SAYILAR KURAMINDA ÇÖZÜLEMEMİŞ ÜNLÜ PROBLEMLER

Şafak Alpay *

Bolu'dan yazan sevgili okurumuz Barış Öztürk, matematikte çözülemeyen problemlerin yayınlanmasını istemişti. Bu istemini sayılar kuramındaki problemlerle yerine getiriyoruz.

Sayılar kuramı, kolayca sorulan ama pek o kadar da kolay yanıtlanamayan sorularla dolu bir alan.

1. 2 ve 8'den farklı olan ve 2^n'nin 3'ün farklı kuvvetlerinin toplamı olarak yazılabildiği bir n tamsayısı bulabilir miyiz?

$\binom{n}{r}$ ifadesi, $(x+y)^n$ ifadesinin açılımında $x^{n-r}y^r$'nin katsayısıdır. Örneğin,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$

yazabiliriz. $1 \leq r \leq n$ olmak üzere, $\binom{n}{r}$, Pascal'a ait olan

$$\binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{1\cdot 2\cdot 3\cdots r} = \frac{n!}{r!\,(n-r)!}$$

ile veriliyor.

2. 105 sayısının $\binom{2n}{n}$ sayısını böldüğü sonsuz tane n doğal sayısı var mıdır?

3. Anımsanacağı gibi *asal sayılar* bölenlerinin sadece 1 ve sayının kendisinin olduğu sayılardır; $2, 3, 5, 7, 11, 13, 17, \ldots$ gibi. Asal sayıların sonsuz tane olduğunu biliyoruz. Öte yandan, $2n-1$ ve $2n+1$ sayılarından her ikisi de asal sayılar ise bunlara *ikiz asallar* diyoruz. $(3,5)$ ve $(5,7)$ çiftleri ikiz asallardır. İkiz asallar sonsuz tane midirler?

4. n^2+1 şeklinde olan asal sayılar sonsuz tane midirler?

5. n^2+n+1 şeklinde olan asal sayılar sonsuz tane midirler?

6. $2p+1$ sayısının asal olduğu p asal sayıları kaç tanedirler?

7. Hem Fibonaci sayısı, hem de asal olan sayılar kaç tanedir [1], [2]?

8. p asal olmak üzere, 2^p-1 şeklinde olan asal sayılara *Mersenne asalı* diyoruz. Mersenne asalları sonsuz tane midir [5]?

9. $2^{2^n}+1$ sayısının asal olduğu ve $5 \leq n$ olan n doğal sayısı var mıdır?

10. Goldbach savı [3]: $4 \leq n$ olan her n doğal sayısı için $p+q=2n$ eşitliğini sağlayan p ve q asal sayıları var mıdır?

11. Her n doğal sayısı için $n^2 < p < (n+1)^2$ eşitsizliği sağlayan asal p sayısı var mıdır?

12. Özbölenlerinin toplamına eşit olan doğal sayılara *mükemmel sayı* denir [5]. En küçüklerinin $6 = 1+2+3$ olduğu 32 tane mükemmel sayı biliniyor. 23 yüzyıldır çözülemiyen soru şu: Tek sayıların mükemmel sayı olup olamayacakları.

Sonraki sorularımız için ortak ve en büyük ortak bölen kavramlarına gereksinimiz var. Birçoğumuz tarafından bilindiğini sanmakla beraber, tekrarlamakta yarar var. c tamsayısı a ve b tamsayılarını bölüyor ise $c|a$, $c|b$ yazarız ve c'ye a ve b'nin *ortak böleni* deriz. Örneğin, 36 ve 60 sayılarının ortak bölenleri $1, 2, 3, 4, 6$ ve 12'dir. Kuşkusuz a ve b verildiğinde $1|a$, $1|b$ olduğundan ortak bölenlerin kümesi boş değildir. $c|a$ ve $c|b$ olduğunda $c \leq \min\{a,b\}$ olduğu besbellidir. a ve b sayıların bölenleri içinde en önemlilerinden biri *en büyük ortak bölen*dir ve (a,b) ile gösterilir. $d=(a,b)$ ise $d|a$ ve $d|b$'dir ve eğer $c|a$, $c|b$ ise, $c|d$ olduğu besbellidir. Örneğin, $(36,60)=12$ ve $(20,30)=10$.

* ODTÜ Matematik Bölümü öğretim üyesi

13. Şimdi Euler (1707–1783) tarafından bulunan ünlü bir fonksiyon ile ilgili bir soru soracağız. n doğal sayısı için $\phi(n)$, $1 \leq k < n$ olan ve n ile *aralarında asal*, yani $(k, n) = 1$, olan k sayılarının sayısı olsun. Örneğin, $k = 1, 2, 4, 5, 7$ ve 8 için $(k, 9) = 1$ olduğundan $\phi(9) = 6$'dır. Aynı şekilde, $\phi(10) = 4$'tür, çünkü sadece $k = 1, 3, 7$ ve 9 için $(k, 10) = 1$'dir. Bu fonksiyonla ilgili sorumuz, $\phi(x) = n$ eşitliğinin tek çözümü olduğu n tamsayısının olup olmadığı.

