FERMAT VE EULER TEOREMLERİ ÜZERİNE UYGULAMALAR

Emre Alkan *

Fermat ve Euler teoremlerini daha önce kanıtlarıyla beraber vermiştik [1]. Bu teoremlerin kullanılışını sergilemek amacıyla bu yazıda bir dizi uygulama yapacağız. Bu yazıda sayı kelimesi tamsayı anlamında kullanılacak.

Lemma. *$(a,m) = 1$ olsun. $a^x \equiv 1 \pmod{m}$ olacak şekildeki en küçük x sayısı n olsun. $a^k \equiv 1 \pmod{m}$ ise $n \mid k$ olur.*

Kanıt. $a^x \equiv 1 \pmod{m}$ olacak şekilde en küçük bir x sayısı vardır, çünkü Euler teoremiyle $a^{\phi(m)} \equiv 1 \pmod{m}$ olduğunu biliyoruz. Bu en küçük sayı n olsun. Bölme algoritmasıyla $k = qn + r$ $(0 \leq r < n)$ yazılabilir. Böylece $a^k \equiv a^{qn+r} \equiv a^r \equiv 1 \pmod{m}$ elde edilir. n en küçük pozitif sayı olduğundan $r = 0$, dolayısıyla $n \mid k$ elde edilir.

Problem. *p bir asal sayı ve $(p,m) = 1$ olmak üzere $n = p^k m$ olsun. $p \mid 2^n - 1$ ise, $p \mid 2^m - 1$ olduğunu gösteriniz.*

Çözüm. $n = pt$ olsun.

$$2^{tp} - 1 = (2^p - 1)(2^{(t-1)p} + 2^{(t-2)p} + \cdots + 2^p + 1).$$

Fermat teoremiyle $2^p \equiv 2 \pmod{p}$ olduğundan p, $2^p - 1$'i bölmez. Böylece

$$p \mid 2^{(t-1)p} + 2^{(t-2)p} + \cdots + 2^p + 1.$$

Kolayca

$$2^{(t-1)p} + 2^{(t-2)p} + \cdots + 2^p + 1 \equiv$$
$$2^{t-1} + 2^{t-2} + \cdots + 2 + 1 \equiv 2^t - 1 \pmod{p}$$

olduğundan, $p \mid 2^t - 1$ elde edilir. Bu sonucu yineleyerek $p \mid 2^m - 1$ elde ederiz.

Problem. *$n > 1$ ise n, $2^n - 1$'i bölmez.*

Çözüm. $n > 1$ ise n asal çarpanlarına ayrılabilir. En küçük asal çarpan p olsun. $n = p^k p_1^{k_1} \cdots p_r^{k_r}$ yazalım. $n \mid 2^n - 1$ kabul edelim. Böylece $2^n \equiv 1 \pmod{p}$ ve Fermat teoremiyle $2^{p-1} \equiv 1 \pmod{p}$ elde ederiz. Lemma ile $2^k \equiv 1 \pmod{p}$ olacak şekilde en küçük $k > 1$ sayısı vardır. $k = 1$ olamaz; $k \mid n$ ve $k \mid p - 1$ olur. Fakat böyle bir k sayısının olamıyacağı açıktır. Dolayısıyla n, $2^n - 1$'i bölmez.

Problem. *$n_1, n_2, \ldots, n_k$ pozitif tamsayıları için $n_1 \mid 2^{n_2} - 1$, $n_2 \mid 2^{n_3} - 1$, $\ldots$, $n_{k-1} \mid 2^{n_k} - 1$ ve $n_k \mid 2^{n_1} - 1$ ise, $n_1 = n_2 = \cdots = n_k = 1$ olduğunu gösteriniz.*

