

## $Z/p^kZ$ Halkalarının Geçit Resmi: $p$ -sel Tamsayılar

### I. Resim. Geçen yazıda

$Z/p^kZ$  halkalarının her birinin ayrı bir resmini yapmıştık. Geçen yazıdaki resim  $Z/p^kZ$  halkasını çalışırken çok kullanışlıdır ve çok işe yarar. Ama değişik  $k$ 'ler için değişik  $Z/p^kZ$  halkaları gerektiğinde,  $Z/pZ$ ,  $Z/p^2Z$ , ...,  $Z/p^kZ$ , ... halkalarının hepsini birden resmeden çok daha kullanışlı bir başka resim vardır. Bu yazıda, sabit bir  $p$  için,  $Z/p^kZ$  halkalarının hepsinin birden resmini yapacağız. Resimde  $p$  sabit kalacak ama  $k$  değişecek.

Örnek olarak  $p = 3$ ,  $k = 3$  alalım, yani  $p^k = 3^3 = 27$ . Bu sayfanın en altındaki şekilden izleyin. En üst katta modülo 27 tüm sayılar var: Bunlar 0'dan 26'ya kadar olan sayılarla gösterilen elemanlar. Onun altında modülo 9 sayılar var: 0'dan 8'e kadar. Onun altında da modülo 3 sayılar var: 0, 1 ve 2.

En üst kattaki modülo 27 sayılar modülo 9 alınır, her sayı bir alt katındaki sayıyı verir. İkinci kattaki modülo 9 sayılar modülo 3 alınır, her sayı gene bir alt katındaki sayıyı verir. En üst kattaki modülo 27 sayılardan biri modülo 3 alınır, o sayının iki kat altındaki modülo 3 sayı bulunur.

Bu çizelgeyi bir kat daha çıkıp modülo 81 sayı-

ları bulabilirdik. (Sayfanın ortasındaki şekilden izleyin şimdi.) Bunun için üçüncü kattaki her sayıya üç dal daha eklemek gerekirdi. Üçüncü katın her sayısına 0, 27 ve 54 ekleyerek dördüncü katın sayılarını (modülo 81 sayıları) bulabiliriz. Örneğin,

$$58 = 1 \cdot 3^0 + 1 \cdot 3 + 0 \cdot 3^2 + 2 \cdot 3^3$$

olduğundan, 58 sayısı

$$1 \cdot 3^0 + 1 \cdot 3 + 0 \cdot 3^2$$

sayısının, yani üçüncü kattaki 4'ün sağ üstüne gelecek, en alttan başlayarak 1-4-4-58 çizgisini izleyecek. 1-4-4 dizisinin üstüne gelecek sayılar soldan sağa doğru,

$$1 \cdot 3^0 + 1 \cdot 3^1 + 0 \cdot 3^2 + 0 \cdot 3^3 = 4$$

$$1 \cdot 3^0 + 1 \cdot 3^1 + 0 \cdot 3^2 + 1 \cdot 3^3 = 31$$

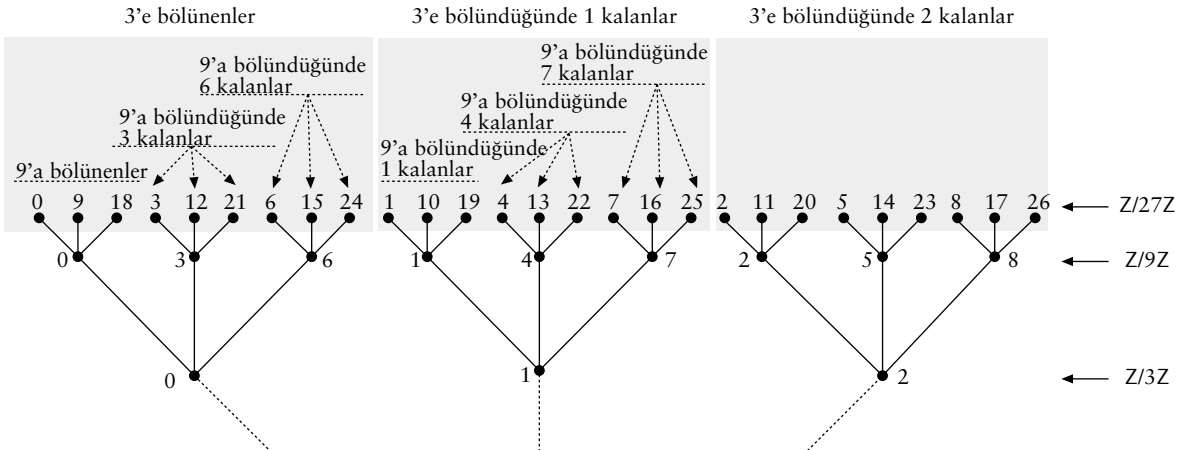
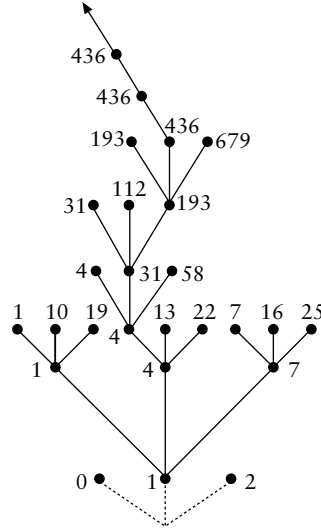
$$1 \cdot 3^0 + 1 \cdot 3^1 + 0 \cdot 3^2 + 2 \cdot 3^3 = 58$$

sayıları olacak.

