

## $Z/nZ$ Halkasını Parçalamak

**I. Örnekler.**  $Z/nZ$  halkasında  $x^2 = x$  gibi son derece basit bir denklemi çözmeye çalışın. Ya da  $Z/nZ$  halkasındaki karelerin sayısını bulmaya çalışın. Eğer bu yazıda yapacaklarımızı önceden bilmiyorsanız, bu soruların hiç de kolay olmadığını göreceksiniz, ki bunlar oldukça basit sorulardır,  $Z/nZ$  halkalarıyla ilgili çok daha zor sorular vardır. Bu yazıda  $Z/nZ$  halkasında  $x^2 = x$  denklemini çözmeye yarayacak ve bu tür cebirsel soruların yanıtlanmasında son derece yararlı bir sonuç ve yöntem göreceğiz.

### Eşgüçlüler

Eğer  $x^2 = x$  ise, her  $k > 0$  doğal sayısı için,  $x^k = x$ 'dir elbette. Bu yüzden bu denklemi sağlayan elemanlara eşgüçlü elemanlar denir.  $Z/180Z$  yapısında 8 eşgüçlü vardır: Sırasıyla, 0, 36, 100, 136, 45, 81, 145, 1. Çözümlerin hangi sırayla yazıldıklarını ancak bu yazıyı okuyan anlayabilecektir!

$Z/nZ$  halkasını "parçalayarak",  $Z/nZ$  halkası üzerine sorduğumuz soruları daha basit halkalara indirgeyeceğiz. Örneklerle yola çıkalım.

**Örnek 1.** Tamsayıları aşağıdaki gibi bir çizelge halinde modülo 4 ve modülo 3 yazalım. Birinci sütuna  $Z$ 'nin elemanlarını yazdık; ikinci ve üçüncü sütunlara da tamsayıların modülo 4 ve 3 değerlerini.

$Z$	$Z/4Z$	$Z/3Z$	$Z/4Z \times Z/3Z$
0	0	0	(0, 0)
1	1	1	(1, 1)
2	2	2	(2, 2)
3	3	0	(3, 0)
4	0	1	(0, 1)
5	1	2	(1, 2)
6	2	0	(2, 0)
7	3	1	(3, 1)
8	0	2	(0, 2)
9	1	0	(1, 0)
10	2	1	(2, 1)
11	3	2	(3, 2)
12	0	0	(0, 0)
13	1	1	(1, 1)
14	2	2	(2, 2)

Son sütunda bu iki değeri bir parantez içinde belirttik.

Böylece en soldaki sütun olan  $Z$ 'den en sağdaki sütun olan  $Z/4Z \times Z/3Z$ 'e giden bir fonksiyon elde ederiz. Örneğin bu fonksiyonun 5'teki değeri (1, 2)'dir, daha doğrusu

$(\bar{1}, \bar{2})$ 'dir, yazılımda kolaylık olsun diye sayıların üstüne koymamız gereken çizgileri koymadık. Bu

radaki  $(\bar{1}, \bar{2})$ 'nin ilk koordinatı olan  $\bar{1}$ ,  $Z/4Z$  kümesindedir ve  $4Z + 1$  anlamına gelmektedir; ikinci koordinat olan  $\bar{2}$  ise  $Z/3Z$  kümesindedir ve  $3Z + 2$  anlamına gelmektedir. Belki de fonksiyonun 5'te aldığı değeri, (1, 2) yerine

$$(5 \pmod{4}, 5 \pmod{3})$$

olarak, yani

$$(1 \pmod{4}, 2 \pmod{3})$$

olarak göstermek daha doğru olurdu.

Bu fonksiyona  $\varphi$  adını verelim.

$\varphi : Z \rightarrow Z/4Z \times Z/3Z$  fonksiyonunun aldığı değerlerin birkaçını yandaki çizelgede yazdık. Bu çizelgeden de görüleceği üzere 12'den sonra bir döngü elde ediyoruz, her 12 sayıda bir fonksiyonun aldığı değerler yineleniyor. Bunun nedeni basit:  $n$  hangi tamsayı olursa olsun,

$$n + 12 \equiv n \pmod{3}$$

ve

$$n + 12 \equiv n \pmod{4}$$

dir. Yani, her  $n \in Z$  için,

$$\varphi(n) = \varphi(n + 12).$$

Bu sayede,  $Z$ 'den  $Z/4Z \times Z/3Z$ 'e giden  $\varphi$  fonksiyonu  $Z/12Z$ 'den  $Z/4Z \times Z/3Z$ 'e giden bir fonksiyon doğurur. Nitekim, yukarda tanımlanmış olan

$$\varphi : Z \rightarrow Z/4Z \times Z/3Z$$

fonksiyonunun yardımıyla, her  $\bar{a} \in Z/12Z$  için,

$$\varphi(\bar{a}) = \varphi(a),$$

yani

$$\varphi(a \pmod{12}) = (a \pmod{4}, a \pmod{3})$$

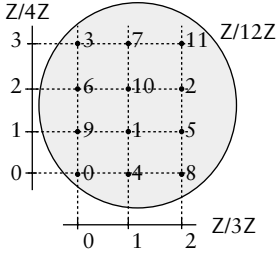
kuralı sayesinde,

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

$$\bar{\varphi} : \mathbb{Z}/12\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

fonksiyonunu tanımlayabiliriz:

Yazılım yoğunlaşmasını diye en sağdaki  $\bar{\varphi}$  değerlerinin koordinatlarının üstüne çizgi çekmedik. Bunların birinci koordinatlarının  $\mathbb{Z}/4\mathbb{Z}$ 'de, ikincisinin  $\mathbb{Z}/3\mathbb{Z}$ 'de olduğunu unutmayalım.



$\bar{\varphi}$  fonksiyonunu aşağıdaki şekildeki gibi resmedebiliriz. Gri alan içinde  $\mathbb{Z}/12\mathbb{Z}$ 'nin elemanlarını görüyorsunuz, 0'dan 11'e kadar (0'dan 11'e kadar olmalı aslında.) İki eksen den dikey olanı  $\mathbb{Z}/4\mathbb{Z}$ 'yi, yatay olan diğeri  $\mathbb{Z}/3\mathbb{Z}$ 'yi simgeliyor. Gri alan içindeki bir elemanın bu iki eksen üzerindeki izdüşümleri, elemanın  $\bar{\varphi}$ 'de aldığı değerini iki koordinatını veriyor.

Bu şekilden ya da yukardaki yaptıklarımızdan,  $\bar{\varphi}$ 'nin bir eşleme olduğu anlaşılıyor. Zaten hem  $\mathbb{Z}/12\mathbb{Z}$ 'nin hem de  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ 'nin 12'ser tane elemanı var, dolayısıyla bu iki küme arasındaki birebir her fonksiyon örten, örten her fonksiyon birebir olmak zorunda, ve  $\bar{\varphi}$ 'nin de birebir olduğunu kanıtlamak çok kolay.

