MA 111, Topic 2: Cryptography

Our next topic is something called **Cryptography**, the mathematics of making and breaking **Codes**! In the most general sense, **Cryptography** is the mathematical ideas behind changing a message that is written plainly in some language (usually English) to make it appear unreadable to everyone except the intended recipient. In this chapter we will discuss several different ways of doing this.

Definition 1. The process of changing the message from readable to unreadable is called **Encryption**. This process often requires using something called a **Encryption Key**.

Somehow the intended recipient must read the message. They will have to perform a **Decryption** before the message will be readable.

Definition 2. Decryption is the process of changing from unreadable back to readable. This process is designed to use something called a **Decryption Key**.

Before we start encrypting and decrypting we will need to learn something called *modular arithmetic*. Modular arithmetic is a new type of adding and multiplying for integers where integers "wrap around" upon reaching a certain number called the modulus. Usually for us we will be working mod 26 since there are 26 letters in the alphabet.

$\boxed{\text{Long Division Remainder}}$

Consider the long division problem

$$5\overline{)\,42\quad}$$

We have

$$\begin{array}{r} 8 \text{ R } 2 \\ 5\ \overline{)\,42\quad} \end{array}$$

This means that $42 = 8 \times 5 + 2$

Definition 3. The number 8 is called the **quotient**. The number 2 is called the **remainder**.

We will not be using the quotient in MA111. The remainder however will be very important for us.

Finding Remainders, Method 1

Here is a procedure for using your calculator to find the remainder of $n\overline{)\,a\quad}$.

This procedure works when a is not negative.

(1.) Is a less than n? If yes, then **STOP**! a is the remainder! If no, go on to the next step.

(2.) Replace a by $a - n$. Now consider $a - n$ as a new value.

(3.) Is $a - n$ less than n? If yes, then **STOP**. If not, go back to step (2.) and subtract n again. In symbols this means now consider $a - n - n = a - 2n$ now.

Repeat Steps (2.) and (3.) as many times as necessary until you reach the first value that is less than n.

Example 4 (Drill Time: Remainders from Long Division)**.** Get some practice finding remainders. Use your calculator (if you want)).

- Find the remainder for $5\overline{)\,87\quad}$.

- Find the remainder for $7\overline{)\,92\quad}$.

- Find the remainder for $13\overline{)\,111\quad}$.

- Find the remainder for $26\overline{)\,185\quad}$.

Finding Remainders, Method 2 (Quick)

Here is a *QUICK* procedure for finding the remainder of $n\overline{)\,a\quad}$.

This procedure works when a is is not negative.

(1.) Divide a by n. If the result is a whole number <u>without</u> a decimal then **STOP**. The remainder is 0!

If the result has a decimal, go to step (2.)

(2.) Remove the number that precedes the decimal. Do this by subtracting the preceding value in your calculator. This should give you only a *decimal amount*.

(3.) Multiply this *decimal amount* by n. Usually this gives a whole number (no decimal). Sometimes, because of round-off error, your calculator gives a decimal number that is really close to a whole number. Use normal rounding conventions to find the best whole number (no decimal) b. The remainder is b!

Example 5 (Drill Time: Quick Remainders from Long Division)**.** You should definitely use a calculator to do the following! Try to use the "Quick" method (Method 2) for finding each remainder.

- Find the remainder for $3\overline{)\,400\quad}$.

- Find the remainder for $13\overline{)\,400\quad}$.

- Find the remainder for $23\overline{)\,400\quad}$.

- Find the remainder for $33\overline{)\,400\quad}$.

Modular Arithmetic

It will be best to use alternate language to talk about remainders.

Definition 6. We say a **is equal to** b **modulo** n and write $a = b(\text{mod } n)$ or $a(\text{mod } n) = b(\text{mod } n)$ to mean that

$$n\overline{)\,a\quad}$$

produces a quotient q (which we ignore) and a remainder b (which we want). That is

$$n\ \overset{q\ \mathrm{R}\ b}{\overline{)\,a\quad}}$$

We write $a = 0(\text{mod } n)$ if n divides (no remainder) into a.

We write $a = 1(\text{mod } n)$ if n divided into a gives a remainder of 1.

We write $a = 2(\text{mod } n)$ if n divided into a gives a remainder of 2.

$\vdots$

This is a simple mathematical idea to describe but it still takes some practice. Amazingly, this simple idea is the basis for many different types of codes, both ancient and modern.

Related Idea: Simplifying Positive Mods, Method 1

Often our code calculations will produce unsimplified modular arithmetic answers. By *simplified* we mean that $a(\text{mod } n)$ is written so that a is between 0 and $n-1$; in symbols $0 \leq a < n$.

Here is a procedure for simplifying $a(\text{mod } n)$ when a is positive.

(1.) Is a less than n? If yes, then **STOP**! $a(\text{mod } n)$ is already simplified. If no, go on to the next step.

(2.) If $a(\text{mod } n)$ is not simplified and a is positive, replace a by $a - n$. In symbols this means

$$a(\text{mod } n) = a - n(\text{mod } n).$$

So $a - n$ is the new value for us to consider.

(3.) Is this new value simplified? If yes, then **STOP**. If not, go back to step (2.) and subtract n again. In symbols this means

$$a - n(\text{mod } n) = a - 2n(\text{mod } n).$$

Repeat Steps (2.) and (3.) as many times as necessary until you reach a simplified value.

Example 7 (Drill Time: Simplifying Mods)**.** Get some practice simplifying the following modular arithmetic! Use your calculator (if you want).

- Simplify 45(mod 26).

- Simplify 19(mod 26).

- Simplify 37(mod 20).

- Simplify 14(mod 16).

- Simplify 53(mod 26).

- Simplify $100 (\mathrm{mod}\ 20)$.

Related Idea: Simplifying Positives, Method 2 (Quick)

Here is the *QUICK* procedure for simplifying positive $a(\mathrm{mod}\ n)$

(1.) If $a(\mathrm{mod}\ n)$ is not simplified, divide a by n. If the result is a number without a decimal then **STOP**. $a(\mathrm{mod}\ n)$ simplifies as

$$0(\mathrm{mod}\ n).$$

If the result has a decimal, go to step (2.)

(2.) Remove the number that precedes the decimal. Do this by subtracting the preceding value in your calculator. This should give you only a *decimal amount*.

(3.) Multiply this *decimal amount* by n. Usually this gives an exact number (no decimal) b. Sometimes, because of round-off error, your calculator gives a decimal number that is really close to an exact number. Use normal rounding conventions to find an exact number (no decimal) b. This is your answer

$$a = b(\mathrm{mod}\ n).$$

Example 8 (Drill Time: Quick Simplifying)**.** You should definitely use a calculator to do the following! Try to use the "Quick" method (Method 2) for simplifying each.

- Simplify $103 (\mathrm{mod}\ 100)$.

- Simplify $103 (\mathrm{mod}\ 25)$.

- Simplify $145(\text{mod } 26)$.

- Simplify $237(\text{mod } 20)$.

- Simplify $353(\text{mod } 26)$.

- Simplify $400(\text{mod } 20)$.

Modular Arithmetic Exponent Law 1

Definition 9 (Modular Arithmetic Exponent Law)**.** Applying exponents in modular arithmetic can be done before or after simplifying! In symbols this says that

$$a^k(\text{mod } n) = (a(\text{mod } n))^k$$

for any integer exponent k.

If we apply the exponent after simplifying, we may need to simplify again!

Example 10 (Modular Arithmetic Exponent Law 1)**.** Here are a couple of examples that illustrate the above law.

- For $6^2(\text{mod } 4)$ we can calculate that $6^2(\text{mod } 4) = 36(\text{mod } 4)$, then simplify to find $36(\text{mod } 4) = 0$.
- Or we can use our exponent law first, then simplify: $6^2(\text{mod } 4) = (6(\text{mod } 4))^2 = (2(\text{mod } 4))^2 = 4(\text{mod } 4) = 0$.