Durmanın anlamı yok, modülo 81 sayıları yazdıktan sonra bir kat daha çıkararak modülo 243 sayıları da yazabiliriz. Daha sonra modülo 729 sayıları yazabiliriz...

Bu yöntemle hiç durmadan devam ederek, her dalı üçe ayırıp yukarı doğru çıkararak, değişik  $k$ 'ler için tüm  $Z/3^kZ$  halkalarını resmedebiliriz.

Diyelim 436'nın sonsuz ağaçtaki yerini bulmak istiyoruz. Yani 436'yı modülo 3, modülo 9,





$$1 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4 + \dots$$

“sayı”sı (artık  $3^0$  yerine 1 yazıyoruz.) Pek yakında bu “sayı”nın  $-1/2$  olduğunu göreceğiz!

Biraz önce  $-1$  için yazdığımız denklemleri (her  $2^i$  için bir tane olmak üzere sonsuz sayıda denklik vardı),

$$-1 \equiv 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

olarak tek bir denklikle göstereyim.

Şimdi de  $-2$ 'nin yolunu bulalım.  $-2$ 'nin yolunu bulmak için  $-1$ 'e yaptığımızı yapabiliriz, yani  $-2$ 'yi modülo 3, modülo  $3^2$ , modülo  $3^3$ , modülo  $3^3$  bulup bu yazılımda katsayıların aldıkları değerlere göre  $-2$ 'nin her adımda üç yoldan hangisini seçtiğini bulabiliriz. Ama daha ilginç, daha kolay ve daha çok bilgi veren bir yöntem daha var.  $-2$ 'nin yolunu  $-1$ 'in yolundan çıkarabiliriz.  $-1$ 'in yolunu biliyoruz:

$$-1 \equiv 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots,$$

hep sağa gidiyor (yani katsayılar hep 2). Denkliğin her iki tarafından da 1 çıkarırsak  $-2$ 'nin yolunu buluruz:

$$-2 \equiv 1 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

Demek ki  $-2$  önce orta yolu seçip, sonra hep sağa gidiyor.  $-2$ 'den 1 çıkarıp  $-3$ 'ün yolunu bulalım:

$$-3 \equiv 0 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

Bir kez daha 1 çıkarıp  $-4$ 'ün yolunu bulalım:

$$-4 \equiv 2 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

İşte ilk birkaç negatif sayının güzergâhı:

$$-1 \equiv 2 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-2 \equiv 1 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-3 \equiv 0 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-4 \equiv 2 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-5 \equiv 1 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-6 \equiv 0 + 1 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-7 \equiv 2 + 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-8 \equiv 1 + 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-9 \equiv 0 + 0 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-10 \equiv 2 + 2 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-11 \equiv 1 + 2 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$-12 \equiv 0 + 2 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

Görüldüğü gibi pozitif sayılar bir zaman sonra hep sola gidiyorlar, negatif sayılarsa tam tersine bir zaman sonra hep sağa. Ama sonuç olarak her tam sayı ağacın en tepesinde, daha doğrusu en dipten başlayarak hiç durmadan yükselen sonsuz bir dalın ucunda beliriyor.

Ağacın en tepesinde tamsayılardan başka “sayılar” da beliriyor. Örneğin, biraz önce sözünü ettiğimiz ağacın en “orta”sındaki (yani hep orta yolu seçen)

$$1 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4 + \dots$$

“sayı”sı. Bu “sayı”ya  $x$  diyelim ve  $x$ 'e modülo 3,  $3^2$ ,  $3^3$ ,  $3^4$  vs bakalım:

$$x \equiv 1 \pmod{3}$$

$$x \equiv 1 + 1 \cdot 3 = 4 \pmod{3^2}$$

$$x \equiv 1 + 1 \cdot 3 + 1 \cdot 3^2 = 13 \pmod{3^3}$$

$$x \equiv 1 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 = 40 \pmod{3^3}$$

...

elde ederiz. Şimdi  $x$ 'i  $2$ 'yle çarpalım:

$$2x \equiv 2 \equiv -1 \pmod{3}$$

$$2x \equiv 8 \equiv -1 \pmod{3^2}$$

$$2x \equiv 26 \equiv -1 \pmod{3^3}$$

$$2x \equiv 80 \equiv -1 \pmod{3^3}$$

...

Çok tuhaf!  $2x \equiv -1$ , yani  $x \equiv -1/2$  gibi bir şey çıkıyor!

Bir önceki sayfadaki şekildeki her sonsuz dal gerçekten de bir tür “sayı” olarak addedilebilir. Bu sayılara  $p$ -sel tamsayılar denir. Birazdan  $p$ -sel tamsayıları daha matematiksel bir biçimde tanımlayacağız.

