

FERMAT VE EULER TEOREMLERİ

Emre Alkan *

Bu yazıda sayılar teorisinin klasikleşmiş iki teoremini verip, ilginç kanıtlarını yapacağız.

Teorem. (Fermat) p bir asal sayı ve $p \nmid a$ olsun. $a^{p-1} \equiv 1 \pmod{p}$ olur.

Kolayca görüleceği üzere buna eşdeğer bir sonuç şöyledir.

Teorem. p asal bir sayı ise $a^p \equiv a \pmod{p}$ olur.

Kanıt 1. Her a pozitif sayısı için $a^p \equiv a \pmod{p}$ olduğunu göstereceğiz. Tümevarım $a = 1$ için doğru. $a^p \equiv a \pmod{p}$ olsun. $(a+1)^p \equiv a+1 \pmod{p}$ olduğunu görelim. $(a+1)^p \equiv a^p + 1 \pmod{p}$ olduğundan tümevarım tamamlanır.

Kanıt 2. $p \nmid a$ olsun ve $a, 2a, 3a, \dots, (p-1)a$ sayılarını ele alalım. $i \neq j$ ve $i, j \in \{1, 2, \dots, p-1\}$ olmak üzere $ia \equiv ja \pmod{p}$ ise $p \nmid a$ olduğundan $i = j$ çelişkisi elde edilir. Böylece

$$a(2a)(3a) \cdots (p-1)a \equiv (p-1)! \pmod{p}$$

ve $(p-1)! a^{p-1} \equiv (p-1)! \pmod{p}$ olur. p ve $(p-1)!$ aralarında asal olduğundan $a^{p-1} \equiv 1 \pmod{p}$ elde edilir.

Şimdi bu teoremin bir genellemesini vereyim.

Teorem. (Euler) $\phi(m)$ bir m sayısından küçük ve m ile arasında asal olan sayıların sayısı olsun. $(a, m) = 1$ ise $a^{\phi(m)} \equiv 1 \pmod{m}$ olur.

Kanıt 1. $x_1, x_2, \dots, x_{\phi(m)}$ sözü edilen sayılar olsun. $(ax_i, m) = 1$ olur. Ayrıca $ax_i \equiv ax_j \pmod{m}$, $i \neq j$, ise $x_i \equiv x_j \pmod{m}$ çelişkisi elde edilir. Böylece

$$(ax_1)(ax_2) \cdots (ax_{\phi(m)}) \equiv x_1 x_2 \cdots x_{\phi(m)} \pmod{m}$$

ve m ile $x_1 x_2 \cdots x_{\phi(m)}$ aralarında asal olduğundan $a^{\phi(m)} \equiv 1 \pmod{m}$ elde edilir.

Kanıt 2. m sayısını asal çarpanlarına $m = \prod p^\alpha$ şeklinde ayıralım. Çarpımdaki her p^α için $a^{\phi(m)} \equiv 1 \pmod{p^\alpha}$ olduğunu görmek yeterlidir. Bu ise, $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ olduğundan.

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha}$$

olduğunu görmeye denktir. Şimdi şunu göstereyim. $\alpha > 0$ ve $m \equiv 1 \pmod{p^\alpha}$ ise $m^p \equiv 1 \pmod{p^{\alpha+1}}$ olur. $m = 1 + kp^\alpha$ alalım.

$$\begin{aligned} m^p &= (1 + kp^\alpha)^p \\ &= (kp^\alpha)^p + \binom{p}{1}(kp^\alpha)^{p-1} + \binom{p}{2}(kp^\alpha)^{p-2} \\ &\quad + \cdots + \\ &\quad + \binom{p}{p-2}(kp^\alpha)^2 + \binom{p}{p-1}kp^\alpha + 1, \end{aligned}$$

$1 \leq k \leq p-1$ için $p \mid \binom{p}{k}$ ve $\alpha + 1 < 2\alpha + 1 < 3\alpha + 1 < \cdots$ olduğundan göstermek istediğimiz $m^p \equiv 1 \pmod{p^{\alpha+1}}$ elde edilir. $a^{p-1} \equiv 1 \pmod{p^\alpha}$ olduğunu biliyoruz. Az önceki yardımcı sonucu kullanarak

$$a^{p(p-1)} \equiv 1 \pmod{p^2}$$

$$a^{p^2(p-1)} \equiv 1 \pmod{p^3}$$

⋮

ve

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha}$$

elde ederiz.

