Oto Pilot Güvenilir mi?

BITCOIN MADENCİLİĞİ

MICHAEL JORDAN VE MATEMATİK

DÜNYANIN EN GELİŞMİŞ ARAZİ ROBOTU

5 EN GARİP MATEMATİKÇİ

YÜKSEL - İLHAN ALANYALI FEN LİSESİ

# YİAFL TECHMATH

E - DERGİ

YAPAY ZEKAYA YÖN VEREN BİLİM İNSANI

0! NEDEN 1'E EŞİTTİR?

ASAL SAYILAR VE ŞİFRELEME

WWW.E-DERGİ.YİAFL.COM

1234567890

**YİAFL TECHMATH**
YIL: 2 SAYI: 2 MAYIS 2018

# İÇİNDEKİLER

**Adına İmtiyaz Sahibi**
Muammer OKUMUŞ

**Genel Yayın Yönetmeni**
Kamil Baran YÜCEL

**Yazı İşleri Sorumluları**
Samet ZENGİN
Yusuf EKMEKÇİ

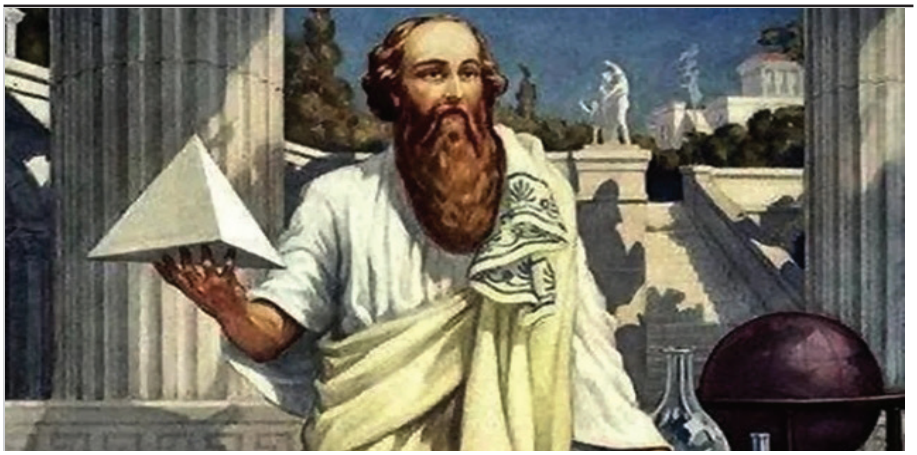
**YÜKSEL - İLHAN ALANYALI FEN LİSESİ**
Dergimiz 13.01.2005 tarih, 25699 sayılı Resmi Gazetede yayınlanan "Milli Eğitim Bakanlığı İlköğretim ve Ortaöğretim Kurumları Sosyal Etkinlikler Yönetmeliği" ne uygun olarak hazırlanmıştır.

**Yazışma Adresi**
Karlıktepe Mahallesi,
Güneş Sokak No:1
Kartal/İstanbul

Tel : 0 216 353 46 47
Belgegeçer : 0 216 353 46 45
Resmi Web Sitesi
www.yiafl.meb.k12.tr

WWW.E-DERGİ.YİAFL.COM





# BITCOIN MADENCİLİĞİ

16

**Bitcoin Madenciliği**
Bitcoin ile para kazanmak

**Bitcoin madenciliği, Bitcoin piyasası içinde yapılan finansal işlemleri onaylamak, transferleri sağlamak ve yeni Bitcoin'ler üretmek içindir.** Bitcoin madenciliği hem blok zincirine işlemler katmakta hem de yeni Bitcoin'i serbest bırakmaktadır.

---

20

Michael Jordan ve Matematik
Havada asılı kalmasının matematiği

21

Asal Çarpanlar ve Şifreleme
Matematik ve kriptoloji

24

BIGDOG
Dünyanın en gelişmiş arazi robotu

# HOŞGELDİNİZ

Bilim ilerlemekten asla sıkılmaz, ama onu takip etmezseniz kısa sürede size çok fark atar. O halde bizim yapmamız gereken bilimin her yönünden fazlasıyla faydalanmak olacaktır. Bilimin dahil olduğu her alan hızla ilerliyor, bu sebeple her nesil birçok yeni teknoloji ile karşılaşmaktadır. Hangi yaşta olsak da olalım adapte olmaya gayret etmediğimizi söyleyemeyiz.
İşte bu nesillerin yetiştiği en güzel okullardan birinde ve bu nesillerden çıkmış en zeki öğrencilerin oluşturduğu bir derginin 2. baskısında yeni bir içerik ile baş başayız. Emeği geçen herkese teşekkürler.

K.Baran YÜCEL / Matematik Öğretmeni

## Genel Yayın Yönetmeni

# Editörlerin Mektubu

Merhaba Sevgili Okuyucularımız,
Büyük bir sevinç ve heyecanla derginizin ikinci sayısını sunuyoruz. Bu sayıyı da öncekiler gibi dolgun bir muhtevayla hazırlamaya çalıştık. Dikkatinizi çekmiştir e-dergimizin ismi artık "**YİAFL TECHMATH**" oldu. Peki, neden böyle bir karar aldık?
Gelişen dünya ile birlikte her geçen gün teknolojinin önemi daha fazla artmakta ve bunların hepsinin matematikle ayrılmaz bir ilişkisi var. E-dergide değindiğimiz yapay zekâ, asal çarpanlar ve şifreleme Buna en güzel örnektir. Bu doğrultuda e-dergimizin sonraki sayılarında da teknolojiye yer vereceğimizden mutluluk duyuyoruz.
Dergiyi keyifle okumanız dileğiyle,

Samet Zengin & Yusuf Ekmekci

Editörler

Elektrikli araç üreticisi Tesla, California'da ölümlü bir kazaya karışan araçlarının otopilot modunda olduğunu açıkladı.

# Otopilot Güvenilir mi?

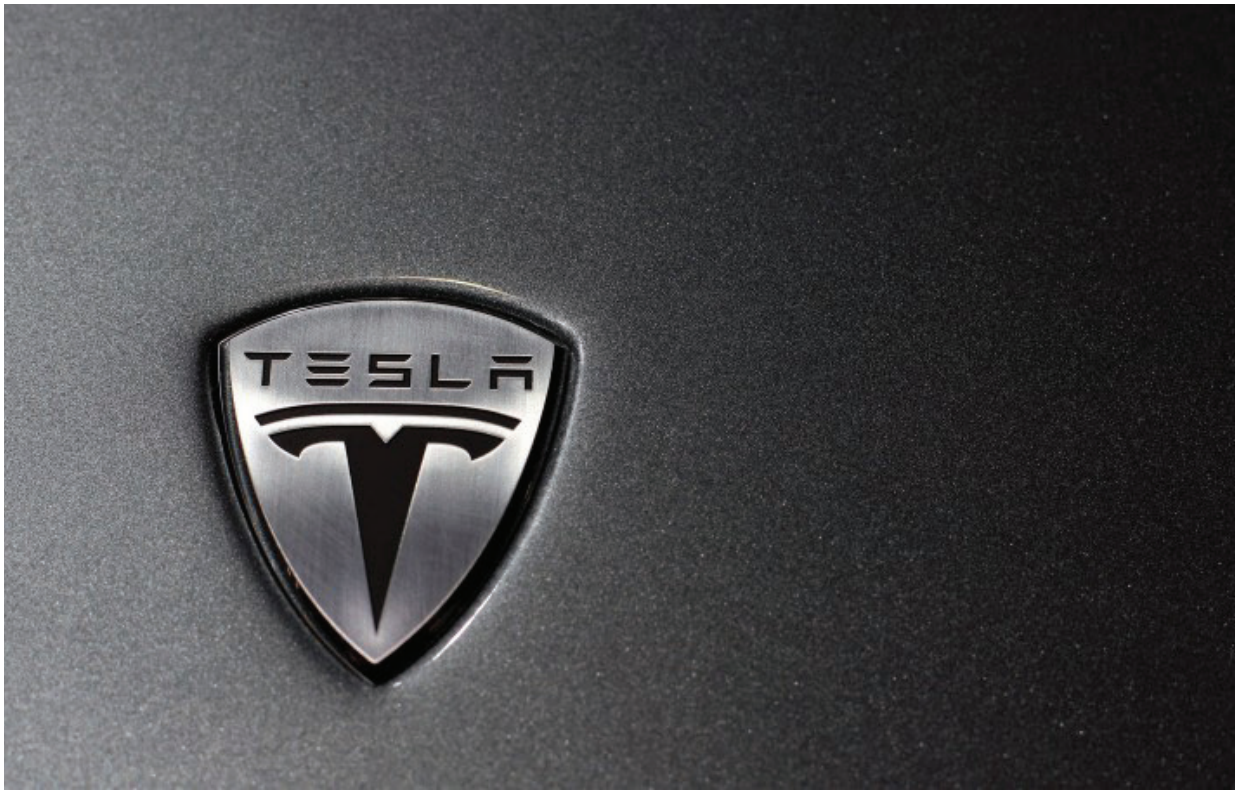
23 Mart'taki kazada Tesla'nın Model X aracı yol kenarındaki bariyerlere çarpıp, alev almıştı.