**II. Baklayı Ağzımızdan Çıkarıyoruz:  $p$ -sel Tamsayılar.** Yukardaki şekildeki her sonsuz yol sonsuz tane durak'tan oluşur. Örneğin,

$$1 \pmod{3}$$

$$1 + 1 \cdot 3 \pmod{3^2}$$

$$1 + 1 \cdot 3 + 1 \cdot 3^2 \pmod{3^3}$$

$$1 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 \pmod{3^4}$$

$$1 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4 \pmod{3^5}$$

...

durakları hep orta dalı seçen sonsuz bir yolun duraklarıdır. Bu durakları,

$$(1 + 1 \cdot 3 + 1 \cdot 3^2 + \dots + 1 \cdot 3^{k-1} \pmod{3^k})_k$$

biçiminde bir dizi olarak ya da

$$1 + 1 \cdot 3 + 1 \cdot 3^2 + \dots + 1 \cdot 3^{k-1} + \dots$$

gibi (sadece simgesel bir değeri olan, yani biçimsel) bir sonsuz “toplam” olarak gösterebiliriz. Bu yazılım sonsuz bir yolu simgeler, hep orta dalı seçen yolu. Kısmi toplamlar da bu yolun duraklarıdır. Her durağın sonuna eklenen  $3^k$  adımı bizi bir sonraki durağa götürür.

Daha genel olarak, 3 asalı yerine herhangi bir  $p$  asalı alalım ve yukarıda 3'le yaptığımızı  $p$ 'yle yapalım. Her adımda  $p$  dala ayrılan sonsuz bir ağaç elde ederiz. Bu sonsuz ağacın her sonsuz yolu, herbiri  $0, 1, \dots, p - 1$ 'e eşit olan

$$a_0, a_1, a_2, \dots, a_k, \dots$$

sonsuz sayı dizisi için,

$$\begin{aligned}
 &a_0 \bmod p \\
 &a_0 + a_1p \bmod p^2 \\
 &a_0 + a_1p + a_2p^2 \bmod p^3 \\
 &\dots \\
 &a_0 + a_1p + a_2p^2 + \dots + a_{k-1}p^{k-1} \bmod p^k \\
 &\dots
 \end{aligned}$$

duraklarından oluşur. Atılan her  $a_k p^k$  adımı bizi bir önceki duraktan bir sonraki durağa götürür ve bu böylecene durmadan devam eder. Buradaki  $a_k$  katsayısı  $k$ -inci adımda önümüze çıkan  $p$  yoldan hangisini seçeceğimizi söyler. Bu sonsuz yolu, yolu oluşturan duraklardan oluşan

$(a_0 + a_1p + a_2p^2 + \dots + a_{k-1}p^{k-1} \bmod p^k)_k$  dizisi olarak kısaca gösterebileceğimiz gibi, sadece simgesel bir anlamı olan

$a_0 + a_1p + a_2p^2 + \dots + a_k p^k + \dots$  gibi “sonsuz bir toplam”la da gösterebiliriz. O zaman, bu sonsuz toplamın kısmi (ve sonlu)

$a_0 + a_1p + a_2p^2 + \dots + a_{k-1}p^{k-1} \bmod p^k$  toplamları sonsuz yolun durakları olur.

Eğer  $x_k$  doğal sayısını

$x_k = a_0 + a_1p + a_2p^2 + \dots + a_k p^k$  olarak tanımlarsak, o zaman, her  $k$  için,

$$x_k \equiv x_{k+1} \pmod{p^{k+1}}$$

denklikleri geçerli olur ve sonsuz yolumuzu kısaca

$$(x_k)_k$$

dizisi olarak da gösterebiliriz. Bu son gösterimde duraklar  $(x_k \bmod p^{k+1})$  modüler sayılarıdır.

Yukardaki  $x_k$ , 0'dan büyüğeşit,  $p^{k+1}$ 'den küçük bir sayıdır. Ama aslında  $x_k$ 'leri,

$$x_k \equiv x_{k+1} \pmod{p^{k+1}}$$

koşullarını sağlayan tamsayılar olarak da seçebiliriz, farketmez. Bir başka deyişle, her  $k$  için yukardaki  $x_k \equiv x_{k+1} \pmod{p^{k+1}}$  denkliklerini sağlayan her  $(x_k)_k$  tamsayı dizisi, bize durakları

$$x_k \bmod 3^{k+1}$$

olan sonsuz bir yol verir. Ayrıca eğer  $(y_k)_k$  tamsayı dizisi

$$y_k \equiv x_k \pmod{p^{k+1}}$$

koşulunu sağlıyorsa, o zaman,  $(y_k)_k$  tamsayı dizisi de sonsuz bir yolu simgeler ve bu sonsuz yol, aynen  $(x_k)_k$  tamsayı dizisiyle simgelenen yola eşittir.

Bir  $p$ -sel tamsayıyı yukardaki değişik biçimlerden biri olarak tanımlayabiliriz. Bu biçimlerden birini seçmeliyiz. Sonuncusunu seçelim.

**Tanım:**  $p$  bir asal sayıysa<sup>1</sup>, bir  $p$ -sel tamsayı,  $x_k \equiv x_{k+1} \pmod{p^{k+1}}$  (\*) denkliklerinin geçerli olduğu  $(x_k \bmod p^{k+1})_k$  dizisidir.

