortak böleni 1 olan) pozitif sayıların sayısıdır. Daha matematiksel bir deyişle, $\varphi(n)$ sayısı, $0 < d \leq n$ ve $\text{EBOB}(d, n) = 1$ özelliğini sağlayan d 'lerin sayısıdır¹.

Örneğin, 10'dan küçük ve 10'a asal olan sayılar 1, 3, 7, 9 olduğundan, $\varphi(10) = 4$ 'dür. Okur, $\varphi(6) = 2$, $\varphi(8) = 4$, $\varphi(12) = 4$, $\varphi(25) = 20$ eşitliklerinin doğruluğunu sınavabilir.

$\varphi(1) = 1$ 'dir elbette.

Eğer p asalsa, $\varphi(p) = p - 1$ eşitliği geçerlidir, çünkü bir asal kendinden küçük her sayıya asaldır. Kolayca görüleceği üzere bunun tersi de doğrudur: $\varphi(n) = n - 1$ ise n bir asal sayıdır.

İlk amacımız $\varphi(n)$ 'nin değerini kolayca hesaplayan bir formül bulmak. Bunun için şu adımları atacağız:

Birinci Adım. Eğer n ve m birbirine asal iki sayıysa, $\varphi(nm) = \varphi(n)\varphi(m)$ eşitliğini kanıtlayacağız.

Böylece, bir n sayısını

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

olarak çarpanlarına ayırırsak (p_i 'ler birbirinden değişik asal sayılar), o zaman,

$$\varphi(n) = \varphi(p_1^{a_1}) \varphi(p_2^{a_2}) \dots \varphi(p_k^{a_k})$$

eşitliğini kanıtlamış olacağız.

İkinci Adım. Birinci adımı aştığımızı varsayarsak, $\varphi(n)$ sayısını hesaplayabilmek için, bir p asalı ve bir a pozitif doğal sayısı için, $\varphi(p^a)$ sayısını hesaplamasını bilmemiz gerektiğini anlarız. $\varphi(p^a)$ sa-

yısını bulmak oldukça kolay. Pek yakında, $\varphi(p^a) = p^a - p^{a-1}$ eşitliğini kolaylıkla kanıtlayacağız.

Bu iki adımı başarıyla tamamlarsak, aşağıdaki sonucu bulmuş oluruz.

Ana Teorem. Eğer $n > 1$ doğal sayısı asal çarpanlarına,

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

olarak ayrılıyorsa, o zaman,

$$\begin{aligned} \varphi(n) &= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1}) \\ &= n(1 - 1/p_1)(1 - 1/p_2) \dots (1 - 1/p_k) \end{aligned}$$

dir.

Örneğin, yukardaki teoreme göre,

$$\begin{aligned} \varphi(1323) &= \varphi(3^3 \times 7^2) = \varphi(3^3) \times \varphi(7^2) \\ &= (3^3 - 3^2)(7^2 - 7) = 18 \times 42 = 756. \end{aligned}$$

Demek ki 1323'ten küçük 1323'e asal tam 756 tane sayı var, yukardaki teorem doğruysa elbet...

Teoremi kullanarak birinci soruyu hemen şimdi yanıtlayabiliriz. Belli ki soru bizden $\varphi(180)$ sayısını istiyor. Yukardaki teoremi bildiğimizi varsayarsak, sorunun pek ilginçliği kalmadı! İkinci soruyu da hemen şimdi yanıtlayabiliriz ama yanıtı daha sonraya bırakıp hemen teoremimizin kanıtına girişelim.

Dediğimiz gibi teoremi iki adımda kanıtlayacağız. Daha kolay olan ikinci adımdan başlayalım:

Önsav 1. Eğer p asalsa, $\varphi(p^a) = p^a - p^{a-1}$ 'dir.

Kanıt: p^a ile ortak böleni olmayan p^a 'dan küçüğeşit sayıları sayacağımıza, tam tersine, p^a ile ortak böleni olan p^a 'dan küçüğeşit sayıları sayalım.

p bir asal olduğundan, p^a 'yla ortak böleni olan bir sayı mutlaka p 'ye bölünür. Demek ki p^a 'dan küçüğeşit ve p^a ile ortak böleni olan sayılar

$$p, 2p, 3p, \dots, (p^{a-1})p$$

sayılarıdır ve bunlardan tam p^{a-1} tane vardır. p^a 'dan küçüğeşit toplam p^a tane sayı olduğundan, $\varphi(p^a) = p^a - p^{a-1}$ dir. \square

Sıra birinci adıma geldi. Eğer n ve m birbirine asal iki sayıysa, $\varphi(nm) = \varphi(n)\varphi(m)$ eşitliğini kanıtla-

* Üsküdar Amerikan Lisesi üçüncü sınıf öğrencisi.

