LECTURE 9 NUMBER THEORY I : GCD Ten 19 2026 ROHIT VAISH	· · · · · ·	COL 202:	DIS CRETE	MATHEMATICAL	STRUCTURES
LECTURE 9 NUMBER THEORY I : GCD TAN 19 2024 ROHIT VAISH					
NUMBER THEORY I : GCD Ten 19 2024 ROHIT VAISH	· · · · · ·	· · · · · · · · · · · ·	I F.C.	TUPF. 9	
NUMBER THEORY I : GCD Tan 19 2024 ROHIT VAISH	· · · · · ·	· · · · · · · · · · ·			
TAN 19 2024 ROHIT VAISH	· · · · · ·		MBER T	HEORY I :	GCD
Ten 19 2024 ROHIT VAISH	· · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	••••••
TAN 19 2024 ROHIT VAISH	· · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
TAN 19 2024 ROHIT VAISH	· · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
TAN 19 2024 ROHIT VAISH	· · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
	· · · · · ·	JAN 10	2024	LOHIT	VAISH

ARITHMETIC A	SSUMPTIONS
Assume usual rules for t,	• ,
a.(b+c) = a.b +	a, c (Distributivity)
a.b = b.a	(Commutativity)
a.(b.c) = (a.b).c	(Associativity)
a + o = a	(Addifive Identity)
a - a = 0	(Addéfive Inverse)
a + 1 7 a	

· · ·	•	· · ·	· · ·	•	· · ·	•	•	· ·	•	•		D	- - - -	V) 	•		TH ,	E	0	R	E	M	· ·	•	· ·	•	· ·	· ·	•	•	· ·	•	•	· ·	•	•
· · · · · · · · · · · · · · · · · · ·	•		et	- - - -			Ar Ar	d	•	d			be		р [~	<u></u> -}-	ge	٢Ŧ	· · ·	s Su		h		th	at	· · ·	0		Ę	0	· · · · · · · · · · · · · · · · · · ·	•	•		•		· · ·	•	•
· · ·	•		he	n	,	th.	ور	Ł	e	Xn	sł	3	0	Ļ	U	In	iq	ne		 	0	vr	•	q	ι [Υ	\ \	ge	5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5		1	Ør	d	ן או י	-	2	:.t	· · ·	•	•
· · ·	•	· · ·	· · ·	•	· · · · · · · · · · · · · · · · · · ·	•	•	· ·	•	•	· ·		ר ר ר		-	•	9	, 	[d	 	F))	L L	· · ·		λni	d d		, } ∠ ,	<pre></pre>	h	2	- 0	Ľ			· ·	•	•
· ·	•	· ·	· ·	•	· ·	•	•	· ·	•	•	• •	• •	•	· ·	•	•	· ·	•	••••	•	• •	· ·	•	· ·	•	· ·	•	· ·	•	· ·	• •	•	•		•	• •	· ·	•	•
· ·	•	· ·	• •	•	· · ·	•	•	• •	•	•	• •	• •	•	••••		•	· ·	•	• •	•	•	· ·	•	· ·	•	• •	•	• •	•	· ·	· ·	•	•		•	•	· ·	•	•
· ·	•	· ·	• •	•	· ·	•	•	• •	•	•		· ·	•	• •	•	•	· ·	•	• •	•	• •		•	• •	•	· ·	•	· ·	•	• •		•	•		•	• •	· ·	•	•

	DIVISION	THEOREM
Let n and	d be integers	such that $d \neq 0$.
Then, there ex	rists a unique	pair of integers q and h s.t.
	$n = q_1 d$	$ + n$ and $0 \le n < d $.
	quotient (n, d)	remainder (n, d)
		· · · · · · · · · · · · · · · · · · ·

DIVISION THEOREM
Let n and d be integers such that $d \neq 0$.
Then, there exists a unique poir of integers q and h s.t.
$n = q d + n \text{and} 0 \le n < d .$
Eq., Say d=3. Then, for any n, thus is a
Unique q such that $n=3q$ or $n=3q+1$ or $n=3q+2$.

	DIVISION	THEOREM	
Let n and d	be integers	such that $d \neq 0$	
Then, there exis	sts a unique	pair of integers q	, and r s.t.
· · · · · · · · · · · · · · · · · · ·	$n = q_1 q$	$d + h$ and $0 \leq$	n < d
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
-2 d -1d1	0 [d]	2 d 3 d n 4 d 5	

· ·	DIVISION	THEOREM
Let n and	d be integers	such that $d \neq 0$.
Then, there ex	cists a unique	poir of integers q and n s.t.
. .	$n = q_{1}$	$d + h$ and $0 \le h \le d $.
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	> r = offset in the block
-2 d - d	[0] [d]	2 d 3 d n 4 d 5 d
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · ·	g: The block where n is in

•	•	•	•	•	•	•	· · ·	•	· ·	•	•	•	•	•	•	•	•	•	•		?1	N	۲ ۱	S I I I I I I I I I I I I I I I I I I I		51	L	. `	T	Y	•	•	· · ·	•	•	•	•	· · ·	· · ·	· ·	•	•	•		· ·		•	•
•	•	•	•	•	•	•	d	•	d d	0 \ 	1 1 1	de	2	•	•	v V v		•	•	•	Ņ		•	•	n M			C	V	• C	l l	•	-	f	عر	•	S	571	nl 1	•		Y	•		, , , ,	•	•	•
•	•	•	•	•	•	•	• •	 •	•	•	•	•	•	0	•	•	•	•	•	•	• •		•	•	•	•	•	••••	•	•	•	•	••••	•	0	•	•	• •	•	•	•	•	•	•		•	•	•
•	•	•	•	•	•	•	• •	 •	•	•	•	•	•	•	•	•	•		•	•	• •		•	•	•	0		o o		0	•	0	• •		•	•	•	• •	•	•	•			•	• •	•	•	•
•	•	•	•	•	•	•	• •	 •	•	•	•	•	•	•	•	•	•	•	•	•	· ·		•	•	•	•	•	• •	•	•	•	•	• •	•	•	•	•	· ·	•	•	•	•	•	• •	• •	•	•	•
•	•	•	•	•	•	•	• •	 •	•	•	•	•	•	•	•	•	•	•	•	•	••••		•	•	•	•	•	• •	•	•	•	•	••••	•	•	•	•	••••	•	•	•	•	•		· ·	•	•	•
•	•	•	•	•			• •	 •	•	•	•	0	•	0	•	•	•	•	•	•	• •		•	•	•	•	•	• •		•		•	••••	•	•			• •		•	•	•	•	•	• •	•	•	•
•	•	•	•	•	•	•	• •	 •	•	•	•	•	•	•	•	•	•	•	•	•	• •		•	•	•	•	•	• •	•	•	•	•	· ·	•	•	•	•	• •	•	•	•	•	•	• •	••••	•	•	•
•	•	•	•				• •	 •	•	•	•	0	•	•	•	•	•	•	•					•	•	•	•	••••		•		•	• •		•		•			•	•	•	•	•	•••	•	•	•
•	•	•	•	•	•		• •	 •	•	•	•	0	•	•			•			•	• •		•	•	•	•		• •		•		•	• •		•			• •	•	•	•	•	•	• •		•	•	•
•	•	•	•	•	•	•	• •	•	•	•	•	•	•	•	•	•	•	•	•	•	• •		•	•	•	•	•	• •	•	•	•	•	• •	•	•	•	•	• •	•	•	•	•	•			•	•	•

