COL 202: DIS CRETE MATHEMATICAL STRUCTURES LECTURE 13 NUMBER THEORY I: EULER'S THEOREM ROHIT VAISH JAN 30, 2024

14 1	NEAR CO	MBINATION V/S COMMON DIVISOR
Greatest	Common	divisor
gcd(	(n,m) =	largert number a such that d/n and d/m.
Smallest	positive	integer linear combination
spc (n	m) = Sm	allest positive integer d such that d=s.n+t.m
· · · · · · · · · · · · · ·	· · · · · · · ·	s,t integers
· · · · · · · · · · · · · ·	Theorem	qcd(n,m) = spc(n,m)
· · · · · · · · · · · · ·	· · · · · · · · ·	

FAUCET/TAP aL 6L Theorem Given water jugs of capacity aL and bL, it is possible to have cL	APPLICAT	TION I : W	iater fill	LING	
FAUCET/TAP aL bL Theorem Given water jugs of capacity aL and bL, it is possible to have CL			1		
FANCET/TAP aL bL Theorem Given water jugs of capacity aL and bL, it is possible to have cL					
FAUCET/TAP aL bL Theorem Given water jugs of capacity aL and bL, it is possible to have cL					
FAUCET/TAP aL bL Theorem Given water jugs of capacity aL and bL, it is possible to have cL			· · · · · · · · · ·		
FAUCET/TAP aL 6L Theorem Given water jugs of capacity aL and bL, it is possible to have cL		· · · · · · · · · · · ·	· · · · · · · · · ·		
FAUCET/TAP aL 6L Theorem Given water jugs of capacity aL and bL, it is possible to have cL	· · · • · · · · · · · · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · ·		
Theorem Given water jugs of capacity at and bt, it is possible to have ct	AUCET/TOP	<b>a I .</b>	L ]		
Given water jugs of capacity a L and bL, it is possible to have CL				· · · · · · · · · ·	· · · · · · · · · · ·
	water jugs of	Cabacity aL o	und bL. it is	bossible -	to have CL
in a jug if and only if c is a multiple of gcd (a,b) st. 0 < c < b	jng if and on	ly if C is a	multiple of	ged (a,b) s	$t = 0 \le c \le b$
	0 0	<b>U '</b>			· · · · · · · · · ·

	APPLIC	ATION 1	E: Prim	E FAC	TO RIZATIO	N	
Every	intge	L N 7 1	has a	uniqu	e factori:	Cation	· ·
into p	nimes	P1, P2, -	· Pĸ (	þossi bly	nepeoting)	such that	· · ·
	γ	$n = p_1$ .	P2	·Pĸ	and		
.		$P_1 Z P_2$	2	ZPK	• • • • • • • • • •		· · ·
aka	Fund	amental	Theorem	of 1	Inthretic		· · ·

•	•	· · ·	•	•	•	· · ·	•	•	•	•	•	•	· · ·	•	•		0	Ŋ	Ę	r A		E	1	1	C	E	•	· · · · · · · · · · · · · · · · · · ·	•	•	· · ·		•	•		· · ·	•		•	•	· · ·	•	•
		• •				• •													•												• •									•	• •		
																																								•			
						• •													•									• •												•			
		• •										•	. 1	•				1								<u>.</u> .						1.	1.		. 1	1	1			•	• •		
		• •				N.		-	-		h	2	·	1	h	÷.,	n	÷			1	 <u> </u>		•	) <b>1</b> 1	10	ì	-		Y				- 1	7	D	].			•			
		• •				, v		-						_		•		. /			1	<u>y</u>		-		K	1			×.		<b>,</b> .'		1	•		1			•			
		• •																								V									•					•			
	•	• •				• •							• •					•	•					•	• •			• •			• •				•					•	• •	•	•
	•	• •			•				•	•	•	•	• •					•	•				•		• •		•	• •		•	•				•		•			•	• •		•
		• •			•						•								•						• •			• •							•	• •	•			•		•	•
	•	• •			•				•	•	•	•	• •					•	•				•		• •		•	• •		•	•				•		•			•	• •		
	•	• •				• •							• •					•	•					•	• •			• •			• •				•					•	• •	•	•
	•	• •				• •							• •					•	•					•	• •			• •			• •				•					•	• •	•	•
	•	• •				• •							• •					•	•					•	• •			• •			• •				•					•	• •	•	•
	•	• •				• •							• •					•	•					•	• •			• •			• •				•					•	• •	•	•
	•	• •				• •							• •					•	•					•	• •			• •			• •				•					•	• •	•	•
	•	• •				• •							• •					•	•					•	• •			• •			• •				•					•	• •	•	•
	•	• •				• •							• •					•	•					•	• •			• •			• •				•					•	• •	•	•
		• •			•						•								•						• •			• •							•	• •	•			•		•	•
		• •			•						•								•						• •			• •							•	• •	•			•		•	
		• •			•						•								•						• •			• •							•	• •	•			•		•	
		• •			•						•		• •						•						• •			• •							•	• •	•			•		•	•
		• •			•						•		• •						•						• •			• •							•	• •	•			•		•	•
•		• •			•	• •					•	•	• •					•	•						• •			• •			•				•		•			•			•
•		• •			•	• •					•	•	• •					•	•						• •			• •			•				•		•			•			
•		•			•	• •			•	•	•	•	•					•	•					•	•			• •			•				•	•	•			•			
•	•	•			•	• •		•	•	•	•	•	• •		•		•	•	•				•	•	• •	•	•	• •		•	•							•	•	•	• •		•
		• •																										• •															

CONGRUENCE
$a \equiv b \pmod{n}$ if and only if $n (a-b)$
hesembles equality
+ If $A \equiv b \pmod{n}$ and $C \equiv d \pmod{n}$ , then $A + c \equiv b + d \pmod{n}$ .
• If, then $a \cdot c \equiv b \cdot d \pmod{n}$ .
· · · · · · · · · · · · · · · · · · ·

· ·	•	• •	•	• •	•	•	· ·	•	•	<b>C</b>	01	J	η R	L	E	N	С С	E	•	•		<u>נ</u>	•	E	0		A	4	Τ.	Ϋ́	•		•	•	• •	• •	•	•		•	•	•
• •	•	M	<b>L</b> h	 	8	li.	f			i n(	L		•	•			ln		e l		n t	iØ	<b>N</b>	• •	•		• •	•	• •	•	•			•	• •	· ·	•	•		•	•	•
• •		••••	•	••••		•	• <b>y</b> •	•	•	•		•	•	•			•	•	•				•	• •	•	•	• •	•	• •	•	•	•	•	•	• •	• •	•	•		•	•	•
• •	•	••••	•	• •	•	•	• •	•	•	•	•	•	•	•	•	• •	•	•	•	•	••••	•	•	• •	•	•	• •	•	• •	•	•		•	•	• •	• •	•	•		•	•	•
· ·	•	••••	•	· ·	•	•	· ·	•	•	•	• •	•	•	•	•	• •	•	•	•	• •	· ·	•	•	· ·	•	•	· ·	•	· ·	•	•		•	•	• •	· ·	•	•	, , , ,	•	•	•
• •	•	••••	•	· ·	•	•	· ·	•	•	•	• •	•	•	•	•	• •	•	•	•	• •	• •	•	•	· ·	•	•	• •	•	• •	•	•	•	•	•	• •	• •	•	•	· ·	•	•	•
• •	•	••••	0	• •	•	•	• •	•	•	•	• •	•	•	•	•		•	•	•	• •	• •	•	•	• •	•	0	• •	•	• •	•	0		•	•	• •	• •	•	0			•	•
· ·	•	••••	•	· ·	•	•	· ·	•	•	•	• •	•	•	•	•	•••	•	•	•	• •	•••	•	•	· ·	•	•	· ·	•	• •	•	•		•	•	• •	· ·	•	•		•	•	•
· ·	•	••••	•	· ·	•	•	· ·	•	•	•	••••	•	•	•	•	•••	•	•	•	• •	· ·	•	•	· ·	•	•	• •	•	• •	•	•		•	•	• •	· ·	•	•		•	•	•
• •	•	• •	•	• •	•	•	• •	•	•	•	• •	•	•	•	•		•	•	•	•		•	•	• •	•	0	• •	•	• •	•	•		•	•	• •	• •	•				•	•
• •	•	• •	•	• •	•	•	• •	•	•	•	• •	•	•	•	•		•	•	•	•	• •	•	•	• •	•	•	• •	•	• •	•	•		•	•	• •	• •	•	•		•	•	•