$x = (x_k \bmod p^{k+1})_k$  herhangi bir  $p$ -sel tamsayı olsun.  $x_0$  yerine  $x_0$ 'ı  $p$ 'ye böldüğümüzde çıkan kalan (yani 0'dan büyüğeşit,  $p$ 'den küçük bir sayı) olarak alabiliriz.  $x_1$  yerine de  $x_1$ 'i  $p^2$ 'ye böldüğümüzde kalanı (yani 0'dan büyüğeşit,  $p^2$ 'den küçük bir sayı olarak) alabiliriz. Genel olarak, her  $k$  için,  $x_k$  yerine  $x_k$ 'yi  $p^{k+1}$  sayısına böldüğümüzde çıkan kalan (yani 0'dan büyüğeşit ve  $p^{k+1}$ 'den küçük bir sayı) olarak alabiliriz. Sonuç olarak, yukardaki tanımdaki her  $x_k$  tamsayısını (\*) denkleğini sağlayan 0'dan büyüğeşit,  $p^{k+1}$ 'den küçük bir sayı olarak alabiliriz,  $p$ -sel tamsayıda bir değişiklik olmaz.

(\*)'dan dolayı, her  $k$  için,

$$x_{k+1} = x_k + a_{k+1}p^{k+1}$$

eşitliğini sağlayan bir  $a_{k+1}$  vardır. Eğer bir önceki paragraftaki gibi her  $x_k$ 'yi 0'dan büyüğeşit ve  $p^{k+1}$ 'den küçük bir sayı olarak alırsak, o zaman  $a_{k+1}$ 'i 0'dan büyüğeşit ve  $p$ 'den küçük bir sayı olarak alabiliriz. Bu taktirde,  $x_0$ 'a  $a_0$  dersek,  $0 \leq a_i < p$  eşitsizliklerini sağlayan  $a_i$  tamsayıları için,

$$x_0 = a_0$$

$$x_1 = x_0 + a_1p = a_0 + a_1p$$

$$x_2 = x_1 + a_2p^2 = a_0 + a_1p + a_2p^2$$

$$x_3 = x_2 + a_3p^3 = a_0 + a_1p + a_2p^2 + a_3p^3$$

...

$$x_k = x_{k-1} + a_k p^k = a_0 + a_1p + a_2p^2 + \dots + a_k p^k$$

...

eşitliklerini buluruz, ta en baştaki duraklarımız... Dolayısıyla, bir  $p$ -sel tamsayıyı,  $0 \leq a_i < p$  eşitsizliklerini sağlayan  $a_i$  tamsayıları için, simgesel olarak,

$$a_0 + a_1p + a_2p^2 + \dots + a_k p^k + \dots$$

gibi sonsuz bir toplam olarak da tanımlayabiliriz. Bu sonsuz toplam,

$$(a_0 + a_1p + a_2p^2 + \dots + a_k p^k \bmod p^{k+1})_k$$

$p$ -sel tamsayısı anlamına gelir.

Hatta dileysek, bir  $p$ -sel tamsayıyı,  $0 \leq a_i < p$  eşitsizliklerini sağlayan  $a_i$  tamsayıları için,  $(a_i)_i$  dizisi olarak da tanımlayabilirdik, ama yapmayacağız.

$p$ -sel tamsayıları yukarda verdiğimiz çeşitli tanımlarıyla görebilmek çok yararlıdır, tanımlardan biri diğerinden daha değerli değildir, hepsini gerektiğinde kullanabilmek gerekir.

1 Tanımda  $p$ 'nin asal olması için matematiksel bir neden yoktur aslında. Ama  $p$  asalken  $p$ -sel tamsayıların analizi daha kolay olduğundan,  $p$  hep asal alınır.

Ayrıca, (\*) denklemlerinden, her  $m \leq n$  doğal sayıları için, ilk bakışta (\*)'dan daha genel görünen ama ona eşdeğer olan,

$$x_n \equiv x_m \pmod{p^{m+1}} \quad (**)$$

denkliği çıkar.

**III.  $p$ -sel Sayılarda İşlemler.** Şimdi  $p$ -sel tamsayıları toplayıp çıkarıp çarpacağız.

$$x = (x_k \bmod p^{k+1})_k$$

ve

$$y = (y_k \bmod p^{k+1})_k$$

iki  $p$ -sel tamsayı olsun. Demek ki (\*) ya da (\*\*) denklemleri  $x$  ve  $y$ 'nin terimleri için sağlanıyor. Bu iki  $p$ -sel tamsayıyı,

$$x \pm y = (x_k \pm y_k \bmod p^{k+1})_k$$

ve

$$xy = (x_k y_k \bmod p^{k+1})_k$$

olarak toplayıp çıkarıp çarpmayı öneriyoruz. Bu önerimizin bir anlamı olması için aşağıdaki önsavın birinci kısmının doğru olması gerekmektedir, yoksa bu işlemleri önerdiğimiz gibi tanımlayamayız. Aşağıdaki önsavın ikinci kısmıysa, iki  $p$ -sel tamsayının toplamının, farkının ve çarpımının gene birer  $p$ -sel tamsayı olduğunu söylüyor, ki yukarıda önerilen işlemin gerçekten bir işlem olabilmesi için bunun da doğru olması gerekir elbette.

