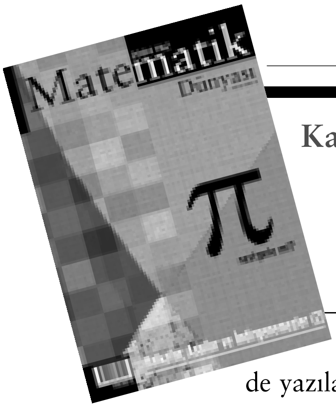

Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (2)

p-sel Sayıları Hissetmek

Geçen yazıda, $n\mathbb{Z} + r$ biçiminde yazılan sonlu sayıda kümenin kesişimi üzerine yoğunlaşmıştık. Bu kesişimlerin ya boşküme ya da gene $n\mathbb{Z} + r$ biçiminde yazılan kümeler olduklarını görmüştük. Bu yazıda, $n\mathbb{Z} + r$ biçiminde yazılan sonsuz sayıda kümenin kesişimi üzerinde duracağız. Tav soruyla başlayalım:

Soru. *Öyle $(n_i)_i$ ve $(r_i)_i$ tamsayı dizileri var mıdır ki,*
$$\bigcap_i (n_i\mathbb{Z} + r_i) = \emptyset$$
olsun, ama bu $n_i\mathbb{Z} + r_i$ kümelerinin sonlu kesişimleri hiçbir zaman boşküme olmasın?

Yani,

$$n_1\mathbb{Z} + r_1$$
$$(n_1\mathbb{Z} + r_1) \cap (n_2\mathbb{Z} + r_2)$$
$$(n_1\mathbb{Z} + r_1) \cap (n_2\mathbb{Z} + r_2) \cap (n_3\mathbb{Z} + r_3)$$
$$....$$

sonlu kesişimlerinin hiçbiri boşküme olmayacak ama, hepsini birden kesiştirdiğimizde boşküme elde edeceğiz... Evet, bu koşulları sağlayan $(n_i\mathbb{Z} + r_i)_i$ sayı kümeleri dizisi vardır. Örnekler aşağıda:

Örnek 1. [Doğan Bilge]

$1 \in 2\mathbb{Z} + 1$,
$3 \in (2\mathbb{Z} + 1) \cap 3\mathbb{Z}$,
$15 \in (2\mathbb{Z} + 1) \cap 3\mathbb{Z} \cap 5\mathbb{Z}$,
$105 \in (2\mathbb{Z} + 1) \cap 3\mathbb{Z} \cap 5\mathbb{Z} \cap 7\mathbb{Z}$,
$1155 \in (2\mathbb{Z} + 1) \cap 3\mathbb{Z} \cap 5\mathbb{Z} \cap 7\mathbb{Z} \cap 11\mathbb{Z}$,
...

Yani tek sayılar kümesine ve 3, 5, 7, 11, 13 gibi tek asalların çarpımlarından oluşan kümelere bakıyoruz... Bunların sonlu tanesinin kesişimi boş değildir ama hepsinin kesişimi boştur, çünkü her tek asala bölünen sadece 0 vardır ve 0 tek sayı değildir.

Örnek 2. [Özlem Beyarslan] $p = 3, 5, 7, 11, 13, 17, 19,...$ tek asalları için, $p\mathbb{Z} + (p - 1)/2$ kümelerine bakalım:

$3\mathbb{Z} + 1$,
$(3\mathbb{Z} + 1) \cap (5\mathbb{Z} + 2)$,
$(3\mathbb{Z} + 1) \cap (5\mathbb{Z} + 2) \cap (7\mathbb{Z} + 3)$,
$(3\mathbb{Z} + 1) \cap (5\mathbb{Z} + 2) \cap (7\mathbb{Z} + 3) \cap (11\mathbb{Z} + 5)$,
...

Çin Kalanlar Teoremi'ne göre [sayfa 15, Sonuç 5] yukardaki sonlu kesişimler boş değildir. Ama hepsinin kesişimi boştur; bunu kanıtlayalım. Hepsinin kesişiminden (eğer varsa) bir x alalım. Demek ki, her tek p asalı için, $x \in p\mathbb{Z} + (p - 1)/2$, yani
$$x = py_p + (p - 1)/2$$
eşitliğini sağlayan bir y_p tamsayısı var. Bundan,
$$2x + 1 = p(2y_p + 1)$$
çıkar, yani 2 dışında her p asalı $2x + 1$'i böler. Demek ki $2x + 1 = 0$ ve $x = -1/2$, çelişki.