Modular Arithmetic Exponent Law 2

Definition 11 (Modular Arithmetic Exponent Law 2)**.** When an exponent calculation is too big for a calculator to handle we have to break the process into smaller pieces using the following exponent law. If ℓ is a big exponent, then write $\ell = k + j$ for two smaller numbers k and j. We can simplify as

$$a^{\ell} (\text{mod } n) = a^{k} (\text{mod } n) \cdot a^{j} (\text{mod } n)$$

Example 12 (Modular Arithmetic Exponent Law 2)**.** Here is an example that illustrate the above law.

- The calculation $23^{14}(\text{mod } 4)$ can be broken up into smaller calculations using the fact that $14 = 7 + 7$.
- Since $23^{7}(\text{mod } 4) = 3404825447(\text{mod } 4) = 3(\text{mod } 4)$ our exponent law says

$$23^{14}(\text{mod } 4) = 23^{7}(\text{mod } 4) \cdot 23^{7}(\text{mod } 4) = 3(\text{mod } 4) \cdot 3(\text{mod } 4).$$

Related Idea: Large # Modular Arithmetic

Example 13 (Large # Modular Arithmetic)**.** Let's compute $8^{29}(\text{mod } 41)$. Even expensive graphing calculators will return an answer that is rounded off.

(1) We need to find an exponent $8^{k}(\text{mod } 41)$ that our calculator *CAN* handle. Smaller calculation we can make (using Method 2) are $8^{9}(\text{mod } 41) = 5$ and $8^{10}(\text{mod } 41) = 40$.

(2) Now break up the big exponent into smaller ones using the previous step. To calculate $8^{29}(\text{mod } 41)$, we will think of 29 as

$$29 = 10 + 10 + 9.$$

(3) The big exponent can be calculated using the pieces from the previous step. Here it turns out that

$$8^{29}(\text{mod } 41) = 8^{10}(\text{mod } 41) \cdot 8^{10}(\text{mod } 41) \cdot 8^{9}(\text{mod } 41).$$

Example 14 (Drill Time: Exponents 1)**.** Use the exponent laws to simplify these. Check your answers with your neighbor(s)!

- If $11^6 \pmod 4 = 1$, what is $11^{12} \pmod 4$?

- For $20^{15} \pmod{13}$, what is a good way to break up the exponent $\ell = 15$?

- Suppose $23^7 \pmod 4 = 3$. Find $23^{21} \pmod 4$.

Example 15 (Drill Time: Exponents 2)**.** Use the exponent laws to simplify these.

- Simplify $7^2 \pmod{20}$.

- Use your answer above to *QUICKLY* find $7^6 \pmod{20}$.

- Can you use your <u>two</u> answers above to find $7^{14} \pmod{20}$?

Related Idea: Cryptography Notation

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Definition 16 (Plaintext $\square$ and Ciphertext $\boxtimes$)**.** We use the word **Plaintext** to describe unencrypted/decrypted, readable English. To describe numbers associated to plaintext, we use the following symbol: $\square$
We use the word **Ciphertext** to describe encrypted, unreadable language.

To describe numbers associated to ciphertext, we use the following symbol: $\boxtimes$

Example 17 (Plaintext $\square$ and Ciphertext $\boxtimes$)**.** For example, the plaintext message "I" would have $\square = 9$.

We could encrypt this as the ciphertext "T", meaning $\boxtimes = 20$.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 18 (Congratulations! You Are Now A Spy 1)**.** Your first mission is to intercept and decipher enemy communications. The enemy is known to use a relatively simple encryption methods.
Enemy agents are after one of several (code named) targets:

DOG, MAN, BOY, DAD, MOM, BIT, BOT

- If you intercept the message "PRP", what is the target?

- Using the enemy agent's method above, how would the word "ZOD" be sent?

Encryption Method: Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Definition 19. The Caesar Cipher is a code that encrypts a letter by moving 3 units to the right (with alphabetic order). For the letters A–W this code can be described using the rule

$$\square + 3 = \boxtimes.$$

The letters X, Y, and Z (respectively) are encrypted as A, B, and C (respectively).
Encryption for the Caesar Cipher can be described completely using modular arithmetic as

$$\square + 3(\text{mod } 26) = \boxtimes.$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 20 (Hail Caesar 1)**.** Gaius Julius Caesar has been surrounded during the battle of Alesia! He needs you to respond to two questions posed by one of his Lieutenants. Unfortunately, those filthy Gauls are everywhere!

You will need to encrypt Caesar's answers:

- Question: What do you need?

  Caesar's Answer: WATER

- Question: Do we attack tomorrow?
  Caesar's Answer: YES

Example 21 (Hail Caesar 2)**.** You return to Caesar with a message from a Lieutenant.

- The message gives the time of the next attack. It is encrypted as the following:

  GDZQ

  When is the next attack?

- Like all Romans, Caesar is extremely superstitious and avoids making actions on the left. If you were to decrypt the message above *by only moving to the right*, how much would you have to move by?

Decryption Method: Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Definition 22. A Caesar Cipher can be decrypted by moving 3 units to the left (against alphabetic order). For the letters A, B, C this decryption can be described using the rule

$$\boxtimes + 23 = \square.$$

Technically, the letters D–Z are decrypted by wrapping back around the alphabet.
Decryption for the Caesar Cipher can be described completely using modular arithmetic as

$$\boxtimes + 23 (\text{mod } 26) = \square.$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 23 (Hail Caesar 3)**.** One last exchange message before the attack:

- Caesar asks you to encrypt and deliver the following message:

  FORTUNA

- You return with the following encrypted message. Decrypt it for Caesar:

  YLFWRULD

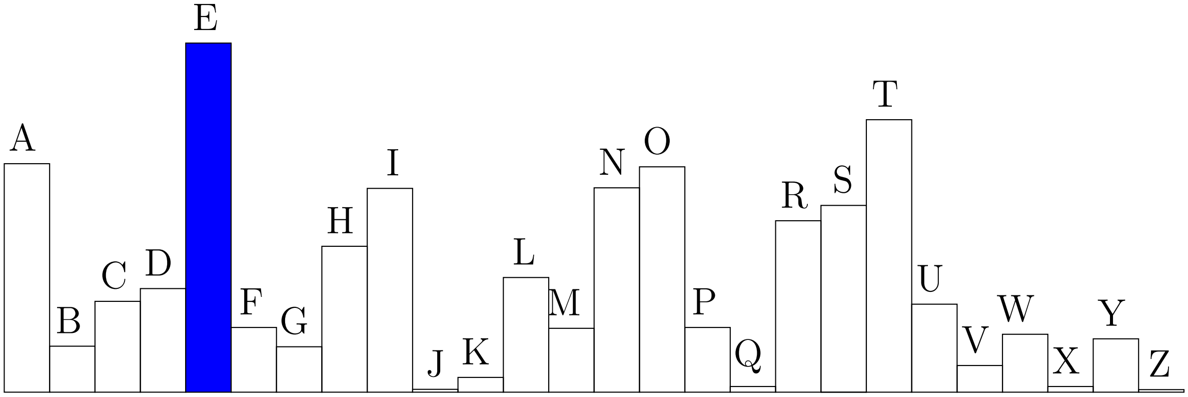
Code Summary: Caesar Cipher

We will talk about several different types of codes during the next few weeks and it will be good to keep a summary for each. The ideas behind **Encryption Key** and **Decryption Key** for the Caesar Cipher will be applicable to all codes. Additionally **Key Secrecy**, the idea for how secret the decryption key must be, and **Letter Frequency**, or how much a cipher changes the nature of how often letters appear, will become increasingly important. The summary below represents information about codes when encrypting and decrypting English language plaintext.

