

Euler'in Teoremi ve Cisimlerin Çarpımsal ve Sonlu Altgrupları

E. Mehmet Kırıl* ve Ali Nesin**

Geçen yazıda kanıtladığımız Fermat'ın Küçük Teoremi, n 'yi bölmeyen bir p asalının $n^{p-1} - 1$ sayısını böldüğünü söylüyordu. Bu yazıda bu sonucu şöyle genelleştireceğiz:

Teorem 1. (Euler) *Eğer n ve m birbirine asal doğal sayılarsa, o zaman, m , $n^{\varphi(m)} - 1$ 'i böler, yani $n^{\varphi(m)} \equiv 1 \pmod{m}$.*

Ayrıca, $n^d \equiv 1 \pmod{m}$ denkleğini sağlayan en küçük d pozitif doğal sayısı $\varphi(m)$ 'yi böler.

Teoremden sözünü ettiğimiz φ , Euler φ -fonksiyonudur ve bir m doğal sayısı için, m 'ye asal ve m 'den küçüğeşit pozitif doğal sayıların sayısı olarak tanımlanır:

$$\varphi(m) = |\{x \in \mathbb{N} : x \leq m \text{ ve } \text{ebob}(x, m) = 1\}|.$$

Örneğin, 6'dan küçüğeşit 6'ya asal sadece 1 ve 5 olduğundan $\varphi(6) = 2$. Bunun gibi $\varphi(8) = 4$, $\varphi(15) = 8$. Eğer p bir asalsa, $\varphi(p) = p - 1$ elbet, dolayısıyla bir önceki yazıda kanıtlanan Fermat'ın küçük teoremi bu teoremin bir sonucudur.

Teoremi uygulamak için $\varphi(m)$ 'yi hesaplayabilmek gerekir elbet. Bunu MD-2004-I, sayfa 39-41'de görmüştük. Anımsatalım: Önce m 'yi asal çarpanlarına ayırırız:

$$m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}.$$

Buradaki p_1, \dots, p_r sayıları m 'yi bölen birbirinden değişik asal sayılardır. m asal çarpanlarına ayrıldıktan sonra, $\varphi(m)$ şöyle bulunur:

$$\begin{aligned} \varphi(m) &= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_r^{k_r} - p_r^{k_r-1}) \\ &= m(1 - 1/p_1)(1 - 1/p_2) \dots (1 - 1/p_r). \end{aligned}$$

Örneğin, $\varphi(24) = \varphi(2^3 \times 3) = (2^3 - 2^2)(3^1 - 3^0) = (8 - 4) \times (3 - 1) = 4 \times 2 = 8$. Dolayısıyla, 24'le 35 birbirine asal olduklarından, yukardaki teoreme göre, $24, 35^{\varphi(24)} - 1$ 'i, yani $35^8 - 1$ 'i böler.

Elimiz değmişken, ayrıca bir de cebirin önemli bir teoremini oldukça zahmetsiz bir biçimde kanıtlayacağız. Kanıtlayacağımız ikinci teoremi yazmak için birkaç tanıma gereksiniyoruz.

* Boğaziçi Üniversitesi, birinci sınıf matematik öğrencisi.

** İstanbul Bilgi Üniversitesi Matematik Bölümü öğretim üyesi.

Eğer R bir halkayı simgeliyorsa, R^* , R 'nin tersinir elemanlarının kümesini simgeler:

$$R^* = \{r \in R : \text{bir } s \in R \text{ için } rs = 1\}.$$

R^* kümesi çarpma altında kapalıdır elbette, yani tersinir iki elemanın çarpımı gene tersinirdir. Ayrıca R^* 'ın bir elemanının tersi de R^* 'dadır ve 1 de bu kümededir. R^* 'ın bu özelliklere sahip altkümelerine R 'nin **çarpımsal grubu** ya da kısaca **grubu** diyelim. Demek ki bir G kümesinin bir R halkasının (çarpımsal) bir grubu olması için,

i) $G \subseteq R^*$ olmalı,

ii) G 'nin elemanlarının çarpımı gene G 'de olmalı. (Yani G çarpma altında kapalı olmalı.)

iii) $1 \in G$ olmalı,

iv) $g \in G$ ise $g^{-1} \in G$ olmalı. (Yani G tersleme altında kapalı olmalı.)