**Önsav 1.**

$$x = (x_k \bmod p^{k+1})_k$$

$$x' = (x'_k \bmod p^{k+1})_k$$

$$y = (y_k \bmod p^{k+1})_k$$

$$y' = (y'_k \bmod p^{k+1})_k$$

dört  $p$ -sel tamsayı olsun. Eğer  $x = x'$  ve  $y = y'$  ise, o zaman,

$$(x_k \pm y_k \bmod p^{k+1})_k = (x'_k \pm y'_k \bmod p^{k+1})_k$$

ve

$$(x_k y_k \bmod p^{k+1})_k = (x'_k y'_k \bmod p^{k+1})_k$$

dir. Ayrıca

$$(x_k \pm y_k \bmod p^{k+1})_k$$

ve

$$(x_k y_k \bmod p^{k+1})_k$$

birer  $p$ -sel tamsayıdır, yani tanımdaki (\*) koşulunu sağlarlar.

**Kanıt:** Önce birinci kısmı kanıtlayalım. Durakların eşit olduklarını, yani

$$x_k \pm y_k \equiv x'_k \pm y'_k \pmod{p^{k+1}}$$

ve

$$x_k y_k \equiv x'_k y'_k \pmod{p^{k+1}}$$

denkliklerini kanıtlamalıyız. Birincileri okura bira-

kıp sonuncusunu kanıtlayalım.  $x = x'$  ve  $y = y'$  eşitliklerinden dolayı,

$$x_k \equiv x'_k \pmod{p^{k+1}} \text{ ve } y_k \equiv y'_k \pmod{p^{k+1}}$$

denkliklerini biliyoruz; yani

$$x_k - x'_k \equiv y_k - y'_k \equiv 0 \pmod{p^{k+1}}.$$

Şimdi bu denklemleri kullanarak hesaplayalım:

$$x_k y_k - x'_k y'_k = x_k (y_k - y'_k) + (x_k - x'_k) y'_k \equiv 0 \pmod{p^{k+1}}.$$

Önsavımızın ikinci kısmını kanıtlayalım.  $p$ -sel tamsayı tanımına göre,  $(x_k \pm y_k \bmod p^{k+1})_k$  ve  $(x_k y_k \bmod p^{k+1})_k$  dizilerinin  $p$ -sel tamsayı olduklarını kanıtlamak için,

$$x_k \pm y_k \equiv x_{k+1} \pm y_{k+1} \pmod{p^{k+1}}$$

ve

$$x_k y_k \equiv x_{k+1} y_{k+1} \pmod{p^{k+1}}$$

denkliklerini kanıtlamalıyız.  $x$  ve  $y$  birer  $p$ -sel tamsayı olduklarından,

$$x_k \equiv x_{k+1} \pmod{p^{k+1}}$$

ve

$$y_k \equiv y_{k+1} \pmod{p^{k+1}}$$

denklikleri geçerlidir, yani

$$x_k - x_{k+1} \equiv y_k - y_{k+1} \equiv 0 \pmod{p^{k+1}}.$$

Gene ilk denklemleri okura bırakıp üçüncüsünü kanıtlayalım:

$$\begin{aligned} x_k y_k - x_{k+1} y_{k+1} &= x_k (y_k - y_{k+1}) + (x_k - x_{k+1}) y_{k+1} \\ &\equiv 0 \pmod{p^{k+1}} \end{aligned}$$

Dilediğimizi kanıtladık. □

Yukardaki önsav sayesinde artık  $p$ -sel tamsayılarda toplama, çıkarma ve çarpma işlemlerini tanımlayabiliriz:

$(x_k \bmod p^{k+1})_k \pm (y_k \bmod p^{k+1})_k = (x_k \pm y_k \bmod p^{k+1})_k$  ve

$(x_k \bmod p^{k+1})_k (y_k \bmod p^{k+1})_k = (x_k y_k \bmod p^{k+1})_k$ .

$p$ -sel tamsayılar kümesi  $Z_p$  olarak gösterilir. Biraz önce tanımladığımız toplama, çıkarma ve çarpma işlemleriyle birlikte  $Z_p$  bir halkadır. Bunun kanıtı çok kolaydır, yukardaki tanımlardan ve  $Z/p^k Z$ 'nin bir halka olmasından doğrudan çıkar.

Kolayca görüleceği üzere, bu halkanın 0, yani toplamanın etkisiz elemanı,

$$(0 \bmod p^{k+1})_k$$

dir, yani

$$0 + 0 \cdot p + 0 \cdot p^2 + \dots + 0 \cdot p^k + \dots$$

elemanıdır ve birim elemanı, yani halkanın 1'i, çarpmanın etkisiz elemanı,

$$(1 \bmod p^{k+1})_k$$

yani,

$$1 + 0 \cdot p + 0 \cdot p^2 + \dots + 0 \cdot p^k + \dots$$

dir. (Bu iki elemanın  $Z_p$ 'de oldukları çok bariz, ama gene de bu soruyu sormayı akıl etmek gerekiyor.)

$Z_p$ 'ye  $p$ -sel tamsayılar halkası denir. (Bir de bunların kesirlieleri vardır, bkz. sayfa xx.)

