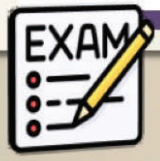
DIVISIBILITY
MODULAR ARITHMETIC

Properties of Integers

Topics for the MIDTERM

Weeks 1-2 Logic and Proof	Weeks 3-5 Sets and Counting	Weeks 6-8 Properties of Integers
Propositions & Logical Operators Rules of Inference and Validity Mathematical Induction	Sets, Operations on Sets PIE, Sum and Product Rules Counting and Combinatorics	Divisibility and Modulo Binary and Base Arithmetic Applications in Cryptography



Closed book, default calculator, scratch paper
In a lab, similar to MyCourses, no internet, no phone/iPad

Score and evaluation: **quiz 30% + exams 70%**

Learning objectives! Know what you will learn today

Self-Reflection! Rate levels of your understanding

❍ Checklist of key topics. Keep catching up with the course.

- ☐ Divisibility, modular arithmetic, cyclicity of remainders
- ☐ Applications of modular arithmetic in cryptography – Caesar (shift) cipher
- ☐ Prime numbers and prime factorization
- ☐ The greatest common divisor GCD and the least common multiple LCM
- ☐ Problem solving involving properties of integers: mod, primes, GCD, LCM

Confident	Got it	Okay	Fuzzy	Not a clue

Fractions – Terminology and Vocabulary

a rational number

$\frac{245}{3}$ ← numerator

← denominator

$a = k \times b + r$

$245 = 81 \times 3 + 2$

dividend quotient divisor remainder

$$\begin{array}{r} 81 \text{ r } 2 \\ 3\overline{)\,245} \end{array}$$

$245 \div 3 = 81 \text{ r } 2$

$$a = k \times b + r$$

Dividend $a \in \mathbb{Z}$	Divisor $b \in \mathbb{Z}^+$	Quotient $k \in \mathbb{Z}$	Remainder $r \in \mathbb{N}$ and $0 \leq r < b$
245	3		
41	8		
-99	11		
2	10		
-17	7		

Modulo function $a/b \Rightarrow a = k \times b + r$

- The **quotient k** is commonly referred to as the integer part of the division. It is what is returned in an **integer division** operation.
- The **modulo** or **mod-n** function returns the **remainder r** when **a** is divided by **b**. Ex. 12 mod 9 = 3 and 245 mod 81 = 2.
- If **r=0** then **a** is a **multiple of b**, or **b divides a**, written $b \mid a$, otherwise $b \nmid a$

Common usage in programming ⇒ quotient or integer division → **k = a / b**
remainder or mod n function → **r = a % b**

WORKED EXAMPLES

- Calculate the following modulo
  - 7558 mod 63
  - 7562 mod 63
  - -7558 mod 63
  - $(2^{32} \times 4^{32})$ mod 19

WORKED EXAMPLES

- What is (2500 + 1555 + 222 + 4) mod 5 ?

$$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

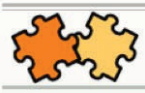
WORKED EXAMPLES

- What is $(12 \times 13 \times 29 \times 69) \bmod 11$?

$$(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$$

WORKED EXAMPLES

- What is the remainder when 1! + 2! + 3! ... + 49! is divided by 20?



PRACTICE PROBLEMS

- Without a calculator, calculate the following:
  - (123 + 234 + 32 + 56 + 22) mod 3
  - (1594 × (−117) × 475) mod 6
  - ((−907) × 17 × (−276)) mod 15
  - (43534569812031 × 12903958235485) mod 2

PRACTICE PROBLEMS

- What is the remainder when 1! + 2! + 3! … 100! is divided by 18?
- If the remainder is 7 when positive integer n is divided by 18, what is the remainder when n is divided by 6?

PRACTICE PROBLEMS

- Using the 12-hour clock format, the current time is 4 o'clock, what time will it be 101 hours from now?

- Given that February 14, 2018, is a Wednesday, what day of the week will February 14, 2090 be? Hint: take into account leap years.

