

# Aritmetiğin Çarpımsal Fonksiyonları

E. Mehmet Kırıl\* / luzumi\_86@yahoo.com

**Euler  $\varphi$  Fonksiyonu.** Önceki sayılarımızda Euler  $\varphi$  fonksiyonundan söz etmiştik. Tanımı anımsatalım: Bu fonksiyon, verilen bir  $n$  sayısından küçük ve  $n$ 'ye asal olan doğal sayıların sayısını verir:

$$\varphi(n) = |\{x \in \mathbb{N} : \text{ebob}(x, n) = 1, x \leq n\}|.$$

Örneğin eğer  $n = 10$  ise,  $10$ 'dan küçük ve  $10$ 'a asal sayıların kümesi  $\{1, 3, 7, 9\}$  olduğundan,  $\varphi(10) = 4$ 'tür.

$\varphi$  fonksiyonunun şöyle bir özelliği vardır: Eğer  $n$  ve  $m$  birbirine asal iki sayıysa,

$$\varphi(nm) = \varphi(n)\varphi(m).$$

Bu özellikten,  $\varphi$ 'nin değerlerini hesaplayabilmek için, her  $p$  asal ve her  $k > 0$  doğal sayısı için  $\varphi(p^k)$  değerini bilmek gerektiği anlaşılır, çünkü eğer  $n$ 'yi,

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

olarak asallarına ayırırsak (burada  $p_i$ 'ler  $n$ 'yi bölen birbirinden değişik asallardır), o zaman,

$\varphi(n) = \varphi(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r})$  bulunur. Ayrıca, asal bir  $p$  için,  $\varphi(p^k)$  değeri kolayca hesaplanır:  $p^k$  sadece  $p, p^2, \dots, p^k$  sayılarına bölündüğünden ve bunlardan  $p^{k-1}$  tane olduğundan,

$$\varphi(p^k) = p^k - p^{k-1}$$

dir. Böylece her  $n$  için  $\varphi(n)$  değeri, en azından teoride hesaplanabilir. Yukarıda söylediklerimizin her birinin kanıtı kolay olduğu gibi, ayrıca, MD-2004-I, sayfa 39-41'de de bu kanıtlar verilmişti.

**Bölen Sayısı Fonksiyonu.** Yukarıda sözünü ettiğimiz özelliği daha birçok fonksiyon sağlar. Şimdi tanımlayacağımız  $d$  fonksiyonu bunlardan biridir. Eğer  $n \neq 0$  ise,  $d(n)$ ,  $n$ 'nin bölenlerinin sayısı olsun:

$$d(n) = |\{d \in \mathbb{N} : d \mid n\}|.$$

Örneğin  $d(6) = 4$  ve asal bir  $p$  için  $d(p) = 2$ .

Eğer  $n$  ve  $m$  birbirine asalsa,  $nm$ 'nin her böleni  $n$  ve  $m$ 'nin birer böleninin çarpımına eşittir. Bu olgudan hareketle  $d(nm) = d(n)d(m)$  eşitliği kolaylıkla kanıtlanır. Dolayısıyla eğer asal  $p$  sayıları için,  $d(p^k)$  bilinirse,  $d$ 'nin her sayıda aldığı değer aynen  $\varphi$  gibi hesaplanabilir.  $d(p^k)$ 'nin kaç olduğunu bulmak da pek zor değildir. Nitekim,  $p^k$ 'nin bölenleri tam tamına  $1, p, p^2, \dots, p^k$  olduğundan,  $p^k$ 'nin tam  $k+1$  tane böleni vardır, yani  $d(p^k) = k + 1$ 'dir.

**Çarpımsal Fonksiyonlar.**  $f$ , pozitif doğal sayılar kümesi  $S$ 'den gerçel sayılar kümesi  $R$ 'ye giden bir fonksiyon olsun. Eğer birbirine asal her  $n, m \in S$  çifti için  $f(n)f(m) = f(nm)$  ise  $f$  fonksiyonuna **çarpımsal** denir.

Demek ki yukarıda tanımladığımız  $\varphi$  ve  $d$  fonksiyonları çarpımsaldır. Daha birçok çarpımsal fonksiyon örneği göreceğiz.

