Math 187A Notes

Introduction to Cryptography

Winter 2023
Taught by Professor Shishir (Sunny) Agrawal

Table of Contents

1 Introduction to Cryptography

We begin with some common definitions.

1.1 Terminology

Definition 1.1: Cipher

A **cipher**, or cryptosystem, is a cryptographic method for confidential communication.

Generally, a cryptographic method includes algorithms for *encryption* and *decryption*, which are inverse processes that convert between plainly readable information called *plaintext*[1] and unintelligible information called *ciphertext*.

Definition 1.2: Sender

A **sender**, often named "Alice" in abstract cryptographic discussions, *encrypts* her plaintext into ciphertext.

Definition 1.3: Receiver

A **receiver**, often named "Bob," *decrypts* (or deciphers) the ciphertext back into plaintext.

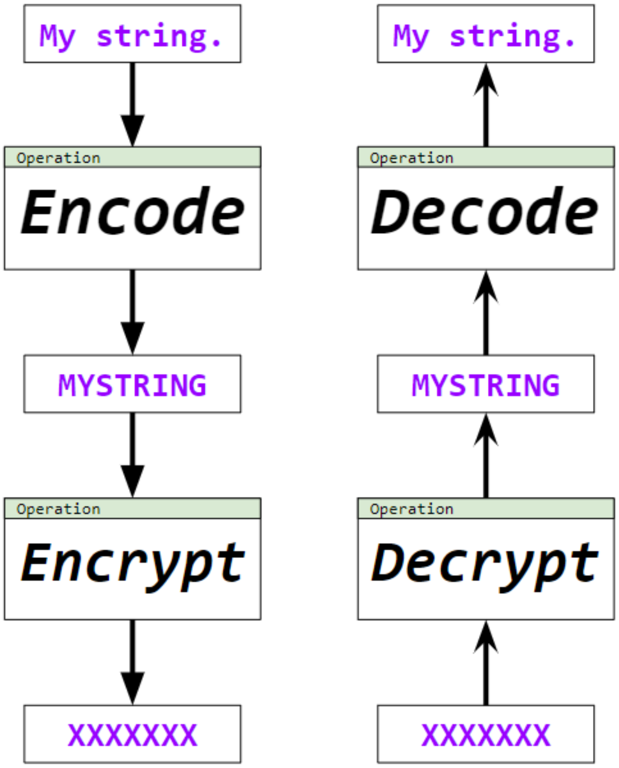
Often times, Bob will use a *key* to decrypt the message. This is sometimes known as a private key or decryption key.

Definition 1.4: Encoding

The (usually) preliminary step where a message is converted into a format which can then be encrypted is called **encoding**.

Note that encoded text is not secure; it is only secure after encryption. So, we can think of encoding as the pre-processing step. In other words, before we encrypt something, we might *encode* the text so it's easier to encrypt. It should also be noted that if a message had to be encoded before encryption, then it will also need to be decoded after decryption.

[1] In cryptography, we use *plaintext* and *ciphertext* instead of *plain text* and *cipher text*.



Definition 1.5: Adversary

An **adversary**, often named "Eve," is one whose aim is to prevent the users of a cryptosystem from achieving their goal.

In our case here, an adversary can intercept a ciphertext. Thus, the adversary will not have Bob's decryption key at the beginning. The idea is that, even if the adversary knows what cryptosystem was used to encrypt the message, if the adversary doesn't have this decryption key, she should ideally not be able to decrypt the message. If she does manage to figure out the plaintext, she has *broken* the code.

Definition 1.6: Attack Model

An **attack model** specifies what Eve is allowed to do in order to break the code.

Some common attack models includes:

- Ciphertext-only attack: Eve must recover the plaintext using only the ciphertext.
- Known-plaintext attack: Eve may have access to some information about the plaintext (e.g., knowledge of portions of the plaintext), which can be used to recover the plaintext entirely.
- Chosen-plaintext attack: Eve can request or generate ciphertexts corresponding to any plaintext message of her choosing, and she can use this information to recover the plaintext.

Classical cryptography was mostly concerned with assuring security against the first two. Modern cryptography tries to assure security against the last.

2 Classical Cryptosystems

We begin with a definition:

Definition 2.1: n-gram

An n-gram is a sequence of n letters.

For example, a 1-gram is just a single letter; a 2-gram (i.e., *bigram*) is a pair of letters; and so on. Generally, we can group many classical cryptosystems into a few different encryption strategies.

<table>
<tr><th>Strategy</th><th>Description</th></tr>
<tr><td>Transposition</td><td>Involves rearranging units of plaintext according to some pattern. We'll see just one example of this type of cipher: rectangular transposition.</td></tr>
<tr><td>Substitution</td><td>Involves replacing units of plaintext with units of ciphertext. We can further group substitution ciphers into some subtypes:
<table>
<tr><th>Subtype</th><th>Description</th></tr>
<tr><td>Simple Substitution</td><td>In these ciphers, single letters of plaintext are replaced by ciphertext. The substitution scheme stays the same over the course of the entire message. Some examples we'll see include:<ul><li>Masonic cipher</li><li>Caesar cipher</li><li>Affine cipher</li><li>Polybius square</li></ul>In essence, though, there is a 1-1 relationship between the letters of the plaintext and the ciphertext alphabets.</td></tr>
<tr><td>Polygraphic Substitution</td><td>In these ciphers, groups of letters in the plaintext are replaced by ciphertext (a group of n letters is called an n-gram).The substitution scheme stays the same over the entire message. Some examples we'll see include:<ul><li>Hill cipher</li><li>Playfair cipher</li></ul>So, in essence, polygraphic substitution is just simple substitution but with <i>groups of letters</i> instead of individual letters.</td></tr>
<tr><td>Polyalphabetic Substitution</td><td>In these ciphers, single letters in the plaintext are replaced by ciphertext, and the substitution scheme changes over the course of the message. Some examples include:<ul><li>Vignere cipher</li><li>One-time pad</li></ul></td></tr>
</table>
In practice, however, most cryptosystems employ a combination of these strategies.</td></tr>
</table>

2.1 Rectangular Tranposition

Rectangular tranposition, known also as *regular columnar transposition*, is a tranposition cipher. The ciphertext is obtained by *permuting* the letters of the plaintext in a particular pattern. The pattern is determined by a secret *keyword*.

Roughly speaking, the steps to perform rectangular transposition are as follows:

1. Using the keyword, rank the letters based on alphabetical ranking.
2. Break up the message into groups of n, where n is the length of the keyword.
3. For each group, do the following:
   - Encrypting: If the ith letter of the keyword has rank j, move the ith letter in the group into the jth position.
   - Decrypting: If the ith letter of the keyword has rank j, move the jth letter of each group into the ith position.

Note that keywords with repeat letters do not work by themselves. We either need to agree not to use words with repeat letters, or remove duplicate letters from the keyword[2].

(Example: Encryption.) Suppose that Alice and Bob share the keyword GUARD, and that Alice wants to send the following message to Bob:

```
Hide! The baboons are coming for you.
```

First, we'll **encode** the message so that it's easier to encrypt. In our example, we'll remove all spaces and punctuation.

```
HIDETHEBABOONSARECOMINGFORYOU
```

Now that encoding is done, we still need to encrypt the message. Notice how the keyword GUARD has 5 letters; we can break the message up into 5-grams and then stack them into rows:

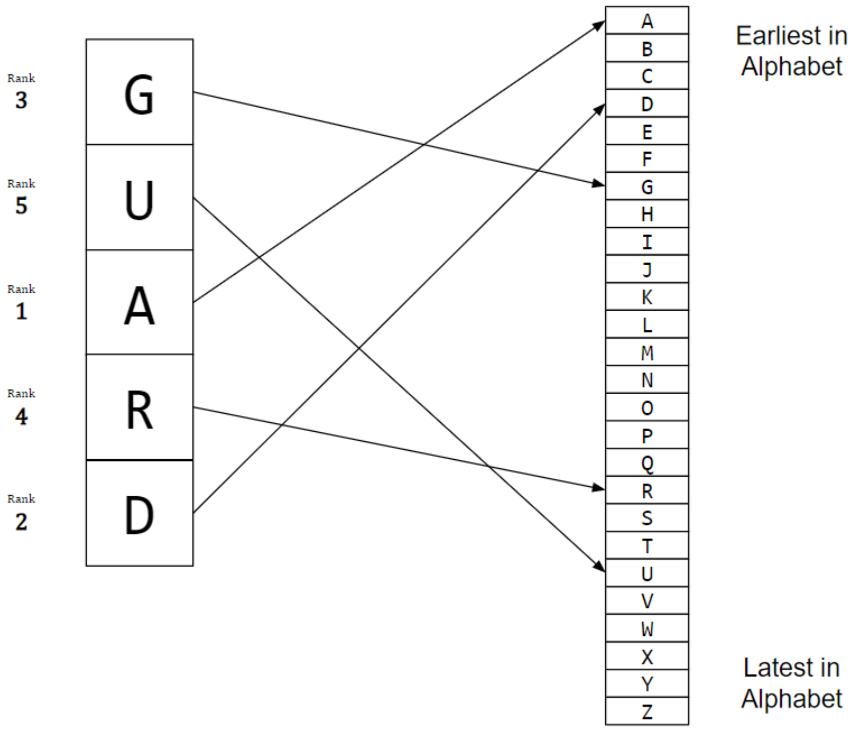
```
HIDET
HEBAB
OONSA
RECOM
INGFO
RYOU
```

We then need to insert some random letters at the end of the message so every row has an equal number of letters. Let's use Q:

```
HIDET
HEBAB
OONSA
RECOM
INGFO
RYOUQ
```

Now, we begin the **encryption** process by rearranging the letters in each row based on the alphabetical ranking of the letters of the keyword GUARD.

[2] In this course, we won't consider words with repeat letters.



We note that the alphabetical rankings of the letters of this keyword are 3, 5, 1, 4, 2. We can see this as a *permutation*; that is,

$$1 \mapsto 3 \qquad 2 \mapsto 5 \qquad 3 \mapsto 1 \qquad 4 \mapsto 4 \qquad 5 \mapsto 2$$

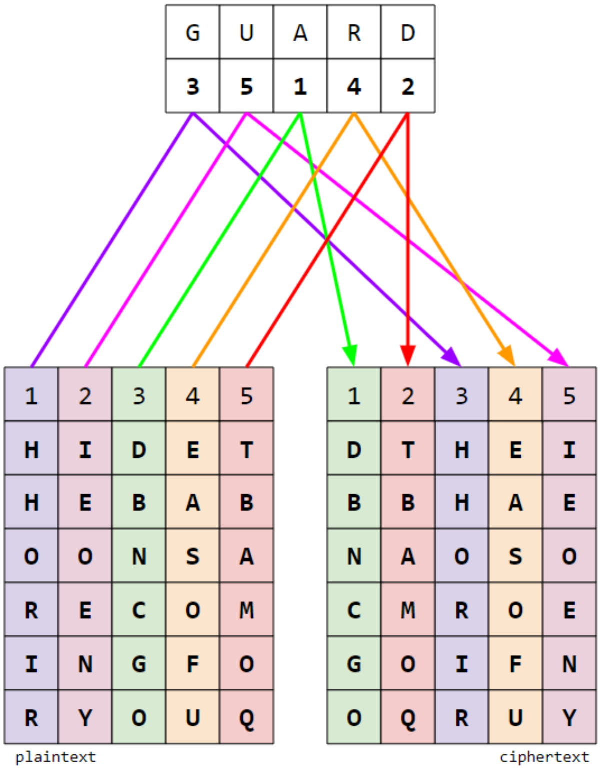
The idea for encryption is that, for each column i, we'll send that column to whatever is mapped by the permutation above. Going back to the stack of letters we have, we can label each individual column:

```
plaintext
position    1 2 3 4 5
            H I D E T
            H E B A B
            O O N S A
            R E C O M
            I N G F O
            R Y O U Q
```

The idea is that

- we can put all letters under position 1 in the plaintext stack to position **3** of the ciphertext stack,
- we can put all letters under position 2 in the plaintext stack to position **5** of the ciphertext stack,
- we can put all letters under position 3 in the plaintext stack to position **1** of the ciphertext stack,
- we can put all letters under position 4 in the plaintext stack to position **4** of the ciphertext stack,
- we can put all letters under position 5 in the plaintext stack to position **2** of the ciphertext stack.

The process, visually, would look like:



1	2	3	4	5
H	I	D	E	T
H	E	B	A	B
O	O	N	S	A
R	E	C	O	M
I	N	G	F	O
R	Y	O	U	Q

1	2	3	4	5
D	T	H	E	I
B	B	H	A	E
N	A	O	S	O
C	M	R	O	E
G	O	I	F	N
O	Q	R	U	Y

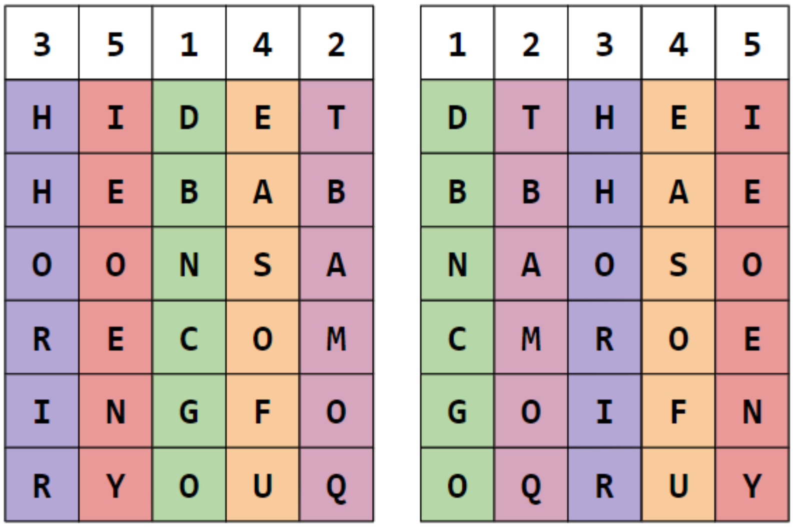
Therefore, the ciphertext stack would look like:

```
DTHEI
BBHAE
NAOSO
CMROE
GOIFN
OQRUY
```

Undoing the stacking gives us the ciphertext:

```
DTHEIBBHAENAOSOCMROEGOIFNOQRUY
```

Remark: An easy way to run through the process is to create two "groups," side-by-side. The first group will be the plaintext stack, and the second group will be the ciphertext text. Then, label each column of the first group with the **alphabetical ranking** of the keyword. Label each column of the second group with **12345**. Finally, map each column from the first group to the second group based on the label.