Modular arithmetic and cyclicity of remainders

- Calculate 2^{98765} mod 10.

k	2^k	2^k mod 10	
0			
1			
2			
3			
4			
5			
6			
7			
8			
9			

WORKED EXAMPLES

- Calculate 7^{358} mod 10.

k	7^k	7^k mod 10	
0			
1			
2			
3			
4			
5			
6			
7			
8			
9			

Modular arithmetic and cyclicity of remainders

- Calculate 7^{358} mod 10.
- What is the ones digit of 7^{358} ?

Same question, asking differently!

Billions	Hundred Millions	Ten Millions	Millions	Hundred Thousands	Ten Thousands	Thousands	Hundreds	Tens	Ones	Tenths	Hundredths	Thousandths	Ten Thousandths	Hundred Thousandths	Millionths
6	7	8	1	2	3	9	4	6	5	.	7	2	4	0	6	9

Decimal Point

k	7^k	7^k mod 10	
0	1		
1	7		
2	49		
3	343		
4	2,401		
5	16,807		
6	117,649		
7	823,543		
8			
9			

Modular arithmetic and cyclicity of remainders

Base number ending with	Powers: seq of ones digit	Period of the cycle
0	0	1
1	1	1
2	2 4 8 6	4
3	3 9 7 1	4
4	4 6	2
5	5	1
6	6	1
7	7 9 3 1	4
8	8 4 2 6	4
9	9 1	2

- **Cycling** of digits is applied for the ones and the tens digits, and a few other pairs of base & mod.

finding remainders of large numbers
ones digit → mod 10

- When solving problems: try it and see if the **pattern** emerges, then use modulo to find the answer

Modular arithmetic and cyclicity of remainders

Base number ending with	Powers: seq of tens digit	Period of the cycle
0	0	1
1	0	1
2	...	20
3	...	20
4	...	10
5	2	1
6	3 1 9 7 5	5
7	0 0 4 4	4
8	...	20
9	...	10

- Know how to answer questions:

Asking for a units or a tens digit
→ answer: a single digit 0-9

Asking for mod 100
→ find both tens and units digit
→ answer: a two-digit number

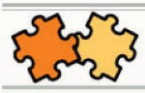
WORKED EXAMPLES

- What is the tens digits of 7^{358} ?

k	7^k		
0			
1			
2			
3			
4			
5			
6			
7			
8			
9			

WORKED EXAMPLES

- Calculate 7^{355} mod 100.



PRACTICE PROBLEMS

- Find the tens digits of $6^{2345789}$

PRACTICE PROBLEMS

- Calculate 4^{1000} mod 10.

PRACTICE PROBLEMS

It does not have to always be mod 10 or mod 100

- What is the remainder when 4^{1000} is divided by 7?

modulo of 7

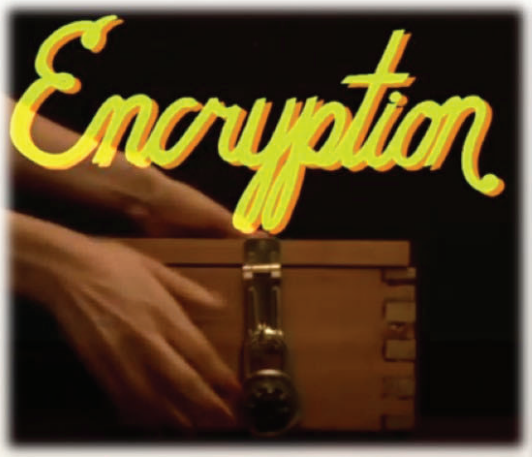
Hint: find a cyclic pattern of modulo 7 of powers of 4

