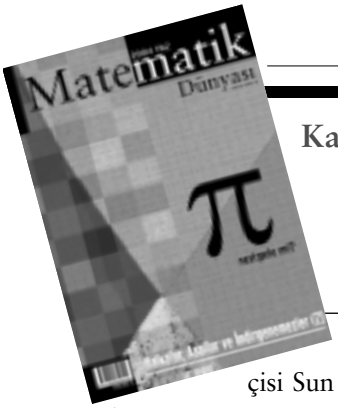

Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (2)

Çin Kalanlar Teoremi

Tarihçe. Çin matematikçisi Sun Zi (yaşadığı kesin tarihler bilinmiyor, 400-460 yılları arasında, belki daha da erken yaşamış olabilir) şu soruyu sorar: Bir sayı 3'e bölündüğünde 2 kalıyor, 5'e bölündüğünde 3 kalıyor, 7'ye bölündüğünde de 2 kalıyor. Sayı kaçtır?

Modern matematik dilinde bu soru,

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 5$$
$$x \equiv 2 \bmod 7$$

denkliklerini çözmeye eşdeğerdir. Bu yazıda bu tür denkliklerin ne zaman bir çözümü olduğunu ve çözüm olduğunda çözümün nasıl bulunduğunu göreceğiz.

$x = 23$, Sun Zi'nin probleminin bir çözümüdür. Ama $x = 128$ de bir çözümdür. Başka çözümler de vardır. Tüm çözümler $23 + 105u$ biçiminde yazılabilir.

İlginçtir, Sun Zi önce $x = 233$ yanıtını bulur, sonra 233'ten çıkarabildiği kadar 105'i ($3 \times 5 \times 7 = 105$) çıkararak 23 yanıtına varır.

İki yüzyıl kadar sonra, Hintli matematikçi Brahmagupta (doğumu 598) şu soruyu sorar: Yaşlı ve yoksul bir kadın pazardan bir sepet yumurta alır. Ama bir at sepeti ezip içindeki yumurtaları kırar. Süvari parasını ödemek için yaşlı kadına sepette kaç yumurta olduğunu sorar. Yaşlı kadın yumurta sayısını anımsamamaktadır ama yumurtaları ikişer ikişer çıkardığında geriye bir yumurta kaldığını anımsar. Aynı şey yumurtaları üçer, dörder, beşer ve altışar çıkardığında da başına gelmiştir, hep bir artmıştır. Ama yedişer yedişer çıkardığında geriye yumurta kalmamıştır. Yaşlı kadının sepetinde kaç yumurta olabilir?

Bu kez,

$$x \equiv 1 \bmod 2$$
$$x \equiv 1 \bmod 3$$
$$x \equiv 1 \bmod 4$$
$$x \equiv 1 \bmod 5$$
$$x \equiv 1 \bmod 6$$
$$x \equiv 0 \bmod 7$$

denkliklerini çözmeliyiz. Bu tür denkliklerin tüm çözümlerini bulacağız. 301, bu sorunun yanıtlarından biridir. Ayrıca 301'e eklenen 420'nin tüm katları bir başka yanıt verir. Göreceğimiz üzere bunlardan başka da yanıt yoktur.

Bir söylentiye göre, Eski Yunanlılar bu tür denklikleri çözmesini Çinlilerden önce biliyorlarmış...

Söylentilere dayanmaya başlayan tarihi kesip, kesin olan matematiğe başlayalım.

Sun Zi'nin Probleminin Çözümü. Sun Zi'nin sorusunu matematiksel olarak çözelim. Önce soruyu anımsatalım:

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 5$$
$$x \equiv 2 \bmod 7$$

denkliklerini çözmek istiyoruz.

