Voldemath

MATEMATİK KULÜBÜ DERGİSİ

https://voldemath.wordpress.com/

SAYI : 6
01.03.2019

GALATASARAY ÜNİVERSİTESİ MATEMATİK KULÜBÜ

Gerçekten evrenin sırrını arıyorsanız, benim yaptığım gibi sayılara gelin. Sonsuzluk her seyin cevabıdır. Sayı sonsuzdur.

-CAHIT ARF

ŞİFRELEME MUCİDİ SEZAR VE ONUN GALİBİ EL-KİNDİ

KRİPTOGRAFİ(ŞİFRELEME) NEDİR?

Kriptografi bilimi gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bir diğer deyişle bir bilgiyi saklamak veya iletmek için kullanılan güvenlik yöntemleridir. Bilgi güvenliği kavramını incelerken esas alınan ve kullanılan iletişim sistemlerinin sahip olması beklenilen bir takım güvenlik kavramları vardır. Bunların içinde en önemlisi gizliliktir. Var olan bilginin korunması ve gizlenmesi şifreleme biliminin temel felsefesini oluşturur. Bilgiyi korumanın en basit yöntemi fiziksel koruma sağlamak olabilir. Toprağa gömdüğünüz bir hard diskin kimsenin bulamayacağından eminseniz bir çeşit güvenlik sağlamış olursunuz. Bu durumda saldıranın bilgiye erişebilmek için tek yöntemi bilgi sahibi sizden geçer. İlkel zamanlarda ise Çinliler vücutlarına veya kafalarına dövme yaparak bir çeşit bilgi güvenliği sağlamışlardır

Kriptografi kelime olarak yunanca kökenlidir ve “Kryptos Logos” (gizli kelime) ifadelerinden oluşmuştur. Kriptografi temelde iki bölümden oluşur. Birincisi şifre yazmak (enchryption), ikincisi şifre çözmek(dechryption). Kriptografi Matematik biliminin Sayılar Teorisi disiplini altında incelenir.

İLK ŞİFRELEME TEKNİĞİ: SEZAR ŞİFRELERİ

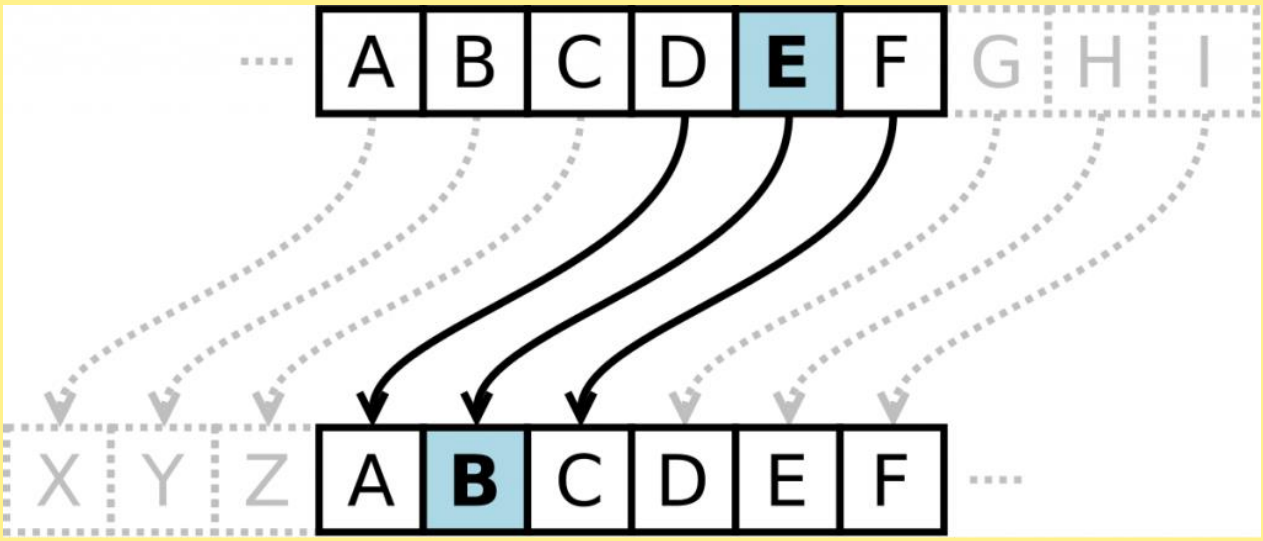
MÖ 60-50 yıllarında Roma imparatoru ve komutanı Julius Caesar (MÖ 100-44) tarihteki en ilkel şifreleme tekniğini icat etmiş ve bunları devlet haberleşmelerinde sıklıkla kullanmıştır. Bu şifreleme tekniğine Sezar Şifresi denilir ve bir tür yer değiştirme(substitution) tekniğidir. Başlangıçta alıcı ile gönderici arasında bilinen bir anahtar seçilir. Gönderilmek istenen mesaj anahtar sayı kadar alfabedeki harfler içinde ötelenir. Bu şekilde mesaj şifrelenir. Ardından mesaj alıcıya ulaştığında anahtar geri çevrilerek öteleme yapılır. Böylece alıcı şifreye ulaşmış olur. Bu şifreleme tekniğinde gerekli olan 3 unsur vardır. Birincisi açık mesaj(plain text), ikincisi anahtar(key). Üçüncüsü ise bunların elde edilmesi halinde oluşan şifreli mesaj(cipher text). Örnek olarak;