1 Euler φ fonksiyonuna bazen Euler "totient" fonksiyonu denildiği olur.

yacağız. Bu adım ikincisinden daha zor. Biraz halkalar kuramı, biraz da modüler aritmetik yapacağız.

Eğer A bir halkaysa, A^* kümesinin A 'nın tersidir, yani belli bir b için $ab = 1$ eşitliğini sağlayan a elemanlarından oluşan küme olarak tanımlamıştık (sayfa 30). Sayfa 16'daki Teorem 3'e göre,

$$(Z/nZ)^* = \{\bar{a} \in Z/nZ : a \text{ ve } n \text{ aralarında asal}\}.$$

Böylece, φ 'nin tanımından şu sonuç çıkar:

Önsav 2. $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$. □

Eğer A ve B birer halkaysa,

$$A \times B := \{(a, b) : a \in A, b \in B\}$$

kümesi üzerine toplama ve çarpma işlemlerini şöyle tanımlayalım:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$$

Kolayca kanıtlanacağı üzere, bu iki işlemle $A \times B$ kümesi bir halka olur. Sözelimi, eğer 1_A ve 1_B , A ve B 'nin çarpma için etkisiz elemanlarıysa, o zaman $(1_A, 1_B)$, $A \times B$ halkasının çarpma için etkisiz elemanı olur, yani $1_{A \times B} = (1_A, 1_B)$ 'dir. Bu halkaya A ve B halkalarının **kartezyen çarpımı** denir.

Örneğin $Z/2Z \times Z/3Z$ kümesinin elemanları $(0, 0)$, $(1, 0)$, $(0, 1)$, $(1, 1)$, $(0, 2)$, $(1, 2)$ dir. Parantezin sol tarafındaki sayıları modülo 2, sağ tarafındaki sayıları modülo 3 toplayıp çarpabiliriz, aynen aşağıdaki gibi:

$$(1, 2) + (0, 2) = (1 + 0, 2 + 2) = (1, 4) = (1, 1),$$

$$(1, 2)(0, 2) = (1 \times 0, 2 \times 2) = (0, 4) = (0, 1).$$

Önsav 3. $(A \times B)^* = A^* \times B^*$.

Kanıt: Çok kolay, okura bırakıyoruz. □

Sonuç 4. $(Z/nZ \times Z/mZ)^*$ kümesinin $\varphi(n)\varphi(m)$ tane, $(Z/nmZ)^*$ kümesinin $\varphi(nm)$ tane ögesi var. □

Sonuç 4 bize bir şey söylemek istiyor. Eğer kanıtlamak istediğimiz $\varphi(n)\varphi(m) = \varphi(nm)$ eşitliği doğruysa, $(Z/nZ \times Z/mZ)^*$ ve $(Z/nmZ)^*$ kümelerinin eleman sayısı aynı olmalı diyor. $Z/nZ \times Z/mZ$ ve Z/nmZ halkalarının da eleman sayısı aynı, her ikisinde de nm tane eleman var. Demek ki Sonuç 4, n ve m birbirine asal olduğunda $Z/nZ \times Z/mZ$ ve Z/nmZ halkalarının birbirine oldukça benzediğini söylemek istiyor. Nitekim birazdan iki halkanın birbirine benzemesinin ne demek olduğunu söyleyip, n ve m birbirine asal olduğunda, $Z/nZ \times Z/mZ$ ve Z/nmZ halkalarının birbirine çok ama çok benzediğini kanıtla-

yacağız. İstedığımız sonuç bundan çıkacak.

A ve B iki halka olsun. A 'dan B 'ye giden bir eşyapı fonksiyonu, her $x, y \in A$ için,

$$f(x + y) = f(x) + f(y)$$

$$f(xy) = f(x)f(y)$$

$$f(1) = 1$$

eşitliklerini sağlayan bir $f : A \rightarrow B$ fonksiyonudur. Görüldüğü gibi, bir eşyapı fonksiyonu A 'nın toplama ve çarpmasını B 'nin toplama ve çarpmasına dönüştürür, ayrıca A 'nın 1'ini B 'nin 1'ine yollar. Yani eşyapı fonksiyonu toplamaya, çarpmaya ve 1'e "**saygı duyar**".