Çözüm. $n_1 > 1$ olsun. n_1 asal çarpanlarına ayrılabilir. n_1'in en küçük asal çarpanı p_1 olsun. $p_1 \mid 2^{n_2} - 1$, yani $2^{n_2} \equiv 1 \pmod{p)_1}$ ve $2^{p_1 - 1} \equiv 1 \pmod{p)_1}$ Fermat teoremi sayesinde yazılabilir. Lemma ile $2^d \equiv 1 \pmod{p)_1}$ olacak şekilde en küçük bir $d > 1$ sayısı bulabiliriz. Buradan şu elde edilir: Öyle bir p_2 asal sayısı vardır ki $p_2 \mid n_2$ ve $p_2 \mid p_1 - 1$. Bu akıl yürütme devam ettirilerek şöyle bir asal sayılar dizisi bulunur: $p_3 \mid n_3$ ve $p_3 \mid p_2 - 1$, $\ldots$, $p_k \mid n_k$ ve $p_k \mid p_{k-1} - 1$. Ve nihayet $n_k \mid 2^{n_1} - 1$ olduğundan $p_k \mid 2^{n_1} - 1$ olur ve bundan dolayı öyle bir asal $p' \mid n_1$ vardır ki $p' \mid p_k - 1$ olur. Böylece $p_1 - 1 > p_2$, $p_2 - 1 > p_3$, $\ldots$, $p_k - 1 > p_k$ ve $p_k - 1 > p'$ elde edilir. Fakat $p' \geq p_1$ olduğundan bu durum mümkün değildir. Dolayısıyla $n_1 = 1$ böylece $n_1 = n_2 = \cdots = n_k = 1$ elde edilir.

Problem. *Bir m pozitif sayısı veriliyor. M, $2^k - 2^m - 1$ $(k = 1, 2, \ldots)$ şeklindeki sayıların kümesi olsun. M'nin herhangi iki elemanı arasında asal bir sonsuz alt kümesi olduğunu gösteriniz.*

Çözüm. İstenen alt kümeyi tümevarımla kuracağız. Herhangi bir $a_1 \in M$ ile başlıyalım. Kabul edelim ki ilk n sayı $a_1, a_2, \ldots, a_n \in M$ şartını sağlasın. a_{n+1} için, $(a_{n+1}, a_i) = 1$ $(i = 1, 2, \ldots, n)$ olmalıdır. $a_1, a_2, \ldots, a_n$ elemanlarının hepsinin asal çarpanlara ayrılışında geçen

* Boğaziçi Üniversitesi Matematik Bölümü öğrencisi

asal sayılar $p_1, p_2, \ldots, p_r$ olsun.

$$a_{n+1} = 2^{(p_1-1)(p_2-1)\cdots(p_r-1)} - 2^m - 1$$

olarak seçelim. Eğer $(a_{n+1}, a_i) > 1$ ise $\{1, 2, \ldots, r\}$ içinde bir j için $p_j \mid a_{n+1}$ olmalıdır. Kolayca

$$2^{(p_1-1)(p_2-1)\cdots(p_r-1)} \equiv 2^m + 1 \pmod{p_j}$$

elde edilir. Öte yandan $2^{p_j-1} \equiv 1 \pmod{p_j}$ Fermat teoremiyle yazılabilir. Bu iki denklikten $2^m + 1 \equiv 1 \pmod{p_j}$ ve $p_j = 2$ elde edilir ki bu mümkün değildir. $(a_{n+1}, a_i) = 1$ olur. Dolayısıyla tümevarımla M'nin böyle bir sonsuz alt kümesinin varlığı anlaşılır.

Problem. *(1990 Uluslararası Matematik Olimpiyadı) $n^2 \mid 2^n + 1$ olacak şekildeki tüm $n > 1$ sayılarını bulunuz.*

Çözüm. $n^2 \mid 2^n + 1$ ise $n \mid 2^n + 1$ olur. $n > p$ ise $3 \mid n$ olduğunu görelim. n'nin en küçük asal çarpanı p olsun. $2^{2n} \equiv 1 \pmod{p}$ ve $2^{p-1} \equiv 1 \pmod{p}$ Fermat teoremiyle yazılabilir. $2^d \equiv 1 \pmod{p}$ olacak şekilde en küçük bir $d > 1$ sayısı vardır. $d \mid 2n$ ve $d \mid p - 1$'den kolayca $d = 2$ elde edilir. Dolayısıyla $p = 3$ ve $3 \mid n$ olur. $n = 3^k d$, $(d, 3) = 1$ ve $k \geq 1$ alalım. $3^{2k} \mid 2^{3^k d} + 1$ yazılabilir. Çarpanlara ayırma ile