Aslında bu örnek ve kanıtı son derece ilginç. Kanıt bize, $\bigcap_{p \text{ tek asal}} (p\mathbb{Z} + (p - 1)/2)$ kümesinde olsa olsa $-1/2$ olacağını söylüyor. $-1/2$ de $\mathbb{Z}$'de olmadığından kesişimin boş olduğuna hükmediyoruz!

Örnek 3. [Özer Çözer] p herhangi bir asal sayı olsun.

$$p\mathbb{Z} + 1$$
$$p^2\mathbb{Z} + 1 + p$$
$$p^3\mathbb{Z} + 1 + p + p^2$$
$$p^4\mathbb{Z} + 1 + p + p^2 + p^3$$
$$...$$

kümelerinin kesişimine bakalım. Bunlar gittikçe küçülen kümeler ve sonlu kesişimleri, kesişimi alınan kümelerin en küçüğüne eşit, dolayısıyla boş değil.

Bu kümelerin sonsuz kesişimleri ne olabilir? İlk bakışta kesişimde olsa olsa
$$1 + p + p^2 + p^3 + p^4 + ...$$
gibi bir "sayı" olabileceği, $\mathbb{Z}$'de de böyle bir "sayı" olamayacağından bu kesişimin boş olacağı düşünülebilir. Ama bu, göreceğimiz üzere, biraz doğrudur, çok doğru değildir.

Kesişimden bir sayı alalım. Bu sayıya x diyelim. Demek ki, her $n \geq 1$ için,
$$x \in p^n\mathbb{Z} + 1 + p + p^2 + ... + p^{n-1}$$
ve
$$x = p^ny_n + (1 + p + p^2 + ... + p^{n-1})$$
eşitliğini sağlayan bir y_n tamsayısı vardır. Her iki tarafı da $1 - p$ ile çarparsak,

$$(1 - p)x = (1 - p)p^n y_n + 1 - p^n$$

buluruz, yani

$$(1 - p)x - 1 = p^n[(1 - p)y_n - 1].$$

Demek ki, $(1 - p)x - 1$ sayısı her n doğal sayısı için p^n'ye bölünüyor, yani $(1 - p)x - 1 = 0$ ve

$$x = 1/(1 - p).$$

Eğer $p \neq 2$ ise bu sayı bir tamsayı olamayacağından kesişim boşkümedir.

Gerçekten ne kanıtladığımıza bakalım. Şunu kanıtladık: Eğer, x tamsayısı her n için,

$$p^n\mathsf{Z} + 1 + p + p^2 + ... + p^{n-1}$$

kümesindeyse, o zaman

$$(1 - p)x = 1$$

dir ve

$$x = 1/(1 - p).$$

Demek kesişimde en fazla bir eleman olabilir ve bu eleman da olsa olsa $1/(1 - p)$ olabilir... Eğer $p \neq 2$ ise bu sayı bir tamsayı olamaz. Yani $p \neq 2$ ise,

$$\bigcap_n (p^n\mathsf{Z} + 1 + p + p^2 + ... + p^{n-1}) = \varnothing.$$

Peki $p = 2$ ise ne oluyor? O zaman, -1 gerçekten tümünün kesişiminde oluyor. Nitekim, her n pozitif doğal sayısı için, kolayca görüleceği üzere,

$$-1 \equiv 1 + 2 + 2^2 + ... + 2^{n-1} \bmod 2^n.$$

Örnek 4 [Oya Oynar] p gene bir asal olsun.

$$p^n\mathsf{Z} + (p-1) + (p-1)p + (p-1)p^2 + ... + (p-1)p^{n-1}$$

kümelerini kesiştirelim. Bu kesişimden bir x alalım. Bakalım x neye eşit olmak zorunda kalacak.

$$(p-1) + (p-1)p + (p-1)p^2 + ... + (p-1)p^{n-1}$$
$$= (p - 1)(1 + p + p^2 + ... + p^{n-1}) = p^n - 1$$

olduğundan, elemanımız aslında,

$$p^n\mathsf{Z} + p^n - 1,$$

yani $p^n\mathsf{Z} - 1$ kümelerindedir. Bunların kesişimi de elbette -1'dir.