Açık mesaj: Matematik

Anahtar:2

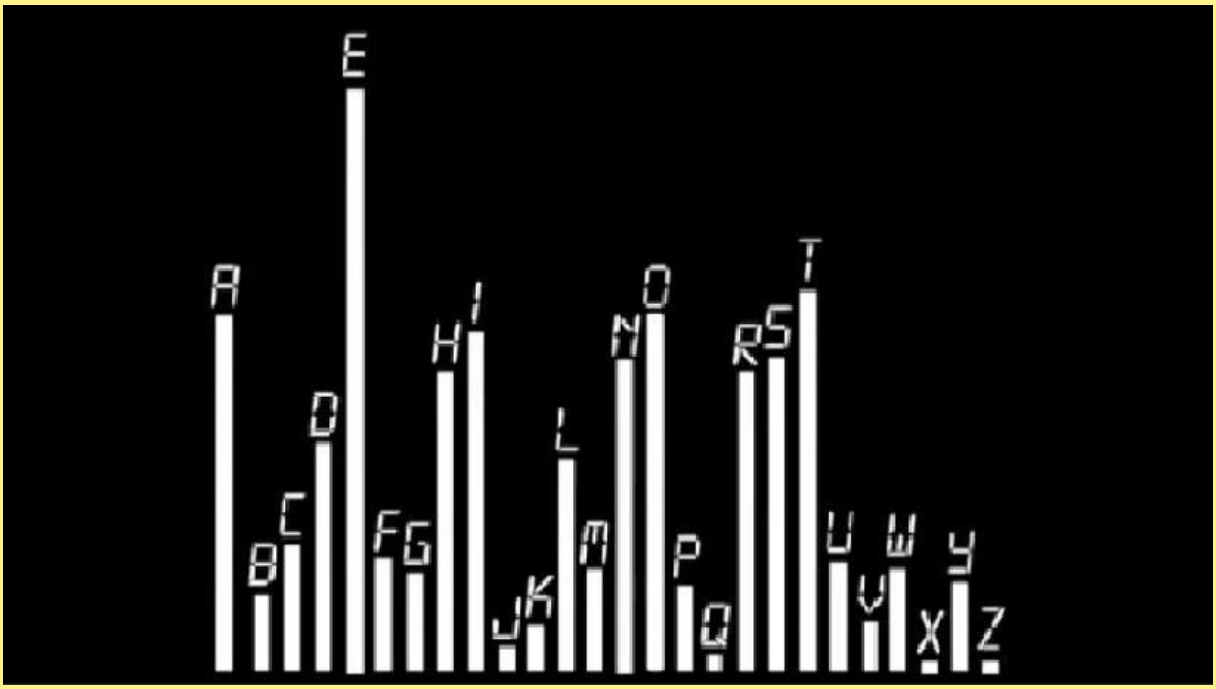
Şifreli mesaj: Ocügocükm

Sezar anahtar olarak “3”ü seçmiş ve şifrelemeleri bu şekilde yapmıştır. Şaşırtıcı ama başarılı olan bu teknik Sezar’ın icadından sonra yaklaşık olarak 800 yıl boyunca devletlerin haberleşmelerinde sıklıkla kullanılmıştır. Bu şifreleri kırmanın birkaç kolay yolu vardır. Gönderilen mesajı ele geçirmişseniz yapmanız gereken tek şey anahtarı bulmaktır. Bütünü incelemektense parçaları incelemek bu yöntem için daha kolay olabilir. Tüm mesajı incelemek yerine bir kelimeyi ele almak zaman kazandırır ve daha hızlı kırmak için en az harften oluşan kelimeyi seçebilirsiniz. Eğer kullanılan alfabeyi biliyorsanız o alfabenin her harfi kadar denemeniz ve anlamlı bir kelime bulmanız yeterli olacaktır. Mesela “Matematik” açık mesajı Türk alfabelerinde yazılmıştır. Anahtar birden yirmi dokuza kadar olabilir. Yapmanız gereken tek şey her bir harfini denemektir. M.S. 9.yy’da ise bu tekniğin analizini yapıp ilk şifre kırma yöntemini geliştiren kişi Bağdatlı El-Kindi’dir.



ŞİFRE KIRMA GELENEĞİNİN MUCİDİ El-KİNDİ

Dokuzuncu yüzyılda Kur'an'daki Arapça yazılar üstünde çalışan Bağdatlı âlim El-kindi, bazı harflerin diğerlerinden daha fazla kullanıldığını fark etmiş ve Kriptografi’nin temellerini atmıştır. El-Kindi, bu gözlemini geliştirerek, “Frekans Analizi” adını