•	• •	•	•	•	••••	•	•	•	· ·	•	0	0	N (	η <b>β</b>		E	N	<b>C</b>	E	•		1/2	• • •	• •	E	Ð	V		- <b> </b>	τ	Y Y	• •	 •	•	• •	· ·	•	•	· ·	•	•	•
•	• •	N	1			ľ	di	f	f٩	Ś		Ľ	· · ·	· · ·	•	(	<b>C</b> 0	r L		e e e	10			<b>^</b>		•	· ·	•	•	· ·	•	• •	•	•	· ·		•	•	· ·	•	•	•
•	· ·		•	•	· · ·	•	•	•	· ·	•	•	•	· · ·	•	   (	).		· · ·	6	•	(	n v	\ 0 <i>0</i>		(0	) 1 1	· · ·	•	•	· ·	•	· ·	•	•	• •		•	•	· · ·	•	•	
•	· · ·		•	•		•	•	•	· · ·	•	•	•	· · ·	б С	1.7 7	¥ }			3	7	(m	(n	\ <i>VC</i>	ار 10	) (	)				· · ·	•	· · ·	•	•			•	•	· · ·	•	•	•
•			•	•	• •	•	•	•	· · ·	•	•	•	· · ·	•	•	•	· · ·	•	•	•			•	• •		•				· · ·	•	• •		•	•	· · ·	•	•	· · ·	•	•	•
•	· · ·		•	•	•	•	•	•	· · ·	•	•	•	· · ·	•	•	•	· · ·	•	•	•	· · ·	•	•	•		•	· · ·	•	•	· · ·	•	• •	•	•			•	•	· · ·	•	•	•

·       ·		
$qcd(k,n) = 1 \implies$	$k$ has an inverse $\Rightarrow$ $k$ is can	cellable
k and n have no	(mod n) (mod n) $f(mod n) = f(mod n)$	ndn)
Common facture > 1	$\Rightarrow$	a≡b(moln)

·       ·		
	K has an inverse $\iff$ (mod n)	K is Concellable (mod n)
k and n have no Common facture 71	∃k'st. k.k =1(mod n) +0.	$b \ ak \equiv bk (mod n) \\ \Rightarrow a \equiv b (mod n)$
· · · · · · · · · · · · · · · · · · ·		

•	•	•	•	· ·	H	0 0	M	•	m	) A	N1	V	••••	ſ	N	N			J.	•	•	h	M	/{	0	N	•	•	) V	Ċ	<u>, s</u>	د	•	M	100	l	n		7	•	•	• •	
										Ī.	1	1																											•				
											. \	J																															
							• •																											• •								• •	
		•	•	• •		•	• •				•	•	• •	•				•					•				•	•			• •			• •			•	•	• •			• •	
•	•		•				• •				•	•	• •					•					•							•	• •			• •			•		• •			• •	
•		•	•	• •			• •	•	•		•	•	• •					•					•	• •			•	•			• •			• •			•	•	• •			• •	•
•			•			•				•	•	•	• •					•					•				•			•	• •			• •			•	•				• •	
		•	•	• •		•	• •		•		•	•	• •	•	•		•	•		•			•	• •			•	•		•	• •	•	•	• •			•	•	• •			• •	
•			•							•			• •			•		•						• •				•			• •	•		•			•	•	• •			• •	
	•	•	•	• •		•	• •		•		•	•	• •	•			•	•					•	• •			•	•		•	• •			• •			•	•	• •			• •	
•			•			•				•			• •											• •							• •	•		• •			•		• •			• •	
			•	• •		•	• •		•		•	•	• •	•			•	•					•	• •			•			•	• •		•	• •			•		• •			•	
•		•	•				• •	•			•	•	• •					•				•	•				•				• •		•	• •					• •				
	•					•	• •		•		•	•						•					•						 •	•	• •		•	• •			•		• •				
							• •											•									•											•				• •	
							• •						• •																		• •			• •									
							• •					•	• •										•				•				• •			• •					• •				
			•	• •			• •				•	•	• •					•					•				•	•			• •			• •			•		• •		•		
	•		•	• •			• •						• •					•						• •			•	•			• •			• •					• •	•		• •	

•	· · ·	•	· · ·	Ha	) 	· ·	n M		ď	· · ·		UY V	nl	50	لل	-	ha		2				<b>n</b> N		se			lod	Y	n	?	•	· ·	•	•
•	· · ·	· · · ·	· · ·	· · ·		· · · · · · · · · · · · · · · · · · ·	· · ·	· · · · · · · · · · · · · · · · · · ·	•	· · · · · · · · · · · · · · · · · · ·	•		E	<b>x (</b> 0				fu	· · · · · · · · · · · · · · · · · · ·	ti ti		· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·				· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·	•	· · · · · · · · · · · · · · · · · · ·	•	· · ·	•	•
•	• •	•	φ	6			•	No	•	ц П	е   	n†	ego	LV P	ļ,	~ {	0	, 1,	· · · · · · · · · · · · · · · · · · ·		n	13	t	hat	- 0			el	nt	ĩ۷ĩ	ly	• • • •	· · ·	• • • •	•
•	· ·	•	••••	•••	•	· ·	•	þr	í m	e		8	Ń	· ·	••••	•	••••	•	· ·	•••	•	•••	• •		• •		· ·	•	•••	•		•	· ·	•	•
		•			•	• •	•		•		•	• •	•			•	• •	•	• •		•							•		•		•	• •	•	•
•	• •	•	• •		•	• •	•	• •	•	• •	•	• •	•	• •	• •	•	• •	•	• •		•	• •	• •				• •	•	• •	•	• •	•	• •	•	•
	• •		• •	• •		• •		•		• •		• •		• •	• •		•		• •	• •	•	• •					•			•	• •		• •		
			• •			• •		• •		• •		• •		• •	• •		•		• •								• •				• •		•		
					•	• •	•	• •	•	• •	•	• •	0	• •		0	• •		• •							•			• •	0	• •	•	• •		
•	• •	•		· · ·	•	· ·	•	· ·	•	· ·	•	· ·	•	· ·	••••	•	••••	•	· ·	••••	•	••••			•		· · ·	•	· ·	•	· ·	•	· ·	•	•
•	· ·	•	· · ·	· · ·	•	· · ·	•	· ·	•	· ·	•	· · ·	•	· ·	· · ·	•	· · ·	•	· ·	• •	•	· ·	· · ·		•		· · ·	- - - -		•	· · ·	•	· ·	•	•