R^* 'ın kendisinin R 'nin çarpımsal bir grubu olduğuna dikkatinizi çekeriz.

Bu yazıda daha çok G 'nin sonlu olduğu durumla ilgileneceğiz.

Örnek. Eğer R bir halka ve n herhangi bir pozitif doğal sayıysa, kolayca görüleceği üzere

$$\{x \in R : x^n = 1\}$$

kümesi R 'nin bir grubudur. Eğer R ayrıca bir tamlık bölgesiyse (yani bir xy çarpımının 0 olması için x ya da y 'nin 0 olması gerektiği bir halkaysa), bu grubun en fazla n elemanı vardır, çünkü grubun her elemanı $X^n - 1$ polinomunun köküdür ve, R bir tamlık bölgesi olduğundan, bu polinomun R 'de en fazla de-

Dikkat!

m 'ye asal her n için $n^k \equiv 1 \pmod{m}$ denkleğini sağlayan en küçük k doğal sayısı $\varphi(m)$ olmayabilir! Örneğin, $m = 8 = 2^3$ ise, $\varphi(m) = 4$ ama, $1^1 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$ dir, yani 8'e asal her n için, $n^2 \equiv 1 \pmod{8}$ 'dir.

Genel olarak, eğer 8, m 'yi bölüyorsa $\varphi(m)/2$, yoksa $\varphi(m)$ 'nin kendisi, m 'ye asal her n tamsayısı için, $n^k \equiv 1 \pmod{m}$ denkleğini sağlayan en küçük pozitif tamsayıdır. Bunu ilerde bir gün MD'de kanıtlarız.

recesi kadar kökü vardır [MD-2004-II, sayfa 29, Sonuç 4]. İkinci teoremimiz, bir tamlık bölgesinin bunlardan başka sonlu grubu olmadığını söylüyor.

Teorem 2. G , bir R tamlık bölgesinin n elemanlı bir grubu olsun. O zaman öyle bir $g \in G$ vardır ki, $G = \{1, g, g^2, \dots, g^{n-1}\}$. Yani $X^n - 1$ polinomunun R 'de tam n kökü vardır ve G bu köklerin kümesidir.

Ayrıca, eğer $g \in G$ yukardaki özelliğe sahipse, o zaman n 'ye asal her i için g^i aynı özelliğe sahiptir ve diğer g^i 'ler bu özelliğe sahip değildirler. Yani G 'de bu tür elemanlardan tam $\varphi(n)$ tane vardır.

Kanıtlara başlıyoruz. Bundan böyle R bir halka, G de R 'nin sonlu bir grubu olsun.

Önsav 3. G 'nin her g elemanı için $g^d = 1$ eşitliğini sağlayan pozitif bir d tamsayısı vardır.

Kanıt: $g \in G$ olsun. G çarpma altında kapalı olduğundan, $1, g, g^2, g^3, \dots$ elemanlarının hepsi G 'dedir. Öte yandan G sonlu olduğundan bunların hepsi birbirinden değişik olamaz. Demek ki birbirinden değişik n ve m tamsayıları için, $g^n = g^m$ eşitliği sağlanır. Diyelim ki $n > m$. O zaman eşitliğin her iki tarafını da $g^{m'nin}$ R 'de tersi olan g^{-m} elemanı ile çarparsak, $g^{n-m} = 1$ elde ederiz. Demek ki pozitif bir d doğal sayısı için $g^d = 1$. □

Yukardaki önsava göre, eğer $g \in G$ ise, $g^d = 1$ eşitliğini sağlayan en küçük bir pozitif d tamsayısı vardır. Bu tamsayıya g 'nin derecesi ya da mertebesi adı verilir ve $o(g)$ olarak gösterilir. Tanımdan dolayı, her $g \in G$ için, $g^{o(g)} = 1$. Ayrıca $o(g) = 1$ an-

cak ve ancak $g = 1$ ise.

