

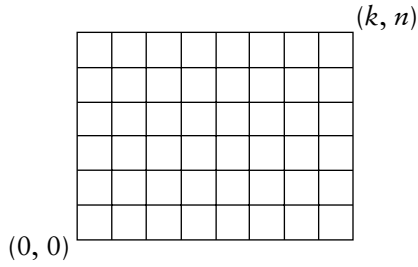
Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (2)

Cahit Arf Matematik Günleri III - 2004

İkinci Gün Soru ve Yanıtları

28 Mart 2004

Problem 1. *Düzlemdeki $Z \times Z$ ızgarasında (aşağıdaki şekil) $(0, 0)$ noktasından herhangi bir (k, n) noktasına hep kuzeye ve doğuya gitmek koşuluyla ve ızgarayı takip ederek kaç değişik biçimde gidilir?*



Çözüm. Doğuya doğru k adım, kuzeye doğru n adım atmalıyız. Demek ki toplam $k + n$ adım atmalıyız. Bu $k + n$ adımın tam k tanesi doğuya olmalı, geri kalanlar zorunlu olarak kuzeye olurlar. Demek ki $k + n$ adımdan doğuya atılacak k adımı seçmeliyiz. Yanıt

$$\binom{n+k}{k}$$

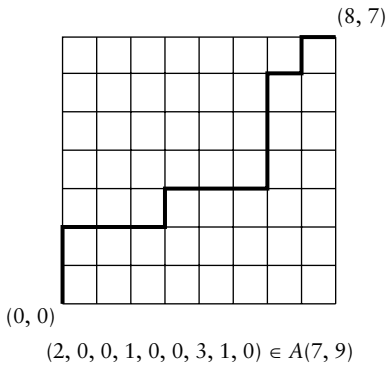
dır.

Problem 2. *n ve k birer doğal sayı olsun.*

$A(n, k) = \{(a_0, \dots, a_{k-1}) : a_0, \dots, a_{k-1} \in \mathbb{N} \text{ ve } a_0 + \dots + a_{k-1} = n\}$ kümesinin eleman sayısını bulun.

Çözüm 1: $(a_0, \dots, a_{k-1}) \in A(n, k)$ olsun. Kendimizi yukardaki ızgaranın üstünde olduğu gibi $(0,0)$ 'dan $(k-1, n)$ noktasına giderken düşünelim ve her a_i sayısını, doğuya doğru i -inci hamle yapıldıktan hemen sonra kuzeye doğru attığımız adım sayısı olarak yorumlayalım.

Bunun geri dönüşü de vardır: Birinci problemdeki her kuzeydoğu yolu bize bu sayede (yandaki şekle bakın) $A(n, k)$ kümesinden bir elemana tekabül eder.



$(0, 0)$
 $(2, 0, 0, 1, 0, 0, 3, 1, 0) \in A(7, 9)$

Sonuç olarak, yanıt

$$\binom{n+k-1}{k-1}$$

dır.

Çözüm 2: n sayısını n tane 1 (ya da çubuk) olarak görelim. Bu n tane 1'i aralarına $k-1$ tane ayrıç koyarak ayıracağız. Ardışık ayrıçların arasındaki 1 sayısı bize a_i sayılarını verecek. (Ayrıçlar başa ya da sona gelebilir. İki ayrıç aynı yere gelebilir.) Her ayırım bize $A(n, k)$ kümesinin ayrı bir elemanını verecek. n tane 1 ve $k-1$ tane ayrıç olmak üzere toplam $n + k - 1$ tane nesnemiz var. Bu $n + k - 1$ nesne arasından ayrıç olacak $k - 1$ nesneyi (ya da 1 olacak n nesneyi) seçmeliyiz. Yanıt

$$\binom{n+k-1}{k-1}$$

dır.

Problem 3. *n elma, adları A_0, \dots, A_{k-1} olan k kişi arasında kaç türlü dağıtılır? (Dikkat: Kişiler arasında ayırım yapıyoruz, ama elmalar arasında yapmıyoruz.)*

Çözüm. $(a_0, \dots, a_{k-1}) \in A(n, k)$ olsun. Her a_i 'yi A_i 'e verilecek elma sayısı olarak yorumlayabiliriz. Yanıt gene

$$\binom{n+k-1}{k-1}$$

dır.