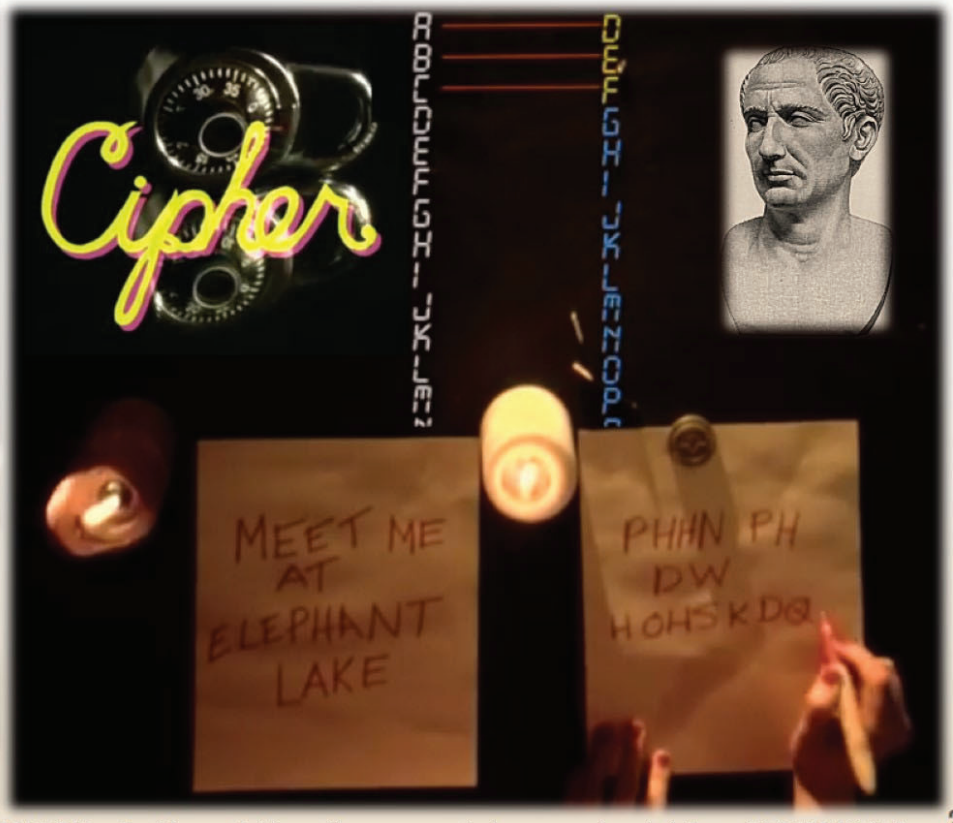
PRACTICE PROBLEMS

It does not have to always be mod 10 or mod 100

- Calculate 7^{5140} mod 4.