verdiği bir kod kırma yöntemi bulmuştur. Bu yöntemde her alfabe analiz edilerek harflerin bir frekansı oluşturulmuştur. Her harfin dil içerisinde kullanım sıklığı incelenmiş ve bu sıklık bir istatistiğe dökülmüştür. Aslında bir nevi kullanılan dilin parmak izi analiz edilmiştir. Bu analize “sıklık analizi” de denir. Sıklık analizi, temel yazı alfabesiyle oluşturulan klasik şifre ve kodların kırılmasında en temel araçtır. Bu yöntemin verimli kullanılabilmesi için, şifreyi çözmek isteyen kişinin şifreleme yapılan dilde lisan ve istatistik bilgisiyle problem çözme becerilerine sahip olması gerekir. Aşağıda İngiliz alfabesinin Frekans Analizi yapılmış ve her harfin hangi sıklıkla kullanıldığı incelenmiştir.



Tablo 1,1: İngiliz alfabesinin Frekans Analizi

Bu tablodan da görüldüğü üzere İngilizcede en çok kullanılan harf “e” ,ikincisi “t”,üçüncüsü “a” şeklinde gitmektedir. Sezar şifresiyle kodlanmış bir metin bu yöntem ile çok kolay analiz edilebilir. Öncelikle ele geçirilen metinde harflerin kullanım sıklığı incelenir. İnceleme sonucunda bu tablodaki sıralamaya benzer bir sıralama ortaya çıkacaktır. Mesela anahtar olarak “2” seçilmiş olsun. O zaman incelenen metinde en çok geçen harf “g” olmalı, ardından ise “v”, “c” şeklinde devam ediyor olmalıdır. Yani gerekli eşleşme sağlandığı takdirde Sezar şifresinin anahtarını bulmak çok kolay olacaktır.