DIVISIBILITY integers _ d divides n ig n = qr. d for some qr

	DIVI	SIBILITY		· · · · · · · · · · · · ·
		integ	eu	· · · · · · · · · · · ·
d div	ides n ÿ	$n = q_{f} \cdot d$	for some	
· · · · · · · · · · · · · · ·		· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · · · · ·
E.g., 2	divider – 6	2 - 6		
a ka - 6	is a multiple	of 2.		· · · · · · · · · · ·
a.k.a. 2	is a divisor o	of -6		· · · · · · · · · · · ·
	· · · · · · · · · · · · · · · · · · ·			· · · · · · · · · · · ·
· · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · ·
	· · · · · · · · · · · · · · · · · · ·		· · · · · · · · · · · ·	· · · · · · · · · · · · ·

DIVISIBILITY	
inter	gen
d divides n ig n = q.d	for some g
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
E.g. , 2 divider -6 2/-6	· · · · · · · · · · · · · · · · · · ·
aka-6 is a multiple of 2.	
a.k.a. 2 is a divisor of -6	
n/o for every n became	$0 = 0 \cdot n$
· · · · · · · · · · · · · · · · · · ·	

 VIVISIBILITY	FACTC	
 		· · · · · · · · · · · · · · · ·

•	•	· ·	•	•	· ·	•	•	· ·	•	•	•	•	•	J)	V	S	Ņ	B		- -	T	Y	· ·	F	F	łC	Л	2	· ·	•	· ·	· •	•	• •		•	•	· ·	•	•	
					• •																																					
•		• •			• •		•	• •				•	• •			• •					Ľ		•	•			• •			• •						•		•	• •		•	• •
•		• •			• •		•	1.	1			•	• •	-		\geq			•	 ·				3	•		• •	•		• •		•		•	•		•	•	• •		•	• •
•	•	• •	1	•	• •		· (()L	ŀ	-Ϋ \		•	• •	0	0	7			. U	Λ.	Y			. • 1			• •			• •	•	•			•				• •	•	•	• •
•		• •	1					• •	•			•	• •	•		• •							•				• •			• •	•	•			• •						•	• •
•	•	• •			• •			• •				•	•		•	•	•			• •		•	•				• •			•									• •			• •
	•		•	•	• •		•	• •				•	• •		•					• •			•		•		• •	•			•	• •		•					• •	•	•	
•	•					•		• •					• •																													
					• •								• •																													
•					• •			• •				•	• •			• •				• •			•				• •			• •					•	•			• •			• •
•		• •	•		• •		•	• •				•	• •		•	• •			•	• •			•		•		• •	•		• •		•		•	•		•	•	• •		•	• •
•	•	• •		•	• •		•	• •				•	• •		•	• •			•	• •			•				• •			• •	•	•			•				• •	•	•	• •
•		• •			• •			• •					•			• •											• •			• •									• •		•	
•	•	• •			• •			• •				•	•		•	•	•			• •		•	•				• •			•									• •			• •
	•			•	• •		•	• •				•	• •		•				•	• •			•				• •												• •			• •
				•			•	• •				•	• •		•					• •			•																• •			

•	• •	 •	•	· ·	•	•	• •	•	•	•	•	• •	D	?]	V	۲ ا)))	BI	Ļ	1-	[` `	1		FI	A (:7	Ŝ	• • • •	•	· ·	•	•	•	 •	•	· ·	•	•	· ·	
•	• •	1	•	· · ·	•		d		Ŷ		•	· · ·			7	•	•	d	•	l V	k	-	Ń		•	· · ·	•	· · ·	•	· · ·	•	•		•	•	· ·	•	•	· ·	
•	• •	2	•	· · ·	•	d		N		•	0	in	d	•	· · ·	J	1	n	•		· · ·	7	• •		d			(M	+	m))	•	• •	 •	•	· ·	•	•	· ·	
•	• •	 •	•	• •	•	•	• •	•	•	•	•	· ·	•	•	· ·	•	•	• •	•	•	• •	•	• •		•	• •	•	• •	•	• •	•	•		 •	•		•	•	• •	
		 •	•	• •	•	•	• •		0	•	•	• •	•	•	• •	•	•		•	•	• •	•			•	• •	•	• •	•	• •	0	•		 •		• •		•	• •	
	• •	•	•	• •	•	•	• •		•	•	•	• •		•	• •	•	•	• •	•	•	• •	•			•	• •	•	• •	•	• •	•	•		 •	•	• •	•	•	• •	
•		 •	•	• •	•	•	• •		•	•	•	• •	•	•	• •		•	• •	•	•	• •	•			•	••••	•	• •	•	• •	•	•		 •	•	• •	•	•	• •	
•	• •	 •	•	· ·	•	•	• •	•	•	•	•	• •	•	•	• •	•	•		•	•	• •	•	• •		•	· ·	•	· ·	0		•	•		 •	•	• •	•	•	• •	
	• •	 •	•	• •	•	•		•	•	•	•			•	• •	•	•		•	•		•	• •		•	• •	•	• •	•			•		 •	•	• •	•	•	• •	
•	• •	 •	•	• •	•	•		•	•	•	•		•	•	• •	•	•		•	•	• •	•	• •		•	• •	•	• •	•		•	•		 •	•		•	•	• •	
	• •	•	0	• •						•	•		•		• •	•	•		0	•	• •	•	• •		•	• •	•	• •	0			•	• •	 •				•		
		•	•	• •	•	•			•	•	•		•	•	• •	•	•	• •	•	•	• •	•	• •		•	• •	•	• •	•	• •	•	•		 •	•	• •	•	•	• •	