$$2^{3^k d} + 1 = (2^d + 1) \prod_{t=0}^{k-1} (2^{3^t 2d} - 2^{3^t d} + 1)$$

yazılabilir. Şunları gözleyelim:

$$2^{3^t 2d} - 2^{3^t d} + 1 \equiv 2^{3^t d} - 2 \equiv 0 \pmod{3}$$

ve $2^{3^t d} \equiv 2 \pmod{9}$ ise, $(-1)^d \equiv 2 \pmod{9}$ olur ki bu mümkün değildir. Öte yandan $(d, 3) = 1$ olduğundan $2^d \equiv -1 \pmod{3}$ ve $2^d \not\equiv -1 \pmod{9}$ olur. Böylece $2^{3^k d} + 1$, tam olarak 3^{k+1} ile bölünür. Kolayca $2k \leq k + 1$ ve $k \geq 1$'den $k = 1$ elde ederiz. $n = 3d$ şeklinde olmalıdır. $d > 1$ ise d'nin en küçük asalçarpanı p_1 olsun. Kolayca $2^{2 \cdot 3d} \equiv 1 \pmod{p_1}$ ve $2^{p_1-1} \equiv 1 \pmod{p_1}$ Fermat teoremiyle yazılabilir. Öte yandan $p_1 \geq 5$ olmalıdır. $2^a \equiv 1 \pmod{p_1}$ olacak şekilde en küçük bir $a > 1$ sayısı vardır. $a \mid 6d$ ve $a \mid p - 1$ olduğundan $a = 2$, 3 veya 6 olur. $a = 2$ ise $p_1 = 3$ olur. $a = 3$ veya 6 ise de $p_1 = 7$ elde edilir. Fakat her $s \in \mathbb{Z}^+$ için $7 \nmid 2^s + 1$ olduğundan, $d > 1$ olamaz; $d = 1$ elde edilir. $n^2 \mid 2^n + 1$ olacak şekildeki tek sayı $n = 3$ olarak bulunur.

Problem. *a ve b pozitif sayıları için, $2a - 1$, $2b - 1$ ve $a + b$ asal sayılar iseler, $a + b$'nin $a^b + b^a$ ve $a^a + b^b$ sayılarını bölmediğini gösteriniz.*

Çözüm. $(a, a + b) = (b, a + b) = (ab, a + b) = 1$ ve

$$a+b \mid (a^a+b^b)(a^b+b^a) = a^{a+b}+b^{a+b}+(ab)^a+(ab)^b$$

olur. $a > b$ ve Fermat teoremiyle

$$a^{a+b} + b^{a+b} \equiv a + b \equiv 0 \pmod{a + b}$$

kabul edebiliriz. Kolayca $(ab)^{a-b} \equiv -1 \pmod{a+b}$, yani $(ab)^{2a-2b} \equiv 1 \pmod{a + b}$ elde edilir. Öte yandan yine Fermat teoremiyle $(ab)^{a+b-1} \equiv 1 \pmod{a + b}$ olur. $(ab)^d \equiv 1 \pmod{a + b}$ sağlayan en küçük bir d sayısı vardır. $d = 1$ ise $ab \equiv 1 \pmod{a + b}$ ve $(ab)^{a-b} \equiv 1 \pmod{a + b}$ olur ki bu mümkün değildir. $d \mid 2a - 2b$ ve $d \mid a + b - 1$'den kolayca $d \mid 2(2a - 1)$ ve $d \mid 2(2b - 1)$, $2a - 1$ ve $2b - 1$ de asal olduğundan $d = 2$ buluruz. $(ab)^2 \equiv 1 \pmod{a + b}$ ve $ab \not\equiv 1 \pmod{a + b}$ olduğundan $ab \equiv -1 \pmod{a + b}$, yani $a + b \mid ab + 1$ elde edilir. Öte yandan $a+b \mid a^2+ab$, $a+b \mid (a-1)(a+1)$, ve $a+b$ asal olduğundan $a + b \mid a - 1$ veya $a + b \mid a + 1$ elde edilir ki her iki durum da mümkün değildir.