**$\sigma_r$  Fonksiyonu.** Sabit bir  $r$  sayısı için,  $\sigma_r$  fonksiyonunu

$$\sigma_r(n) = \sum_{d \mid n} d^r$$

olarak tanımlayalım. Örneğin,

$$\sigma_2(12) = 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2 = 210.$$

Burada,  $\sigma_0(n) = d(n)$  eşitliğine dikkatinizi çekebiliriz. Ayrıca  $\sigma_1(n)$  de  $n$ 'nin bölenlerinin toplamıdır ve  $\sigma(n)$  olarak gösterilir.

$\sigma_r$ 'nin çarpımsal olduğunu kanıtlayalım:

$$\begin{aligned} \sigma_r(n)\sigma_r(m) &= \left(\sum_{d \mid n} d^r\right) \left(\sum_{e \mid m} e^r\right) \\ &= \sum_{d \mid n, e \mid m} d^r e^r = \sum_{d \mid n, e \mid m} (de)^r \\ &= \sum_{de \mid nm} (de)^r = \sigma_r(nm). \end{aligned}$$

Dördüncü eşitlik  $\text{ebob}(n, m) = 1$  eşitliğinden kaynaklanıyor, çünkü bu durumda  $nm$ 'nin her böleni  $n$ 'nin bir böleniyle  $m$ 'nin bir böleninin çarpımıdır.

Bu kanıtı iyi bakın, çünkü bunu birazdan genelleştireceğiz:  $d^r$  yerine, herhangi bir  $f$  çarpımsal fonksiyonu için  $f(d)$  değerini alacağız.

**$\lambda$  Fonksiyonu.** Bir çarpımsal fonksiyon örneği daha:  $n > 1$  olsun;  $n$ 'yi asalların çarpımı olarak yazalım:  $n = p_1 p_2 \dots p_k$ . Buradaki  $p_i$ 'ler  $n$ 'nin asal çarpanlarıdır.  $p_i$ 'lerin birbirinden farklı olmaları gerekmediğine dikkatinizi çekeriz. Şimdi

$$\lambda(n) = (-1)^k$$

olsun. Bu fonksiyon bir sayının asal bölenlerinin sayısının tek mi çift mi olduğunu söylüyor. Eğer  $n = 1$  ise, yukarıdaki tanımla uyum sağlaması için,  $\lambda(1) = (-1)^0 = 1$  olarak tanımlansın. Elbette eğer  $p$  asalsa  $\lambda(p) = -1$ . Herhalde  $\lambda$ 'nın çarpımsal olduğu çok belli olmalı. Ama  $\lambda$ 'nın daha güçlü bir özelliği var:  $n$  ve  $m$  birbirine asal olmasalar da  $\lambda(nm) = \lambda(m)\lambda(n)$ .

**Çarpımsal Fonksiyonların Özellikleri.** Çarpımsal bir  $f$  fonksiyonu ele alıp özelliklerini bulalım.

\* Boğaziçi Üniversitesi Matematik Bölümü 1. sınıf öğrencisi.

Her sayıyı 0'a yollayan "sabit<sub>0</sub> fonksiyonu" çarpımsaldır, ama oldukça sıkıcı bir fonksiyondur, bu yüzden  $f$ 'nin sabit<sub>0</sub> fonksiyonu olmadığını varsayalım. Bu, tam tamına  $f(1) \neq 0$  demektir, çünkü eğer  $f(1) = 0$  ise, 1 her sayıya asal olduğundan, her  $n$  için,  $f(n) = f(1 \cdot n) = f(1)f(n) = 0 \cdot f(n) = 0$  bulunur ve  $f$  sabit<sub>0</sub> fonksiyonudur.

Bundan da  $f(1) = 1$  çıkar, çünkü,  $f(1) = f(1 \cdot 1) = f(1)f(1) = f(1)^2$ ; ayrıca  $f(1) \neq 0$ ; dolayısıyla  $f(1) = 1$ .