Şirket hayatını kaybeden 38 yaşındaki sürücünün kazadan saniyeler önce aracı otopilot moduna geçirdiğini açıkladı. Ancak sistemin beton bariyeri algılayıp algılamadığı konusunda bir açıklama yapılmadı.

Şirketin internet sitesinde yer alan açıklamada "Sürücü, kazadan önce kontrolü alması gerektiğine yönelik sesli ve görsel uyarılar aldı. Beton bariyere çarpmadan önce, beş saniye ve 150 metre boyunca beton bariyeri görebilirdi ancak herhangi bir şey yapmadı" denildi.

Tesla'nın araçlarındaki otopilot sistemi fren yapabiliyor, hızlanabiliyor ve belli koşullar altında direksiyon hakimiyetini alabiliyor.

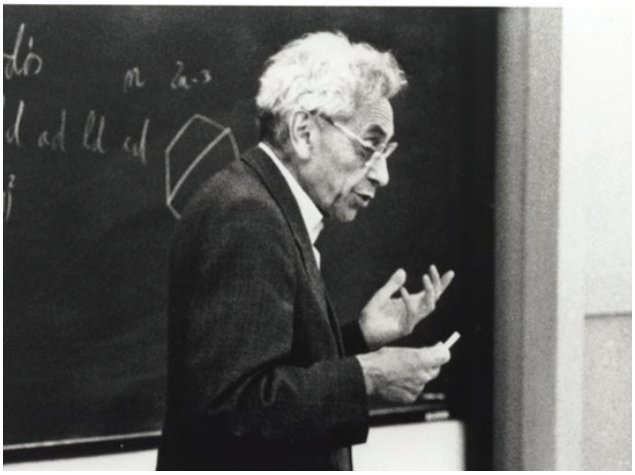
2016'da Fllorida'da Tesla araç kullanan bir sürücü yoluna çıkan kamyonu tespit edemeyince yaşanan kazada ölmüştü.
Bu kazanın ardından araçlarda yeni güvenlik önlemleri alınmış ve sürücü direksiyona uzun süre dokunmadığında otopilot modunun kapanması ve aracın durması gibi özelliklere yer verilmişti.
Yandaki Araç: Tesla Model X




# Tesla'nın Karanlık Yılları

California'da doğan yıldız, yaratıcı fikirler ve güçlü bir ekip çalışması olmasaydı adı daha bilinmeden sönüp gidebilirdi. Tesla, ilk ürünü olan Roadster'ı aslında 2007 yılında 109,000 dolardan satışa sunmayı planlıyordu. Ancak üretimden önce hazırlanan bir denetleme raporu, aracın üretiminin 140,000 dolara geleceğini ortaya koydu. Roadster, bir tane satılmadan borca girilmesine neden olacaktı. Musk, o günlerde Tesla'nın ana yatırımcısı olsa da CEO'su değildi ve kendi hesaplamalarına göre Roadster'ın maliyeti 65,000 dolar olmalıydı. İngiltere'de aracın dış panelini üreten tesise gittiğinde istedikleri malzeme için gerekli malzemelerin bulunmadığını fark etti. Satılması bir yana, Roadster'ın aslında üretilmesi bile mümkün değildi.

# En Garip 5 Matematikçi

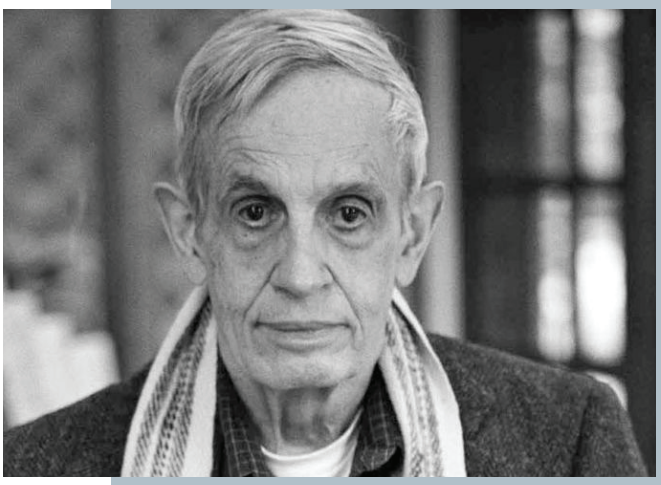


## Paul Erdös (1913-1996)

Tarihteki en heyecan verici matematikçilerden biri olan bu efsanevi matematikçi, hayatını matematiğe adayarak, bir işe ya da eve sahip olmadan başıboş yaşamıştır. Hayatının son senesinde, 83 yaşında, hala teoriler üretiyor, dersler veriyor, matematiğin genç işi olduğu yaygın inanışını reddediyordu. Bu konuyla ilgili olarak bir keresinde: "Bunaklığın ilk göstergesi birinin teoremlerini unutmasıdır. İkincisi fermuarını kapamayı unutmasıdır. Üçüncüsü ise açmayı unutmasıdır," demiştir Erdös .


## Pisagor (MÖ 580-500)

Aynı zamanda bir filozof olarak Pisagor, matematik, astronomi ve müzik teorisinde birçok gelişmeye sebep olmuştur. Filozof Bertrand Russell, "Pisagor, bugüne dek yaşamış insanlar içinde entelektüel açıdan en önemli olanıdır; zeki olsa da olmasa demiştir. Pisagor, aynı zamanda tarihte en çok hakkında teori üretilen matematikçilerdendir; çünkü öğretileri ve okulunda uyguladığı bir sürü tuhaf kural günümüzde halen ilgi çekmektedir.



## John Nash (1928 – 2015)

Oldukça parlak bir matematikçi olan Naslı, Ekonomi dalında 1994 Nobel Ödülü'nü almıştır. 1950'de Princeton Üniversitesi'nden mezun olan John Nash , oyun teorisi alanının modern ekonomide çok önemli bir hale gelmesini sağlayan teoremini formül haline getirmiştir. Hayatıyla ilgili genel ve basit kararları bile -asansöre binmek ya da beklemek, evlenmek ya da evlenmemek- avantaj ve dezavantaj hesaplarına göre yapıp, duygularından matematik kuralları oluşturmaya çabalardı. Kendisine 1959 yılında yapılan muayene sonucu kendisine şizofren teşhisi konmuş, gençken zekasından bahsedilen Nash, hayatının geri kalan kısmını şizofreninin bir içinde bir dışında geçirmiştir. Princeton ve akademik kadro, Nash'in 30 yıl boyunca matematik bölümünde oyalanmasına izin vermiştir. Nash, sessiz kişiliğiyle, tahtaya durmadan tuhaf denklemler yazan ve rakamların gizemlerini araştıran birine dönüşmüştür zamanla.  John Naslı bir keresinde, "Matematikle delilik arasında direk bir ilişki olduğunu söyleyemem ama büyük matematikçilerin delilik ve şizofreni gibi bulgulardan mustarip olduklarına şüphe yok denebilir," demiştir. John Nash ile ilgili en bilindik biyografi örneği, Sylvia Nasar'ın "A Beautiful Mind" adlı yapıtıdır.

# Srinivasa Ramanujan (1887-1920)

Kendisi Hindistan'ın en zeki matematikçisi ve 20. yy. 'ın en büyük matematikçilerinden biri olmuştur. Fakir bir aileden gelen, çekingen ve zorlukla konuşabilen bir çocuk olan Ramanujan'ın matematikle olan ilişkisi bir arkadaşından aldığı ve bir haftada bitirdiği kitapla başlamıştır. Matematik eğitimi alamadığı için, matematiksel gerçeklere ulaşmakta sıra dışı yöntemler kullanmıştır. Matematikçi G.H. Hardy'e göre: "Matematiksel kanıtla ilgili fikirleri en anlaşılmaz olanlarıydı. Tüm sonuçları, yeni ya da eski, doğru ya da yanlış, kendisinin bile kesin olarak açıklamakta güçlük çektiği dolambaçlı yollar, deliller ve başlangıçlarla elde edilmişti."