Problem. *a, m pozitif sayıları için $x_0 = 1$ ve $x_{n+1} = a^{x_n}$ olacak şekilde bir x_n dizisi tanımlanıyor. Öyle bir N pozitif sayısının varlığını gösteriniz ki $N \leq h \leq k$ için $x_h \equiv x_k \pmod{m}$ olsun* [7].

Çözüm. $\langle a \rangle = \{a, a^2, a^3, \ldots\}$ kümesi $\pmod{m}$ de periyodik olur. Periyot uzunluğu b olsun. Bu kümede periyodik olmayan terimler olabilir, ama belli bir sınırdan sonra kümenin kendisi periyodik olmalıdır. Belli bir a^k'den sonra

$$x_h = a^{a^{a^{\cdot^{\cdot^{\cdot}}}}} \qquad \text{ve} \qquad x_k = a^{a^{a^{\cdot^{\cdot^{\cdot}}}}}$$

olduğundan $x_h = x_k \pmod{m}$ ancak ve ancak $x_{h-1} \equiv x_{k-1} \pmod{b}$ elde ederiz. $(a, m) > 1$ ise $a^x \equiv 1 \pmod{m}$ olacak şekilde bir x pozitif sayısı yoktur. Böylece $b < m$ olur. Öte yandan $(a, m) = 1$ ise, Euler teoremiyle $a^{\phi(m)} \equiv 1 \pmod{m}$ olur ki bundan yine $b \leq \phi(m) < m$ elde edilir. Dolayısıyla bu akıl yürütme tekrarlanarak, elde edilen modül tabanları azalan bir dizi oluştururlar. Sonlu sayıda adımdan sonra (diyelim ki t'yinci adım) $x_{h-t} \equiv x_{k-t} \pmod{2}$ eşdeğer koşulu elde edilir. Fakat $\pmod{2}$'de dizinin tüm terimlerinin, x_0 terimi hariç, denk

olacağı açıktır. Eğer N sayısı, $N \geq t$ olacak şekilde seçilirse istenen $N \leq h \leq k$ için $x_h \equiv x_k \pmod{m}$ elde edilir.

Şimdi $N \leq h \leq k$ ve $x_h \equiv x_k \pmod{m}$ olacak şekilde bir N bulmak istiyoruz. Azalan bir modül dizisi bulduk. Böylece (mod 2)'ye indirgeme en fazla m adımda biter. Fakat her adımda bir sonraki modüle geçebilmek için bazı şartlar vardır. $x_h \equiv x_k \pmod{m}$ ise $x_{h-1} \equiv x_{k-1} \pmod{b}$, $a^i \equiv a^j \pmod{m}$ ve $i < j$ olacak şekilde en küçük sayı i ise, $x_{h-1} \geq i$ olmalıdır ve bu şart her adımda olmalıdır. Elde edilen azalan modül dizisi $b, b_1, b_2, \ldots, b_s$ olsun. Her defasında $a^i \equiv a^j \pmod{b_i}$ ve $i < j$ olacak şekildeki en küçük i sayısı için $i < b_i < m$ olur. Şimdi başlangıç için x_h'yi $x_h = a^{a^{a^{\cdot^{\cdot^{\cdot}}}}}$ olarak seçebiliriz. $a^{a^{a^{\cdot^{\cdot^{\cdot}}}}} > m$ olacak şekilde bir x sayısı bulabiliriz. İndirgeme en fazla m adım sürebileceğinden (her adımda bir a eksiliyor), x_h'yi $x_h = a^{a^{a^{a^{\cdot^{\cdot^{\cdot}}}}}}$ olarak seçeriz. $h - 1 = x + m$ olacağından $N = x + m + 1$ almak işimizi görür.

Problem. *a, b pozitif sayılar ve p asal olmak üzere, $a^p \equiv b^p \pmod{p}$ ise, $a^p \equiv b^p \pmod{p^2}$ olduğunu gösteriniz.*

Çözüm. Fermat teoremiyle $a^p \equiv a \pmod{p}$ ve $b^p \equiv b \pmod{p}$ olduğundan, $a \equiv b \pmod{p}$ ve $p \mid a - b$ elde ederiz.