How	many	numbus	have	On	invase	mod	n ?	
· · · · · · · · · · · · · · · ·	· · · · · · ·	Euler's	fun	ctim			· · · · · ·	· · · · · · ·
¢G1:=	No m	integers in	{ 0, 1, -	., n-l	f that an	L Jela	tively	
· · · · · · · · · · · · · ·	prime	to n	· · · · · ·	· · · · · ·				· · · · · ·
gcd 1 {n} ::	= Set	of r			<u></u>		· · · · ·	

• • • •	•	•	•	· · · · · · · · · · · · · · · · · · ·	•	•	· ·	•	•	•	•	•	•	•	•	•	E		21	E	5 - -	<b>R</b> '	2		•	F	U	2		π				•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	· · ·	· · · · · · · · · · · · · · · · · · ·	•
•	•	•	•	· · ·	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	¢	) ) )	ĺ	2		· · ·			•	4	•	· · ·		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	· · ·	•	
•	•	•	•	· · · · · · · · · · · · · · · · · · ·	•	•	•	•	•	•			S		þ	, , , ,	nl	•	•	•	ф		þ	• • • • •	•	· · ·	· · ·	· · · · · · · · · · · · · · · · · · ·		د م ک ک		· · ·	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	· · ·	•	•
•	•	•	•	· · ·	•	•		n M			L.S.				•		Pf	•	•		- - - - - -			k		6			· · · · · · · · · · · · · · · · · · ·	1	•		Pf	•		n N N	•				n N M	b	U		•	•	•	•	· · ·	•	•
•	•	•	•	· · ·	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	· · ·	•	•	•		•	· ·		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	· ·	•	-
•	•	•	•	• •				0	0	0	0		0		•	0				•	•			•	•						•	• •	•		•		0			•		0	0		0		•		• •		

## EULER'S FUNCTION



Souce: Wikipedia auticle on "Enluis Totient Function" (Jan 29, 2023)

## EULER'S FUNCTION



Souce: Wikipedia auticle on "Enluis Totient Function" (Jan 29, 2023)

• •	· ·	•	•	•		•	· ·	•	•	•	•	· ·	•	E		L	E	ľ				Fi	JI		17	- []	0	N	•	•	· ·	•	•	•	· ·	· ·	•	•	•	•	· · ·	•	•	•
						۰L	· ^	~ `\				• •																															•	
•				•		()	· ( (	7)			-	• •				•							• •				• •											•		•	• •			•
		•	•	•		٠Ţ	· /·	••)			•	• •			•					• •	•		• •		•		• •	•		•				•		• •	•	•		•	• •		•	•
•		•	•	•		•		•			•	• •	•		•	•				• •	•	•	• •		•		• •	•	•	•	• •			•		• •	•	•		•	• •			•
			•				• •	Å			•	• •			•					• •			• •		•	•					• •			•	•	• •					• •			
									、.																																			
									$\mathbf{X}$																																			
											~		- 1		۱. ۱.	ľa ľ			$\hat{\mathbf{r}}$																									
														20	ľ'n		Υ.	.9	4		Or		þ٦	∩`a	me		· 1	٦v	lm	nb	ى	٦												
													. 1														• •																•	
				•			• •				•	• •			•	•				• •			• •		•		• •				• •			•		• •		•			• •			•
•		•		•						•	•	• •			•	•				• •			• •				• •				• •			•		• •		•		•	• •			•
•		•	•	•		•	• •					• •		•		•				• •			• •		•	•	• •			•	• •	•	•		• •	• •					• •	•		•
														•												•																		
•	•			•							•	• •				•				• •						•	• •				• •			•	•	• •		•			• •			
•		•	•	•		•	• •					• •				•				• •			• •		•		• •			•	• •			•		• •	•	•		•	• •		•	•
•			•	•			• •		1		•	• •			1	•				• •			• •		•	•	•		•	•	• •			•	• •	• •	•	•		•	•			•
				•		•	• •				•										•		• •		•		• •	•						•		• •					• •			
		•	•			•				•	•			•																									•	•				
• •	· ·	•	•	•	· ·	•	· ·	•	•	•	•	· ·	•	•	•			•	•	• •		•	• •		•	•			•	•	· ·		•	•		••••	•	•	•	•	• •	•	•	•

•	· · ·	•	•	· ·	•	•	· ·	•	•	• •		•	•	E	U	L	E	r F	2			Fi	) [	1 1 1	:T	י <b>הו</b>	0	N	•	•	· ·	•	•	•	•	· · ·	•	•	•	· · ·	•	•	•	•
		•	•		•	•		•	•			•	•	•		•	•	•			•	•		•	•	•			•	•		•	•	•			•	•	•		•	•	•	•
						۰L	· ^	مر ا							• •													• •																
	• •			• •		(	· ( (	11	•	 +	2		•	•	• •	•	•		•	• •			• •				• •	• •		•			•	•	•	• •		•		• •			•	•
	• •			• •	•	٠V	· /·	••)		•					• •		•	•		• •			• •	•			•	• •		•	• •		•	•		• •				• •			•	•
•																				• •																								
	• •	۰		• •									•	レ				Ċ.	۱.	: Li		ŀ.	• •		ć,		• •	· •		D		۰			•	• •		•		• •				•
•	• •			• •			• •			• •			•	1	• 1	7	• .	Л	10	C[]	N.C.	M	• •	Þ٩	In	N		T	-	1			•	•	•	• •				• •				•
					•	•																Ŋ		l j	•																			
																			ſ		)	·~~	م ا م:		:0	- '																		
																			Ţ	, n	na.	.01	1		П																			
	• •			• •						• •			•	•			•	۰.			Ń		. V.	•		•	· 1 ·	• •						•	•	• •		•		• •		•	•	•
•	• •			• •			• •		•	•			1	$\leq$	ΞÌς	י ה א	ſ	N	N	۶V	elj	1	·βγ	n'n	nl	• -	-10	) '	Ľ	•					•	• •				• •			•	•
•		•	•		•	•			•												. (	1	T		•	•			•			•	•				•		•				•	
•																				• •																								
	• •			• •			• •			•				•	• •					• •			• •				• •	• •		•				•		• •		•		• •			•	•
	• •		•	• •			• •		•	•		•	•	•	• •	•	•		•	• •	•	•	• •	•		•	• •	• •		•			•	•	•	• •				• •			•	•
•												•									•	•		•																				•
•				• •																• •			• •								• •				•	• •								
•	• •	•		• •			• •			•			•				•	•	•	• •			• •			•	•	• •		•	• •	•	•	•	•	• •				• •				
	• •			• •			• •								• •					• •											• •													

	EULER'S FUNCTION
$\phi^{(9)} =$	
.       .	k is relatively prime to 9 if and only if k is relatively prime to 3
3 divides every	$\frac{1}{3}$ number $\times 12 \times 45 \times 78$

	EULER'S FUNCTION
$\oint (9) =$	$9 - \frac{9}{3} = 6$
x       x	k is relatively prime to 9 if and only if k is delatively prime to 3
3 divides every	3 number X12X45X78