Problem 4. *$n \geq 1$ ve $k \geq 1$ birer doğal sayı olsun.*

$B(n, k) = \{(b_1, \dots, b_n) : b_1, \dots, b_n \in \mathbb{N} \text{ ve } 0 \leq b_1 \leq \dots \leq b_n \leq k-1\}$ kümesinin eleman sayısını bulun.

Çözüm. $B(n, k)$ kümesinde yukardaki $A(n, k)$ kümesindeki eleman kadar eleman vardır. Nitekim, $(a_0, \dots, a_{k-1}) \in A(n, k)$ olsun. Bu elemanın yardımıyla $B(n, k)$ kümesinden bir (b_1, \dots, b_n) elemanı bulacağız. (b_1, \dots, b_n) elemanının ilk a_0 tanesi 0 olsun, sonraki a_1 tanesi 1 olsun, ..., en son a_{k-1} tanesi $k-1$ olsun. Örneğin, $n = 5, k = 4$ ise, $A(5, 4)$ kümesinin $(0, 2, 1, 2)$ elemanı $B(5, 4)$ kümesinin $(1, 1, 2, 3, 3)$ elemanına tekabül eder (0 tane 0, 2 tane 1, 1 tane 2, 2 tane 3).

Bunun geri dönüşü de vardır: Eğer $(b_1, \dots, b_n) \in B(n, k)$ ise, a_i bu sonlu dizideki i sayısı olsun. Örneğin eğer $n = 5$ ve $k = 4$ ise, $B(5, 4)$ kümesinin $(1, 1, 2, 3, 3)$ elemanına $A(5, 4)$ kümesinin $(0, 2, 1, 2)$ elemanı tekabül eder (0 tane 0, 2 tane 1, 1 tane 2, 2 tane 3).

Problem 5. Birbirinden ayırdedilemeyen n top ve bu topları boyayabileceğimiz k değişik renkte boyamız var. Bu n topu bu k değişik renge kaç türlü boyayabiliriz? Dikkat: Toplar ayırdedilmiyor ama renkler ayırdediliyor. Örnek: Üç top ve kırmızı ve mavi olmak üzere iki rengimiz varsa, (üçü mavi), (iki mavi, bir kırmızı), (bir mavi, iki kırmızı), (üçü kırmızı) olmak üzere dört türlü boyayabiliriz. Eğer üç top ve üç rengimiz varsa boyamayı 10 türlü yapabiliriz.

Çözüm. Bu da aynı sayı! Her topu elma olarak düşünelim. Her renk de bir kişiyi simgelesin. Toplar (yani elmalar) dağıtılan kişinin rengine boyanır. Problem 3'le aynı yanıtı buluruz.

Problem 6. $n \geq 1$ bir doğal sayı olsun. n 'yi kaç değişik biçimde pozitif doğal sayıların toplamı olarak yazabiliriz? (Değişik sıralamalar ayrı ayrı sayılacak, örneğin, $n = 14$ ise,

$$1 + 3 + 5 + 5 \text{ ve } 5 + 3 + 5 + 1$$

toplamları ayrı ayrı sayılacak.)

Çözüm. n pirinç tanesi alıp yanyana sıraya dizelim. Bu n pirinç tanesi arasında $n - 1$ tane aralık vardır. Bu $n - 1$ aralığa belli bir sayıda çubuk yerleştireceğiz. İki çubuk arasında olan pirinç tanesi sayısı toplamı oluşturan bir sayıyı belirleyecek. Örneğin, $n = 9$ ise, çubukların



pozisyonu bize $9 = 3 + 2 + 4$ toplamını verecek. Toplam $n - 1$ aralığımız var ve her aralığa bir çubuk ya yerleştireceğiz ya da yerleştirmeyeceğiz. Demek ki toplam 2^{n-1} seçeneğimiz var.