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1})$$

ve $i = 1, 2, \ldots, p$ için $a^{p-i}b^{i-1} \equiv a^{p-1} \equiv 1 \pmod{p}$ olduğundan,

$$p \mid \frac{a^p - b^p}{a - b}$$

elde edilir. Dolayısıyla $a^p \equiv b^p \pmod{p^2}$ olur. Burada $(a, p) = (b, p) = 1$ olduğunu kabul ettik. Eğer $p \mid a$ ve $p \mid b$ ise $p^p \mid a^p - b^p$ olur ki $p \geq 2$ olduğundan yine $a^p \equiv b^p \pmod{p^2}$ elde ederiz.

Şimdi Euler teoreminin bir genellemesini vereceğiz. Önce bir Lemma.

Lemma. *n pozitif sayısının pozitif bir böleni d ise, $n - \phi(n) \geq d - \phi(d)$ olur.*

Kanıt. Sol taraf n ile ortak asal böleni olan sayıların sayısıdır. Sağ taraf da aynışekilde belirtilebilir. $d \mid n$ olduğundan d ile ortak asal böleni olan bir sayının, n ile de ortak asal böleni olacaktır.

Teorem. *Herhangi a ve m pozitif sayıları için $a^m \equiv a^{m-\phi(m)} \pmod{m}$ olur.*

Kanıt. $m \mid a^{m-\phi(m)}(a^{\phi(m)} - 1)$ olduğunu göreceğiz. $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_k^{\beta_k}$ olacak şekilde çarpanlara ayıralım. Burada $p_1, p_2, \ldots, p_r$, a'nın da asal bölenleri olsunlar. $i \in \{1, 2, \ldots, k\}$ için Euler teoremiyle $a^{\phi(q_i^{\beta_i})} - 1 \mid a^{\phi(m)} - 1$ ve $q_i^{\beta_i} \mid a^{\phi(q_i^{\beta_i})} - 1$ olduğundan, $q_i^{\beta_i} \mid a^{m-\phi(m)}(a^{\phi(m)} - 1)$ elde ederiz. Şimdi bir $p_i^{\alpha_i}$ alalım. $p_i^{\alpha_i} \mid a^{m-\phi(m)}$ olduğunu göstereceğiz. $p_i \mid a$ olduğundan $\alpha_i \leq m - \phi(m)$ olduğunu görmek yeter. Lemma ile $m - \phi(m) \geq p_i^{\alpha_i} - \phi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}$ elde ederiz. $p_i \geq 2$ olduğundan $2^{\alpha_i - 1} \geq \alpha_i$ olduğunu görmek yeter. $n \geq 1$ için $2^{n-1} \geq n$ olduğu tümevarımla gösterilebilir.

Şu sonucu daha önce göstermiştik [2].

Teorem. *Tamsayı katsayılı, sabit olmayan bir $p(n)$ polinomu, belli bir sınırdan sonraki her n sayısı için asal olamaz.*

Bu sonucu benzer daha ilginç bir teoremi göstereceğiz.

Teorem. *$1 \leq a_1 < a_2 < \cdots < a_m$ tamsayılar ve $Q_j(x)$'ler tamsayı katsayılı polinomlar olsun.*

$$f(n) = Q_1(n)a_1^n + Q_2(n)a_2^n + \cdots + Q_m(n)a_m^n$$

ise, $f(n)$ sonsuz sayıda tamsayı n için asal değerler almaz. ($n \to \infty$ iken $f(n) \to \infty$ olduğu kabul ediliyor.)

Kanıt. Tersine $f(n)$'nin belli bir sınırdan sonra hep asal olduğunu kabul edelim. $f(n) \to \infty$ olduğundan öyle bir n bulunabilir ki p asal olmak üzere, $f(n) = p > a_m$ olsun. Her k tamsayısı için $Q_i(n + kp) \equiv Q_i(n) \pmod{p}$ olduğunu biliyoruz. Öte yandan $(a_i, p) = 1$ olduğundan, Fermat teoremiyle $a_i^{p-1} \equiv 1 \pmod{p}$ yazabiliriz. Bu iki sonucu aynı anda kullanabilmek için, $f(n + kp(p-1))$ sayılarına bakılırsa,

$$f(n + kp(p-1)) \equiv f(n) \pmod{p}$$

olduğu görülür ki f hep asal kabul edildiğinden, $f(n + kp(p-1)) = p$ elde edilir. Bu ise $n \to \infty$ iken $f(n) \to \infty$ olmasıyla çelişir.

