CARMICHAEL SAYILARI

Engin Büyükaşık
İYTE, Fen Fakültesi, Matematik Bölümü, Urla, İZMİR

Fermat'ın küçük teoremine göre; n asal bir sayı ise her $a \in Z$ için $a^n \equiv a \pmod{n}$ ya da $n|(a^n - a)$ dır [2]. Doğal olarak asal sayılar dışında bu kongüransı sağlayan tamsayılar bulunup bulunmadığı sorulabilir. Bu soruyu ilk olarak 1910 yılında R. D. Carmichael adlı bir matematikçi yanıtlamış ve her $a \in Z$ için;

$$561(= 3 \cdot 13 \cdot 17)|(a^{561} - a)$$

olduğunu göstermiştir. Daha sonra 1912 yılında "$a^{P-1} \equiv 1 \pmod{P}$ kongüransını sağlayan P bileşik sayıları üzerine" adlı makalesinde bu sayıların bazı özelliklerini tanıtmıştır. Bundan dolayı bu kongüransı sağlayan bileşik sayılara *Carmichael sayıları* denmektedir.
Bu sayıların özelliklerini incelemeden önce bazı tanım ve teoremleri görelim.

$n \in N$, $n \geq 2$ olmak üzere

$$Z_n = \{0, 1, 2, ..., n-1\}$$

kümesini ele alalım. $x, y \in Z_n$ için $x + y$, xy ve n ye Z içinde bölme algoritmasını uygulayalım:

$$x + y = an + r \ , a \in Z, \ r \in Z_n$$

$$xy = bn + s \ , b \in Z, \ s \in Z_n$$

Bu durumda r ve s, sırasıyla, $x + y$ ve xy sayıları n ile bölündüğünde elde edilen en küçük negatif tamsayılar olup tek türlü belirli olduklarından,
$x \oplus y = r$ ve $x \otimes y = s$ tanımlanırsa, Z_n içinde $\oplus$ ve $\otimes$ ikili işlemleri elde edilir.
Z_n nin n ile aralarında asal olan elemanlarının oluşturduğu kümeyi Z_n^* ile gösterelim:

$$Z_n^* = \{k \in Z_n : (k, n) = 1\}.$$

Bu durumda Z_n ve Z_n^* nın sırasıyla $\oplus$, $\otimes$ işlemlerine göre birer grup oldukları kolayca gösterilebilir. Z_n^* nın mertebesi (eleman sayısı) $\phi(n)$ ile gösterilir. Şu halde, $n \geq 2$ için, $\phi(n) = |Z_n^*| =$(n den küçük ve n ile aralarında asal olan doğal sayıların sayısı) dır.

Bir G grubu ve $x \in G$ için

$$G = \{x^n : \ n \in Z\} =< x >$$

ise G ye bir *devirli grup*, x elemanına da G nin bir *üreteci* denir.

Teorem 1 $n \geq 2$ şeklinde bir pozitif tamsayı ve $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$ ise,

$$\phi(n) = \prod_{i=1}^{t} [p_i^{\alpha_i - 1}(p_i - 1)] = n \prod (1 - \frac{1}{p_i})$$

dir.

Kanıt: [2]

Teorem 2 (Euler) m pozitif bir tamsayı ve $(a, m) = 1$ ise $a^{\phi(m)} \equiv 1 \pmod{m}$ dir.

Kanıt: m den küçük ve m ile aralarında asal olan tamsayılar kümesi $\{x_1, ..., x_k\}$ olsun. Diğer taraftan $(a, m) = 1$ olan bir a pozitif tamsayısı için $\{ax_1, ..., ax_k\}$ kümesini ele alalım. Bu kümenin her bir elemanının m ile aralarında asal olduğu açıktır. Bu takdirde her iki kümenin m modülüne göre denk olduklarını söyleyebiliriz. Buradan da $ax_1 \cdots ax_k \equiv x_1 \cdots x_k \pmod{m} \Rightarrow a^{\phi(m)} \equiv 1 \pmod{m}$ elde edilir.

Teorem 3. (Çin Kalan Teoremi) $n_1, ..., n_r$ ikişer ikişer aralarında asal pozitif tamsayılar ve $a_1, ..., a_r$ herhangi tamsayılar ise,

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

olacak biçimde bir x tamsayısı vardır. Ayrıca sözkonusu x tamsayısı $n_1 \cdots n_r$ modülüne göre tek türlü belirlidir.

