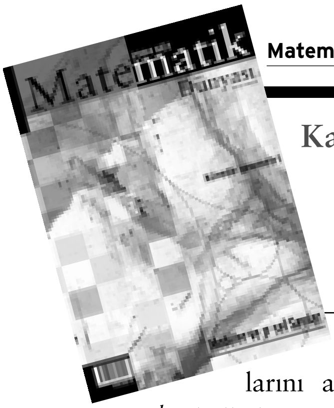


Kapak Konusu: Modüler ve p-sel Sayılar

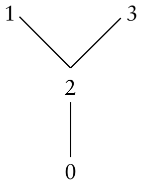
$\mathbb{Z}/p^k\mathbb{Z}$ Halkalarının Resmi

Geçen yazıda $\mathbb{Z}/n\mathbb{Z}$ halkalarını anlamak için, asal p'ler için $\mathbb{Z}/p^k\mathbb{Z}$ halkalarını anlamamız gerektiğini görmüştük. Bu yazıda, $k > 1$ için, $\mathbb{Z}/p^k\mathbb{Z}$ halkalarının resmini çizerek bu halkaların daha iyi anlaşılmasını sağlayacağız. İlerde, Hensel Önsavı yazısında, $\mathbb{Z}/p^k\mathbb{Z}$ halkalarını anlamak için büyük ölçüde $\mathbb{Z}/p\mathbb{Z}$ halkalarını anlamamız gerektiğini göreceğiz.

Örnek 1. $\mathbb{Z}/p^k\mathbb{Z}$ halkalarını incelemeye

$$\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

halkasıyla başlayalım ($p = 2$, $k = 2$). Bu halkanın elemanlarını yandaki şekildeki gibi gösterelim. Yazılımda kolaylık olsun diye $\overline{a}$ yerine a yazdık ve yazmakta da ısrar edeceğiz. Okurun bu yazılıma yabancılık çekmeyeceğini, tam tersine sayıların üstünde beliren çizgilerden kurtulduğuna sevineceğini ve $\mathbb{Z}/4\mathbb{Z}$ halkasının elemanlarıyla $\mathbb{Z}$'nin elemanlarıyla karıştırmayacağını umuyoruz.

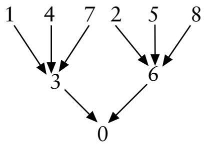


$\mathbb{Z}/4\mathbb{Z}$

Yukardaki şeklin en üst katındaki 1 ve 3 elemanlarını ikiyle çarparsak orta kata, tam 2'ye düşeriz: $2 \times 1 = 2$ ve $2 \times 3 = 2$. Orta katı (yani 2'yi) ikiyle çarparsak zemin kattaki 0'a düşeriz. En üst kattaki elemanlar $\mathbb{Z}/4\mathbb{Z}$ halkasının tersinir elemanlardır, yani bu elemanları başka bir elemanla çarparak birim eleman olan 1'i elde edebiliriz; nitekim $1 \times 1 = 1$ ve $3 \times 3 = 1$.

Örnek 2. Şimdi de $\mathbb{Z}/9\mathbb{Z}$ halkasını benzer bir şemayla gösterelim.

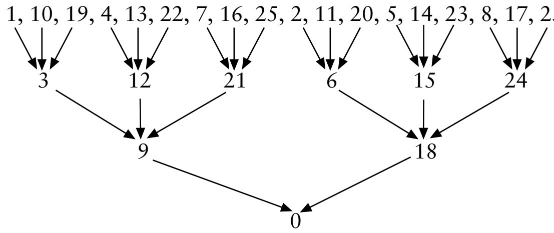
Bu kez her 3'le çarpmada bir alt kata iniyoruz. En alt katta $\mathbb{Z}/9\mathbb{Z}$'nin 9'a bölünen tek elemanı olan 0 var. Onun bir üstünde 3'e bölünen ama 9'a bölünmeyen elemanlar (3 ve 6) var. En tepede de 1'e bölünen ama 3'e bölünmeyen (yani 3'e asal) 1, 4, 7, 2, 5, 8 elemanları var. En üste kattaki bu elemanlar tersinirdir:



$\mathbb{Z}/9\mathbb{Z}$

$$1 \times 1 = 1,\ 4 \times 7 = 1,\ 2 \times 5 = 1,\ 8 \times 8 = 1.$$

Örnek 3. $\mathbb{Z}/27\mathbb{Z}$ halkasını çizelim şimdi (resmi aşağıda). Bir kez daha elemanlar 3'le çarpıldıklarında bir kat aşağı iniyorlar. En alt katta 27'ye bölünen tek eleman olan 0 var. Onun bir üstünde 9'a bölünen ama 27'ye bölünmeyen elemanlar var: 9 ve 18. Onun da üstünde 3'e bölünen ama 9'a bölünmeyen sayılar var: 3, 12, 21, 6, 15, 24 (sırasıyla!) En üst katta da 1'e bölünen ama 3'e bölünmeyen, yani 3'e asal sayılar var; bunlar $\mathbb{Z}/27\mathbb{Z}$ halkasının tersinir elemanlarıdır; terslerini bulmayı okura bırakıyoruz bu kez.



