



## Sınav Kağıdı

KARADENİZ  
TEKNİK ÜNİVERSİTESİ  
Of Teknoloji Fakültesi

Öğrenci No		Bölüm	Yazılım Mühendisliği Bölümü		
Adı Soyadı		Yıl/Yarıyıl	2025-2026	<input type="checkbox"/> Güz	<input checked="" type="checkbox"/> Bahar
İmza		Tarih/Saat/Süre	10/04/2026	13.00	90 dakika
Dersin Kodu / Adı	YZM2008 Ayrık Matematik	Sınav Türü	<input checked="" type="checkbox"/> Arasınav	<input type="checkbox"/> Final	<input type="checkbox"/> Bütünleme
Dersin Sorumlusu	Öğr.Gör. Ömer ÇAKIR		<input type="checkbox"/> Mazeret	<input type="checkbox"/> Diğer:	

Alınan Puan											Toplam Puan
Soru No/Puanı	1/10	2/10	3/10	4/10	5/10	6/10	7/10	8/10	9/10	10/10	
P1.1. (%)	50	50	50	50	50	50	50	50	50	50	
P2.1. (%)	50	50	50	50	50	50	50	50	50	50	
P <sub>Toplam</sub>	100	100	100	100	100	100	100	100	100	100	

### Sınava İlişkin Açıklamalar

- Sınavın ilk 30 dakikasında salondan çıkmak yasaktır.
- İlk 15 dakikadan sonra gelenler sınav salonuna alınmayacaktır.

## SORULAR

4	4	4	4		3	3	2	2	1
5	3	3	3		2	2	3	1	2
3	5	2	2		4	1	1	3	3
2	2	5	1		1	4	4	4	4
1	1	1	5		5	5	5	5	5

4) Aşağıdaki sayılardan hangisi **Carmichael** sayısı değildir?

- (A) 561 (B) 1105 (C) 1729 (D) 2431

**İpucu**

[ 561 = 3\*11\*17, 1105 = 5\*13\*17,  
1729 = 7\*13\*19, 2431 = 11\*13\*17 ]

1) Bubble Sort sıralama algoritmasına göre 5,4,3,2,1 örnek verisinin sıralama adımlarına dair yukarıda boş bırakılan sütun ne olmalıdır?

2) -11 mod 3 işleminin sonucu nedir?

- (A) -2 (B) 2 (C) -1 (D) 1

5) 12345 decimal sayısının octal eşdeğeri nedir?

- (A) 3039  
(B) 30071  
(C) 3000321  
(D) 11000000111001

3) Aşağıdaki sayılardan hangisi **Mersenne** asal sayısı değildir?

- (A) 3 (B) 7 (C) 17 (D) 31

6) 007288008 ISBN-10 check digit deęeri nedir?

7) 074930149X geęerli bir ISBN-10 sayısı mıdır?

8)  $s*110 + t*273 = 1$  eřitlięindeki  $s$  ve  $t$  tam sayıları nedir? [ İpucu  $\gcd(110, 273)=1$  ]

### RSA Şifreleme Adımları

1.  $p$  ve  $q$  asal sayıları belirlenir
2.  $n = p*q$  hesaplanır
3.  $(p-1)(q-1)$  hesaplanır
4.  $1 < e < (p-1)(q-1)$  kořuluna uygun  $e$  seçilir
5.  $d*e = 1 \pmod{(p-1)(q-1)}$  için  $d$  hesaplanır
6.  $M^e = C \pmod n$  ( $M$ :şifrelencek mesaj,  $C$ :şifrelenmiş mesaj)

9) RSA Şifrelemede Ali şifreli mesajı gönderen, Ayşe de şifreli mesajı çözen kiři olsun. Şifreleme öncesi Ayşe Ali'ye hangi bilgileri gönderir?

- (A)  $(p,q)$     (B)  $(d,e)$     (C)  $(n,e)$     (D)  $(n,d)$

10)  $a=144$  ve  $m=233$  olduęunda  $a$ 'nın mod  $m$ 'e göre inverse deęeri nedir? [ İpucu  $\gcd(144, 233)=1$  ]