Hint: find a cyclic pattern of modulo 4 of powers of 7

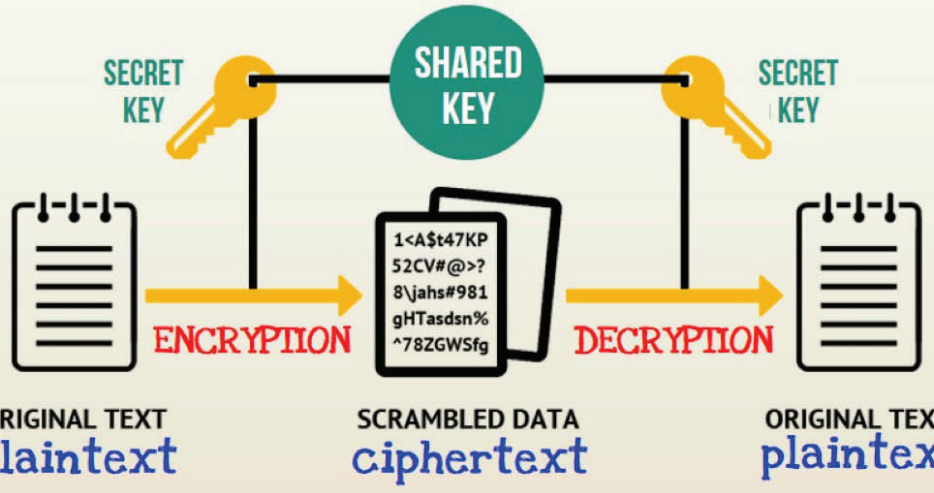




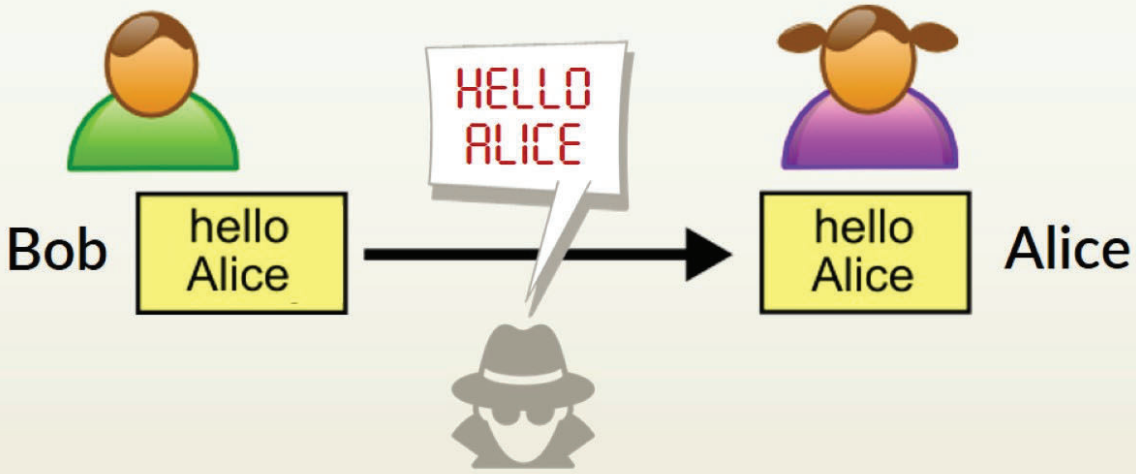
https://www.youtube.com/watch?v=Kf9KjCKmDcU https://www.youtube.com/watch?v=sMOZf4GN3oc

An application of Modular Arithmetic in Cryptography

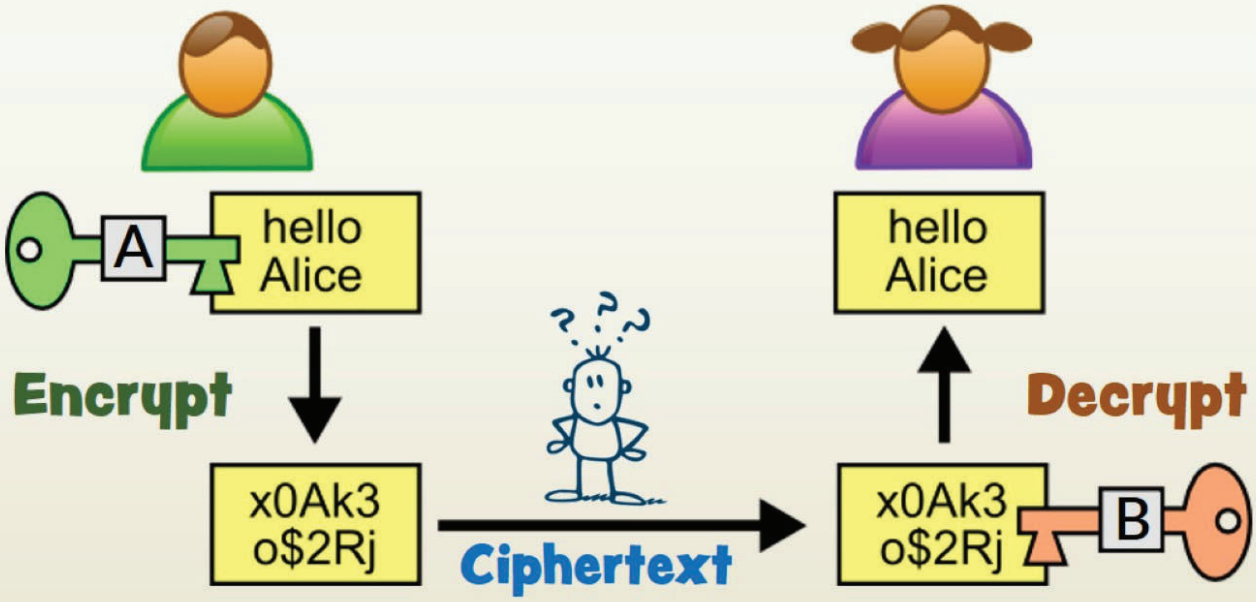
Encryption scrambles readable text so it can only be read by a person who has the secret key and knows which algorithm is implemented. Encryption and decryption help provide data security for sensitive information.