$\mathbb{Z}/27\mathbb{Z}$

$\mathbb{Z}/27\mathbb{Z}$'ye en alt kattan başlayarak bakalım:

Zemin kat: $27(\mathbb{Z}/27\mathbb{Z}) = 27\mathbb{Z}/27\mathbb{Z} = \{0\}$.

İlk iki kat: $9(\mathbb{Z}/27\mathbb{Z}) = 9\mathbb{Z}/27\mathbb{Z} = \{0, 9, 18\}$.

İlk üç kat: $3(\mathbb{Z}/27\mathbb{Z}) = 3\mathbb{Z}/27\mathbb{Z} = \{0, 3, 6, 9, 12, 15, 18, 21, 24\}$.

Tüm katlar: $\mathbb{Z}/27\mathbb{Z}$.

Genel Durum. Eğer p herhangi bir pozitif doğal sayıysa (ama çoğu zaman p bir asal olarak alınır), $\mathbb{Z}/p^k\mathbb{Z}$ halkasını bir sonraki sayfadaki gibi resmedebiliriz. Bu resimde, her kat ve aşağısı, belli bir $i = 0, 1, ..., k$ için, $\mathbb{Z}/p^k\mathbb{Z}$'nin p^i'ye bölünen (ya da p^i'nin çarpımı) olan elemanlarından oluşan

$$p^i\mathbb{Z}/p^k\mathbb{Z}$$

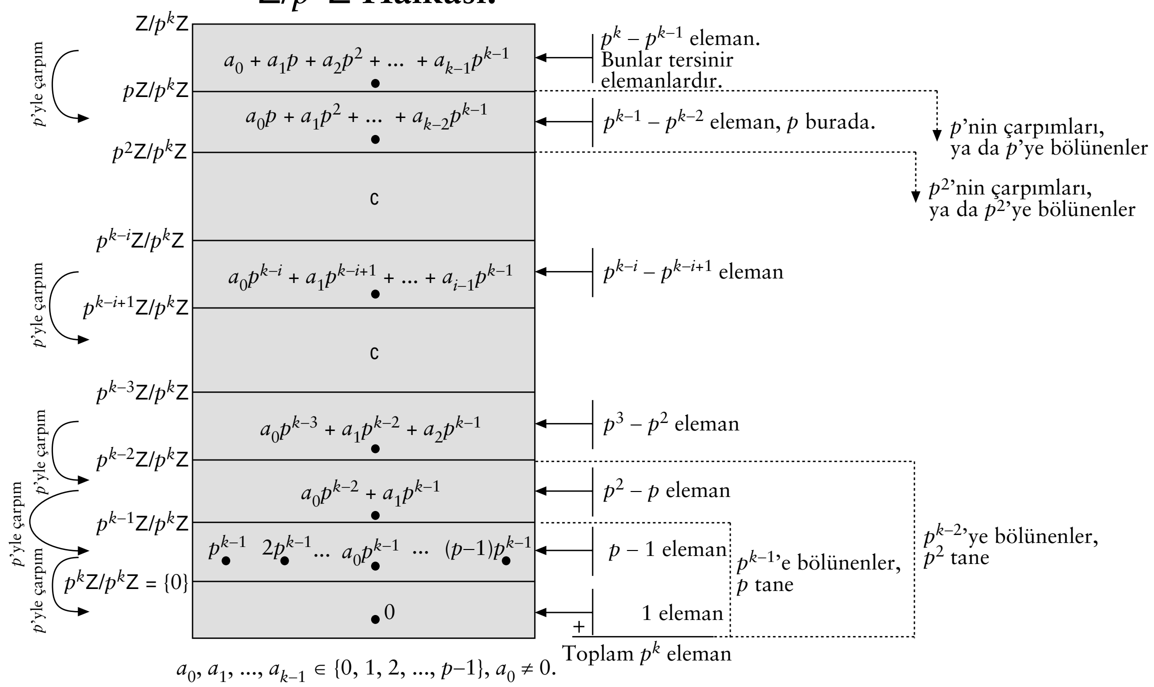
kümesinden oluşur. Kat çıktıkça i küçülür.

Zemin katta $\mathbb{Z}/p^k\mathbb{Z}$ halkasının p^k'ye bölünen tek elemanı olan 0 tek başına yaşar.