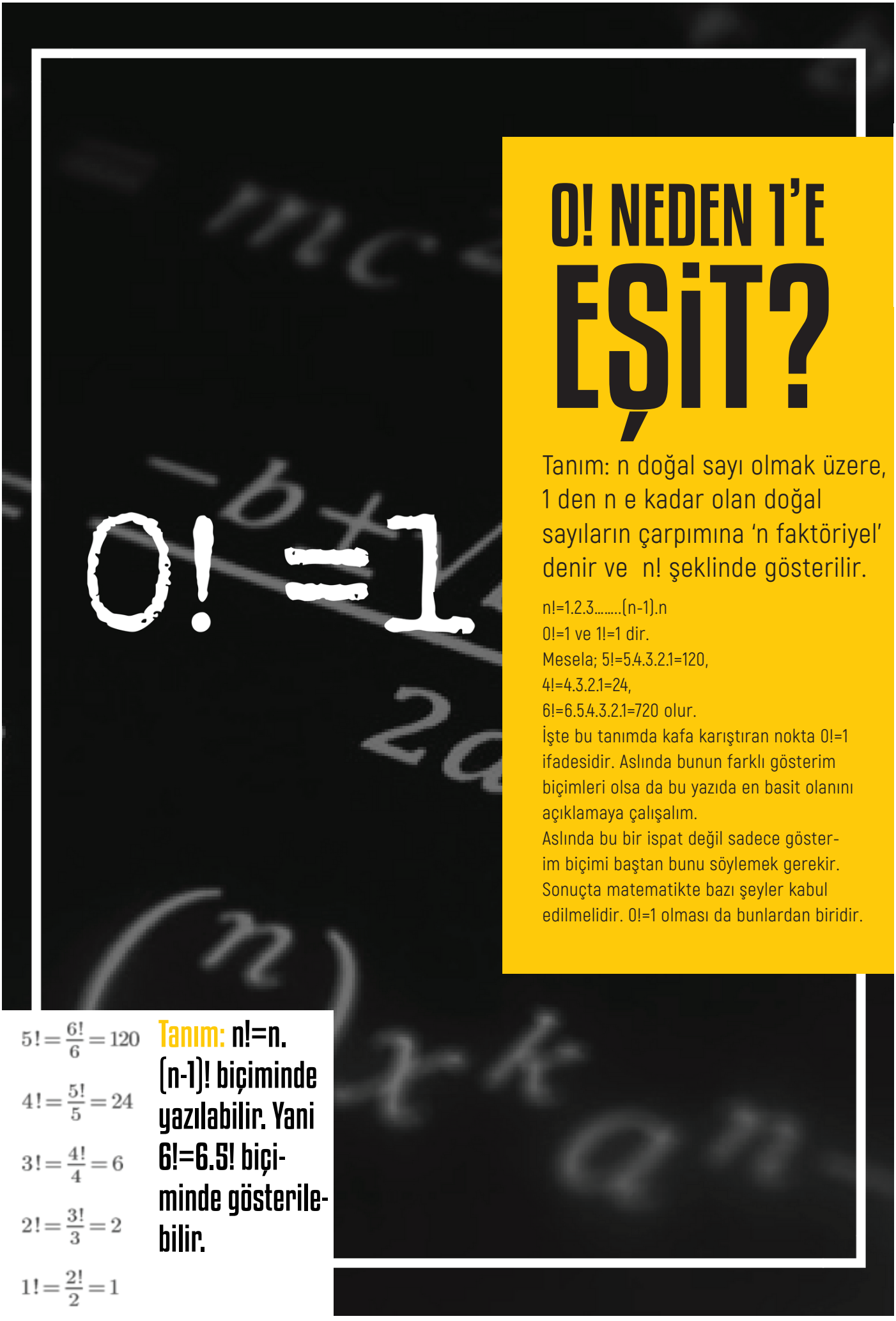
Ramanujan, 1903'te Madras Üniversitesi tarafından bir burs almış; fakat bir sene sonra sadece matematikle ilgilenip, diğer konuları boşladığı için bursunu kaybetmiştir. Trinity Üniversitesi'nde profesör olan Hardy, Ramanujan'ın ona yazdığı ve şu anda tarihi kabul edilen, 100 teorem kapsayan bir mektupla onu Cambridge Üniversitesi'ne kabul etmiştir. Birkaç yıl sonra Ramanujan, katı vejeteryenliği yüzünden zayıflamış ve tüberküloz ölmüştür. O dönem içerisinde sonradan kaybolan sayfalara 600 teorem yazmıştır. Bu kağıtlar ancak 1976'da bulunabilmiş ve Pennsylvania Eyalet Üniversitesi'nden Profesör George Andrews tarafından "Ramanujan'nın Kayıp Defteri" ismiyle derlenmiştir. Ramanujan'nın birçok teoremi, cebir sayılar teorilerindeki modern teoremlerarasında yer almıştır.

> "Ramanujan söylediyse doğrudur."

Buraya kadar herşey normal gözükse de IQ'su 170 olarak bilinen bir insana göre birçok tuhaf huyu göze çarpıyordu: aşırı (patolojik) utangaçlık, vücut seslerine aşırı duyarlılık, sürekli bir sallanma alışkanlığı, mikrop ve hastalık gibi sağlık konularında aşırı hassasiyet. Okuldaki odası biriktirilmiş ve etrafa dağıtılmış yiyeceklerle dolmuş, korkunç bir kokuya sebep olmuştu öğretmenlik yaptığı 2 yıl boyunca. Ancak Kaczynski Berkeley üniversitesindeki görevinden istifa edip, 25 yıllık bir yalnızlığa kapatmıştır kendisini devamında ormanın içinde bir kulübede ve yaşamını tamamen kendi kendine sürdürmenin yollarını aramıştır. Ancak endüstriyel gelişmenin yaşam alanını gittikçe daha çok daralttığına ve çevresindeki doğanın sürekli olarak tahrip edildiğine şahit olması, kendisini önce ufak tefek sabotaj eylemlerine, daha sonra ise kararlı ve planlı bombalamalar yapmaya itmiştir. Bir American Airlines uçağına yerleştirdiği patlamayan bombayla işlediği suçlar "federal suç" kapsamına girmiş ve FBI'ın hakkında dosya açmasına neden olmuştur. University ve Airline kelimelerinden gelen "UN ve A" kısaltmaları ile birlikte bombacı anlamına gelen "bomber" kelimesinin birleşmesinden oluşan Unabomber takma adı ile anılmaya başlamıştır bu tarihten sonra. 1978'den 1995'e kadar 16 bombalama eylemi yapmış, 3 kişinin ölümüne neden olmuş ve sonunda Kaczynski şartlı tahliye ihtimali olmayan ömür boyu hapis cezasına çarptırılmıştır.

## Theodore Kaczynski (d. 1942)

Kendisi, Harvard Üniversitesinden mezun olmuş, sonra Michigan Üniversitesinde matematik alanında doktora yapmış ve Berkeley Üniversitesinin o döneme değin en genç öğretim üyesi olarak görev almıştır. 26 Mayıs 1996 tarihli New York Times "Bir dahiyi, yalnızlık, azim, gizlilik ve titizlikle donatıp, matematiğin gizemi teknolojinin tehlikesinin içine girmesini sağlamak ve onu asla sevmemek, onunla asla arkadaş olamamak ... işte evinin Kaczynski'ye yaptı buydu," diye yazılmıştır.




# 0! NEDEN 1'E EŞİT?

Tanım: n doğal sayı olmak üzere, 1 den n e kadar olan doğal sayıların çarpımına 'n faktöriyel' denir ve n! şeklinde gösterilir.

n!=1.2.3.....(n-1).n
0!=1 ve 1!=1 dir.
Mesela; 5!=5.4.3.2.1=120,
4!=4.3.2.1=24,
6!=6.5.4.3.2.1=720 olur.
İşte bu tanımda kafa karıştıran nokta 0!=1 ifadesidir. Aslında bunun farklı gösterim biçimleri olsa da bu yazıda en basit olanını açıklamaya çalışalım.
Aslında bu bir ispat değil sadece gösterim biçimi baştan bunu söylemek gerekir. Sonuçta matematikte bazı şeyler kabul edilmelidir. 0!=1 olması da bunlardan biridir.

$$5! = \frac{6!}{6} = 120$$

$$4! = \frac{5!}{5} = 24$$

$$3! = \frac{4!}{4} = 6$$

$$2! = \frac{3!}{3} = 2$$

$$1! = \frac{2!}{2} = 1$$

**Tanım:** n!=n.(n-1)! biçiminde yazılabilir. Yani 6!=6.5! biçiminde gösterilebilir.

# Neden Negatif Faktöriyel Yok


gibi bir örüntü çıkar karşımıza. Ve devam edersek...

$$(-1) = \frac{0!}{0} = \frac{1}{0}$$

Eşitliğini elde ederiz. Peki elimiz değmişken biraz daha devam edelim diye düşünürsek orada işler biraz karışacaktır. Neden derseniz...

$$0! = \frac{1!}{1} = 1$$

Ortaya çıkacaktır. Bu da matematikte tanımsız bir bölüme ulaşmak demektir. Demek ki daha fazla devam edemeyiz, örüntü tamamlanmıştır.