Önsav 4. $g \in G$ olsun. O zaman,

i. $\{g^i : i \in \mathbb{Z}\} = \{1, g, g^2, \dots, g^{o(g)-1}\}$ 'dir ve bu kümenin tam $o(g)$ tane elemanı vardır. Dolayısıyla bu küme R 'nin sonlu bir grubudur.

ii. Bir n tamsayısı için, $g^n = 1$ eşitliği ancak ve ancak $o(g)$, n 'yi bölerse sağlanır.

iii. g^i 'nin derecesi $o(g)/\text{ebob}(o(g), i)$ 'dir.

Kanıt: i) $i \in \mathbb{Z}$ olsun. i 'yi $o(g)$ 'ye bölelim: $i = o(g)q + r$ eşitliğini ve $0 \leq r < o(g)$ eşitsizliklerini sağlayan q ve r tamsayıları vardır. O zaman,

$$g^i = g^{o(g)q + r} = (g^{o(g)})^q g^r = 1^q g^r = 1g^r = g^r.$$

Demek ki i tamsayısı ne olursa olsun, g^i , bir $0 \leq r < o(g)$ için g^r biçiminde ifade ediliyor. Dolayısıyla, $\{g^i : i \in \mathbb{Z}\} = \{1, g, g^2, \dots, g^{o(g)-1}\}$.

Eğer bu kümenin $o(g)$ 'den daha az elemanı olsaydı, o zaman, birbirinden değişik iki $i, j = 0, 1, \dots, o(g) - 1$ sayısı için $g^i = g^j$ eşitliği geçerli olurdu. $i > j$ eşitsizliğini varsaymanın bedeli yok, varsayalım. O zaman $g^i = g^j$ eşitliğinin iki tarafını da g^{-j} ile çarparak, $g^{i-j} = 1$ eşitliğini buluruz. Ama $0 < i - j < o(g)$ ve bu da $o(g)$ 'nin tanımıyla çelişir. Demek ki

$$\{1, g, g^2, \dots, g^{o(g)-1}\}$$

kümesinin tam $o(g)$ tane elemanı vardır ve bu küme, $\{g^i : i \in \mathbb{Z}\}$ kümesine eşit olduğundan, çarpma altında kapalıdır, dolayısıyla sonlu bir gruptur.

ii) Önce $g^n = 1$ eşitliğini varsayalım. n 'yi $o(g)$ 'ye bölelim: $n = o(g)q + r$ eşitliğini ve $0 \leq r < o(g)$ eşitsizliklerini sağlayan q ve r sayıları vardır. Aynen biraz önce yaptığımız gibi,

$1 = g^n = g^{o(g)q + r} = (g^{o(g)})^q g^r = 1^q g^r = 1g^r = g^r$ eşitliklerini elde ederiz. Eğer $r \neq 0$ olsaydı, bu eşitlik $o(g)$ 'nin tanımıyla çelişirdi. Demek ki $r = 0$ ve $o(g)$, n 'yi bölüyor.

Şimdi de $o(g)$ 'nin n 'yi böldüğünü varsayalım: $q \in \mathbb{Z}$ için, $n = o(g)q$ olsun. Hesaplayalım:

$$g^n = g^{o(g)q} = (g^{o(g)})^q = 1^q = 1.$$

iii) $d = \text{ebob}(o(g), i)$ olsun. d , i 'yi böldüğünden, $io(g)/d$, $o(g)$ 'ye bölünür. Dolayısıyla, ikinci kısımdan dolayı,

$$(g^i)^{o(g)/d} = g^{io(g)/d} = 1.$$

Öte yandan, eğer $(g^i)^k = 1$ ise o zaman $g^{ik} = 1$ ve ikinci kısma göre $o(g)$, ik 'yi böler. Demek ki $o(g)/d$, $(i/d)k$ 'yi böler. Ama $o(g)/d$ ve i/d birbirlerine asal olduklarından, bundan $o(g)/d$ 'nin k 'yi böldüğü çıkar. □