Bu işlemlere birkaç örnek verelim.

**Örnek 1.** Eğer  $p \neq 2$  ise, yani  $p > 2$  ise,

$$\sum_k p^k + \sum_k p^k = \sum_k 2p^k.$$

Bu, çok bariz olmalı. Ama eğer  $p = 2$  ise, durum değişir:

$$(1 + 2 + 4 + \dots) + (1 + 2 + 4 + \dots) = 2 + 4 + 8 + \dots$$

Nitekim,

$$\begin{aligned} 1 + 1 &= 2 && \equiv 0 \pmod{2} \\ (1 + 2) + (1 + 2) &= 6 && \equiv 2 \pmod{4} \\ (1 + 2 + 4) + (1 + 2 + 4) &= 14 && \equiv 2 + 4 \pmod{8} \\ (1 + 2 + 4 + 8) + (1 + 2 + 4 + 8) &\equiv 2 + 4 + 8 \pmod{16} \\ &\dots \\ (1 + 2 + \dots + 2^k) + (1 + 2 + \dots + 2^k) &\equiv (2 + \dots + 2^k) \pmod{2^{k+1}} \\ &\dots \end{aligned}$$

Bir başka açıklama:

$$\begin{array}{r} 1 + 2 + 4 + \dots \\ + 1 + 2 + 4 + \dots \\ \hline 2 + 4 + 8 + \dots \end{array}$$

Görüldüğü gibi eğer  $x = 1 + 2 + 4 + \dots$  ise,  $x + x$ 'e 1 ekleyerek gene  $x$  elde ederiz, yani  $2x + 1 = x$ , yani  $x + 1 = 0$ , yani  $x = -1$  eşitliği doğrudur. Demek ki,  $Z_2$  halkasında, yani 2-sel tamsayılar da,

$$-1 = 1 + 2 + 4 + 8 + \dots,$$

yani,

$$\sum_k 2^k = -1.$$

Yanlış gelse de, hiç olmazsa ilginç bir eşitlik, üstelik doğru da!

**Örnek 2.**  $p = 3$  olsun ve iki rastgele 3-sel tamsayı alalım:

$$x = 1 + 2 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4 + \dots$$

$$y = 2 + 1 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 1 \cdot 3^4 + \dots$$

olsun (sayıların devamını bilmiyoruz, kimbilir hangi kurallarla verilmişler.) Bu iki 3-sel tamsayıyı toplamak için kısmi toplamları bulmak lazım:

$$\begin{aligned} 1 + 2 &= 3 \equiv 0 \pmod{3} \\ (1+2 \cdot 3) + (2+1 \cdot 3) &= 12 \equiv 3 \pmod{3^2} \\ (1+2 \cdot 3+0 \cdot 3^2) + (2+1 \cdot 3+1 \cdot 3^2) &= 21 \pmod{3^3} \\ (1+2 \cdot 3+0 \cdot 3^2+1 \cdot 3^3) + (2+1 \cdot 3+1 \cdot 3^2+0 \cdot 3^3) &= 48 \pmod{3^4} \\ (1+2 \cdot 3+0 \cdot 3^2+1 \cdot 3^3+2 \cdot 3^4) + (2+1 \cdot 3+1 \cdot 3^2+0 \cdot 3^3+1 \cdot 3^4) &= 291 \equiv 48 \pmod{3^5} \\ &\dots \end{aligned}$$

Demek ki bu iki 3-sel tamsayının toplamı,

$$0 + 1 \cdot 3 + 2 \cdot 3^2 + 1 \cdot 3^3 + 0 \cdot 3^4 + \dots$$

diye başlıyor. Peki ya çarpımları? Aynen toplama da yaptığımız gibi kısmi toplamları çarpabiliriz:

$$\begin{aligned} 1 \times 2 &= 2 \pmod{3} \\ (1+2 \cdot 3) \times (2+1 \cdot 3) &= 35 \equiv 8 \pmod{3^2} \\ (1+2 \cdot 3+0 \cdot 3^2) \times (2+1 \cdot 3+1 \cdot 3^2) &= 98 \equiv 17 \pmod{3^3} \\ (1+2 \cdot 3+0 \cdot 3^2+1 \cdot 3^3) \times (2+1 \cdot 3+1 \cdot 3^2+0 \cdot 3^3) &= 376 \equiv 71 \pmod{3^4} \\ (1+2 \cdot 3+0 \cdot 3^2+1 \cdot 3^3+2 \cdot 3^4) \times (2+1 \cdot 3+1 \cdot 3^2+0 \cdot 3^3+1 \cdot 3^4) &= 3230 \equiv 71 \pmod{3^5} \\ &\dots \end{aligned}$$

Demek ki bu iki 3-sel tamsayının çarpımı,

$$2 + 2 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 + 0 \cdot 3^4 + \dots$$

diye başlıyor. Devamını bilmiyoruz, çünkü 3-sel tamsayıların sadece başlangıcı verilmiş.

#### IV. $Z_p$ Halkasının Başat Özellikleri

$Z_p$  halkası  $Z$  halkasını bir anlamda içerir, yani  $Z_p$  halkasının içinde  $Z$  halkasına çok benzeyen ( $Z$  halkasıyla eşyapısal olan) bir halka vardır.