0!=1 eşitliğinin nedenini basit bir biçimde, bir başka şekilde daha sezinleyebiliriz aslında.

Faktöriyel kavramı permütasyon ve kombinasyon konularının temelini oluşturmaktadır.

n! diye tanımladığımız şey aslında n tane farklı nesneyi kendi içinde nasıl sıralayabileceğimizin sayısıdır.

Yani 3 tane farklı gömleğinizi bir rafa sıraya dizmek isterseniz bunu 3!=6 kadar şekilde yapabilirsiniz.

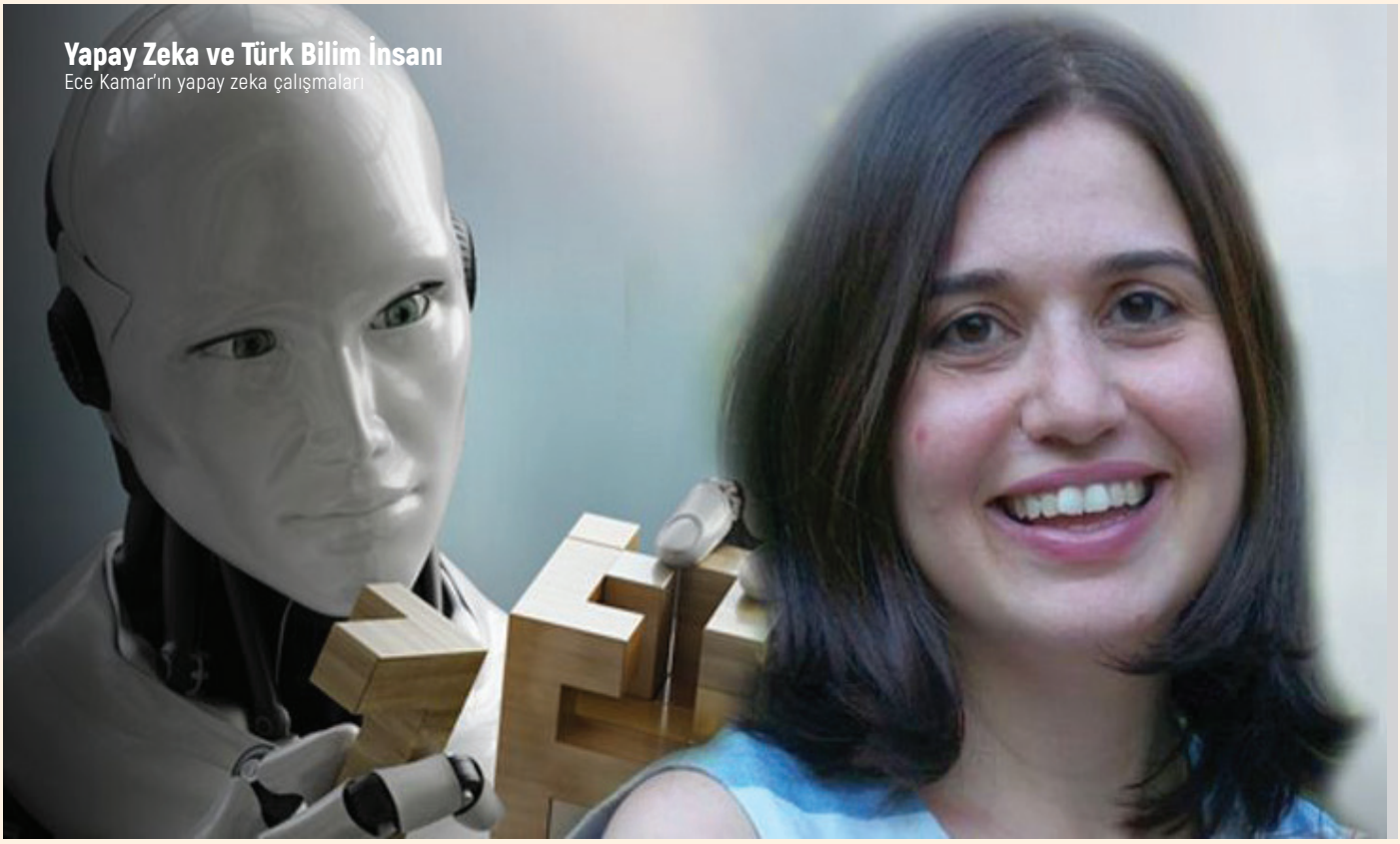
Peki gömlek sayınız iki olursa. Elbette o zaman cevabınız 2!=2 olacaktır. Bir tanecik gömleğiniz varsa da o zaman üzgünüz sadece bulunduğu biçimde kalacaktır. :)

Yani 1!=1 olacaktır.

Eğer hiç gömleğiniz yoksa işin içine biraz felsefe karışıyor. "Hiç gömleğim yok, bunu kaç farklı biçimde sıralayabilirim?" Cevabınız elbette sıralayamam olacaktır ama unutmayın bu cevap matematikte boş kümeye karşılık gelmektedir.

Anlatılanlar inandırıcı gelmedi ise yazıyı hazırlarken referans olarak kullandığımız aşağıdaki videoya da göz atabilirsiniz.

**QR KOD ETKİLEŞİMLİ VİDEO** Ali Nesin neden 0! 1'e eşittir:



**Yapay Zeka ve Türk Bilim İnsanı**
Ece Kamar'ın yapay zeka çalışmaları

# Yapay Zeka'ya Yön Veren Türk Bilim İnsanı

Ece Kamar, 1983 yılında İzmir'de doğdu. Bornova Anadolu ve İzmir Fen Lisesi'ndeki eğitiminin ardından üniversite eğitimini Sabancı Üniversitesi Bilgisayar Bilimi ve Mühendisliği Bölümü'nde tamamladı. Ardından Harvard Üniversitesi Bilgisayar Bilimlerinde doktorasını yaptı.

Harvard'da Robert L. Wallace Ödül Bursuna ve Microsoft Araştırma Lisansüstü Araştırma Bursu ödülüne layık görüldü.

Harvard'daki tez çalışmasında etkili insan-bilgisayar takım çalışması için modeller ve algoritmalar üzerine odaklananan Ece Kamar, şu sıralarda Redmond'taki Microsoft Araştırmaları bünyesinde Uyarlamalı Sistemler ve Etkileşim grubunda kıdemli araştırmacı olarak görev yapıyor.

## Ece Kamar'ın makaleleri en saygın yapay zekâ yayınlarında, 40'tan fazla hakemli dergide yayınlandı.

Halen Microsoft'ta yapay zekâ algoritmaları üzerine araştırmalar yapan Türk mühendis, bir taraftan Beyaz Saray için rapor hazırlıyor, diğer taraftan da Microsoft'a danışmanlık hizmeti veriyor. 34 yaşındaki Kamar'ın uzman olduğu konu ise yapay zekâların ahlaklı ve vicdanlı olması.

Devamını onun sözlerinden aktaralım:

"İnsanların hayatına dokunan kararların bilgisayarlar tarafından alındığı bir döneme giriyoruz. Aynı zamanda kritik zararların da verilebileceği bir dönem. Toplumdaki birçok kritik karar otomasyonla verilmeye başlandı. Mesela şu anda ABD'de hakimlere yapay zekâ algoritmalı yazılımlar veriliyor.

Türk Mühendisin Y

Biri hakim önüne çıkarıldığında kefaletle serbest mi bırakılacağının, yoksa tutuklu mu kalacağının kararı yapay zekâ tarafından veriyor. Yapay zekâ algoritmalarının kullanıldığı eğitimden insan kaynaklarına kadar insana dokunan birçok örneği var. Bir sürücüsüz (otonom) otomobil hata yaptığında insanlar ölebilecek. Mesela bir Tesla sürücüsü hayatını kaybetti. Bu nedenle bizim için çok önemli bir konu haline geldi.

> "Yapay zekânın kötü şeyleri öğrenmesini nasıl engelleriz, eşitlik nasıl sağlarız?"

Yapay zekânın toplum üzerindeki etkisini ele alıp, insanların hayatına gerçekten faydalı olup, iyi değerler katması gerekiyor. Yani sürücüsüz bir otomobil kaza anında kime veya neye vuracağının seçimini yapabilmeli. Birini öldürmek yerine zarar görmeyecek bir cisme çarpabilecek, veya öldürme kaçınılmazsa tercih yapabilecek.