Bir toplumda kriptoanalizin doğabilmesi için üç farklı alanda yüksek standartların yakalanması şarttır: Dilbilim, istatistik ve matematik. Bu şartların oluştuğu bir dönemde yaşayan Kindî, bu üç alanda ve daha nice alanlarda uzmanlaşmıştır." Simon Singh, Kod Kitabı, 1999

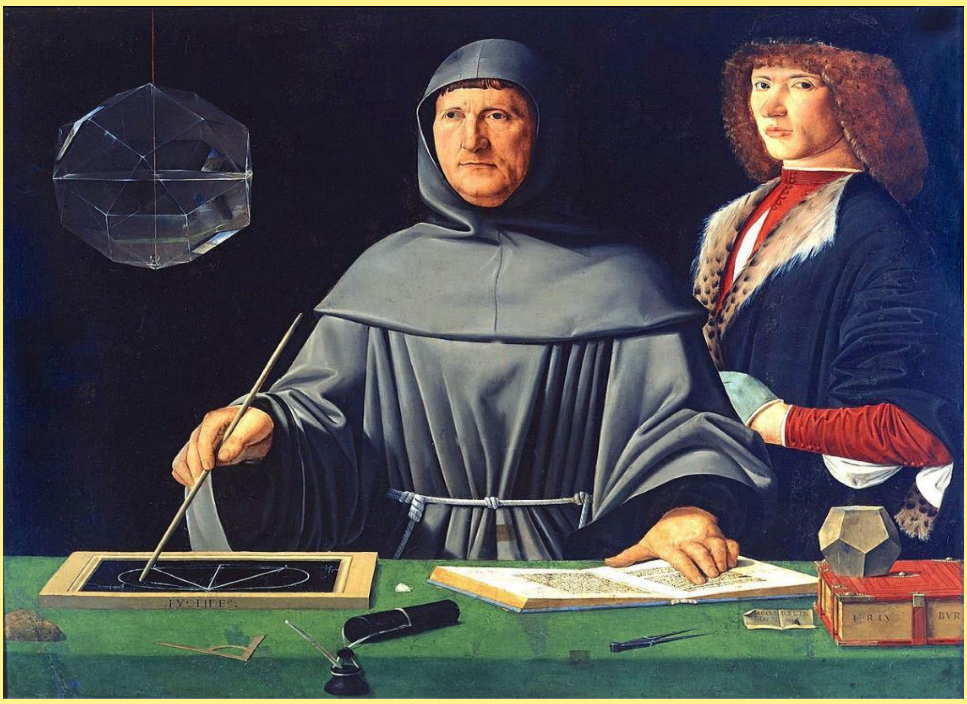
Yararlanılan Kaynaklar: www.khanacademy.com ; www.fikriyat.com

MATEMATİK VE SANAT

Merhabalar,

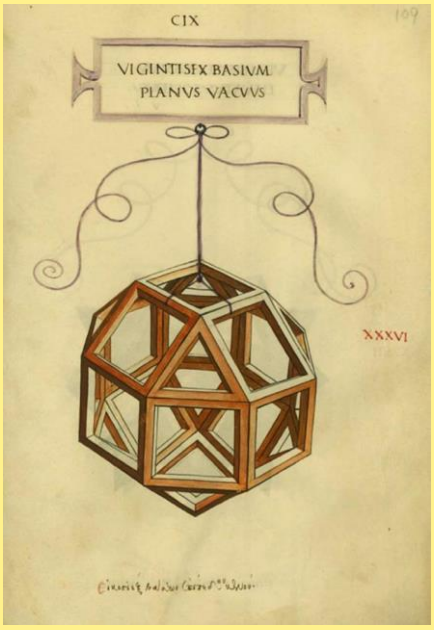
Bu yazıda sanatçının eserlerindeki matematikten ve biraz da hayatından bahsedeceğiz. İlk duyulduğunda kulağa garip gelse de eserlerde sanıldığından daha fazla matematik kullanılıyor. Hatta bazı sanatçılar geometri bilmeden eser ortaya konulamayacağını bile söylemekte bu yüzdendir ki geometri kitabı yazan ressamlar bile vardır.