3	5	1	4	2
H	I	D	E	T
H	E	B	A	B
O	O	N	S	A
R	E	C	O	M
I	N	G	F	O
R	Y	O	U	Q

plaintext

1	2	3	4	5
D	T	H	E	I
B	B	H	A	E
N	A	O	S	O
C	M	R	O	E
G	O	I	F	N
O	Q	R	U	Y

ciphertext

Decrypting is merely the inverse of the encryption process.

(Example: Decryption.) Consider the above example again. Suppose Alice successfully sends the following ciphertext to Bob:

```
DTHEIBBHAENAOSOCMROEGOIFNOQRUY
```

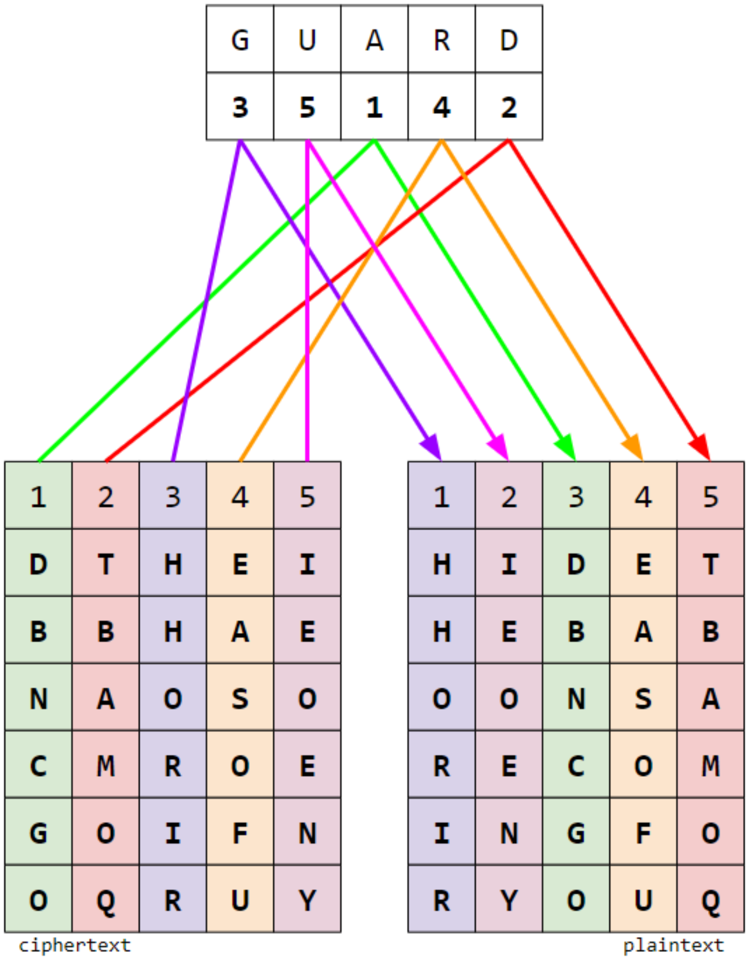
Bob knows that the keyword is `GUARD`. He can use this keyword to decrypt the message. He can begin by taking the letters of the ciphertext and stacking them into rows of 5, since `GUARD` has 5 letters:

```
DTHEI
BBHAE
NAOSO
CMROE
GOIFN
OQRUY
```

Bob also knows the alphabetical ranking of the letters of `GUARD` (which is the same rankings as described above). In particular, the alphabetical ranking is `35142`. So, we need to do the following:

- The letters in position 1 of the ciphertext stack needs to be moved to position **3**,
- the letters in position 2 of the ciphertext stack needs to be moved to position **5**,
- the letters in position 3 of the ciphertext stack needs to be moved to position **1**,
- the letters in position 4 of the ciphertext stack needs to be moved to position **4**,
- the letters in position 5 of the ciphertext stack needs to be moved to position **2**.

The process, visually, would look like:



G	U	A	R	D
3	**5**	**1**	**4**	**2**

1	2	3	4	5
D	T	H	E	I
B	B	H	A	E
N	A	O	S	O
C	M	R	O	E
G	O	I	F	N
O	Q	R	U	Y

`ciphertext`

1	2	3	4	5
H	I	D	E	T
H	E	B	A	B
O	O	N	S	A
R	E	C	O	M
I	N	G	F	O
R	Y	O	U	Q

`plaintext`

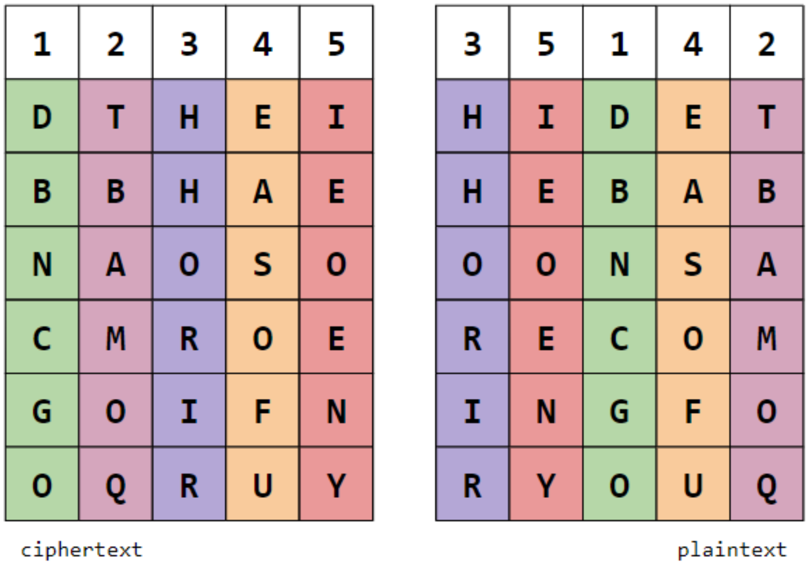
Undoing the stacking gives us:

```
HIDETHEBABOONSARECOMINGFORYOUQ
```

At this point, Bob needs to make an educated guess as to what the encoded message says (recall that we had to encode the message before encrypting it). By removing the `Q` and correctly punctuating the message, we get

```
Hide! The baboons are coming for you.
```

Remark: We can easily decrypt an encrypted word by doing the inverse of what we did above. Create two "groups," side-by-side. The first group will be the ciphertext stack, and the second group will be the plaintext text. Then, label each column of the first group with **12345**. Label each column of the second group with the **alphabetical ranking** of the keyword. Finally, map each column from the first group to the second group based on the label.



1	2	3	4	5
D	T	H	E	I
B	B	H	A	E
N	A	O	S	O
C	M	R	O	E
G	O	I	F	N
O	Q	R	U	Y

ciphertext

3	5	1	4	2
H	I	D	E	T
H	E	B	A	B
O	O	N	S	A
R	E	C	O	M
I	N	G	F	O
R	Y	O	U	Q

plaintext

(Exercise: Encryption.) *Encrypt the message* `There is always hope.` *using the keyword* `CRASH`*.*

First, we encode the message so that we can easily encrypt it:

```
THEREISALWAYSHOPE
```

Noting that `CRASH` has length 5, we break the now encoded message into groups of 5 letters (5-grams):

```
THERE
ISALW
AYSHO
PE
```

Let's now add nonsense letters at the end of the last row so every row has 5 letters:

```
THERE
ISALW
AYSHO
PEABC
```

Now, we note the alphabetical ranking of each letter in `CRASH`:

$$C \mapsto 2 \quad R \mapsto 4 \quad A \mapsto 1 \quad S \mapsto 5 \quad H \mapsto 3.$$

Using the streamlined way discussed above, we have

```
2 4 1 5 3 | 1 2 3 4 5
T H E R E | E T E H R
I S A L W | A I W S L
A Y S H O | S A O Y H
P E A B C | A P C E B
```

Unstacking the new rows gives us the ciphertext:

```
ETEHRAIWSLSAOYHAPCEB
```

(Exercise: Decryption.) *Decrypt the message* `ETIHGFREAFRSLAESOXOE` *using the keyword* `CRASH`*.*

Begin by grouping the letters into 5-grams, since `CRASH` has length 5:

```
ETIHG
FREAF
RSLAE
SOXOE
```

Recall that the alphabetical ranking of each letter in `CRASH` is `24153`. Using the streamlined way discussed above, we have

```
1 2 3 4 5    2 4 1 5 3
E T I H G -> T H E G I
F R E A F -> R A F F E
R S L A E -> S A R E L
S O X O E -> O O S E X
```

Unstacking the new rows gives us the plaintext:

```
THEGIRAFFESARELOOSEX
```

Decoding the message gives us:

```
The giraffes are loose.
```

(Exercise.) Encrypt the message `Meet at the trolley station.` using keyword `UCSD`.

Encoding, grouping the resulting letters into groups of 4, and adding a nonsense letter gives us:

```
MEET
ATTH
ETRO
LLEY
STAT
IONX
```

Noting that the alphabetical ranking of `UCSD` is `4132`, we can use the streamlined way discussed above to get the encrypted result:

```
4 1 3 2    1 2 3 4
M E E T -> E T E M
A T T H -> T H T A
E T R O -> T O R E
L L E Y -> L Y E L
S T A T -> T T A S
I O N X -> O X N I
```

Unstacking the result gives us:

```
/ETEMTHTATORELYELTTASOXNI
```

(Exercise.) Alice and Bob share the keyword `ZEUS`. Alice uses rectangular tranposition to encrypt the following nonsense message:

```
MTSQAGXY
```

What is the corresponding ciphertext?

Encoding, grouping the resulting letters into groups of 4, and adding a nonsense letter gives us:

```
MTSQ
AGXY
```

Noting that the alphabetical ranking of `ZEUS` is `4132`, we can use the streamlined way discussed above to get the encrypted result:

```
4 1 3 2    1 2 3 4
M T S Q -> T Q S M
A G X Y -> G Y X A
```

Unstacking the result gives us:

```
TQSMGYXA
```

(Exercise.) The following message was encrypted using rectangular transposition with the keyword `SNAKE`. What is the plaintext?

```
        DSUEMSEDIAJQQDA
```

`SNAKE` has alphabetical ranking `54132`. With this in mind, stacking the letters of the encrypted message into groups of 5 and then running the streamlined process gives us:

```
1 2 3 4 5    5 4 1 3 2
D S U E M -> M E D U S
S E D I A -> A I S D E
J Q Q D A -> A D J Q Q
```

Unstacking the result gives us:

```
MEDUSAISDEADJQQ
```

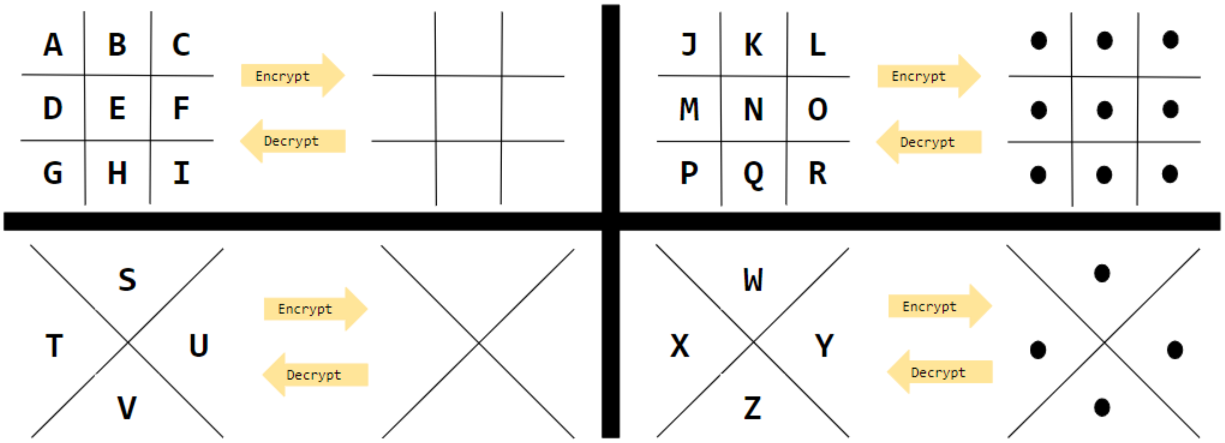
Decoding gives us:

```
Medusa is dead.
```

2.2 Masonic Cipher

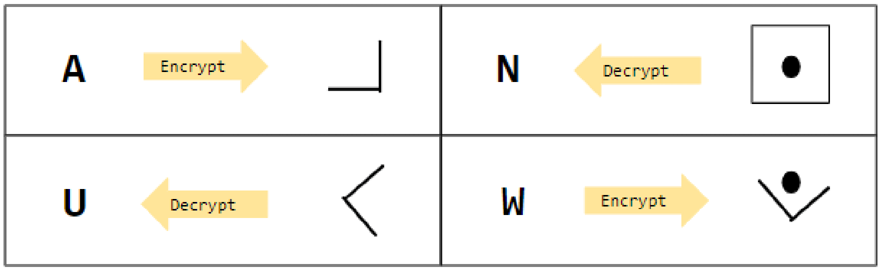
The masonic cipher (also known as the *pigpen cipher* or *tic-tac-toe cipher*) is a simple substitution cipher that replaces individual letters with certain geometric shapes.

For example, consider the following diagram, which represents a Masonic cipher for the English letters:



The idea is that we can replace a letter (e.g., `A`) with a corresponding geometric shape (e.g., the backwards `L` represented by the top-left part of the grid.)

Some other examples based on the above cipher are shown below:



Note that there is *no key* associated with this cipher. There is only a decryption function (which is just mapping the geometric shape back to the letter). Therefore, the adversary, who knows that a message was encrypted using a masonic cipher, can recover the plaintext easily.

2.3 Caesar Cipher

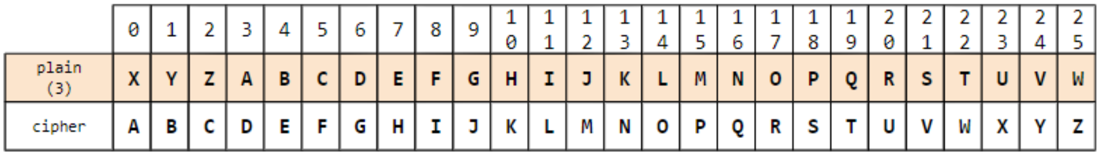
The Caesar cipher, also known as a *shift cipher*, is a simple substitution cipher that *shifts* a letter by some amount n. Hence, the key for this cipher is an integer n. The idea is that we initially assign each letter an integer, perhaps by their alphabetical ranking (e.g., A is 0, B is 1, and so on.) If we want to shift the letters by some number, we can just "move" the letters by that amount. If a letter gets a new integer that's greater than 25, we can "wrap" the letter back.