| | | | | | | | | | | | | | | | | | | |
|----------|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| x^2 | 1 | 4 | 9 | 16 | 6 | 17 | 11 | 7 | 5 | 5 | 7 | 11 | 17 | 6 | 16 | 9 | 4 | 1 |
| x^3 | 1 | 8 | 8 | 7 | 11 | 7 | 1 | 18 | 7 | 12 | 1 | 18 | 12 | 8 | 12 | 11 | 11 | 18 |
| x^4 | 1 | 16 | 5 | 9 | 17 | 4 | 7 | 11 | 6 | 6 | 11 | 7 | 4 | 17 | 9 | 5 | 16 | 1 |
| x^5 | 1 | 13 | 15 | 17 | 9 | 5 | 11 | 12 | 16 | 3 | 7 | 8 | 14 | 10 | 2 | 4 | 6 | 18 |
| x^6 | 1 | 7 | 7 | 11 | 7 | 11 | 1 | 1 | 11 | 11 | 1 | 1 | 11 | 7 | 11 | 7 | 7 | 1 |
| x^7 | 1 | 14 | 2 | 6 | 16 | 9 | 7 | 8 | 4 | 15 | 11 | 12 | 10 | 3 | 13 | 17 | 5 | 18 |
| x^8 | 1 | 9 | 6 | 5 | 4 | 16 | 11 | 7 | 17 | 17 | 7 | 11 | 16 | 4 | 5 | 6 | 9 | 1 |
| x^9 | 1 | 18 | 18 | 1 | 1 | 1 | 1 | 18 | 1 | 18 | 1 | 18 | 18 | 18 | 1 | 1 | 1 | 18 |
| x^{10} | 1 | 17 | 16 | 4 | 5 | 6 | 7 | 11 | 9 | 9 | 11 | 7 | 6 | 5 | 4 | 16 | 17 | 1 |
| x^{11} | 1 | 15 | 10 | 16 | 6 | 17 | 11 | 12 | 5 | 14 | 7 | 8 | 2 | 13 | 3 | 9 | 4 | 18 |
| x^{12} | 1 | 11 | 11 | 7 | 11 | 7 | 1 | 1 | 7 | 7 | 1 | 1 | 7 | 11 | 7 | 11 | 11 | 1 |
| x^{13} | 1 | 3 | 14 | 9 | 17 | 4 | 7 | 8 | 6 | 13 | 11 | 12 | 15 | 2 | 10 | 5 | 16 | 18 |
| x^{14} | 1 | 6 | 4 | 17 | 9 | 5 | 11 | 7 | 16 | 16 | 7 | 11 | 5 | 9 | 17 | 4 | 6 | 1 |
| x^{15} | 1 | 12 | 12 | 11 | 7 | 11 | 1 | 18 | 11 | 8 | 1 | 18 | 8 | 12 | 8 | 7 | 7 | 18 |
| x^{16} | 1 | 5 | 17 | 6 | 16 | 9 | 7 | 11 | 4 | 4 | 11 | 7 | 9 | 16 | 6 | 17 | 5 | 1 |
| x^{17} | 1 | 10 | 13 | 5 | 4 | 16 | 11 | 12 | 17 | 2 | 7 | 8 | 3 | 15 | 14 | 6 | 9 | 18 |
| x^{18} | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

$\mathbb{Z}/19\mathbb{Z}$ 'de elemanların güçleri. Görüldüğü gibi 2, 3, 10, 13, 14 ve 15 elemanlarının derecesi 18; 4, 5, 6, 9, 16 ve 17 elemanlarının derecesi 9; 8 ve 12 elemanlarının derecesi 6; 7 ve 11 elemanlarının derecesi 3; 18'in (yani -1'in) derecesi 2 ve her zaman olduğu gibi 1'in derecesi 1.

Eğer $g \in G$ ve $X \subseteq G$ ise, G 'nin gX altkümelerini en doğal biçimde tanımlayalım: $gX = \{gx : x \in X\}$.

Önsav 5. $g \in G$ ve H , G 'nin sonlu bir grubu olsun.

i. Her $x, y \in G$ için, ya $xH \cap yH = \emptyset$ dir ya da $xH = yH$ eşitliği geçerlidir.

ii. $g \in G$ ise, $o(g)$, $|G|$ 'yi böler.

iii. Her $g \in G$ için, $g^{|G|} = 1$.