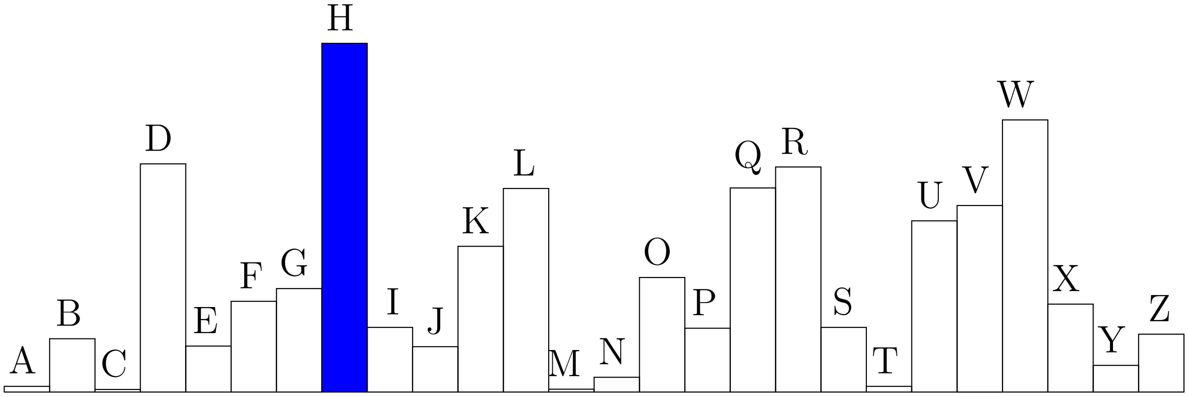
Cipher	Encrypt Key(s)	Decrypt Key(s)	Key Secrecy	Letter Frequency
Caesar	3	23	Private	Normal

Related Idea: Frequency Analysis

Anyone who has watched *Wheel of Fortune* or played *Scrabble* knows that the English language uses some letters more frequently than others.



Some codes do not hide the natural frequency of letters. The Caesar Cipher disguises letters, but does not disguise the natural frequency of letters!



The most frequent symbol used in the ciphertext will correspond to the letter "E" in the plaintext. For the Caesar Cipher, this corresponds to the numeric $5 + 3$ and is the ciphertext letter "H".

Encryption Method: Shift Cipher

Definition 24. An English Language **Shift Cipher** using the **shift** Δ moves every letter of the alphabet Δ places to the right. The conversion from English plaintext $\square$ to ciphertext $\boxtimes$ is represented by the formula

$$\square + \Delta \pmod{26} = \boxtimes.$$

So the Caesar Cipher is just a type of Shift Cipher, but with the specific value of $\Delta = 3$.

Allowing for more values for the shift Δ means more options and makes for a code that is more challenging to break!

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

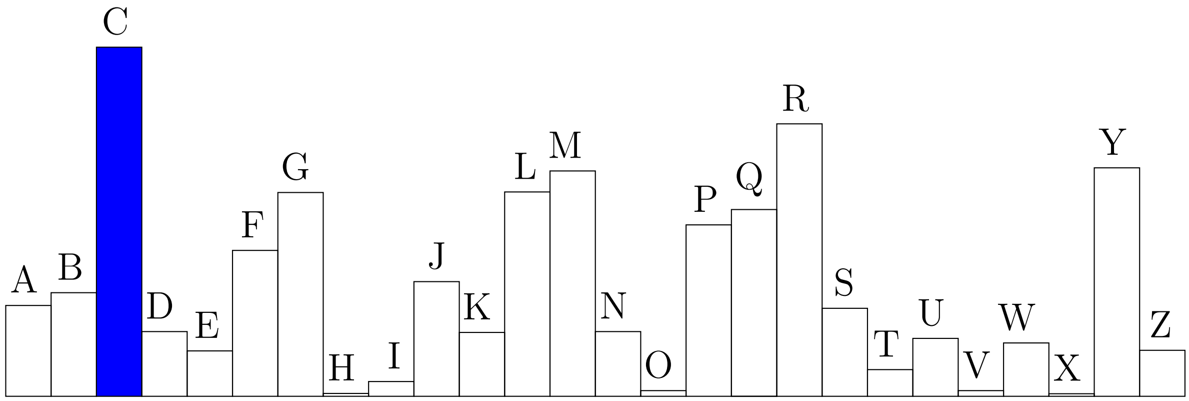
Example 25 (Hail Caesar 4)**.** The attack was a success and the Gauls are now on the run! Unfortunately, they managed to capture a messenger who knows Caesar's secrets for encryption and decryption. Caesar decides to try something new. Help him figure it out!

- Caesar decides to use a shift cipher with $\Delta = 5$. Encrypt the message "ATTACK" using this cipher.

- The message "KQJJ" was encrypted using the shift cipher with $\Delta = 5$. Decrypt the message!

Related Idea: Frequency Analysis

Like the Caesar Cipher, a Shift Cipher disguises letters, but does not disguise the natural frequency of letters!



The most frequent symbol used in the ciphertext will correspond to the letter “E” in the plaintext. For a Shift Cipher, this is the ciphertext letter for the shift $5 + \Delta$.

Decryption Method: Shift Cipher

Definition 26 (Decryption: Shift Cipher)**.** An English Language **Shift Cipher**

$$\Box + \Delta (\text{mod } 26) = \boxtimes.$$

can be decrypted by undoing the shift Δ. Some letters will be easy to decrypt and some letters will wrap around the alphabet.

Decryption for an English Language Shift Cipher can be described completely using modular arithmetic as

$$\boxtimes + \nabla (\text{mod } 26) = \Box,$$

where ∇ is a value so that $\nabla + \Delta = 26$.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 27 (Hail Caesar 5)**.** Caesar has used so many different values of Δ to make shift ciphers that he can’t remember how to decrypt!

- Caesar decides to use a shift cipher with $\Delta = 11$. Tell Caesar how much he will have *to shift to the right* in order to decrypt messages encoded with this cipher.

- Write a modular equation to represent decryption for this shift cipher. What does this decryption equation do to the letter “P”?

Example 28 (Hail Caesar 6)**.** Caesar has used so many different values of Δ to make shift ciphers that he can’t remember how to decrypt!

- If Caesar used $\Delta = 12$, what is ∇?

- If Caesar used $\Delta = 20$, what is ∇?

- Caesar remembers one shift cipher with $\nabla = 24$. What is Δ?

- Caesar remembers one shift cipher with $\nabla = 9$. What is Δ?

Example 29 (It’s Greek To Me 1)**.** Enemy agents have started to use different alphabets for encryption.

α	β	γ	δ	ϵ	ζ	η	θ	ι	κ	λ	μ
1	2	3	4	5	6	7	8	9	10	11	12
ν	ξ	o	π	ρ	σ	τ	υ	ϕ	χ	ψ	ω
13	14	15	16	17	18	19	20	21	22	23	24

- What would the encryption rule $\Box + 9 = \boxtimes$ do to the Greek letter ζ?

- Write a modular arithmetic equation to represent a shift cipher that sends α to κ?

Example 30 (It's Greek To Me 2)**.** Enemy agents have started to use different alphabets for encryption.

- If they the equation $\Box + 9 = \boxtimes (\text{mod } 24)$ to encrypt, what will be the equation to decrypt?

- If they the equation $\Box + 20 = \boxtimes (\text{mod } 24)$ to encrypt, what will be the equation to decrypt?

Example 31 (It's Greek To Me 3)**.** Enemy agents have started to use different alphabets for encryption.

- If they use the equation $\Box + 7 = \boxtimes (\text{mod } 24)$ to encrypt, what are Δ and ∇?

- If they use a shift cipher that sends the letter "γ" to "τ", what are Δ and ∇?

!	@	#	$	%	&	$\emptyset$	Q	$\oplus$	Σ	Ψ
1	2	3	4	5	6	7	8	9	10	11

Example 32 (Alien Invasion 1)**.** Aliens from Outer Space arrive on Earth. Despite having mastered interstellar travel, they still use simple encryption techniques. Fortunately, the written symbols for their alien language are eerily familiar.

- Write the equation for the shift cipher that will encrypt the letter "@" as the letter Σ.

- Write the decryption equation for the shift cipher above.

Example 33 (Alien Invasion 2)**.** The aliens have no idea how easy it is to break their code!

- If they use the equation $\square + 7 = \boxtimes (\text{mod } 11)$ to encrypt their messages, what are Δ and ∇?