In plaintext, an intruder can always read your secret conversation



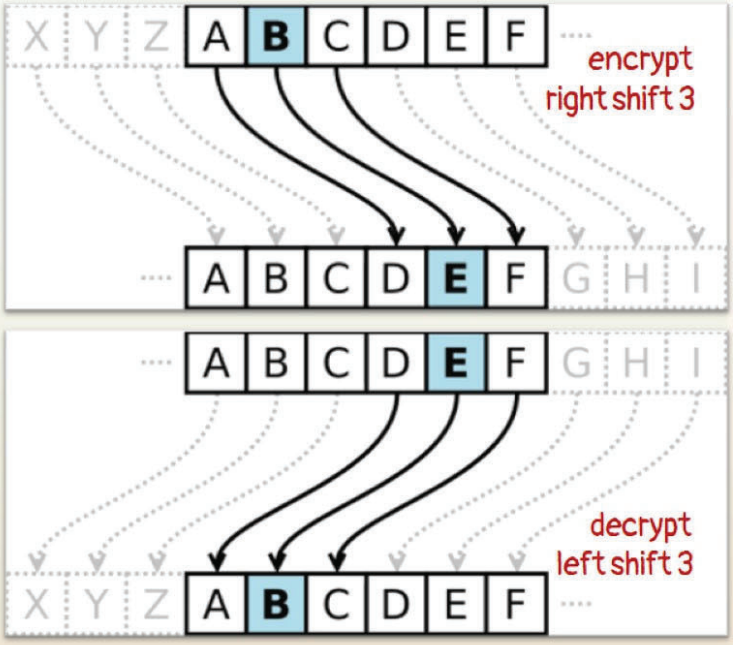
An intruder may catch your encrypted message but not able to read it



Caesar Cipher, also called Caesar shift or shift cipher

- Caesar cipher hides (***encrypts***) a message by moving each letter a certain number (***a shifted key***) of places to the right along the sorted list of alphabets A-Z

- Each letter in the original plaintext is replaced with a different letter that is **a fixed right-shift** of the alphabets A–Z



https://www.youtube.com/watch?v=BdI2whtMyzU

WORKED EXAMPLES

- Using Caesar Cipher with key=7, encrypt the word **FOX**

- Using Caesar Cipher with key=7, decrypt the word **THW**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

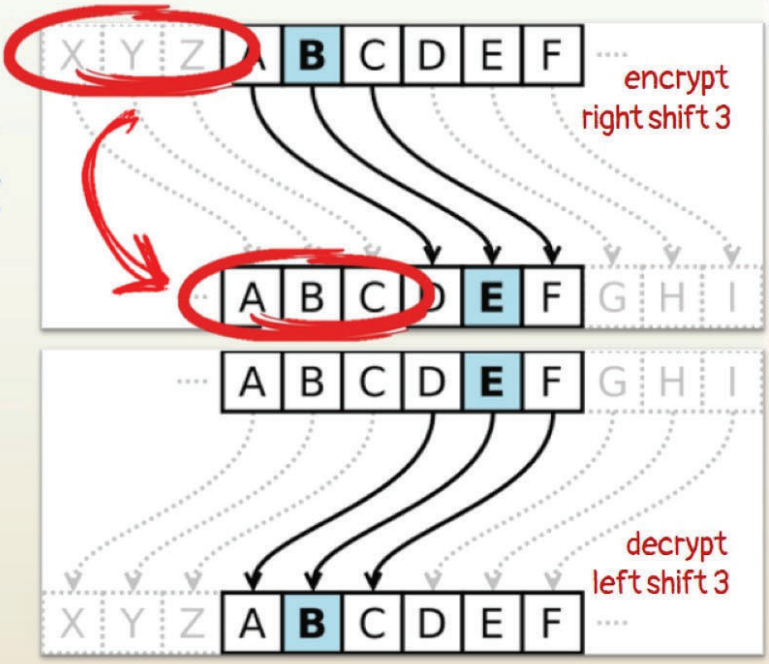
The role of modular arithmetic in Caesar Cipher