Consider the following diagram, which shows the correspondence between the plaintext alphabet and the ciphertext alphabet.

	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
plain	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
cipher	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

In this particular diagram, when we apply a shift, we apply the shift to the *plain* row. By doing this, we can translate whatever plaintext we have to ciphertext.

(Example.) If we shift each letter by 3 (i.e., $n = 3$), we have



	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
plain (3)	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
cipher	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

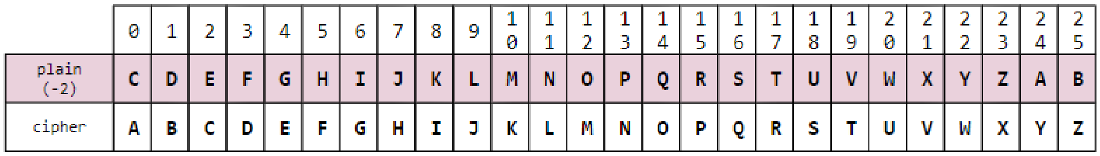
Notice how A now corresponds to 3. Recall that A's original position was 0; if we shift each letter by 3, we essentially add 3 to A's original position to get the new position

$$0 + 3 = 3.$$

The same idea applies to any other letter. One key thing to notice is how X, Y, and Z were *wrapped back* to the beginning. In any case, let's see how translation would work in this case:

- To convert a letter from plaintext to ciphertext, look for the letter in the(shifted) plaintext row and then look at the corresponding ciphertext column. For example, R in plaintext would become U in ciphertext.
- To convert a letter from ciphertext to plaintext, look for the letter in the ciphertext row and then look at the corresponding (shifted) plaintext column. For example, U in ciphertext becomes R in plaintext.

(Example.) If we shift each letter by -2 (i.e., $n = -2$), we have



	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
plain (-2)	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
cipher	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

As with rectangular tranposition, we should encode the message by removing any non-alphabetic characters and capitalizing everything.

(Exercise.)

- *Using a shift of 3, encrypt the message* `Meet at La Jolla Shores.`

Encoding the message gives us `MEETATLAJOLLASHORES`. Then, we can use the example above (with the shift of 3) to give us the proper correspondence.

```
plain     M E E T A T L A J O L L A S H O R E S
cipher    P H H W D W O D M R O O D V K R U H V
```

This gives us `PHHWDWODMROODVKRUHV`.

- *Using a shift of 3, decrypt the message* ***PHHWDWVXQJRGODZQ***

Using the example above (with the shift of 3), we have

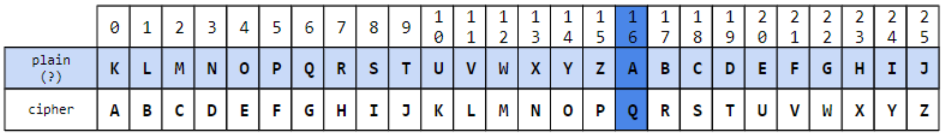
```
cipher     P H H W D W V X Q J R G O D Z Q
plain      M E E T A T S U N G O D L A W N
```

Decoding this gives us `Meet at Sun God Lawn.`

(Exercise.) *You are Eve. You have just intercepted the following message that Alice was trying to send to Bob:* `Q TQDM IB QPWCAM`*. You know that Alice used a Caesar cipher, but she didn't remove spaces before encrypting: she left the spaces in her original message as-is. What is the original message?*

`Q` itself could be a word; specifically, it could either be `A` or `I`. We can try to figure out what the message by guessing which word the first word could be.

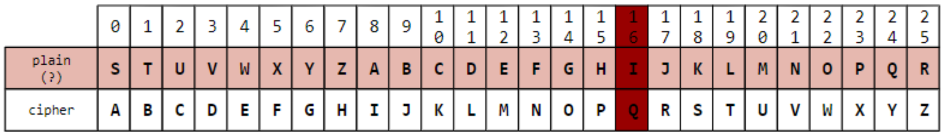
- If `Q` maps to `A`, then we have



	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
plain (?)	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
cipher	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

  Partially decrypting the ciphertext gives us `A DANW`, but `DANW` is meaningless. Therefore, it cannot be `A`.

- If `Q` maps to `I`, then we have



	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
plain (?)	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
cipher	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

  Decrypting this gives us:

  `I LIVE AT IHOUSE`

Therefore, the message is `I LIVE AT IHOUSE`. The shift was 8.

(Exercise.) Alice encrypts the following message using a Caesar cipher with a shift of 1.

`Zeus is hiding in a cave`

What is the corresponding ciphertext?

```
plain     ZEUSISHIDINGINACAVE
cipher    AFVTJTIJEJOHJOBDBWF
```

Essentially, we just move all letters forward by 1.

2.4 Interlude: Modular Arithmetic

One fundamental idea in number theory, which is used in cryptography, is modular arithmetic.

2.4.1 Quotients and Remainders

Lemma 2.1: Euclid's Division

For any integer a and positive integer n, there exists a unique pair of integers q and r such that $0 \leq r < n$ and $a = qn + r$. The integers q and r are called the quotient and remainder, respectively. We also write $a \pmod{n}$ to refer to the remainder.

For the proof, the deal is that we can keep subtracting, or adding, n from a until we end up in the range $[0, n)$. Therefore, the number of times we had to subtract, or add, n is the *quotient*, and the number in the range $[0, n)$ that we end up with at the end is the *remainder*.

(Example.) Divide $a = 17$ by $n = 5$. Find the quotient and remainder.

Using the proof idea, we note that:

- Subtracting 5 to a once gives us 12.
- Subtracting 5 to a twice gives us 7.
- Subtracting 5 to a thrice gives us 2.

It took us 3 subtractions to get to a number that's in the range $[0, 5)$, so the quotient is $\boxed{3}$ and the remainder is $\boxed{2}$.

We should note that this is pretty standard when $a \geq 0$. However, for $a < 0$, it might be less familiar, albeit the same process.

(Example.) Divide $a = -7$ by $n = 5$. Find the quotient and remainder.

Using the proof idea, we note that:

- Adding 5 to a once gives us 2.
- Adding 5 to a twice gives us 3.

It took us 2 additions to get to a number that's in the range $[0, 5)$, so the quotient is $\boxed{-2}$ (because we had to *add*, not subtract) and the remainder is $\boxed{3}$.

Remark:

- If we have to **add** n to a x times to get a number that's in the range $[0, n)$, then our final quotient will be negative (that is, $-x$).
- If we have to **subtract** n from a x times to get a number that's in the range $[0, n)$, then our final quotient will be positive (that is, x).

(Exercise.) For each of the following, calculate the quotient and remainder when a is divided by n. Do these calculations by hand.

- $a = 13$, $n = 3$.

  We know that $13/3 = 4$, and $13 - (3 \cdot 4) = 1 \in [0, 3)$. So, the quotient is $\boxed{4}$ and the remainder is $\boxed{1}$.

- $a = 134$, $n = 10$.

We know that $134/10 = 13$ and $134 - (10 \cdot 13) = 4 \in [0, 10)$. So, the quotient is $\boxed{13}$ and remainder is $\boxed{4}$.

- $a = -37$, $n = 10$.

We know that we need to add n to a **4** times to get a number, 3, that is in the range $[0, 10)$. To be precise,

$$-37 + 10 + 10 + 10 + 10 = -37 + 40 = 3 \in [0, 10).$$

Therefore, the quotient is $\boxed{-4}$ and the remainder is $\boxed{3}$.

- $a = -15$, $n = 60$.

We have to add n to a **1** time to get $45 \in [0, 60)$. Therefore, the quotient is $\boxed{-1}$ and the remainder is $\boxed{45}$.

- $a = 13$, $n = 12$.

We know that $13/12 = 1$ and $13 - (12 \cdot 1) = 1$. So, the quotient is $\boxed{1}$ and the remainder is $\boxed{1}$.

(Exercise.) What is $-13 \pmod 5$?

$$-13 + 5 + 5 + 5 = 2 \in [0, 5),$$

so the quotient is -3 (since we had to perform 3 additions) and the remainder is $\boxed{2}$. Therefore,

$$-13 \pmod 5 = 2.$$

Proposition. *Suppose a and n are integers and $n > 0$. All the following statements are equivalent:*

- $a \pmod n = 0$.
- *There is no remainder when a is divided by n.*
- *a is a multiple of n.*
- *a is divisible by n.*
- *n is a divisor of a.*
- *n is a factor of a.*
- *n divides a (in notation[3]: $n|a$).*
- *a/n is an integer.*

[3] Note that $|$ is read as "*divides*."

2.4.2 Congruences

Definition 2.2: Congruence

Fix a positive integer n. If a and b are integers, we say that "a is **congruent** to b mod n," or that "a and b are congruent mod n," if a and b have the same remainder when each is divided by n. This can be denoted in symbols as follows:

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

For example, $19 \equiv 7 \pmod{4}$ since 19 and 7 both have remainder 3 when divided by 4. Observe also that $19 - 7 = 12$ is a multiple of 4. This can be generalized:

Lemma 2.2

Fix a positive integer n. Two integers a and b are congruent mod n if and only if $a - b$ is a multiple of n.

Proof. Divide a and b by n to write $a = q_1 n + r_1$ and $b = q_2 n + r_2$. If

$$a \equiv b \pmod{n},$$

this by definition means that $r_1 = r_2$ so

$$a - b = (q_1 n + r_1) - (q_2 n + r_2) = q_1 n - q_2 n = n(q_1 - q_2).$$

So, $a - b$ is a multiple of n. Conversely, suppose $a - b$ is a multiple of n. Then,

$$(a - b) - (q_1 - q_2)n = ((q_1 n + r_1) - (q_2 n + r_2)) - (q_1 - q_2)n = r_1 - r_2$$

is a multiple of n. Since $0 \le r_1, r_2 < n$, however, we must have $|r_1 - r_2| < n$. The only way that $r_1 - r_2$ can be a multiple of n is if $r_1 - r_2 = 0$, i.e., if $r_1 = r_2$. That means $a \equiv b \pmod{n}$. □

Theorem 2.1: Modular Arithmetic Theorem

Fix a positive integer n. Suppose a, a', b, b' are integers such that

$$a \equiv a' \pmod{n}$$

$$b \equiv b' \pmod{n}$$

and k is any positive integer. Then, all of the following are also true:

$$a + b \equiv a' + b' \pmod{n}$$

$$a - b \equiv a' - b' \pmod{n}$$

$$ab \equiv a'b' \pmod{n}$$

$$a^k \equiv (a')^k \pmod{n}$$

(Exercise.) Use the Modular Arithmetic Theorem to quickly calculate the following.

- $417 \cdot 22 \pmod{10}$.

$$\begin{aligned} 417 \cdot 22 &\equiv 7 \cdot 2 \\ &= 14 \\ &\equiv 4 \pmod{10}. \end{aligned}$$

- $333333 + 666 \pmod 3$.

$$\begin{aligned} 333333 + 666 &\equiv 0 + 0 \\ &\equiv 0 \pmod 3. \end{aligned}$$

- $7^{202320232023} \pmod 6$.

$$\begin{aligned} 7^{202320232023} &= 7 \cdot 7 \cdot \ldots \cdot 7 \\ &\equiv 1 \cdot 1 \cdot \ldots \cdot 1 \\ &= 1 \pmod 6. \end{aligned}$$

- What is $5^{2023202320232023} \pmod 6$?

$$\begin{aligned} 5^{2023202320232023} &= 5 \cdot 5 \cdot \ldots \cdot 5 \\ &\equiv (-1) \cdot (-1) \cdot \ldots \cdot (-1) \\ &= (-1)^{2023202320232023} \\ &\equiv -1 \\ &\equiv 5 \pmod 6. \end{aligned}$$

Therefore, the answer is $\boxed{5}$.

(Exercise.) Fix positive integers k and n. Suppose a and a' are integers such that $a \equiv a' \pmod n$. It is not true in general that $k^a \equiv k^{a'} \pmod n$. Show this by example: in other words, find k, n, a, and a' such that $a \equiv a' \pmod n$ but $k^a \not\equiv k^{a'} \pmod n$.

Let $k = 2$, $n = 5$, $a = 6$, and $a' = 1$ so that

$$6 \equiv 1 \pmod 5.$$

Then, we note that

$$k^a = 2^6 = 64$$

and

$$k^{a'} = 2^1 = 2.$$

From this, it's clear that

$$64 \not\equiv 2 \pmod 5.$$

(Exercise.) *Suppose that the number $273x49y5$, where x and y are unknown digits, is divisible by 495. Find x and y.*

We are asked to solve

$$273x49y5 \equiv 0 \mod 495.$$

We can write $273x49y5$ as

$$20000000 + 7000000 + 300000 + 10000x + 4000 + 900 + 10000y + 5.$$

With this in mind, we have

$$\begin{aligned} &20000000 + 7000000 + 300000 + 10000x + 4000 + 900 + 10y + 5 \\ &\equiv 20 + 205 + 30 + 100x + 40 + 405 + 10y + 5 \\ &= 705 + 100x + 10y \\ &\equiv 210 + 100x + 10y \mod 495. \end{aligned}$$

We note that the next multiple of 495 is 990. So, effectively, we want to find some x and y such that $0 \leq x < 10$ and $0 \leq y < 10$ and

$$210 + 100x + 10y = 990.$$

This gives us

$$100x + 10y = 780.$$

One obvious solution is $x = 7$ and $y = 8$.

2.4.3 Revisiting the Caesar Cipher

Suppose we identify the letters A through Z with the numbers 0 through 25. In other words, we have $A \mapsto 0$, $B \mapsto 1$, and so on. Suppose we want to apply the Caesar cipher with a shift of 5 to encrypt the letter Y. Consider the following

$$E(x) = (x + 5) \text{ (mod 26)}.$$

We note that Y corresponds to the number 24. Then, it follows that

$$E(24) = (24 + 5) \text{ (mod 26)} = 29 \text{ (mod 26)} = 3.$$

The number 3 corresponds to the letter D, the desired result. In other words, if we can identify the letters with numbers, the function E is the encryption function of the Caesar cipher with a shift of 5.

The decryption function is given by

$$D(y) = (y - 5) \text{ (mod 26)}.$$

So, if we wanted to decrypt the letter D, which corresponds to the number 3, then

$$D(3) = (3 - 5) \text{ (mod 26)} = -2 \text{ (mod 26)} = 24,$$

which corresponds to Y.