Kanıt: i) $x, y \in G$ için, $xH \cap yH \neq \emptyset$ olsun. $xH = yH$ eşitliğini göstereceğiz. Durum, x ve y 'ye göre simetrik olduğundan, sadece $xH \subseteq yH$ ilişkisini göstermek yeterli. Madem ki $xH \cap yH \neq \emptyset$, bu kümeden bir eleman alabiliriz: $xh = yh' \in xH \cap yH$ olsun. Burada, $h, h' \in H$ elbette. Şimdi, xH 'den herhangi bir eleman alalım, diyelim xh'' . O zaman,

$$xh'' = xhb^{-1}h'' = yh'b^{-1}h'' \in yH,$$

çünkü, $h', b^{-1}, h'' \in H$ olduğundan, $h'b^{-1}h'' \in H$. Böylece xH 'nin herhangi bir xh'' elemanı yH 'de olduğunu, yani $xH \subseteq yH$ ilişkisini kanıtladık.

ii) Yukarıda, H yerine $\{g^i : i \in \mathbb{Z}\}$ alalım. Önsav 4.i'den dolayı, $|H| = o(g)$.

Şimdi, eğer $x \in G$ ise, $|xH| = o(g) = |H|$ eşitliğini kanıtlıyoruz: H 'nin bir h elemanını xH 'nin xh elemanına götüren fonksiyon H 'den xH 'ye giden bir eşlemedir, nitekim xH 'nin bir z elemanını H 'nin $x^{-1}z$ elemanına yollayan fonksiyon, bu fonksiyonun tersidir. H ile xH arasında eşleme olduğundan, bu iki kümenin eleman sayısı aynıdır, yani $o(g)$ 'dir.

$x = x1$ eşitliğinden ve $1 \in H$ ilişkisinden, $x \in xH$ çıkar. Dolayısıyla xH altkümelerinin bileşimi G 'yi kaplar, yani

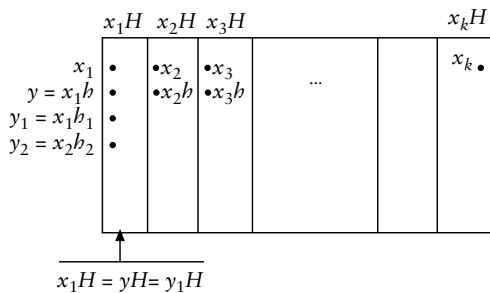
$$G = \bigcup_{x \in G} xH.$$

Önsavın birinci kısmı sayesinde x 'lerden sadece bazıları seçerek, bileşimi alınan xH altkümelerinin ayrık olduklarını varsayabiliriz: Bazı x_1, \dots, x_k için,

$$G = x_1H \cup \dots \cup x_kH.$$

(Bknz. aşağıdaki şekil.) Dolayısıyla $|G| = k|H| = ko(g)$ ve $o(g)$, $|G|$ 'yi böler.

(iii) Yukarıda kanıtlanandan doğrudan çıkar. \square



Teorem 1'in Kanıtı: $\mathbb{Z}/m\mathbb{Z}$, m elemanlı bir halkadır. Bu halkanın tersinir elemanlarının m 'ye asal n tamsayıları için \bar{n} elemanlarının olduklarını biliyoruz [MD-2004-I, sayfa 16, Sonuç 5]. Dolayısıyla,

$$(\mathbb{Z}/m\mathbb{Z})^* = \{\bar{n} : n \text{ ve } m \text{ birbirine asal}\},$$

ve bu kümenin, ϕ 'nin tanımı gereği, tam $\phi(m)$ tane elemanı var. Eğer Önsav 5.iii'te, $R = \mathbb{Z}/m\mathbb{Z}$ ve $G = (\mathbb{Z}/m\mathbb{Z})^*$ alırsak Teorem 1'in ilk kısmı kanıtlanmış olur. Son kısım, eğer $d = o(n)$ alırsak, Önsav 4.ii'den çıkar. \square

Teorem 2'yi kanıtlamak için bir önsava daha gereksiniyoruz. Kaldığımız yerden devam edelim.

Önsav 6. $u, v \in G$ olsun. Birbirine asal a ve b doğal sayıları için, $o(u) = a$ ve $o(v) = b$ ise, o zaman $o(uv) = ab$.

Kanıt: $(uv)^{ab} = u^{ab}v^{ab} = (u^a)^b(v^b)^a = 1$ eşitliği bariz. Demek ki $o(uv)$, ab 'yi bölüyor.