ABD'deki şirketlerin insan kaynakları departmanında kullandığı yapay zekâ algoritmalarının en büyük sorunu kadınlara yapılan ayrımcılık. Makineler verilerden öğrenim çıkarırken o pozisyonda daha önce çalışmış kişilere bakıyor. Yazılımcılar arasında kadınların oranı %10 olduğu için yapay zekânın insan kaynaklarına önerdiği kişiler de çoğunluk erkek oluyor. Çünkü yapay zekânın kanıtı böyle. Bu tarz önyargıları yapay zekâ algoritmalarında çok fazla görmeye başladık.

İyi niyetli bir yapay zekâ kullanıyorum diye bir konu yok. Örneğin; Los Angeles'taki hangi evsiz gençlere AIDS eğitimi verilmesi gerektiği üzerine bir yapay zekâ uygulaması geliştirildi. 'Ne kadar iyi niyetli bir algoritma' diye düşünebilirsiniz. Ancak işin arka planı öyle değil. Hangi gençler bu eğitimi alacak veya alamayacak. Oldukça eşit olmayan bir durum söz konusu olabilir.

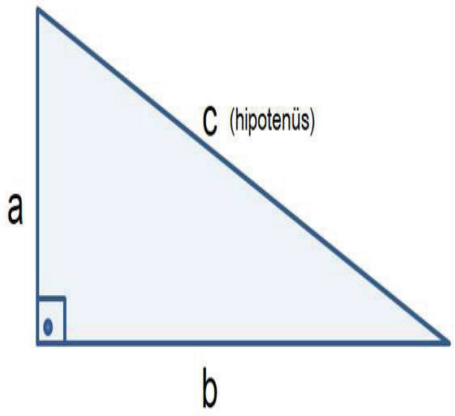
Şu anda Microsoft'ta bilgisayarları verilerle eğitirken verinin temizlenmesi üzerine çalışıyoruz. Bu tarz problemleri makinelere öğretmeye çalışıyoruz. Bazı koşulları öğreterek, makinelerin insanlar hakkında daha adil kararlar vermesini sağlıyoruz. Yapay zekânın öğrenme mekanizmasını değiştirip, değer yargılarıyla öğrenmesi üzerine çalışıyoruz. Aynı zamanda birçok problem verinin kötülüğünden kaynaklanıyor. Hiçbir veri mükemmel değil. Verinin içinde normalde bilgisayarın bilmesi gereken ama temsil edilmeyen taraflar var.

Sistemler, yazılımlar sana şunları beğenmelisin diyor. Siz bu seçeneklerden seçince, buna göre öneriler oluşturuyor. Ancak oluşturulan bu öneriler oldukça kısıtlı ve bu kısıtlı seçenekler kırılamıyor. Amacımız bunu aşmak. Şu anda geliştirdiğimiz yapay zekâ örneklerine sadece veriler yerine insanların keşfetme duygusunu da aşılamaya çalışıyoruz."

apay Zeka Başarısı

# Sayılara Tapma

Yazdığı eserlerin hiçbiri günümüze ulaşmasa da matematiğe olan büyük katkısı yani Pisagor Teoremi ile tanıyoruz onu.




$$a^2+b^2=c^2$$

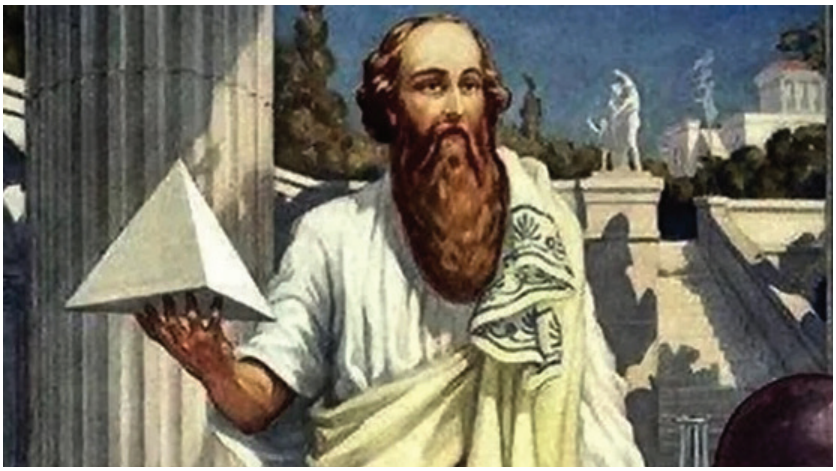
## Pythagoras of Samos

Matematiğin başlı başına bir inanç olabileceğini hiç düşündünüz mü? Ya da sayıları Tanrı'nın yaratmadığını, sayıların Tanrı'nın ta kendisi olduğunu? Bize çok uzak görünse de bu fikirler bundan yaklaşık iki bin beş yüz yıl önce bazı matematikçiler tarafından kabul görmüştü. Öyle ki, felsefesi matematiğe dayanan bir din bile oluşturulmuştu. Matematiği inancın temeline koyan bu toplumun lideri ve kurucusu ise neredeyse hepimizin aşina olduğu bir isimdi: Pisagor...

Peki MÖ 570'li yıllarda doğan ve yaklaşık yetmiş yıllık hayatıyla binlerce yılı etkilemiş olan Pisagor'u Pisagor yapan neydi? Ne yapmıştı da matematikçi oluşunun yanı sıra bir din adamı, bir filozof ve bir lider olmayı başarabilmişti?..

Tales ile aynı zamanda yaşamış olması ve Tales kaynaklı matematik eğitimi alması onun için büyük bir şanstı. Doğduğu şehir olan Sisam'dan bir süre sonra ayrılmış ve Babil ile Hindistan'a gitmişti. Böylece Konfüçyüsçülük ve Budizm'i öğrendi. Bunlarla felsefesini ilerlettikten sonra matematiğini de ilerletmek için Mısır'a ve Anadolu'ya gitti. Kendi eğitimini tamamladıktan sonra yeniden, doğduğu şehir olan Sisam'a gitmiş ve burada dersler vermeye başlamıştı. Kendisine ev sahipliği yapan ve aynı zamanda öğrencisi olan bir aristokratın kızıyla evlendi. Dik üçgendeki en uzun kenar olan 'hipotenüs'ün Pisagor'un karısı olduğuna dair söylentiler olsa da kesin olarak bir bilgimiz yok. Bir süre matematik dersleri verdikten sonra, burada bir cemiyet kurdu. Tuhaf ve katı kuralları bulunan bu cemiyet ilk başlarda gizliydi.

# k Pisagor



1. Aklın sembolü
2. Fikrin sembolü
3. Uyumun sembolü
4. Tanrısal gücün sembolü
5. Evliliğin sembolü
6. Yaratmanın sembolü
7. Neslin sembolü
8. Kuvvetin sembolü
9. Adaletin sembolü
10. Kutsal karenin sembolü

Pisagor, Pisagorcular ile birlikte kurduğu okulda matematik ve müzik üzerine eğitim veriyor ve araştırmalar yapıyordu. Pisagor Teoremi de bu okulda bulunmuştu. Dik üçgendeki dik kenarların kareleri toplamının uzun kenarın karesine eşit olduğunu söyleyen bu teoremde 3-4-5 veya 5-12-13 gibi rasyonel sayılar kullanıldığında hiçbir sorun oluşmamıştı.

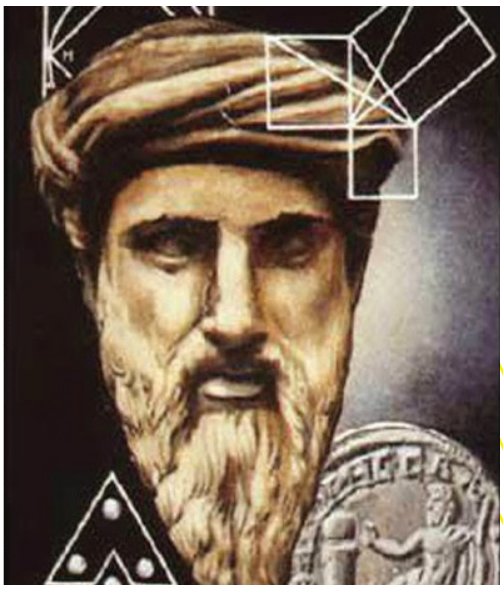
Pisagor öğretisine göre Tanrı, rasyonel sayılardı...
Fakat mesela dik kenarları ikişer birim olan bir dik üçgende hipotenüs, rasyonel olmayan yani irrasyonel çıkıyordu. Pisagor öğretisini derinden sarsan bu teorem, cemiyetin dağılmasını engellemek için bir süre saklandı. Hatta bir deniz yolculuğunda Pisagorculardan birinin "Düşündüm de bu soruna bir çözüm bulamadım." demesi üzerine denize atıldığına dair söylentiler bile var.