What we just did is actually a consequence of the Modular Arithmetic Theorem; for a quick little "proof," notice how

$$\begin{aligned} D(E(x)) &= D(y) \\ &\equiv (y - 5) \text{ (mod 26)} \\ &\equiv ((x + 5) - 5) \text{ (mod 26)} \\ &= x. \end{aligned}$$

(Exercise.) Decipher the message below, which was encrypted using a Caesar cipher with a shift of 3 and then using a rectangular transposition with the keyword `EARLY`.

```
DKSSBUIGLDEBXOX
```

To decrypt this message, we need to work backwards: first, use rectangular transposition to undo the first encryption, and then Caesar cipher to undo the second encryption.

1. For the rectangular transposition, note that the keyword has alphabetical ranking `21435`, so using the streamlined way discussed earlier, we have

   ```
   12345    21435
   DKSSB -> KDSSB
   UIGLD -> IULGD
   EBXOX -> BEOXX
   ```

   Unstacking gives us `KDSSBIULGDBEOXX`.

2. Next, we need to undo the Caesar cipher encryption on the message that we found from the previous step. Since the encryption used a positive shift of 3, undoing it requires us to use a negative shift of 3. This gives us:

   ```
   encrypted   KDSSBIULGDBEOXX
   decrypted   HAPPYFRIDAY....
   ```

   Note that the last four letters were omitted. In any case, this gives us the decoded message `Happy Friday`.

Remark: You should not assume that these operations are commutative. That is, if we were to decrypt the message by applying the Caesar cipher first and then the rectangular transposition, as opposed to the reverse order, we may get a different answer!

2.5 Interlude: GCDs

Definition 2.3: Greatest Common Divisor

The **greatest common divisor** (or *GCD*) of two integers a and b that are not both zero is denoted $\gcd(a, b)$ and is defined to be the largest integer which is both a divisor of a and a divisor of b.

(Example.) Suppose we wanted to compute $\gcd(14, 21)$.

- The factors of 14 are 1, 2, 7, and 14.
- The factors of 21 are 1, 3, 7, and 21.

Therefore, as 7 is the *largest integer* which is both a divisor of 14 and 21, it follows that $\gcd(14, 21) = 7$.

Note that, while intuitive, this is actually not the best way of finding GCDs. Finding the factors of a number, especially a large one, is difficult. However, there exists algorithms that we can use to quickly calculate GCDs.

(Example.) Suppose a is a nonzero integer. What is $\gcd(a, 0)$?

The answer is $\gcd(a, 0) = |a|$. To see why this is the case, consider the following points.

1. If $a \neq 0$, the largest value that divides a is $|a|$.

   For example, the largest value that divides 100 is $|100| = 100$. Likewise, the largest value that divides -100 is still $|-100| = 100$.

2. If you think about it, all integers divide 0.

   Recall that, if a and b are integers, a divides b if there is an integer c such that

   $$ac = b.$$

   Here, we write that $a|b$ to mean that a divides b.

   With this in mind, we note that

   $$a \cdot 0 = 0$$

   and therefore

   $$a|0.$$

3. Therefore, it follows that $\gcd(a, 0) = |a|$.

   To see this, note that the factors of 10 and -10 are

   $$\{-10, -5, -2, -1, 1, 2, 5, 10\},$$

   and we know that all factors of 0 are effectively all integers. Therefore, it follows that 10 would be the answer here.

2.5.1 Euclidean Algorithm

The Euclidean Algorithm for computing GCDs relies on the following observation, defined as a lemma.

Lemma 2.3

Let n be a positive integer and $a \equiv b \pmod{n}$. Then, $\gcd(a, n) = \gcd(b, n)$.

Proof. Let $c = \gcd(a, n)$ and $d = \gcd(b, n)$. Let k be an integer such that

$$a - b = nk.$$

Since c is a factor of both a and n, it is also a factor of $a - nk = b$. Thus, c is a common factor of both b and n as well, so $c \leq d$ bby definition of d. On the other hand, the same logic shows that d is a common factor of both a and n, so $d \leq c$ and thus $d = c$. □

Corollary 2.1

Let n be a positive integer and let r be the remainder when an integer a is divided by n. Then, $\gcd(a, n) = \gcd(r, n)$.

This brings us to the Euclidean Algorithm:

Suppose a and b are two positive integers, and assume without loss of generality (WLOG) that $b \geq a$. To find $\gcd(a, b)$, we can do the following:

- Divide b by a and let r be the remainder. Then,
  - If $r = 0$, output a.
  - Otherwise, replace b with a and a with r. Then, repeat.

(Example.) Suppose we wanted to compute $\gcd(115, 35)$. We divide the bigger number by the smaller one and get

$$115 = 3 \cdot 35 + 10.$$

The remainder, $r = 10$, is nonzero, so we'll divide again, but this time, we'll divide the dividend (35) by the remainder (10) to get

$$35 = 3 \cdot 10 + 5.$$

The remainder is nonzero again, so we repeat to get

$$10 = 2 \cdot 5 + 0.$$

Since the remainder is 0, we output the dividend: $\boxed{5}$. Therefore,

$$\gcd(115, 35) = 5.$$

(Exercise.) Compute the following GCDs using the Euclidean Algorithm.

- $\gcd(180, 120)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
120	180	$180 = 120q + r$	1	60
60	120	$120 = 60q + r$	2	0

Therefore, the answer must be $\boxed{60}$.

- $\gcd(180, 81)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
81	180	$180 = 81q + r$	2	18
18	81	$81 = 18q + r$	4	9
9	18	$18 = 9q + r$	2	0

Therefore, the answer must be $\boxed{9}$.

- $\gcd(121, 77)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
77	121	$121 = 77q + r$	1	44
44	77	$77 = 44q + r$	1	33
33	44	$44 = 33q + r$	1	11
11	33	$33 = 11q + r$	3	0

Therefore, the answer must be $\boxed{11}$.

2.5.2 Bezout's Theorem

Theorem 2.2: Bezout's Theorem

Suppose a and b are integers not both 0. Then, $\gcd(a, b)$ can be written as an *integer linear combination* of a and b, i.e., it can be written as $ax + by$ for some integers x and y. Integers x and y such that

$$\gcd(a, b) = ax + by$$

are called **Bezout's coefficients**.

We can use the Euclidean Algorithm to find the Bezout coefficients, as seen in the example below.

(Example.) Suppose we want to find the Bezout coefficients for $\gcd(115, 35)$. Recall the sequence of operations we had to do:

$$115 = 3 \cdot 35 + 10.$$

$$35 = 3 \cdot 10 + 5.$$

$$10 = 2 \cdot 5 + 0.$$

Suppose we rearrange the first and second equations, like so:

$$10 = 115 - 3 \cdot 35.$$

$$5 = 35 - 3 \cdot 10.$$

Plugging in the first equation into the second equation gives us

$$5 = 35 - 3 \cdot (115 - 3 \cdot 35).$$

Simplifying this gives us

$$\begin{aligned} 5 &= 35 - 3 \cdot (115 - 3 \cdot 35) \\ &= 35 - 3(115) + 9(35) \\ &= 10(35) - 3(115). \end{aligned}$$

Notice how we wrote $\gcd(115, 35)$ as an integer linear combination of those two numbers.

Essentially, the steps are as follows:

1. Find the GCD using the Euclidean Algorithm.
2. Rewrite the division for the *last nonzero remainder*.
3. Alternate between substitution for the remainder directly above, and then simplify. Alternatively, start from the last equation with a nonzero remainder and then keep using the equations before that equation (e.g., from equation n, the last equation with a nonzero remainder, substitute equation $n - 1$ in the next step. Then, in the next step, substitute equation $n - 2$. Keep doing this until you reach equation 1.)

(Example.) Suppose we want to find the Bezout coefficients for $\gcd(240, 46)$.

1. First, let's compute the GCD, keeping note of the sequence of operations we made.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
46	240	$240 = 46q + r$	5	10
10	46	$46 = 10q + r$	4	6
6	10	$10 = 6q + r$	1	4
4	6	$6 = 4q + r$	1	2
2	4	$4 = 2q + r$	2	0

This tells us that $\gcd(240, 46) = 2$. The operations we did were

- (Eq. 1) $240 = 46(5) + 10 \implies 10 = 240 - 46 \cdot 5$
- (Eq. 2) $46 = 10(4) + 6 \implies 6 = 46 - 10 \cdot 4$
- (Eq. 3) $10 = 6(1) + 4 \implies 4 = 10 - 6 \cdot 1$
- (Eq. 4) $6 = 4(1) + 2 \implies 2 = 6 - 4 \cdot 1$
- (Eq. 5) $4 = 2(2) + 0$

2. Rewriting the division for the last equation with the nonzero remainder (Eq. 4) gives us $2 = 6-4\cdot 1$.

3. Starting from the division for the last nonzero remainder, let's rewrite it:

$$\begin{aligned}
2 &= 6 - 4 \cdot 1 && \text{From Eq. 4} \\
&= 6 - (\underbrace{10 - 6 \cdot 1}_{\text{Eq. 3}}) \cdot 1 && \text{Substitute Eq. 3} \\
&= 6 - 10 + 6 && \text{Expand} \\
&= 2 \cdot 6 - 1 \cdot 10 && \text{Rewrite to group like terms} \\
&= 2 \cdot (\underbrace{46 - 10 \cdot 4}_{\text{Eq. 2}}) - 1 \cdot 10 && \text{Substitute Eq. 2} \\
&= 2 \cdot 46 - 2 \cdot 10 \cdot 4 - 1 \cdot 10 && \text{Expand} \\
&= 2 \cdot 46 - 8 \cdot 10 - 1 \cdot 10 && \text{Simplify} \\
&= 2 \cdot 46 - 9 \cdot 10 && \text{Rewrite to group like terms} \\
&= 2 \cdot 46 - 9 \cdot (\underbrace{240 - 46 \cdot 5}_{\text{Eq. 1}}) && \text{Substitute Eq. 1} \\
&= 2 \cdot 46 - 9 \cdot 240 + 46 \cdot 5 \cdot 9 && \text{Expand} \\
&= 2 \cdot 46 - 9 \cdot 240 + 46 \cdot 45 && \text{Simplify} \\
&= 47 \cdot 46 - 9 \cdot 240 && \text{Rewrite to group like terms}
\end{aligned}$$

Notice how the Bezout coefficients are 47 and -9.

(Exercise.) Calculate Bezout's coefficients for the following GCDs using the extended Euclidean Algorithm.

- $\gcd(180, 120)$.

1. First, compute the GCD. We already did this in a previous exercise, but just to reiterate:

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
120	180	$180 = 120q + r$	1	60
60	120	$120 = 60q + r$	2	0

   Therefore, the GCD is 60. The operations that we did were

   - (Eq. 1) $180 = 120(1) + 60 \implies 60 = 180 - 120(1)$
   - (Eq. 2) $120 = 60(2) + 0$

2. Next, we just need to rewrite the last equation with a nonzero remainder.

$$180 = 120(1) + 60 \implies 60 = 180 - 120(1)$$

3. Finally, we need to work backwards, substituting the previous equations. Because we only have one operation which resulted in a non-zero remainder, it follows that we only need to do:

$$60 = 180 - 120(1).$$

   Therefore, the Bezout coefficients are $\boxed{1}$ and $\boxed{-1}$.

- $\gcd(180, 81)$.

1. First, we need to compute the GCD. We already did this in a previous exercise, but to reiterate:

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
81	180	$180 = 81q + r$	2	18
18	81	$81 = 18q + r$	4	9
9	18	$18 = 9q + r$	2	0

   Therefore, the GCD is 9. The operations we did were

   - (Eq. 1) $180 = 81(2) + 18 \implies 18 = 180 - 81(2)$
   - (Eq. 2) $81 = 18(4) + 9 \implies 9 = 81 - 18(4)$
   - (Eq. 3) $18 = 9(2) + 0$

2. Next, we need to rewrite the last equation with a nonzero remainder.

$$81 = 18(4) + 9 \implies 9 = 81 - 18(4).$$

3. Finally, we need to work backwards, substituting the previous equations as needed.

$$\begin{aligned} 9 &= 81 - 18(4) \\ &= 81 - \underbrace{(180 - 81(2))}_{\text{Eq. 1}} \cdot 4 \\ &= 81 - 180(4) + 81(8) \\ &= 81(9) - 180(4) \end{aligned}$$

   Therefore, the Bezout coefficients are $\boxed{9}$ and $\boxed{-4}$.

- $\gcd(121, 77)$.

1. First, compute the GCD. To reiterate:

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
77	121	$121 = 77q + r$	1	44
44	77	$77 = 44q + r$	1	33
33	44	$44 = 33q + r$	1	11
11	33	$33 = 11q + r$	3	0

   Therefore, the GCD is 11. The operations that we did were

   - (Eq. 1) $121 = 77(1) + 44 \implies 44 = 121 - 77(1)$
   - (Eq. 2) $77 = 44(1) + 33 \implies 33 = 77 - 44(1)$
   - (Eq. 3) $44 = 33(1) + 11 \implies 11 = 44 - 33(1)$
   - (Eq. 4) $33 = 11(3) + 0$

2. Next, rewrite the last equation with a nonzero remainder.

$$44 = 33(1) + 11 \implies 11 = 44 - 33(1).$$

3. Finally, work backwards.

$$\begin{aligned} 11 &= 44 - 33(1) \\ &= 44 - \underbrace{(77 - 44(1))}_{\text{Eq. 2}} \cdot 1 \\ &= 44 - 77 + 44(1) \\ &= 44(2) - 77 \\ &= \underbrace{(121 - 77(1))}_{\text{Eq. 1}} \cdot 2 - 77 \\ &= 121(2) - 77(2) - 77 \\ &= 121(2) - 77(3). \end{aligned}$$

   Thereforem the Bezout coefficients are $\boxed{2}$ and $\boxed{-3}$.

(Exercise.) Observe that $\gcd(42, 12) = 6$. Show that the pairs $(-1, 4)$ and $(1, -3)$ are both Bezout coefficients for 42 and 12.

- For the pair $(-1, 4)$, we have

$$42(-1) + 12(4) = -42 + 48 = 6.$$

- For the pair $(1, -3)$, we have

$$42(1) + 12(-3) = 42 - 36 = 6.$$

(Exercise.) Consider $\gcd(150, 90)$.

1. How many divisions do we need to do until we see a remainder of 0 when we use the Euclidean algorithm to compute $\gcd(150, 90)$?

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
90	150	$150 = 90q + r$	1	60
60	90	$90 = 60q + r$	1	30
30	60	$60 = 30q + r$	2	0

We had to perform **3** divisions.