Problem 7. $1 + t - 2t^2 + 6t^3 - 3t^6 + \dots$ gibi sonsuza dek uzayabilen (polinoma benzeyen ancak sonsuza dek uzayabildiklerinden illa polinom olmayan) terimlere **güç serisi** adı verilir. Dikkat: Buradaki t bir sayı değildir, değişken adı verilen bir "şey"dir. Güç serileri de aynen polinomlar gibi toplanıp çarpılabilirler:

$$\begin{aligned} (a_0 + a_1t + a_2t^2 + \dots) + (b_0 + b_1t + b_2t^2 + \dots) &= \\ a_0 + b_0 + (a_1 + b_1)t + (a_2 + b_2)t^2 + \dots & \\ (a_0 + a_1t + a_2t^2 + \dots)(b_0 + b_1t + b_2t^2 + \dots) &= \\ a_0b_0 + (a_0b_1 + a_1b_0)t + (a_0b_2 + a_1b_1 + a_2b_0)t^2 & \\ + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)t^3 + \dots & \end{aligned}$$

Bir güç serisi kısaca

$$\sum_{m=0}^{\infty} a_m t^m$$

biçiminde yazılabilir. Burada, a_m katsayılarını gerçel sayılar olarak alacağız. Eğer a_m katsayıları belli bir aşamadan sonra hep 0'sa, o zaman güç serisi bir polinomdur, yoksa değildir. Eğer tüm a_m 'ler 0'sa o zaman güç serisi de 0'dır.

Kolayca görüleceği üzere güç serilerini toplama ve çarpma kuralları şöyledir:

$$\begin{aligned} \sum_{m=0}^{\infty} a_m t^m + \sum_{m=0}^{\infty} b_m t^m &= \sum_{m=0}^{\infty} (a_m + b_m) t^m \\ \left(\sum_{m=0}^{\infty} a_m t^m \right) \left(\sum_{m=0}^{\infty} b_m t^m \right) & \\ = \sum_{m=0}^{\infty} \left(\sum_{m_1+m_2=m} a_{m_1} b_{m_2} \right) t^m. & \end{aligned}$$

Sayfa 32-38'de güç serilerini oldukça ayrıntılı bir biçimde inceledik, hatta aşağıdaki soruların bir kısmını orada yanıtladık.

7.1.i. $(1 - t)(1 + t + t^2 + t^3 + t^4 + \dots) = 1$ eşitliğini gösterin. (Not: Her polinom gibi, $1-t$ polinomu da bir güç serisidir.)

Çözüm. $a_0 = 1, a_1 = -1, a_2 = a_3 = \dots = 0$ olsun. $b_0 = b_1 = b_2 = \dots = 1$ olsun. O zaman,

$$\begin{aligned} (1-t)(1+t^2+t^3+\dots) &= \left(\sum_{m=0}^{\infty} a_m t^m \right) \left(\sum_{m=0}^{\infty} b_m t^m \right) \\ &= \sum_{m=0}^{\infty} \left(\sum_{m_1+m_2=m} a_{m_1} b_{m_2} \right) t^m \\ &= \sum_{m=0}^{\infty} \left(\sum_{m_1+m_2=m} a_{m_1} \right) t^m. \end{aligned}$$

Şimdi

$$\sum_{m_1+m_2=m} a_{m_1}$$

katsayılarını hesaplayalım. Sadece a_0 ve $a_1 \neq 0$ olduğundan, bu toplamda sadece $m_1 = 0$ ve $m_1 = 1$ önemlidir, gerisi gereksizdir. Eğer $m = 0$ ise $m_1 = m_2 = 0$ olduğundan toplam a_0 , yani 1'dir. Eğer $m > 0$ ise,

$$\sum_{m_1+m_2=m} a_{m_1} = a_0 + a_1 = 1 + (-1) = 0.$$

Birincisi dışında bütün katsayılar 0 olduğundan, ilk katsayı da 1 olduğundan, çarpım 1'dir.

7.1.ii. $(1+t)g(t) = 1$ eşitliğini sağlayan bir $g(t)$ güç serisi bulun.

Çözüm. Yukardaki

$$(1-t)(1+t+t^2+t^3+t^4+\dots) = 1$$

eşitliğinden esinlenerek,

$$(1+t)(1-t+t^2-t^3+t^4-\dots) = 1$$

eşitliği tahmin edilip kolaylıkla kanıtlanır. Demek ki

$$g(t) = \sum_{m=0}^{\infty} (-1)^m t^m.$$

7.1.iii. $(1-2t)g(t) = 1$ eşitliğini sağlayan bir $g(t)$ güç serisi bulun.

Çözüm. Yukardaki gibi çözülür. Yanıt:

$$g(t) = \sum_{m=0}^{\infty} 2^m t^m.$$

$$7.2. \left(\sum_{m=0}^{\infty} t^m \right)^2 = \sum_{m=0}^{\infty} (m+1)t^m$$

eşitliğini gösterin.