- If they use a shift cipher that sends the letter "$\emptyset$" to "#", what are Δ and ∇?

$\boxed{\text{Related Idea: Additive Inverse}}$

Definition 34. The additive inverse for $a(\text{mod } n)$ is a value $\overline{a}$ so that

$$a + \overline{a} = 0(\text{mod } n)$$

For English (or any Roman alphabet) Language, we will always have

$$\Delta + \nabla = 0(\text{mod } 26).$$

If a Language has n letters, then we have

$$\Delta + \nabla = 0(\text{mod } n).$$

From working with codes, we can understand that using the additive inverse ∇ "really" works by moving all letters to the left Δ places.

Example 35 (Drill Time: Additive Inverse)**.** Find the additive inverse for each of the following. Use your calculator to first simplify (if needed). Then find the number to add that gets you up to n. Check your answers with a neighbor!

- Find the additive inverse for $14(\text{mod } 26)$.
- Find the additive inverse for $19(\text{mod } 26)$.
- Find the additive inverse for $37(\text{mod } 26)$.
- Find the additive inverse for $14(\text{mod } 16)$.

- Find the additive inverse for 53(mod 20).

Related Idea: Simplifying Negative Mods, Method 1

Recall that by *simplified* we mean that $a(\text{mod } n)$ is written so that a is between 0 and $n-1$. In particular, a cannot be a negative quantity.

Here is a procedure for simplifying $a(\text{mod } n)$ when a is negative.

(1.) Replace a by $a+n$. In symbols this means

$$a(\text{mod } n) = a + n(\text{mod } n).$$

So $a+n$ is the new value for us to consider.

(2.) Is this new value simplified? If yes, then **STOP**.

If not, go back to step (1.) and add n again. In symbols this means

$$a + n(\text{mod } n) = a + 2n(\text{mod } n).$$

Repeat Steps (1.) and (2.) as many times as necessary until you reach a simplified value.

Example 36 (Additive Inverses and Negatives)**.** Any time you see a negative "–" in modular arithmetic, it means "Find the additive inverse to whatever follows". Answer these related questions.

- The quantity $-4(\text{mod } 10)$ means the additive inverse of what?

- Simplify $-4(\text{mod } 10)$.

- The quantity $-9 \pmod{16}$ means the additive inverse of what?

- Simplify $-9 \pmod{16}$.

- The quantity $-14 \pmod{26}$ means the additive inverse of what?

- Simplify $-14 \pmod{16}$.

!	@	#	$	%	&	∅	Q	⊕	Σ	Ψ
1	2	3	4	5	6	7	8	9	10	11

Example 37 (Alien Invasion 3)**.** The aliens detect that humans have been breaking their encrypted messages. They frantically try to make the code more sophisticated by using larger shifts. Help humanity by answering the following.

- What letter would $39 \pmod{12}$ correspond to in this language?

- What letter would $-39 \pmod{12}$ correspond to in this language?

Example 38 (Drill Time: Simplifying Negatives)**.** Simplify the following negative modular arithmetic quantities using Method 1.

- Simplify $-4 \pmod{15}$.
- Simplify $-6 \pmod{20}$.
- Simplify $-23 \pmod{10}$.
- Simplify $-37 \pmod{20}$.
- Simplify $-43 \pmod{10}$.
- Simplify $-87 \pmod{20}$.

Related Idea: Simplifying Negatives, Method 2 (Quick)

Here is the *QUICK* procedure for simplifying negative $a \pmod{n}$

(1.) If $a \pmod{n}$ is not simplified, divide a by n. If the result is a number without a decimal then **STOP**. $a \pmod{n}$ simplifies as

$$0 \pmod{n}.$$

If the result has a decimal, go to step (2.)

(2.) You need to get a negative decimal out of step (1.) Ignore the sign and look at just the number that precedes (to the left) the decimal. ADD THIS NUMBER! So if you see something like -4.246, add 4 to get -0.246. This should always give you a *negative decimal amount.*

(3.) Add 1 to this *negative decimal amount.* This should give you a *positive decimal amount.*

(4.) Multiply this *positive decimal amount* by n. Usually this gives an exact number (no decimal) b, but sometimes you need to round up or down. This is your answer

$$a \pmod{n} = b.$$

Example 39 (Drill Time: Quick Simplifying Negatives)**.** Simplify the following negative modular arithmetic quantities using Method 2.

- Simplify $-44 \pmod{15}$.

- Simplify $-66 \pmod{13}$.

- Simplify $-100 \pmod{27}$.

- Simplify $-1000 \pmod{37}$.

Code Summary: Add in the Shift Cipher

The summary below represents information about codes when encrypting and decrypting English language plaintext.

Cipher	**Encrypt Key(s)**	**Decrypt Key(s)**	**Key Secrecy**	**Letter Frequency**
Caesar	3	23	Private	Normal
Shift	Δ	∇	Private	Normal

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 40 (Congratulations! You Are Now A (Better) Spy 2)**.** Enemy agents have started to make their codes more sophisticated. They now *use multiple shifts at once*! You intercept a message and learn that the shifts being used correspond to

$$\Delta_1 = 4,\ \Delta_2 = 15,\ \Delta_3 = 7.$$

- How would you encrypt the plaintext "ATE"?

- How would you encrypt the plaintext "TEA"?

Encryption Method: Vigenère Cipher

Definition 41. An English Language **Vigenère Cipher** uses a different shift for each letter, depending on the position of the letter in the message.

Encryption uses the rule

$$\begin{aligned}\square_1 + \Delta_1 (\text{mod } 26) &= \boxtimes_1 \\ \square_2 + \Delta_2 (\text{mod } 26) &= \boxtimes_2 \\ \square_3 + \Delta_3 (\text{mod } 26) &= \boxtimes_3 \\ &\vdots\end{aligned}$$

where $\square_1$ is the first plaintext letter and Δ_1 is the first shift, $\square_2$ is the second plaintext letter and Δ_2 is the second shift, etc...

Related Idea: Keyword

Definition 42. We use a **Keyword** to represent all of the different shifts (and the order) to be used with a Vigenère Cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 43. The keyword `ENEMY` gives the following shifts:

$$\Delta_1 = 5 \quad \Delta_2 = 14 \quad \Delta_3 = 5 \quad \Delta_4 = 13 \quad \Delta_5 = 25$$

So the first letter in our message will get shifted 5 places to the right, the second letter will get shifted 14 places to the right, and so on.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 44 (Congratulations! You Are Now A (Better) Spy 3)**.** An enemy agent uses a Vigenère Cipher. Here are the shifts that are used:

$$\Delta_1 = 4, \ \Delta_2 = 15, \ \Delta_3 = 7.$$

- What `Keyword` is being used for this Vigenère Cipher?

- How would you encrypt the plaintext “MANY”?

Decryption Method: Vigenère Cipher

Definition 45. A **Vigenère Cipher** can be decrypted as follows:

(i) Identify Δ_1,Δ_2, Δ_3, etc ...corresponding to the letters of the `Keyword`.

(ii) Find the <u>additive inverse</u> ∇_1 to Δ_1. Next find the <u>additive inverse</u> ∇_2 to Δ_2. Continue for all values Δ_k.

Together, the numbers $\nabla_1,\ \nabla_2,\ \nabla_3, \ldots$ are called the **Decryption Sequence**.

To decrypt a Vigenère Cipher, we use the rule

$$\boxtimes_k + \nabla_k (\text{mod } 26) = \square_k.$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 46 (Congratulations! You Are Now A (Better) Spy 4)**.** The enemy agent starts using a new keyword. You *MUST* break this new code! You figure out the shifts being used are

$$\Delta_1 = 1,\ \Delta_2 = 16,\ \Delta_3 = 16\ \Delta_4 = 12,\ \Delta_5 = 5.$$

- What `Keyword` is being used for this Vigenère Cipher?

- Decrypt the ciphertext message “FDUYD”.

