Kapak Konusu: Modüler ve p-sel Sayılar

Fermat'nın Küçük Teoremi

Fermat'nın Büyük Teoremi'ni herkes bilir, ama ilk iddia edilişinden 350 yıl sonra, yani ancak birkaç yıl önce Andrew Wiles tarafından bulunan kanıtını yeryüzünde üç beş kişi ya bilir ya bilmez. Fermat'nın kanıtlanması o kadar güç olmayan bir de Küçük Teoremi vardır. Fermat'nın Küçük Teoremi'ne göre, örneğin, 127, $145^{127} - 145$'i ve $145^{126} - 1$'i böler. İmkânsız çarpmayı yapmanıza gerek yok; bu, aşağıdaki teoremden ve 127'nin asal olmasından çıkacak.

Teorem. [Fermat'nın Küçük Teoremi]. *p bir asal sayı, n bir tamsayı olsun. O zaman p, $n^p - n$'yi böler. Ayrıca eğer p asalı n'yi bölmüyorsa, p, $n^{p-1} - 1$'i böler; dolayısıyla n'nin modülo p tersi n^{p-2}'dir.*

Teorem büyük olasılıkla Fermat tarafından kanıtlanmıştı, ama o zamanlar kanıtlar pek ortalığa yayılmazdı, matematikçiler kanıtlarını genellikle saklarlardı. Teoremin kanıtını ilk kez Euler 1749'da yayımlamıştır.

Kanıt: $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ fonksiyonu, $f(x) = x^p$ kuralıyla tanımlansın. Önce her $x, y \in \mathbb{Z}/p\mathbb{Z}$ için,

$$f(x + y) = f(x) + f(y)$$

eşitliğini, yani,

$$(x + y)^p = x^p + y^p$$

eşitliğini kanıtlayacağız. Her halkada olduğu gibi $\mathbb{Z}/p\mathbb{Z}$ halkasında da, her $x, y \in \mathbb{Z}/p\mathbb{Z}$ için,

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$$

eşitliği geçerlidir [MD-2003-I, sayfa 33, Teorem 5; sadece asal bir p için değil, her n doğal sayısı için geçerli olan bu eşitlik, n'nin i'lisinin aşağıda (p için) verilen tanımı kullanılarak n üzerine tümevarımla kolaylıkla kanıtlanabilir.] Öte yandan,

$$\binom{p}{i} = \frac{p!}{i!(n-i)!}$$

dir ve eğer $i \neq 0$ ve $i \neq p$ ise, paydadaki $i!(n-i)!$ teriminde, pay'daki p'yi sadeleştirecek bir p yok. Dolayısıyla, eğer $i \neq 0$ ve $i \neq p$ ise, p asalı p'nin i'lisini böler. Ama $\mathbb{Z}/p\mathbb{Z}$ halkasında, her $x \in \mathbb{Z}/p\mathbb{Z}$ için, $px = 0$. Demek ki,

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p.$$

İstediğimizi kanıtladık. Şimdi teoremin kanıtına dönelim. $f(\bar{1}) = \bar{1}^p = \bar{1}$ olduğundan,

$$f(\bar{2}) = f(\bar{1} + \bar{1}) = f(\bar{1}) + f(\bar{1}) = \bar{1} + \bar{1} = \bar{2},$$
$$f(\bar{3}) = f(\bar{2} + \bar{1}) = f(\bar{2}) + f(\bar{1}) = \bar{2} + \bar{1} = \bar{3},$$
$$f(\bar{4}) = f(\bar{3} + \bar{1}) = f(\bar{3}) + f(\bar{1}) = \bar{3} + \bar{1} = \bar{4},$$
$$\ldots$$

Görüldüğü gibi, her $x \in \mathbb{Z}/p\mathbb{Z}$ için, $f(x) = x$, yani $x^p = x$. Şimdi, eğer $n \in \mathbb{Z}$ ise, x yerine $\bar{n}$ alarak, $\bar{n}^p = \bar{n}$ eşitliği görülür. Yani p, $n^p - n$'yi böler.

Eğer n ve p birbirine asalsa, $\bar{n} \neq \bar{0}$ ve, $\mathbb{Z}/p\mathbb{Z}$ bir cisim olduğundan, $\bar{n}$, $\mathbb{Z}/p\mathbb{Z}$'de tersinirdir. Şimdi $\bar{n}^p = \bar{n}$ eşitliğinde $\bar{n}$'yi sadeleştirerek, $\bar{n}^{p-1} = \bar{1}$ buluruz. Bundan da p'nin $n^{p-1} - 1$'i böldüğü çıkar. □

Sonuç. *Eğer belli bir $1 < n < p$ için, p, $n^{p-1} - 1$'i bölmüyorsa, o zaman p asal olamaz.*

Yukardaki sonuç bir p sayısının asal olmadığını anlamaya yarar ama asal olduğunu anlamaya yetmez ne yazık ki, yani bir p sayısı her $1 < n < p$ için $n^{p-1} - n$'yi bölebilir ama gene de asal olmayabilir. Bu tür sayılara **yalancı Fermat asalları** ya da **Carmichael sayıları** denir. Carmichael 1910'da, ilk üçü 561, 1105 ve 1729 olmak üzere bu sayılardan 15 tane buldu ve bunlardan sonsuz tane olduğu sanısını ortaya attı. 1956'da Erdos'ün bir düşüncesini takip eden Alford, Granville ve Pomerance, 1994'te sonsuz tane Carmichael sayısı olduğunu kanıtladılar, hatta eğer x çok büyük bir sayıysa, x'ten küçük Carmichael sayılarının sayısının en az $x^{2/7}$ olduğunu kanıtladılar. Bu ilginç sayılardan bir başka sayımızda söz ederiz. ♦