Çözüm. Çarpmanın tanımından doğrudan çıkar:

$$\left(\sum_{m=0}^{\infty} t^m \right)^2 = \sum_{m=0}^{\infty} \left(\sum_{m_1+m_2=m} 1 \right) t^m = \sum_{m=0}^{\infty} (m+1)t^m,$$

çünkü,

$\{(m_1, m_2) : m_1 + m_2 = m\} = \{(i, m-i) : i = 0, 1, \dots, m\}$ dir ve bu kümenin $m+1$ elemanı vardır.

7.3. İki güç serisini çarpabildiğimiz gibi, üç güç serisini de çarpabiliriz:

$$\begin{aligned} & \left(\sum_{m=0}^{\infty} a_m t^m \right) \left(\sum_{m=0}^{\infty} b_m t^m \right) \left(\sum_{m=0}^{\infty} c_m t^m \right) \\ &= \sum_{m=0}^{\infty} \left(\sum_{m_1+m_2+m_3=m} a_{m_1} b_{m_2} c_{m_3} \right) t^m. \end{aligned}$$

Anlaşılabacağı üzere sonlu sayıda güç serisini çarpabiliriz.

$$\left(\sum_{m=0}^{\infty} t^m \right)^k = \sum_{m=0}^{\infty} \binom{m+k-1}{k-1} t^m$$

eşitliğini gösterin.

Çözüm. Çarpmanın tanımını ve Problem 2'yi uygulayacağız:

$$\begin{aligned} \left(\sum_{m=0}^{\infty} t^m \right)^k &= \sum_{m=0}^{\infty} \left(\sum_{m_1+\dots+m_k=m} 1 \right) t^m \\ &= \sum_{m=0}^{\infty} \binom{m+k-1}{k-1} t^m \end{aligned}$$

7.4. Aşağıdaki çarpımları bulun:

$$(1+t)(1+t^2)$$

$$(1+t)(1+t^2)(1+t^4)$$

$$(1+t)(1+t^2)(1+t^4)(1+t^8)$$

$$(1+t)(1+t^2)(1+t^4)(1+t^8)(1+t^{16})$$

Bunlardan kimi zaman sonsuz tane güç serisini çarpabildiğimiz çıkar.

$$(1+t)(1+t^2)(1+t^4)(1+t^8) \dots (1+t^{2^n}) \dots$$

çarpımının ne olması gerektiğini söyleyin.

Çözüm.

$$(1+t)(1+t^2) = 1+t+t^2+t^3$$

$$(1+t)(1+t^2)(1+t^4) = 1+t+t^2+\dots+t^7$$

$$(1+t)(1+t^2)(1+t^4)(1+t^8) = 1+t+t^2+\dots+t^{15}$$

$$(1+t)(1+t^2)(1+t^4)(1+t^8)(1+t^{16}) = 1+t+t^2+\dots+t^{31}$$

Kolayca tahmin edileceği üzere,

$$(1+t)(1+t^2)(1+t^4)(1+t^8) \dots (1+t^{2^n}) \dots = \sum_{m=0}^{\infty} t^m.$$

Bunun nedeni her m doğalsayısının 2'lik tabanda tek bir biçimde yazılmasıdır.

7.5. $(1+t)(1+t)(1+t)(1+t)(1+t)\dots$ sonsuz çarpımı bir güç serisi olarak yazılamaz. Neden?

Yanıt. Çünkü $(1+t)^n = 1+nt+\dots$ ve kısmi çarpımlarda t 'nin katsayısı durmadan artar.

Problem 8. Aşağıdaki çarpımları bulun:

$$(1+t)(1+t^2),$$

$$(1+t)(1+t^2)(1+t^3),$$

$$(1+t)(1+t^2)(1+t^3)(1+t^4),$$

$$(1+t)(1+t^2)(1+t^3)(1+t^4)(1+t^5).$$

Bundan,

$$(1+t)(1+t^2)(1+t^3) \dots (1+t^n) \dots$$

sonsuz çarpımının var olduğu anlaşılmalı.