Şimdi Fermat teoreminin tersinden bahsedeceğiz. a, m pozitif sayıları için, $a^{m-1} \equiv 1 \pmod{m}$ ise m asal olur mu? Bunun her zaman doğru olmadığını görelim.

Teorem. *a pozitif bir sayı ise, $a^{m-1} \equiv 1 \pmod m$ olacak şekilde asal olmayan sonsuz tane m sayısı bulunabilir.*

Kanıt. $(a,p) = 1$ olacakşekilde bir $p \geq 3$ asal sayısı alalım.

$$m = \frac{a^{2p}-1}{a^2-1} = \left(\frac{a^p-1}{a-1}\right)\left(\frac{a^p+1}{a+1}\right)$$

olsun; m asal değildir. Kolayca, $a^{2p} \equiv 1 \pmod m$ olur. Eğer $2p \mid m-1$, eşdeğer olarak

$$2p(a^2-1) \mid a^2(a^{p-1}-1)(a^{p-1}+1)$$

olmasını sağlarsak teorem kanıtlanmış olacak. Fermat teoremiyle, $p \mid a^{p-1}-1$. Öte yandan $p-1$ çift olacağından $a^2-1 \mid a^{p-1}-1$, ve p üzerine $p \nmid a^2-1$ şartı da getirilirse, $p(a^2-1) \mid a^{p-1}-1$ elde edilir. $2 \mid a^2(a^{p-1}+1$ olduğu açıktır. $p \nmid a(a^2-1)$ olacakşekilde sonsuz tane p seçimi bulunacağından teorem elde edilir.

Tanım. *$a^{m-1} \equiv 1 \pmod m$ ve m asal olmayacak şekildeki m sayılarına yalancı asal denir.*

Şu sonuç Fermat teoreminin tersi olarak kabul edilebilir.

Teorem. *$a^{m-1} \equiv 1 \pmod m$, $x < m-1$ ve $x \mid m-1$ için $a^x \not\equiv 1 \pmod m$ ise, m asaldır.*

Kanıt. $a^d \equiv 1 \pmod m$ olacak şekilde en küçük bir d sayısı vardır. $d \mid m-1$ olacağından $d = m-1$ olmalıdır. Öte yandan $(a,m) = 1$ olduğundan, Euler teoremiyle $a^{\phi(m)} \equiv 1 \pmod m$ yazılabilir ve kolayca $m-1 \mid \phi(m)$ olur. Fakat $\phi(m) \leq m-1$ olduğundan $\phi(m) = m-1$ olur ki bu m'in asal olması demektir.

Problem. *$n > 3$ bir tek sayı olsun. $p \mid 2^{\phi(n)}-1$ ve $p \nmid n$ olacakşekilde bir p asal sayısının var olduğunu gösteriniz* [5].

Çözüm. $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ ve p_i'ler asal olsun.

$$\phi(n) = p_1^{k_1-1}p_2^{k_2-1}\cdots p_r^{k_r-1}(p_1-1)\cdots(p_r-1)$$

olur. $2^{(p_1-1)\cdots(p_r-1)}-1$ sayısını ele alalım. Bu sayının $p_1, p_2, \ldots, p_r$ sayılarından farklı bir asal böleni olduğunu gösterirsek,

$$2^{(p_1-1)\cdots(p_r-1)}-1 \mid 2^{\phi(n)}-1$$

olacağından problem sonuçlanmış olur. Eğer her $i = 1,2,\ldots,r$ için $p_i \geq 5$ sağlanırsa, kolayca $3 \mid 2^{(p_1-1)\cdots(p_r-1)}-1$ elde edilir. Bu halde işimiz biter.