2. Find Bezout coefficients for $\gcd(150, 90)$.

Noting that $\gcd(150, 90) = 30$ and the equations we worked with are

- (Eq. 1) $150 = 90(1) + 60 \implies 60 = 150 - 90(1)$
- (Eq. 2) $90 = 60(1) + 30 \implies 30 = 90 - 60(1)$
- (Eq. 3) $60 = 30(2) + 0$

Starting with Eq. 2, we have

$$\begin{aligned} 30 &= 90 - 60(1) \\ &= 90 - \underbrace{(150 - 90(1))}_{\text{Eq. 1}}(1) \\ &= 90 - 150 + 90 \\ &= 90(2) + 150(-1). \end{aligned}$$

So, the Bezout coefficients are $\boxed{2}$ and $\boxed{-1}$.

2.5.3 Modular Inversion

Suppose you are asked to solve the equation

$$5z = 7.$$

Intuitively, we can just divide both sides by 5. Stated differently, we can multiply both sides by $\frac{1}{5}$:

$$\left(\frac{1}{5}\right) \cdot 5z = \left(\frac{1}{5}\right) 7 \implies z = \frac{5}{7}.$$

In other words, we're able to "cancel out" the 5 that appears on the left-hand side, thus isolating z.

With modular inversion, we can recreate this process with *congruences*. For example, suppose we want to solve

$$5z \equiv 7 \pmod{11}.$$

We cannot "divide both sides by 5" because congruences only make sense when both sides of the congruence are *integers*. But, if we find an integer x with the property that

$$5x \equiv 1 \pmod{11},$$

then we can multiply both sides of our congruence by x to effectively eliminate the 5 on the left-hand side. In this example, there *is* an integer: $x = 9$. Using this integer, we have

$$5x = 9 \cdot 5 = 45 \equiv 1 \pmod{11}.$$

Therefore, multiplying both sides of our congruence by 9 gives us

$$z = 1 \cdot z \equiv (5 \cdot 9)z = 9 \cdot (5z) \equiv 9 \cdot 7 \pmod{11}.$$

Thus,

$$z \equiv 9 \cdot 7 = 63 \equiv 8 \pmod{11},$$

and we've solved our congruence: $z \equiv 8 \pmod{11}$. While we solved this congruence, note that we basically guessed what the solution is. However, there's a way to get such x.

Definition 2.4

Fix a positive integer n. An integer a is *invertible* mod n (or a *unit* mod n) if there exists another integer x such that $ax \equiv 1 \pmod{n}$. The number x is then called an *inverse of* a mod n and, in symbols, one writes $x \equiv a^{-1} \pmod{n}$.

So, in the above example, we found that $9 \equiv 5^{-1} \pmod{11}$ because $5 \cdot 9 \equiv 1 \pmod{11}$.

(Exercise.) Explain why 2 is not invertible mod 4.

Essentially, we need to show why there does not exist an integer x such that

$$2x \equiv 1 \pmod{4}.$$

However, notice that both 2 and 4 are even. Therefore, multiplying 2 by any integer gives us an even number. Because 4 is even as well, it follows that we'll never be able to find an x such that $2x \equiv 1 \pmod{4}$.

Theorem 2.3: Modular Inversion Theorem

Fix a positive integer n and another integer a. Then, a is invertible mod n if and only if $\gcd(a, n) = 1$. Moreover, if $\gcd(a, n) = 1$ and x and y are Bezout coefficients for a and n, then x is an inverse of a mod n.

(Example.) Suppose we want to find the inverse of 7 (mod 23). Using the Euclidean Algorithm to compute $\gcd(23, 7)$, we get

$$23 = 3 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0.$$

So, $\gcd(23, 7) = 1$ and thus 7 is in fact invertible mod 23. Working backwards, we find that

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3 \cdot (23 - 3 \cdot 7) \\ &= 10 \cdot 7 - 3 \cdot 23. \end{aligned}$$

Therefore, the Modular Inversion Theorem tells us that 10 is the inverse of 7 mod 23.

(Exercise.) Which of the following integers is invertible mod 210?

(a) 3

(b) 4

(c) 5

(d) None of the above

The answer is **D**. Note that

(a) $\gcd(3, 210) \neq 1$.

(b) $\gcd(4, 210) \neq 1$.

(c) $\gcd(5, 210) \neq 1$.

So, by theorem (2.3), the answer must be D.

(Exercise.) For each of the following, determine whether a is invertible mod n. If it is, find an inverse of a mod n.

- $a = 14, n = 21$.

First, let's calculate $\gcd(14, 21)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
14	21	$21 = 14q + r$	1	7
7	14	$14 = 7q + r$	2	0

Therefore, $\gcd(14, 21) = 7$. By Theorem (2.3), it follows that 14 is not invertible mod 21.

- $a = 3, n = 7$.

First, we calculate $\gcd(3, 7)$.

$\mathbf{a}$	$\mathbf{b}$	$\mathbf{b = aq + r}$	$\mathbf{q}$	$\mathbf{r}$
3	7	$7 = 3q + r$	2	1
1	3	$3 = 1q + r$	3	0

Therefore, $\gcd(3, 7) = 1$. By Theorem (2.3), it follows that 3 is invertible mod 7.

With this in mind, let's find the Bezout coefficients. We note that the equations we used to find the GCD were

- (Eq. 1) $7 = 3(2) + 1 \implies 1 = 7 - 3(2)$
- (Eq. 2) $3 = 1(3) + 0$

Starting with the last equation with a nonzero remainder, which is Eq. 1, we have

$$7 = 3(2) + 1 \implies 1 = 7 - 3(2).$$

Because we are able to write an equation in terms of 3 and 7, we find that

$$\gcd(3, 7) = 1 = 3(-2) + 7(1).$$

From this, it follows that $x = -2$ and $y = 1$. So, by Theorem (2.3), it follows that -2 is an inverse of 3 (mod 7).

We should note that Bezout coefficients are not unique. If we wanted a positive answer, we note that

$$-2 \equiv 5 \pmod 7$$

so that another possible answer is $\boxed{5}$.

- $a = 41, n = 50$.

First, we calculate $\gcd(41, 50)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
41	50	$50 = 41q + r$	1	9
9	41	$41 = 9q + r$	4	5
5	9	$9 = 5q + r$	1	4
4	5	$5 = 4q + r$	1	1
1	4	$4 = 1q + r$	4	0

Therefore, $\gcd(41, 50) = 1$. By Theorem (2.3), it follows that 41 is invertible mod 50.

Next, we need to find the Bezout coefficients. We note that the equations we used to find the GCD were

- (Eq. 1) $50 = 41(1) + 9 \implies 9 = 50 - 41(1)$
- (Eq. 2) $41 = 9(4) + 5 \implies 5 = 41 - 9(4)$
- (Eq. 3) $9 = 5(1) + 4 \implies 4 = 9 - 5(1)$
- (Eq. 4) $5 = 4(1) + 1 \implies 1 = 5 - 4(1)$
- (Eq. 5) $4 = 1(4) + 0$

Now, working backwards from the last equation with a nonzero remainder (i.e., Eq. 4):

$$\begin{aligned}
1 &= 5 - 4(1) \\
&= 5 - \underbrace{(9 - 5(1))}_{\text{Eq. 3}}(1) \\
&= 5 - 9 + 5 \\
&= 5(2) - 9 \\
&= \underbrace{(41 - 9(4))}_{\text{Eq. 2}}(2) - 9 \\
&= 41(2) - 9(4)(2) - 9 \\
&= 41(2) - 9(8) - 9 \\
&= 41(2) - 9(9) \\
&= 41(2) - \underbrace{(50 - 41(1))}_{\text{Eq. 1}}(9) \\
&= 41(2) - 50(9) + 41(9) \\
&= 41(11) - 50(9)
\end{aligned}$$

Therefore, we have

$$\gcd(41, 50) = 1 = 41(11) + 50(-9)$$

and so $x = 11$ and $y = -9$. From this, by Theorem (2.3) it follows that $\boxed{11}$ is an inverse of 41 (mod 50).

(Exercise.) Find an inverse of 54 (mod 131), if possible.

Begin by finding the GCD.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
54	131	$131 = 54q + r$	2	23
23	54	$54 = 23q + r$	2	8
8	23	$23 = 8q + r$	2	7
7	8	$8 = 7q + r$	1	1
1	7	$7 = 1q + r$	7	1

Because $\gcd(54, 131) = 1$, there exists Bezout coefficients and hence an inverse. Note that the equations used to find the GCD were

- (Eq. 1) $131 = 54(2) + 23 \implies 23 = 131 - 54(2)$
- (Eq. 2) $54 = 23(2) + 8 \implies 8 = 54 - 23(2)$
- (Eq. 3) $23 = 8(2) + 7 \implies 7 = 23 - 8(2)$
- (Eq. 4) $8 = 7(1) + 1 \implies 1 = 8 - 7(1)$
- (Eq. 5) $7 = 1(7) + 0$

Starting from Eq. 4 (last operation with a nonzero remainder), we have

$$\begin{aligned}
1 &= 8 - 7(1) \\
&= 8 - (\underbrace{23 - 8(2)})_{\text{Eq. 3}})(1) \\
&= 8 - 23 + 8(2) \\
&= 8(3) - 23 \\
&= (\underbrace{54 - 23(2)}_{\text{Eq. 2}})(3) - 23 \\
&= 54(3) - 23(6) - 23 \\
&= 54(3) - 23(7) \\
&= 54(3) - (\underbrace{131 - 54(2)}_{\text{Eq. 1}})(7) \\
&= 54(3) - 131(7) + 54(14) \\
&= 54(17) - 131(7)
\end{aligned}$$

Therefore, we have

$$\gcd(54, 131) = 54(17) + 131(-7),$$

So, the answer must be 17.

(Exercise.) Solve the following congruences for z.

- $2z \equiv 3 \pmod{11}$

Trivially, $\gcd(2, 11) = 1$. However, let's find the GCD using the Euclidean Algorithm regardless.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
2	11	$11 = 2q + r$	5	1
1	2	$2 = 1q + r$	2	0

Therefore, the GCD is 1. We can now find the Bezout coefficients. Note that the equations used to find the GCD were

- (Eq. 1) $11 = 2(5) + 1$
- (Eq. 2) $2 = 1(2) + 0$

Starting with the last equation with a nonzero remainder, which is Eq. 1, we have

$$1 = 11 - 2(5).$$

Immediately, it follows that

$$\gcd(2, 11) = 1 = 11(1) + 2(-5).$$

Hence, by Theorem (2.3), $x = -5 \equiv 6 \pmod{11}$ is the inverse of $2 \pmod{11}$.

With this in mind, we now know that

$$\begin{aligned} &2z \equiv 3 \pmod{11} \\ &\quad \implies 6(2z) \equiv 6(3) \pmod{11} \\ &\quad \implies 12z \equiv 18 \pmod{11} \\ &\quad \implies z \equiv 7 \pmod{11}. \end{aligned}$$

Therefore, the answer is $z \equiv \boxed{7} \pmod{11}$.

- $3z \equiv 2 \pmod{7}$

Using the strategy of trial-and-error, we find that $z \equiv 3 \pmod{7}$.

- $5z \equiv 3 \pmod{15}$

We note that $\gcd(5, 15) = 5$. Therefore, by Theorem (2.3), there is no solution that satisfies this congruence.

- $5z \equiv 17 \pmod{101}$

First, we want to find $\gcd(5, 101)$. Using the Euclidean Algorithm gives us:

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
5	101	$101 = 5q + r$	20	1
1	5	$5 = 1q + r$	5	0

Therefore, the GCD is 1. We can now find the Bezout coefficients. Note that the equations used to find the GCD were

- (Eq. 1) $101 = 5(20) + 1 \implies 1 = 101 - 5(20)$
- (Eq. 2) $5 = 1(5) + 0$

Starting with the last equation with a nonzero remainder, which is Eq. 1, we have

$$1 = 101 - 5(20).$$

Immediately, it follows that

$$\gcd(5, 101) = 1 = 101(1) + 5(-20).$$

Hence, by Theorem (2.3), $x = -20 \equiv 81 \pmod{11}$ is the inverse of 5 (mod 101).

With this in mind, we now know that

$$\begin{aligned} 5z &\equiv 17 \pmod{101} \\ &\implies 81(5z) \equiv 81(17) \pmod{101} \\ &\implies 405z \equiv 1377 \pmod{101} \\ &\implies z \equiv 64 \pmod{101}. \end{aligned}$$

Therefore, the answer is $z \equiv \boxed{64} \pmod{101}$.

If we use $x = -20$ instead, we have

$$\begin{aligned} 5z &\equiv 17 \pmod{101} \\ &\implies -20(5z) \equiv -20(17) \pmod{101} \\ &\implies -100z \equiv -340 \pmod{101} \\ &\implies z \equiv -340 \pmod{101} \\ &\implies z \equiv 64 \pmod{101}. \end{aligned}$$

So, in summary, given the congruence $az \equiv b \pmod{n}$, the steps for solving for z are as follows:

1. Find $\gcd(a, n)$. If $\gcd(a, n) \neq 1$, then there are no possible solutions.
2. Find the Bezout coefficients for $\gcd(a, n)$. Specifically, for

$$\gcd(a, n) = ax + ny,$$

   find x (the Bezout coefficients for a). This represents your inverse of a (mod n).

3. Multiply both sides of the congruence by x; that is,

$$x(az) \equiv x(b) \pmod{n},$$

   and then simplify.

As you can tell, Bezout coefficients are not unique, and inverses aren't strictly unique either. Notice, for example, that $3(2) \equiv 1 \pmod 5$ and $8(2) \equiv 1 \pmod 5$ so that 8 and 3 are both inverses of 2 (mod 5). However, notice that $8 \equiv 3 \pmod 5$. In other words, inverses are *kind of* unique when they exist: they are unique mod n.

Lemma 2.4

Fix a positive integer n and suppose a is invertible mod n. If x and x' are both inverses of a mod n, then

$$x \equiv x' \pmod n.$$

2.6 Affine Cipher

Recall that the encryption function for the Caesar cipher is given by

$$E(x) = (x + b) \pmod{26},$$

where $b = 0, 1, 2, \dots, 25$ is the shift. Here, x represents the number associated with the letter (e.g., A is 0, B = 1, C = 2, and so on). We can generalize this to the *affine cipher.* Specifically, an **affine cipher** is one whose encryption function is of the form

$$E(x) = (ax + b) \pmod{26},$$

where a and b are integers which form the key.

(Example.) Suppose that $a = 3$ and $b = 5$. The encryption function is defined by

$$E(x) = (3x + 5) \pmod{26}.$$

Suppose we wanted to encrypt the letter `Y`.

Note that the letter `Y` corresponds to the number `24`. So,

$$E(24) = (3 \cdot 24 + 5) \pmod{26} = (72 + 5) \pmod{26} = 77 \pmod{26} = 25.$$

Therefore, the encryption of `Y` is `Z`, which corresponds to 25.