· ·	• •	•	· ·	· ·	•	· ·	•	· ·	•		D	21 ' 1 '	VI	ן ג ג	B	11	-1'	T'	1		FI	40	7	2	•	· ·	•	• •	•	•	· ·	•	• •	• •	•	· ·
· · · · · · · · · · · · · · · · · · ·	· · ·	1	•	· · · · · · · · · · · · · · · · · · ·		d		n	•	· · ·			?	· · ·		d		k		n .	•	· ·	•	· · ·	•	· · ·	•	· · ·	•	•	· ·	•		· ·	•	· · ·
· · · · · · · · · · · · · · · · · · ·	· · ·	2	· · ·	· · · · · · · · · · · · · · · · · · ·	d		n	· · ·) n	d	· · · · · · · · · · · · · · · · · · ·	д		ŝ	· · ·	•	· · ·	7	· · · · · · · · · · · · · · · · · · ·		d	l		n-I		۲ ۲)	· · ·		•	· · ·	•		· · ·	•	· · ·
· ·	• •	3	• • •	· ·	d	ใา		· ·	0	Inc	d	· · ·	d		m	• •	•		7	· ·	C	λ		<u></u> S-	n M	• •	+	ł	- Y	m))	•	• •	• •	•	· ·
• •	••••	•	• •	••••	•	•••	•	· ·	•	• •	•	••••	•	· ·	•	••••	•	• •	• •	•••	•	• •	•	••••	•	· ·	•	• •	•	•	• •	•	• •	• •	•	• •
• •	• •	•	· ·	• •				• •	•	• •		• •	•	• •		• •		• •		• •	•		•	• •	•	• •	•	• •	•	•	• •					
			• •	• •								• •		• •				•	• •					• •						•		•	•			• •
• •	• •		• •	• •				• •		• •		• •		• •		•		•	• •	• •		•		• •		• •		• •		•	• •	•	•	• •		• •
			• •																												• •			• •		• •
• •	• •	•		• •								• •																	•	•			•	• •	•	
• •	• •	•	•••	••••	•	• •	•	• •	•	• •	•	•••	•	• •	•		•			• •	•		•			• •	0	• •	•	•	• •	•	•	•••	•	• •

• • •	· · · · · ·		DIVISIBILITY	Facts
· · · ·	1.	dln	$\Rightarrow d k.r$	n
· · · ·	2.	dln	and $d \mid m \Rightarrow$	$d \left(\left(n+m \right) \right)$
· · · ·	3.	dln	and $d \mid m \Rightarrow$	$d \mid (s \cdot n + t \cdot m)$
· · · ·	3.	dlm	and $d \mid m \Rightarrow$	d (s.n + t.m) integer linear combination
· · · · · · · · · · · · · · · · · · ·	3.	dlm	and dlm ⇒	d (s.n + t.m) integer linear combination
· · · · · · · · · · · · · · · · · · ·	3.	dlm	and dlm ⇒	d (s.n + t.m) integer linear combination

· · · · · · · ·		DIVI	SIBILITY	FACTS	· · · · · · · ·		• •
1.	dln	\Rightarrow	d K.	n			· · · · · · · · · · · · · · · · · · ·
2.	dln	and d	llm ⇒	, d [(n-t-m)	.	· · · · · · · · · · · · · · · · · · ·
3.	dlm	and d	lm ⇒	d (s-	n + t	m)	· · ·
d is	A Common	n divicer	of n and n	n intege	r linea	Com binati	
· · · · · · · ·	· · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · ·				• •

•	GREATEST						τ	•	() D) [1		0 1	Ч		1	D	11	J/	۲ ۲			· · ·	•	•	• •		•	•	•	• •		•	•												
•	•	•			d (ן (א	J L	m) 1)	•			· ·	c (γ	e	a+	-U	 		C	-0'	r Ma V	n M	101	2 / /		di	۰ ۷	۲ ۲ ۲	<i>۴</i> /		of	•	n		λr	d	Ŷ	m M	•	•	• •		•	•
															J.																															
•			• •		• •				•	•	•	•																• •							• •			•			•	•				
•	•	•	• •	•	• •				•	•		•	• •		•	•	•	•	•	•	• •				•	•	•	• •			•				• •		•	•	•	•	•	•	• •	•		•
•	•	•	• •		• •			•	•	•	•	•		•	•	•	•	•	•	•	• •		•			•	•	• •	•	•					• •		•	• •			•	•	• •	•		1
•	•		• •		• •			•		•	•	•	• •								• •				•	•		• •							• •								• •			1
			• •		• •							•																							• •											
•			• •		• •				•	•	•	•						•		•	• •					•	•	• •							• •			•				•	• •			
		•	• •		• •		•		•		•		• •		•			•		•	• •					•	•	• •			•				• •			•	•		•	•	• •	•		•
•	•	•	• •		• •				•	•	•	•	• •		•	•		•		•	• •				•	•	•	• •			•				•			•	•		•	•	• •			
•	•	•	• •		• •		•		•	•		•	• •		•	•		•		•	• •				•	•	•	• •			•				• •			•		•		•	• •	•		
•			• •		• •				•	•		•	• •					•			• •						•	• •							• •			• •				•				
			• •		• •																																									
•			• •		• •					•	•	•									• •							• •			•				• •			•			•	•	• •			
•	•	•	• •		• •		•	•	•	•	•	•	• •			•		•	•	•	• •					•	•	• •			•				• •			•			•	•	• •			•
•	•	•	• •		•			•	•	•	•	•	• •			•		•	•	•	• •					•	•	• •		•	•				•			•					•	•		•
			•		• •								• •								• •						•	• •							•			•					•			

		· · · · ·	G	REATEST	Common	DINIS	OR		
	fcd (n	, m)		greatest	Common	divisor	of n	and	
E		jcd ((8,1	0) = 2	· · · · · · · · · ·	· · · · · · ·	· · · · · ·	· · · · ·	· · · · · · · · · ·
	l' (icd	(7,8	P) = 1					
· · · · ·	 	· · · · ·	· · · ·	· · · · · · · · · · ·	· · · · · · · · · ·		· · · · · ·	· · · · ·	· · · · · · · · · ·
· · · · ·	· · · · ·	· · · · ·	· · · ·	· · · · · · · · · · ·			· · · · · ·	· · · · ·	· · · · · · · · · ·
		· · · · ·		· · · · · · · · · · ·					
· · · · ·	· · · · ·	· · · · ·	· · · ·	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · ·	· · · · · ·	· · · · ·	· · · · · · · · · ·

GREATEST COMMON DIVISOR gcd(n,m) := greatest common divisor of n and m $E_{1}, gcd(8, 10) = 2$ gcd (7,8) = 1 gcd(0,n) = for n 70