Birinci denklikten, bir $t \in \mathbb{Z}$ için,

$$x = 3t + 2$$

buluruz. Bunu ikinci denkliğe yerleştirirsek,

$$3t + 2 \equiv 3 \bmod 5,$$

yani

$$3t \equiv 1 \bmod 5$$

buluruz. Her iki tarafı da 2'yle çarparsak (2, 3'ün modülo 5 tersidir: $2 \times 3 \equiv 1 \bmod 5$),

$$t \equiv 2 \bmod 5$$

buluruz. Demek ki, belli bir $s \in \mathbb{Z}$ için,

$$t = 5s + 2.$$

Bunu yukardaki $x = 3t + 2$ eşitliğine yerleştirirsek,

$$x = 15s + 8$$

buluruz. Bunu da üçüncü denkleme yerleştirelim:

$$15s + 8 \equiv 2 \bmod 7,$$

yani

$$s \equiv 15s \equiv -6 \equiv 1 \bmod 7$$

buluruz. Demek ki, belli bir $u \in \mathbb{Z}$ için,

$$s \equiv 7u + 1.$$

Bunu $x = 15s + 8$'e yerleştirirsek,

$$x \equiv 105u + 23$$

bulunur. En küçük pozitif çözüm $u = 0$ içindir, yani 23'tür. Denklikleri teker teker çözme ilkesine dayanan, ilkel ve oldukça karmaşık bir çözüm...

Sun Zi bu soruyu bizden daha akıllı bir biçimde çözer. Önce,

$a \equiv 1 \bmod 3$, $b \equiv 0 \bmod 3$, $c \equiv 0 \bmod 3$,
$a \equiv 0 \bmod 5$, $b \equiv 1 \bmod 5$, $c \equiv 0 \bmod 5$,
$a \equiv 0 \bmod 7$, $b \equiv 0 \bmod 7$, $c \equiv 1 \bmod 7$

denkliklerini sağlayan a, b ve c sayılarını bulur: $a = 70$, $b = 21$, $c = 15$ bu denklikleri sağlar. Şimdi $x = 2a + 3b + 2c$, yukardaki üç denkliğin üçünü de sağlar. Dikkat edilirse, a, b ve c bulunduktan sonra, sadece yukardaki üç denkliği değil,

$x \equiv 1 \bmod 3$
$x \equiv 4 \bmod 5$
$x \equiv 5 \bmod 7$

gibi herhangi bir denklik sistemini de çözebiliriz: $x = a + 4b + 5c$ bu denklik sisteminin bir çözümüdür. Yazının en sonundaki teoremde Sun Zi'nin bu akıllı çözümünü daha teorik olarak bulacağız.

İkinci sorunun çözümünü okura bırakıp biraz teori yapalım.

Teoriye Başlangıç. Bir önceki yazıda tanımladığımız $n\mathbb{Z}$ kümesinin öğelerine belli bir tamsayı da ekleyebiliriz. Örneğin $13\mathbb{Z}$ kümesine 5'i eklersek,

$$13\mathbb{Z} + 5 = \{13z + 5 : z \in \mathbb{Z}\}$$
$$= \{5, \pm 13 + 5, \pm 26 + 5, \pm 39 + 5, ...\}$$
$$= \{ ..., -34, -21, -8, 5, 18, 31, 44, 57, ... \}$$

kümesini elde ederiz. Bunun gibi, $2\mathbb{Z} + 1$, tek sayılar kümesidir. $5\mathbb{Z} + 2$ kümesi de, 5'e bölündüğünde kalanın 2 olduğu sayılardan oluşur. Bu dile çevrildiklerinde, yukardaki problemler, sırasıyla,

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

ve

$$(2\mathbb{Z}+1) \cap (3\mathbb{Z}+1) \cap (4\mathbb{Z}+1) \cap (5\mathbb{Z}+1) \cap (6\mathbb{Z}+1) \cap 7\mathbb{Z}$$

kesişimlerinin bir elemanını sorar.

Genel olarak, $n\mathbb{Z} + r$ kümesini,

$$n\mathbb{Z} + r = \{nz + r : z \in \mathbb{Z}\}$$

olarak tanımlayalım. Elbette,

$$n\mathbb{Z} + r = \{nz + r : z \in \mathbb{Z}\}$$
$$= \{r, \pm n + r, \pm 2n + r, \pm 3n + r, ...\}$$
$$= \{m \in \mathbb{Z} : n, m - r\text{'yi böler}\}.$$

n'nin katlarına n'yi eklersek ya da n'nin katlarından n'yi çıkarırsak gene n'nin katlarını bulacağımızdan, $n\mathbb{Z} + n = n\mathbb{Z} - n = n\mathbb{Z}$ eşitlikleri geçerlidir. Örneğin,

$5\mathbb{Z} - 2 = 5\mathbb{Z} + 5 - 2 = 5\mathbb{Z} + 3$,
$7\mathbb{Z} + 16 = 7\mathbb{Z} + 14 + 2 = 7\mathbb{Z} + 2$,
$9\mathbb{Z} - 25 = 9\mathbb{Z} + 2$.