**Önsav 2.** Her  $n \in Z$  için,

$$i(n) = (n \pmod{p^{k+1}})_k$$

olarak tanımlanmış dizi  $Z_p$ 'nin bir elemanıdır. Ayrıca  $i$ ,  $Z$ 'den  $Z_p$ 'ye giden toplamaya, çıkarmaya ve çarpmaya saygı duyan birebir bir fonksiyondur; yani, her  $n, m \in Z$  için,  $Z_p$ 'de,

$$i(n \pm m) = i(n) \pm i(m)$$

$$i(nm) = i(n)i(m)$$

eşitliği sağlanır. Ayrıca<sup>1</sup>, her  $n \in Z$  ve her  $x \in Z_p$  için,  $nx = i(n)x$ .

**Kanıt:** Kanıt çok basit.  $i(n) = i(m)$  ise, her  $k$  için,  $p^k, n - m$ 'yi böler, demek ki  $n = m$ . Bu da  $i$  birebir demektir. Geri kalan kısmın kanıtına nerdeyse ihtiyacı yok.  $\square$

Yukarıdaki önsav,  $Z$  halkasıyla  $i(Z)$  halkasını özdeşleştirerek (daha doğrusu,  $Z$ 'nin  $n$  elemanı ile  $Z_p$ 'nin  $i(n)$  elemanını özdeşleştirerek),  $Z_p$ 'yi,  $Z$  halkasını genişleten bir halka olarak görebileceğimizi söylüyor.

Şimdi  $Z_p$  halkasının bir tamlık bölgesi olduğunu kanıtlayacağız. Ama bunun kanıtı yukarıdakiler kadar kolay değildir. İlgili okur önce kendi başına kanıtlamaya çalışmalıdır.

<sup>1</sup> Burada  $nx, x + \dots + x$  ( $x, n$  defa toplanıyor) anlamına gelir..

**Önsav 3.**  $Z_p$  halkası bir tamlık bölgesidir, yani  $x, y \in Z_p$  için  $xy = 0$  ise, ya  $x = 0$  ya da  $y = 0$ 'dir.

**Kanıt:** Terimleri 0'la  $p-1$  arasında değişen  $(a_k)_k$  ve  $(b_k)_k$  tamsayı dizileri için,

$$x = a_0 + a_1p + a_2p^2 + \dots + a_kp^k + \dots$$

ve

$$y = b_0 + b_1p + b_2p^2 + \dots + b_kp^k + \dots,$$

çarpımı sıfır olan iki  $p$ -sel tamsayı olsun. Bu kez,  $p$ -sel tamsayıların bir başka tanımını kullanıyoruz. Eski tanıma dönmek için,  $x_k$  ve  $y_k$  sayılarını

$$x_k = a_0 + a_1p + a_2p^2 + \dots + a_kp^k$$

ve

$$y_k = b_0 + b_1p + b_2p^2 + \dots + b_kp^k$$

olarak tanımlayıp,  $x = (x_k)_k$  ve  $y = (y_k)_k$  almak gerekir. Ya her  $a_k$ 'nin 0 ya da her  $b_k$ 'nin 0 olduğunu kanıtlayacağız. Her  $k$  için,  $x_k y_k \equiv 0 \pmod{p^{k+1}}$  denkleğini biliyoruz ve kullanacağız.  $a_i$  ve  $b_j$ , 0 olmayan ilk katsayılar olsun. Bir çelişki elde edeceğiz.

$x_{i+j}$  ile  $y_{i+j}$ 'yi modülo  $p^{i+j+1}$  çarpalım:

$$0 \equiv x_{i+j} y_{i+j}$$

$$= (a_0 + a_1p + \dots + a_{i+j}p^{i+j})(b_0 + b_1p + \dots + b_{i+j}p^{i+j})$$

$$= (a_i p^i + \dots + a_{i+j} p^{i+j})(b_j p^j + \dots + b_{i+j} p^{i+j})$$

$$\equiv p^{i+j} a_i b_j \pmod{p^{i+j+1}}.$$

Demek ki,  $0 \equiv p^{i+j} a_i b_j \pmod{p^{i+j+1}}$  ve  $0 \equiv a_i b_j \pmod{p}$ , yani  $p$  asalı  $a_i b_j$  çarpımını bölüyor, dolayısıyla ya  $a_i$ 'yi ya da  $b_j$ 'yi bölüyor, dolayısıyla  $a_i$ 'yle  $b_j$ 'den biri 0 olmak zorunda, bir çelişki.  $\square$

Okur,  $Z_p$  halkasının  $Z/p^k Z$  halkalarını althalka olarak içerdiğini sanmasın, Önsav 4'ten anlaşılacağı üzere içermez, hem de hiç içermez!

**Önsav 4.**  $n \in \mathbb{N}$  ve  $x \in Z_p$  olsun. Eğer  $nx = 0$  ise, o zaman ya  $n = 0$  ya da  $x = 0$ 'dir<sup>2</sup>.

**Kanıt:** Önsav 2 ve 3'ten doğrudan çıkar.  $\square$

**Teorem 5.**  $Z_p$ 'nin tersinir elemanları,  $0 < a_0 < p$  için,  $a_0 + a_1p + a_2p^2 + \dots + a_kp^k + \dots$  olarak yazılan elemanlardır.