Kanıt 3. Grup kavramından yararlanacağız.

$$M = \{ k : (k, m) = 1 \text{ ve } 1 \leq k < m \}$$

olsun. M üzerinde şöyle bir \cdot işlemi tanımlayalım. $a \in M$ ve $b \in M$ alalım. $1 \leq c < m$ için $ab \equiv c \pmod{m}$ ise $a \cdot b = c$ olsun. M 'nin bir grup olduğunu gözleyeceğiz. Birleşme özelliği doğal olarak var. M 'nin kapalı olduğunu görelim. $a, b \in M$ ise $a \cdot b = c \in M$ olduğunu

* Boğaziçi Üniversitesi Matematik Bölümü öğrencisi

görelim. $(a, m) = (b, m) = 1$, $1 \leq c < m$, $ab \equiv c \pmod{m}$, $m \mid ab - c$ ve $(m, c) > 1$ ise $q > 1$ için $q \mid ab$ ve $q \mid m$ elde edilir. Fakat $(ab, m) = 1$ olduğundan bir çelişki elde ederiz. $a \in M$ için $a1 \equiv a \pmod{m}$ olduğundan 1 etkisiz elemandır. Ters elemanın varlığı için, $a \cdot a^{-1} = 1$, yani $ax \equiv 1 \pmod{m}$ olacak şekilde bir x lazım. $(a, m) = 1$ ise $ax_0 + my_0 = 1$ olacak şekilde $x_0, y_0 \in \mathbb{Z}$ vardır (bu sayılar Öklit algoritmasıyla bulunabilir) $ax_0 \equiv 1 \pmod{m}$ 'dir. $x_0 \equiv z_0 \pmod{m}$ ve $1 \leq z_0 < m$ olacak şekilde bir z_0 alırsak $a^{-1} = z_0$ olur. M bir gruptur. Bu grubun eleman sayısı $\phi(m)$ 'dir. Bir $a \in M$ alalım. M sonlu olduğu için $a^t = 1$ olacak şekilde minimum bir t sayısı vardır. Böylece $1, a^1, a^2, \dots, a^{t-1}$ elemanları M 'nin bir çembersel alt grubunu oluştururlar. Alt grubun eleman sayısı $\phi(m)$ 'nin bir böleni olduğundan $a^{\phi(m)} = 1$ ve $a^{\phi(m)} \equiv 1 \pmod{m}$ elde edilir.

Son olarak $\phi(x)$ fonksiyonundan söz edelim.

Teorem. $(a, b) = 1$ ise $\phi(ab) = \phi(a) \cdot \phi(b)$.

Kanıt. $s_1, s_2, \dots, s_{\phi(b)}$ sayıları b ile aralarında asal sayılar, $r_1, r_2, \dots, r_{\phi(a)}$ ise a ile aralarında asal sayılar olsun. $as_i + br_j$ sayılarına \pmod{ab} 'de bakalım.

$$as_i + br_j \equiv as_{i'} + br_{j'} \pmod{ab}$$

olur ve buradan da

$$\begin{aligned} s_i &\equiv s_{i'} \pmod{b} \\ r_j &\equiv r_{j'} \pmod{a} \\ i &= i' \\ j &= j' \end{aligned}$$

elde edilir. $(as_i + br_j, ab) = d$ olsun. $d \mid as_i + br_j$, $d \mid ab$, $p \mid d$ ve p asal olacak şekilde bir p alalım. $p \mid ab$ ise $p \mid a$ veya $p \mid b$ 'dir. $p \mid as_i + br_j$ ve $p \mid a$ ise $p \mid br_j$ ve $(a, r_j) = 1$ vereceğinden $p \mid b$ olur, fakat bu mümkün değil. $p \mid b$ hali de aynı; dolayısıyla $d = 1$ olmalı. Böylece $\phi(a) \cdot \phi(b) \leq \phi(ab)$ elde ettik. Eğer $(x, ab) = 1$

ise $(x, a) = 1$ ve $(x, b) = 1$ olduğu görülebilir. Böylece $\phi(ab) \leq \phi(a) \cdot \phi(b)$ ve $\phi(ab) = \phi(a) \cdot \phi(b)$ elde ederiz, ve kanıt sona erer.

$\phi(x)$ fonksiyonu çarpımı koruyan bir aritmetik fonksiyon örneğidir.

$$m = p_1^{r_1} \cdots p_k^{r_k}$$

ise,

$$\phi(m) = \phi(p_1^{r_1}) \cdots \phi(p_k^{r_k})$$

elde edilir. Kolayca

$$\phi(p_i^{r_i}) = p_i^{r_i} \left(1 - \frac{1}{p_i}\right)$$

olduğundan

$$\phi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$$

elde edilir.

Teorem. $\sum_{d \mid n} \phi(d) = n$ olur.

Kanıt. Sağ taraf $1 \leq x \leq n$ şeklindeki sayıların sayısı; şimdi bu sayıları farklı bir şekilde sayalım. $(x, n) = d$ ise $\left(\frac{x}{d}, \frac{n}{d}\right) = 1$ olur. Bu tür sayıların sayısı $\phi\left(\frac{n}{d}\right)$ 'dir. Böylece

$$n = \sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)$$

elde ederiz.

$\phi(a) \cdot \phi(b) = \phi(ab)$ olduğu kullanılarak da

$$\sum_{d \mid n} \phi(d) = n$$

olduğu gösterilebilir. Bunu okuyucuya bırakacağız.

KAYNAKÇA

- [1] G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers*, 5. baskı, Oxford.