· ·	•	••••	•	· ·	••••	•	· ·	· · ·	· · ·	•	Eu	LE	TR	ב'	•	Fi		10	τI	0 r	<b>J</b>	• •	· ·	••••	•	· · ·	· •		•	••••	•	· · ·	•
• •		þ.	21	þ	rim	ne Ne	  	k ≯	: 1	•	· ·	· ·	· ·	· ·	•	· ·	· ·	• •	•	· ·	· ·	• •	· ·	· ·	•	• •		• •	•	· ·	•	• •	•
· · ·	•	· · ·	•	· · ·	· · ·	•	· · ·	· · ·	· · ·	•	¢	(þ	K)	· · · · · · · · · · · · · · · · · · ·		· · ·	k þ	· · · ·		k þ	· · ·	• •	· · ·	· · ·	•	· · ·		• •	•	· · ·	•	· · ·	
· ·	•	• •	•	· ·	• •	•	· ·	• •	· ·	•	· ·	· ·	· ·	· ·	•	· ·	· · ·	• •	•	þ	· ·	• •	· ·	• •		· ·		• •	•	• •	•	· ·	•
· ·	•	••••	•	· ·	••••	•	· · ·	· · ·	· · ·	•	· · ·	· ·	· · ·	· · ·			b b	-	Þ	К- ,	) 	• •	· ·	••••	•	· · ·	· •	· ·	•	••••	•	· · ·	•
• •	•	••••	•	· ·	••••	•	· ·	· · ·	· ·	•	· ·	· ·	· ·	· ·	•	· ·	· · ·	• •	•	· ·	· · ·	• •	· ·	••••	•	• •		• •	•	••••	•	· ·	•
• •	•	· ·	•	• •	· ·	•	· ·	· ·	· ·	•	· ·	· ·	· ·	• •	•	· ·	· ·	• •	•	· ·	· ·	• •		· ·	•	• •	•	• •	•	· ·	•	• •	•
• •	•	· ·	•	• •	· ·	•	• •	• •	• •	•	• •	• •	• •	• •	•	• •	• •		•		• •			· ·	•	• •		• •	•	· ·	•	••••	•

•	• •	•	•	· · ·	· ·	•	•	· · ·	•	• •		•	ŀ	Ē	۲ ۲	E	<b>Ľ</b> .	2	· · ·	Fi	JN	1 C	Τ	10	2	•	· · ·	•	· · ·	•	•	· ·	•	· ·	· ·	•	· ·	•	•
•	• •	k	2			•	•	· · ·	F	On	· ·	þ	, 9	, 1 1 1	ι       	์ ใ้กา	ne	S	· · ·	Su	rch	•	+1	ot	· · · · ·	þ	<i>≠</i>	r V	· · ·	•	•	· ·	•	· ·	· ·	•	· ·	•	•
•	• •	•	•	• •	· ·	•	•	· · ·	•	• •		•	· · ·	φ		þ.	q,				φ	(p	· · ·		b (a	7)		•	· · ·	•	•	· ·	•		· ·	•	· ·	•	•
•	· ·	•	•	• •	· ·	•	•	· ·	•			•	· ·	•	· ·	•	· ·	•	· ·	•	• •	•	· ·	•	· ·	•	· ·	•	· ·		•	· ·	•	· ·	· ·	•	• •	•	•
•	• •	•	•	• •	· ·	•	•	· ·	•	• •		•	· · ·	•	· ·	•	· ·	•	· · ·	•	••••	•	· ·	•	· · ·	•	· ·	•	· · ·	•	•	· ·	•	• •	· ·	•	· ·	•	•
•	• •	•	•	• •	· ·	•	•	· · ·	•			•	· · ·	•	· ·	•	· ·	•	· ·	•	• •	•	· · ·	•	· · ·	•	· · ·	•	· · ·	•	•	· ·	•		· ·	•	• •	•	
•	• •	•	•	• •	• •	•	•	· ·	•	• •		•	· ·	•	· ·	•	· ·	•	• •	•	• •	•	· ·	•	· ·	•	• •	•	· ·	•	•	• •	•	• •			• •	•	•
•	• •	•	•	• •	• •	•	•	• •	•	• •		•	• •	•	• •	•	• •	•	• •	•	• •	•	••••	•	• •	•	• •	•	••••	•	•	• •	•	• •	· ·	•	• •	•	•

έυ	LER'S FUNC	TION	· · · · · · · ·	
For p, q	primes such.	that $p \neq q$	  	
$\phi_{i}$	$(p.q) = \phi(p$	$) \cdot \phi(q_{\prime})$	· · · · · · · · ·	
Any number	not relatively	prime to po	y must	be
a mw	Utiple of p or	a muttiple	¥91.	
· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · ·
· · · · · · · · · · · · · ·		· · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · ·
· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · ·	
	For $p, q$ Any number a min	For $p, q$ primes such $\varphi(p, q) = \varphi(p$ Any number not relatively a multiple of $p$ or	For $p : q$ primes such that $p \neq q$ $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$ Any number not relatively prime to per a multiple of p or a multiple	For $p, q$ primes such that $p \neq q$ , $\phi(p, q) = \phi(p) \cdot \phi(q)$ . Any number not relatively prime to by must a multiple of p or a multiple of $q$ .

· · · · · · · · · · · · ·	EULER'S FUNCTION
Lemma :	For $p, q$ primes such that $p \neq q$
	$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$
Proof:	Any number not relatively prime to pay must be a multiple of b or a multiple of a
· · · · · · · · · · · · · ·	In the set $\{0, 1, 2, \dots, pqr-1\}$ , there are
· · · · · · · · · · · · ·	

· · · · · · · · · · · · ·	EULER'S FUNCTION
Lemma :	For $p, q$ primes such that $p \neq q$
· · · · · · · · · · · · · ·	$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$
Proof:	Any number not relatively prime to pay must be a multiple of b or a multiple of a.
	In the set $\{0, 1, 2, \dots, pqr-1\}$ , there are
*	q multiples of p,

· · · · · · · · · · · · · · · · · · ·	EULER'S FUNCTION
Lemma :	For $p, q$ primes such that $p \neq q$
	$\phi(\mathbf{p} \cdot \mathbf{q}) = \phi(\mathbf{p}) \cdot \phi(\mathbf{q})$
Proof:	Any number not relatively prime to by must be a multiple of p or a multiple of q.
***	In the set $\{0, 1, 2, \dots, pq-1\}$ , there are $q$ , multiples $rq p$ ,
· · · · · · · · · · · · · · · · · · ·	p muttiple of q

	EULER'S FUNCTION
Lemma :	For $p, q$ primes such that $p \neq q$
	$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$
Proof:	Any number not relatively prime to pay must be a multiple of b or a multiple of q.
· · · · · · · · · · · · · · · · · · ·	In the set $\{0, 1, 2, \dots, pqr - 1\}$ , there are $q$ , multiples $H \to 1$
× · · · · · · · · · · · · · · · · · · ·	p muttiple of q
$\begin{array}{c} \cdot \\ \cdot $	1 Common multiple of p and q

· · · · · · · · · · ·	· · ·	EULER'S FUNCTION	
Lemma	· · · ·	For $p, q$ primes such that $p \neq q$	
· · · · · · · · · · · · · · · · · · ·	· · · ·	$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$	
Proof	· · · ·	Any number not relatively prime to pay must be	•
· · · · · · · · ·		a minispre of p or a minispre of y.	•
· · · · · · · · ·		In the set 20, 1, 2,, pg-1], there are	
 	**	q, multiples of p,	
p and q are whatively brime	n n n n <del>∦</del> n n	p muttiples of q1	
· · · · · · · · · · · · · · · · · · ·	Ħ	1 Common multiple of p and q	

·       ·	EULER'S FUNCTION
kemma :	For $p, q$ primes such that $p \neq q$
·       ·	$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$
Proof:	Any number not relatively prime to pay must be
	In the set $\{0, 1, 2, \dots, pqr-1\}$ , there are
p and g are *	q multiples of p, p multiples of p, p+q-1 numbers are
sulatively prime ~	1 Common multiple of p and q ] evlatively prime to pq.