When shifted, an alphabet **wraps around** to the first letter A upon reaching the last letter Z

ENCRYPT: $e_k(x) = (x + k) \bmod 26$

DECRYPT: $d_k(x) = (x - k) \bmod 26$

A right rotation of 3 places is equivalent to a left shift of 23



https://www.secplicity.org/2017/05/25/historical-cryptography-ciphers/

Caesar Cipher

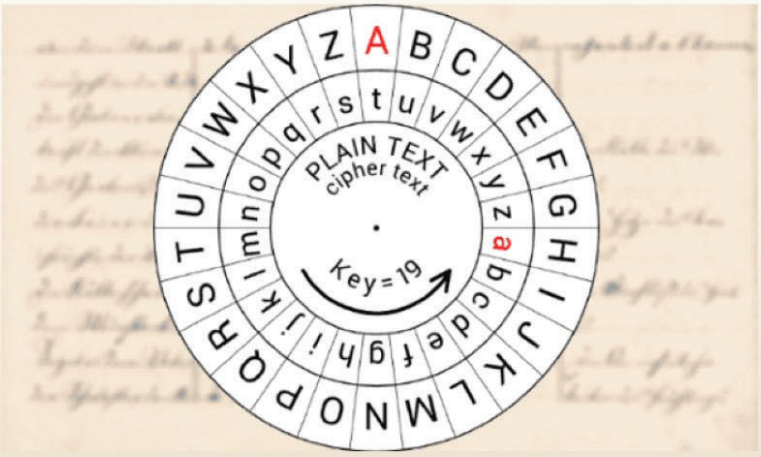
- Map 26 letters of English alphabet to numbers: A=0, B=1, ..., Z=25
- Sender: encrypt each letter x in a message: $e_k(x) = (x + k) \bmod 26$
- Receiver: decrypt each letter x in a message: $d_k(x) = (x - k) \bmod 26$

key=18 M A T H

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Codebreaker

Given a ciphertext encoded using Caesar Cipher encryption, you do not know the key to decrypt it. But, can you crack it?



Cracking the Caesar Cipher

- Use frequency analysis – the most common letters in the ciphertext are related to the most common letters in the plaintext (in the language)
- Look at one-, two-, or three-letter words, e.g., in English, a single letter word in ciphertext is likely to be an encryption of "a" or "I" in plaintext

Can you crack this? What encryption key was used?

TRVJRI TZGYVIJ RIV HLZKV VRJP KF TIRTB

PRACTICE PROBLEMS

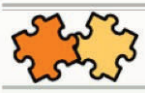
- With key=13, encrypt a message: TREATY IMPOSSIBLE

- With key=4, decrypt a message: GSQTYXIV WGMIRGI

PRACTICE PROBLEMS

- With key=444, encrypt a message: GREGORIAN CALENDARS

- The ciphertext "KBKXEUTK" is the result of encrypting the word "EVERYONE" using Caesar Cipher with the key equals to ____



PRACTICE PROBLEMS

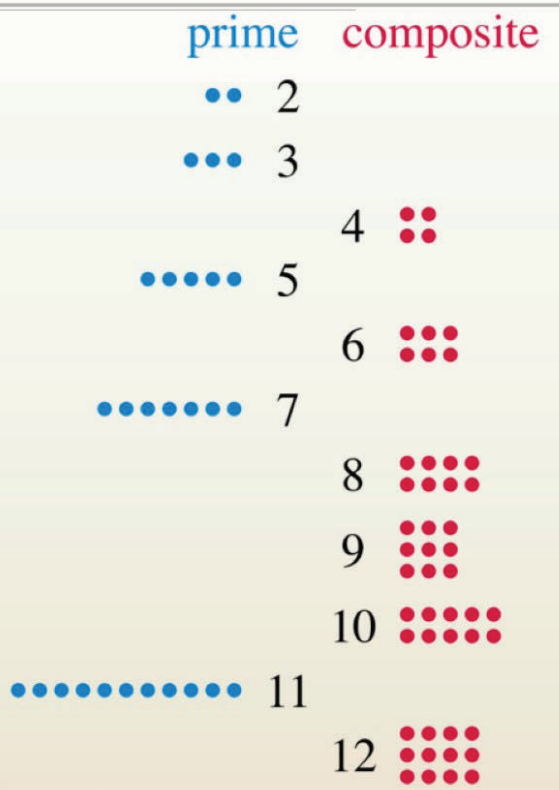
- Traditionally, the alphabets in the Caesar Cipher consists of 26 English letters 'A' through 'Z'. In an extended cipher, digits '0' through '9' are included and ordered after the English letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789. In this extended version, perform the following encryption.
- Encrypt `IC0S32T` with key `8`
- Decrypt `0X22B058` with key `23`