Öteki durumda genelliği bozmadan $p_1 = 3$ kabul edelim. Elimizdeki sayı $2^{2(p_2-1)\cdots(p_r-1)}-1$ olur; veya n sayısında 3'ten başka asal sayı yoktur, yani $n = 3^k$'tür.

$$2^{2(p_2-1)\cdots(p_r-1)}-1 = \underbrace{(2^{(p_2-1)\cdots(p_r-1)}-1)}_{a}\underbrace{(2^{(p_2-1)\cdots(p_r-1)}+1)}_{b}$$

ve $(a,b) = 1$ olur. Öte yandan Fermat teoremiyle $p_2p_3\cdots p_r \mid a$ elde edilir. $b \equiv 2 \pmod 3$ olduğundan $3 \nmid b$. Ayrıca $i = 2,3,\ldots,r$ için $p_i \mid a$ olduğundan, b sayısının yeni bir asal bölene ihtiyacı vardır: $p_{r+1} \mid b$. Kolayca $p_{r+1} \mid 2^{\phi(n)}-1$ ve $p_{r+1} \nmid n$ olur.

$n = 3^k$ durumunda ise, $k \geq 1$ ise

$$2^{\phi(n)}-1 = 2^{2\cdot 3^{k-1}}-1$$

olur. $k \geq 2$ ise $7 \mid 2^{\phi(n)}-1$ ve $7 \nmid n$ elde edilir. $k = 1$ ise $n = 3$ olmak üzere problemin şartı sağlanmaz. Dolayısıyla $n > 3$ olan her tek n sayısı için $p \mid 2^{\phi(n)}-1$ ve $p \nmid n$ olacak şekilde bir p asal sayısı vardır.

Fermat ve Wilson teoremleri aynı teoremde birleştirilebilirler [3]:

Teorem. *(Leo & Moser) Her a pozitif sayısı ve p asal sayısı için $p \mid (p-1)!a^p + a$ olur.*

Kanıt. $(p-1)!a^p + a \equiv -a^p + a \equiv 0 \pmod p$ Fermat ve Wilson teoremleriyle elde edilir. Tersine her a için $p \mid (p-1)!a^p + a$ ise $a = 1$ alarak $p \mid (p-1)! + 1$ Wilson teoremiyle elde edilir. Böylece $p \mid (p-1)!a^p + a^p$ ve $p \mid a^p - a$ elde edilir ki bu da Fermat teoremidir.

Not. [1]'de sondan bir önceki teoremde $\phi(ab) = \phi(a)\phi(b)$ olduğunu gösterirken nasıl $\phi(ab) \leq \phi(a)\phi(b)$ elde ettiğimizi belirgin bir şekilde şöyle gösterebiliriz: $(x,ab) = 1$ ise $(x,a) = (x,b) = 1$ olur. Şu halde $x \equiv r_i \pmod a$ ve $x \equiv s_j \pmod b$ yazılabilir. $(a,b) = 1$ olduğundan Çinli Kalan Teoremi'yle bu sistemin bir x çözümü vardır ve x, a ve b'nin lineer kombinasyonu olarak yazılabilir. $x \equiv 1 \pmod a$ ve $x \equiv 0 \pmod b$ denkliklerinden $x = bt$ ve $bt \equiv 1 \pmod a$ olacak şekilde bir t bulunabilir, çünkü $(a,b) = 1$'dir. $(t,a) = 1$ olduğundan $t \in \{r_1, r_2, \ldots, r_{\phi(a)}\}$. Benzer şekilde $x \equiv 0 \pmod a$ ve $x \equiv 1 \pmod b$ denkliklerinden $x = at'$ ve $at' \equiv 1 \pmod b$ olacak şekilde bir t' bulunabilir; $(t',b) = 1$ olduğundan $t' \in \{s_1, s_2, \ldots, s_{\phi(b)}\}$.

Şimdi $bt \equiv 1 \pmod{a}$, $t' \equiv 0 \pmod{a}$, $t \equiv 0 \pmod{b}$ ve $at' \equiv 1 \pmod{b}$ denkliklerinden

$$btr_i \equiv r_i \pmod{a} \qquad at's_j \equiv 0 \pmod{a}$$
$$btr_i \equiv 0 \pmod{b} \qquad at's_j \equiv s_j \pmod{b}$$

bulunur. Bunlar taraf tarafa toplanarak $btr_i + at's_j \equiv r_i \pmod{a}$ ve $btr_i + at's_j \equiv s_j \pmod{b}$ elde edilir. Kolayca $(tr_i, a) = 1$ ve $(t's_j, b) = 1$ olduğundan, $x = as_i + br_j$ biçiminde yazılır ve $\phi(ab) \leq \phi(a)\phi(b)$ olur.