**Örnek 2.** Yukarıda yaptığımızı sadece 3 ve 4'le değil, iki ya da daha fazla doğal sayıyla da yapabiliriz, en azından bir yere kadar yapmaya çalışabiliriz. Örneğin,  $\mathbb{Z}$ 'den  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ 'ye giden “doğal” (yani tahmin edileceği gibi sayılar sırasıyla modülo 4, 9 ve 30 alınarak tanımlanan)  $\varphi$  fonksiyonunu ele alalım:

$$\begin{aligned} \varphi(35) &= (3, 8, 5), \\ \varphi(325) &= (1, 1, 25), \\ \varphi(835) &= (3, 7, 25). \end{aligned}$$

Her 180 sayıda bir bu fonksiyon aynı değeri alır, yani fonksiyonun periyodu 180'dir (yukardakinin 12'ydii.) Aslında  $\varphi$ , her 360 ya da 540 sayıda bir de aynı değeri alır, ama en küçük periyodu bulmak daha ekonomik.

Böylece,

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$$

fonksiyonu bize, her  $\bar{a} \in \mathbb{Z}/180\mathbb{Z}$  için,

$$\bar{\varphi}(\bar{a}) = \varphi(a),$$

yani,

$$\bar{\varphi}(a \bmod 180) = (a \bmod 4, a \bmod 9, a \bmod 30)$$

kuralıyla tanımlanmış

$$\bar{\varphi} : \mathbb{Z}/180\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$$

fonksiyonunu verir.

$\varphi$  değil ama  $\bar{\varphi}$  birebirdir, çünkü eğer  $\bar{\varphi}(\bar{a}) = \bar{\varphi}(\bar{b})$  ise,  $a - b$  sayısı 4'e, 9'a ve 30'a bölünür, dolayısıyla bu sayıların en küçük ortak katı olan 180'e bölünür.

$\bar{\varphi}$  birebirdir ama örten olamaz, çünkü fonksiyonun imgesi olan  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$  kümesinde  $4 \times 9 \times 30 = 1080$  tane eleman var, kalkış kümesinin tam 6 misli kadar.

**Örnek 3.** Bu kez, gene doğal bir biçimde tanımlanmış olan,

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

fonksiyonuna bakalım. Örneğin,

$$\begin{aligned} \varphi(325) &= (1, 1, 0), \\ \varphi(834) &= (2, 6, 4). \end{aligned}$$

Gene 180 sayıda bir fonksiyon kendini yineler,  $\varphi$ 'nin periyodu 180'dir. Dolayısıyla  $\varphi$  fonksiyonu sayesinde,

$$\bar{\varphi} : \mathbb{Z}/180\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

fonksiyonunu

$$\bar{\varphi}(\bar{a}) = \varphi(a)$$

kuralıyla tanımlayabiliriz:

$$\bar{\varphi}(a \bmod 180) = (a \bmod 4, a \bmod 9, a \bmod 5).$$

Tanımlanan bu  $\bar{\varphi}$  fonksiyonunun bu kez bir eşleme olduğu aynen yukarda birinci örnekte yaptığımız gibi kanıtlanabilir.

**II. Ana Teorem.** İlk üç örnekte tanımlanan  $\bar{\varphi}$  fonksiyonlarının önemli bir özelliği vardır: Matematiksel deyişle,  $\bar{\varphi}$  fonksiyonu toplamaya, çıkarmaya ve çarpmaya saygı duyar. Burada tam ne demek istediğimizi anlatmak için biraz tanıma ihtiyacımız var.

Yukardaki  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  örneğine geri dönelim.  $\mathbb{Z}/4\mathbb{Z}$  ve  $\mathbb{Z}/3\mathbb{Z}$  kümeleri üzerinde toplama, çıkarma ve çarpma adını verdiğimiz üç işlem tanımlamıştık geçen yazıda. Benzer bir yapıyı  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  kümesinde de tanımlayacağız. Ve bunu son derece “doğal” bir biçimde yapacağız.

$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  kümesinden iki  $(a, b), (a', b')$  elemanı alalım. Bunları toplamak, birbirinden çıkarmak ve birbirleriyle çarpmak istiyoruz. Çok kolay! Koordinatları ayrı ayrı toplayıp çıkarıp çarpalım:

$$(a, b) \pm (a', b') = (a \pm a', b \pm b')$$

$$(a, b)(a', b') = (aa', bb').$$

Böylece  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  kümesi üzerine toplama, çıkarma ve çarpma adını verdiğimiz üç işlem tanımlanmış oluruz ve bu işlemler sayesinde  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  kümesi cebirsel bir yapıya bürünmüş olur,

**Dikkat!** İkinci ve üçüncü örneklerde  $\bar{\varphi}$  fonksiyonunu tanımlamak için  $\varphi$ 'nin periyodu olan 180'yi seçmemiz rastlantı değildi. 180 yerine 180'in herhangi bir katını da alabilirdik ve birebir olmasa da gene bir fonksiyon bulabilirdik, ama 180'in katları dışında bir sayı alamazdık, çünkü o zaman bir fonksiyon bile elde etmezdik.

Benzer sorunu modülo  $n$  yazılmış sayıları modülo  $m$  almak istediğimizde yaşarız. Örneğin  $n = 7$ ,  $m = 5$  olsun ve  $\bar{\varphi} : Z/7Z \rightarrow Z/5Z$  fonksiyonunu,

$$\bar{\varphi}(a \bmod 7) = (a \bmod 5)$$

kuralıyla “doğal olarak” tanımlamaya çalışalım. O zaman,

$(7 \bmod 5) = \bar{\varphi}(7 \bmod 7) = \bar{\varphi}(0 \bmod 7) = (0 \bmod 5)$ , yani  $7 \equiv 0 \pmod{5}$  gibi saçmasapan bir sonuç çıkar. Demek ki tanımlamaya çalıştığımız fonksiyon yoktur, olamaz.

Genel olarak,

$$\bar{\varphi}(a \bmod n) = (a \bmod m)$$

kuralının  $Z/nZ$ 'den  $Z/mZ$ 'ye giden bir fonksiyon tanımlayabilmesi için, her  $a$  ve  $b$  tamsayısı için,

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

koşulunun,

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

sonucunu doğurması gerekmektedir, ki bu da ancak  $m, n$ 'yi bölüyorsa mümkündür (okura alıştırmaya.) Örneğin,  $Z/24Z$ 'den  $Z/8Z$ 'ye giden “doğal” bir fonksiyon vardır (çünkü 8, 24'ü böler) ama  $Z/24Z$ 'den  $Z/7Z$ 'ye giden “doğal” bir fonksiyon yoktur.

üstelik  $Z/nZ$  ve  $Z/mZ$ 'nin cebirsel yapılarını yansıtan cebirsel bir yapıya, sayfa 14'teki “halka özelliklerini” sağlayan bir yapıya... Nasıl  $Z$ 'nin,  $Z/nZ$ 'nin ve  $Z/mZ$ 'nin çarpma için etkisiz elemanları varsa, ki böyle bir elemana **birim eleman** adı verilir,  $Z/nZ \times Z/mZ$ 'nin de çarpma için bir etkisiz elemanı vardır:  $(\bar{1}, \bar{1})$ .  $Z/nZ \times Z/mZ$  bu cebirsel yapısı da,  $Z, Z/nZ$  ve  $Z/mZ$ 'ninkiler gibi halka özelliklerini sağlar, yani bir halkadır.