Bugün bizim inceleyeceğimiz sanatçı Luca Pacioli , 1445'de İtalya' da doğdu ve 1494'de Soma adındaki ilk matematik kitabını yayımladı, kitapta pek fazla yeni bilgi yoktu ancak o zamana kadar olan matematiğin Latinceden İtalyancaya çevirisiydi bu kitap, bu da Avrupa'da matematiğin gelişmesine büyük katkı sağladı.

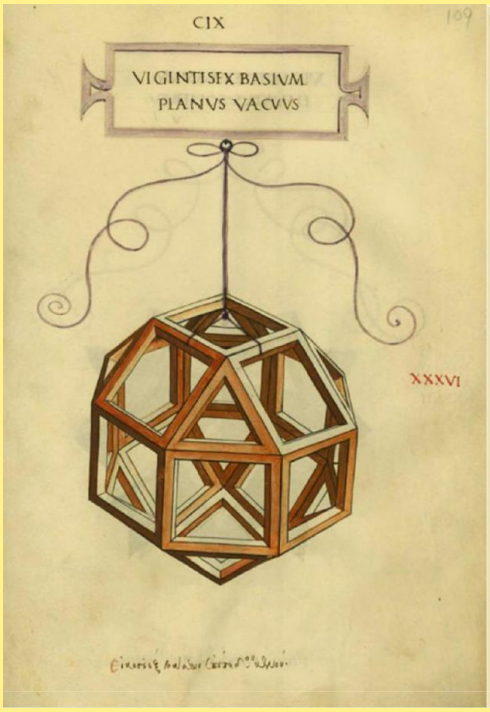


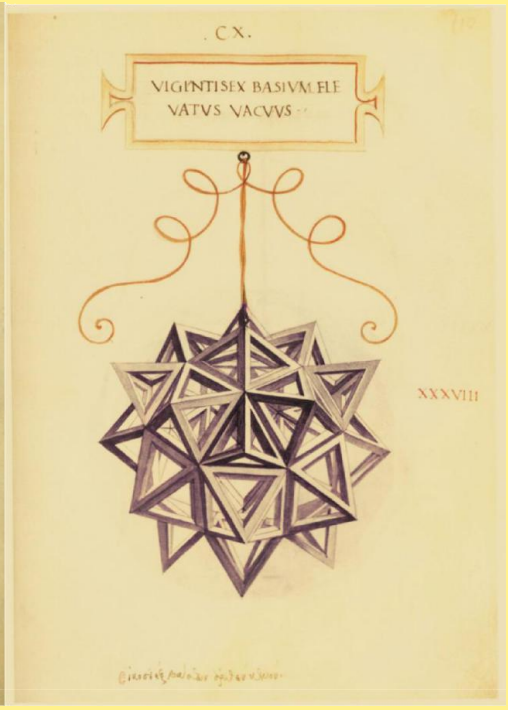
Gördüğünüz resimde ortadaki rahip Luca Pacioli' dir. Geçim kaygısı çekmeden matematik yapmanın en kolay yolunun rahiplik olduğunu düşünüyordu. Yanındaki genç adamın kim olduğu tam olarak bilinmemekte ama ya Pacioli' ye parasal açıdan destek olan bir muhasebeci ya da Alman ressam ve matematikçi Albert Dürer olduğu düşünülmektedir.

Arkadaki çok yüzlüye biraz daha yakından bakalım. Camdan yapılmış ve yarıya kadar su ile doldurulmuştur. Işığı soldan almaktadır. Cismin kötü çizildiği ve yansımaların yanlış olduğu hakkında tartışmalar süre gelsin biz şekli incelemeye devam edelim. Bu şekle "Archimedean Solid" denir. Aslında Arşimet tarafından adlandırılan 13 cisimden birisidir. Bu çok yüzlü, düzgün çokgenlerden kare ve üçgenlerin birleştirilmesiyle elde edilmiştir. Toplamda 8 üçgen ve 18 kareden oluşturulmaktadır. Ayrıca Pacioli'nin " De divina proportionne " olarak adlandırdığı ikinci kitabının da odak noktalarından biri olacaktır.