Pisagor Teoremi ile derinden sarsılan Pisagor ve yandaşlarına halkın bir süre sonra inancı ve tahammülü kalmamış ve matematiği inançları edinen Pisagor ve yandaşları, halk tarafından kendi okulları içinde diri diri yakılmış...

Fakat üyelerinin sayısı artınca halka da tanıtıldı. **Kadın üyesi bulunmayan bu cemiyetin tuhaf kurallarından bazıları şunlardı:**

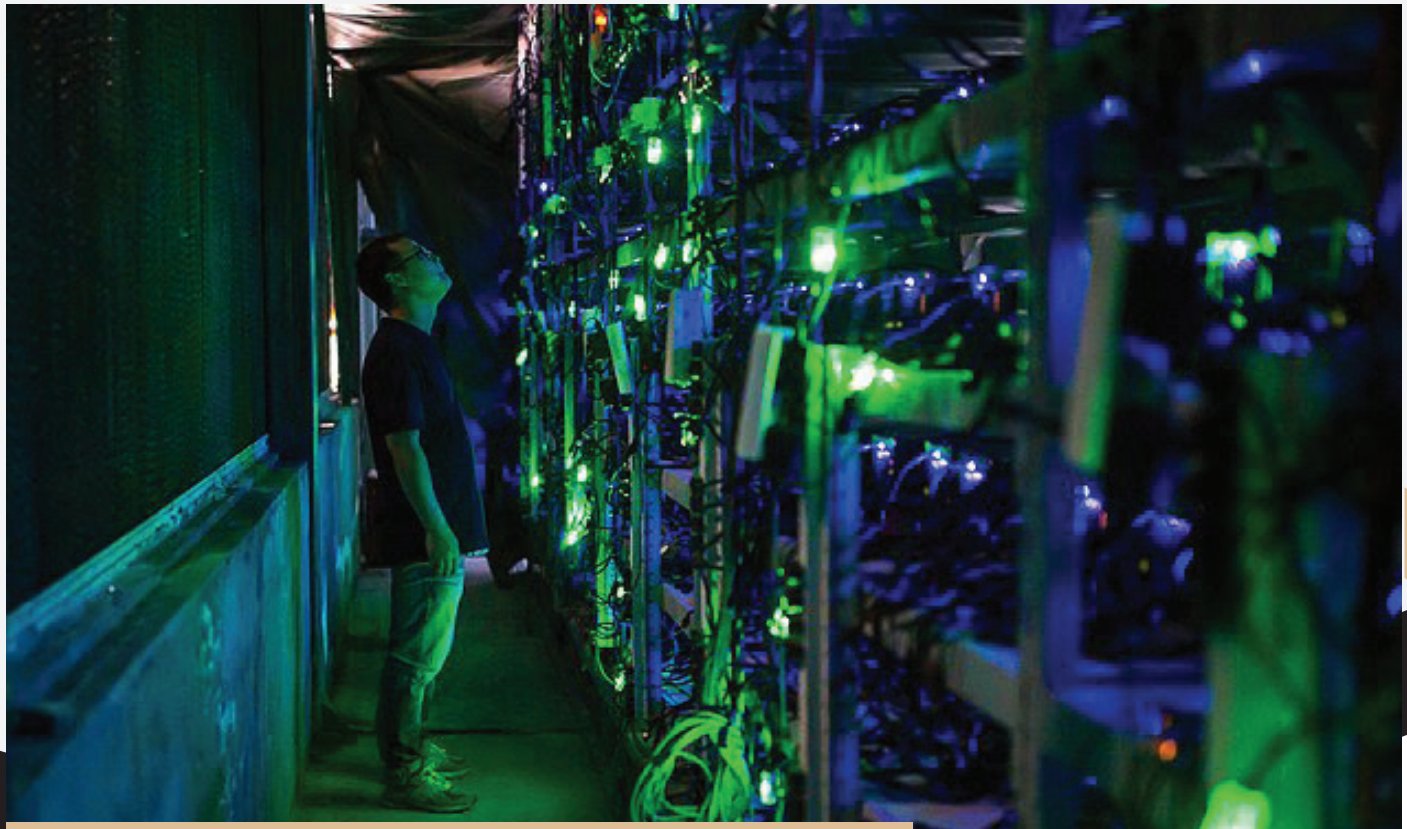
Bu tuhaf kurallar sebebiyle, Pisagor; halkın gözünde bir kahin. hokkabaz ve şarlatandı. Fakat cemiyet üyelerine bakıldığında, Pisagor; çağının azizlerinden biriydi, hatta kimine göre bir peygamberdi...

Galileo Galilei, "Evrenin kitabı, rakamlarla yazılmıştır." demiştir. Pisagor'un yaşam felsefesi tam da bu sözdü. Rasyonel sayıların tapılacak şeyler olduğunu düşünen Pisagor ve yancıları, rakamların bazı özellikler taşıdığına inanıyordu:



Şifa MUTLU

# Bitcoin Madenciliği



## Bitcoin Madenciliği Nedir? Neden Yapılır?

Bitcoin madenciliği, Bitcoin piyasası içinde yapılan finansal işlemleri onaylamak, transferleri sağlamak ve yeni Bitcoin'ler üretmek içindir.

### Bitcoin ile Para Kazanın

Blockchain temelinde, merkezi olmayan bir sistemle çalışan Bitcoin madenciliği en hızlı blok üreten ve işlemleri onaylayan kullanıcıya ödül verir. Her yeni Bitcoin üretildiğinde oluşan blokların zorluk seviyeleri de artmaktadır ve bu nedenle madencilik(mining) için çok güçlü işlemcilere sahip bilgisayarlar gerekmektedir.

# Bitcoin Madenciliği Nasıl Çalışıyor?

Bitcoin madenciliği hem blok zincirine işlemler katmakta hem de yeni Bitcoin'i serbest bırakmaktadır.

Madencilik süreci, son işlemleri blok halinde derlemek ve hesaplamada zor bir bulmacayı çözmeye çalışmakla ilgilidir. Bulmacayı çözen ilk katılımcı, bir sonraki bloğu blok zincirine yerleştirip ödülleri topluyor. Ödüller madenciliği teşvik ediyor ve hem işlem ücretlerini (Bitcoin şeklinde madene ödenen) hem de yeni çıkan Bitcoin'i içeriyor. Piyasada bulunabilecek en fazla Bitcoin sayısı 21 milyondur. Çok sorulan bir soruya da hemen burada cevap verelim. Peki en fazla Bitcoin sayısına ulaşıldığında madencilik bitecek mi? Cevap tabiki hayır.

Tüm Bitcoin alım-satım, transfer işlemleri Bitcoin'in bağlı olduğu Blockchain kayıtlarına işlenir ve üyelerden yapılan her işlemin onaylanması istenir. Yapılan Bitcoin işlemleri üyeler tarafından onaylandığında ilgili tutar cüzdanınızdan düşülür ve karşı tarafa eklenir. Bitcoin'lerinizi bir dijital cüzdan aracılığı ile tutar ve saklarsınız. Bu cüzdanın adresine herkes ulaşabilir ve bakiyenizi bile görüntüleyebilirler ancak sizin kim olduğunuzu bilemezler. Cüzdanın şifrelenmesi de iki farklı katman ile yapılır. Birisi genel bir şifre ile ulaşabilirsiniz.

## Blockchain Güvenilirliği

### Sadece size özel bir şifre ile alım-gönderim işlemi yapılabilir.

Madencilik(mining) sayesinde bu transfer işlemleri Blok zincirlerine eklenir ve işlenir, bu zamana kadar yapılan ve gelecekte yapılacak olan tüm Bitcoin işlemleri blockchain kayıtları üzerinden herkes tarafından görüntülenebilir. Madenci de bu işlem sonunda bloğu tamamladığı için ödül olarak belirli bir miktarda ödül BTC alır. Bitcoin'de yapılan işlemlerin sayısı her geçen gün arttıkça blok uzunlukları da oldukça fazla olmakta(defterde tutulan kayıtlar gibi düşünün). Maksimum BTC sayısına yaklaşıldıkça da blok başı dağıtılan ödül BTC miktarları zamanla düşmektedir. Tüm bu sistemi Bitcoin'in üretildiği ve işlemlerinin yapıldığı yazılımsal altyapıda takip edilir ve onaylanır.