Önsav 1. *Aşağıdaki önermelerden biri doğruysa diğerleri de doğrudur*:

i. $n\mathbb{Z} + r = n\mathbb{Z} + s$.

ii. $s \in n\mathbb{Z} + r$.

iii. $s - r \in n\mathbb{Z}$.

Kanıt: (i $\Rightarrow$ ii $\Rightarrow$ iii $\Rightarrow$ i) döngüsünü izleyerek kanıtlamak son derece kolay; okura bırakılmıştır. □

● Her sayı 9'a bölündüğünde 0'la 8 arasında (0 ve 8 dahil) bir kalan vereceğinden, her sayı, bir ve bir tek $r = 0, 1, 2, ..., 8$ için, $9\mathbb{Z} + r$ kümesindedir. Örneğin, $48 = 9 \times 5 + 3 \in 9\mathbb{Z} + 3$. Demek ki,

$$\mathbb{Z} = 9\mathbb{Z} \cup (9\mathbb{Z} + 1) \cup (9\mathbb{Z} + 2) \cup ... \cup (9\mathbb{Z} + 8)$$

eşitliği geçerlidir. Değişik $r = 0, 1, ..., 8$ için $9\mathbb{Z} + r$ altkümeleri ayrık olduklarından,

$$\mathbb{Z} = 9\mathbb{Z} \text{ ø } (9\mathbb{Z} + 1) \text{ ø } (9\mathbb{Z} + 2) \text{ ø } ... \text{ ø } (9\mathbb{Z} + 8)$$

yazarız. (Buradaki ø simgesi, bileşimi alınan kümelerin ayrık olduklarını gösterir, yani bize ek bilgi verir, başka bir anlamı yoktur.) Genel olarak, eğer $n \neq 0$ ise,

$$\mathbb{Z} = n\mathbb{Z} \text{ ø } (n\mathbb{Z} + 1) \text{ ø } (n\mathbb{Z} + 2) \text{ ø } ... \text{ ø } (n\mathbb{Z} + n - 1).$$

● Bir önceki yazıdan, $n\mathbb{Z} \cap m\mathbb{Z} = \text{ekok}(n, m)\mathbb{Z}$ eşitliğini biliyoruz. (Bu yazıda ekok hep bir doğal sayı olsun.) Şimdi $(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s)$ kesişiminin ne olduğunu bulalım. Bu biraz daha zor bir soru. Önce birkaç örnek:

$(14\mathbb{Z} + 2) \cap (21\mathbb{Z} + 8) = \emptyset$,
$(8\mathbb{Z} + 3) \cap (7\mathbb{Z} + 5) = 56\mathbb{Z} + 19$,
$(14\mathbb{Z} + 1) \cap (21\mathbb{Z} + 8) = 42\mathbb{Z} + 29$.

Görüldüğü gibi hiç de kolay değil kesişimin ne olduğunu bulmak. İkinci örnekteki 56'nın bir şeyler söylemek ister gibi bir hali var... Üçüncü örnekteki 42 de... Ama 19 ve 29'un anlamları hiç de açık değil. Birinci örneğin neden boşküme olması gerektiği de şimdilik bir muamma... Okur aşağıdaki kanıtı okumadan önce yukardaki örneklere benzer örnekler üzerinde çalışmalıdır (ki yapacaklarımızın ve Çinlilerin yüzyıllar önce yaptıklarının değerini daha iyi algılayabilsin!)

Teorem 2. *Eğer $n \neq 0$ ve $m \neq 0$ ise,*

$$(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s)$$

kümesi ya boşkümedir ya da herhangi bir $t \in (n\mathbb{Z} + r) \cap (m\mathbb{Z} + s)$ için, $\text{ekok}(n, m)\mathbb{Z} + t$ kümesine eşittir.