GREATEST COMMON DIVISOR gcd(n,m) := greatert common division of n and m $E_{1}, gcd(8, 10) = 2$ gcd(7,8)=1gcd (0,n) = n for n70

GREATEST COMMON DIVISOR gcd(n,m) := greatest common divisor of n and m $E_{1}, gcd(8, 10) = 2$ gcd (7,8) = 1 gcd (0,n) = n for n70 If p is prime, then ged (p,n) =

	GREATEST	Common	DIVISOR	· · · · · · · · · · · · · · · · · · ·
gcd(n,m)	:= greatert	Common	divisor of n	and m
F g, gcd gcd gcd	(8, 10) = 2 (7, 8) = 1 (0, n) = n	for n	7 0	Only divisors f p are $\pm 1, \pm p$.
If (s is prime, -	then ged (p(n) = 1 or p	· · · · · · · · · · · · · · · · · · ·

GREATEST COMMON DIVISOR gcd(n,m) := greatert common divisor of n and m $E_{1}, gcd(8, 10) = 2$ gcd(7,8) = 1Only divisors of gcd(0,n) = n for $n \neq 0$ ~ pare ±1, ±p. If p is prime, then ged(p,n) = 1 or p gcd (nim) always exists and is unique (Exercise)

•	•	• •	•	•	• •	•	•	•	•	• •	••••	•	•	•	F	Ň	r D		N	G	•	FH	IE	· ·	6	, } (Ľļ		•	•	•	· ·	•	•	•	• •	•	•	•	• •	•	•	
		• •			• •										• •			• •										• •				• •			•	• •	•		•	• •			• •
		• •			• •				•	•					• •			• •					• •				•	• •				• •			•	• •			•	•			• •
		• •			• •										• •			• •										• •				• •			•	• •	•		•	• •			• •
		• •			• •										• •			• •										• •				• •			•	• •	•		•	• •			• •
		• •			• •										• •			• •										• •				• •			•	• •	•		•	• •			• •
		• •			• •				•						• •			• •										• •				• •			•	• •	•		•	• •			• •
		• •			• •				•	•				•	• •		•	• •		•		•	• •				•	• •			•	• •	•		•	• •	•		•	• •			• •
		• •			• •				•	•				•	• •		•	• •		•		•	• •				•	• •			•	• •	•		•	• •	•		•	• •			• •
		• •		•	• •	•		•	•	•		•			• •			• •		•		•	• •		•	•	•	• •			•	• •	•	•	•	• •			•	•			• •
	•	• •		•	• •	•		•	•	•		•			• •			• •		•		•	• •		•	•	•	• •			•	• •	•	•	•	• •			•	•			• •
	•	• •		•	• •	•		•	•	•		•			• •			• •		•		•	• •		•	•	•	• •			•	• •	•	•	•	• •			•	•			• •
		• •			• •			•	•	•					• •			•					• •		•		•	• •			•	• •		•	•	• •	•		•	•			• •
		• •			• •			•	•	•					• •			•					• •		•		•	• •			•	• •		•	•	• •	•		•	•			• •
	•	• •			• •			•	•	• •		•			• •			• •								•	•	• •			•				•	• •	•		•	•			• •
		• •			• •			•	•	•					• •			•					• •		•		•	• •			•	• •		•	•	• •	•		•	•			• •
	•	• •			• •			•	•	• •		•			• •			• •								•	•	• •			•				•	• •	•		•	•			• •
		• •			• •			•	•	•					• •			•					• •		•		•	• •			•	• •		•	•	• •	•		•	•			• •
	•	• •			• •			•	•	• •		•			• •			• •								•	•	• •			•				•	• •	•		•	•			• •
	•	• •			• •			•	•	• •		•			• •			• •								•	•	• •			•				•	• •	•		•	•			• •
		• •			• •				•					•				• •				•					•	• •			•				•	• •			•	•			• •
	•	• •			• •			•	•	• •		•			• •			• •								•	•	• •			•				•	• •	•		•	•			• •
	•	• •			• •			•	•	• •		•			• •			• •								•	•	• •			•				•	• •	•		•	•			• •
		• •		•	• •	•			•	•				•	• •		•	• •		•		•	• •				•	• •			•	• •	•		•	• •			•	•			• •
	•	• •			• •			•	•	• •		•			• •			• •								•	•	• •			•				•	• •	•		•	•			• •
	•	• •			• •			•	•	• •		•			• •			• •								•	•	• •			•				•	• •	•		•	•			• •
	•	• •			• •			•	•	• •		•			• •			• •								•	•	• •			•				•	• •	•		•	•			• •
	•	• •		•	• •	•		•	•	•		•			• •			• •		•		•	• •		•	•	•	• •			•	• •	•	•	•	• •			•	•			• •
	•	• •		•	• •	•		•	•	•		•			• •			• •		•		•	• •		•	•	•	• •			•	• •	•	•	•	• •			•	•			• •
•		•		•	•	•			•	•				•	• •		•	•		•		•	• •	•	•			•			•	• •	•			• •				• •			• •
•		• •			• •				•	•					• •		•	• •				•	• •					• •			•	• •			•	• •	•		•	• •			• •
•		• •			• •				•	•					• •			•					• •					•			•	• •			•	• •	•			•			• •

Can try every number 1, 2,, min { lml, lnl }	· · ·	• •	•	· · ·	••••	•	· · ·	· ·	•	•	· · ·	•	F	in I	1 [] 1		N	G	· · ·	T	HI	E		a (ĊŢ		• • • •	• •		•	· · ·	•	•	•	· ·	•	•	· ·	•	• •	
	· ·	• •			n -	t	J.	· ·	د م	Ú 6	نگ (1	r 1	۱ ۱ ۱	m	be	K K	•	<u>1</u>	1 2) _)	1	· · · · · · · · · · · · · · · · · · ·	•		- ·	min	n {	Įr	nl	, l	ν. 		•	· ·	•	•	· ·	•	· · ·	
																																									,
				• •				• •			• •					• •			•																			• •			
	• •	• •		• •	• •		• •	• •		•	• •		•	• •		• •			•											•	• •		•	•				• •	•		
	• •	• •		• •	• •			• •		•	• •	•	•	• •	•	•			•					•		• •		•		•	• •			•				• •		• •	
	• •	• •		• •	• •		• •	• •		•	• •		•	• •	•	• •			•			•			•	•	• •			•	• •			•	• •		•	• •		•	l
	• •	• •		• •	• •		• •	• •		•	• •		•	• •		• •			•			•				•	• •				• •				• •		•	• •		• •	l
					• •		• •	• •						• •		• •	•					•					• •	•			• •						•				
																																									ļ
				• •	• •			• •			• •			• •		• •															• •							• •			
		• •		• •	• •		• •	• •		•	• •		•	• •	•	• •			•	•						•	• •			•	• •			•	• •			• •			
	• •	• •		• •	• •		• •	• •			• •			• •		• •			•				• •			•	• •				• •				• •			• •			
	• •	• •		• •	• •			• •		•	• •	•	•	• •	•	•			•					•		• •				•	• •			•				• •		• •	
· · · · · · · · · · · · · · · · · · ·	• •	• •		• •	• •		• •	• •	•	•	• •		•	• •	•	• •			•			•				•	• •			•	• •			•	• •			• •		•	l
· · · · · · · · · · · · · · · · · · ·	• •	• •		• •	• •		• •	• •		•	•		•	• •	•	•			•				• •			•	• •			•	• •		•		• •			• •		•	
				0 0	• •		• •	• •			• •			• •		• •			•							•					• •							• •			
																																			• •						