Kitabın çoğunluğu çok yüzlüler hakındadır. Kitabın arkasındaki çizimler -gördüğünüz çizim bunlardan biridir- Pacioli'nin ev arkadaşı olan Leonardo da Vinci tarafından yapılmıştır. Pacioli aynı zamanda Leonardo da Vinci'nin matematik hocasıdır. Leonardo bir dahi olmasına rağmen matematiği o kadar iyi değildi, bunu çalışma notlarında yaptığı basit aritmetik hatalarından ve kitaptaki çizim hatalarından anlayabiliriz. Mesela alttaki iki çizimi karşılaştıralım.





İlk çizim üçgen ve karelerden oluşmaktadır ikinci çizimde ise bu kare ve üçgenlerin üstüne karelere kare piramit, üçgenlere ise üçgen piramit gelecek şekilde oluşturulmuştur ancak çizimde üçgen piramit olması gereken bazı yerlerde kare piramit vardır. Bu bir skandal olmasa da ilk fark edildiğinde öyleymiş gibi gösterildi. Bu hata matematik tarihinde büyük resim kadar detaylara da odaklanmamızı hatırlatan bir hata olarak kaldı.

AY

Bildiğiniz üzere çinli bir bilim insan dünya tarihindeki Lulu ve Nana adındaki tasarım bebeklerini üretti. HIV virüsüne dayanıklı bu bebeklerin ilgili genleri mutasyona uğratıldı. Bu mutasyonun başka bir mutasyonu, örneğin süper zekâ olma gibi, ortaya çıkarıp çıkarmayacağı tartışılıyor. Bunu bize zaman gösterecek. Biz yine de bundan bahsetmeyeceğiz. Bunama ile ilgili yapılan araştırmalar diyet yapılarak ve stresten uzak durularak bunamanın etkilerinin azaltılacağını gösteriyor. Yaslı insanların bir özelliği olan camdan bakıp, kim nereye arabasın park etmiş, kim binaya girdi, kim sokaktan geçiyor gibi sorulara cevap aramaları onların üzerinde olumlu etki yaratıyormuş. Biz bunu da boş verelim. Size güzel araştırma örnekleri verdim ama siz araştırırsınız zaten. Okumak önemli arkadaşlar. Yine de insan bir gün yaşlanacağı gerçeğinden uzaklaşamıyor. Ben yaslı değilim. Yani bundan yüz bin yıl önceki atalarıma göre yaşlı sayılabilirim. Siz de öyle. Bu arada Antalya'da Neandertal yaşıyormuş bir zamanlar. Antalya Müzesi'ne gidip sekilsiz bir kafatası parçasından bunu anlayabiliyorsunuz. Oraya kadar gitmem diyorsanız Neandertal dostlarımıza sitem dolu bir mesajı dergimiz aracılığıyla gönderebilirsiniz. Evet bu hizmeti ayağınıza getirdik. Ayrıca Neantinder uygulamasıyla siz de yakın çevrenizden Neandertal arkadaşlar edinebilirsiniz. Çok konuşmuyorlar benden size söylemesi. Zaten ne anlarlar dertten halden hepsi gelmiş Neandertalden.

ARİTMETİK FONKSİYONLAR

Bu yazıda aritmetik fonksiyonlara kısa bir giriş yapacağız. Genel olarak Euler Phi fonksiyonuna değineceğiz.
Aritmetik fonksiyonlar, asalların dağılımında ve tam sayıların bölünebilirlik özelliklerinde önemli bir rol oynamaktadır.