Kanıt: $(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s)$ kümesinin boş olmadığını varsayalım. Bu kümeden herhangi bir t alalım. Önsav 1 (ii $\Rightarrow$ i)'e göre,

$$n\mathbb{Z} + r = n\mathbb{Z} + t \text{ ve } m\mathbb{Z} + r = m\mathbb{Z} + t.$$

Dolayısıyla,

$$(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s) = (n\mathbb{Z} + t) \cap (m\mathbb{Z} + t)$$
$$= (n\mathbb{Z} \cap m\mathbb{Z}) + t = \text{ekok}(n, m)\mathbb{Z} + t. \quad \square$$

Demek ki $n\mathbb{Z} + r$ biçiminde yazılan sonlu sayıda altkümenin kesişimi ya boşkümedir ya da gene bu türden bir kümedir. Aşağıdaki örnekte de göreceğimiz üzere, aynı şey, $n\mathbb{Z} + r$ biçiminde yazılan sonsuz sayıda altkümenin kesişimi için geçerli değildir:

Örnek. 1 ve -1 dışında her tamsayı en az bir asala bölündüğünden,

$$\bigcup_{p \text{ asal}} p\mathbb{Z} = \mathbb{Z} \setminus \{1, -1\}.$$

Her iki tarafın da $\mathbb{Z}$'de tümleyenini alacak olursak,

$$\bigcap_{p \text{ asal},\, r \neq 0 \bmod p} (p\mathbb{Z} + r) = \{1, -1\}$$

buluruz.

$(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s)$ kesişiminin hangi koşullarda boşküme olduğunu da bulabiliriz:

Teorem 3. *Eğer $n \neq 0$ ve $m \neq 0$ ise, $(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s)$ kümesinin boş olmaması için gerek ve yeter koşul*, ebob(n, m)*'nin $s - r$'yi bölmesi, yani*

$$r \equiv s \bmod \text{ebob}(n, m)$$

denkliğidir. Bir başka deyişle,

$$x \equiv r \bmod n$$
$$x \equiv s \bmod m$$

denklemlerinin aynı anda çözülebilmesi için gerek ve yeter koşul

$$r \equiv s \bmod \text{ebob}(n, m)$$

denkliğidir. Ayrıca, eğer x_1 ve x_2 yukardaki denkliklerin bir çözümüyse, o zaman

$$x_1 \equiv x_2 \bmod \text{ekok}(n, m),$$

yani denklemlerin modülo ekok(n, m) *tek bir çözümü vardır.*

Kanıt: Eğer $(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s) \neq \emptyset$ ise, o zaman, iki x, y tamsayısı için, $nx + r = my + s$ eşitliği geçerlidir. Bundan $nx - my = s - r$ çıkar. Dolayısıyla n ve m'yi bölen her sayı $s - r$'yi de böler. Bundan da ebob(n, m)'nin $s - r$'yi böldüğü çıkar.

Şimdi ebob(n, m)'nin $s - r$'yi böldüğünü varsayalım. Demek ki bir u tamsayısı için,

$$s - r = \text{ebob}(n, m)u.$$

Öte yandan, iki y, z tamsayısı için,

$$\text{ebob}(n, m) = ny + mz$$

[sayfa 10, Önsav 6]. Şimdi,

$$s - r = \text{ebob}(n, m)u = (ny + mz)u$$

ve $nyu + r = -mzu + s \in (n\mathbb{Z} + r) \cap (m\mathbb{Z} + s)$.

Teoremin son tümcesini kanıtlamak kaldı: x_1, $x_2 \in (n\mathbb{Z} + r) \cap (m\mathbb{Z} + s)$ olsun; o zaman hem n hem de m, $x_1 - x_2$'yi böler; yani ekok(n, m), $x_1 - x_2$'yi böler. □

Çözümü Gerçekten Bulmak. Bir önceki teoremde,

$$x \equiv r \bmod n$$
$$x \equiv s \bmod m$$

denkliklerinin ortak çözümünün ne zaman olduğunu gördük. Şimdi de ortak çözüm olduğunda tüm ortak çözümleri, yani

$$(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s)$$

kümesinin elemanlarını gerçekten bulalım.