· · · ·		Euler's	FUNCTION	
· · · ·	Lemma :	For p, q primes	such that $p \neq q$	/
· · · ·		$\phi(p,q)$	$= \phi(p) \cdot \phi(q)$	
· · · ·	Proof:	$\phi(pq) = pq$	-(p+q-l)	
· · · ·				
· · · ·		· · · · · · · · · · · · · · · · · · ·		
· · · ·	· · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		

	EULER'S FUNCTION
Lemma :	For $p, q$ primes such that $p \neq q$
· · · · · · · · · · · · · ·	$\phi(p \cdot q) = \phi(p) \cdot \phi(q)$
Proof:	$\phi(pq) = pq - (p+q-1)$
· · · · · · · · · · · · · · ·	= (p-1)(q-1)
· · · · · · · · · · · · · · · · · · ·	

	EULER'S FUNCTION	· ·	· ·				•	• •
Lemma :	For p, q primes such that p = q	· · ·	· · · · · · · · · · · · · · · · · · ·	· · · ·				•
· · · · · · · · · · · · · · · · · · ·	$\phi(\mathbf{p} \cdot \mathbf{q}) = \phi(\mathbf{p}) \cdot \phi(\mathbf{q})$	· ·	· ·	· · · ·				•
Proof:	$\Phi(pq_1) = pq_1 - (p+q_1-1)$	• •	· ·	· · ·	• •			•
· · · · · · · · · · · · · ·	$= (p-1)(q_{1}-1)$	· ·	· ·	· · ·	· · ·	· ·	•	• •
· · · · · · · · · · · · · · ·	$= \phi(\varphi)  \phi(\varphi).$	· ·	· · ·	· · ·	· · ·			
		· ·	· ·	· · ·	•	Ley	•	•
<th><math display="block">= (p-1)(q_{1}-1)</math><math display="block">= \phi(p) \phi(q_{1}).</math></th> <th><ul> <li>.</li> <li>.&lt;</li></ul></th> <th><ul> <li>.</li> <li>.&lt;</li></ul></th> <th><ul> <li>.</li> <li>.</li></ul></th> <th></th> <th><u>Veu</u></th> <th></th> <th></th>	$= (p-1)(q_{1}-1)$ $= \phi(p) \phi(q_{1}).$	<ul> <li>.</li> <li>.&lt;</li></ul>	<ul> <li>.</li> <li>.&lt;</li></ul>	<ul> <li>.</li> <li>.</li></ul>		<u>Veu</u>		

· ·	•	•	•	•	•	· ·	•	•	•	• •	•	•	•	ŀ		2	E	۲ ۲	ן ר ר			Fi		1 C	π		ין כ י י	J :	•	•	• • • • • •	•	•	· ·	•	•	•	• • • • • •	•	· ·	•	•
· ·					- 	· ·	•	•		-0	r	•	0 0	k	· · ·	•	he	10	ti	Ve	لى بىل	f	þ	י רי ר	n m	ie	•	· ·	•	•		M	ul	hĩ	'þl	ر ر	`Q-	₽°~		y		•
· · ·	•	•	•	•	•	· ·	•	•	•	· · ·	•	•	•	· ·	φ		A	k		· ·		•	φ	(a	)     	· · ·	φ	( b	) ) )	•	· ·	•	•	· ·	•	•	•	· ·	•	· · ·	-	•
· ·	•	•	•	•	•	· ·	•	•	•	• •	•	•	•	· ·	•	•	• •	•	•	· ·	•	•	· ·	•	•	· ·	•	• •	•	•	••••	•	•	· ·	•	•	•	• •	•	• •	•	•
• •	•	•	•	•	•	•••	•	•	•	• •	•	•	•	· ·	•	•	• •	•	•	•••	•	•	• •	•	•	· ·	•		•	•	••••	•	•	· ·	•	•	•	• •	•		•	•
· ·	•	•	•	•	•	· ·	•	•	•	• •	•	•	•	· ·	•	•	· ·	•	•	· ·	•	•	· ·	•	•	· ·	•	••••	•	•	· ·	•	•	· ·	•	•	•	· ·	•	•••	•	•
· ·	•	•	•	•	•	· ·	•	•	•	•	•	•	•	· ·	•	•	• •	•	•	· ·	•	•	• •	•	•	• •	•	• •	•	•	· ·	•	•	• •	•	•	•	• •	•	• •	•	•
• •	•	•	•	•	•	••••	•	•	•	• •	•	•	•	· ·	•	•	• •	•	•	• •	•	•	•	•	•	· ·	•		•	•	• •	•	•	· ·	•	•	•	• •	•	•••	•	•

	EULER'S FUNCTION	
Lemma :	For a, b relatively prime	(Multiplicativity)
·       ·	$\phi(a.b) = \phi(a) \cdot \phi(b)$	
Proof:	Exercise	
·       ·		
.       .		

•	· · ·	•	•	•	• •	•	•	· · ·	•	• •	•	•		ミレ	)L	E	r'	2	•	F	U	N	C	τı	0	N	· · ·	•	• •	•	•	• •	•	•	• • • • • •	•	· ·	• • •	· ·
•	· · ·	k,	20	nn N			•	· · ·	F	On	•	n Q	, k		· · ·	re	10-	ŧ١	sc	ly J	•	þ	γŇ	ne	· · ·	•	· · ·	•		м М	ul	ti	þl	ĩC	27	า้งไ			· · · · · ·
•	· ·	•	•	•	· · ·	•	•	· · ·	•	· · ·	•	•	· · ·	φ		<b>X</b> -	Ь	)	-		Č	þ. (	(A)	•	φ		b)	•	· · ·		•	• • • •	•	•	· ·	•			· · ·
•	· · ·	E		7 .		•		Rei	â	U	•	¢	) (	12	· · ·		4		•	· · ·	•	g	cd	1	21	2}	· · · · · ·		۲ ۲ ک	, ;	, 27	7	-, 1	1	<u>}</u>	•	· ·	· ·	· · ·
•	• •	•	•		• •	•	•	• •	•	• •	•	•	· ·	•	· ·	•	•	• •	•	• •	•		· ·	•	• •	•	• •	•	• •	•	•	• •	•	•	• •	•	• •		• •
•	· · ·	•	•	•	· · ·	•	•	· · ·	•	· ·	•	•	· · ·	•	· · ·	•	•	· ·	•	· · ·	•	•	· · ·	•	· · ·	•	· · ·	•	• •	•	•	· ·	•	•	· ·	•	• •	• • •	· ·
•	• •	•	•	•	• •	•	•	• •	•	• •	•	•	• •	•	• •	•	•	• •	•	• •	•	•	• •	•	• •	•	• •	•	• •	•	•	• •	•	•	• •	•			· ·
•	• •	•	•	•	• •	•	•	• •	•	• •	•	•	• •	•	· ·	•	• •	• •	•	• •		•	• •	•	• •	•	• •	•	• •	•	•	• •	•	•	• •	•			• •

