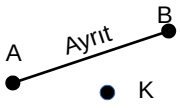
ÇİZGELER (GRAFLAR)

Çizge kuramı, nesneler arasındaki ilişkileri düğümler (noktalar) ve bu düğümleri birbirine bağlayan ayrıtlar (kenar-çizgi) kullanarak inceler. Çizgelerle yapılan problemlerde kullanılan işlemlere çizge algoritmaları denir.

Çizge kavramı, İsviçreli matematikçi *Leonhard Euler* tarafından 1736 yılında Königsberg'in yedi köprüsü problemi üzerine yaptığı çalışmalarla ortaya çıkmıştır. Bu problem, modern graf teorisinin temelini oluşturmuştur.

Yandaki şekilde A ve B komşu düğümleri (aralarındaki yola (ya da kenara) ayrıt denir) ve ayrık K düğümü görülmektedir

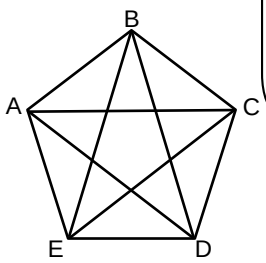


Bir çizgedeki **tüm noktaların sayısına** o çizgenin derecesi, **bir noktadan çıkan kenar sayısına** o noktanın derecesi denir.
Çizge teorisi ulaşım , ekonomi, elektrik devreleri, ağ tasarımı, veri yönetimi ve algoritma analizi gibi pek çok alanda kullanılabilmektedir.

www.matbaz.com

Örnek...1 :

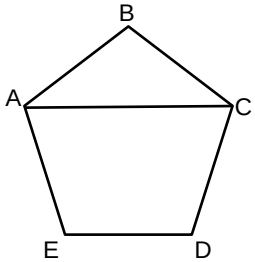
El Sıkışma Problemi:
5 kişilik bir toplantıda herkes birbiriyle el sıkıştığında toplam el sıkışma sayısı, cebirsel bir işlem yapmadan çizge kuramıyla bulunabilir. Kişileri beşgenin köşe noktaları ile, her el sıkışma çizgi ile gösterilsin. Noktaları birbirine bağlayan kenar sayısı 10 olduğundan toplam el sıkışma sayısı 10'dur.



Örnek...2 :

Yandaki şekli
a) el kaldırmadan ve her kenarın üzerinden tam olarak bir kez geçerek

b) el kaldırmadan , başladığınız noktada bitirmek ve her kenarın üzerinden tam olarak bir kez geçmek koşuluyla çizebilir misiniz? (Geçilen bir noktadan tekrar geçilebilir, kenardan geçilemez)



EULER YOLU VE EULER DEVRESİ

Euler yolu bir çizge üzerinde her kenarı tam olarak bir kez geçen bir yol olarak tanımlanır. Bu yol, aynı düğümden başlayıp aynı düğümde bitiyorsa **Euler devresi (döngüsü)** ; farklı düğümlerde başlayıp bitiyorsa **Euler yolu** adını alır.

Euler Devresi Koşulları
Çizgede Euler Devresi olması için:
- Çizge ***bağlantılı*** olmalıdır (tüm düğümler birbirine bağlı olmalı).
- Her düğümün derecesi (düğüme bağlı kenar sayısı) çift olmalıdır.
- Bu durumda, yol başladığı düğümde biter.

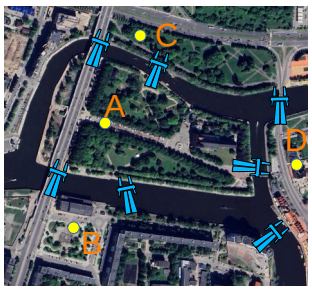
Örneğin bir çizge üzerinde A-B-C-D-A şeklinde bir döngü , her kenarı bir kez kullanıyorsa ve tüm düğümlerinin derecesi çift ise , bu bir Euler devresidir.

Euler Yolu Koşulları
Çizgede Euler Yolu olması için:
- Çizge ***bağlantılı*** olmalıdır.
- Tam olarak iki düğümün derecesi tek olmalıdır (diğer tüm düğümlerin derecesi çift olmalı).
- Bu durumda, yol tek dereceli düğümlerden birinde başlar, diğerinde biter.

Örneğin bir çizge üzerinde A-B-C-D şeklinde bir yol , her kenarı bir kez kullanıyorsa ve sadece A ve D düğümlerinin derecesi tek ise , bu bir Euler yoludur.