Şimdi şunu kanıtlamak istiyoruz: Eğer  $n$  ve  $m$  birbirine asal iki doğal sayıysa,  $Z/nmZ$  cebirsel yapısıyla yukarıda tanımlanan  $Z/nZ \times Z/mZ$  cebirsel yapısı arasında hemen hemen hiç fark yoktur. Örneğin, birinci yapıda  $x^2 = x$  denkleminin kaç tane çözümü varsa, ikinci yapıda da o kadar vardır. Ya da, birinci yapıdaki karelerin sayısı ikinci yapıdaki karelerin sayısına eşittir. Böylece,  $Z/nmZ$  halkası

üzerine sorulan cebirsel bir soruyu  $Z/nZ \times Z/mZ$  yapısına indirgemiş olacağız.

Öte yandan,  $Z/nZ \times Z/mZ$  yapısı,  $Z/nZ$  ve  $Z/mZ$  yapıları tarafından belirlenir. Sonuç olarak,  $Z/nmZ$  yapısı üzerine sorulan cebirsel bir soruyu,  $Z/nZ$  ve  $Z/mZ$  yapılarına indirgemiş olacağız.

İlerde daha fazla ayrıntı ve örnek vereceğiz. Önce, “cebirsel yapılar arasında hemen hemen hiç fark yoktur” teoremini yazıp kanıtlatalım. Teoremin kendisi uzun ama kanıtı bu aşamada oldukça kısa.

### Z/14Z'de Kareler

$$\begin{array}{ll} 0^2 = 0 & 7^2 = 1 \\ 1^2 = 1 & 8^2 = 8 \\ 2^2 = 4 & 9^2 = 11 \\ 3^2 = 9 & 10^2 = 2 \\ 4^2 = 2 & 11^2 = 9 \\ 5^2 = 11 & 12^2 = 4 \\ 6^2 = 8 & 13^2 = 1 \end{array}$$

Demek ki  $Z/14Z$  halkasında sadece 0, 1, 2, 4, 8, 9 ve 11 bir kare, başka da yok. Toplam yedi tane. Bu sayıdaki yazılardan  $Z/nZ$ 'deki kare sayısı bulunabilir.

**Ana Teorem.**  $n$  ve  $m$  iki pozitif doğal sayı olsun.  $\varphi, Z'$ 'den  $Z/nZ \times Z/mZ$ 'ye giden ve

$$\varphi(a) = (a \bmod n, a \bmod m)$$

kuralıyla “doğal” olarak tanımlanmış fonksiyon olsun.  $\varphi$  fonksiyonu toplamaya, çıkarmaya ve çarpmaya saygı duyar, yani her  $a, b \in Z$  için,

$$\varphi(a \pm b) = \varphi(a) \pm \varphi(b)$$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

eşitlikleri geçerlidir ve  $\varphi, Z'$ 'nin birim elemanı olan 1'i  $Z/nZ \times Z/mZ$ 'nin birim elemanı olan  $(\bar{1}, \bar{1})$ 'e götürür.

Ayrıca, bu fonksiyonun en küçük periyodu  $\text{ekok}(n, m)$ 'dir. Yani eğer  $\text{ekok}(n, m) = k$  ise ve  $a, b \in Z$  sayıları  $a \equiv b \pmod{k}$  denklğini sağarlarsa, o zaman,  $\varphi(a) = \varphi(b)$  eşitliği geçerlidir. Dahası,  $k$ , bu eşitliğin her  $a$  ve  $b$  için sağlandığı en küçük pozitif doğal sayıdır. Dolayısıyla  $\varphi$  fonksiyonu, her  $\bar{a} \in Z/kZ$  için,

$$\bar{\varphi}(\bar{a}) = \varphi(a)$$

kuralıyla tanımlanmış

$$\bar{\varphi} : Z/kZ \rightarrow Z/nZ \times Z/mZ$$

fonksiyonunu doğurur.  $\bar{\varphi}$  fonksiyonu da  $\varphi$  gibi toplamaya, çıkarmaya ve çarpmaya saygı duyar ve  $Z/kZ$ 'nin birim elemanı olan  $\bar{1}$ 'i  $Z/nZ \times Z/mZ$ 'nin birim elemanı olan  $(\bar{1}, \bar{1})$ 'e götürür. Dahası  $\bar{\varphi}$  fonksiyonu birebirdir.

Son olarak,  $\bar{\varphi}$  fonksiyonunun örten (yani eşleme) olması için yeter ve gerek koşul  $n$  ve  $m$  sayılarının birbirine asal olması, yani  $k = nm$  eşitliğidir.

**Kanıt:** Kanıt çok basit, her şey tanımlardan çıkıyor. Biz gene de birkaç ayrıntıyı yazalım.

$$\varphi(a) = (a \bmod n, a \bmod m)$$

kuralıyla tanımlanmış  $\varphi : Z \rightarrow Z/nZ \times Z/mZ$  fonksiyonun toplamaya, çıkarmaya ve çarpmaya saygı duyduğu ve birim elemanı birim elemanına götürdüğü,  $\varphi$ 'nin ve  $Z/nZ \times Z/mZ$  üzerine koyduğumuz cebirsel yapının tanımlarından hemen çıkar.

Şimdi  $\overline{\varphi(\bar{a})} = \varphi(a)$  kuralıyla

$$\overline{\varphi} : Z/kZ \rightarrow Z/nZ \times Z/mZ$$

fonksiyonunu tanımlayabileceğimizi kanıtlayalım. Bunun için, her  $a, b \in Z$  için,  $Z/kZ$  yapısındaki  $\bar{a} = \bar{b}$  eşitliğinin,  $Z/nZ \times Z/mZ$  yapısında,  $\varphi(a) = \varphi(b)$  eşitliğini doğurduğunu kanıtlamalıyız, yoksa  $\overline{\varphi}$  diye bir fonksiyon tanımlayamayız. Yani

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

denkliğinin,

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

denkliklerini doğurduğunu kanıtlamalıyız. Yani eğer  $k, a - b$ 'yi bölüyorsa,  $n$  ve  $m$ 'nin  $a - b$ 'yi böldüğünü kanıtlamalıyız. Ama  $k = \text{ekok}(n, m)$  olduğundan, bu bariz. Demek ki yukardaki gibi,  $\overline{\varphi(\bar{a})} = \varphi(a)$  kuralıyla tanımlanmış

$$\overline{\varphi} : Z/kZ \rightarrow Z/nZ \times Z/mZ$$

fonksiyonu gerçekten var.

$\overline{\varphi(\bar{a})} = \varphi(a)$  eşitliğinden ve  $\varphi$ 'nin toplama, çıkarma ve çarpmaya saygı duyduğundan,  $\overline{\varphi}$  fonksiyonu da bu işlemlere saygı duyar. Aynı nedenden  $\overline{\varphi}$  fonksiyonu birim elemanını birim elemanına götürür.