Eğer n pozitif bir tamsayıysa, $q(n)$, n 'yi birbirinden değişik pozitif tamsayıların toplamı olarak yazma biçimi olsun, yani $q(n)$,

$$A(n) = \{(a_1, \dots, a_k) : k \in \mathbb{N}, a_1, \dots, a_k \in \mathbb{N},$$

$$1 \leq a_1 < \dots < a_k \text{ ve } a_1 + \dots + a_k = n\}$$

kümesinin eleman sayısı olsun. Ayrıca $q(0) = 1$ olsun. Örneğin $q(0) = 1, q(1) = 1, q(2) = 1, q(3) = 2, q(4) = 2, q(5) = 3, q(6) = 4, q(7) = 5$. Şimdi,

$$(1+t)(1+t^2)(1+t^3)(1+t^4) \dots (1+t^n) \dots = \sum_{n=0}^{\infty} q(n)t^n$$

eşitliğini kanıtlayın.

Çözüm. Sonsuz tane çarpım olsa da, çarpımın şu şekilde olması gerektiği kolaylıkla anlaşılır:

$$(1+t)(1+t^2)(1+t^3) \dots (1+t^n) \dots = \sum_{m=0}^{\infty} \left(\sum_{i=1}^n 1 \right) t^m$$

Sağdaki toplamda beliren soru işaretini bulmalıyız. O soru işareti, toplamı m olan birbirinden değişik ve 1'den büyük sayıların sayısıdır, yani yukardaki $A(m)$ kümesinin eleman sayısı olan $q(m)$ kadar 1'i toplarız.

Problem 9. $\prod_{k=1}^{\infty} \left(\sum_{m=0}^{\infty} t^{mk} \right)$ sonsuz çarpımı, yani,

$$\left(\sum_{m=0}^{\infty} t^m \right) \left(\sum_{m=0}^{\infty} t^{2m} \right) \left(\sum_{m=0}^{\infty} t^{3m} \right) \dots \left(\sum_{m=0}^{\infty} t^{km} \right) \dots$$

ya da

$$(1+t+t^2+t^3+\dots)(1+t^2+t^4+t^6+\dots)(1+t^3+t^6+t^9+\dots)\dots$$

sonsuz çarpımı bir güç serisidir. Bu sonsuz çarpımı

$$\prod_{k=1}^{\infty} \left(\sum_{m=0}^{\infty} t^{mk} \right) = \sum_{n=0}^{\infty} p(n)t^n$$

olarak yazalım. Buradaki $p(n)$ sayılarının daha güncel bir dille (yukardaki sorulardan esinlenerek belki) neyi ifade ettiğini bulun.

Yanıt.

$$\prod_{k=1}^{\infty} \left(\sum_{m=0}^{\infty} t^{mk} \right) = \sum_{n=0}^{\infty} \left(\sum_{m_1+2m_2+\dots+km_k=n} 1 \right) t^n$$

eşitliği bu aşamada artık anlaşılmalı. Demek ki $p(n)$ katsayıları, n sayısının $m_1 + 2m_2 + \dots + km_k$ olarak yazılış biçimidir. Bu $m_1 + 2m_2 + \dots + km_k$ sayısını $(1 + \dots + 1) + (2 + \dots + 2) + \dots + (k + \dots + k)$ olarak yazabiliriz (burada m_1 tane 1 var, m_2 tane 2 var, ..., m_k tane k var.) Yani $p(n)$ sayısı n 'nin kaç türlü küçükten büyüğe sıralanmış pozitif doğal sayıların toplamı olarak yazılacağıdır. Belki $p(0)$ sayısını ayrıca 1 olarak tanımlamak gerekli olabilir. Bu sayıya n 'nin parçalanmış sayısı denir. Örneğin, $n = 4$ ise,

$$4 = 1 + 3 = 2 + 2 = 1 + 1 + 2 = 1 + 1 + 1 + 1$$

olduğundan $p(4) = 5$ 'tir. Eğer $n = 5$ ise,

$$5 = 1 + 4 = 2 + 3 = 1 + 1 + 3 = 1 + 2 + 2 \\ = 1 + 1 + 1 + 2 = 1 + 1 + 1 + 1 + 1$$

olduğundan, $p(5) = 7$ 'dir. $p(0)$, tanım gereği 1'dir. ♥

Bézout Önsavı'nın Bir Başka Kanıtı

Sayfa 30'da kanıtladığımız önsavın bir başka kanıtını verelim:

Önsav [Bézout]. K bir cisim olsun. Eğer $a, b \in K[X]$ polinomlarının sabit polinomlardan başka ortak böleni yoksa, o zaman $au + bv = 1$ eşitliğini sağlayan u ve v polinomları vardır.