**Kanıt:** Önce,  $x = a_0 + a_1p + \dots + a_kp^k + \dots$  elemanının tersinir olduğunu varsayalım. Her zaman olduğu gibi,  $0 \leq a_0 < p$  eşitsizliklerini varsayabiliriz. Demek ki belli bir

$$y = b_0 + b_1p + b_2p^2 + \dots + b_kp^k + \dots$$

elemanı için  $xy = 1$ . Dolayısıyla,

$$a_0 b_0 \equiv 1 \pmod{p}$$

ve  $a_0, 0$ 'a eşit olamaz.

Şimdi  $0 < a_0 < p$  için,

$$x = a_0 + a_1p + a_2p^2 + \dots + a_kp^k + \dots$$

olsun.  $xy = 1$  eşitliğini sağlayan bir  $y \in Z_p$  bulacağız. Bulacağımız  $y$ 'yi,

$$y = b_0 + b_1p + b_2p^2 + \dots + b_kp^k + \dots$$

olarak yazalım ve  $xy = 1$  eşitliğini sağlayacak  $b_k$ 'leri bulalım. Demek ki, her  $k$  için,

$(a_0 + a_1p + \dots + a_kp^k)(b_0 + b_1p + \dots + b_kp^k) \equiv 1 \pmod{p^{k+1}}$  denklemlerini sağlayacak  $b_k$ 'ler bulmamız lazım. Bu denklemleri teker teker yazalım:

$$a_0 b_0 \equiv 1 \pmod{p}$$

$$(a_0 + a_1p)(b_0 + b_1p) \equiv 1 \pmod{p^2}$$

$$(a_0 + a_1p + a_2p^2)(b_0 + b_1p + b_2p^2) \equiv 1 \pmod{p^3}$$

...

Birinci denkleği kullanarak  $b_0$ 'i bulacağız. Sonra ikinci denkleği kullanarak  $b_1$ 'i bulacağız.  $b_0$  ve  $b_1$ 'i bulduktan sonra üçüncü denkleği kullanarak  $b_2$ 'yi bulacağız. Böyle gide gide bütün  $b_k$ 'leri bulacağız.

$b_0$ 'i bulmak kolay:  $a_0 \neq 0$  ve  $p$  bir asal olduğundan,  $a_0$  ve  $p$  birbirine asaldır, dolayısıyla  $a_0$  modülo  $p$  tersinirdir. Bu sayede  $a_0 b_0 \equiv 1 \pmod{p}$  denkleğinden,  $b_0 \equiv a_0^{-1} \pmod{p}$  elde edilir.

Şimdi  $k \geq 0$  için  $b_0, b_1, \dots, b_k$ 'yi bulduğumuzu varsayıp (tümevarım varsayımı),  $b_{k+1}$ 'i bulalım.

$$x_k = a_0 + a_1p + a_2p^2 + \dots + a_kp^k$$

$$y_k = b_0 + b_1p + b_2p^2 + \dots + b_kp^k$$

olsun. Tümevarım varsayımına göre,

$$x_k y_k \equiv 1 \pmod{p^{k+1}}$$

denkleği, dolayısıyla belli bir  $z_k$  tamsayısı için,

$$x_k y_k = 1 + z_k p^{k+1}$$

eşitliği geçerlidir. Şimdi,

$$(x_k + a_{k+1}p^{k+1})(y_k + b_{k+1}p^{k+1}) \equiv 1 \pmod{p^{k+2}}$$

eşitliğini sağlayan bir  $b_{k+1}$  sayısı bulacağız. Soldaki terimi modülo  $p^{k+2}$  hesaplayalım:

$$(x_k + a_{k+1}p^{k+1})(y_k + b_{k+1}p^{k+1})$$

$$\equiv x_k y_k + (a_{k+1}y_k + b_{k+1}x_k)p^{k+1}$$

$$\equiv 1 + z_k p^{k+1} + (a_{k+1}y_k + b_{k+1}x_k)p^{k+1} \pmod{p^{k+2}}$$

Demek ki,

$$z_k + (a_{k+1}y_k + b_{k+1}x_k) \equiv 0 \pmod{p}$$

denkleği sağlanmalı. Ama  $x_k \equiv a_0 \pmod{p}$  olduğundan, bu denklik yerine,

$$z_k + (a_{k+1}y_k + b_{k+1}a_0) \equiv 0 \pmod{p}$$

denkleğini yazmaya hakkımız var.  $a_0$  tersinir olduğundan, yukardaki denkleği sağlayan bir  $b_{k+1}$  bulmak mümkündür:  $b_{k+1}$ 'i,

$$b_{k+1} \equiv -(z_k + a_{k+1}y_k)a_0^{-1} \pmod{p}$$

denkleğini sağlayan bir tamsayı olarak seçmek yeterli. Böylece teoremimiz kanıtlanmıştır.  $\blacklozenge$

2 Burada  $nx, x + \dots + x$  ( $x, n$  defa toplanıyor) anlamına gelir. Ama istersek,  $Z_p$ 'deki çarpmayı ve Önsav 2'yi kullanarak  $i(n)x$  anlamında da alabiliriz.