Şimdi $k = o(uv)$ olsun. Demek ki $(uv)^k = 1$ ve $u^k = v^{-k}$, dolayısıyla $o(u^k) = o(v^{-k})$. Ama $(u^k)^a = (u^a)^k = 1^k = 1$ eşitliğinden ve Önsav 4.ii'den $o(u^k)$ 'nin a 'yı böldüğü çıkar. Aynı nedenden, $o(v^{-k})$, b 'yi böler. a ve b birbirine asal olduklarından, bundan, $o(u^k) = o(v^{-k}) = 1$ çıkar. Yani $u^k = v^{-k} = 1$. Gene Önsav 4.ii'den, a ve b 'nin k 'yi böldükleri çıkar. Demek ki ab de k 'yi böler. Dolayısıyla $o(uv) = ab$. \square

Teorem 2'nin Kanıtı. G 'nin eleman sayısı üzerine tümevarımla kanıtlayacağız. G 'nin eleman sayısına n diyelim. G 'de derecesi n olan bir elemanın varlığını kanıtlamalıyız. İki şıkkımız var: Ya n bir asal sayının gücüdür ya da değildir. İki şıkkı ayrı ayrı irdeleyeceğiz.

Birinci Şık. Bir p asalı ve bir k doğal sayısı için, $|G| = p^k$ ise. Önsav 5.ii'ye göre, G 'nin elemanlarının derecesi bir $i = 0, 1, \dots, k$ için p^i olmak zorunludur. Derecesi p^i olan elemanlar $X^{p^i} - 1$ denkleminin kökleri olduklarından ve bir tamlık bölgesinde bir polinomun en fazla derecesi kadar kökü olabileceğinden, derecesi p^i olan en fazla p^i tane eleman vardır. Demek ki derecesi p^k 'den küçük elemanların sayısı en fazla

$$1 + p + p^2 + \dots + p^{k-1} = \frac{p^k - 1}{p - 1}$$

dir. Ama bu sayı $p^k - 1$ 'den küçüktür, yani p^k den küçüktür. Dolayısıyla G 'de derecesi p^k olan en az bir eleman vardır.

İkinci Şık: n bir asal sayının gücü değilse.

Bu durumda, n 'yi birbirine asal ve 1'den büyük iki a ve b sayısı için ab olarak yazabiliriz.

$$U = \{g \in G : g^a = 1\}$$

$$V = \{g \in G : g^b = 1\}$$

olsun. U ve V birer gruptur. Bir tamlık bölgesinde olduğumuzdan, U 'nın en fazla a , V 'nin en fazla b tane elemanı vardır. Dolayısıyla tümevarım varsayımını U 'ya ve V 'ye uygularsak sonuç Önsav 6'dan çıkar: Tümevarım varsayımına göre U 'da derecesi a olan bir u elemanı vardır; aynı nedenden V 'de derecesi b olan bir v elemanı vardır; Önsav 6'ya göre uv 'nin derecesi ab 'dir, yani n 'dir.

Teoremin ikinci kısmı Önsav 4.i'den, üçüncü kısmı da Önsav 4.iii'ten ve φ 'nin tanımından doğrudan çıkar. $\square \square$

Sonuç 7. Z/pZ halkasında (cisminde),
 $Z/pZ = \{0, g, g^2, \dots, g^{p-1}\}$
 eşitliğini sağlayan bir g elemanı vardır.

Kanıt: Z/pZ bir cisim (yani 0'a eşit olmayan her elemanın tersinir olduğu bir halka) olduğundan [MD-2004-I, sayfa 16, Sonuç 4],

$$Z/pZ = \{0\} \cup (Z/pZ)^*.$$

Sonuç, şimdi Teorem 2'den çıkar. \square

Bir sonraki sonucun kanıtı da aynen yukarıdakinin kanıtı gibidir.

Sonuç 8. Eğer F sonlu bir cisimse (yani 0 dışındaki her elemanın tersinir olduğu bir halkaysa), o zaman bir n tamsayısı ve bir $g \in F$ için,

$$F = \{0, g, g^2, \dots, g^{n-1}\}.$$

Ne yazık ki matematik bilgisi MD'yle sınırlı olan okur, bu aşamada, asal p 'ler için Z/pZ dışında sonlu bir cisim bilemez. Bunlardan başka cisimlerin varlığını bir başka sayımızda görürüz.