Şimdi  $f$ 'nin diğer sayılarda alabileceği değerlere bakalım.  $n \in \mathbb{S}$  olsun.  $n$ 'yi asallarına ayıralım:

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}.$$

O zaman,  $f$  çarpımsal olduğundan,

$$f(n) = f(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}) = f(p_1^{k_1}) f(p_2^{k_2}) \dots f(p_r^{k_r})$$

olur. Demek ki  $f(n)$  değerini hesaplayabilmek için, bir  $p$  asalı ve her  $k > 0$  doğal sayısı,  $f(p^k)$  değerini hesaplamak gerekiyor.

Bu aşamada can alıcı soru, herhangi bir asal  $p$  sayısı ve  $k > 0$  doğal sayısı için,  $f(p^k)$  değerinin ne olabileceğidir. Yanıt kolay, hatta biraz fazla kolay:  $f(p^k)$ 'nin alabileceği değer üzerine herhangi bir koşul koyamayız,  $f(p^k)$  herhangi bir gerçel sayı olabilir. Bir başka deyişle, eğer her  $p$  asalı ve  $k > 0$  doğal sayısı için bir  $a_{p,k}$  gerçel sayısı verilmişse, o zaman,  $f(p^k) = a_{p,k}$  eşitliğini sağlayan çarpımsal bir  $f$  fonksiyonu tanımlanabilir. Buradaki  $a_{p,k}$  sayıları rastgele seçildiğinden,  $f(p^k)$  değerleri alabildiğine özgürdürler, herhangi bir yasaya, eşitliğe, özdeşliğe vb uymazlar. Ama geri kalan  $n$ 'ler için,  $f$  çarpımsal olmanın koşulunu yerine getirmelidir.

Yukardaki örneklerde asal  $p$  ve  $k > 0$  doğal sayısı için,

$$\varphi(p^k) = p^k - p^{k-1},$$

$$d(p^k) = k + 1,$$

$$\sigma_r(p^k) = 1^r + p^r + p^{2r} + \dots + p^{kr} = \frac{p^{r(k+1)} - 1}{p^r - 1},$$

$$\lambda(p^k) = (-1)^k$$

değerlerini bulmuştuk.

**Eskileri Alıp Yenilerini Veriyoruz.** Şimdi bir çarpımsal fonksiyondan yararlanarak yeni bir çarpımsal fonksiyon yaratacağız.  $f$ , herhangi bir çarpımsal bir fonksiyon olsun.  $f^*$  fonksiyonunu şöyle tanımlayalım:

$$f^*(n) = \sum_{d|n} f(d).$$

$f^*$  da çarpımsaldır çünkü ger  $n$  ve  $m$  birbirine asalsa,

$$\begin{aligned} f^*(nm) &= \sum_{d|nm} f(d) = \sum_{a|n, b|m} f(ab) \\ &= \sum_{a|n, b|m} f(a)f(b) \end{aligned}$$

$$\begin{aligned} &= (\sum_{a|n} f(a))(\sum_{b|m} f(b)) \\ &= f^*(n)f^*(m). \end{aligned}$$

İkinci eşitlik  $\text{ebob}(n, m) = 1$  olmasından kaynaklanıyor, çünkü  $nm$ 'yi bölen her sayı,  $n$ 'yi bölen bir  $a$ 'nın ve  $m$ 'yi bölen bir  $b$ 'nin çarpımıdır.

Yukardaki kanıtın  $\sigma_r$ 'nin çarpımsal olduğunun kanıtına ne kadar çok benzediğine dikkatinizi çekebiliriz. Hatta kanıtlar aynı, sadece  $\sigma_r$ 'nin çarpımsal olduğunun kanıtında  $f(n) = n^r$  almak gerekiyor. Nitekim, eğer  $f$  fonksiyonu  $f(n) = n^r$  kuralıyla tanımlanmış çarpımsal fonksiyonsa, o zaman,  $f^* = \sigma_r$ . Bunun özel bir hali olarak da ( $r = 1$  alarak)  $\text{Id}^* = \sigma$  bulunur.