$\overline{\varphi}$  fonksiyonunun birebir olduğunu kanıtlayalım şimdi.  $\overline{\varphi(\bar{a})} = \overline{\varphi(\bar{b})}$  eşitliğini varsayalım. Demek ki,  $\varphi(a) = \varphi(b)$ , yani  $\varphi$ 'nin tanımından dolayı,

$$(a \bmod n, a \bmod m) = (b \bmod n, b \bmod m),$$

yani  $a \equiv b \pmod{n}$  ve  $a \equiv b \pmod{m}$ , yani  $n$  ve  $m$  sayıları  $a - b$  sayısını bölüyor, demek ki  $\text{ekok}(a, b)$ , yani  $k, a - b$  sayısını bölüyor, yani  $Z/kZ$  halkasında  $\bar{a} = \bar{b}$ . Böylece  $\overline{\varphi}$  fonksiyonunun birebir olduğu kanıtlanmış oldu.

Bir üst paragrafta birebir olduğunu kanıtladığımız  $\overline{\varphi}$  fonksiyonunun örten olması için  $k = |Z/kZ| = |Z/nZ \times Z/mZ| = nm$  olmalı, yani  $\text{ekok}(n, m) = nm$  olmalı, yani  $n$  ile  $m$  birbirine asal olmalı.  $\square$

Okur dikkat etmişse, yukardaki teoremden tanımlanan  $\overline{\varphi}$  fonksiyonu sadece  $k = \text{ekok}(n, m)$  için değil,  $\text{ekok}(n, m)$ 'nin tüm tam katları için de tanımlanabilir, ama  $\overline{\varphi}$ 'nin birebir olması için illa ve illa  $k = \pm \text{ekok}(n, m)$  olmalıdır.

**III. Eşyapısallık.** Ana Teorem'de, eğer  $n$  ve  $m$  birbirine asalsa,  $Z/nmZ$  ile  $Z/nZ \times Z/mZ$  yapılarının birbirine çok benzediği kanıtlandı, yani  $Z/nmZ$ 'den  $Z/nZ \times Z/mZ$ 'ye giden, toplama, çıkarma ve çarpmaya saygı duyan ve birim elemanını birim elemanına götüren bir eşlemenin varlığı kanıtlandı. Bu durumda,  $Z/nmZ$  ve  $Z/nZ \times Z/mZ$  halkalarına eşyapısal denir, cebirsel işlemlere ve birim elemana saygı duyan eşlemeye de eşyapı dönüşümü adı verilir. İki halkanın eşyapısal olması demek, iki halka arasında pek az bir ayrım vardır demektir, hatta elemanlarının adları dışında, toplama, çıkarma ve çarpma sözkonusu olduğunda, aralarında hiçbir ayrım yoktur demektir. Bu durumda, hemen hemen eşit anlamında,

$$Z/nmZ \approx Z/nZ \times Z/mZ$$

yazarız. Örneğin,

$$Z/6Z \approx Z/2Z \times Z/3Z,$$

$$Z/12Z \approx Z/4Z \times Z/3Z,$$

$$Z/50Z \approx Z/2Z \times Z/25Z,$$

$$Z/30Z \approx Z/2Z \times Z/3Z \times Z/5Z,$$

$$Z/60Z \approx Z/4Z \times Z/3Z \times Z/5Z.$$

Eğer  $n$  ve  $m$  birbirine asal iki pozitif tamsayıysa,  $Z/nmZ$  halkasından  $Z/nZ \times Z/mZ$  halkasına giden bir eşyapı dönüşümü (yani toplamaya, çıkarmaya ve çarpmaya saygı duyan ve birim elemanı birim elemana götüren bir eşleme) olduğunu gördük. Bulduğumuz bu eşyapı dönüşümü,  $Z/nmZ$  halkasının  $(x \bmod nm)$  elemanını  $Z/nZ \times Z/mZ$  halkasının  $(x \bmod n, x \bmod m)$  elemanına götürüyordu. Bu iki halka arasında, bundan başka da eşyapı dönüşümü olamaz. Çünkü  $\varphi$  bir eşyapı dönüşümüyse,  $\varphi(1)$ ,  $Z/nZ \times Z/mZ$  halkasının  $(1, 1)$  birim elemanına eşittir ve  $Z/nmZ$  halkasının her  $x$  elemanı  $1$ 'in kendisiyle birkaç kez toplamıyla elde edildiğinden,  $\varphi(x)$ 'in ne olduğu bellidir:

$$\varphi(x) = \varphi(1 + \dots + 1) = \varphi(1) + \dots + \varphi(1).$$

**IV. Eşyapısallık Ne İşe Yarar?**  $A$  ve  $B$  iki eşyapısal halka olsun. Aralarındaki eşyapısal dönüşüme  $\varphi$  diyelim. Demek ki  $\varphi$ ,  $A$ 'dan  $B$ 'ye giden bir eşleme ve her  $a, a' \in A$  için,

$$\varphi(a \pm a') = \varphi(a) \pm \varphi(a')$$

$$\varphi(aa') = \varphi(a)\varphi(a')$$

$$\varphi(1_A) = 1_B$$

eşitlikleri sağlıyor. (Burada  $1_A$ ,  $A$ 'nın,  $1_B$  ise  $B$ 'nin birim elemanlarıdır.)

Diyelim  $B$ 'de  $x^2 = x$  denklemini çözmek istiyoruz. Aynı denklemi  $A$ 'da çözüp,  $A$ 'daki çözümlerin  $\varphi$ -imgelerini alarak  $B$ 'deki tüm çözümleri bulabiliriz. Nitekim, eğer  $a$ ,  $x^2 = x$  denkleminin  $A$ 'da bir çözümüyse, yani  $a^2 = a$  denkleminin  $A$ 'da sağlanıyorsa, o zaman  $b = \varphi(a)$  yazıp hesaplayalım:

$b^2 = \varphi(a)^2 = \varphi(a)\varphi(a) = \varphi(aa) = \varphi(a^2) = \varphi(a) = b$  eşitliğini elde ederiz. Demek ki  $b$ ,  $x^2 = x$  denkleminin  $B$ 'de bir çözümüdür.

Bunun tersi de doğrudur. Eğer  $b$ ,  $x^2 = x$  denkleminin  $B$ 'de bir çözümüyse, o zaman,  $a = \varphi^{-1}(b)$  aynı denklemin  $A$ 'daki bir çözümüdür. Bunun kanıtı da oldukça kolaydır ve okura bırakılmıştır.

Özetleyecek olursak, denklemin  $A$ 'daki ve  $B$ 'deki çözüm kümeleri,  $\varphi$  eşyapı dönüşümü sayesinde birbirlerine tekabül ederler, yani eğer  $\mathcal{C}_A$  ve  $\mathcal{C}_B$  denklemin  $A$ 'daki ve  $B$ 'deki çözüm kümeleriyse, o zaman  $\varphi(\mathcal{C}_A) = \mathcal{C}_B$  ve  $\varphi^{-1}(\mathcal{C}_B) = \mathcal{C}_A$ 'dır.

Sonuç olarak, denklemi  $B$ 'de çözebiliyorsak,  $\varphi$  sayesinde aynı denklemi  $A$ 'da da çözebiliriz. Eğer  $A$ 'da çözebiliyorsak,  $\varphi$  sayesinde aynı denklemi  $B$ 'de de çözebiliriz.

Bu dediğimiz sadece  $x^2 = x$  denklemi için değil,  
 $(3x^2 - 5y)z = 4xy$

gibi toplama, çıkarma, çarpma ve tamsayılar kullanılarak yazılan bir ya da daha çok bilinmeyenli her denklem ya da denklem ailesi için de geçerlidir.