· · · ·		· · · ·	· · · · · ·		Find	ING	The	GCD		· · · · ·	
· · · ·		Car	, try	eve	y num	ber 1	12, -	, min	{ [m], [r	
· · · ·	· · ·	Ts	the	LA	better	Way?	· · · · · ·	· · · · · · · · · ·	· · · · · · ·	· · · · ·	· · · · · · · · ·
· · ·			· · · · · ·	· · · · · ·	· · · · · · ·	· · · · · ·			· · · · · ·	· · · · ·	· · · · · · · ·
· · ·		· · ·	· · · · · ·	· · · · · ·	· · · · · · ·	· · · · · ·	· · · · · ·	· · · · · · · · · ·	· · · · · ·	· · · · ·	· · · · · · · · ·
• • •	• •	· · ·	· · · · · ·	· · · · · ·	· · · · · · ·	· · · · · ·	· · · · ·	· · · · · · · · · ·	· · · · · ·	· · · · ·	· · · · · · · · ·
· · ·		· · ·	· · · · · ·	· · · · · ·	· · · · · · ·	· · · · · ·	· · · · · ·	· · · · · · · · · ·	· · · · · ·	· · · · ·	· · · · · · · · ·
• • •			· · · · · ·	· · · · · ·	· · · · · · ·	 	· · · · ·	· · · · · · · · ·	· · · · · ·	· · · · ·	· · · · · · · ·
			· · · · · ·		· · · · · · ·	· · · · · ·		· · · · · · · · ·	· · · · · ·		

FINDING THE GCD														
Recall division theorem: Unique $0 \le \Re \le m $ s.t. $n = q/m + \Re$														
REMAINDER	LEMMA :	gcd (n, m) = gcd(m, k)	for m≠0										
			• • • • • • • • • • • • •											
			• • • • • • • • • • • • • •											

FINDING THE GCD													
Recall division theorem: Unique $0 \le \Re \le m \text{ s.t. } n = q/ m + \Re$													
REMAINDER	Lemma :	gcd (n, m)	= gcd(m, k)	frr m≠0									
Proof !		· · · · · · · · · ·											
· · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · ·									
· · · · · · · · · · · · · · · ·		· · · · · · · · · ·		· · · · · · · · · · · · · ·									
· · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·									
· · · · · · · · · · · · ·			· · · · · · · · · · · · · · ·										
· · · · · · · · · · · · · · ·	· · · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · ·									

FINDING THE GCD Recall division theorem: Unique $0 \le \Re < |m| \text{ s.t. } n = q/m| + \Re$ REMAINDER LEMMA : gcd(n,m) = gcd(m,k) for $m \neq 0$ Proof: Suffices to show that far any integer p, $p|n and p|m \iff p|m$ and p|n

FINDING THE GCD							
Recall	division	theorem: l	longue $0 \leq \Re$.	$\leq m $ s.t. $n =$	9/m/+ 92		
REMAIND	DER LEM	mA : g	rcd(n,m) =	gcd(m, k)	for m≠0		
Proof :	Suffices	to show -	that far any	integer p,	Why?		
· · · · · · · · · · · · · · · · · · ·	pIn and	- p m <i>≤</i>	<>> plm	and plac			
· · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · · · ·		
· · · · · · · · · ·	· · · · · · · · · ·						

FINDING THE GCD								
Red	all	div	lsion	theorem	: Unique	$0 \leq \mathcal{H} \leq r $	$n \mid s.t. n =$	= q/m + 2
Remp	HNI	DER	LEN	nm A 😳	gcd (r	n,m) = gc	$d(m, \kappa)$	for m≠0
Prov	f÷	Suf	fices	to sh	ow that f	hr any inte	ger þ,	Why? Same set of
						N		
· · · · · ·	· · ·	þIn	and	- p]m		plm and	t plr	Common Livisors
· · · · · · ·	· · · ·	þ n	and	- p m		plm and	t plr	Common Livisors
	· · · · · · · · · · · · · · · · · · ·	þĺn	and	- þ]m		plm and	t plr	Common Livisors
	· · · · · · · · · · · · · · · · · · ·	þIn	and	- p m		plm and	t plr	Common Livisors
	· · · · · · · · · · · · · · · · · · ·	þIn	and	- þ]m		plm an	t plr	Common Livisors
	 · · · · · · ·	þIn	and	- þ]m		plm and	k plr.	Common Livisors
	· · · · · ·	þſn	and	- p m		plm and	k plr.	Common Livisors
. 	· · · · · ·	þIn	and	- þ]m		plm and	k plr.	Common Livisors

FINDING THE GCD						
Recall	division	theorem:	Unique $0 \leq \Re$.	$\leq m $ s.t. n =	= q/m + 9L	
REMAIND	DER LEI	nma :	gcd(n,m) =	gcd(m, k)	fr m≠0	
Proof :	Suffices	to show	, that far any	integer p,	Why? Same set of	
	p/n and	d þ]m	<⇒ plm	and pla	Common Livisors	
	· · · · · · · ·	· · · · · · · · · ·			\downarrow	
				ged (n.	m) = gcd(m, r)	
			· · · · · · · · · · · · · · · ·			