PRIME FACTORIZATION GCD AND LCM

Properties of Integers

Prime Numbers

- **Prime number** is a natural number greater than 1 that has no positive divisors other than 1 and itself
- The only positive integers that divide a prime number p are 1 and p
- A natural number greater than one that is not a prime number is called a **composite number**



https://en.wikipedia.org/wiki/Prime_number

Factoring a number into its primes

- Divide by primes: 2, 3, 5, 7, …
- Continue until you get to 1
- Write down the products of all prime divisors

1386 =

	1386

Every positive integer n > 1 can be broken into multiples of primes

$n = p_1^{k1} p_2^{k2} p_3^{k3} \ldots p_s^{ks}$ where $p_1 < p_2 < p_3 < \ldots < p_s$ are prime numbers

Factoring a number into its primes

- Keep dividing the number by a prime
- Stop when you get to 1

140 =

Every positive integer n > 1 can be broken into multiples of primes

$n = p_1^{k1} p_2^{k2} p_3^{k3} \ldots p_s^{ks}$ where $p_1 < p_2 < p_3 < \ldots < p_s$ are prime numbers

WORKED EXAMPLES

Write each integer as a product of powers of primes

- 75 =
- 512 =
- 3038 =
- 3401 =

WORKED EXAMPLES

- Find the largest prime divisor of 5! + 6!

- Find the largest prime divisor of $2^{16} - 1$

PRACTICE PROBLEMS

Write each integer as a product of powers of primes

- 107 =
- 589 =
- 828 =
- 1781 =

PRACTICE PROBLEMS

- Find the prime factorization of 10!

- There are 9 six-digit natural numbers with the property that all of their digits are the same (111111, 222222, ..., 999999). Find the largest prime number that is a divisor of all of them.

GCD Greatest Common Divisor

HCF – Highest Common Factor

The largest int that is a common divisor of a given set of numbers. It divides all integers in the set.

Factors of 15: 1, 3, 5, and 15

Factors of 20: 1, 2, 4, 5, 10, and 20

The GCD of 15 and 20 is 5

LCM Least Common Multiple

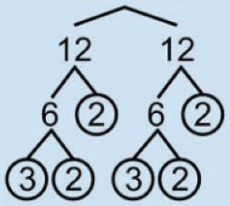
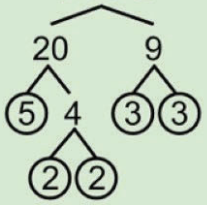
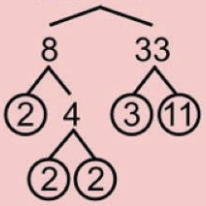
The smallest multiple that two or more numbers have in common. It is a multiple of all int in the set.

Multiples of 15: 15, 30, 45, 60, ...

Multiples of 20: 20, 40, 60, 80, ...

The LCM of 15 and 20 is 60

Recall & Review Your GCM & LCM!