α	β	γ	δ	ϵ	ζ	η	θ	ι	κ	λ	μ
1	2	3	4	5	6	7	8	9	10	11	12
ν	ξ	o	π	ρ	σ	τ	υ	ϕ	χ	ψ	ω
13	14	15	16	17	18	19	20	21	22	23	24

Example 47 (It's Greek To Me 4)**.** You intercept an enemy message that uses a Vigenère Cipher.

- If the shifts

$$\Delta_1 = 16,\ \Delta_2 = 9,\ \Delta_3 = 17,\ \Delta_4 = 15$$

were used, what is the `Keyword`?

- How is the ciphertext "$\pi o\lambda\alpha$"? decrypted?

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 48 (Congratulations! You Are Now A (Better) Spy 5)**.**

- An enemy agent uses a Vigenère Cipher with shifts

$$\Delta_1 = 1,\ \Delta_2 = 16,\ \Delta_3 = 16\ \Delta_4 = 12,\ \Delta_5 = 5.$$

What is the decryption sequence?

- An enemy agent uses the keyword `TOME`. What is the decryption sequence?

α	β	γ	δ	ϵ	ζ	η	θ	ι	κ	λ	μ
1	2	3	4	5	6	7	8	9	10	11	12
ν	ξ	o	π	ρ	σ	τ	υ	ϕ	χ	ψ	ω
13	14	15	16	17	18	19	20	21	22	23	24

Example 49 (It's Greek To Me 5)**.**

- An enemy agent uses a Vigenère Cipher with shifts

  $$\Delta_1 = 12,\ \Delta_2 = 1,\ \Delta_3 = 8.$$

  What is the decryption sequence?

- What is the decryption sequence for the keyword“$\alpha\epsilon\rho\sigma$”?

!	@	#	$	%	&	∅	Q	⊕	Σ	Ψ
1	2	3	4	5	6	7	8	9	10	11

Example 50 (Alien Invasion 4)**.** Aliens start using Vigenère Cipher! You determine that the aliens are using the keyword Σ$∅.

- How would the alien word “! & # #” be encrypted?

- What is the decryption sequence for this Vigenère Cipher?

- How is the ciphertext “@ΨQ@ decrypted?

Related Idea: Advantages of the Vigenére Cipher

The Vigenère Cipher is a HUGE improvement over Shift Ciphers because any single letter can be encrypted in many different ways.

Theorem (Counting Possibilities for the Vigenère Cipher)**.** The number of different ways a letter can be encrypted using the Vigenère Cipher is at most the length of the keyword being used. If the keyword has no repeats in letters then this number is exactly the length of the keyword.

Example 51. For a Vigenère Cipher that uses the `keyword` “TWIN”, the letter “E” could be encrypted using “T”, “W”, “I”, or “N”. This means that “E” could be encrypted as

`Plaintext Numeric` □	5	5	5	5
`Keyword Numeric`	20	23	9	14
Ciphertext ⊠	Y	B	N	S

Code Summary: Add in the Vigenère Cipher

The summary below represents information about codes when encrypting and decrypting English language plaintext.

Cipher	**Encrypt Key(s)**	**Decrypt Key(s)**	**Key Secrecy**	**Letter Frequency**
Caesar	3	23	Private	Normal
Shift	Δ	∇	Private	Normal
Vigenère	$\Delta_1\Delta_2\Delta_3\ldots$	$\nabla_1\nabla_2\nabla_3\ldots$	Private	Less Predictable

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 52 (New Cipher Times)**.** Enemy agents are trying to invent a new type of cipher. He decides on the following encryption scheme:

Plaintext $\square$	converts to	Ciphertext $\boxtimes$
A	$\rightarrow$	C
B	$\rightarrow$	F
C	$\rightarrow$	I

- How will the plaintext letter “D” be encrypted?

- How will the plaintext letter “K” be encrypted?

Encryption Method: Times Cipher

Definition 53. A **Times Cipher** (also called a **Decimation Cipher**) can be encrypted by scaling each letter position by an amount $\star$.

The conversion from English plaintext $\square$ to ciphertext $\boxtimes$ is represented by the formula

$$\star \times \square \pmod{26} = \boxtimes.$$

The conversion from plaintext $\square$ in a Language with n letters to ciphertext $\boxtimes$ is represented by the formula

$$\star \times \square \pmod{n} = \boxtimes.$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 54 (Trouble with Times Cipher)**.** An enemy agent uses the **Times cipher**

$$\star \times \square \pmod{26} = \boxtimes.$$

- For the times cipher $4 \times \square \pmod{26} = \boxtimes$, how is the letter “I” encrypted?

- For the times cipher $4 \times \square \pmod{26} = \boxtimes$, how is the letter “V” encrypted?

- What could be wrong with the cipher $4 \times \square \pmod{26} = \boxtimes$?

Related Idea: Zero-Divisors

A weird thing can happen when using a **Times Cipher**. Two letters might be encrypted as the same letter. The reason behind this are something called zero-divisors.

Definition 55. A **zero divisor modulo** n for a is a non-zero simplified a where some other non-zero simplified value b gives

$$a \cdot b (\text{mod } n) = 0.$$

Example 56 (Zero-Divisor for $n = 6$)**.** The values $a = 2(\text{mod } 6)$ and $b = 3(\text{mod } 6)$ are simplified and not equal to zero-divisor. However,

$$a \cdot b(\text{mod } n) = 2 \cdot 3(\text{mod } 6) = 0$$

Because $a \cdot b(\text{mod } n) = 0$, we can say that both $a = 2(\text{mod } 6)$ and $b = 3(\text{mod } 6)$ are zero-divisors.

Example 57 (Drill Time: Zero–Divisors 1)**.** Answer these questions about zero-divisors.

- Does 3 multiply with $2(\text{mod } 6)$ to make zero?

- Does 3 multiply with $12(\text{mod } 18)$ to make zero?

- Is there a non-zero number to multiply $2(\text{mod } 4)$ to make zero?

- Is there a non-zero number to multiply $3 \pmod 4$ to make zero?

- Is there a non-zero number to multiply $2 \pmod{10}$ to make zero?

Example 58 (Drill Time: Zero–Divisors 2)**.** Answer these questions about zero-divisors.

- Is $6 \pmod{15}$ a zero-divisor?

- Is $10 \pmod{15}$ a zero-divisor?

- Is $14 \pmod{21}$ a zero-divisor?

- Is $9 \pmod{33}$ a zero-divisor?

- Find a value n so that $4 \pmod n$ is a zero-divisor.

- Find a value n so that $11 \pmod{n}$ is a zero-divisor.

Related Idea: Factors; Prime and Composite Numbers

Definition 59. A **factor** of an integer n is any number a that has a partner b with

$$a \cdot b = n.$$

An positive integer n is **prime** if n has exactly two factors, 1 and n.
An positive integer n greater than one is **composite** if it is not prime.
That is, n is composite means that n has more than two factors.

Example 60 (Factors; Prime and Composite Numbers)**.** Since $3 \cdot 8 = 24$, the integer $n = 24$ has factors $a = 3$ and $b = 8$. Other factors for $n = 24$ are 1, 2, 4, 6, and 12. So $n = 24$ is definitely a *composite number.*

The integer $n = 17$ has no factors other than 1 and 17. So 17 is a *prime number.*

Example 61 (Times Cipher and Zero–Divisors 1)**.**

- Why is $13 \pmod{26}$ a zero–divisor for an English language times cipher?

- Why is $8 \pmod{26}$ a zero–divisor for an English language times cipher?

- Find other values for $\star$ so that $\star$(mod 26) is a zero-divisor.

Example 62 (Times Cipher and Zero–Divisors 2)**.**

- Why is 12(mod 24) a zero–divisor for a Greek language times cipher?

- Why is 10(mod 24) a zero–divisor for a Greek language times cipher?

- Find other values for $\star$ so that $\star$(mod 24) is a zero-divisor.

!	@	#	$	%	&	∅	Q	⊕	Σ	Ψ
1	2	3	4	5	6	7	8	9	10	11

Example 63 (Times Cipher and Zero–Divisors 3)**.**

- Is 3(mod 11) a zero–divisor for an alien language times cipher?