Gene [1]'de Euler Teoremi'nin 3. kanıtında M'nin bir grup olduğunu gözlemeye çalıştık. $(a, m) = 1$ olan her a için $ax_0 \equiv 1 \pmod{m}$ olacak şekilde bir x_0 bulup $x_0 \equiv z_0 \pmod{m}$ alarak $z_0 = a^{-1}$ dedik. Burada $(z_0, m) = 1$ olduğu belirtilmelidir. $(x_0, m) = 1$ olduğundan $(z_0, m) = 1$ olduğu açıktır. Ters elemanın varlığı yetmez, o elemanın ayrıca M'nin bir elemanı olması gerekir.

KAYNAKÇA

[1] E. Alkan, *Fermat ve Euler Teoremleri*, *Matematik Dünyası*, 4, sayı 3, 7–8 (1994).

[2] E. Alkan, *Sayılar TeorisindeÇözülmemiş Problemler*, *Matematik Dünyası*, **3**, sayı 3, 17–21 (1993).

[3] Ş. Alpay, *Wilson Teoremi*, *Matematik Dünyası*, **3**, sayı 4, 12–14 (1993).

[4] G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers*, 5. baskı, Clarendon, Oxford, 1979.

[5] C. A. Nicol & J. L. Selfridge, Problem E3452, *American Mathematical Monthly*, **98**, 645 (1991).

[6] W. Sierpinski (çeviren A. Sharma), *A Selection of Problems in the Theory of Numbers*, Pergamon, Oxford, 1964.

[7] W. P. Wardlaw, Problem 10324, *American Mathematical Monthly*, **100**, 688 (1993).

PROBLEMLERLE EĞLENELİM (Mİ?) (III)

1. Bir sayının 7, 11 veya 13 ile bölünebilmesi için gerekli ve yeterli koşulun sayının basamaklarını sağdan başlayarak üçlü gruplar halinde sırayla bir toplayıp, bir çıkartarak elde edilen sayının 7, 11 veya 13 ile bölünebilmesi olduğunu kanıtlayınız. Örneğin, $N = 48286615$ alalım; $48 - 286 + 615 = 377$ ve $13 \mid 377$ olduğundan, $13 \mid N$ dir, fakat $7 \nmid N$ ve $11 \nmid N$ olur.

2. Bir sayının $10^k + 1$ ile bölünebilmesi için gerekli ve yeterli koşulun sayının basamaklarını sağdan aşlayarak k'lı gruplar halinde sırayla bir toplayıp, bir çıkartarak elde edilen sayının $10^k + 1$ ile bölünebilmesi olduğunu kanıtlayınız. Örneğin, $7 - 55 + 48 = 0$ ve $101 \mid 0$ olduğundan $101 \mid 75548$.

3. $(a, b) = 1$ olmak üzere, bir sayının ab ile bölünebilmesi için a ve b ile bölünebilmesinin yeterli olduğunu gösteriniz.

4. M, şu koşulları sağlayan $n \times n$ matrislerin kümesi olsun:

   (i) Birim matris $I \in M$.

   (ii) $A, B \in M$ ise, ya $AB \in M$ veya $-AB \in M$; fakat aynı anda AB ve $-AB$, M'de olamazlar.

   (iii) $A, B \in M$ ise, ya $AB = BA$ ya da $AB = -BA$.

   (iv) $A \in M$ ve $A \neq I$ ise, $AB = -BA$ koşulunu sağlayan en az bir $B \in M$ vardır.

   M kümesinde n^2 tane matris olduğunu kanıtlayınız.

5. Burhaniye'de hiç kimsenin 13.000'den fazla saç teli yoksa ve orada 13.000'den fazla kişi yaşıyorsa, orada en az iki kişinin saç tellerinin aynı sayıda olduğunu kanıtlayınız [1].

KAYNAKÇA

[1] A. Nesin, *Şapkadan Güvercin Çıkarmak*, *Bilim ve Ütopya*, Kasım, 1994.