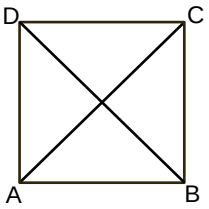
Örnek...3 :

7 Köprü Problemi:
"Pregel nehri, Königsberg kasabasını 4 parçaya ayırır ve bu parçaları bağlayan 7 köprü vardır. Yola istediğiniz yerden başlayıp, istediğiniz yerde bitirerek ve her köprüden tam olarak bir kez geçerek şehri dolaşmak mümkün mü?
Euler, bu gezintinin <u>mümkün olmadığını</u> ispatlamıştır. Sebebini açıklayınız.



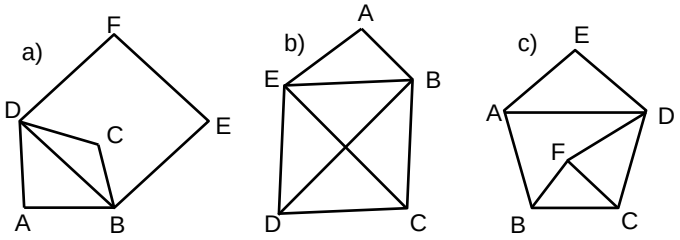
Örnek...4 :

Yandaki çizgenin Euler yolu veya Euler devresi içerip içermediğini belirleyiniz.



Örnek...5 :

Aşağıdaki şekillerden hangileri elinizi kaldırmadan ve çizilen yerden tekrar geçmeden çizilebilir?

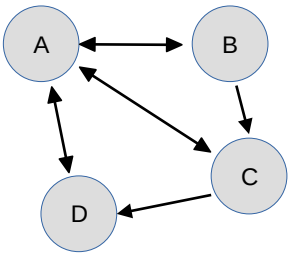


YÖNLÜ ÇİZGE (GRAF)

Çizgedeki ayrıtların yönleri temsil eden oklarla gösterildiği çizgedir.
Çizge içerisindeki birbirine bağlı iki düğüm noktası arasında, sadece ilgili okun işaret ettiği yönde ilerlenebilmesi mümkündür.

Örnek...6 :

Bir işyerinde çeşitli bilgisayarlar arasında veri transferinin hangi bilgisayarlar arasında olabileceği şekilde verilmiştir. Buna göre ağdaki en etkin bilgisayar A olmaktadır.



AĞIRLIKLI (MALİYETLİ) ÇİZGELER

Bir çizgenin üzerindeki ayrıtların değerleri eşit değilse ve her biri bir değer alabiliyorsa bu tip çizgelere maliyetli ya da ağırlıklı çizgeler denir.(örneğin farklı noktalar arasındaki mesafelerin kenarlara değer olarak atandığı çizgeler ya da sosyal medya platformlarındaki takipleşmeleri temsil eden çizgeler)

www.matbaz.com

EN AZ MALİYETLİ YOL ALGORİTMALARI

Bir çizgenin iki düğümü arasındaki en az maliyetli yolun belirlenmesi bu iki düğüm arasındaki en kısa yolun bulunması problemi olarak karşımıza çıkabilir. En az maliyetli yol algoritmaları; kargo şirketlerinin teslimatlarını yapması, bir şehrin altyapı ihtiyaçlarına ait binalara en az maliyetle ulaşması problemi gibi durumlarda karşımıza çıkabilir.

Örnek...7 :

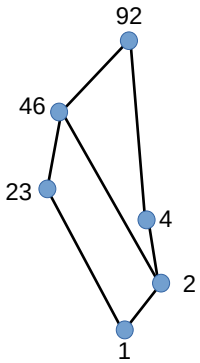
Bir kargo şirketi; bir köyde bulunan A, B, C ve D adlı dört çiftlik arasında bir yolculuk gerçekleştirecektir. Kargoya ait araç; başlangıç noktası olan A çiftliğinden hareket ederek B, C ve D çiftliklerini tek bir kez ziyaret ettikten sonra yine A çiftliğine dönecektir.

Çiftlikler	A-B	B-C	C-A	C-D	D-A	B-D
Mesafe	23	35	41	45	15	65

Tabloda her iki çiftlik arasındaki mesafeler (km cinsinden) verilmiştir. Haftada bir gün çalışan ve bütün çiftliklere uğrayan bu kargo arabasının yakıt tüketimini daha temiz bir çevreye sahip olmak amacıyla azaltmak gerekmektedir. Bu nedenle kargo arabasının sorumluluk sahasındaki çiftlikleri en kısa yoldan dolaşabilmesi için bu mesafelerin toplamının en az olması istenmektedir. Tablodaki verileri kullanarak toplam mesafeyi en aza indirirsek toplam kaç km yol gidilir?