- Is 5(mod 11) a zero–divisor for an alien language times cipher?

- Is 10(mod 11) a zero–divisor for an alien language times cipher?

Related Idea: Greatest Common Divisor or *gcd*

Definition 64. The **greatest common divisor** of two numbers a and n, often written as

$$gcd(a, n)$$

is the largest integer that is a factor of both a and n.

Two numbers a and n are said to be **relatively prime** if

$$gcd(a, n) = 1.$$

This means that 1 is the only factor both a and n share.

Example 65 (gcd).

- For $a = 12$ and $n = 18$, we have $gcd(12, 18) = 6$.
- For $a = 12$ and $n = 19$, we have $gcd(12, 19) = 1$.
  So 12 and 19 are *relatively prime.*

Related Idea: Finding *gcd* (Greatest Common Divisor)

Our previous definition of $gcd(a, n)$ is really important! We should have a way of finding $gcd(a, n)$.

Theorem (Finding *gcd*)**.** To find $gcd(a, n)$, list all of the factors of both a and n. Once the lists are complete, identify the largest number that appears in both lists. If 1 is the largest number, then a and n are *relatively prime.*

Example 66 (Finding gcd)**.** For $a = 12$ and $n = 18$ we know the following.

Factors of 12: 1, 2, 3, 4, 6, 12 and
Factors of 18: 1, 2, 3, 6, 9, 18.
Since 6 is the largest number that appears in both lists, $gcd(12, 18) = 6$.

For $a = 12$ and $n = 19$ we have the factors of 12 above, but 19 is prime and only has factors 1 and 19. So $gcd(12, 19) = 1$.

Example 67 (Drill Time: Factors, GCD, and Relatively Prime)**.**

- Is 6 a factor of 42?

- What are the factors of 56?

- What is $gcd(15, 30)$?

- What is $gcd(15, 20)$?

- What is $gcd(12, 40)$?

- Are 8 and 12 relatively prime?

- Are 5 and 12 relatively prime?

Related Idea: Unit

Definition 68. A value $a < n$ with $gcd(a, n) = 1$ is called a **unit** modulo n.

Stated with mathematical notation, the simplified value

$$a(\text{mod } n)$$

is a **unit** when $gcd(a, n) = 1$.
If $a > n$ (a is bigger than n), we usually first simplify
$a(\text{mod } n) = b(\text{mod } n)$, then determine if $b(\text{mod } n)$ is a unit.

Example 69 (Identifying units $\mod n$)**.** The value $12(\text{mod } 19)$ is a unit. This is because $gcd(12, 19) = 1$.

The value $23(\text{mod } 20)$ is not simplified!
Note that $23(\text{mod } 20) = 3(\text{mod } 20)$. Since $gcd(3, 20) = 1$ we have $3(\text{mod } 20)$ a unit.
This says that $23(\text{mod } 20) = 3(\text{mod } 20)$ is a unit too!

Example 70 (English Times Cipher)**.**

- Is $3(\text{mod } 26)$ an unit? Why or why not?

- What is $3 \times 9(\text{mod } 26)$?

- What is $17 \times 23 (\text{mod } 26)$?

Related Idea: Zero-Divisor and Unit Connection

Theorem (Related Idea: Zero-Divisor and Unit Connection)**.** A nonzero modular arithmetic value $a(\text{mod } n)$ is either a unit or a zero-divisor (but not both).

- If $gcd(a, n) = 1$ then $a(\text{mod } n)$ is a unit.
- If $gcd(a, n) \neq 1$ then $a(\text{mod } n)$ is a zero-divisor.

Example 71 (Identifying zero-divisors and units $\mod n$)**.** The theorem above allows us to easily list out units and zero-divisors by using gcd. For (mod 12) the units are

$$1, \ 5, \ 7, \ 11$$

and the zero-divisors are every other non-zero value

$$2, \ 3, \ 4, \ 6, \ 8, \ 9, \ 10.$$

Related Idea: Multiplicative Inverse

There's an idea related to units:

Definition 72. The unit $a(\text{mod } n)$ has **multiplicative inverse** $b(\text{mod } n)$ if

$$a \cdot b = 1(\text{mod } n).$$

This also says that the **multiplicative inverse** of $b(\text{mod } n)$ is $a(\text{mod } n)$.

Example 73 (Multiplicative Inverses)**.** For (mod 10), the units are $1, \ 3, \ 7, \ 9$. Notice that

- $1 \cdot 1 = 1(\text{mod } 10)$, so 1 is the multiplicative inverse of 1
  (This is true for all n.)
- $3 \cdot 7 = 21(\text{mod } 10) = 1(\text{mod } 10)$, so 3 and 7 are multiplicative inverses.
- $9 \cdot 9 = 81(\text{mod } 10) = 1(\text{mod } 10)$, so 9 is the multiplicative inverse of itself!

Finding Multiplicative Inverses, Method 1

Remember, only **units** have multiplicative inverses. This leads to our first method for finding multiplicative inverses.

Theorem. To find the multiplicative inverse to $a \pmod{n}$, where $gcd(a, n) = 1$, do the following:

(i) Make a list of **ALL** units $b \pmod{n}$. This list will always start with 1 and end with $n - 1$.

(ii) For each value $b \pmod{n}$ in the list above, calculate $a \cdot b \pmod{n}$.
   If $a \cdot b \pmod{n} = 1$ then b is the multiplicative inverse.
   If $a \cdot b \pmod{n} \neq 1$ then go to the next number in the list.

For some values of n (like $n = 12$) there are very few units, so it is easy to quickly check all products $a \cdot b \pmod{n}$.

Example of finding Multiplicative Inverses, Method 1

Example 74. For English language Times Ciphers, we use (mod 26). It is easy to check that the **units** a(mod 26) are *the odd values, excluding 13*. You can easily use Method 1 above to find the multiplicative inverse of all units (mod 26):

Unit Value	1	3	5	7	9	11	15	17	19	21	23	25
Mult. Inverse	1	9	21	15	3	19	7	23	11	5	17	25

Notice that multiplicative inverses come in pairs;
9 is the multiplicative inverse of 3(mod 26) but this also says that 3 is the multiplicative inverse of 9(mod 26)!

Finding Multiplicative Inverses, Method 2

Theorem. To find the multiplicative inverse to $a \pmod{n}$, make two lists:

(i) Make multiples of the value n:

$$\{n,\ 2n,\ 3n,\ 4n, \ldots\}$$

(ii) Add 1 to every member of the list from step (i):

$$\{n+1,\ 2n+1,\ 3n+1,\ 4n+1, \ldots\}$$

Starting with $n+1$, divide each of the numbers from Step (ii) list by a. If this division makes a number that is whole (no remainder/decimal) then this number is the multiplicative inverse for a.

If not, move onto the next number. Sometimes you have to go back and extend your lists.

Example of finding Multiplicative Inverses, Method 2

Example 75. The Ancient Roman Alphabet had only 23 letters. For this language we would use (mod 23). Because there are so many units, it is much easier to find multiplicative inverses using Method 2.

Let's find the multiplicative inverse of 7(mod 23). Start by making our lists:

(i) Make multiples of the value 23:

$$\{23,\ 46,\ 69,\ 92,\ 115,\ 138,\ 161,\ 184,\ 207,\ 230,\ \ldots\}$$

(ii) Add 1 to every member of the list from step (i):

$$\{24,\ 47,\ 70,\ 93,\ 116,\ 139,\ 162,\ 185,\ 208,\ 231,\ \ldots\}$$

Now divide each number in list two by 7. On the third number we get $7 \div 70 = 10$. This says that 10(mod 23) is the multiplicative inverse of 7(mod 23). We can check that $7 \cdot 10 \pmod{23} = 1$.

Example 76 (Drill Time: Multiplicative Inverse)**.**

- Is 3 the multiplicative inverse to 2(mod 5)?

- Is 3 the multiplicative inverse to 7(mod 11)?

- Does 4(mod 7) have a multiplicative inverse?

- What is the multiplicative inverse to 3(mod 10)?