· · · · · · · · · ·	· · · · · ·	· · · · · ·	Find	ING T	he G	ĊD	· · · · · · ·	
Recall	divis	ion th	corem:	Unique	$0 \leq \mathcal{H}$	∠ [m]	s.t. n=	= q/lml+ 9L
REMAINI	der	Lemn	A :	gcd (m	(m) =	gcd	(m, k)	fr m≠0
Proof :	Suff	fices	to show	that for	ir any	integen	· p,	Why? Same, set of
	pIn	and	plm	$\not\models$	plm	and	plr	Common Livisors
* p m <i>∠</i>	$\Rightarrow p$	Im	· · · · · · ·	· · · · · · ·	· · · · · ·	· · · · · ·	· · · · · · ·	
		· · · · · ·					gcd(n,	m) = gcd(m, n)
· · · · · · · · · · ·	· · · · · ·	· · · · · ·	· · · · · · ·	· · · · · · ·	· · · · · ·	· · · · · ·	· · · · · · · ·	· · · · · · · · · · · · · · · · ·

FINDING THE GCD	
Recall division theorem: Unique $0 \le 9c \le r $	n s.t. $n = q/m + n$
REMAINDER LEMMA : gcd (n, m) = gc	$d(m, k)$ for $m \neq 0$
Proof: Suffices to show that fir any inte	gap, Same set of
$p n and p m \iff p m and$	d pla Common divicees
$\star \rho m \iff \rho m $	
* Linear combination $n = q/m + r$	gcd(n,m) = gcd(m,r)
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·

FINDING THE GCD	
Recall division theorem: Unique $0 \le 9c \le m $	n s.t. n = q/ m + 9L
REMAINDER LEMMA : $gcd(n,m) = gc$	$d(m, k)$ for $m \neq 0$
Proof: Suffices to show that far any integ	ger p, Same set of
pIn and pIm <> pIm and	t pla Common Livisors
$\star p m \iff p m $	
* Linear combination $n = q/m + r$	gcd(n,m) = gcd(m,r)
=> Common divisor of any two of	
n, m, n divides the third	· · · · · · · · · · · · · · · · · · ·

FINDING THE G	CD
Recall division theorem: Unique $0 \leq 9c$	$\leq m $ s.t. $n = q/ m + n$
REMAINDER LEMMA : gcd (n, m) =	$=$ gcd(m, k) for m $\neq 0$
Proof: Suffices to show that far any	integer p, Same set of
$p n$ and $p m \iff p m$	and pla Common divisors
$\star \rho m \iff \rho m $	
* Linear combination $n = q/m + r$	gcd(n,m) = gcd(m,n)
=> Common divisor of any two of	F
n, m, n divides the third	

· · · · · · · · ·	· · · · · · · · · · · · · ·	FINDING	The	GCD		· · · · · ·	
Eg.,	n = 899	m = 493	· · · · · ·	· · · · · · ·	· · · · ·	· · · · · ·	· · · · · · · · · · · · ·
· · · · · · · · ·	gcd (899, 49	3)	· · · · ·		· · · · ·	· · · · · ·	· · · · · · · · · · · ·
· · · · · · · ·				· · · · · · ·			
· · · · · · · · ·		· · · · · · · · · · · · ·	· · · · ·	· · · · · · ·	· · · · ·	· · · · · ·	· · · · · · · · · · · ·
· · · · · · · ·		· · · · · · · · · · · · ·	· · · · · ·	· · · · · · ·	· · · · ·	· · · · · ·	
	· · · · · · · · · · · · ·	· · · · · · · · · · · · ·		· · · · · · ·	· · · · ·	· · · · · ·	· · · · · · · · · · · ·
· · · · · · · ·	· · · · · · · · · · · · · · ·	· · · · · · · · · · · · ·			· · · · ·		· · · · · · · · · · · · · · ·
	· · · · · · · · · · ·						· · · · · · · · · · · ·
· · · · · · · ·	· · · · · · · · · · · ·	· · · · · · · · · · · ·		· · · · · · ·	· · · · ·	· · · · · ·	· · · · · · · · · · · ·

· · · · · · · · · · · · · · ·		FINDING	The	GCD	· · · · · ·	· · · · · ·	· · · · · · · · · ·	· ·
Eg., n=8	399 rr	n = 493	· · · · ·	· · · · · ·	· · · · · ·	· · · · · ·	· · · · · · · · · ·	•••
gcd (899, 493)		· · · · · ·	· · · · · ·	· · · · · ·	· · · · · ·		••••
= $gcd(A$	93 406)	· · · · · · · · · · ·		· · · · · ·	· · · · · ·	 	· · · · · · · · · · · · · · · · · · ·	•••
	, t ²) , t			· · · · · ·	· · · · · ·	· · · · · ·		••••
· · · · · · · · · · · · · · ·	· · · · · · ·	· · · · · · · · · · ·			· · · · · ·	 	· · · · · · · · · ·	
· · · · · · · · · · · · · · ·	· · · · · · ·	· · · · · · · · · · ·	· · · · ·	· · · · · ·	· · · · · ·	· · · · · ·	· · · · · · · · · · ·	•••
· · · · · · · · · · · · · · · ·				· · · · · ·	· · · · · ·	· · · · · ·		••••
· · · · · · · · · · · · · · ·	· · · · · · ·	· · · · · · · · · · ·			· · · · · ·	 	· · · · · · · · · ·	• •
· · · · · · · · · · · · · · · ·					· · · · · ·	· · · · · ·	· · · · · · · · · · ·	• •

· · · · · · · · · · · · · · · · · · ·	FINDING	The	GCD	· · · · ·	· · · · ·	· · · · · ·	
E_{g} , $n = 899$	n = 493	· · · · · ·	· · · · · · ·	· · · · ·	· · · · ·	· · · · · ·	· · · · · · ·
gcd (899, 493		· · · · · ·	· · · · · · ·	· · · · ·	· · · · ·	· · · · · ·	· · · · · · ·
= gcd (493, 406)	· · · · · · · · · · ·			· · · · ·	· · · · ·		
= gcd (406, 87)		· · · · · ·	· · · · · · ·	· · · · ·	· · · · ·	· · · · · ·	
· · · · · · · · · · · · · · · · · · ·		· · · · · ·	· · · · · · ·		· · · · ·	· · · · · ·	
· · · · · · · · · · · · · · · · · · ·		· · · · · ·	· · · · · · · ·	· · · · ·	· · · · ·	· · · · · ·	· · · · · · · ·
	· · · · · · · · · · · ·	· · · · · ·	· · · · · · ·	· · · · ·	· · · · ·	· · · · · ·	· · · · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · ·	· · · · · ·	· · · · · · ·	· · · · ·	· · · · ·	· · · · · ·	· · · · · · ·