Kanıt : [2]

Tanım: n bileşik bir tamsayı ve $b^{n-1} \equiv 1 \pmod{n}$ kongüransı $\forall b \in Z_n^*$ için sağlanırsa n bir *Carmichael sayısı*'dır denir.

Teorem 4. n tek ve bileşik bir tamsayı olsun. Eğer n'nin 1'den büyük bir tamkare böleni varsa n Carmichael sayısı olamaz.

Kanıt: p asal ve $p^2|n$ olduğunu varsayalım. Bu takdirde, $\phi(p^2) = p(p-1)$ olduğundan Teorem 2'den

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

olacak şekilde bir $g \in Z$ olduğunu söyleyebiliriz.
m : p dışında n'yi bölen asal sayıların sayısı olsun. Şu halde $(p^2, m) = 1$ ve Teorem 3'den dolayı

$$\begin{aligned} x &\equiv g \pmod{p^2} \\ x &\equiv 1 \pmod{m} \end{aligned}$$

sistemini sağlayan $x = b$ tamsayısı vardır.
Diğer taraftan $(b, n) = 1$ ve $b^{p(p-1)} \equiv 1 \pmod{p^2}$ olduğundan b tamsayısı $Z_{p^2}^*$'nin bir üreteci olur.
Şimdi $b^{n-1} \not\equiv 1 \pmod{n}$ olduğunu gösterirsek, Carmichael sayısı tanımından n'nin bir Carmichael sayısı olamayacağını söyleyebiliriz.
Kabul edelim ki $b^{n-1} \equiv 1 \pmod{n}$ olsun. Bu durumda

$$\begin{aligned} b^{n-1} &\equiv 1 \pmod{p^2} \\ b^{p(p-1)} &\equiv 1 \pmod{p^2} \end{aligned}$$

böylece

$$\begin{aligned} &p(p-1)|(n-1) \\ \Rightarrow\ &n-1 = p(p-1)s \\ \Rightarrow\ &n-1 \equiv 0 \pmod{p} \end{aligned}$$

elde edilir. Bu ise $p|n$ olduğundan bir çelişkidir. Sonuç olarak bir p asal sayısı için $p^2|n$ ise n Carmichael sayısı olamaz.

Teorem 5 (Korselt kriteri) n tamsayısının Carmichael sayısı olması için gerek ve yeter koşul her $p|n$ asal sayısı için $(p-1)|(n-1)$ olmasıdır.

Kanıt: $\Rightarrow$ n bir Carmichael sayısı olsun. Bu durumda her $b \in Z_n^*$ için;

$$b^{n-1} \equiv 1 \pmod{n}$$

sağlanır. $p|n$ için $((p-1) \not| (n-1)$ olduğunu varsayalım.
g, Z_p^*'nin bir üreteci olsun bu durumda $g^{p-1} \equiv 1 \pmod{p}$ olur. Bu durumda Teorem 3'e göre

$$b \equiv g \pmod{p}$$

$$b \equiv 1 \pmod{\frac{n}{p}}$$

denkliklerini sağlayan bir $b \in Z$ vardır. Buradan da $(b, n) = 1$ ve $b^{n-1} \equiv g^{n-1} \pmod{n}$

$$\Rightarrow g^{n-1} \equiv 1 \pmod{n}$$

$$\Rightarrow (p-1)|(n-1)$$

bu ise varsayımla çelişir. O halde $(p-1)|(n-1)$ olmalıdır.
$\Leftarrow$: $p|n$ ve $a \in Z_n^*$ olsun. Fermat'ın küçük teoremine göre $a^{p-1} \equiv 1 \pmod{p}$ dir. Hipoteze göre $(p-1)|(n-1)$ olduğundan;

$$a^{n-1} = a^{(p-1)k} \equiv 1 \pmod{p}$$

ve dolayısıyla

$$a^{n-1} \equiv 1 \pmod{n}$$

elde edilir. Böylece n tamsayısının bir Carmichael sayısı olduğu görülür.