Onun bir üst katında (buna birinci kat diyelim) p^{k-1}'e bölünen ama p^k'ye bölünmeyen, yani belli bir $a_0 = 1, 2, ..., p-1$ için, a_0p^{k-1} şeklinde yazılan

$$p^{k-1}, 2p^{k-1}, 3p^{k-1}, ..., (p-1)p^{k-1}$$

$\mathbb{Z}/p^k\mathbb{Z}$ Halkası:



elemanları yaşar. Bunlardan tam $p-1$ tane vardır ve her birinin p'yle çarpımı 0'dır.

İkinci katta, p^{k-2}'ye bölünen ama p^{k-1}'e bölünmeyen, yani $a_0 = 1, 2, ..., p-1$ ve $a_1 = 0, 1, 2, ..., p-1$ için,
$$a_0p^{k-2} + a_1p^{k-1}$$
şeklinde yazılan $p^2 - p$ tane eleman yaşar. Bunları p'yle çarparsak bir alt kata düşeriz ($p^k \equiv 0$ denkliğini unutmayın):
$$p(a_0p^{k-2} + a_1p^{k-1}) \equiv a_0p^{k-1} \pmod{p^k}$$

Böylece ilk üç katta (zemin, birinci, ve ikinci katlarda) p^{k-2}'ye bölünen toplam p^2 tane eleman yaşar. Bunlar, $a_0, a_1 = 0, 1, ..., p-1$ için
$$a_0p^{k-2} + a_1p^{k-1}$$
biçiminde yazılırlar ve p^2'yle çarpımları 0'dır.

Bu yöntemle kat kat çıkarız. i-inci katta p^{k-i}'ye bölünen ama p^{k-i+1}'e bölünmeyen elemanlar, yani, $a_0, a_1, ..., a_{i-1} = 0, 1, 2, ..., p - 1$ ve $a_0 \neq 0$ için,
$$a_0p^{k-i} + a_1p^{k-i+1} + ... + a_{i-1}p^{k-1}$$
biçiminde yazılan elemanları yaşar.

i-inci ve altındaki katlarda p^{k-i}'ye bölünen elemanların tümü (toplam p^i tane) yer alır.

En üst kat olan k-inci katta da p^{k-k}'ye bölünen ama p^{k-k+1}'e bölünmeyen, yani 1'e bölünen ama p'ye bölünmeyen, yani sadece p'ye bölünmeyen elemanlar yaşar. Bütün tersinir elemanlar en üst katta otururlar, onların böyle bir ayrıcalığı vardır. Örneğin 1 en üst kattadır. Eğer p asalsa, ki genellikle asal alınır, en üst kattaki her sayı tersinirdir, aksi halde en üst katta tersinir olmayan elemanlar da bulunur.

p elemanı üstten bir altta oturur, p^2 ise üstten iki altta...

p asal olduğunda, tersinir elemanlar tam tamına p'ye asal elemanlar olduklarından, tersinir elemanlar belli bir $0 < a_0 < p$ için,
$$a_0 + a_1p + a_2p^2 + ... + a_{k-1}p^{k-1}$$
biçiminde yazılırlar. Tersinir elemanlar kümesinin $(\mathbb{Z}/p^k\mathbb{Z})^*$ olarak yazıldığını geçen sayılardan anımsayalım. Demek ki,
$$(\mathbb{Z}/p^k\mathbb{Z})^* = \{a_0 + a_1p + a_2p^2 + ... + a_{k-1}p^{k-1} : \text{her } i = 0, 1, ..., k-1 \text{ için}, 0 \leq a_i < p, a_0 \neq 0\} = \mathbb{Z}/p^k\mathbb{Z} \setminus p\mathbb{Z}/p^k\mathbb{Z}.$$

$\mathbb{Z}/p^k\mathbb{Z}$'nin 0 olmayan her elemanının belli bir $i = 1, 2, ..., k-1$ ve $a_0 \neq 0$ için,
$$a_0p^{k-i} + a_1p^{k-i+1} + ... + a_{i-1}p^{k-1}$$
biçiminde yazıldığı anlaşılıyor. Bu elemanı,
$$p^{k-i}(a_0 + a_1p^1 + ... + a_{i-1}p^{i-1})$$
biçiminde de yazabiliriz. $a_0 \neq 0$ eşitsizliğinden, parantezdeki elemanın tersinir olduğu anlaşılır. Dolayısıyla 0 olmayan her eleman, belli bir $i = 1, 2, ..., k-1$ için
$$p^{k-i}(\mathbb{Z}/p^k\mathbb{Z})^*$$
kümesindedir. Bu aşamada artık aşağıdaki teoremin kanıtı kolay olmalı:

Teorem. *Eğer p asalsa $\mathbb{Z}/p^k\mathbb{Z}$'nin 0 olmayan her elemanı bir ve bir tek $j = 0, 1, ..., k-1$ ve $\alpha \in (\mathbb{Z}/p^k\mathbb{Z})^*$ için, $p^j\alpha$ olarak yazılır.* ♦