Eğer bir eşyapı fonksiyonu ayrıca birebir ve örtense, yani bir eşlemeyse, o zaman A ve B halkaları arasında, elemanlarının ve işlemlerinin adları dışında bir fark yok demektir. A 'nın elemanlarının ve işlemlerinin adlarını f eşlemesini kullanarak B 'nin elemanlarına dönüştürürsek, aynen B 'nin halka yapısını buluruz. Aynı zamanda bir eşleme olan eşyapı fonksiyonlarına **eşyapı eşlemesi** diyelim.

Aralarında bir eşyapı eşlemesi olan halkalar arasında gerçekten pek bir fark yoktur, tek fark elemanlarının ve işlemlerinin adlarıdır ki bu da çok yüzeysel bir farktır. Örneğin, eğer $f : A \rightarrow B$ bir eşyapı eşlemesiye, f , A^* ile B^* arasında bir eşleme verir. Bunu kanıtlayalım:

Önsav 5. Eğer $f : A \rightarrow B$ iki halka arasında bir eşyapı eşlemesiye, $f(A^*) = B^*$ 'dir.

Kanıt: Önce $f(A^*) \subseteq B^*$ ilişkisini kanıtlayalım. $a \in A^*$ olsun. Demek ki, belli bir $x \in A$ için $ax = 1$. Şimdi her iki tarafa da f 'yi uygulayalım: $1 = f(1) = f(ax) = f(a)f(x)$. Görüldüğü gibi $f(a) \in B^*$.

Şimdi de $B^* \subseteq f(A^*)$ ilişkisini kanıtlayacağız. $b \in B^*$ olsun. $y \in B$, $by = 1$ eşitliğini sağlasın. f örten bir fonksiyon olduğundan, A 'da $f(a) = b$ ve $f(x) = y$ eşitliklerinin sağlayan a ve x vardır. Şimdi $f(ax) = f(a)f(x) = by = 1 = f(1)$. Demek ki $f(ax) = f(1)$. Ama f birebir bir fonksiyon. Demek ki $ax = 1$, yani $a \in A^*$. Dolayısıyla $b = f(a) \in f(A^*)$. □

Dikkat edilirse yukardaki kanıtta f 'nin toplamaya saygı duyduğunu kullanmadık, f 'nin sadece çarpmaya saygı duyması bize yetti. Nitekim, çarpma ile ilgili bir önerme kanıtlamak istiyorduk.

Önsav 5'e göre, n ve m birbirine asal olduğunda $\varphi(n)\varphi(m) = \varphi(nm)$ eşitliğini kanıtlamak için Z/nmZ ve $Z/nZ \times Z/mZ$ halkaları arasında bir eşyapı eşlemesi bulmak yeterli.

Bir sonraki teoremi okumadan önce, okur Z/nZ halkalarını nasıl tanımladığımızı anımsamalıdır (sayfa 14-15): Z/nZ halkalarının elemanları, belli bir $x \in Z$ için,

$$nZ + x = \{nz + x : z \in Z\}$$

altkümeleriydi. Ayrıca “ $nZ + x = nZ + y$ ancak ve ancak $n, x - y$ 'yi bölerse” önermesi anımsanmalıdır.

Teorem 6. n ve m birbirine asalsa Z/nmZ ve $Z/nZ \times Z/mZ$ halkaları arasında bir eşyapı eşleşmesi vardır. Hatta Z/nmZ halkasının her $nmZ + x$ elemanını $Z/nZ \times Z/mZ$ halkasının $(nZ + x, mZ + x)$ elemanına götüren fonksiyon bir eşyapı eşleşmesidir.