· · · · · · · · · · · · · · · · · · ·	FINDING	The	GCD	· · · · ·	· · · · ·		· · · · · ·	· · · · ·
Eg., n= 899	m = 493	· · · · ·	· · · · · ·	· · · · ·	· · · · ·	· · · ·	· · · · · ·	· · · · ·
gcd (899, 4	93)	· · · ·			· · · · ·		· · · · · ·	
= gcd (493, 40k	6) · · · · · · · · · · · · · · · · · · ·	· · · · ·	· · · · · ·	· · · · ·			· · · · · ·	· · · · ·
= gcd (406, 87		· · · · ·	· · · · · ·	· · · · ·	· · · · ·		· · · · · ·	· · · · ·
= gcd (87, 58))	because	n 401	;; = ·	4x 8	7 -	+ 58	· · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · ·	· · · · ·	· · · · · ·	· · · · ·	· · · · ·		· · · · · ·	· · · ·
				• • • •				
			· · · · · ·	· · · ·			· · · · · ·	
					· · · ·			

	FINDING	The	GCD	· · · · ·		· · · · ·	· · · · ·	· · · · · ·
E_{g} , $n = 899$	m = 493	· · · · ·	· · · · · ·	· · · · ·	· · · ·	· · · · ·	· · · · ·	· · · · · ·
gcd (899	, 493)	· · · · ·	· · · · · ·	· · · · ·		· · · · ·	· · · · ·	· · · · · ·
= gcd (493,	406)	· · · · ·	· · · · · ·	· · · · ·		· · · · ·	· · · · ·	· · · · · ·
= gcd (406,	87)	· · · · ·	· · · · · ·	· · · · ·	· · · ·	· · · · ·	· · · · ·	· · · · · ·
= 9 cd (87)	58)	becaus	a 40	6 =	4x 6	37 -	+ 58	?
= gcd (50,	29)	· · · · ·	· · · · · ·	· · · · ·		· · · ·	· · · · ·	· · · · · ·
	· · · · · · · · · · · · · · · · · · ·	· · · · ·	· · · · · ·	· · · · ·		· · · · ·	· · · · ·	· · · · · ·
· · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · ·	· · · · ·	· · · · · ·	· · · · ·			· · · · ·	· · · · · ·

FINDING	The	GCD	· · · · ·		· · · · ·	
E_{g} , $n = 899$ $m = 493$	· · · · · ·	· · · · · ·	· · · ·	· · · · ·	· · · · ·	· · · · · · · · · ·
gcd (899, 493)		· · · · · ·	· · · · ·		· · · · ·	
= gcd(493, 406)	· · · · · ·	· · · · · ·	· · · · ·	· · · · ·	· · · · ·	· · · · · · · · ·
= gcd (406, 87)		· · · · · ·	· · · · ·		· · · · ·	
= gcd (87, 58)	becan	n 401	; =	4×0	7 +	- 58
= g(d(50, 29))	· · · · · ·	· · · · · ·	· · · · ·	· · · · ·	· · · · ·	
= gcd(29,0)			· · · · ·		· · · · ·	
	· · · · · ·	· · · · ·	· · · · ·	· · · · ·	· · · · ·	· · · · · · · · · ·

FINDING TI	he GCD	· · · · · · · · · ·	· · · · · · · · · · · · · · ·
899 m = 493	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · ·
(899,493)	· · · · · · · · · ·	· · · · · · · · ·	
493,406)	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · ·
(406,87)	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · · ·
(87,58) be	caner 406	$5 = 4 \times 8$	7 + 58
(50, 29)	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · · · · ·
(29,0)			· · · · · · · · · · · · · · · · · · ·
· · · · · · · · · · · · · · · · · · ·	· · · · · · · · ·	· · · · · · · · ·	· · · · · · · · · · · · · · ·
(493, 406) (406, 87) (87, 58) (50, 29) (29, 0)	caner 406	$b = 4 \times 8$	7 + 58

Euclidean Algorithm	• •
Euclidean Algorithm	
Euchdean Algorithm	
	• •
	• •
	• •
	• •
	• •
	• •
	• •
	• •
	• •
	• •
	• •
· · · · · · · · · · · · · · · · · · ·	• •
	• •

	FINDING	The	GCD	· · · · ·			· · ·	
Euchdean Ai	GORITHM					· · · ·	· · · ·	
ged (n, m)							· · · ·	
if m=0	\sim					· · · ·	· · · ·	
else n - am		· · · · ·	· · · · · ·	· · · · ·	· · · ·	· · · ·	· · ·	· · · · · · · ·
return	$gcd(m_1r)$		· · · · · ·	· · · · ·	· · · ·		· · · ·	· · · · · · ·
				· · · · ·		· · · ·	· · · ·	

FINDING THE GCD	•	•	· ·	•	• •	•	• •		• •	•	• •
FURLISEAN ALCORITHM Termination	•	•	••••	•	•••	•			• •	•	• •
	•	•	• •	•	• •	•	• •) 0) 0	• •	•	• •
g cd (n, m)	•	•	• •	•	• •	•	• •	• •	• •	•	• •
i f m = 0	•	•	• •	•	• •	•	• •	· ·	• •	•	• •
else	•	•	· ·	•	• •	•	• •		• •	•	• •
n = qm + r Concernese	•	•	· ·	•	• •	•	• •		• •	•	
return gcd (m, r)	•	•	•••	•	•••	•			•••	•	• •
	•	0	• •		• •			5 0 6 0	• •	•	

FINDING	The GCD
EUCHDEAN ALGORITHM	Terminatim At each step
ged (n, m)	* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
1f m =0	
return n	
else $n = q_m + r$	
return gcd (m, r)	Contectness
· · · · · · · · · · · · · · · · · · ·	

FINDING	The GCD
EUCLIDEAN ALGORITHM	Termination At each step
g cd (n, m)	* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
if m =10	* if $m \ge \frac{n}{2}$,
setwin n	
else $n = q_m + r$	
return gcd (m, r)	Connectness
· · · · · · · · · · · · · · · · · · ·	
· · · · · · · · · · · · · · · · · · ·	

FINDING	The GCD
EUCHDEAN ALGORITHM	Termination At each step
g cd (n, m)	* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
1f m =0	* if $m \ge \frac{n}{2}$, ged $(n, m) \longrightarrow ged (m, n-m)$
between n	
else $n = q_m + r$	
return gcd (m, r)	Correctness
· · · · · · · · · · · · · · · · · · ·	
· · · · · · · · · · · · · · · · · · ·	

FINDING	The GCD
EUCLIDEAN ALGORITHM	Terminatim At each step
g cd (n, m)	* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
1€ m =0	* if $m \ge \frac{n}{2}$, ged $(n, m) \longrightarrow ged (m, n-m)$ ged (n-m, m)
lise	
n = ym + rc return gcd (m, r)	Correctness