Teorem 6 Her Carmichael sayısı en az üç farklı asal sayının çarpımıdır.

Kanıt: Teorem 4'e göre her Carmichael sayısı farklı asal sayıların çarpımıdı şeklindedir. Bu nedenle kanıtı tamamlamak için; n bir Carmichael sayısı ve p, q asal olmak üzere $n = qp$ biçiminde olamayacağını göstermek yeterlidir.
Kabul edelim ki $n = qp$, $p > q$ ve n bir Carmichael sayısı olsun. Bu durumda Teorem 5'e göre $(p-1)|(qp-1)$ dir. Buradan da bir $k \in Z$ için $(p-1)k = qp - 1$. Böylece

$$k = \frac{qp-1}{p-1} = q + \frac{q-1}{p-1}$$

elde edilir bu ise $(p-1) \not| (q-1)$ olduğundan bir çelişkidir.

Teorem 7 (Chernick) Eğer $6m+1$, $12m+1$, $18m+1$ sayıları bir $m \in Z$ için asal ise

$$n = (6m+1)(12m+1)(18m+1)$$

sayısı bir Carmichael sayısıdır.

Kanıt: Corselt kriterine göre her $p|n$ için $(p-1)|(n-1)$ olduğunu göstermeliyiz.

$$n = (6m+1)(12m+1)(18m+1)$$

$$= 6 \cdot 12 \cdot 18m^3 + (6 \cdot 12 + 6 \cdot 18 + 12 \cdot 18)m^2 + 36m + 1$$

ve

$$p = 6m+1,\ q = 12m+1,\ r = 18m+1$$

asal olmak üzere;

$$(p-1)|(n-1),\ (q-1)|(n-1),\ (r-1)|(n-1)$$

olduğu açıktır. O halde n bir Carmichael sayısıdır.

Örnek : $m = 1$ için

$$p = 6 \cdot 1 + 1 = 7$$

$$q = 12 \cdot 1 + 1 = 13$$

$$r = 18 \cdot 1 + 1 = 19$$

p, q, r asal olduğundan $n = 7 \cdot 13 \cdot 19$ sayısı bir Carmichael sayısıdır.

Teorem 8 (Duparc) m, q ve r asal sayılar ve $n = m \cdot q \cdot r$ bir Carmichael sayısı ise $q < r$ için, $q < 2m^2$ ve $r < m^3$ dir.

Kanıt: n bir Carmichael sayısı olduğundan "Corselt kriteri" nden $(r-1)|(n-1)$ ve $(q-1)|(n-1)$'dir. Buna göre

$$1 \equiv n = m \cdot q \cdot r \equiv m \cdot q \pmod{(r-1)}$$

$$1 \equiv n = m \cdot q \cdot r \equiv m \cdot r \pmod{(r-1)}$$

denkliklerini yazabiliriz. Şimdi

$$C = \frac{m \cdot q - 1}{r - 1} \quad D = \frac{m \cdot r - 1}{q - 1}$$

olsun. Bu durumda $1 \leq C < m < D$ olduğu açıktır. Buradan

$$D \cdot (q-1) = m \cdot r - 1 = m \cdot (\frac{m \cdot q - 1}{C} + 1) - 1$$

$$(C \cdot D - m^2)(q-1) = m^2 - m + m \cdot C - C = (m + C)(m-1) > 0$$

buradan da

$$(q-1) \leq (m+C)(m-1) < m^2 + (C-1)m \pmod{n_1}$$

elde edilir. Diğer taraftan $C < m$ olduğundan; $q - 1 < 2m^2$ ve dolayısıyla $q < 2m^3$ bulunur. Şimdi (1)'den,

$$r - 1 = \frac{m \cdot q - 1}{C} < \frac{m^3 + (C-1) \cdot m^2}{C} \leq m^3$$

buradan da $r < m^3$ elde edilir.

Bu teorem E. Pinch adlı bir matematikçi tarafından 10^{15}'e kadar olan Carmichael sayılarının bulunmasında kullanılmış. E. Pinch bu sayıya kadar 105212 tane Carmichael sayısı bulunduğunu göstermiştir.