Demek ki Oya Oynar'ın örneğinde kesişimler boşküme değil, -1'i içeriyorlar.

Sorumuzu üç örnekle yanıtladık ama soruyu yanıtlarken ilginç matematik içeren bazı sonuçlara ulaştık. Sözgelimi, Özer Çözer'in örneğine bakalım:

$$p\mathsf{Z} + 1$$
$$p^2\mathsf{Z} + 1 + p$$
$$p^3\mathsf{Z} + 1 + p + p^2$$
$$p^4\mathsf{Z} + 1 + p + p^2 + p^3$$
$$...$$

Sanki,

$$1 + p + p^2 + ... + p^{n-1} + ...$$

gibi bir "sayı" bu kümelerin kesişimindeymiş gibi bir his var içimizde... Oysa kesişimde olabilecek tek eleman $1/(1 -p)$... Yoksa

$$1 + p + p^2 + ... + p^{n-1} + ... = \frac{1}{1-p}$$

gibi bir eşitlik mi sözkonusu? Bilindiği gibi eğer $-1 < p < 1$ ise, bu eşitliğin bir anlamı ve bir tanımı vardır. Ama burada p bir asal sayı ve en az 2... Sol taraf sonsuz...

Baştan Başlayalım

Sanki sorumuzun yanıtını bilmiyormuş gibi davranıp düşünmeye en baştan başlayalım. Hatta soruyu umursamayalım bile... Sonlu kesişimleri durmadan küçülen (dolayısıyla sonlu kesişimlerin hiçbir zaman boşküme olmayan) $(n_i\mathsf{Z} + r_i)_i$ sayı kümeleri alalım. Hepsinin kesişimi boş olsun ya da olmasın, bunu şimdilik hiç umursamayalım. Kesişimde bir şeyin olup olmadığını değil, kesişimde ne olabileceğini bulmak istiyoruz! Yalnız,

$$n_1\mathsf{Z} + r_1$$
$$(n_1\mathsf{Z} + r_1) \cap (n_2\mathsf{Z} + r_2)$$
$$(n_1\mathsf{Z} + r_1) \cap (n_2\mathsf{Z} + r_2) \cap (n_3\mathsf{Z} + r_3)$$
$$...$$

sonlu kesişimlerinin hiç sabit kalmadan durmadan küçüldüklerini aklımızda tutalım. (Dolayısıyla $n_i \neq 0$.) Amacımız,

$$\bigcap_{i=1}^{\infty} (n_i\mathsf{Z} + r_i)$$

kesişiminde ne olabileceğini kestirmek.

$(n_i\mathsf{Z} + r_i)_i$ dizisinin en başına Z koyarak $n_0 = 1$ ve $r_0 = 0$ eşitliklerini varsayabiliriz (sonlu ve sonsuz kesişimler değişmez o zaman.) Bu varsayım bize yazılımda kolaylık sağlayacak.

Sayfa 14, Teorem 2'ye göre, boş olmayan

$$(n_0\mathsf{Z} + r_0) \cap ... \cap (n_i\mathsf{Z} + r_i)$$

kesişimi, m_i ve s_i tamsayıları için, $m_i\mathsf{Z} + s_i$ biçiminde yazılan bir kümeye eşittir:

$$(n_0\mathsf{Z} + r_0) \cap ... \cap (n_i\mathsf{Z} + r_i) = m_i\mathsf{Z} + s_i.$$

Hatta aynı teoreme göre,

$$m_i = \text{ekok}(n_0, n_1, ..., n_i)$$

olmalı. Böylece gittikçe küçülen, yani,

$$m_0\mathsf{Z} + s_0 \supset m_1\mathsf{Z} + s_1 \supset ... \supset m_i\mathsf{Z} + s_i \supset ...$$

ilişkilerini sağlayan bir $(m_i\mathsf{Z} + s_i)_i$ dizisi elde ederiz. Ayrıca, $n_i\mathsf{Z} + r_i$ kümelerinin hepsinin kesişimi $m_i\mathsf{Z} + s_i$ kümelerinin hepsinin kesişimine eşittir:

$$\bigcap_{i=0}^{\infty} (n_i\mathsf{Z} + r_i) = \bigcap_{i=0}^{\infty} (m_i\mathsf{Z} + s_i).$$

Yazılımda kolaylık sağlayacak olan $m_0 = n_0 = 1$ ve $s_0 = 0$ eşitliklerini de unutmayalım, yeri gelecek.