Kanıt. Her şeyden önce, teoremin ikinci tuncesinde belirtildiği gibi Z/nmZ halkasının her $nmZ + x$ elemanını $Z/nZ \times Z/mZ$ halkasının $(nZ + x, mZ + x)$ elemanına götüren bir fonksiyonun gerçekten olduğunu kanıtlamalıyız. Yandaki karede bunu niye kanıtlamak zorunda olduğumuzu bir örnekle gösterdik. Yani, eğer

$$nmZ + x = nmZ + y$$

ise,

$$nZ + x = nZ + y \text{ ve } mZ + x = mZ + y$$

eşitliklerini kanıtlamalıyız, yoksa böyle bir fonksiyon tanımlamaya hakkımız olmaz. Kanıtlayalım: $nmZ + x = nmZ + y$ ise, $nm, x - y$ 'yi böler. Dolayısıyla hem n hem de $m, x - y$ 'yi böler ve $nZ + x = nZ + y$ ve $mZ + x = mZ + y$. Demek ki teoremin ikinci tuncesinde ifade edilen fonksiyon gerçekten varmış. Bu fonksiyona f diyelim:

$$f(nmZ + x) = (nZ + x, mZ + x).$$

Şimdi f fonksiyonunun birebir olduğunu göstereyim. Diyelim $f(nmZ + x) = f(nmZ + y)$, yani $(nZ + x, mZ + x) = (nZ + y, mZ + y)$, yani

$$nZ + x = nZ + y \text{ ve } mZ + x = mZ + y.$$

Demek ki hem n hem de $m, x - y$ 'yi bölüyor. Ama n ve m birbirine asal. Bundan da nm 'nin $x - y$ 'yi böldüğü (neden?), yani $nmZ + x = nmZ + y$ eşitliği çıkar, ki bu da f birebir demektir.

f birebir olduğundan, kümelerin de eleman sa-

yısı da aynı (nm) olduğundan, f fonksiyonu bir eşlemedir.

Şimdi f 'nin toplamaya ve çarpmaya saygı duyduğunu göstermeliyiz. Ama bu çok açık, tanımın kendisinden çıkıyor nerdeyse. Örneğin f 'nin çarpmaya saygı duyduğunu kanıtlayalım:

$$\begin{aligned} f((nmZ + x)(nmZ + y)) &= f(nmZ + xy) \\ &= (nZ + xy, mZ + xy) \\ &= ((nZ + x)(nZ + y), (mZ + x)(mZ + y)) \\ &= (nZ + x, mZ + x)(nZ + y, mZ + y) \\ &= f(nmZ + x)f(nmZ + y). \end{aligned}$$

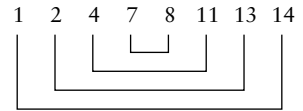
Birinci eşitlik Z/nmZ halkasında çarpmanın, ikinci eşitlik f 'nin, üçüncü eşitlik Z/nZ ve Z/mZ halkalarında çarpmanın, dördüncü eşitlik $Z/nZ \times Z/mZ$ halkasında çarpmanın, beşinci eşitlik gene f 'nin tanımından çıkar. Toplama için de aynı şeyi yapabiliriz. (Ama toplamaya ihtiyacımızın olmadığını biliyoruz, sadece çarpmaya saygı duyan bir eşleme bize yeter.) \square

Böylece Ana Teorem kanıtlanmış oldu.

Şimdi artık yazının başında verdiğimiz ikinci soruyu yanıtlayabiliriz. 15'ten küçük ve 15 ile aralarında asal olan doğal sayılarının toplamını bulmak istiyoruz. Önce 15 için bu toplamı bir yazalım, oradan genel bir formül bulacağız:

$$1 + 2 + 4 + 7 + 8 + 11 + 13 + 14 = 60$$

Dikkat edilirse bu sayılar ortadan simetrik olacak şekilde $7 + 8, 4 + 11, 2 + 13, 1 + 14$ gibi toplanırsa hep 15 sonucunu verirler. Bu bir rastlantı mıdır? Burada bahsettiğime göre değildir ve öyle olmadığını da şimdi göstereceğim: Eğer d, n 'ye asalsa, $n - d$ de n 'ye asaldır. Bu tür $\{d, n - d\}$ çiftlerinden $\varphi(n)/2$ tane olduğuna göre, n 'den küçük ve n 'ye asal sayıların toplamı $n\varphi(n)/2$ biçiminde bir formülde gizlidir. (Artık gizliliği kalmadı tabii!)



Sonuç 7. Eğer $n > 2$ ise

$$\sum_{1 \leq d \leq n \text{ ved, } n' \text{ ye asal}} d = n\varphi(n)/2.$$

İlk sorunun yanıtının $15\varphi(15)/2$ olduğu bu açıklamadan sonra aşikârdır: $15 \times 8/2 = 60$.

Sorular

1. $\varphi(x) = a$ denkleminin sonlu sayıda çözümü olduğunu kanıtlayın.

2. $\sum_{d|n} \varphi(d) = n$ eşitliğini kanıtlayın. \spadesuit