Carmichael sayılarının sonsuz sayıda olduğu bu sayıların keşfedilmesinden yaklaşık bir asır sonra ispatlanabilmiştir. Sözkonusu ispat 1994'de W. R. Alford, Andrew Granwille ve Carl Pomerance tarafından yapılmış ve ispat *"Sonsuz çoklukta Carmichael sayısı vardır"* adlı makalede tanıtılmıştır. Sözkonusu makalede, yeterince büyük x tamsayıları için x e kadar olan Carmichael sayılarının sayısının $x^{2/7}$ den büyük olduğu ispatlanmıştır.

KAYNAKLAR

[1] H. İbrahim Karakaş: Soyut Cebire Giriş, M⊕V yayınları, 1998

[2] J. A. Anderson & J. M. Bell: Number Theory With Applications, Prentice Hall, 1997

[3] W. R. Alford, A. Granville & C. Pomerance: "There are Infinitely Many Carmichael Numbers," Ann. Math., Volume 140, 703-722, 1994

EĞLENCELİK...

KİMLER NASIL FİL AVLAR

Matematikçiler

Fil avlamak için Afrika'ya gider, fil olmayan herşeyi dışarı atıp kalanları avlarlar.

Deneyimli Matematikçiler

Matematikçilerin
yaptığı işe girişmeden önce Afrika'da en az bir filin bulunduğunu kanıtlarlar.

Matematik Profesörleri

Afrika'da en az bir filin varlığını kanıtlarlar ve onun bulunup yakalanması için de Yüksek Lisans öğrencilerine ödev verirler.

Bilgisayar Mühendisleri

- Afrika'ya giderler.
- Ümit Burnu'ndan başlayarak düzenli bir şekilde tüm kıtayı tarayarak kuzeye doğru ilerlerler.
- Bu esnada her arama anında;
  - Görülen tüm hayvanları avlarlar.
  - Her yakalanan hayvanı bilinen bir fille karşılaştırırlar.
  - Bulunca o hayvanı yakalarlar.

İstatistikçiler

Ardışık olarak "n" kez karşılaştıkları hayvana "fil" adını verip onu avlarlar.

****

HATA NEREDE

Öncelikle, $a \neq 1$ pozitif sabit bir sayı, x pozitif bir sayı ve c herhangi bir sayı olmak üzere

$$\log_a(x^c) = c.\log_a x$$

formülünü anımsayalım. Şimdi de şu gözlemi yapalım:

$$0 = \log(1) = \log((-1)^2) = 2.\log(-1)$$

O halde, $2.\log(-1) = 0$ olup buradan da $\log(-1) = 0$ elde ederiz (mi acaba?)

****

İLGİNÇ TEOREM

Bütün pozitif tamsayılar ilginçtir.

İspat: Karşıtını kabul edelim. Yani, ilginç olmayan enaz bir pozitif tamsayı bulunsun. O halde ilginç olmayan enküçük bir pozitif tamsayı vardır. Fakat, bir saniye, bu oldukça ilginç! Çelişki.

****

- En kısa matematik şakası: $\varepsilon < 0$ olsun.
- Yeteri kadar büyük 1'ler için $1 + 1 = 3$ tür.
- Einstein ve Pisagor buluşlarının kombinasyonu:

$$E = mc^2 = m(a^2 + b^2)$$

- $\lim_{3 \to 4} 3^2 = 16$

****

Yanlış aranan telefon numarası için santraldan alınan yanıt:

"Sanal bir sayıyı tuşladınız. Lütfen telefonunuzu 90° çevirerek yeniden deneyiniz."

****

Çılgın bir matematikçi otobüse biner ve bütün yolcuları tehdit etmeye başlar."İntegralini alacağım, türevini alacağım" Otobüsteki herkes korkup kaçar ama sadece nazik bir kadın kalır. Adam kadına yaklaşır ve "Korkmuyor musun! Senin de integralini alacağım, türevini alacağım" Kadın sâkin bir ses tonuyla adamı yanıtlar."Hayır korkmuyorum, çünkü ben e^x im."

****

π NEDİR

Fizikçinin yanıtı: π eşittir 3.141592 ± 0.0000007

Mühendisin yanıtı: π? yaklaşık olarak 3

Matematikçinin yanıtı: π, bir çemberin çevre uzunluğunun çap uzunluğuna oranı ile elde edilen sabit bir sayıdır.