Örnek...8 :

Hasse diyagramı, kısmen sıralı bir kümenin elemanlarının ilişkisinin grafiksel bir temsilidir. Kümenin her elemanı için bir nokta çizilir.
Yanda 92 sayısının pozitif tam sayı bölenleri için Hasse diyagramı oluşturulmuştur. 92 sayısının asal çarpanları 2 ve 23 düğümler olarak yer almaktadır. Yukarıya doğru çıkıldıkça bu çarpanların çeşitli kombinasyonları daha büyük çarpanları oluşturmaktadır . İnceleyiniz.



(çeşitli sayılar için Hasse diyagramları için
https://demonstrations.wolfram.com/HasseDiagramsOfInteg

erDivisors)

ŞİFRELEME ALGORİTMALARI (KRİPTOLOJİ)

Kriptoloji (şifre bilimi) kısaca bilgileri koruma ve gizleme bilimi olarak tanımlanabilir. Başkalarınca anlaşılması istenmeyen bilgiler (askeri istihbarat, kredi kartı bilgileri v.b.)şifrelenerek korunmuştur.
Harf, sembol ve rakamlar kullanılarak mevcut verinin şifrelenmesi ve teslim alanın gönderilen şifreyi çözümleyebilmesi genellikle belirli matematiksel işlemlere (algoritmalara) göre yapılır. (Kriptoloji sayılar teorisiyle sıklıkla ilişkilendirilebilir)

Günümüzde kullanılan modern şifreleme algoritmaları üç ana kategoriye ayrılır: (Simetrik, Asimetrik ve Karma şifreleme algoritmaları)

Simetrik şifreleme : Aynı gizli anahtar hem şifreleme hem de şifre çözme işlemi için kullanılır. Hızlı bir yöntemdir fakat anahtarın güvenli bir şekilde paylaşılması saklanması önemlidir. AES, DES, 3DES, Blowfish popüler simetrik şifreleme algoritmalarına örnektir.

Asimetrik Şifreleme: Şifreleme ve şifre çözme işlemleri için birbirinden farklı iki anahtarın kullanıldığı bir şifreleme yöntemidir. Bu anahtarlardan biri açık anahtar (public key) diğeri ise gizli anahtar (private key) olarak adlandırılır. Açık anahtar herkesçe bilinirken gizli anahtar sadece sahibi tarafından bilinir. Simetrik şifrelemeye göre kıyasla güvenli ama yavaş olan bu yöntem karmaşık matematiksel işlemler gerektirmektedir. RSA, ECC, Diffie-Hellman, DSA popüler asimetrik şifreleme algoritmalarına örnektir.

Karma şifreleme algoritmaları: Verileri sabit uzunlukta bir çıktıya (hash) dönüştüren matematiksel fonksiyonlardır. En önemli özellikleri geri döndürülemez olmaları ve farklı verilerin aynı çıktıya sahip olma ihtimalinin çok az olmasıdır. MD5, SHA-1/2/3, BLAKE2 ,RIPEMD-160 popüler karma şifreleme algoritmalarına örnektir.

www.matbaz.com

RSA ŞİFRELEME ALGORİTMASI

Sayıların çarpanlara ayrılması, kriptoloji alanında önemli bir yere sahiptir. RSA şifreleme algoritması (adını buluşçuları olan (Rivest- Shamir- Adleman) şifreleme algoritması; büyük asal sayıların çarpımına dayanır. Bu algoritma yeterince büyük bir sayının asal çarpanlarına ayrılmasının zorluğuna dayanır, mesajın şifresini çözmek için gerekli özel anahtar, bu büyük asal sayıları çarpanlarına ayırma işlemine bağlıdır.

Asal sayıların çarpanlara ayrılması için geliştirilen başlıca algoritmalar; deneme bölme algoritması, Pollard'ın rho algoritması ve Shor algoritması şeklinde sıralanabilir. (wiki link)

DOĞRUSAL ŞİFRELEME

Harflerin sayısal karşılıkları kullanılarak şifreleme yapmak mümkündür.
a ve b birer doğal sayı ($a \neq 0$) ve x şifrelenecek metindeki harflerin sayısal karşılığı olmak üzere, ax+b örüntüsüne sahip şifrelemelere doğrusal şifreleme denir.