Aritmetik Fonksiyonlar

Tanım kümesi doğal sayılar olan $f : \mathbb{N} \to \mathbb{R}$ veya $\mathbb{C}$ şeklindeki fonksiyonlara aritmetik fonksiyonlar denir.

Aritmetiğin Temel Teoremi

Birden büyük her n doğal sayısı, asal sayıların çarpımı olarak yegâne şekilde yazılabilir. Ayrıca, eğer $p_1, p_2, ..., p_n$ ve $q_1, q_2, ...q_m$ asalları için, $p_1p_2...p_n = q_1q_2...q_m$ ise $n = m$ olur.

Mobius Fonksiyonu

Mobius fonksiyonu şu şekilde tanımlıdır:
$\mu(1) = 1$; Eğer $n > 1$ ise, $n = p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ olsun, o zaman $\mu(n) = (-1)^k$ eğer $a_1 = a_2 = ... = a_k = 1$ ise, $\mu(n) = 0$ değilse.
Burada Mobius fonksiyonu için kısa bir tablo veriyoruz:

n:	1	2	3	4	5	6	7	8	9	10
$\mu(n)$:	1	-1	-1	0	-1	1	-1	0	0	1

Teorem 1

Eğer $n \geq 1$ ise,

$$\sum_{d|n} \mu(d) = [1/n] = \begin{cases} 1 & n = 1 \; ise \\ 0 & n > 1 \; ise \end{cases}$$

Euler Phi Fonksiyonu

Eğer $n \geq 1$ ise, Euler phi(φ) Fonksiyonu, n'den küçük ve n ile aralarında asal olan pozitif tam sayıları hesaplar. Yani

$$\varphi(n) = \sum_{k=1}^{n} 1$$

ve $(k, n) = 1$.
Burada Euler φ fonksiyonu için kısa bir tablo veriyoruz:

n:	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4

Teorem 2

Eğer $n \geq 1$ ise, $\sum_{d|n} \varphi(d) = n$ olur.

Bölenlerin Toplamı Fonksiyonu

Bu fonksiyon şu şekilde tanımlıdır:

$$\sigma(n) = \sum_{d|n} d$$

Örnek

$\sigma(n) = \sum_{d|n} d$ bu fonksiyonu daha genel biçimde yazacağız;
$n = 1 \Rightarrow \sigma(1) = 1$
$n = 2 \Rightarrow \sigma(2) = 1 + 2 = 3$
.
.
.
$n = p \Rightarrow \sigma(p) = 1 + p$
$n = p^a \Rightarrow \sigma(p^a) = 1 + p + p^2 + ... + p^a = \frac{p^{a+1}-1}{p-1}$
Daha genel olarak eğer $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ ise, o zaman

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a+1} - 1}{p - 1}$$

olur.
Şimdi mobius fonksiyonu ve Euler fonksiyonu arasında bir ilişki kuracağız.

Teorem 3

Eğer $n \geq 1$ ise,

$$\varphi(n) = \sum_{d|n} \mu(d) n/d$$

olur.

İspat

Bir $\varphi(n)$ tanımlıyoruz: n'e küçük ve eşit tam sayılar için, $\varphi(n) = \sum_{k=1}^{n} [1/(n,k)]$ olsun. Şimdi teorem 1'i kullanarak, n ile (n,k)'yı yer değiştiriyoruz ve şunu elde ediyoruz:

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{d|n, d|k} \mu(d)$$

Sabitlenmiş bir $d|n$ için, $1 \leq k \leq n$ aralığındaki k sayılarını toplayacağız, bu k sayıları d'nin katları. Eğer $k = qd$ ise, o zaman $1 \leq k \leq n$ ancak ve ancak $1 \leq q \leq n/d$. Böylece, $\varphi(n)$ şu şekilde yazılabilir:

$$\varphi(n) = \sum_{d|n} \sum_{q=1}^{n|d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n|d} 1 = \sum_{d|n} \mu(d) n/d$$

bu da bizim teoremimizi ispatlar. □