	Eul	er's fu	NCTION	
Lemma :	For a, b 1	relatively	prime	(Multiplicativity)
·       ·	φ (	a.b) =	$\phi(a) \cdot \phi(b)$	
<b>E</b> ·g., R	ecall $\phi(12)$ :	= 4	gcd 1 { 12} =	= {1, 5, 7, 11 }
H	eu's another h	Nay !	· · · · · · · · · · · · ·	
	$\oint(12) = \phi(3)$	$) \phi(2)$	= (3-1)	$\left(2^{2}-2^{-1}\right)$
			= 2 (4 = 4	-2)

•	•	· · ·	•	•	· · ·	· •	•	•	•	· · ·	· ·	•	•	•	E	J	L	E	r F I		2	· · ·	T	H	E	0	R	E	M		•	· · ·	•	•	· · ·	•	•	•	· ·	•	•	•	· ·	•
•		Th	20 20	h	e. En	· ·	•	•	F	0 >	L	•	k		•	h	J			iv		ly	•	-  -	ri			•	+	  D .	<b>N</b>		•	•	• •	•	•	•	• •	•	•	•	•••	•
•	•	· · ·	•	•	· · ·		-	•	•	· · ·	· · ·	•	•	•	•	k k	φ	(n (	)			<b>V</b>			•	· · ·	1	104					•	•	· · ·	· · ·	•	•	· ·	•	•	•	· · ·	•
•	•	· ·	•	•	• •		•	•	•	• •	••••	•	•	•	•	· ·	· ·	•	•	•	•	· ·	•	•	•	· ·	-	•	•	· ·		••••	•	•	• •	•	•	•	•••	•	•	•	• •	•
•	•	· ·	•	•	• •		•	•	•	• •	· ·	•	•	•	•	· ·	· ·	•	•	•	•	· ·	•	•	•	· ·	•	•	•	· ·	•	· ·	•	•	· ·	•	•	•	· ·	•	•	•	· ·	•
•	•	· ·	•	•	• •		•	•	•	• •	· ·	•	•	•	•	· ·	· ·	•	•	•	•	· ·	•	•	•	· ·	•	•	•	· ·	•	· ·	•	•	· ·	•	•	•	•••	•	•	• •	•••	•
•	•	· ·	•	•	• •		•	•	•	• •	• •	•	•	•	•	· ·	· ·	•	•	•	•	· ·	•	•	•	· ·	•	•	•	· ·	•	· ·	•	•	• •	•	•	•	• •	•	•	• •	· ·	•
•	•	• •	•	•	• •		•	•	•	• •	••••	•	•	•	•	• •	· ·	•	•	•	•	• •	•	•	•	· ·	•	•	•	• •	•	•	•	•	• •	•	•	•	•••	•	•	•	• •	•

·       ·	Euler's	THEOREM	· · · · · · · ·		
Theorem: For k	$ \begin{array}{l} \text{relatively} \\ \phi(n) \\ k \equiv \end{array} $	prime to 1 (mod n	n , ,		
E.g., n=12	φ(12) =	4 gcd 1	£123=	{1,5,7,	11 3.
.	4 = 1 $5^{4} = 1$ $7^{4} = 1$	(mod 12) (mod 12)	4  7 ≡	(mod 12)	
	T = 1 (	mod 12) mod 125			

	E	uler's -	THEOREM		· · · · · · · · · · · · · ·
Lemma 1:	For k	relatively	prime to	n and	· · · · · · · · · · · · ·
· · · · · · · · · · · · · ·	any s	inbaet S	⊆ [0, ۱,	-, n-13	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · ·		[KS]	=  S		· · · · · · · · · · · · ·
· · · · · · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · ·		
	· · · · · · · ·				
· · · · · · · · · · · · · · ·		· · · · · · · · · · ·	· · · · · · · · · · · · ·	· · · · · · · ·	
· · · · · · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · ·	· · · · · · · ·	· · · · · · · · · · · · · ·
	· · · · · · · ·	· · · · · · · · · · · · ·		· · · · · · · ·	· · · · · · · · · · · · ·

	Euler's	THEOREM		
Lemma 1:	For k relatively	y prime to n	a and a	
· · · · · · · · · · · · · · · ·	Any Subcet S	⊆ [0, 1,,	n-13,	
	KS KS	=  S		
n=5	$S = \{0, 2_1 3\}$	S =	3	
k= 2	ks = {0,4,1	}  ks =	3	
	$\mathbf{h} = \mathbf{h} + $	· · · · · · · · · · · · · ·		
· · · · · · · · · · · · · ·	mod n		· · · · · · ·	
· · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · ·		

	Euler's T	HEOREM
Lenna 1:	For k relatively	prime to n and
	any subcet S	⊆ {0, 1,, n-1},
· · · · · · · · · · · · ·	ks.	=  S
Proof	For any SISGES,	by concelability of k,
· · · · · · · · · · · · · ·	$ks_1 \equiv ks_2 \pmod{2}$	$n \iff S_1 \equiv S_2 \pmod{n}$
· · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	
	· · · · · · · · · · · · · · · · · · ·	
· · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·

	Euler's Theorem
Lemma 1:	For k relatively prime to n and
	any subset $S \subseteq \{0, 1,, n-1\}$ ,
	kS  =  S
Prof	For any SISCES, by concelability of k,
· · · · · · · · · · · · ·	$k_{S_1} \equiv k_{S_2} \pmod{n} \iff S_1 \equiv S_2 \pmod{n}$
· · · · · · · · · · · · ·	
· · · · · · · · · · · · · ·	
· · · · · · · · · · · · · · ·	

EULER'S IHEOREM	· · · · · · ·
Lemma 1: For k relatively prime to n and	· · · · · · ·
any subset $S \subseteq \{0, 1, \dots, n-1\}$ ,	· · · · · · ·
KS  =  S	· · · · · · ·
Proof: For any SISCES, by concelability of K,	· · · · · · ·
$k_{S_1} \equiv k_{S_2} \pmod{n} \iff S_1 \equiv S_2 \pmod{n}$	· · · · · · ·
$\Leftrightarrow S_1 = S_2 \text{ (Since C)}$	$(\leq S_1, S_2 \leq n)$
Distinct elements in S are mapped to distinct elements u	n KS.