144	180	264
		
$144 = 2^4 \cdot 3^2$	$180 = 2^2 \cdot 3^2 \cdot 5$	$264 = 2^3 \cdot 3 \cdot 11$

SCALAR LEARNING www.ScalarLearning.com

$$GCF = 2^2 \cdot 3 = 12$$

$$LCM = 2^4 \cdot 3^2 \cdot 5 \cdot 11 = 7920$$

2	48 , 72 , 108
2	24 , 36 , 54
3	12 , 18 , 27
3	4 , 6 , 9
2	4 , 2 , 3
	2 , 1 , 3

$GCD = 2 \times 2 \times 3 = 12$

$LCM = 2 \times 2 \times 3 \times 3 \times 2 \times 2 \times 1 \times 3 = 432$

Using prime factors to find GCD and LCM

GCD – Greatest Common Divisor

$540 = 2^2 \times 3^3 \times 5$

$504 = 2^3 \times 3^2 \times 7$

Product of common **min**-power

LCM – Least Common Multiple

$540 = 2^2 \times 3^3 \times 5$

$504 = 2^3 \times 3^2 \times 7$

Product of every **max**-power

$$GCD(a,b) \times LCM(a,b) = ab$$

PRACTICE PROBLEMS

- Find the GCD and LCM of 27, 90, and 84

WORKED EXAMPLES

- The GCD of 70 and some $n \in N$ is 10. Their LCM is 210. Find n.

WORKED EXAMPLES

- The LCM of two numbers is six times their GCD. The sum of the LCM and the GCD is 210. If one number is 60, then what is the other?

PRACTICE PROBLEMS

- The LCM of two numbers is 174. Their GCD is 29. The numbers are in a ratio 1:6. What is the largest number amongst the two?

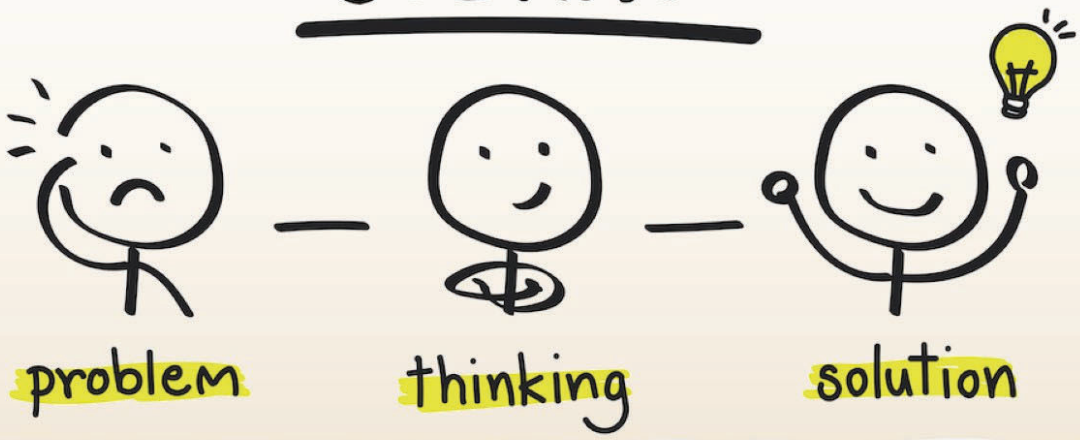
PRACTICE PROBLEMS

- The sum and the difference between LCM and GCD of two numbers are 369 and 351, respectively. If one number is 72, find the other number.

PRACTICE PROBLEMS

- Find the least number, which is a multiple of 11 and when divided by 3, 5 and 9 leaves 2 as remainder.

PROBLEM SOLVING



Divisibility & Primes AND PIE & Counting

PRACTICE PROBLEMS

- How many positive integers less than 1001 are multiples of either 6 or 8, but not both at once?

PRACTICE PROBLEMS

$U = \{1, 2, 3, ..., 1689\}$, $A = \{x \mid x \in U \text{ and } 3 \mid x\}$, $B = \{y \mid y \in U \text{ and } 5 \mid y\}$, and $C = \{z \mid z \in U \text{ and } 11 \mid z\}$. Compute each of the following.

- $|A| =$
- $|B| =$
- $|C| =$
- $|A \cup B| =$
- $|A \cup B \cup C| =$

Ch1.4, Q.38,40

PRACTICE PROBLEMS

How many positive divisors does $2000 = 2^4 5^3$ have?

PRACTICE PROBLEMS

- How many positive divisors does 6! have?

Hint: prime factorization and counting (product rule)

What's next?