(Exercise.) Use the same encryption function as above with $a = 3$ and $b = 5$.

(a) What is the encryption of `A`?

Note that `A` corresponds to the number `0`. So,

$$E(0) = (3 \cdot 0 + 5) \pmod{26} = 5 \pmod{26}.$$

Here, the number 5 corresponds to the letter `F`.

(b) What is the encryption of `D`?

`D` corresponds to the number `3`, so

$$E(3) = (3 \cdot 3 + 5) \pmod{26} = 14 \pmod{26}.$$

Here, the number 14 corresponds to the letter `O`.

Lemma 2.5: Affine Cipher

Suppose

$$E : \{0, \dots, 25\} \mapsto \{0, \dots, 25\}$$

is a function of the form

$$E(x) = (ax + b) \pmod{26}$$

for some integers a and b. Then, there exists a function

$$D : \{0, \dots, 25\} \mapsto \{0, \dots, 25\}$$

such that $D(E(x)) = x$ if and only if a is invertible mod 26. Moreover, if $c \equiv a^{-1} \pmod{26}$, then

$$D(y) = c(y - b) \pmod{26}.$$

(Example.) Suppose again $a = 3$ and $b = 5$. Using the process for finding the inverse of a mod 26, we find that this must be 9. So, the Affine Cipher Lemma tells us that the decryption function must be given by

$$D(y) = 9(y - 5) \pmod{26}.$$

Suppose we wanted to decrypt the letter `Z`, which corresponds to the number 25. Then,

$$D(25) = 9(25 - 5) \pmod{26} = 9 \cdot 20 \pmod{26} = 180 \pmod{26} = 24,$$

which corresponds to `Y` as expected.

(Exercise.) Alice and Bob are using the same affine encryption function as above with $a = 3$ and $b = 5$. Bob has just received the message `LNKRLFKH`. Decrypt it.

The letters correspond to the numbers:

$$L \mapsto 11 \qquad N \mapsto 13 \qquad K \mapsto 10 \qquad R \mapsto 17 \qquad F \mapsto 5 \qquad H \mapsto 7.$$

Decrypting each letter results in

- L: $D(11) = 9(11 - 5) \pmod{26} = 9(6) \pmod{26} = 2 \mapsto C$
- N: $D(13) = 9(13 - 5) \pmod{26} = 9(8) \pmod{26} = 20 \mapsto U$
- K: $D(10) = 9(10 - 5) \pmod{26} = 9(5) \pmod{26} = 19 \mapsto T$
- R: $D(17) = 9(17 - 5) \pmod{26} = 9(12) \pmod{26} = 4 \mapsto E$
- F: $D(5) = 9(5 - 5) \pmod{26} = 9(0) \pmod{26} = 0 \mapsto A$
- H: $D(7) = 9(7 - 5) \pmod{26} = 9(2) \pmod{26} = 18 \mapsto S$

Therefore, we have `CUTECATS`, or `cute cats`.

(Exercise.) Suppose the encryption function for an affine cipher is $E(x) = (5x + 17) \pmod{26}$. What is the corresponding decryption function D?

We need to find the inverse of $a = 5 \bmod 26$. So, first, let's find $\gcd(5, 26)$.

a	**b**	$\mathbf{b = aq + r}$	**q**	**r**
5	26	$26 = 5q + r$	5	1
1	5	$5 = 1q + r$	5	1

Since the GCD is 1, there exists an inverse. Moreover, because we only have one equation with a nonzero remainder, it follows that

$$\gcd(5, 26) = 1 = 26(1) + 5(-5).$$

Therefore, the inverse is $-5 \equiv 21 \pmod{26}$. From here, it follows that the decryption function is

$$D(y) = 21(y - 17) \pmod{26}.$$

Remark: Of the numbers between 0 and 25, there are 12 that are invertible mod 26:

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

So, the number of pairs (a, b) such that $E(x) = ax + b \pmod{26}$ is a legitmate encryption function for an affine cipher is $12 \cdot 26 = 312$.

(Exercise.) The *Atbash cipher* is a simple substitution cipher in which encryption and decryption both simply reverse the order of the alphabet. In other words, `A` and `Z` are interchanged, `B` and `Y` are interchanged, and so forth. For example, the plaintext `APPLE` corresponds to the ciphertext `ZKKOV`. Show that the Atbash cipher is a special case of the affine cipher. What are the corresponding values of a and b?

To see why this is a special case of the affine cipher, we need to understand how the affine cipher works. Consider the encryption function

$$E(x) = (ax + b) \pmod{26}.$$

First, let's set $b = 0$. This way, we just need to try all valid values of a. Notice that, when $a = 25$, we have

- $(25 \cdot 0) \pmod{26} = 0$.
- $(25 \cdot 1) \pmod{26} = 25$.
- $(25 \cdot 2) \pmod{26} = 24$.
- $(25 \cdot 3) \pmod{26} = 23$.
- $(25 \cdot 4) \pmod{26} = 22$.
- $\ldots$
- $(25 \cdot 24) \pmod{26} = 2$.
- $(25 \cdot 25) \pmod{26} = 1$.

This looked very similar to what the Atbash cipher does, albeit with one of the numbers being off (remember that A is supposed to map to Z, but with $a = 25$ and $b = 0$, A maps to A still). However, at that point, it became kind of obvious that if you set $b = -1 \equiv 25$, you'll end up with the correct values of a and b.

(Exercise.)

(a) Make sense of and justify the following statement: “Two affine ciphers in succession result in just another affine cipher.”

Consider

$$E_1(x) = (a_1x + b_1) \pmod{26}$$

and

$$E_2(x) = (a_2x + b_2) \pmod{26}.$$

We note that

$$\begin{aligned} E_1(E_2)(x) &= (a_1(a_2x + b_2) + b_1) \pmod{26} \\ &= a_1a_2x + a_1b_2 + b_1 \pmod{26} \\ &= (a_1a_2x) + (a_1b_2 + b_1) \pmod{26}. \end{aligned}$$

(b) Is it possible for “two affine ciphers in succession” to result in a Caesar cipher? Explain.

Consider $a_1 = a_2 = 1$. Then, from the previous part, we’ll end up with

$$E_1(E_2)(x) = x + (b_2 + b_1) \pmod{26}.$$

So, it’s possible.

2.7 Simple Substitution

We can use a general **simple substitution cipher**, also known as a *simple monoalphabetic substitution cipher* or *monoalphabetic substitution cipher*, by using a full conversion table as a key. For example, we might use a table like the following:

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
P	V	J	W	D	C	H	T	S	K	Z	F	N	Q	E	Y	O	R	I	G	A	U	M	L	X	B

This tells us that

- to *encrypt*, we just need to convert every instance of the top letter to the corresponding bottom letter. For example, encrypting A becomes P, encrypting B becomes V, and so on.
- to *decrypt*, we just need to convert every instance of the bottom letter to the corresponding top letter. For example, decrypting P becomes A, decrypting V becomes B, and so on.

(Example.) Suppose Alice wants to encrypt the message `You must destroy all of the horcruxes!` She starts by encoding the message[a]:

`YOUMUSTDESTRYALLOFTHEHORCRUXES`

Then, she converts each letter using the table:

`XEANAIGWDIGREXPFFECGTDTERJRALDI`

This is the ciphertext she sends to Bob. To decrypt the message, Bob uses the same table backwards.

[a] Removing all spaces, punctuations, and then capitalizing everything.

Notice that, if the entire table is our key, the number of possible keys is 26!, a *huge* number. Despite this, simple substitution can still be broken relatively easily using some ideas from probability theory.

(Exercise.) Using the same table given above, do the following by hand.

(a) Encrypt the message `The moon is pitted with holes!`

Encoding the message gives `THEMOONISPITTEDWITHHOLES`. Then, we just need to map each letter appropriately.

```
plaintext  T H E M O O N I S P I T T E D W I T H H O L E S
ciphertext G T D N E E Q S I Y S G G D W M S G T T E F D I
```

The answer is `GTDNEEQSIYSGGDWMSGTTEFDI`.

(b) Decrypt the message `TEMPRDXEAWESQHGEWPX`.

Mapping each letter appropriately gives us

```
ciphertext T E M P R D X E A W E S Q H G E W P X
plaintext  H O W A R E Y O U D O I N G T O D A Y
```

Which, decoded, gives us `How are you doing today?`

2.8 Polybius Square

The **Polybius Square** is another simple substitution cipher which replaces each letter of the plaintext with *two* letters of ciphertext. The idea behind a Polybius square is that it's a table with labeled rows and columns; the alphabet for the messages we're encrypting lives inside the table. For example, if the alphabet we're encrypting includes the capital letters `A` through `Z` and the digits `0` through `9`, then we have 36 letters – perfectly enough to fit in a 6 × 6 grid. Consider the following arrangement, using the rows and columns `ADFGVX`:

	A	D	F	G	V	X
A	N	A	1	C	3	H
D	8	T	B	2	O	M
F	E	5	W	R	P	D
G	4	F	6	G	7	I
V	9	J	0	K	L	Q
X	S	U	V	X	Y	Z

This table represents our key. To encrypt a message, we convert each letter in the plaintext to a pair of letters indicating the *row* and *column* of that letter in the table above. For example, `K` would be replaced with `VG`. Similarly, `S` would be replaced with `XA`.

(Example.) Suppose Alice wants to encrypt the message

`Storm the gates at 14:37.`

She begins by encoding the message:

`STORMTHEGATESAT1437`

Then, she goes through and replaces each letter by the corresponding pairs as described above:

`XADDDVFGDXDDAXFAGGADDDFAXAADDDAFGAAVGV`

This is the ciphertext. Bob, who knows the table, can undo this process to decrypt the message.

(Exercise.) Use the square given above.

(a) Encrypt the message `Hide tide at 7:01am`.

Encoding the message gives us `HIDETIDEAT701AM`. Then, we can map each individual character in the plaintext to its ciphertext representation:

Plain	**Cipher**
H	AX
I	GX
G	GG
H	AX
T	DD
I	GX
D	FX
E	FA
A	AD
T	DD
7	GV
0	VF
1	AF
A	NN
M	DX

Combining all of this gives us

`AXGXGGAXDDGXFXFAADDDGVVFAFNNDX`

(b) Decrypt the message `XAAAADVGFAFVADDDAXADDDDGFVDX`.

To decrypt, we can map each pair of characters in the ciphertext to its plaintext representation:

Cipher	**Plain**
XA	S
AA	N
AD	A
VG	K
FA	E
FV	P
AD	A
DD	T
AX	H
AD	A
DD	T
DG	2
FV	P
DX	M

Combining and decoding gives us

```
Snake path at 2pm
```

2.9 Interlude: Modular Linear Algebra

Before going into polygraphic ciphers, let us first discuss how *linear algebra* interacts with modular arithmetic. We'll just work on 2×2 matrices for now.

2.9.1 2×2 Matrices

Definition 2.5

A 2×2 integer **matrix** (or just *matrix* for short) is a 2×2 box of numbers $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where $a, b, c, d \in \mathbb{Z}$.

- The **determinant** of A is the integer $\det(A) = ad - bc$.
- The **identity matrix** is the matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
- Suppose $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ are two matrices. Their product AB is defined to be

$$AB = \begin{bmatrix} aa' + bc' & ba' + db' \\ ca' + dc' & cb' + dd' \end{bmatrix}.$$

(Example.) Let $A = \begin{bmatrix} 3 & 2 \\ 1 & 7 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix}$. We know that

$$\det(A) = 3 \cdot 7 - 2 \cdot 1 = 19.$$

We also know that

$$AB = \begin{bmatrix} 7 & 18 \\ 15 & 25 \end{bmatrix}$$

and

$$BA = \begin{bmatrix} 7 & 30 \\ 9 & 25 \end{bmatrix}.$$

Remark: It should be clear from the above example that $AB \neq BA$. That is, matrix multiplication is not commutative.

(Exercise.) Let A be a 2×2 integer matrix. Show that

$$AI = IA = A.$$

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then,

$$IA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

and

$$AI = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Theorem 2.4: Multiplicativity of Determinant

If A and B are matrices, then $\det(I) = 1$ and

$$\det(AB) = \det(A)\det(B).$$

Definition 2.6

A **vector** v is a vertical column

$$v = \begin{bmatrix} x \\ y \end{bmatrix},$$

where $x, y \in \mathbb{Z}$.

Definition 2.7

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is a matrix, then the product $Ab = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$.

2.9.2 Congruences and Inversion for Matrices

Definition 2.8

Fix a positive integer n and suppose A and B are both matrices:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}.$$

We say that $A \equiv B \pmod{n}$ if all four of the entries of the two matrices are congruent mod n, i.e., if all of the following are true:

$$a \equiv a' \pmod{n}$$
$$b \equiv b' \pmod{n}$$
$$c \equiv c' \pmod{n}$$
$$d \equiv d' \pmod{n}$$

Definition 2.9

A matrix A is *invertible mod n* if there exists a matrix X such that $AX \equiv I \pmod{n}$. In this case, X is called an inverse of $A \pmod{n}$. In symbols, we write $X \equiv A^{-1} \pmod{n}$.

Theorem 2.5: Modular Inversion Theorem

Suppose $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is a matrix. Then, A is invertible if and only if $\det(A)$ is invertible mod n. Moreover, if $e \equiv \det(A)^{-1} \pmod{n}$, then

$$X = \begin{bmatrix} ed & -eb \\ -ec & ea \end{bmatrix}$$

is an inverse of $A \pmod{n}$.

(Example.) Suppose we have $A = \begin{bmatrix} 3 & 2 \\ 1 & 7 \end{bmatrix}$. We know that $\det(A) = 19$ is invertible mod 26, so A is also invertible mod 26. We have

$$19^{-1} \equiv 11 \pmod{26},$$

so the formula for the inverse from the Matrix Inversion Theorem tells us that

$$A^{-1} \equiv \begin{bmatrix} 11 \cdot 7 & -11 \cdot 2 \\ -11 \cdot 1 & 11 \cdot 3 \end{bmatrix} \equiv \begin{bmatrix} 77 & -22 \\ -11 & 33 \end{bmatrix} \equiv \begin{bmatrix} 25 & 4 \\ 15 & 7 \end{bmatrix} \pmod{26}.$$

In other words,

$$X = \begin{bmatrix} 15 & 4 \\ 15 & 7 \end{bmatrix}$$

is an inverse of A mod 26. It follows that $AX = I$.

(Exercise.) Which of the following matrices is invertible mod 26?