Teorem 3'ün kanıtının ikinci kısmını izleyecek olursak şunu buluruz: u, y ve z tamsayıları,

$$s - r = \text{ebob}(n, m)u$$

ve

$$\text{ebob}(n, m) = ny + mz$$

eşitliklerini sağlarsa, o zaman,

$$nyu + r = -mzu + s \in (n\mathbb{Z} + r) \cap (m\mathbb{Z} + s).$$

Teorem 2'den dolayı, bundan,

$$\begin{aligned}(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s) &= \text{ekok}(n, m)\mathbb{Z} + (nyu + r) \\ &= \text{ekok}(n, m)\mathbb{Z} + (-mzu + s)\end{aligned}$$

çıkar. Demek ki,

$$x \equiv r \bmod n$$
$$x \equiv s \bmod m$$

denkliklerinin ortak çözümlerini bulmak için u, y ve z'yi, yani ebob(n, m)'yi ve y ve z'yi bulmalıyız. Bunları bulmayı bir önceki yazıda öğrenmiştik.

Bir sonraki paragrafta çözümü daha genel bir durumda bulacağız.

Çin Kalanlar Teoremi. Yukarda yaptıklarımızdan şu sonuç çıkar:

Sonuç 4 (Çin Kalanlar Teoremi). *Eğer $n \neq 0$ ve $m \neq 0$ birbirine asalsa, r ve s ne olursa olsun*

$$(n\mathbb{Z} + r) \cap (m\mathbb{Z} + s) \neq \emptyset.$$

Bir başka deyişle, eğer $n \neq 0$ ve $m \neq 0$ birbirine asalsa, r ve s ne olursa olsun,

$$x \equiv r \bmod n$$
$$x \equiv s \bmod m$$

denkliklerinin çözümü vardır.

Teorem 2 ve 3'ü birkaç kez üstüste kullanarak şu sonucu da bulabiliriz:

Sonuç 5 (Çin Kalanlar Teoremi). *$n_1, n_2, \ldots, n_k$ ikişer ikişer aralarında asal olsunlar. $r_1, r_2, \ldots, r_k \in \mathbb{Z}$ herhangi k tamsayı olsun. O zaman,*

$$(n_1\mathbb{Z} + r_1) \cap (n_2\mathbb{Z} + r_2) \cap \ldots \cap (n_k\mathbb{Z} + r_k) \neq \emptyset.$$

Sonuç 6. *n_1, n_2, ..., n_k ikişer ikişer aralarında asal olsunlar. r_1, r_2, ..., $r_k \in \mathbb{Z}$ olsun. O zaman*

$$x \equiv r_1 \bmod n_1$$
$$\ldots$$
$$x \equiv r_k \bmod n_k$$

denklik sisteminin bir çözümü vardır. Ayrıca,

$$N = n_1 n_2 \ldots n_k$$

olsun ve s_i sayıları

$$s_i N/n_i \equiv 1 \bmod n_i$$

denkliklerini sağlasın. O zaman çözümlerden biri,

$$x = r_1 s_1 N/n_1 + \ldots + r_k s_k N/n_k$$

dir.

Kanıt: Önce, N/n_i sayısı n_i'ye asal olduğundan teoremdeki koşulu sağlayan bir s_i sayısının olduğunu belirtelim [MD-2004-I, sayfa 16, Teorem 3].

$r_1 s_1 N/n_1 + \ldots + r_k s_k N/n_k$ sayısını modülo n_i hesapladığımızda, i'den farklı tüm j'ler için $r_j s_j N/n_j$ sayıları sıfırlanır ve geriye sadece $r_i s_i N/n_i$ sayısı kalır, ki varsayıma göre, modülo n_i bu da r_i'dir:

$$r_1 s_1 N/n_1 + \ldots + r_k s_k N/n_k \equiv r_i s_i N/n_i \equiv r_i \bmod n_i.$$

Kanıt tamamlanmıştır. ♥

Sonsuz Sayıda Asal Vardır'ın Muhteşem Bir Kanıtı

Kudüs Üniversitesi'nden Harry Fürstenberg 1955'te sonsuz tane asal sayının varlığının olağanüstü güzel ve şaşırtıcı bir kanıtını verdi [1]. Bilindiği gibi bu teoremi ilk Öklid kanıtlamıştır ve bu kanıt matematiğin en güzel kanıtlarından biri olarak anılır. Harry Fürstenberg'in kanıtının da Öklid'in kanıtından aşağı kalır bir yanı yok.