Demek ki, sonlu kesişimlerinin durmadan küçülen $(n_i\mathbb{Z} + r_i)_i$ kümeleri yerine, hiç sabit kalmadan durmadan küçülen $(m_i\mathbb{Z} + s_i)_i$ dizilerine bakmak yeterli.

Belli ki $m_i\mathbb{Z} + s_i \supset m_{i+1}\mathbb{Z} + s_{i+1}$ ilişkisini irdelemeliyiz. Bu ilişki, m_i, s_i, m_{i+1} ve s_{i+1} sayıları açısından ne demektir? Bu sayılar arasında nasıl bir ilişki olmalı ki, $m_i\mathbb{Z} + s_i \supset m_{i+1}\mathbb{Z} + s_{i+1}$ ilişkisi sağlansın?

Önsav. *$a\mathbb{Z} + u \supseteq b\mathbb{Z} + v$ ilişkisi için gerek ve yeter koşul a'nın b'yi ve $v - u$'yu bölmesidir. $a\mathbb{Z} + u \supset b\mathbb{Z} + v$ ilişkisi için, ayrıca $a \neq b$, yani $b > a$ olmalıdır.*

Kanıt: Önce $a\mathbb{Z} + u \supseteq b\mathbb{Z} + v$ ilişkisini varsayalım. Elbette $v \in a\mathbb{Z} + u$ olmalı, yani $v - u \in a\mathbb{Z}$, yani a, $v - u$ sayısını bölmeli, bir başka deyişle,

$$a\mathbb{Z} + u = a\mathbb{Z} + (u - v) + v = a\mathbb{Z} + v$$

eşitliği geçerli olmalı. Demek ki,

$$a\mathbb{Z} + v = a\mathbb{Z} + u \supseteq b\mathbb{Z} + v.$$

Bundan $a\mathbb{Z} \supseteq b\mathbb{Z}$ çıkar, yani a, b'yi bölmeli.

Şimdi, a'nın b'yi ve $v - u$'yu böldüğünü varsayalım. O zaman,

$$b\mathbb{Z} + v \subseteq a\mathbb{Z} + v = a\mathbb{Z} + (v - u) + u = a\mathbb{Z} + u.$$

En sondaki "ayrıca" kısmı kolay. □

Kaldığımız yerden düşünmeye devam edelim. Demek ki m_0, m_1'i, m_1, m_2'yi, m_2, m_3'ü bölüyor. Dolayısıyla, belli $p_1, p_2, p_3, \ldots$ tamsayıları için,

$$m_1 = m_0p_1$$
$$m_2 = m_1p_2$$
$$m_3 = m_2p_3$$
$$\ldots$$

Yani,

$$m_1 = m_0p_1$$
$$m_2 = m_0p_1p_2$$
$$m_3 = m_0p_1p_2p_3$$
$$\ldots$$

Ayrıca $m_i\mathbb{Z} + s_i$ kümeleri küçüldüğünden, her $p_i > 1$ olmalıdır.

Buraya kadar her şey yolunda, önsav sayesinde m_i'ler hakkında elde edilebilecek tüm bilgileri elde ettik. Bundan böyle yukardaki eşitlikleri varsayabiliriz. Hatta m_i'leri unutup sadece m_0 sayısını ve $(p_i)_i$ dizisini aklımızda tutabiliriz.

Bakalım aynı önsav, s_i'ler hakkında bize ne bilgi veriyor. Önsava göre,

m_0, $s_1 - s_0$'ı bölmeli,
m_1, $s_2 - s_1$'i bölmeli,
m_2, $s_3 - s_2$'yi bölmeli,
m_3, $s_4 - s_3$'ü bölmeli,
...

Bu bilgiler ışığında, bu ilişkiler şu hale döner:

m_0, $s_1 - s_0$'ı bölmeli,
m_0p_1, $s_2 - s_1$'i bölmeli,
$m_0p_1p_2$, $s_3 - s_2$'yi bölmeli,
$m_0p_1p_2p_3$, $s_4 - s_3$'ü bölmeli,
...