Bir sonraki paragrafta, yukardaki düşünceyi  $Z/nZ$ 'ye uyarlayıp,  $x^2 = x$  denkleminin  $Z/nZ$ 'deki çözüm sayısını bulacağız. Ama önce aşağıdaki sonuca ihtiyacımız var.

Aşağıdaki sonucun, yukardaki Ana Teorem'den hareketle,  $n$ 'yi bölen asal sayıların sayısı üzerine tümevarımla nasıl kanıtlanacağı bariz olmalı.

**Sonuç.**  $n > 1$  bir doğal sayı olsun.  $n$ 'yi asallarına ayıralım:  $n = p_1^{k_1} \dots p_r^{k_r}$ . Burada  $p_1, \dots, p_r$ ,  $n$ 'yi bölen birbirinden değişik asalardır. O zaman,

$$Z/nZ \approx Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z.$$

Ayrıca,  $Z/nZ$ 'nin bir  $(x \bmod n)$  elemanını,  $Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$ 'nin

$$(x \bmod p_1^{k_1}, \dots, x \bmod p_r^{k_r})$$

elemanına götüren fonksiyon bir eşyapı dönüşümüdür.

Bu sonuç şu anlama gelir:  $Z/nZ$  yapılarını anlamak için, asal  $p$ 'ler ve pozitif  $k$  doğal sayıları için,  $Z/p^kZ$  yapılarını anlamak yeterlidir. Bir başka deyişle,  $Z/nZ$  yapısında herhangi bir denklemi çözmek

için, bu denklemi, asal  $p$  ve pozitif  $k$ 'ler için  $Z/p^kZ$  yapısında çözebilmek yeterlidir. Daha sonraki yazılardan birinde (Hensel Önsavı yazısı), hepsi olmasa da birçok denklemi  $Z/p^kZ$  halkasında çözebilmek için, bu denklemin  $Z/pZ$  halkasında özel bir çözümü olduğunu kanıtlamanın yeterli olduğunu göreceğiz. Örneğin,  $Z/p^kZ$  halkasında hangi elemanların kare olduğunu anlamak için,  $Z/pZ$  halkasında hangi elemanların kare olduğunu anlamak yeterlidir. Ama bu konuya daha sonra değineceğiz.

Umarım burada yaptıklarımızın zevkine ve güzelliğine varıyorsunuzdur. Bugün olmazsa da yarın varırsınız, bu yazıyı yarın bir daha okuyun!

**Notlar. 1.** Bir  $A$  halkasından bir  $B$  halkasına giden bir  $\varphi$  eşlemesinin sadece toplamaya ve çarpmaya saygı duyması, eşlemenin çıkarmaya saygı duyması için yeterlidir. Bunu kanıtlayalım. Her şeyden önce  $\varphi(0_A) + 0_B = \varphi(0_A) = \varphi(0_A + 0_A) = \varphi(0_A) + \varphi(0_A)$  eşitliğinden,  $\varphi(0_A) = 0_B$  elde ederiz (MD-2004-II, sayfa 22, Önsav 1.i). Buradan da, her  $x \in A$  için,  $\varphi(x) + (-\varphi(x)) = 0_B = \varphi(0_A) = \varphi(x + (-x)) = \varphi(x) + \varphi(-x)$  ve dolayısıyla  $\varphi(-x) = -\varphi(x)$  elde edilir (MD-2004-II, sayfa 22, Önsav 1.i). Buradan da, her  $x, y \in A$  için,  $\varphi(x - y) = \varphi(x + (-y)) = \varphi(x) + \varphi(-y) = \varphi(x) + (-\varphi(y)) = \varphi(x) - \varphi(y)$  elde edilir. Demek ki  $\varphi$  çıkarmaya da saygı duyuyor.

**2.** Toplamaya saygı duyan ve  $Z/nZ$ 'nin birim elemanını  $\varphi(Z/nZ)$ 'nin birim elemanına götüren her  $\varphi : Z/nZ \rightarrow B$  fonksiyonu çarpmaya da saygı duyar. Bunun tümevarımla kanıtı oldukça kolaydır ve okura bırakılmıştır. (Dikkat:  $\varphi(Z/nZ)$ 'nin birim elemanı  $B$ 'nin birim elemanı olmak zorunda değildir.)

**V. Devede Kulak Bir Uygulama.**  $x^2 = x$  denklemini  $Z/nZ$  halkasında çözmeye çalışalım. Önce  $n$ 'yi asallarına ayırarak, yukardaki sonuçtaki gibi bir

$$Z/nZ \approx Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$$

eşyapısallık bulalım (ki böyle bir eşyapı dönüşümü biliyoruz: Bu dönüşüm,  $Z/nZ$ 'nin modülo  $n$  elemanlarını, her  $i = 1, \dots, r$  için modülo  $p_i^{k_i}$  yazıyor. Bir önceki sayfadaki gri karede bundan başka bir eşyapı dönüşümü olmadığını kanıtlamıştık.) Şimdi,  $x^2 = x$  denklemini  $Z/nZ$  halkasında çözmek yerine, aynı denklemi, daha kolay hesap yapabileceğimizi umduğumuz ve bu halkaya eşyapısal olan  $Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$  halkasında çözelim.

$Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$ 'nin elemanları,  
 $(x_1, \dots, x_r)$

olarak yazılırlar ve bu elemanların kareleri,  
 $(x_1^2, \dots, x_r^2)$

dir. Demek ki,  $Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$ 'de,  
 $(x_1^2, \dots, x_r^2) = (x_1, \dots, x_r)$

denklemini çözmeliyiz. Bu da, her  $i$  için,  $Z/p_r^{k_r}Z$ 'de  $x^2 = x$  denklemini çözmek demektir. O zaman biz de  $Z/p_r^{k_r}Z$ 'de  $x^2 = x$  denklemini çözelim:

**Önsav.**  $p$  bir asal ve  $k > 0$  bir tamsayı olsun. O zaman  $Z/p^kZ$  halkasında  $x^2 = x$  denkleminin tam iki çözümü vardır:  $\bar{0}$  ve  $\bar{1}$ .

**Kanıt:**  $a \in Z$ ,  $x^2 \equiv x \pmod{p^k}$  denkleminin bir çözümü olsun, yani  $\bar{a} \in Z/p^kZ$  elemanı  $x^2 - x \equiv \bar{0}$  denkleminin  $Z/p^kZ$ 'de bir çözümü olsun.  $a$ 'nın modülo  $p^k$ , ya 0 ya da 1 olduğunu kanıtlayacağız.

Önce  $k$ 'nin 1 olduğu duruma bakalım.  $a^2 \equiv a \pmod{p}$  denkleminin,  $p$  asalının  $a^2 - a$ 'yı böldüğü çıkar. Ama  $a^2 - a = a(a - 1)$  eşitliğinden dolayı, bundan,  $p$ 'nin  $a$  ya da  $a - 1$ 'i böldüğü çıkar. Demek ki  $a$  modülo  $p$  elemanı ya 0'a ya da 1'e eşit. Bu durumda önsav kanıtlanmıştır.