**Örnek 1.** Eğer  $f$ , sabit 1 değerini alan fonksiyonsa,  $f^* = d$ 'dir.

**Örnek 2.**  $\varphi$ , Euler fonksiyonu olsun.  $\varphi^*$  fonksiyonunu bulalım. Çarpımsal olduğunu biliyoruz, bunu yukarda gördük. Dolayısıyla asal  $p$ 'ler ve  $k$  doğal sayıları için  $\varphi^*(p^k)$  değerlerini bilmek yetiyor. Bulalım:

$$\begin{aligned} \varphi^*(p^k) &= \sum_{d|p^k} \varphi(d) = \sum_{i=0, \dots, k} \varphi(p^i) \\ &= \varphi(1) + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^k) \\ &= 1 + (p-1) + (p^2 - p) + \dots + (p^k - p^{k-1}) \\ &= p^k. \end{aligned}$$

Demek ki  $\varphi^*(p^k) = p^k$ . Bundan her  $n$  için  $\varphi^*(n) = n$ , yani  $\varphi^* = \text{Id}$  çıkar. Dolayısıyla  $\varphi^{**} = \text{Id}^* = \sigma_1$ .

**Yenileri Alıp Eskilerini Veriyoruz.** Yukarda  $f^*$  fonksiyonunu  $f$  fonksiyonunu kullanarak bulduk. Acaba  $f$  fonksiyonunu  $f^*$  fonksiyonunu kullanarak bulabilir miyiz? Evet!

Möbius  $\mu$  fonksiyonunu şöyle tanımlayalım:

$$\mu(n) = \begin{cases} 1 & \text{eğer } n = 1 \text{ ise} \\ 0 & \text{eğer } n, 1 \text{ dışında bir tamkareye bölünüyorsa} \\ (-1)^t & \text{eğer } n, t \text{ değişik asalın çarpımıysa} \end{cases}$$

Kolayca kontrol edilebileceği üzere  $\mu$  fonksiyonu çarpımsaldır. Ayrıca eğer  $p$  bir asalsa  $\mu(p) = -1$  ve eğer  $k > 1$  ise,  $\mu(p^k) = 0$ .

**Alıştırma.**  $n \neq 1$  için,  $\mu^*(n) = 0$  ve  $\mu^*(1) = 1$  eşitliklerini kanıtlayın.

$$\text{Teorem. } f(n) = \sum_{d|n} \mu(d) f^*(n/d).$$

Bu teorem, ürettiğimiz  $f^*$  fonksiyonundan eski  $f$  fonksiyonunu tekrar elde etmemizi sağlıyor. Bu-

nun bir anlamı da  $f^*$  fonksiyonunu aynı yöntemle başka bir fonksiyondan elde edemeyeceğimizdir, yani  $f^* = g^*$  ise  $f = g$ 'dir.

**Teoremin Kanıtı:**  $f$  ve  $g$  herhangi iki çarpımsal fonksiyon olsunlar. Bir hesap yapalım:

$$\begin{aligned} \sum_{d|n} g(d)f^*(n/d) &= \sum_{d|n} [g(d)\sum_{e|(n/d)} f(e)] \\ &= \sum_{d|n} \sum_{e|(n/d)} g(d)f(e) = \sum_{ed|n} g(d)f(e). \end{aligned}$$

Burada, birinci eşitlik  $f^*$  fonksiyonunun tanımından kaynaklanıyor. Üçüncü eşitlik, " $d|n$  ve  $e|(n/d)$ " koşullarının " $ed|n$ " koşuluna eşdeğer olmasından kaynaklanıyor. Demek ki,

$$\sum_{d|n} g(d)f^*(n/d) = \sum_{ed|n} g(e)f(d).$$

Benzer biçimde,  $g$  ile  $f$ 'nin rollerini değiştirirsek,

$$\sum_{d|n} f(d)g^*(n/d) = \sum_{ed|n} f(e)g(d)$$

buluruz. Ama son iki denklemin sağ tarafları birbirine eşit. Demek ki,

$$\sum_{d|n} g(d)f^*(n/d) = \sum_{d|n} f(d)g^*(n/d).$$

Şimdi  $g$  yerine  $\mu$  alalım:

$$\sum_{d|n} \mu(d)f^*(n/d) = \sum_{d|n} f(d)\mu^*(n/d)$$

buluruz. Ama  $\mu^*$  fonksiyonu yukardaki alıştırma-da hesaplanmış olmalı: Eğer  $n \neq 1$  ise  $\mu^*(n) = 0$  ve  $\mu^*(1) = 1$ . Demek ki,