$n \neq 0$ ve k tamsayıları için $n\mathbb{Z} + k$ biçiminde yazılan kümelere **aritmetik küme** diyelim. Ayrıca bir de boşkümeye aritmetik küme diyelim. Aritmetik kümelerin herhangi bir bileşimine de **yarı aritmetik küme** diyelim. Aritmetik kümeler yarı aritmetik elbette. Ama her yarı aritmetik küme aritmetik olmak zorunda değil.

Şimdi yarı aritmetik kümelerin birkaç özelliğini kanıtlayalım:

1. *Boşküme dışında her yarı aritmetik küme sonsuzdur.*

Kanıt: Tanımdan dolayı boş olmayan her aritmetik küme sonsuzdur. Dolayısıyla bunların bileşimi olan yarı aritmetik kümeler de sonsuzsdur.

2. *Yarı aritmetik kümelerin bileşimi yarı aritmetik bir kümedir.*

Kanıt: Yarı aritmetik kümeler aritmetik kümelerin bileşimi olduklarından, yarı aritmetik kümelerin bileşimi de aritmetik kümelerin bileşimidir.

3. *Sonlu sayıda yarı aritmetik kümenin kesişimi de yarı aritmetik kümedir.*

Kanıt: Herhangi iki yarı aritmetik kümenin kesişiminin bir yarı aritmetik küme olduğunu kanıtlamak yeterli. X ve Y birer yarı aritmetik küme olsunlar. X'i ve Y'yi aritmetik kümelerin bileşimi olarak yazalım: $X = \cup_{i \in I} A_i$ ve $Y = \cup_{j \in J} B_j$. Buradaki A_i ve B_j'ler aritmetik kümelerdir. Elbette,

$$X \cap Y = (\cup_{i \in I} A_i) \cap (\cup_{j \in J} B_j) = \cup_{i \in I,\, j \in J} (A_i \cap B_j).$$

Demek ki her $A_i \cap B_j$'nin bir aritmetik küme olduğunu kanıtlamak yeterli. Ama bu bir önceki yazıda (Teorem 2, sayfa 14'te) kanıtlanmıştır .

4. *Bir aritmetik kümenin tümleyeni yarı aritmetiktir.*

Kanıt: $n\mathbb{Z} + r$ bir aritmetik küme olsun.

$$\mathbb{Z} = n\mathbb{Z} \sqcup (n\mathbb{Z} + 1) \sqcup (n\mathbb{Z} + 2) \sqcup \ldots \sqcup (n\mathbb{Z} + n - 1)$$

eşitliğinden dolayı, $n\mathbb{Z} + r$ kümesinin tümleyeni, diğer $n\mathbb{Z} + i$ kümelerinin bileşimidir. Bunların da herbiri aritmetik olduğundan, $n\mathbb{Z} + r$ kümesi yarı aritmetiktir.

Teorem. *Sonsuz sayıda asal vardır.*

Kanıt: Sonlu sayıda asal olduğunu varsayalım. Bunlara p_1, ..., p_k diyelim. O zaman 1 ve –1 dışında her sayı bu k asaldan birine bölünür. Yani

$$\cup_i p_i\mathbb{Z} = \mathbb{Z} \setminus \{1, -1\}.$$

Buradaki bileşimin sonlu bir bileşim olduğuna dikkatinizi çekerim. Her iki tarafın da tümleyenini alırsak,

$$\cap_i (\mathbb{Z} \setminus p_i\mathbb{Z}) = \{1, -1\}$$

buluruz. Buradaki kesişim de sonlu bir kesişim. (4)'ten dolayı, her $\mathbb{Z} \setminus p_i\mathbb{Z}$ yarı aritmetik bir küme. (3)'ten dolayı, sonlu kesişim olan $\cap_i (\mathbb{Z} \setminus p_i\mathbb{Z})$ de yarı aritmetik. Ama bu yarı aritmetik küme $\{1, -1\}$ kümesine eşit ve bu (1)'le çelişiyor. Demek ki sonlu sayıda asal yok... Yani sonsuz sayıda asal var. □

Kaynakça

[1] Harry Fürstenberg, *On the Infinitude of Primes*, Amer. Math. Monthly 62 (1955) 353.