Şimdi  $k > 1$  olsun.  $a^2 \equiv a \pmod{p^k}$  denklemini modülo  $p$  alırsak,  $k = 1$  şikkından dolayı,

$$ya \ a \equiv 0 \pmod{p} \text{ ya da } a \equiv 1 \pmod{p}$$

buluruz. Duruma göre  $\varepsilon = 0$  ya da 1 olsun. Demek ki  $p$ ,  $a - \varepsilon$ 'yi bölüyor.

Eğer  $a - \varepsilon$ ,  $p^k$ 'ye bölünüyorsa, o zaman, modülo  $p^k$ ,  $a \equiv \varepsilon \pmod{p^k}$  ya da 1 ve sorun yok. Bundan böyle  $p^k$ 'nin  $a - \varepsilon$ 'yi bölmediğini varsayalım. Bir çelişki elde edeceğiz. Bu varsayımdan dolayı  $a - \varepsilon$ ,  $p$ 'ye bölünüyor ama  $p^k$ 'ye bölünmüyor.  $i = 1, \dots, k - 1$  için,  $p^i$ ,  $p$ 'nin  $a - \varepsilon$ 'yi bölen en büyük gücü olsun. Dolayısıyla,  $p$ 'ye bölünmeyen bir  $b$  için,  $a - \varepsilon = p^i b$ . Şimdi modülo  $p^k$  hesaplayalım:

$\varepsilon + p^i b = a \equiv a^2 = (\varepsilon + p^i b)^2 = \varepsilon^2 + 2\varepsilon p^i b + p^{2i} b^2$ .  
 Ama  $\varepsilon = 0, 1$  olduğundan,  $\varepsilon^2 = \varepsilon$ , dolayısıyla, sadeleştirerek,

$$(1 - 2\varepsilon)p^i b \equiv p^{2i} b^2 \pmod{p^k}$$

buluruz, yani,

$$(1 - 2\varepsilon)b \equiv p^i b^2 \pmod{p^{k-i}}$$

Hem  $i$  hem  $k - i > 0$  olduğundan, bundan,

$$(1 - 2\varepsilon)b \equiv 0 \pmod{p}$$

çıkar. Ama  $\varepsilon = 0$  ya da 1 olduğundan,  $1 - 2\varepsilon = \pm 1$ . Demek ki,  $\pm b \equiv 0 \pmod{p}$ , yani  $b \equiv 0 \pmod{p}$ , bir çelişki.  $\square$

**Sonuç.**  $n > 0$ , tam  $r$  tane değişik asal böleni olan bir tamsayı olsun. O zaman  $Z/nZ$  halkasında  $x^2 = x$  denkleminin tam  $2^r$  tane çözümü vardır.

**Kanıt:**  $p_1, \dots, p_r$  asal sayıları  $n$ 'nin  $r$  değişik asal böleni olsun.  $n = p_1^{k_1} \dots p_r^{k_r}$  ise, yukardaki sonuca göre,

$$Z/nZ \approx Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$$

olduğundan,  $Z/nZ$ 'deki  $x^2 = x$  denkleminin her çözümü,  $Z/p_i^{k_i}Z$ 'deki  $x^2 = x$  denklemini sağlayan bir ve bir tek  $\varepsilon_i$  elemanı için (ki yukardaki önsava göre bunlardan 0 ve 1 olmak üzere tam iki tane olduğunu biliyoruz),  $Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$  yapısının

$$(\varepsilon_1, \dots, \varepsilon_r)$$

elemanına tekabül eder.  $\varepsilon_i = 0, 1$  olduğundan, bu  $(\varepsilon_1, \dots, \varepsilon_r)$  elemanlarından tam  $2^r$  tane vardır.  $\square$

Biraz daha ilerde  $Z/nZ$  halkasında  $x^2 = x$  denkleminin çözümlerini teker teker nasıl bulacağımızı göreceğiz.

## VI. Ana Teoremin Önemli Bir Uygulaması:

**Çin Kalanlar Teoremi.** Yukardaki uygulama iyi güzel de, çok çok önemli bir sonuç değil. Oysa kanıtladığımız teorem çok genel ve uygulama sahası sonsuz. Bu paragrafta, yukardaki teoremin bir başka sonucunu ele alacağız: Çin Kalanlar Teoremi. Bu teoremi geçen sayıda da kanıtlamıştık [MD-2004-II, sayfa 13-16].

**Sonuç 6 (Çin Kalanlar Teoremi).**  $n_1, n_2, \dots, n_r$  pozitif doğal sayıları ikişer ikişer aralarında asal olsunlar.  $s_1, s_2, \dots, s_r \in Z$  olsun. O zaman,

$$x \equiv s_1 \pmod{n_1}$$

...

$$x \equiv s_r \pmod{n_r}$$

denklik sisteminin bir çözümü vardır. Ayrıca bu çözüm modülo  $n_1 \dots n_r$  bir tanedir.

**Kanıt:** Ana Teorem'i tekrar tekrar uygulayalım: Ana teorem sayesinde,

$$Z/n_1 \dots n_r Z \text{ ile } Z/n_1 Z \times \dots \times Z/n_r Z$$

cebirsel yapıları arasında bir  $\varphi$  eşyapı dönüşümü buluruz. ( $\bar{\varphi}$  yerine  $\varphi$  yazıyoruz, okur anlayışla karşılar herhalde.) Ana Teorem'den de anlaşılacağı üzere,  $\varphi$ ,  $Z/n_1 \dots n_r Z$ 'nin bir

$$(x \pmod{n_1 \dots n_r})$$

elemanını  $Z/n_1 Z \times \dots \times Z/n_r Z$ 'nin

$$\varphi(x \pmod{n_1 \dots n_r}) = (x \pmod{n_1}, \dots, x \pmod{n_r})$$

elemanına yollar. Şimdi  $x$ ,  $Z/n_1 Z \times \dots \times Z/n_r Z$ 'nin

$(s_1 \bmod n_1, \dots, s_r \bmod n_r)$  elemanının  $Z/n_1 \dots n_r Z$ 'deki önimgesi olsun, yani,  
 $\varphi(x \bmod n_1 \dots n_r) = (s_1 \bmod n_1, \dots, s_r \bmod n_r)$  eşitliği sağlansın.  $\varphi$  örten olduğundan böyle bir  $x$  vardır. Demek ki,  
 $(x \bmod n_1, \dots, x \bmod n_r) = (s_1 \bmod n_1, \dots, s_r \bmod n_r)$ , yani her  $i = 1, \dots, r$  için,  
 $(x \bmod n_i) = (s_i \bmod n_i)$ ,  
yani  
 $x \equiv s_i \bmod n_i$ .  
Teorem kanıtlanmıştır.  $\square$

**VII.  $\varphi$ 'nin Tersisi.** Yukarlarda bir yerde  $Z/nZ$  halkasında  $x^2 = x$  denkleminin çözüm sayısını bulmak için,  $n$ 'yi  $n = p_1^{k_1} \dots p_r^{k_r}$  olarak asallarına ayırmış, ardından,  $x^2 = x$  denklemini  $Z/nZ$  halkası yerine bu halkaya eşyapısal olan  $Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$  halkasında çözmüştük. Toplam  $2^r$  çözüm bulmuştuk. Ama  $Z/nZ$  halkasında  $x^2 = x$  denkleminin çözümlerini teker teker bulmamıştık, sadece çözümlerini bulmakla yetinmiştik. Bu bölümde  $x^2 = x$  denkleminin  $Z/nZ$  halkasındaki çözümleri teker teker bulmayı öğreneceğiz.