# Bitcoin Madenciliği Güvenli Mi?

Bitcoin madenciliği merkezi olmayan bir yapı üzerinde ilerler(-decentralized). İnternet bağlantısı olan herkes uygun donanıma katılabilir. Bitcoin ağının güvenliği, bu merkezi olmayan decentralized yapıya bağlıdır, çünkü Bitcoin ağı, karar üzerine "fikir birliğine" dayalı kararlar verir. Bir bloğun blok zincirine dahil edilip edilmeyeceği konusunda bir anlaşmazlık veya çakışma varsa, karar basit bir çoğunluk konsensusu ile etkili bir şekilde, madencilik gücünün yarısından fazlasını kabul ederse, karar verilir ve madencilikteki blok ekleme işi tamamlanır. Yani sistem tamamen kullanıcılara bağlıdır ve oy birliği ile ilerler.

## Bitcoin Madenciliği Nasıl Yapılır?

Bitcoin madenciliği yapabilmeniz için öncelikli olarak bir internet bağlantısına ve uygun donanıma/sisteme ihtiyacınız vardır. Bitcoin madenciliği üretilen blokların şifrelenmiş versiyonlarını oluşturmak ve bunu onaylamak üzerine çalışır. Bu bloklar içerisinde yukarıda daha önce söylediğimiz gibi Bitcoin sistemi içerisinde yapılan finansal işlemler yer alır. Bitcoin madenciliği şuanda ASIC cihazlar üzerinden yapılıyor. Bunu da yazının hemen alt kısmında, bir sonraki maddede aktaracağız.

Bitcoin madenciliği yapabilmek için birden fazla yol var;

* Donanım ile Bitcoin(BTC) Madenciliği Yapmak
* Cloud Mining ile Bitcoin(BTC) Madenciliği Yapmak
* Bilgisayar ile Bitcoin(BTC) Madenciliği Yapmak

Şimdi gelin hep birlikte Bitcoin(BTC) madenciliğinin nasıl yapıldığını inceleyelim.

# Madencilik Yöntemleri

## Antminer, Dragonmint ve Avalon ile Bitcoin Madenciliği

500 dolardan başlayan Antminer serileri, Dragonmint ve Avalon serileri bulunmaktadır. Antminer'ın son cihazı S9 20 bin TL'den başlamaktadır. Yurtdışında satılan bu cihazların ülkemize girişi fiyatından dolayı gümrüğe takıldığı için fiyatları yüksektir. Amazon ve Türkiye'deki popüler e-ticaret siteleri üzerinden satın alınabilmektedir. Bir yılın sonunda tahmini 0.01 BTC üretebilmek için en az 320 GHz'lik işlemci kapasitesine sahip olmalısınız.

## Cloud Mining ile Bitcoin(BTC) Madenciliği Yapmak

Donanım maliyetleri oldukça fazla ve elektrik giderleri oldukça fazla. Peki elinizde 100 dolar var diyelim. Bu parayla Bitcoin madenciliği yapmak mümkün mü? Cevap evet. Cloud yani bulut tabanlı, birden fazla cihazın bulunduğu web servislerine kayıt olarak, online cihaz gücü kiralayabilir ve bu sayede üretime başlayabilirsiniz. Bunun için Hashflare, Genesis-mining, S4mining(Türk girişimi) gibi platformları kullanarak Bitcoin üretebilirsiniz.

## Bilgisayar ile Bitcoin(BTC) Madenciliği Yapmak

Geldik zurnanın zırt dediği yere. Yukarıda bilgisayar ile Bitcoin madenciliğinin 2010 ve 2013 yıllarında karlı olduğunu ve yapılabilirliğini söylemiştik. Şuanda 0.01 BTC kazanmak için(o da 12 ayda) 320 GHz'lik bir işlemciye sahip olmamız gerektiğini belirtmiştik. Yılda ben diyeyim 2, zorlarsanız belki 3 TL kazanabilirsiniz. Bilgisayar ile BTC madenciliği yapamazsınız. Ama biz yine de size denemek isterseniz diye Bitcoin madencilik programlarının listelerini aşağıya bırakalım. Bitcoin üretmek için; Nicehash  Computta Minergate indirebilirsiniz.

## Bitcoin Madenciliği Karlı Bir İş Mi? Hadi Açık Konuş Editör Kardeş...

Derseniz ki bu işe girelim mi ne yapalım diye; bu yazı bir yatırım tavsiyesi değil. Sizlere işin nasıl olduğunu ve döndüğünü aktarmak istedik. Sizlere 0.01 BTC üretmek için 320 GHz'lik bir işlemci gücüne sahip olmanız gerektiğini de aktardık. Bitcoin madenciliğine girmek için bir sene öncesi çok ama çok karlı bir tablo çıkarabilirdi sizin için. Ancak her geçen yıl üretilen blok başına dağıtılan Bitcoin miktarı da azalmakta. İlk üretimin olduğu yıllarda blok başına 50 BTC dağıtılırken, 210 bin blok sonra 25 BTC, ardından 12,5 BTC'ye kadar düştü. 2 sene içerisinde de 6,25 BTC'ye düşeceğini bitcoinblockhalf.com üzerinden takip edebilirsiniz.


# Jordan ve Matematik

$$h = h_0 + V_0(t) + \frac{1}{2} g(t^2)$$

## Jordan'ın Havada Asılı Kalmasının Matematiği

NBA'in resmi sitesine göre, Michael Jordan tüm zamanların en büyük basketbolcusu. Onu bu kadar popüler yapan sporcu kimliğinin yanısıra sıçrama yeteneği. Faul çizgisinden potaya yaptığı smaçlar Jordan'a "Air Jordan" ve "His Airness" lakaplarını getirdi. Michael Jordan'ın bir keresinde şöyle dediği bilinir: "Uçup uçmayacağımı bilmiyorum. Bildiğim, havadayken bazen aşağı inmek zorunda olmadığımı hissediyorum." Fakat yukarı çıkanın eninde sonunda aşağı inmesi gerektiği gerçekliğini hepimiz biliyoruz. Aslında desteksiz olarak yerden zıpladığınız da ayağınızı yerden kestiğiniz zamanla dokunduğunuz zaman arasındaki fark zaman en fazla bir saniyedir. Çünkü atlar atlamaz yer çekimi bizi kendisine geri çeker hem de 9,8 metre/saniye kare bir hızla.

İki matematikçi, Andy Peterson ve Zack Patterson, bir insanın havada kalma süresinin ne kadar olabileceğini bir denkleme döktü sonunda. Soldaki denkleme göre bir nesnenin alabileceği yükseklik, nesnenin yerden ilk yüksekliği, artı ilk hızıyla havada kaldığı saniye sayısının çarpımı, artı yerçekimi ivmesinin yarısının havada kaldığı saniye sayısının karesiyle çarpımıdır. Şimdi Michael Jordan'ın muhteşem smaçlarını modellemede bu denklemi kullanalım.

Diyelim ki MJ, herkes gibi, yerden sıfır metreden başlasın ve saniyede 4,51 metre ilk hızla zıplasın. Dikkat ederseniz denklem ikinci dereceden yani bu denklemi koordinat düzleminde havada harcanan zaman ile yükseklik arasındaki ilişki biçiminde çizersek karşımıza bir parabol çıkacaktır.Parabolün tepe noktası, yerden 1,038 metre ile azami yüksekliği ve x eksenini kestiği yerlerde yerden havalanma ve iniş zamanlarını gösterir bize. Jordan'ın harcadığı toplam zaman 0,92 saniye. Gördüğünüz gibi dünyanın yerçekimi işleri oldukça zorlaştırıyor. Bu arada Micheal aynı oyunu ayda oynasaydı aynı eforu harcayarak 6 metreden daha fazlasına zıplayabilir ve beş buçuk saniyeden fazla havada asılı kalabilirdi.Bu uçabildiğine inanmak için yeterli bir süre...

# Asal Çarpanlar ve Şifreleme

## İnsan asal sayıları tanımladığı zamandan itibaren, sürekli asal sayıların ardından koşar oldu. Verilen bir sayı asal mıdır, değil midir? Sayının asal çarpanları nelerdir?