$$\sum_{d|n} \mu(d)f^*(n/d) = \sum_{d|n} f(d)\mu^*(n/d) = f(n).$$

Teoremimiz kanıtlanmıştır.  $\square$

**Uygulama.** Şimdi birkaç uygulamaya geçelim. Uygulama dediysek öyle ahım şahım bir şey yapmayacağız. Alt tarafı şu bulduğumuz yeni formüle bildiğimiz fonksiyonları yerleştireceğiz. Örneğin  $\varphi^* = \text{Id}$  eşitliğini biliyoruz ya, teoremimiz sağolsun, artık

$$\sum_{d|n} \mu(d)(n/d) = \varphi(n)$$

eşitliğini de biliyoruz, yani,

$$\sum_{d|n} \mu(d)/d = \varphi(n)/n.$$

Aynı şekilde

$$\sum_{d|n} \mu(d)\sigma_r(n/d) = n^r$$

eşitliğini de biliyoruz.

**Son Söz Değil.** Bu yazıda belli bir yerden sonra yaptıklarımız bazı okurlara garip gelmiş olabilir. Neden tanımlandıkları çok açık olan birtakım fonksiyonlardan neden tanımlandıkları hiç de açık olmayan başka fonksiyonlar elde ettik. Sonra ilk fonksiyonumuzu sanki kaybetmiş gibi yeniden bulmak için bir başka fonksiyon daha ( $\mu$  fonksiyonunu) tanımladık.

Aslında bu yaptıklarımızın hepsinin çok geçerli nedenleri vardır. Bu yazının devamı niteliğinde olan gelecek yazıda konuya biraz tepeden bakacağız ve o irtifadan tüm bu fonksiyonların aslında birbirlerine göbekten bağlı olduğu ortaya çıkacak. Ayrıca tüm bu yaptıklarımız da meşruiyet kazanacak.  $\clubsuit$

### Tekzip!

Geçen sayımızda, sayfa 34-37'de bir  $m > 1$  tamsayısına asal her  $n$  için  $n^{\varphi(m)} \equiv 1 \pmod{m}$  denkleğini kanıtlamıştık. Editörden kaynaklanan bir hata sonucu, aynen bunun gibi bir gri kutucuk içinde,  $m$ 'ye asal her  $n$  için  $n^k \equiv 1 \pmod{m}$  denkleğini sağlayan en küçük  $k$  sayısı yanlış verilmişti. Bu denkleği sağlayan en küçük  $k$ ,

eğer  $m$  tekse  $\varphi(m)$ ,

eğer  $8|m$  ise  $\varphi(m)/4$

diğer hallerde  $\varphi(m)/2$

dir. Düzeltir özür dileriz.



#### E. Mehmet Kırал

1986 İstanbul Doğumluyum. İlkokulu Sezgin Topçu ile okudum (hocamdı). Ortaokul ve lisede de Üsküdar Amerikan Lisesi'nde ydım. Sahneye çıkmayı çok severim.

Dolayısıyla lisede pekçok oyunda oynadım. Bir ara içimden tiyatrocı olma isteği geçmişti, daha önce de (ortaokulda) reklam metin yazarı olmak istiyordum. En sonunda bir kıskançlık sonucu matematiğe olan ilgim alevlendi. Derhal elime bir MD aldım... Ve alış o alış!

Bir ara sporla, özellikle de uzun mesafe spor-

larıyla ilgilendim (babam sağolsun). Bir triatlon bitirmişliğim de vardır! Lise 2'de gayrimeşru bir çay ocağının üç hissedarından biri ve işletmecisiydim. Oralet içmeyi severim. Model Birleşmiş Milletlercilik ve FRP oynamaktan hoşlanırım. FRP'de özellikle savaşlarda hiç işe yaramayan karakterleri oynamak hoşuma gider. (Bkz. OOTS'deki Elan. Google'da OOTS yazarsanız karşınıza çıkacaktır.) Ayrıca uzun süredir piyano çalıyorum.

Çok zayıfım ve dolayısıyla sert sandalyelere oturmamı sevmem. Eğer mümkünse oturmam, tünırım (öyle derler). Gülmeyi somurtmaya, zıplamayı yürümeye tercih ederim.