- What is the multiplicative inverse to 7(mod 11)?

- What is the multiplicative inverse to 5(mod 12)?

Decryption Method: Times Cipher

Definition 77. An English Language **Times Cipher**

$$\star \times \square \pmod{26} = \boxtimes.$$

can be decrypted by finding a value $\ast$ (called snowflake) so that

$$\star \cdot \ast = 1 \pmod{26}$$

Decryption can be described completely as

$$\ast \times \boxtimes \pmod{26} = \square,$$

where $\star \cdot \ast = 1 \pmod{26}$. Note: $\ast$ and $\star$ are multiplicative inverses!

Big Connection: Which English Times Ciphers Work?

Theorem. The English Times Cipher

$$\star \times \square \pmod{26} = \boxtimes$$

is only valid when $gcd(\star, 26) = 1$.

This says that $\star$ and 26 share only the factor 1. In other words, $\star \pmod{26}$ is a unit!

Example 78 (English Times Ciphers that work)**.** The values that $\star$ can be in an English Times Cipher are

$$1,\ 3,\ 5,\ 7,\ 9,\ 11,\ 15,\ 17,\ 19,\ 21,\ 23,\ 25$$

Big Connection: Which General Times Ciphers Work?

Theorem. The Times Cipher

$$\star \times \square \pmod{n} = \boxtimes$$

is only valid when $gcd(\star, n) = 1$.

This says that $\star$ and n share only the factor 1. In other words, $\star \pmod{n}$ is a unit!

Decryption of this Times Cipher is given by $\ast \times \boxtimes = \square \pmod{n}$, where $\ast$ is the multiplicative inverse to $\star$.

Example 79 (A Language with 18 Characters)**.** The values that $\star$ can be in a language with 18 characters are

$$1,\ 5,\ 7,\ 11,\ 13,\ 17$$

A curious fact: In any language with more than 2 characters, there are always an even number of values that $\star$ could be!

Greek Alphabet

α	β	γ	δ	ϵ	ζ	η	θ	ι	κ	λ	μ
1	2	3	4	5	6	7	8	9	10	11	12
ν	ξ	o	π	ρ	σ	τ	υ	ϕ	χ	ψ	ω
13	14	15	16	17	18	19	20	21	22	23	24

Alien Alphabet

!	@	#	$	%	&	∅	Q	⊕	Σ	Ψ
1	2	3	4	5	6	7	8	9	10	11

Example 80 (Times Ciphers in Different Languages)**.**

- Is $5 \times \square = \boxtimes$ a valid cipher for the English alphabet?

- Is $4 \times \square = \boxtimes$ a valid cipher for the Greek alphabet?

- Is $8 \times \square = \boxtimes$ a valid cipher for the Alien alphabet?

Code Summary: Add in the Times Cipher

The summary below represents information about codes when encrypting and decrypting English language plaintext.

Cipher	**Encrypt Key(s)**	**Decrypt Key(s)**	**Key Secrecy**	**Letter Frequency**
Caesar	3	23	Private	Normal
Shift	Δ	∇	Private	Normal
Vigenère	$\Delta_1\Delta_2\Delta_3\ldots$	$\nabla_1\nabla_2\nabla_3\ldots$	Private	Less Predictable
Times	$\Delta_1\Delta_2\Delta_3\ldots$ $\star$	$\nabla_1\nabla_2\nabla_3\ldots$ $*$	Private	Even Less Normal

Related Ideas: Key Distribution & Public Key Cipher

Definition 81 (Related Ideas: Key Distribution & Public Key Cipher)**.** The problem of **Key Distribution** in cryptography is that of giving all intended recipients the necessary key to decrypt messages, while simultaneously keeping those keys secret in general.

A major goal of cryptography is a **Public Key Cipher**. This is a code system where the encryption key can be freely visible to anyone, but only the intended recipient has the means of using the decryption key.

Example 82 (Related Ideas: Key Distribution & Public Key Cipher)**.** You want to check your savings account balance online, but you'd rather nobody else knows what this is. You can use a login and password so your bank can verify your identity. But how does the bank actually *SEND* you your account information? The number has to go through various routing points, all of which can be hacked. The bank could *ENCRYPT* the account information, but how would you (or your computer) know how to decrypt it?

Encryption: DHM Key Exchange

Definition 83. The **DHM Key Exchange** allows two parties that have no prior knowledge of each other to exchange a secret key over (possibly insecure) communication lines.

- DHM is named after the scientists, Diffie, Hellman, and Merkle, who first published an article about the key exchange.
- British Intelligence actually knew about DHM before Diffie, Hellman, and Merkle, but kept the key exchange a secret for national security reasons.
- The idea of how this works is based on a mathematical process that is *EASY* to do, but *SUPER HARD* to undo.

Related Ideas: DHM Key Mechanics

Example 84. Two parties, Alice and Bob, calculate a key that a third person Carl will never know, even if Carl intercepts all communication between Alice and Bob.

First off, Alice & Bob agree on numbers n and M (not secret).

1. Alice chooses a secret value a.
2. Bob chooses a secret value b.
3. Alice computes $\alpha = M^a (\text{mod } n)$
4. Bob computes $\beta = M^b (\text{mod } n)$

5. Alice sends α to Bob.
6. Bob sends β to Alice.
7. Alice computes that the key is $K = \beta^a (\text{mod } n)$.
8. Bob computes that the key is $K = \alpha^b (\text{mod } n)$.

Note that K is the same for both Alice and Bob since $K = (M^a)^b = (M^b)^a (\text{mod } n)$.

Example 85 (DHM Practice 1)**.** Bob and Alice are trying to send a key over unsecured communication lines. They agree to use $M = 6$ and $n = 23$.

- For $a = 3$, compute $\alpha = M^a (\text{mod } n) = 6^3 (\text{mod } 23)$.

- For $b = 5$, compute $\beta = M^b (\text{mod } n) = 6^5 (\text{mod } 23)$.

- For $a = 21$, the value $\alpha = M^a (\text{mod } n) = 6^{21} (\text{mod } 23)$ is too big. What is a good way to break up this exponent?

Example 86 (DHM Practice 2)**.** Bob and Alice are trying to send a key over unsecured communication lines. They agree to use $M = 6$ and $n = 23$.

- For $\beta = 2$, compute $\beta^a (\text{mod } n) = 2^3 (\text{mod } 23)$.

- For $\alpha = 9$, compute $\alpha^b (\text{mod } n) = 9^5 (\text{mod } 23)$.

- What is the key for this exchange?

Example 87 (DHM Practice 2)**.** Bob and Alice are trying to send a key over unsecured communication lines. They agree to use $M = 4$ and $n = 37$.

- For $a = 11$, compute $\alpha = M^a (\text{mod } n)$.

- For $b = 9$, compute $\beta = M^b (\text{mod } n)$.

- For $b = 30$, the value $\beta = M^b (\text{mod } n) = 4^{30} (\text{mod } 37)$ is too big. What is a good way to break up this exponent?

Example 88 (DHM Practice 2)**.** Bob and Alice are trying to send a key over unsecured communication lines. They agree to use $M = 6$ and $n = 23$.

- Note that $36 (\text{mod } 37) = -1 (\text{mod } 37)$. Can you use this to simplify $\beta^a (\text{mod } 37) = 36^{11} (\text{mod } 37)$?

- Note that $21^4 (\text{mod } 37) = 9$. Can you use this to simplify $\alpha^b (\text{mod } 37) = 21^9 (\text{mod } 37)$.

- What is the key for this exchange?

Example 89 (DHM Practice 3)**.** Bob and Alice are trying to send a key over unsecured communication lines. They agree to use $M = 10$ and $n = 41$.

- Compute $M^2 (\text{mod } n) = 10^2 (\text{mod } 41)$.

- Compute $M^5 (\text{mod } n) = 10^5 (\text{mod } 41)$.

- Can you use your answers above to easily calculate $\alpha = M^{17} \pmod{41}$?