14. g ve n, $0 < g < m$ ile $(g, m) = 1$ koşulları sağlayan tamsayılar olsun. Euler'a ait bir teorem $g^{\phi(m)} \equiv 1 \pmod m$ olduğunu verir. Çoğu kez daha küçük bir k sayısı için $g^k \equiv 1 \pmod m$ doğrudur. Örneğin $g = 4$ ve $m = 7$ için $(4, 7) = 1$ ve $\phi(7) = 6$, fakat $4^3 \equiv 1 \pmod 7$'dir. h tamsayısı, $g^h \equiv 1 \pmod m$ eşitliğini sağlayan en küçük tamsayı ve $h = \phi(m)$ ise g tamsayısına $\pmod m$'de *ilkel kök* denir. Örneğin, 3 ve 5, $\pmod 7$'de ilkel köklerdir. 2 sayısının $\pmod p$'de ilkel kök olduğu sonsuz tane asal p var mıdır?

Asal olmayan n tamsayısı, n ile aralarında asal, yani $(b, n) = 1$, olan her b tamsayısı için $b^{n-1} \equiv 1 \pmod n$ eşitliğini sağlıyorsa, n sayısına *Carmichael sayısı* deniyor. $561 = 3 \cdot 11 \cdot 17$ sayısının en küçük Carmichael sayısı olduğunu biliyoruz. Bunu hemen görebiliriz de: $(b, 561) = 1$ olsun. 3, 11 ve 17, 561'in asal bölenleri olduğundan, $(b, 3) = (b, 11) = (b, 17) = 1$ olmalıdır. Fermat'nın küçük teoreminden $b^2 \equiv 1 \pmod{31}$ ve dolayısı ile $b^{560} = (b^2)^{280} \equiv 1^{280} = 1 \pmod 3$ elde ederiz. Benzer şekilde, $b^{10} \equiv 1 \pmod{11}$ denkliğinden, $b^{560} = (b^{10})^{56} \equiv 1^{56} = 1 \pmod{11}$ elde ederiz. Son olarak, $b^{16} \equiv 1 \pmod{17}$ denkliğinden elde ettiğimiz $b^{560} = (b^{16})^{35} \equiv 1^{35} = 1 \pmod{17}$, bize $b^{560} \equiv 1 \pmod{561}$ verir. Her Carmichael sayısının tek ve en az üç tane asal çarpanı olduğunu da biliyoruz. 1980 yılına dek 10^{10} sayısından küçük Carmichael sayılarının sadece 1547 tane olduğu biliniyordu.

İlk bir kaç Carmichael sayısı $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$, $1821 = 7 \cdot 13 \cdot 31$. Görüldüğü gibi ilk beş Carmichael sayısının üç asal çarpanı var. Gerçekten Carmichael sayılarının tek ve en az üç tane asal çarpanı olduğu biliniyor. Dört asal çarpanı olan Carmichael sayısı bulmak için 41041'e çıkmak gerekiyor, çünkü $41041 = 7 \cdot 11 \cdot 13 \cdot 41$. Beş asal çarpanı olan Carmichael sayısı ise asal çarpanları $5, 7, 17, 19, 73$ olan 825265 sayısı. Carmichael 1912 tarihinde yazdığı makalesinde onbeş tane böyle sayı veriyordu ve kendi adı ile anılacak bu sayıların sonsuz tane olduklarını ileri sürüyordu.

1980 yılında Pomerance, Selfridge ve Wagstaff'in 25×10^{10} sayısından küçük Carmichael sayılarının 2163 tane olduğunu, 1990'da Jaesche'nin 10^{12}'den küçük Carmichael sayılarının 8241 tane ve 1992 yılında ise Pinch'ın 10^{15}'ten küçük Carmichael sayılarının 1052212 tane olduğunu göstermesi bu sayıların gerçekten sonsuz tane olduğuna işaret ederken, hesaplar onların 10^{15}'e kadar nadir olduklarını gösteriyordu. Hatta Paul Erdős 1949'da Carmichael sayıların çarpımsal terslerinden oluşan serinin, yani P_k Carmichael sayısı olmak üzere

$$\sum_{k=1}^{\infty} \frac{1}{P_k}$$

serisinin yakınsak olduğunu göstererek bu sayıların ne kadar nadir olduklarına bir ölçü bile veriyordu.

1956 yılında Paul Erdős Carmichael sayıları için bir reçete veriyor. Buna göre, verilen bir N doğal sayısı için

(i) $p - 1$ sayısının N sayısını böldüğü, fakat p'nin N sayısını bölmediği p asal sayıları seçilir;

(ii) birinci adımda bulunan asal sayıların altkümelerinden seçilen asalların çarpımları $\pmod N$'de 1'e eşit olanlar alınır;

bu çarpımlar Carmichael sayılarıdır.

Erdős algoritmasını daha iyi anlayabilmek için $N = 120$ alalım. 120 sayısını bölmeyen, fakat $p - 1$'in 120'i böldüğü asal p sayıları $7, 11, 13, 31, 41, 61$'dir. Böylelikle (i) adımında bulmamız gereken sayıları bulduk. Bunlar arasından

$$41041 = 7 \cdot 11 \cdot 13 \cdot 41 \equiv 1 \pmod{120}$$
$$172081 = 7 \cdot 13 \cdot 31 \cdot 61 \equiv 1 \pmod{120}$$
$$852841 = 11 \cdot 31 \cdot 41 \cdot 61 \equiv 1 \pmod{120}$$

olduğunu hesaplayabiliriz. Dolayısı ile 41041, 172081 ve 852841 sayıları Carmichael sayılarıdır.

1992 yılına kadar on bin taneden az Carmichael sayısı bilinirken Erdős'ün yukarıdaki reçetesini geliştiren Alford, 21 Ocak 1992'de en