Türk alfabesindeki Harflerin Sayısal Karşılıkları

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K
1	2	3	4	5	6	7	8	9	10	11	12	13	14

L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

SEZAR ŞİFRELEMESİ

Sezar şifrelemesinde (Julius Sezar tarafından kullanıldığı bilinmektedir) şifrelenecek kelime içindeki her bir harf, alfabedeki sırasının önceden anahtar olarak belirlenen miktar kadar kaydırılmasıyla dönüştürülerek şifrelenmiş metin elde edilir.(Kaydırma işleminde toplam harf sayısı aşılırsa başa tekrar dönülür.) Güvenli olmayan bu yöntem şifreleme kavramlarını anlamak için başlangıç noktası olarak görülebilir

Örnek...9 :

YÖN kelimesini **Sezar şifreleme** metoduyla (anahtar 5) şifreleyiniz. (Kelime içindeki her bir harfin alfabedeki sırasını bulup anahtar kadar kaydırıp, liste biterse başa dönerek.)

Örnek...10 :

Türkçe harfler alfabetik sıralamaya göre aşağıdaki gibi 1'den 29'a kadar numaralandırılmıştır.
Bu sayısal değerlerin "3 katının 1 fazlası ile elde edilen sayının 29'a bölümünden kalan sayı" değerlerine göre bu metnin şifrelenmiş olduğunu varsayalım. Buna göre, "YAZ" metnini şifreleyiniz.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K
1	2	3	4	5	6	7	8	9	10	11	12	13	14

L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Örnek...11 :

Şifrelenmiş bir metni deşifre etmeye çalışan kriptoanalistler (şifre çözücüler) şifrelenmiş metindeki yaptıkları çalışmalar soncunda yazışmalarda " EDI" olarak geçen kelimenin karşılığının "MAÇ" olduğunu tespit etmişlerdir.
Buna göre şifrelemede kullanılan örüntüyü cebirsel olarak genelleyiniz.

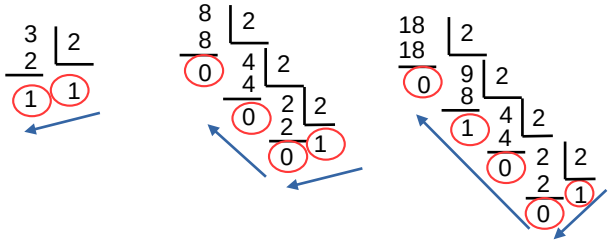
İKİLİ SİSTEM (BİNARY) ŞİFRELEMESİ

İkili sayma sistemi (Binary) Sadece 0 ve 1 sayılarından oluşan bir sayı sistemidir. Binary (İkili) sayı sisteminin tabanı 2'dir. Kullandığımız sayıları ikili tabana çevirirken sayıyı kalanlı olarak sürekli olarak 2 ye böler son bölüm ve geriye doğru kalanları alırız. (Taban 10 ise yazılmaz)

Örnek...12 :

Örneğin 3,8 ve 18 sayılarının 2 tabanında karşılıkları bulunmuştur. İnceleyiniz.

$3=(3)_{10}=(11)_2$ $8=(8)_{10}=(1000)_2$ $18=(18)_{10}=(10010)_2$



ASCII KARAKTER KÜMESİ

"Amerikan Bilgi Değişimi İçin Standart Kod" ifadesinin İngilizce karşılığının baş harflerinden elde edilen ASCII karakter kümesinden seçilen harfler, sayılar ve sembollerden oluşur. Aşağıda bir kısmı verilen ASCII karakter kümesindeki her bir karakter, belirli bir sayısal değerle temsil edilir.

Bazı ASCI kodları aşağıdaki tabloda verilmiştir.

Karakter	ASCII	Karakter	ASCII	Karakter	ASCII
@	64	.	96	[	91
A	65	a	97	\	92
B	66	b	98	]	93
C	67	c	99	^	94
...	...	...	...	...	...

Bilgisayarlarda tüm veriler (harfler, sayılar, resimler gibi) 0'lar ve 1'ler olarak saklanır ve işlenir. Örneğin A harfinin ASCII karşılığı 65'tir. Onluk sistemdeki
65 sayısını bilgisayar, 1000001 olarak saklar ve işler.

Örnek...13 :

HEY kelimesinin bilgisayar sisteminde saklanması için uygulanan adımlar verilmiştir. İnceleyiniz

1. adım: Her karakter kendisine karşılık gelen ASCII karakterine dönüştürülür.

H	E	Y
72	69	89

Bu durumda HEY kelimesinin ASCII karşılığı
72 69 89
olur.

2. adım: 72 69 89 değerlerinin bilgisayar sistemindeki karşılıkları bulunur.

72	69	89
1001000	1000101	1011001

HEY kelimesinin bilgisayar sistemindeki karşılığı 1001000 1000101 1011001 şeklindedir.

Örnek...14 :

"KLAS" kelimesinin bilgisayar sisteminde saklanması için uygulanan adımları yazınız.