Example 90 (DHM Practice 3)**.** Bob and Alice are trying to send a key over unsecured communication lines. They agree to use $M = 6$ and $n = 23$. Alice receives $\beta = 18 \pmod{41}$ from Bob. Her secret value is $a = 13$.

- Calculate $\beta^4 \pmod{41} = 18^4 \pmod{41}$.

- Use your answer above to quickly calculate $\beta^{12} \pmod{41} = (18^4 \pmod{41})^3$.

- What is the key for this exchange?

Example 91 (Master Spy 1)**.** You've been promoted to the highest rank in the Spy Agency! It's now time to learn about a modern and sophisticated code. See if you can handle the following questions:

- How long does it take you to factor 2173 as a product of two primes $2173 = p \cdot q$?

- How long does it take you to multiply the numbers 41 and 53?

- If n is a big number, is it easy to factor? If p and q are big numbers, is it easy to multiply them?

Encryption: RSA Cipher

Definition 92. The **RSA Cipher** is a public key cipher publicly discovered in the 1970s. The RSA cipher uses a form of multiplication for encryption and is secure because factoring large numbers is (currently) very difficult to do.

- RSA stands for Rivest, Shamir, and Adleman, the people responsible for first publicizing the RSA cipher.
- The British and US governments may have known about RSA prior to the 1970s, but did not announce their discovery.
- Even though this is the basis for most modern cryptography, there is current speculation that the US government (specifically the NSA) has the ability to break this code.

RSA Encryption

Example 93. Here is how Alice and Bob can do to share a secret from Carl:

What Alice Does

1. Alice chooses two (large) *prime* numbers p and q, which she keeps secret.

2. She then multiplies to find $n = p \cdot q$. This can be done quickly because multiplication is "easy".

3. Alice also calculates a value $m = (p-1)(q-1)$.

4. She selects a value $e (\text{mod } m)$ that is a *unit.*

   So any choice of e with $gcd(e, m) = 1$ will work. The value e is called the **encryption exponent**.

5. Next, Alice tells Bob (and anyone else) the values for n and e. The fact that Alice can publicly state n and e is what makes RSA a public key cipher.

What Bob Does To Send Alice a Message

6. Bob converts letters (or blocks of letters) into numbers. We can do this is the standard way, but in real-life this gets done by a computer.

7. For each letter $\square$, he uses the rule

$$\square^e (\text{mod } n) = \boxtimes$$

   to find the ciphertext. He sends this ciphertext to Alice.

Example 94 (Master Spy 2)**.** You've been promoted to the highest rank in the Spy Agency! It's now time to learn about a modern and sophisticated code. See if you can handle the following questions:

- If $p = 71$ and $q = 59$, find $n = p \cdot q$.

- If $p = 71$ and $q = 59$, find $m = (p-1) \cdot (q-1)$.

- If $p = 101$ and $q = 103$, find $n = p \cdot q$.

- If $p = 101$ and $q = 103$, find $m = (p - 1) \cdot (q - 1)$.

Example 95 (Master Spy 3)**.** You've been promoted to the highest rank in the Spy Agency! It's now time to learn about a modern and sophisticated code. See if you can handle the following questions:

- If $p = 41$ and $q = 53$, find n and m.

- If $p = 101$ and $q = 107$, find n and m.

- If $p = 521$ and $q = 641$, find n and m.

Example 96 (Master Spy 4)**.** You've been promoted to the highest rank in the Spy Agency! It's now time to learn about a modern and sophisticated code. See if you can handle the following questions:

- If $p = 17$ and $q = 19$, find n and m.

- If $p = 7$ and $m = 132$, find q and n.

- If $p = 3$ and $q = 5$, find all units $(\bmod\ m)$.

- If $p = 5$ and $q = 11$, what is $27 \cdot 3 (\bmod\ m)$?

Example 97 (Master Spy 5)**.** A fellow agent wants you to send her a message. She broadcasts the numbers $n = 33$ and $e = 3$, expecting that these will be intercepted.

- Use this RSA cipher to encrypt the letter "H" as a number.

- Use this RSA cipher to encrypt the letter “I” as a number.

- Use this RSA cipher to encrypt the letter “J” as a number.

- The letters “H”, “I” and “J” are consecutive. Does RSA encrypt these letters as consecutive numbers?

Example 98 (Master Spy 6)**.** You want a fellow agent to send you a secret message. You decide on the numbers $n = 77$ and $e = 7$ and publish these to an open webpage.

- What number will the letter “B” be encrypted as?

- What number will the letter “C” be encrypted as?

- Encrypt the number “0203”? Is this connected to the answers above in any way?

Example 99 (Master Spy 7)**.** An enemy agent starts using RSA encryption. Fortunately, a mole on the inside shares some secret information.

- The agent uses $n = 33$ and $e = 3$. What are $5 \cdot e (\text{mod } m)$ and $7 \cdot e (\text{mod } m)$?

- The agent uses $n = 55$ and $e = 27$. What are $3 \cdot e (\text{mod } m)$ and $7 \cdot e (\text{mod } m)$?

Related Idea: RSA Decryption

Example 100 (RSA Decryption)**.** 1. Alice knows p, q, and $m = (p-1) \cdot (q-1)$.

2. She finds the value d that is the multiplicative inverse to $e (\text{mod } m)$. This is called the **decryption exponent**.

3. Alice takes the ciphertext ⊠ she receives from Bob and applies the decryption exponent in the following way to get back the plaintext message:

$$\boxtimes^d (\text{mod } n) = \square$$

This works because e and d are multiplicative inverses and the algebra rule that says

$$\boxtimes^d = (\square^e)^d = \square^{e \cdot d}.$$

Which RSA Encryption/Decryption Exponents Work?

Theorem (Which RSA Encryption/Decryption Exponents Work?)**.** The for an RSA cipher that uses primes p and q with

- $n = p \cdot q$
- $m = (p - 1) \cdot (q - 1)$

The encryption exponent $e(\text{mod } m)$ must be a unit. In other words $gcd(e, m) = 1$.

The encryption exponent has a multiplicative inverse $d(\text{mod } m)$ which is the decryption exponent. Then $d(\text{mod } m)$ is also a unit and $gcd(d, m) = 1$.

Example 101 (RSA Encryption/Decryption Exponents)**.** For an RSA cipher, if $p = 43$ and $q = 67$, is $e = 11$ a valid choice for an encryption exponent?

Note that $m = (43 - 1)(67 - 1) = 2772$. It is easy to check that $gcd(11, 2772) = 11$, so $e = 11$ WILL NOT WORK.

Example 102 (Master Spy 8)**.** The mole on the inside shares some more secret information about an enemy agent's code.

- The enemy agent uses $n = 143$ and $p = 11$. Find q and m.

- Which of the following numbers of the form $120 \cdot k + 1$ is divisible by 7?

$$121,\ 241,\ 361,\ 481,\ 601,\ 721,\ 841,\ 961$$

- Use your answers from above to find the multiplicative inverse to $7(\text{mod } 120)$.

Example 103 (Master Spy 9)**.** More information about the enemy agent's code:

- The enemy agent uses $n = 77$ and $e = 7$ for encryption. Find p, q and m.

- Find the decryption key $d(\text{mod } m)$. (Recall that $d(\text{mod } m)$ is the multiplicative inverse to $e(\text{mod } m)$.)

- Decrypt "62" using your answer above. It might help to know that $62^{10}(\text{mod } 77) = 1(\text{mod } 77)$.

Code Summary

The summary below represents information about codes when encrypting and decrypting English language plaintext.

Cipher	**Encrypt Key(s)**	**Decrypt Key(s)**	**Key Secrecy**	**Letter Frequency**
Caesar	3	23	Private	Normal
Shift	Δ	∇	Private	Normal
Vigenère	$\Delta_1\Delta_2\Delta_3\ldots$	$\nabla_1\nabla_2\nabla_3\ldots$	Private	Less Predictable
Times	$\star$	$*$	Private	Normal
RSA	n, e	m, d	Public	"Random"

With RSA, private (encrypted) messages can be sent after keys are publicly (open for interceptions) exchanged. This is what allow you to shop or access your bank account online.