Demek ki, belli $t_0, t_1, t_2, \ldots$ sayıları için,

$$s_1 - s_0 = m_0t_0,$$
$$s_2 - s_1 = m_0p_1t_1,$$
$$s_3 - s_2 = m_0p_1p_2t_2,$$
$$s_4 - s_3 = m_0p_1p_2p_3t_3,$$
$$\ldots$$

Yani, şimdiye dek kullanmadığımız $m_0 = 1$ ve $s_0 = 0$ eşitliklerini de kullanarak,

$$s_1 = t_0,$$
$$s_2 = s_1 + p_1t_1,$$
$$s_3 = s_2 + p_1p_2t_2,$$
$$s_4 = s_3 + p_1p_2p_3t_3,$$
$$\ldots$$

elde ederiz. Yani

$$s_1 = t_0,$$
$$s_2 = t_0 + p_1t_1,$$
$$s_3 = t_0 + p_1t_1 + p_1p_2t_2,$$
$$s_4 = t_0 + p_1t_1 + p_1p_2t_2 + p_1p_2p_3t_3,$$
$$\ldots$$

Galiba her şeyi bulduk:

Teorem. *$(m_i)_i$ ve $(s_i)_i$ sayı dizilerinin,*

$$\mathbb{Z} \supset m_1\mathbb{Z} + s_1 \supset \ldots \supset m_i\mathbb{Z} + s_i \supset \ldots$$

ilişkisini sağlaması için yeter ve gerek koşul,

$$m_i = p_1p_2 \ldots p_i$$

ve

$$s_i = t_0 + t_1p_1 + \ldots + t_{i-1}p_1p_2 \ldots p_{i-1}$$

eşitliklerini sağlayan $(p_i > 1)_i$ ve $(t_i)_i$ tamsayı dizilerinin olmasıdır. Ayrıca,

$$s_i = t_0 + t_1m_1 + \ldots + t_{i-1}m_{i-1}$$

ve $s_{i+1} = s_i + t_im_i$. Dahası, $m_i\mathbb{Z} + s_i$ kümelerinin kesişiminde en çok bir sayı olabilir.

Kanıt: "Ayrıca" kısmı çok kolay, ilk kısımdan çıkıyor. İlk kısmı kanıtlayalım. Gerekliği gördük. Yeterlik üzerinde duralım. Her i için,

$$m_i = p_1p_2 \ldots p_i,$$

$p_i > 1$ ve

$$s_i = t_0 + t_1p_1 + \ldots + t_{i-1}p_1p_2 \ldots p_{i-1}$$

ilişkilerini sağlayan $(p_i)_i$ ve $(t_i)_i$ sayı dizilerinin olduğunu varsayıp

$$m_i\mathbb{Z} + s_i \supset m_{i+1}\mathbb{Z} + s_{i+1}$$

ilişkisini kanıtlayalım. Önsav'a göre m_i'nin m_{i+1}'i ve $s_{i+1} - s_i$'yi böldüğünü ve $m_i \neq m_{i+1}$ eşitsizliğini kanıtlamak gerekiyor. m_i'nin m_{i+1}'i böldüğü ve $m_i \neq$

m_{i+1} eşitsizliği besbelli. m_i'nin $s_{i+1} - s_i$'yi böldüğünü kanıtlamak kalıyor. Hesaplayalım:

$$s_{i+1} = t_0 + t_1p_1 + ... + t_ip_1p_2...p_i$$
$$= s_i + t_ip_1p_2...p_i = s_i + m_it_ip_i,$$

dolayısıyla $s_{i+1} - s_i = m_it_ip_i$ ve $s_{i+1} - s_i$, m_i'ye bölünüyor.

En sondaki "dahası" kısmını kanıtlayalım. x ve y sonsuz kesişimde olsunlar. O zaman $x - s_i$ ve $y - s_i$ sayıları m_i'ye bölünürler, demek ki farkları olan $x - y$ de m_i'ye bölünür. m_i'ler de gittikçe arttığından, bundan $x = y$ çıkar. □

Teoremden, $m_i\mathbb{Z} + s_i$ kümelerinin kesişimindeki tek sayının olsa olsa,

$$s_\infty = \sum_{i=0}^{\infty} t_im_i = \sum_{i=0}^{\infty} t_i p_0p_1p_2...p_i$$

(burada $m_0 = p_0 = 1$) gibi bir "sayı"nın olabileceği anlaşılır. Bu s_∞ terimlerini sonsuz kesişimde olması gereken, hatta belki de gerçekten olan "ideal sayı"lar olarak görebiliriz.