Kanıt: Bir tanımla başlayalım:

$$I = \{au + bv : u, v \in K[X]\}$$

olsun. Bu kümeden derecesi en küçük olan ama sıfır olmayan polinomlardan birini alalım, diyelim e polinomu. Demek ki, $e \neq 0$ ve $u, v \in K[X]$ polinomları için $au + bv = e$ eşitliği geçerli, ayrıca bu tür bir eşitliği sağlayan e 'den daha küçük dereceli bir polinom yok. e 'nin hem a 'yı hem de b 'yi böldüğünü kanıtlayacağız. Durum simetrik olduğundan, e 'nin a 'yı böldüğünü kanıtlamak yeterli. Şimdi a 'yı e 'ye bölelim [MD-2004-I, Teorem 3, sayfa 35]: Belli bir $q, r \in K[X]$ için, $a = qe + r$ ve $d^{\circ}(r) < d^{\circ}(e)$. Demek ki,

$$r = a - qe = a - q(au + bv) = a(1 - qu) - bqv \in I.$$

Ama r 'nin derecesi e 'nin derecesinden küçük. Dolayısıyla, e 'nin seçiminden dolayı, $r = 0$ olmalı ve e, a 'yı bölmeli. Bu kanıtın bir benzeri, e 'nin b 'yi de böldüğünü gösterir. Önsavın varsayımına göre, $K[X]$ 'in tersinir bir ögesidir, yani K^* 'dadır. Artık hesap yapma zamanı geldi:

$$a(e^{-1}u) + b(e^{-1}v) = e^{-1}(au + bv) = e^{-1}e = 1.$$

Önsav kanıtlanmıştır. □

Okur bu aşamada aynı kanıtın $K[X]$ yerine Z alındığında da geçerli olduğunu farketmelidir. ♥

$Z[X]$ 'te indirgenemezler

$Z[X]$ 'in indirgenemezlerini bulmanın bir algoritması varsa da, bu, pek kolay bir problem değildir. Bu konuda çok bilinen iki yöntem aşağıda.

1) Eğer $n > 1$ bir tamsayıysa, başkatsayısı 1 olan bir $f \in Z[X]$ polinomunun katsayılarını modülo n alıp, $Z/nZ[X]$ halkasının bir \bar{f} polinomunu buluruz. Eğer \bar{f} , $Z/nZ[X]$ 'te indirgenemezse, o zaman f , $Z[X]$ 'te indirgenemezdir, çünkü $f = gh$ olsaydı, $Z/nZ[X]$ halkasında $\bar{f} = \bar{g}\bar{h}$ olurdu.

Ahştırma. $X^4 + nX + 5n^2 + 1$ polinomu hangi n 'ler için $Z[X]$ 'te indirgenemezdir?

2) **Eisenstein Kriteri.** $p \in Z$ bir asal olsun. $f \in Z[X]$, başkatsayısı 1 olan, diğer başkatsayılarının p 'ye bölündüğü, ama sabit katsayısı f_0 'ın p^2 'ye bölünmediği bir polinom olsun. O zaman f indirgenemezdir.

Kanıt: $f = gh$ olsun. $d^{\circ}(f) = n$, $d^{\circ}(g) = i$ ve $d^{\circ}(h) = j$ olsun. p asal olduğundan Z/pZ bir cisimdir ve $Z/pZ[X]$ bir TÇB'dir (sayfa 31). Dolayısıyla $f = gh$ eşitliğini $Z/pZ[X]$ 'te görüp tekrar $Z[X]$ 'e çıktığımızda, $\bar{f} = X^n$ olduğundan, dereceleri sırasıyla i ve j 'den küçük g_1 ve h_1 polinomları için, $g = \pm X^i + pg_1$, $h = \pm X^j + ph_1$ eşitliklerini buluruz. Eğer i ve $j > 0$ ise, $f = gh = (\pm X^i + pg_1)(\pm X^j + ph_1)$ eşitliğinden, p^2 'nin f_0 'ı böldüğü çıkar. Demek ki ya i ya da $j = 0$. Bundan da kolaylıkla $g = \pm 1$ ya da $h = \pm 1$ çıkar. □

Ahştırma. p bir asalsa,

$$X^{p-1} + X^{p-2} + \dots + X + 1$$

polinomu $Z[X]$ 'te indirgenemezdir. **İpucu:** Bu polinom $(X^p - 1)/(X - 1)$ 'e eşittir. Burada X yerine $Y + 1$ yazın.