$\varphi : Z/nZ \rightarrow Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$ , daha önce bulduğumuz eşyapı dönüşümü olsun.  
 $\varphi(x \bmod n) = (x \bmod p_1^{k_1}, \dots, x \bmod p_r^{k_r})$  eşitliğini bir kez daha anımsatırım.  $\varphi$  eşleşmesinin tersi olan

$\varphi^{-1} : Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z \rightarrow Z/nZ$  eşleşmesini bulmalıyız ki,  $x^2 = x$  denkleminin  $Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$  halkasında bulduğumuz her  $(\varepsilon_1, \dots, \varepsilon_r)$  çözümünün (buradaki  $\varepsilon_i$ 'lerin 0 ya da 1 oldukları bu yazıda kanıtlandı)  $Z/nZ$  halkasında tekabül ettiği  $\varphi^{-1}(\varepsilon_1, \dots, \varepsilon_r)$  çözümünü bulalım.

Eğer  $Z/nZ$  halkasında,

$$\varphi(\alpha_1) = (1, 0, 0, \dots, 0, 0)$$

$$\varphi(\alpha_2) = (0, 1, 0, \dots, 0, 0)$$

...

$$\varphi(\alpha_r) = (0, 0, 0, \dots, 0, 1)$$

eşitliklerini sağlayan  $\alpha_1, \alpha_2, \dots, \alpha_r$  elemanları bulabilirsek, o zaman, her

$$(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_r) \in Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$$

için (şart değil ama eğer istersek  $y_i$ 'leri doğal sayı alabiliriz),

$$\begin{aligned} \varphi(y_1\alpha_1 + y_2\alpha_2 + \dots + y_r\alpha_r) &= \varphi(y_1\alpha_1) + \varphi(y_2\alpha_2) + \dots + \varphi(y_r\alpha_r) \\ &= y_1\varphi(\alpha_1) + y_2\varphi(\alpha_2) + \dots + y_r\varphi(\alpha_r) \end{aligned}$$

$$= y_1(1, 0, \dots, 0) + y_2(0, 1, \dots, 0) + \dots + y_r(0, 0, \dots, 1)$$

$$= (\bar{y}_1, \bar{y}_2, \dots, \bar{y}_r)$$

elde ederiz. Böylece,

$\varphi^{-1}(\bar{y}_1, \bar{y}_2, \dots, \bar{y}_r) = y_1\alpha_1 + y_2\alpha_2 + \dots + y_r\alpha_r$  olur ve  $\varphi^{-1}$  eşleşmesi bulunmuş olur. Demek ki  $\varphi^{-1}$  eşleşmesini bulmak için  $Z/nZ$ 'nin yukardaki eşitlikleri sağlayan  $\alpha_1, \alpha_2, \dots, \alpha_r$  elemanlarını bulmalıyız. Birini bulmak demek hepsini bulmak demek olduğundan, biz sadece birincisini bulalım.

$$\varphi(\bar{a}) = (1, 0, 0, \dots, 0, 0)$$

eşitliğini, yani,

$$a \equiv 1 \bmod p_1^{k_1}$$

$$a \equiv 0 \bmod p_2^{k_2}$$

...

$$a \equiv 0 \bmod p_r^{k_r}$$

denkliklerini sağlayan bir  $a$  tamsayısı arıyoruz ( $\alpha_1 = \bar{a}$  olacak.) Demek ki  $a$  tamsayısı  $p_2^{k_2}, \dots, p_r^{k_r}$  sayılarına bölünmeli. Bunlar aralarında asal olduklarından,  $a$  tamsayısı  $p_2^{k_2} \dots p_r^{k_r}$  çarpımına bölünmeli. Dolayısıyla bir  $u$  tamsayısı için,

$$a = up_2^{k_2} \dots p_r^{k_r}$$

eşitliği sağlanmalı. Bu eşitlik bize birincisi dışında son  $r - 1$  denkliği verecek. Birinci denkliği elde etmek için,  $u$  bir de ayrıca

$$up_2^{k_2} \dots p_r^{k_r} \equiv 1 \bmod p_1^{k_1}$$

denkliğini sağlayacak biçimde seçilmelidir, yani,

$$up_2^{k_2} \dots p_r^{k_r} - 1 = vp_1^{k_1}$$

eşitliğini, yani,

$$up_2^{k_2} \dots p_r^{k_r} - vp_1^{k_1} = 1$$

eşitliğini sağlayan bir  $v$  olmalıdır. Ama  $p_2^{k_2} \dots p_r^{k_r}$  ve  $p_1^{k_1}$  aralarında asallar. Demek ki yukardaki

$$up_2^{k_2} \dots p_r^{k_r} - vp_1^{k_1} = 1$$

eşitliğini sağlayan bir  $u$  ve  $v$  vardır. Geçen sayımız-

## Z/180Z Halkasının Eşgüçlülere

$Z/180Z$  halkasında  $x^2 = x$  denklemini çözelim.

$$\varphi : Z/180Z \rightarrow Z/4Z \times Z/9Z \times Z/5Z$$

eşyapı dönüşümünün tersini bulmamız gerekiyor. Açıklanan yöntemi kullanalım. Oldukça kolay bir şekilde  $\alpha_1 = 45, \alpha_2 = 100, \alpha_3 = 36$  bulunur. Dolayısıyla,

$$\varphi^{-1}(y_1, y_2, y_3) = 45y_1 + 100y_2 + 36y_3,$$

ve,

$$\varphi^{-1}(0, 0, 0) = 0 \quad \varphi^{-1}(1, 0, 0) = 45$$

$$\varphi^{-1}(0, 0, 1) = 36 \quad \varphi^{-1}(1, 0, 1) = 81$$

$$\varphi^{-1}(0, 1, 0) = 100 \quad \varphi^{-1}(1, 1, 0) = 145$$

$$\varphi^{-1}(0, 1, 1) = 136 \quad \varphi^{-1}(1, 1, 1) = 181 = 1.$$

Demek ki,  $Z/180Z$  halkasının eşgüçlülere, sırasıyla (!) 0, 36, 100, 136, 45, 81, 145 ve 1.

da bu  $u$  ve  $v$  sayıların sadece varlığını değil, gerçekten nasıl bulunacağını da göstermiştik [MD-2004-II, sayfa 14].  $\square$

**VIII. Bir Uygulama:  $Z/nZ$ 'de  $x^2 = 1$  Eşitliği.**  $Z/nZ$  halkasında  $x^2 = 1$  denkleminin çözüm sayısını bulalım. Elbette  $x = 1$  ve  $x = -1$  bu denklemin iki çözümü. Acaba başka çözüm var mı? Varsa kaç tane çözüm var?