Yukardaki teoremi hemen uygulayalım. p_i'lerin hepsini aynı sayı, örneğin bir asal seçelim, diyelim $p_i = p$. O zaman, teoreme göre,

$$m_i = p^i$$

ve

$$s_i = t_0 + t_1p + t_2p^2 + ... + t_{i-1}p^{i-1}$$

buluruz. i'yi sonsuza götürürsek, kesişimdeki "ideal sayı"

$$s_\infty = \sum_{i=0}^{\infty} t_ip^i$$

olur. Eğer her t_i'yi 1 olarak alırsak, Özer Çözer'in "sayı"sını buluruz. Eğer her t_i'yi $p - 1$ olarak alırsak, Oya Oynar'ın "ideal sayı"sını, yani bir anlamda -1'i buluruz.

Özlem Beyarslan'ın örneğindeki "ideal sayı"yı bulmak kolay değil. Ta en baştan hesaplamaya çalışalım.

$3\mathbb{Z} + 1$,
$(3\mathbb{Z} + 1) \cap (5\mathbb{Z} + 2)$,
$(3\mathbb{Z} + 1) \cap (5\mathbb{Z} + 2) \cap (7\mathbb{Z} + 3)$,
$(3\mathbb{Z} + 1) \cap (5\mathbb{Z} + 2) \cap (7\mathbb{Z} + 3) \cap (11\mathbb{Z} + 5)$

kümeleri sırasıyla

$3\mathbb{Z} + 1$,
$15\mathbb{Z} + 7$,
$105\mathbb{Z} + 52$,
$1155\mathbb{Z} + 577$

kümelerine eşit. m'leri bulmak kolay:

$m_0 = 1$ (her zamanki gibi)
$m_1 = 3$,
$m_2 = 3 \times 5 = 15$,
$m_3 = 3 \times 5 \times 7 = 105$,
$m_4 = 3 \times 5 \times 7 \times 11 = 1155$,
...

Sorun s'leri bulmakta. İlk birkaç s'yi bulduk:

$s_1 = 1$,
$s_2 = 7$,
$s_3 = 52$,
$s_4 = 577$,
$s_5 = 7507$,
$s_6 = 127627$.

Genel bir yöntem görmediğimizden, geri kalanları hesaplamanın bir anlamı olmadığını düşündük.

Teoremdeki $s_{i+1} = s_i + t_im_i$ eşitliğinden, ilk birkaç t_i'yi de bulabiliriz:

$t_0 = 1$,
$t_1 = 2$,
$t_2 = 3$,
$t_3 = 5$,
$t_4 = 6$,
$t_5 = 8$.

Demek ki Özlem Beyarslan "ideal sayı"sı,

$$1 + 2\times3 + 3\times3\times5 + 5\times3\times5\times7 + 6\times3\times5\times7\times11 + 8\times3\times5\times7\times11\times13 + ...$$

diye başlıyor ve anlayamadığımız bir biçimde devam ediyor. Bu "sayı"nın t'lerini bulan herhalde kocaman bir bravo'yu hakediyordur.

Doğan Bilge "ideal sayı"sını bulmayı okura bırakıyoruz. Biz çok eğlendik, biraz da okur eğlensin!

Özer Çözer ve Oya Oynar sayıları bilinen sayılardır. Bu tür sayılara ***p*-sel sayılar** denir. Fazla değil, biraz daha matematiksel olalım:

$$s_\infty = \sum_{i=0}^{\infty} t_ip^i$$

türünden yazılan yazılan "sayı"lara p-sel sayı denir. Bir sonraki sayımızda p-sel sayıları tüm ihtişamıyla göreceğiz. Şimdilik p-sel sayıları hissetmekle yetinelim.

t_i'leri 0 ya da 1 alarak sayılamaz sonsuzlukta p-sel sayı olduğu görülür. Oysa $\mathbb{Z}$'de sadece sayılır sonsuzlukta sayı vardır. Demek ki gerçek tamsayı olmayan sayılamaz sonsuzlukta "ideal sayı" vardır. Bir başka deyişle yukarda verdiğimiz Doğan Bilge'nin, Özlem Beyarslan'ın ve Özer Çözer'in boş kesişim örnekleri sayılamaz sonsuzluktaki örneklerin sadece üçü. ♥