Sonuç 9. [Wilson Teoremi]. Asal bir p sayıyı,
 $(p - 1)! + 1$

sayısını böler.

Kanıt: Eğer $p = 2$ ise, sonuç bariz. Bundan böyle p 'nin 2 olmadığını varsayalım.

x , $(p - 1)!$ tamsayısının Z/pZ halkasındaki imgesi olsun. $x = -1$ eşitliğini göstermemiz gerekiyor.

$(p - 1)!$, 1'den $p - 1$ 'e kadar olan tüm sayıların çarpımı olduğundan, x , Z/pZ halkasının 0 olmayan tüm elemanlarının çarpımıdır. Demek ki Sonuç 7'den, derecesi $p - 1$ olan bir $g \in Z/pZ$ için, $x = gg^2 \dots g^{p-1} = g^{1+2+\dots+(p-1)} = g^{p(p-1)/2} = g^{(p-1)/2}$ $\neq 1$ çıkar. Demek ki, $x \neq 1$, $x^2 = g^{p-1} = 1$ ve

$$0 = x^2 - 1 = (x - 1)(x + 1)$$

Bir tamlık bölgesinde olduğumuzdan, bunlardan $x = -1$ çıkar. \blacklozenge

Wilson Teoremi'nin Başka Bir Kanıtı

Teorem [Wilson]. Eğer p bir asalsa, p ,
 $(p - 1)! + 1$

sayısını böler, yani, $(p - 1)! \equiv -1 \pmod{p}$ dir.

Kanıt: $(p - 1)!$, 1'den $p - 1$ 'e kadar olan tüm sayıların çarpımıdır. Dolayısıyla, bu çarpım, Z/pZ halkasında, Z/pZ 'nin sıfır olmayan tüm elemanlarının çarpımı olan

$$\alpha = \prod_{x \neq 0} x$$

elemanına tekabül eder. Z/pZ 'nin bu α elemanının -1 'e eşit olduğunu kanıtlamalıyız.

Z/pZ 'de her $x \neq 0$ için bir x^{-1} vardır. Dolayısıyla eğer $x \neq x^{-1}$ ise, x ve x^{-1} elemanları bu çarpımda sadeleşirler ve geriye sadece $x = x^{-1}$, yani $x^2 = 1$, yani $(x - 1)(x + 1) = 0$ eşitliğini sağlayan elemanların çarpımı kalır. Bir bölgede olduğumuzdan, Z/pZ 'nin sadece $x = 1$ ve $x = -1$ elemanları bu eşitliği sağlar. Demek ki, Z/pZ 'nin α elemanı, 1'le -1 'in çarpımına, yani -1 'e eşittir. \square

Yukarıdaki yazıda Sonuç 9 olarak da kanıtlanan bu teoremi ilk olarak John Wilson 1770'de ortaya atmış ama kanıtı daha sonra Lagrange tarafından 1773'te yayımlanmıştır.

Fermat'ın Küçük Teoremi'nin aksine, Wilson Teoremi'ndeki koşul bir sayının asal olması için yeter ve gerek koşuldur. Nitekim, eğer $n \neq 4$ ise ve bir asal sayı değilse, o zaman,

$$(n - 1)! \equiv 0 \pmod{n}.$$

Bunun kanıtı oldukça kolaydır: Eğer n bir asalın karesi değilse, o zaman 1'den büyük iki farklı a ve b sayısı için $n = ab$ 'dir ve denklik barizdir; eğer n , bir asalın karesiyse, diyelim $n = p^2$ ise ve $p \neq 2$ ise, o zaman, modülo p , p ve $2p$ 'nin çarpımı 0'dır.

Öte yandan, $(4 - 1)! = 3! = 6 \equiv 2 \pmod{4}$.

Aıştırma. Eğer p , $4k + 1$ biçiminde yazılan bir asalsa, o zaman $[(2k)!]^2 \equiv -1 \pmod{p}$. \blacklozenge