Bu sorulara cevap arayışı çoğu zaman bir çok kişiye anlamsız gibi gözükse de, soruların cevapları bulunduğu zaman güvenliğimiz tehlikeye düşebilir. Çünkü asallar 1977'den beri şifrelemenin bel kemiği, şifrelemeyse banka hesaplarımızdan tutun da ulusal güvenliğimize kadar gizlilik içeren her türlü konunun güvenliğinin temeli.Bilinen ilk şifreleme örneğine M.Ö. 1900'lerde Mısırlıların hiyeroglif yazısında rastlanır. O zamandan günümüze değişen çok şey oldu elbette. Bunlardan biri de iletişim sistemleri. Bugün düz metinlerimizi ulakla göndermek yerine elektronlarla gönderiyoruz, ancak yolladığımız metin ne olursa olsun hala güvenli bir biçimde ulaşmasını istiyoruz. İşte bu aşamada kullandığımız aletin yani bilgisayarın doğasına dönüp onun yapısına uygun bir koruma sistemi geliştirmek gerekir.Diyelim ki karşı tarafa bir mesaj yollayacaksınız. Ama kimsenin eline geçmemesi gerekiyor. Bir yolu şu olabilir. Karşı tarafla mesajlaşmaya başlamadan önce bir toplantı yaparsınız ve kullanacağınız şifreye karar verirsiniz. Böyle iki tarafın da şifreyi bilmesi **simetrik** şifreleme örneğidir.

Fakat şifreniz bir şekilde yanlış kişilerin eline geçerse her şey biter! Kaldı ki her zaman şifre konusunda ortak bir karara varmak için toplantı yapmak mümkün olmayabilir. Üstelik konu iki kişi değil de daha çok insan arasında iletişim olunca şifreyi bilen bir o kadar da insan olması gerekir ki durum gittikçe tehlikeli olmaya başlar.

1960'ların sonlarına kadar simetrik şifrelerle idare edilmeye çalışılmış olsa da daha güvenli bir şifreleme sistemine şiddetli bir şekilde ihtiyaç duyulduğu aşikardı.
1970'de İngiliz matematikçi James Ellis yeni bir şifreleme sistemi üzerinde çalışmaya başladı. Basit fikri, bir anahtarı; şifreleme anahtarı ve şifre çözme anahtarı biçiminde ikiye bölmeye dayanıyordu.

Her ne kadar kendisi matematiksel bir çözüme ulaşamasa da bu fikir kendinden sonra gelenlere yol gösterdi.
Devamında sahneye İngiliz matematikçi Clifford Cox çıktı. Cox asal çarpanları kullanarak şifreleme fikrini ortaya attı. Çalışmasının temelinde Euler'in henüz bilgisayarın olmadığı yıllarda ürettiği bir teorem vardı.p asal ve n sıfırdan farklı olmak üzere $n^{p-1}=1 \pmod p$


ANKA
corporation
BİLİNMEZDEN
BİLİME
Bilim, sanat ve teknoloji projelerimiz için genç beyinler arıyoruz.
Hayallerini şimdi gerçekleştir, fırsatı kaçırma.
HEMEN BAŞVUR!
iletisim@bilimx.net
BİLİMX

# Açık Anahtarlı Şifreleme

1977'de üç bilim insanı başkalarının kolay kolay çarpanlarına ayıramayacağı sayıyı ilan edip çarpanları yalnızca mesajı alacak kişinin bildiğini temel alan güvenli bir algoritma yazmayı başardılar. Böylece "Öyle bir şifre olsun ki onu çözecek anahtar sadece benim elimde olsun" hayali gerçek olmuştu çünkü artık sadece sayının asal çarpanlarını bilen kişi metni okumaya hak kazanıyordu. RSA şifrelemesi, Ron Rivest, Adi Shamir ve Leonard Adleman tarafından bulunan ve kendi isimlerinin baş harflerini kullanan açık anahtarlı bir şifreleme yönetimidir.


Her ne kadar bu algoritma çok büyük sayılar sayesinde güvenliğimizi sağlıyor olsa da, biz anlaşılmasını kolaylaştırmak açısından iki küçük asal sayı seçerek işe başlayalım. Seçtiğimiz 2 asal da p=2 ve q=5 olsun ki çarpımları pq=10. Algoritma kurallarımız şöyle diyor:

Önce A=(p-1)(q-1) çarpanını hesaplayın:

A =(2-1)(5-1)=4

A ile ortak böleni olmayan ve 10'dan küçük bir sayı seçin: Örneğin e=7

Sonra e x d = 1(mod A) denkliğini sağlayan d sayısını bulun:

7 x 3=1(mod4)] olduğuna göre o zaman d=3

Metni bize gönderecek kişiye ve herkese ilan ettiğimiz bilgi iki asalın çarpımı(10) ve aklımızdan seçtiğimiz e(7) sayısı. İstediğimiz şifre ise metnin karşılık geldiği sayının e dereceden kuvvetinin mod pq sayısında eşiti...Şimdi bir deneme yapalım: Yollamak istediğimiz şifre DERS olsun, kolaylık olması açısından her harfi bir rakam ile eşleştirelim.

D=1 E=2 R=3 S=4

DERS=1234 oldu e=7 ve p.q yani modumuz ise 10

$1^7 = 1 (mod 10)$

$2^7 = 8 (mod 10)$

$3^7 = 7 (mod 10)$

$4^7 = 4 (mod 10)$

Başlangıçta seçtiğiniz sayının bir değil de 100 basamaklı olduğunu düşünürseniz, bu iki sayının çarpımının çarpanlarının bulunması aylar ya da yıllar alacaktır. Kullanılan algoritma ve harcanan para bu süreyi biraz değiştirse de sonuç yine de istendiği kadar hızlı olmayacaktır.

RSA dünyada en yaygın kullanılan açık anahtarlı algoritmadır. Aynı zamanda tarihte en çok kopyalanan yazılımdır. Dünyadaki her internet kullanıcısı bilerek ya da bilmeyerek RSA ya da bir çeşidini kullanıyor. Bu sistemin başarısı da asal çarpanlarına ayırmanın zorluğundan kaynaklanıyor.

# BIGDOG

## Dünyanın En Gelişmiş Engebeli Arazi Robotu

Boston Dynamics, ürettiği robotlarla insanların yapacağı iş yükünü daha da azaltmak amacına doğru ilerliyor gibi görünüyor. Tabii ki teknolojinin kullanımının suistimal edilmemesi şartı sağlanırsa kötü gelişmeler değil bunlar. Çeşitli arazilerde, insanların giremediği yerlerde, arama kurtarmalarda, yangın, deprem, sel gibi durumlarda kurtarıcı olarak geliştirilebilecek makineler çıkacaktır ortaya. Yine de bu satırların yazarı olarak endişe duymadığımı söyleyemem. İnsanlık tarihimiz, teknolojinin kötü amaçlarla kullanımının bir dolu örneğine sahip maalesef. Bir yandan bütün kötü ihtimallere rağmen teknolojiler geliştirmenin kaçınılmaz bir olgu olarak ele alınması gerçeği var.

# En Gelişmiş Robo-Köpek

**1 metre boyunda, 109 kg ağırlığında bir robo-köpekle tanışın. Metanol motoruyla çalışan ve 45 kilo yük taşıyabilen 4 ayaklı arazi robotu: BigDog. Büyük Köpek (BigDog) bacaklarındaki şok emici unsurları, her adımda enerjiyi geri dönüştüren teknolojisiyle ve tıpkı bir hayvan gibi eklemlendirilmiş bacaklarıyla çok farklı arazi tiplerinde ilerleyebilen bir robot.**

Büyük Köpek, üzerindeki bilgisayarla hareket kabiliyetini, etrafını algılama işlemlerini ve kullanıcıyla olan iletişimini kontrol ediyor. Bilgisayarıyla dengesini sağlama, hareketlerini geniş yelpazedeki arazi tiplerinde yönetebilme ve yön bulma duyusunu kontrol etmegibi işlemler yapabiliyor.

Eklem pozisyonları, eklemlerdeki güç, yerle temas algısı, jiroskop, LIDAR ve üç boyutlu görüş gibi teknik özellikleri içeren hareket algılama sisteminin dışında; kendi iç durumunu, hidrolik basıncını, yağ sıcaklığını, motor işlevlerini, pil şarjını kontrol eden algı sistemlerine sahip olan Büyük Köpek, 10 km/sa hızla koşup 35 derecelik eğimli arazileri tırmanabiliyor.

Molozların üzerinden yürüyüp çamurlu dağ yollarında yol alabiliyor, karda ve suda ilerlerken 150 kg yük taşıyabiliyor.
Orijinal Büyük Köpek tasarımının gelişmesinde DARPA maddi kaynak sağlamıştır. Manipülatör ve dinamik manipulasyon özelliklerinin eklenmesi için ise Ordu Araştırma Laboratuvarı'nın (Army Research Laboratory) programı kapsamında desteklenmiştir.

**QR KOD ETKİLEŞİMLİ** Büyük Köpek ve marifetleri için… Hatta küçük bir buz dansı bile var:

# YİAFL TECHMATH

HAZIRLAYANLAR

SAMET ZENGİN VE YUSUF EKMEKÇİ

WWW.E-DERGİ.YİAFL.COM

E-DERGİ