Yukarda yaptığımız gibi bu denklemi önce asal  $p$  sayıları için  $Z/p^kZ$  halkasında çözeceğiz.

$$a \in \{0, 1, \dots, p^k - 1\} \text{ sayısı,}$$

$$a^2 \equiv 1 \pmod{p^k}$$

denkliğini sağlasın. O zaman  $p^k, a^2 - 1$ 'i, yani

$$(a - 1)(a + 1)$$

sayısını böler. Dolayısıyla bir  $i = 0, 1, \dots, k$  için,  $p^i, a - 1$ 'i ve  $p^{k-i}, a + 1$ 'i böler. Eğer  $i = 0$  ya da  $i = k$  ise (örneğin  $k = 1$  ise bu böyle olmak zorunda), o zaman ya  $a \equiv 1 \pmod{p^k}$  ya da  $a \equiv -1 \pmod{p^k}$  ve bunlar en başından beri bildiğimiz çözümler. Bundan böyle  $0 < i < k$  eşitsizliğini varsayalım (dolayısıyla  $k > 1$  olmalı). Eğer  $j, i$  ve  $k - i$ 'nin en küçüğüyse, o zaman  $p^j$  hem  $a - 1$ 'i hem de  $a + 1$ 'i böler. Dolayısıyla,  $p^j$  bu iki sayının farkı olan,

$$(a + 1) - (a - 1) = 2$$

sayısını da böler. Dolayısıyla  $p = 2$  ve  $j = 1$ 'dir. Demek ki, ya  $i = 1$  ya da  $i = k - 1$ . Yani  $\varepsilon = \pm 1$  için,  $p^{k-1}, a + \varepsilon$  sayısını böler ( $p$ 'nin 2 olduğunu unutmayın), yani ya  $a = \varepsilon$  ya da  $a = p^{k-1} + \varepsilon$  (çünkü  $p = 2$ ). Eğer  $k = 2$  ise, bu bize,  $a = p^{k-1} + \varepsilon = 2 + \varepsilon = \varepsilon\varepsilon$ , yani eski çözümleri verir. Sonuç olarak şunu buluruz:

**Önsav.**  $p$  bir asal ve  $k > 0$  bir doğal sayı olsun.  $x^2 = 1$  denkleminin  $Z/p^kZ$  halkasında,

- Eğer  $p \neq 2$  ya da  $p = k = 2$  ise, tam iki çözümü vardır:  $\pm 1$ .
- Eğer  $p = 2$  ve  $k > 2$  ise, tam dört çözümü vardır:  $\pm 1, 2^{k-1} \pm 1$ .
- Eğer  $p = 2$  ve  $k = 1$  ise, tek çözümü vardır: 1.

Şimdi  $Z/nZ$ 'de  $x^2 = 1$  denkleminin çözüm sayısını bulabiliriz. Önce  $n$ 'yi daha önce yaptığımız gibi  $n = p_1^{k_1} \dots p_r^{k_r}$  olarak asallarına ayırırız, ardından,  $x^2 = 1$  denklemini  $Z/nZ$  halkası yerine bu halkaya eşyapısal olan  $Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$  halkasında çözeriz. Eğer  $p_i$ 'lerden biri 2 ise (yani  $n$  çiftse), bunun  $p_1$  olduğunu varsayalım.

• Eğer 2,  $n$ 'yi bölmüyorsa, yani her  $p_i \neq 2$  ise, o zaman  $x^2 = 1$  denkleminin  $Z/nZ$ 'de tam  $2^r$  tane

çözümü vardır. Bu çözümler  $Z/p_1^{k_1}Z \times \dots \times Z/p_r^{k_r}Z$  halkasının  $\varepsilon_i = \pm 1$  için ( $\varepsilon_1, \dots, \varepsilon_r$ ) elemanlarına tekabül ederler.

• Eğer  $n$ , 4'e bölünmeyen bir çift sayıysa, yani  $p_1 = 2$  ve  $k_1 = 1$  ise, o zaman  $x^2 = 1$  denkleminin  $Z/nZ$ 'de tam  $2^{r-1}$  tane çözümü vardır. Her çözüm,  $Z/2Z \times Z/p_2^{k_2}Z \times \dots \times Z/p_r^{k_r}Z$  halkasının,  $\varepsilon_i = \pm 1$  için, ( $1, \varepsilon_2, \dots, \varepsilon_r$ ) elemanına tekabül ederler.

• Eğer  $n$ , 4'e bölünen ama 8'e bölünmeyen bir sayıysa, yani  $p_1 = 2$  ve  $k_1 = 2$  ise, o zaman  $x^2 = 1$  denkleminin  $Z/nZ$ 'de tam  $2^r$  tane çözümü vardır. Her çözüm,  $Z/4Z \times Z/p_2^{k_2}Z \times \dots \times Z/p_r^{k_r}Z$  halkasının,  $\varepsilon_i = \pm 1$  için ( $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r$ ) elemanına tekabül eder.

• Eğer  $n$ , 8'e bölünen bir sayıysa, yani  $p_1 = 2, k_1 > 2$  ise, o zaman  $x^2 = 1$  denkleminin  $Z/nZ$ 'de tam  $2^{r+1}$  tane çözümü vardır. Her çözüm,  $Z/2^{k_1}Z \times Z/p_2^{k_2}Z \times \dots \times Z/p_r^{k_r}Z$  halkasının,  $v = 0, 1$  ve  $\varepsilon_i = \pm 1$  için,  $(v2^{k_1-1} + \varepsilon_1, \varepsilon_2, \dots, \varepsilon_r)$  elemanına tekabül eder.

#### Alıştırılmalar.

1.  $Z/6Z$  halkasından rastgele  $a$  ve  $b$  sayıları seçiliyor.  $ax + b = 0$  denkleminin  $Z/6Z$ 'de bir çözümü olma olasılığı kaçtır?

2.  $Z/5Z$  halkasından rastgele  $a$  ve  $b$  sayıları seçiliyor.  $x^2 + ax + b = 0$  denkleminin  $Z/5Z$ 'de bir çözümü olma olasılığı kaçtır?

3. Eğer  $n$  tek bir sayıysa,  $Z/nZ$ 'de  $x^2 + ax + b = 0$  denkleminin çözümü olması için yeter ve gerek koşulun  $b - a^2/4$ 'ün  $Z/nZ$ 'de bir karekökünün olması olduğunu kanıtlayın. (Burada,  $a^2/4$  ne anlama gelmektedir?)

4.  $Z/6Z$  halkasından rastgele  $a, b$  ve  $c$  sayıları seçiliyor.  $ax^2 + bx + c = 0$  denkleminin  $Z/6Z$ 'de bir çözümü olma olasılığı kaçtır?

5.  $Z/nZ$  halkasında,  $x^2 = 1$  denkleminin çözümlerinin çarpımını bulun.

6.  $Z/nZ$  halkasında,  $x^2 = -x$  denkleminin kaç çözümü vardır?

7\*. Hangi  $p$  asalları için  $x^2 = -1$  denkleminin  $Z/pZ$  halkasında bir çözümü vardır?

8\*\*\*. Hangi  $p$  asalları için  $x^2 = 2$  denkleminin  $Z/pZ$  halkasında bir çözümü vardır?

9\*\*\*.  $Z/pZ$  ( $p$  asal) halkasında rastgele bir sayının kare olma olasılığı kaçtır?  $Z/p^kZ$  halkasında rastgele bir sayının kare olma olasılığı kaçtır? (Bknz. Hensel Önsavı yazısı).  $k$  sonsuza giderken bu olasılıkların bir limiti var mıdır ve varsa bu limit kaçtır?  $\blacklozenge$