•	· · ·		•	•	· · ·	•	•	•			• •	•	•	•	E	Ú	) L	E	- <b>f</b> -	- 2	2	•	1	H	E	50	) <b>R</b>	E	51 1	Ŋ	•	· ·	•	•	• •	•	•	•	· ·	•	•	•	· ·	•	•
•	· ·	k	l			. 2		•	: <b> </b>	70	1		•	Ù	j	, - , -	E		0	),	. <b> </b>  -	1	. – .	-			n	· 		5	•	· ·	•	•	· ·	•	•	•	••••	•	•	•	· ·	•	•
•	· · ·	L	E		90	d	1	Ş	n	J	· ·	<u>A</u> 1	nd		j	•	e		ļc	٦	1	Ł	n	3	•		17	· · · · · · · · · · · · · · · · · · ·		l	j		<b>N U</b>	1,	•)	e		9	c	1	- 9		3	•	•
•	• •	•	•	•	••••	•	•	•		• •		0	•	0	•	•	· ·	•	•	•	•	•	· ·	•	•	•	•	• •	•	•	•	· ·	•	•	• •	•	•	•		•		•	• •	•	•
	••••	•	•	•	••••	•	•	•	•	• •		•	•	•	•	•	• •	•	•	•	•	•	• •	•	•	•	•	••••	•	•	•	• •	•	•	•••	•	•	•	• •	•	•	•	• •	•	•
•	• •	•	•	•	• •		•	•				•	0	•	•	•	• •		•	•	•	•	••••		•	•	•	••••	•	0	•	• •	•	•	••••		•	•	• •	•	•	•	• •	•	•
	• •	•	•	•	• •		•	0	•	• •	• •		0	•	•	•	• •		•	•	•	•	• •			•	•	••••		0	•	• •	•		••••	•	•		• •	•	•	•	• •	•	•
	• •		•	•	• •	•	•	•	•	• •			•	•	•	•	• •		•		•	•	• •		•	•	•	• •	•	•	•	• •		•	• •		•		• •		•	•	• •	•	•
			•				•	•					•																	•	•			•											
		•	•	•		•	•	•				•	•	•	•			•	•	•	•			•	•	•	•		•	•	•		•	•		•	•	•		•	•			•	•
		•		•		•		•				•	•	•	•	•			•	•		•			•	•				•			•			•	•			•	•	•		•	
	• •	•	•			•	•	•		• •		•	•	•	•	•		•	•	•		•		•	•	•	•	• •	•	•			•	•	• •	•	•	•		•	•	•		•	•
•	• •	•	•	•		•	•	•	•			•	•	•	•	•		•	•	•	•	•		•	•	•			•	•	•		•			•	•	•		•	•	•		•	•

	enna 2	For	EULER'	s Th	EOREM			•
i	e ged !	L{n} an	d j e ged	12n3	, , ⇒ i.j	(med n) E	gcd1 {n }	
	Proof:	By prime	factorizat	ion Ne	sult,			•
• • • •			· · · · · · · · · · · · · · · · · · ·	· · · · ·		· · ·	0 1 -	
			l and r	n have	No Common	prime -	factors	•
· · · · ·			j and n	have have	No Common	prime -	factors	•
			l and r j and n	have have	No Common	prime -	factors	· · · · · · · · · · · · · · · · · · ·
			l and r j and n	have have	No Common	prime -	factors	
			l and r j and n	have have	No Common	prime -	factors	
			l and r j and n	have have	No Common	prime -	factors	
			l and r j and n	have have	No Common	prime -	factors	
			l and r j and n	have have	No Common	prime -	factors	

· · · · · · · · · · · · · · · · · · ·	Euler's Theorem	<b>1</b>
Lemma 2: For i,	j e {0, 1,, n-1	
ie gcd 1 {n} and	je ged1∑n3 ⇒ i	·j(modn) e gcd1 {n}
Proof: By prime of	'actorization result,	
· · · · · · · · · · · · · · · · · · ·	i and n have no com	mon prime factors
· · · · · · · · · · · · · · · · · · ·	j and n have —	· · · · · · · · · · · · · · · · · · ·
$\Rightarrow$ i	.j and n have	· · · · · · · · · · · · · · · · · · ·

	Euler's Theorem
Lemma 2: For i,	i e {0, 1,, n-1}
iegcd1{n} and	je gedl{n} => i.j(modn)e gedl{n}
Prof: By prime fo	actorization result,
	and n have no common prime factors
⇒ i	j'ard n have
⇒ ij(mad r	n) and n have ?

Lemma 2: For i,	EULER'S THEOREM $j \in \{0, 1,, n-1\}$	<b>1</b>
ie gcd1 {n} and	je gedl {n} =>	·j(modn) e gcd1 {n }
.       .	NOT true for i+j	
	$\tilde{l} = 2$ $\tilde{l} = 2$	
	( <sup>2</sup> n=5	

	Eυ	ler's T	THEOREM	
Conollery:	For any k	e ged l	{n},	
	K ga	d1 {n3	= gcdLfn	3
· · · · · · · · · · · · · ·			· · · · · · · · · · · · · ·	
· · · · · · · · · · · · · · ·			· · · · · · · · · · · · · ·	
· · · · · · · · · · · · · ·			· · · · · · · · · · · · · ·	
· · · · · · · · · · · · · · ·			· · · · · · · · · · · · · · ·	
· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·		· · · · · · · · · · · · · ·	

· · · · · · · · · · · · · · · · · · ·	Euler's	THEOREM		· · · ·
Conollary : Fo	r any k e gcd	1 {n},		
.       .	K gcd I En 3	= gcdLin	3	· · · ·
Proof: Bi	y Lemma L   k	:, gcd1 {n}] =	gcd 1 {n3	
· · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	
	· · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	

	Euler's Theorem	· · · · · · ·
Conollary: For	any k e gcd1 {n},	· · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	$k \operatorname{gcdl} \{n\} = \operatorname{gcdl} \{n\}$	· · · · · · · ·
Proof: By	Lemma L $ k, gcdl \{n\}  =  gcdl \{n\} $	· · · · · · · ·
By Lemma 2,	for any ie gcd 1 {n3, kie gcd 1 {n3	
	1       1	.         .

EULER'S THEOREM Convelong: For any k e gcd 1 {n},  $k \operatorname{gcdl} \{n\} = \operatorname{gcdL} \{n\}$ Proof: By Lemma L  $|k, gcdl \{n\}| = |gcdl \{n\}|$ By Lemma 2, for any ie gcd  $1 \le n3$ , kie egcd  $1 \le n3$ .  $\Rightarrow k \cdot gcd 1 \le n3 \leq gcd 1 \le n3$ .

	Euler's Theorem
Conollary :	For any k e gcd1 {n},
	$k \operatorname{gcdl} \{n\} = \operatorname{gcdl} \{n\}$
Proof:	By Lemma L $ k, gcdl \{n\}  =  gcdl \{n\} $
By Lemma	$22$ , for any ie gcd 1 {n}3, ki e gcd 1 {n}3. ⇒ K gcd 1 {n}3 ⊆ gcd 1 {n}3.
Thus,	$k gcd1 \{n\} = gcd1 \{n\}$

	Euler's	THEOREM	
Conolley: For	any k e gcd	1 {n},	
	k gcd 1 {n}	= gcdL{n}	
<b>E.g.</b> , n=5	gcd 1 §n3	$= \{1, 2, 3, 4\}$	
k = 3	k.gcd 1 {n} =	= {3, 1, 4, 2}	· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · ·	

	Euler's Theorem
Conolley: For	$any \ k \in gcd1 \{n\},$
<b>E</b> g., n=5	$gcd 1 \{n\} = \{1, 2, 3, 4\}$
k = 3	$k \cdot g \cdot d \cdot 1 \{ n \} = \{ 3, 1, 4, 2 \}$
	multiplying by k reorders/permites the original set of elements