(a) $\begin{bmatrix} 7 & 5 \\ 3 & 3 \end{bmatrix}$

(b) $\begin{bmatrix} 8 & 1 \\ 3 & 2 \end{bmatrix}$

(c) $\begin{bmatrix} 4 & 2 \\ 1 & 2 \end{bmatrix}$

(d) $\begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$

The answer is **D**. By calculating the determinant of each matrix, we see that the GCD of the determinant of the matrix and 26 is 1 for only D.

(Exercise.) As a follow-up to the previous exercise, what is the inverse of the invertible matrix?

TODO

2.10 Hill Cipher

The *Hill Cipher* is the first polygraphic cipher we'll talk about. We'll focus on the digraphic case, which replaces 2 letters of plaintext at a time. Our **key** for this cipher is a matrix that is invertible mod 26.

(Example.) Suppose we want to encrypt the message `You have saved us all`. Begin with the usual encoding process:

```
 Y  O  U  H  A  V  E  S  A  V  E  D  U  S  A  L  L
24 14 20  7  0 21  4 18  0 21  4  3 20 18  0 11 11
```

(The numbers below the letters represent the ranking of each letter.) Let's suppose our key is

$$A = \begin{bmatrix} 3 & 2 \\ 1 & 7 \end{bmatrix},$$

which has determinant 19 and is thus invertible mod 26. It follows that A is an invertible matrix mod 26, which can thus be used as a key.

For encrypting, the idea is to go through the list of numbers, replacing each pair of numbers with the result of multiplying that pair by the matrix A (mod 26). For example, for the pair 24 and 14, we can make a vector containing these numbers,

$$v = \begin{bmatrix} 24 \\ 14 \end{bmatrix},$$

and then compute

$$Av = \begin{bmatrix} 3 & 2 \\ 1 & 7 \end{bmatrix} \begin{bmatrix} 24 \\ 14 \end{bmatrix} \pmod{26} = \begin{bmatrix} 100 \\ 122 \end{bmatrix} \pmod{26} = \begin{bmatrix} 22 \\ 18 \end{bmatrix}.$$

So, we replace the numbers 24 and 14 with the numbers 22 and 18, respectively. In other words, the first two letters of the message will be replaced by `W` and `S`, respectively.

We can continue this process with the next pair of numbers (20, 7), and so on. Eventually, we'll reach the end. Note that, if you have an odd number of letters, you can add an additional random letter at the end (e.g., `Z`). With this in mind, the net result is the ciphertext

```
WSWRQRWAQRSZSQWZFE
```

As you might expect, to decrypt a message, we just need to multiply the pairs of numbers by the *inverse* of A mod 26.

(Exercise.) Use the matrix

$$A = \begin{bmatrix} 3 & -1 \\ 2 & 5 \end{bmatrix}$$

as the key for a Hill cipher. Encrypt the message `Go to Lake Lerna`.

First, we verify that this matrix can be used as a key by checking the determinant.

$$\det(A) = 15 - 2(-1) = 15 + 2 = 17.$$

Because 17 is invertible mod 26, it follows that we can use A as a key. So, begin by encoding the message:

```
G  O  T  O  L  A  K  E  L  E  R  N  A  Z
6 14 19 14 11  0 10  4 11  4 17 13  0 25
```

Note that we put a `Z` at the end so that the length of the plaintext is even (that way, we can do pairwise encryption.) We'll now process each pair of letters.

- For pair $(6, 14)$, we have

$$\begin{bmatrix} 3 & -1 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 6 \\ 14 \end{bmatrix} \pmod{26} = \begin{bmatrix} 4 \\ 82 \end{bmatrix} \pmod{26} = \begin{bmatrix} 4 \\ 4 \end{bmatrix},$$

  which corrsponds to `E` and `E`.

- For pair $(19, 14)$, we have

$$\begin{bmatrix} 3 & -1 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 19 \\ 14 \end{bmatrix} \pmod{26} = \begin{bmatrix} 43 \\ 108 \end{bmatrix} \pmod{26} = \begin{bmatrix} 17 \\ 4 \end{bmatrix} \pmod{26},$$

  which corresponds to `R` and `E`.

- For pair $(11, 0)$, we have

$$\begin{bmatrix} 3 & -1 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 0 \end{bmatrix} \pmod{26} = \begin{bmatrix} 33 \\ 22 \end{bmatrix} \pmod{26} = \begin{bmatrix} 7 \\ 22 \end{bmatrix} \pmod{26},$$

  corresponding to `H` and `W`.

By continuing this process, we end up with the ciphertext

```
EEREHWAODQMVBV
```

(Exercise.) Use the matrix

$$A = \begin{bmatrix} 3 & -1 \\ 2 & 5 \end{bmatrix}$$

as the key for a Hill cipher. Decrypt the message `RNCQYVFRRLZI`.

Note again that $\det(A) = 17$. In order to decrypt the message, we need to find the inverse of A mod 26.

Finding GCD: Recall that the Matrix Inversion Theorem states that A is invertible if and only if $\det(A)$ is invertible mod n. To see if $\det(A)$ is invertible mod n, we need to see if $\gcd(\det(A), n) = 1$. So, let's find $\gcd(17, 26)$.

a	b	$b = aq + r$	q	r
17	26	$26 = 17q + r$	1	9
9	17	$17 = 9q + r$	1	8
8	9	$9 = 8q + r$	1	1
1	8	$8 = 1q + r$	8	0

Therefore, $\gcd(17, 26) = 1$ as desired. Thus, an inverse must exist.

Finding Bezout: Now, we need to find the Bezout coefficients. Labeling each equation, we have

- (Eq. 1) $26 = 17(1) + 9 \implies 9 = 26 + 17(-1)$
- (Eq. 2) $17 = 9(1) + 8 \implies 8 = 17 + 9(-1)$
- (Eq. 3) $9 = 8(1) + 1 \implies 1 = 9 + 8(-1)$

Now that we've labeled each relevant operation, we can find the Bezout coefficients:

$$\begin{aligned}
1 &= 9 + 8(-1) \\
&= 9 + (\underbrace{17 + 9(-1)}_{\text{Eq. 2}})(-1) \\
&= 9 + 17(-1) + 9(-1)(-1) \\
&= 9 + 17(-1) + 9 \\
&= 9(2) + 17(-1) \\
&= (\underbrace{26 + 17(-1)}_{\text{Eq. 1}})(2) + 17(-1) \\
&= 26(2) + 17(-1)(2) + 17(-1) \\
&= 26(2) + 17(-2) + 17(-1) \\
&= 26(2) + 17(-3)
\end{aligned}$$

From this, it follows that $x = -3$, which is the desired inverse.

Decrypting: With this in mind, we have

$$X = \begin{bmatrix} -3(5) & 3(-1) \\ 3(2) & -3(3) \end{bmatrix} = \begin{bmatrix} -15 & -3 \\ 6 & -9 \end{bmatrix} \pmod{26}.$$

Now that we have the matrix needed to decrypt the message, we can proceed. Labeling each character in the message gives us

```
R  N C  Q  Y  V F  R  R  L  Z I
17 13 2 16 24 21 5 17 17 11 25 8
```

Iterating over each pair, we have

- For $(17, 13)$,
$$X \begin{bmatrix} 17 \\ 13 \end{bmatrix} \pmod{26} = \begin{bmatrix} -294 \\ -15 \end{bmatrix} \pmod{26} = \begin{bmatrix} 18 \\ 11 \end{bmatrix} \pmod{26},$$
or `S` and `L`.
- For $(2, 16)$,
$$X \begin{bmatrix} 2 \\ 16 \end{bmatrix} \pmod{26} = \begin{bmatrix} -78 \\ -132 \end{bmatrix} \pmod{26} = \begin{bmatrix} 0 \\ 24 \end{bmatrix} \pmod{26},$$
or `A` and `Y`.

By continuing this process, we end up with

```
SLAYTHEHYDRA
```

(Exercise.) Use the Hill cipher with key
$$A = \begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$$
to encrypt the word `AREA`.

Labeling each letter with its corresponding number, we have

```
0 17 4 0
A  R E A
```

Then, we just need to multiply each pair of numbers, like so:
$$\begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 17 \end{bmatrix} = \begin{bmatrix} 4 \cdot 0 + 3 \cdot 17 \\ 1 \cdot 0 + 2 \cdot 17 \end{bmatrix} = \begin{bmatrix} 51 \\ 34 \end{bmatrix} \equiv \begin{bmatrix} 25 \\ 8 \end{bmatrix} \pmod{26},$$
and
$$\begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 4 \\ 0 \end{bmatrix} = \begin{bmatrix} 16 + 0 \\ 4 + 0 \end{bmatrix} \equiv \begin{bmatrix} 16 \\ 4 \end{bmatrix} \pmod{26}.$$
Therefore, the answer is `ZIQE`.

(Exercise.) The matrix
$$A = \begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$$
is used to encrypt `CRZX`. What is the plaintext?

We know that the inverse of A is

$$X = \begin{bmatrix} 16 & 15 \\ 5 & 6 \end{bmatrix}.$$

Then, going through each pair of numbers gives us

$$\begin{bmatrix} 16 & 15 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 17 \end{bmatrix} = \begin{bmatrix} 16 \cdot 2 + 15 \cdot 17 \\ 5 \cdot 2 + 6 \cdot 17 \end{bmatrix} = \begin{bmatrix} 287 \\ 112 \end{bmatrix} = \begin{bmatrix} 1 \\ 8 \end{bmatrix},$$

and

$$\begin{bmatrix} 16 & 15 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 25 \\ 23 \end{bmatrix} = \begin{bmatrix} 16 \cdot 25 + 15 \cdot 23 \\ 5 \cdot 25 + 6 \cdot 23 \end{bmatrix} = \begin{bmatrix} 745 \\ 263 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 3 \end{bmatrix}.$$

This gives us `BIRD`.

(Exercise.) Suppose you want to encrypt a sequence of bits (i.e., a sequence of `0`'s and `1`'s) using a 2×2 Hill cipher. How many different encryption functions are there? In other words, how many different congruence classes of 2×2 can be used as a key for a Hill cipher?

If we assume that our alphabet contains only binary numbers, then there are 2 possible numbers. Therefore, our Hill cipher must be a matrix mod 2. We want to know how many of these matrices are invertible mod 2.

There are $2 \cdot 2 \cdot 2 \cdot 2$ choices for what our 2×2 matrix can be. There are three possible determinants: 0 and ± 1. Note that $-1 \equiv 1 \pmod 2$ so there's actually *2* possible determinants. Of these determinants, note that $\gcd(1, 2) = 1$ while $\gcd(0, 2) = 2$.

With this in mind, we know that any matrix with determinant 1 is valid. There are $\boxed{6}$ such matrices.

2.11 Playfair Cipher

The **Playfair Cipher** is another digraphic cipher, like the Hill cipher we just discussed above. The key for a Playfair cipher is a 5×5 grid of letters, where each letter appears exactly once. Because there are 26 letters in the English alphabet but 25 letters can fit in a grid, we treat `I` and `J` as the same letter[4].

How do we start constructing a grid? An easy and convenient way of doing this is to start with a secret keyword. For example, suppose `ALPHABET` is our keyword. We can start filling out our grid by writing out the letters of our keyword across the rows, skipping over the letters we've written.

A	**L**	**P**	**H**	**B**
E	**T**			

We can then fill out the remaining squares with the remaining letters of the alphabet, skipping over anything we've already written down and remembering that `I` and `J` are the same.

[4] We could also use a variant where we use a 6×6 grid that includes all 26 letters and 10 digits, instead.

A	L	P	H	B
E	T	C	D	F
G	I	K	M	N
O	Q	R	S	U
V	W	X	Y	Z

We can encode our message by doing the following:

1. Remove all non-alphabet characters and capitalize everything.
2. Replace all instances of `J` with `I`.
3. Group the letters into pairs.
4. If there are any pairs where both letters are the same, insert the letter `X` in between the two letters of that pair and regroup into pairs.
5. If there's an unpaired letter at the end, insert the letter `X` after it.

Remark: You may need to apply rule 4 multiple times.

(Example.) Suppose we want to encode the message **`hidden jewels in trees.`** Here's what will happen after each step described above.

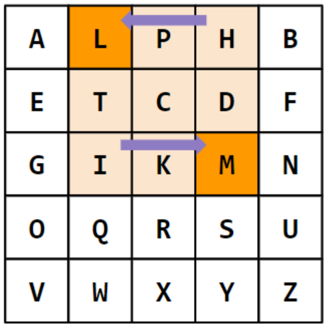
1. `HIDDENJEWELSINTHETREES`
2. `HIDDENIEWELSINTHETREES`
3. `HI DD EN IE WE LS IN TH ET RE ES`
4. `HI DX DE NI EW EL SI NT HE TR EX ES`
5. `HI DX DE NI EW EL SI NT HE TR EX ES`

To encrypt, we need to replace each pair with another pair using the grid by following the rules:

- (Row Rule.) If both letters in the pair occur in the same row, replace each letter of the pair with the letter that appears immediately to its right (wrapping around to the left side of the row if needed).
- (Column Rule.) If both letters in the pair occur in the same column, replace each letter of the pair with the letter that appears immediately below it (wrapping around to the top of the column if needed).
- (Rectangle Rule.) Otherwise, the two letters define a rectangle inside the grid, and we replace each letter with the letter on the same row but the opposite of that rectangle.

(Example.) Suppose we want to encrypt the message `HI DX DE NI EW EL SI NT HE TR EX ES` (see previous example for encoding). Let's look at each pair.

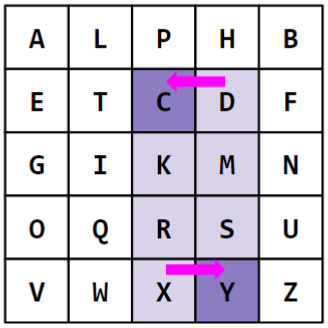
- For `HI`, notice that `H` and `I` do not appear in the same row or column. Therefore, the rectangle rule applies. Observe the highlighted cells:



A	L	P	H	B
E	T	C	D	F
G	I	K	M	N
O	Q	R	S	U
V	W	X	Y	Z

Here, the letter in the same row as `H` but opposite side is `L`, and the letter in the same row as `I` but the opposite side is `M`. Therefore, `HI` becomes `LM`.

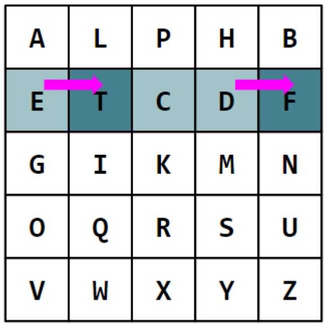
- For `DX`, we also apply the rectangle rule. Observe the highlighted cells:



A	L	P	H	B
E	T	C	D	F
G	I	K	M	N
O	Q	R	S	U
V	W	X	Y	Z

So, it follows that `DX` gets replaced with `CY`.