FINDING	The GCD
EUCLIDEAN ALGORITHM	Terminatin At each step
g cd (n, m)	* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
if m =0	* if $m \ge \frac{n}{2}$, ged $(n, m) \longrightarrow ged (m, n-m)$ ged (n-m, m)
else = am + h	
return gcd (m, n)	Conrectness

FINDING	The GCD
EUCHDEAN ALGORITHM	Termination At each step
ged (n, m)	* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
$i\rho m = 0$	* if $m \ge \frac{n}{2}$, ged $(n,m) \longrightarrow ged (m, n-m)$
return n	again, "n" is (at least) halved < n
else $n = q_m + r$	
return gcd (m, r)	

FINDING	The GCD
EUCHDEAN ALGORITHM	Terminatin At each step
g cd (n, m)	* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
j₽ m =0	* if $m \ge \frac{n}{2}$, ged $(n,m) \longrightarrow ged (m, n-m)$
return n	again, "n" is (at least) halved $< \frac{n}{2}$
else	O (log2(min(n,m))) steps
n = gm + n return gcd (m, n)	Correctness
· · · · · · · · · · · · · · · · · · ·	
· · · · · · · · · · · · · · · · · · ·	

FINDING	The GCD
EUCLIDEAN ALGORITHM	Termination At each step
ged (m, m)	* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
if m = 0	* if $m \ge \frac{n}{2}$, ged $(n, m) \longrightarrow ged (m, n-m)$ ged $(n-m, m)$
betwin n	again, "n" is (at least) halved $< \frac{n}{2}$
else $n = q_m + r$	$O\left(\log_2(\min(n,m))\right)$ steps
return gcd (m, n)	Invariant maintained by algo
	due to remainder therein

•	•	•	•				Ĺ	I c	N1	F.	A	R	•	ſ	ń	Ň	Δ	• •	M	A~	T	O	N			Y	Le		•	С.	O I	Ň	M	ີ ດ	N	Ъ	11	J	2	0	K	0	•	•	• •			
•								-						C	V	-	V	ų								-	12	•						v			•		_									
•		•		•			•	•	• •	•	•	• •	•					•	•	•	•	•	•	•	•	•	•						•	•		•	•	• •	•		•							*
•	•	•		•	•	•	•	•	• •	•	•	• •					•	•	•	•	•	•	•	•								•	•	•		•	•	• •		•	•			•	• •			1
•	•	•		•	•	•	•	•	• •	•	•	• •					•	•	•	•	•	•	•	•								•	•	•		•	•	• •		•	•			•	• •			1
•	•	•		•	•	•	•	•	• •	•	•	• •					•	•	•	•	•	•	•	•								•	•	•		•	•	• •		•	•			•	• •			1
•		•		•			•	•	• •	•	•	• •	•					•	•	•	•	•	•	•	•	•	•						•	•		•	•	• •	•		•							*
•		•	•					•	• •	•								•		•			• •	• •												•	•							•	• •		•	•
•					•	•	•	•	•									•		•			• •	• •							•						•	• •										
•		•	•				•	•	• •		•	• •							•	•	•	•	•	•										•										•				•
•	•	•		•			•	•	• •	•	•	• •						•	•	•	•	•	•	•									•			•	•	• •			•			•	• •		•	•
•		•	•		•	•	•	•	•											•			• •	• •					•		•							• •						•	• •			•
•								•	• •											•																												•
•								•	• •											•																												•
•		•	•	•	•	•	•	•	• •	•	•	• •					•	•	•	•	•	•	•	•								•	•	•	•	•	•	• •		•				•	• •		•	•
•		•	•	•	•	•	•	•	• •	•	•	• •					•	•	•	•	•	•	•	•								•	•	•	•	•	•	• •		•				•	• •		•	•
•				•			•	•	• •	•	•	• •						•	•	•	•	•	•	•									•	•		•	•	• •						•	• •		•	
•		•					•		• •	•		• •						•					•	•													•							•			•	•
•			•		•	•	•	•	•											•			• •	• •													•											•
•			•		•	•	•	•	•											•			• •	• •													•											•
			•					•	• •											•																								•				•
•		•					•	•	• •	•	•	• •						•		•	•	•	•	•											•		•	• •						•	• •	•		•
•		•					•	•	• •	•	•	• •						•		•	•	•	•	•									•		•		•	• •						•	• •	•		•
									• •																																							
									• •																																							
									• •														• •	• •																				•				
									• •														• •	• •																				•				
									• •																																							
											•										•	•																						•				

· ·	L	NEAR CO	MBINATION) v/c	Common	DIVISOR	
· ·	Greatest	Common	divisor	· · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · · ·	
· · ·	gcd	(n,m) =	largert nu	nber d	such that	d/n and	dlm.
•••							
• •							
• •							
						· · · · · · · · · · ·	
	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · · · · ·	· · · · · · ·	· · · · · · · · · ·	· · · · · · · · · · ·	· · · · · · · ·

· · ·	4	NEAR CO	MBINATION V/S COMMON DIVISOR	•
· · · ·	Greatest	Common	divicer	
· · · ·	gcd	(n,m) =	largert number d such that d/n and d/m.	•
· · · ·	Smallest	positive	integer linear combination	•
· · ·	spc (n	m) = Sm	allest positive integer d such that d=sin+tim	
· · ·	· · · · · · · ·	· · · · · · · · ·	s,t integers	•
· · ·				
• • •				

41	NEAR CO	MBINATION V/2 COMMON DIVISOR
Greatest	Commin	divisor
gcd	(n,m) =	largert number d such that d/n and d/m.
Smallest	positive	integer linear combination
sþc (n	m) = Sm	allest positive integer d such that $d = s.n + t.m$ s,t integers
	Theorem	: qcd(n,m) = spc(n,m)

LIN	iear co	MBINATION V/2 COMMON DIVISOR
Greatest	Commin	diviser
gcd (<u>n</u> (m) =	lægert number d such that d/n and d/m.
Smallest	positive	integer linear combination
spc (n,	m) = Sm	allest positive integer d such that d=sin+tim
· · · · · · · · · · · · · · · · · · ·		s,t integers
· · · · · · · · · · ·	Theorem	gcd(n,m) = spc(n,m)
gcd is	the sm	allest positive number that can be constructed by taking linear combinations.

LINEAR COMBINATION V/S COMMON DIVISOR
Greatest common divisor
gcd(n,m) = largert number d such that d/n and d/m .
Smallest positive integer linear combination
spc(n,m) = smallest positive integer d such that $d = s.n + t.ms,t integers$
Theorem : $gcd(n,m) = spc(n,m)$
Corollery: Any multiple of gcd (n,m) is a linear combination of n and m and vice versa.