•	•	· · ·	•	•	· · ·	· •	•	•	•	· · ·	· ·	•	•	•	E	J	L	E	r F I		2	· · ·	T	H	E	0	R	E	M		•	· · ·	•	•	· · ·	•	•	•	· ·	•	•	•	· ·	•
•		Th	20 20	h	e. En	· ·	•	•	F	0 >	L	•	k		•	h	J			iv		ly	•	-  -	ri			•	+	  D .	<b>N</b>		•	•	• •	•	•	•	• •	•	•	•	•••	•
•	•	· · ·	•	•	· · ·		-	•	•	· · ·	· · ·	•	•	•	•	k k	φ	(n (	)			<b>V</b>			•	· · ·	1	104					•	•	· · ·	· · ·	•	•	· ·	•	•	•	· · ·	•
•	•	· ·	•	•	• •		•	•	•	• •	••••	•	•	•	•	· ·	· ·	•	•	•	•	· ·	•	•	•	· ·	-	•	•	• •		• •	•	•	• •	•	•	•	•••	•	•	•	• •	•
•	•	· ·	•	•	• •		•	•	•	• •	· ·	•	•	•	•	· ·	· ·	•	•	•	•	· ·	•	•	•	· ·	•	•	•	· ·	•	· ·	•	•	· ·	•	•	•	· ·	•	•	•	· ·	•
•	•	· ·	•	•	• •		•	•	•	• •	· ·	•	•	•	•	· ·	· ·	•	•	•	•	· ·	•	•	•	· ·	•	•	•	· ·	•	· ·	•	•	· ·	•	•	•	•••	•	•	• •	•••	•
•	•	· ·	•	•	• •		•	•	•	• •	• •	•	•	•	•	· ·	· ·	•	•	•	•	· ·	•	•	•	· ·	•	•	•	· ·	•	· ·	•	•	• •	•	•	•	• •	•	•	• •	· ·	•
•	•	• •	•	•	• •		•	•	•	• •	••••	•	•	•	•	• •	· ·	•	•	•	•	• •	•	•	•	· ·	•	•	•	• •	•	•	•	•	• •	•	•	•	•••	•	•	•	• •	•

	Euler's T	THEOREM	· · ·	· · · · ·	· · · · ·	
Theorem :	For k relatively	prime to n		· · · · · · · · · · · · · · · · · · ·	· · · · ·	
Proof:	K ≡ By Corrollary,	1 (med n)	•	· · · · · · · · · · · · · · · · · · ·	· · · · ·	
	() K·gcd1 {n}	= gcd1{r	3-1	· · · · · ·		
			· · ·			

·       ·	Euler's	THEOREM	· ·	· ·	· · ·		· ·	· ·	· ·	
Theorem :	For k nelatively $\phi(n) =$	prime to n 1 (mod n)	,	· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · ·
Proof:	By Corollary, K.gcd1{n3	= gcd1{r	3-	· · · · · · · · · · · · · · · · · · ·	<ul> <li>.</li> <li>.&lt;</li></ul>		· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	
.       .	Consider		· ·	· ·	· ·		· ·	· ·	· ·	
	TT S S $\in k$ gcd $I$ s $n$ s		· · ·	· · ·	· · ·	•	· ·	· · ·	· ·	· · ·

	Euler's	THEOREM		· · ·		· · ·	
Theorem :	For k relatively $\phi(n)$	prime to n 1 (mod n)	<b>j</b>		<ul> <li></li></ul>	· · · ·	
Proof:	By Convellary, K·gcd1{nz	= gcd1{r	3-				
····································	Consider $TT S \equiv$ $S \in k \operatorname{gcdJsnz}$	$\frac{1}{1} S (modsegcd1{n}{}$	1 n )	<ul> <li></li></ul>	·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·           ·         ·         ·	<ul> <li>.</li> <li>.&lt;</li></ul>	

	Euler's	THEOREM	
Theorem :	For k relatively	prime to n	<b>f</b>
· · · · · · · · · · · · ·	$\varphi_{(n)}$ k =	1 (mod n)	•
Proof:	∏ s ≡	TT S (mod	n)
· · · · · · · · · · · · ·	SE K gcd]şnz	segcd1{n}	
· · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·	
· · · · · · · · · · · · · ·		.       .	

	Euler's	THEOREM	
Theorem :	For k relatively	prime to n	,
· · · · · · · · · · · · ·	φ(m) k Ξ	1 (mod n)	•
Proof:	TTS≡	TT S (mod	(n)
	SE Kgcd]{n}	$s \in gcd1\{n\}$	
· · · · · · · · · · · · · ·			

· · · · · · · · · · · · · · ·	Euler's	THEORE	M	
Theorem :	For k relative $\phi(n) =$	ly prime - 1 (mod	ton,	
Proof:	TT S = S E k gcd]{n}	$= \prod S$ Segcd1{n}	(mod n)	$\left(\begin{array}{cccccccccccccccccccccccccccccccccccc$
	$\Rightarrow \prod ks \equiv$ S $\in gcds \{n\}$	$= \prod S$ segcd1{n}	(mod n)	.       .
· · · · · · · · · · · · · · · · · · ·				

	Euler's	THEOREM	
Theorem :	For k relatively \$\overline{(n)}\$	prime to n	<b>J</b> .
Proof:	K = TT S = S E k gcd]{n?	I (mod n) TTS (mod segcd1{n}	• • • •
	$ = \frac{1}{\sum_{k \in gcdJ \{n\}}} $	$\frac{1}{11} S (mod)$ segcd1{n}	$\left( \nu \right)$
=	$ \geq k^{p(n)} \prod_{\substack{S \in gcd1\{n\}}} \equiv $	TTS (mod r egedlard	· )

Theorem : For k helatively prime to n, $\phi(n)$ $k \equiv 1 \pmod{n}$ . Proof: $k^{\phi(n)} \prod S \equiv \prod S \pmod{n}$ $segcdl\{n\} = egcdl\{n\}$	· · · · · · · · · · · · · ·	Euler's T	HEOREM	
$k \equiv 1 \pmod{n}.$ Proof: $k^{p(n)} \equiv T \subseteq (mod n)$ . segcd1{n} $s \in gcd1$ {n} $(mod n)$	Theorem :	For k relatively	prime to n,	
$K^{(n)} = \prod_{s \in gcd1\{n]} (mod n)$	<b>D</b> - (	$\phi(n) \qquad \qquad$	(mod n)	
	1.00+:	$k^{(11)} \text{TT} S \equiv \text{TT} \\ \text{segcd1}\{n\}  \text{segco}$	C (mod n) Higrz	
	· · · · · · · · · · · · · · ·			· · · · · · · ·
	.       .	.       .		

·       ·	Euler's	THEOREM		· · · ·	· · · ·		•
Theorem :	For k relatively $\phi(n) = \phi(n)$	prime to n 1 (mod n)	j	<ul> <li></li></ul>	· · · · · · · · · · · · · · · · · · ·		• • • • • •
Proof:	$k^{(n)} T S \equiv -$ Segcd1{n} Se	TTS (mod n) gcdlfrz	•	<ul> <li></li></ul>	· · · · · · · · · · · ·		
	E gcd 1 {	n} (by Limma	2)	· · · ·	· · · ·	· · · · · · ·	•

·       ·	Euler's	THEOREM	· · · · ·	· · · · ·	· · · ·	• •
Theorem :	For k relatively $\phi(n)$	prime to n, 1 (mod n)				
Proof:	$k^{(n)} T S \equiv -$ Segcd1{n} Sec	TTS (mod n) Jedlfrz				
·       ·	E gcd 1 {r	n} -> Cancelable				· · ·
·       ·						

	Euler's Theorem
Theorem :	For k relatively prime to n,
Proof:	$k^{\emptyset(n)}$ TTS = TTS (mod n) Segeds{n] segeds{n}
	€ gcd 1 {n} → Cancelable
	$\implies k^{Q(n)} \equiv 1 \pmod{n}$