- For `DE`, both letters are on the same row so we apply the row rule. Observe that



A	L	P	H	B
E	T	C	D	F
G	I	K	M	N
O	Q	R	S	U
V	W	X	Y	Z

So, it follows that `DE` becomes `FT`.

Continuing this process yields the desired result.

(Exercise.) You are constructing a 5×5 grid for a Playfair cipher starting with the keyword `FAJITAS`. What letter falls in the very center of the grid (i.e., in the 3rd row and the 3rd column)?

(a) K

(b) L

(c) M

(d) None of the above.

Constructing the grid looks something like:

F	A	I	T	S
B	C	D	E	G
H	K	L	M	N
O	P	Q	R	U
V	W	X	Y	Z

So, the answer is (b).

(Exercise.) Encode the message `Little Fluffy` for encryption using a Playfair cipher. How many pairs of letters are in the encoded message?

(a) 6

(b) 7

(c) 8

(d) None of the above.

Encoding gives us

- LITTLEFLUFFY
- LITTLEFLUFFY
- LITXTLEFLUFXFY
- LI TX TL EF LU FX FY

The answer is (b).

(Exercise.) Use a Playfair cipher with a key given by the grid below, decrypt `WZ LT OP WK SH ES VX PH`.

C	W	F	Q	Y
G	I	Z	R	B
H	M	K	L	U
V	A	D	E	N
O	P	X	T	S

For decryption, we just perform the inverse of the encryption process (e.g., for the row rule, when encrypting is replacing the letter with the one immediately to the right, decrypting is replacing the letter with the one immediately to the left.)

- WZ maps to FI.
- LT maps to RE.
- OP maps to SO.
- WK maps to FM.
- SH maps to OU.
- ES maps to NT.
- VX maps to DO.
- PH maps to OM.

The answer is FIRESOFMOUNTDOOM, or Fires of Mount Doom.

2.12 Vigenere Cipher

The Vigenere cipher is our first example of a *polyalphabetic substitution*, or a substitution cipher in which the substitution scheme changes over the course of the message.

More specifically, the Vigenere cipher makes use of *modular arithmetic* and the correspondence between the letters A through Z and the numbers 0 through 25. The **key** for a Vigenere cipher is a *finite* sequence of shifts.

A convenient and, perhaps easy-to-remember, way of constructing such a sequence is to have a secret *keyword*, and then associate each letter of that word with the corresponding number to get the sequence of shift. For example, if our secret keyword is ASGARD, the corresponding sequence of numbers is $(0, 18, 6, 0, 17, 3)$ because A corresponds to 0, S corresponds to 18, and so on.

(Example.) Suppose we want to encrypt the message Keep Loki Away. We begin by encoding the message through the usual way: remove all non-alphabet characters and capitalize everything.

```
KEEPLOKIAWAY
```

Then, we can associate, to each letter in the encoded message, the corresponding numbers 0 through 25.

```
 K E E  P  L  O  K I A  W A  Y
10 4 4 15 11 14 10 8 0 22 0 24
```

We can then perform addition mod 26 to each of these numbers. Specifically, we use the first element of our key sequence for the first number, the second for the second, and so on. When we finish the key, we can just repeat it from the beginning until we're done. From there, we convert those sums back to numbers using te usual correspondence. So, using the key $(0, 18, 6, 0, 17, 3)$ corresponding to the key ASGARD from above, we have

Encoded	K	E	E	P	L	O	K	I	A	W	A	Y
Numbers (1)	10	4	4	15	11	14	10	8	0	22	0	24
Keyword	A	S	G	A	R	D	A	S	G	A	R	D
Key Number (2)	0	18	6	0	17	3	0	18	6	0	17	3
(1) + (2) mod 26	10	22	10	15	2	17	10	0	6	22	17	1
Encrypted	K	W	K	P	C	R	K	A	G	W	R	B

From this, it follows that `KWKPCRKAGWRB` is the ciphertext.

Remarks:

- As mentioned earlier, the Vigenere cipher is polyalphabetic. Notice how the first `E` in the example above was encrypted to `W`, whilethe second `E` was encrypted to `K`.
- For decryption, the process is nearly the same. The only difference is that we *subtract* mod 26 instead of add.

(Exercise.) Using the keyword `ASGARD`,

- Encrypt the message `Protect Odin from Fenrir`.

Encoding the message gives us `PROTECTODINFROMFENRIR`. From there, we can label each letter:

P	R	O	T	E	C	T	O	D	I	N	F	R	O	M	F	E	N	R	I	R
15	17	14	19	4	2	19	14	3	8	13	5	17	14	12	5	4	13	17	8	17

Noting that the key, `ASGARD`, has numerical correspondence $(0, 18, 6, 0, 17, 3)$, we can run through the encryption process:

Encoded	P	R	O	T	E	C	T	O	D	I	N
Numbers (1)	15	17	14	19	4	2	19	14	3	8	13
Keyword	A	S	G	A	R	D	A	S	G	A	R
Key Numbers (2)	0	18	6	0	17	3	0	18	6	0	17
(1) + (2) mod 26	15	9	20	19	21	5	19	6	9	8	4
Encrypted	P	J	U	T	V	F	T	G	J	I	E

Encoded	F	R	O	M	F	E	N	R	I	R
Numbers (1)	5	17	14	12	5	4	13	17	8	17
Keyword	D	A	S	G	A	R	D	A	S	G
Key Numbers (2)	3	0	18	6	0	17	3	0	18	6
(1) + (2) mod 26	8	17	6	18	5	21	16	17	0	23
Encrypted	I	R	G	S	F	V	Q	R	A	X

This yields the ciphertext

`PJUTVFTGJIEIRGSFVQRAX.`

- Decrypt the message `RSMNRUOCOSTRMATG`.

We begin by labeling each letter:

R	S	M	N	R	U	O	C	O	S	T	R	M	A	T	G
17	18	12	13	17	20	14	2	14	18	19	17	12	0	19	6

From there, we can run through the decryption process:

Encoded	R	S	M	N	R	U	O	C	O	S	T	R	M	A	T	G
Numbers (1)	17	18	12	13	17	20	14	2	14	18	19	17	12	0	19	6
Keyword	A	S	G	A	R	D	A	S	G	A	R	D	A	S	G	A
Key Numbers (2)	0	18	6	0	17	3	0	18	6	0	17	3	0	18	6	0
(1) - (2) mod 26	17	0	6	13	0	17	14	10	8	18	2	14	12	8	13	6
Decrypted	R	A	G	N	A	R	O	K	I	S	C	O	M	I	N	G

Decoding the message yields

```
Ragnarok is coming
```

(Exercise.) Use a Vigenere cipher with keyword `AND` to encrypt the message `Six Meals`.

Encoding and mapping each letter to the corresponding number, we have

S	I	X	M	E	A	L	S
18	8	23	12	4	0	11	18

From there, we can run through the encryption process:

Encoded	S	I	X	M	E	A	L	S
Numbers (1)	18	8	23	12	4	0	11	18
Keyword	A	N	D	A	N	D	A	N
Key Numbers (2)	0	13	3	0	13	3	0	13
(1) + (2) mod 26	18	21	0	12	17	3	11	5
Encrypted	S	V	A	M	R	D	L	F

Therefore, the answer is `SVAMRDLF`.

(Exercise.) Use a Vigenere cipher with keyword `AND` to decrypt `YEX SUD LYQ OGS AFV`.

Running through the decryption process yields

Encoded	Y	E	X	S	U	D	L	Y	Q	O	G	S	A	F	V
Numbers (1)	24	1	23	18	20	3	11	24	16	14	6	18	0	5	21
Keyword	A	N	D	A	N	D	A	N	D	A	N	D	A	N	D
Key Numbers	0	13	3	0	13	3	0	13	3	0	13	3	0	13	3
(1) - (2) mod 26	24	14	20	18	7	0	11	11	13	14	19	15	0	18	18
Decrypted	Y	O	U	S	H	A	L	L	N	O	T	P	A	S	S

This yields `YOUSHALLNOTPASS`, or `You shall not pass`.

2.13 One-Time Pad

The *one-time pad* is a special case of the Vigenere cipher where the key sequence is

- never re-used,
- at least as long as the plaintext,
- "unrelated to the plaintext," and
- "totally random," in the sense that each number 0 through 25 is equally likely in each position of the key.

Essentially, the way the one-time pad functions is very similar to the Vigenere cipher, except that the key sequence must not be generated using a keyword[5].

In any case, we'll revisit this section later – it's important to be precise when talking about what "unrelated to the plaintext" and "totally random" means. We'll also see, later on, that this has a property known as *perfect secrecy*, which means that the security of the one-time pad can be mathematically guaranteed.

[5] The issue with this is that words won't have the property that each letter is equally likely.

3 Codebreaking

In the previous section, we mostly looked at encryption and decryption of many ciphers. Now, we'll look at how to *break* some of these ciphers. It should be noted that codebreaking is not necessarily "exact science"; that is, there's not necessarily an algorithm that guarantees producing the correct plaintext from ciphertext in one shot without access to the key. Instead, these techniques can help constrain the search for the correct ciphertext.

3.1 Frequency Analysis

Frequency analysis is a powerful technique used to break simple – and sometimes also polygraphic – substutition ciphers. The idea is relatively simple.

> **Heuristic:** The relative frequencies of letters remain *roughly* stable across different samples of English texts, and `ETAOINSHRDLU` is the *approximate* order of the 12 most common letters.

We can use this heuristic to break simple substutition ciphers. Ideally, the technique works best with longer ciphertexts, but the idea is to guess the decryption key one letter at a time, doing one of the following at each step:

1. Assign the most frequent unassigned letter of ciphertext to be the most frequent unassigned letter in some sample English text (or perhaps some other letter with a similar frequency).
2. Look through the ciphertext and see if you can make any guesses about words that seem to appear there. If you see something, fill in the blanks in that word by making appropriate guesses for the key.

If, at any point, it seems like your guesses are leading to nonsense or implausible sequences of letters, backtrack and make another guess. A few comments:

- Usually, we can start with two applications of option 1. For example, we can guess that the most common letter in the ciphertext is `E` and the second most commmon letter is `T`.
- We can also note that `THE` occurs frequently in English (and other similar words like `THEY` or `THEIR` or `THEN`).
- If, after you make the `T` and `E` substutitions, you see the `T*E` pattern frequently (`*` being some *fixed* letter in ciphertext), you can make the assumption that `*` could be `H`.
  - Also, perhaps if you see `TH*T` occurring in your ciphertext after making the substutitions and with `*` fixed, you can probably assume that `*` is `A`.
- If you can't spot any possible words, you can always try using option 1 instead and match the most frequent letters.

Usually, the first few guesses after `E` and `T` are the hardest. Once you've made a few correct guesses, it becomes easy to see words.

3.2 Interlude: Probability

Notice how, in the previous observation, we made use of the Heuristic to help us mount attacks on substutition ciphers. We can use variants of this observation for other ciphers, but this requires us to first talk about **probability**.

3.2.1 Experiments and Events

In probability thoery, the word *experiment* is used to talk abstractly and heuristically about processes which generate "outcomes" and which might be rather intricate. These experiments are formally modeled by *probability spaces*. For now, we'll use the following definition.

Definition 3.1: (Discrete) Probability Space

A **(discrete) probability space** is a nonempty countable[a] set Ω called the **sample space** and whose elements are called **outcomes**. Each outcome $x \in \Omega$ is assigned a real number $\mathbb{P}[x]$ between 0 and 1 called its **probability**. The probabilities of all the outcomes must sum to 1; that is,

$$\sum_{x\in\Omega} \mathbb{P}[x] = 1.$$

[a] "Countable" means that the outcomes can be put in a list so that the summation $\sum_{x\in\Omega} \mathbb{P}[x]$ makes sense. Any finite set, and some infinite sets, are countable. For now, we'll focus on the finite case.

The probability associated to each outcome should be thought of as some measure of our "confidence" that our experiment will produce that outcome. For example, it might be the percentage of times we expect the experiment to produce that outcome if the experiment were to be releated many times.

(Example.) Rolling a dice is an example of an experiment.

- The possible outcomes of this experiment are the numbers 1 through 6; that is, the **sample space** is
$$\Omega = \{1, 2, 3, 4, 5, 6\}.$$
- Assigning each outcome a probability of $\frac{1}{6}$, that is, for $x \in \Omega$,
$$\mathbb{P}[x] = \frac{1}{6},$$
means that the dice is "fair" and each outcome is equally likely.

Thus, we constructed a probability space; we have a finite set Ω that enumerates the possible outcomes, and we assigned a probability to each outcome.

A single experiment can also have "multiple parts," as seen in the next example.

(Example.) Flipping a fair coin twice can be thought of as a single experiment.

- Possible outcomes of this experiment might be something like "heads and then heads again" or "heads and then tails" and so on. All these outcomes taken together as a set form the sample space,
$$\Omega = \{HH, HT, TH, TT\},$$
where H means "Heads" and T means "Tails."
- We can assign each of these four outcomes probability $\frac{1}{4}$, that is for some $x \in \Omega$
$$\mathbb{P}[x] = \frac{1}{4}.$$

Here, we've modeled the situation where the coin is fair and the result of each coin flip is unrelated to the other.

Notice how both examples above have outcomes with the same probabilities. This is a common situation, and thus has a name.

Definition 3.2: Uniform Distribution

A probability space is **uniform** if all of its outcomes have equal probability.

Sometimes, we might be interested in grouping the various outcomes together. We can do so with a definition.

Definition 3.3: Event

Given a probability space, an **event** E is a subset of the sample space Ω; that is,

$$E \subset \Omega.$$

We define

$$\mathbb{P}[E] = \sum_{x \in E} \mathbb{P}[x].$$

Remark: The words "event" and "outcome" have distinct definitions in probability theory.

(Example.) Consider the example of rolling a dice again. An *event* might be something like "the dice roll is odd." Formally, if we think of the sample space $\Omega = \{1, 2, 3, 4, 5, 6\}$, the event "the dice roll is odd" corresponds to the event

$$E = \{1, 3, 5\}.$$

This event is also assigned a probability, by summing together the probabilities of all outcomes that comprise the event:

$$\mathbb{P}[E] = \mathbb{P}[1] + \mathbb{P}[3] + \mathbb{P}[5] = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{3}{6} = \frac{1}{2}.$$

(Exercise.) Suppose you have 4 boxes (labeled 1, 2, 3, and 4), and you have 8 colors available (red, blue, green, yellow, pink, purple, teal, brown). Consider an experiment where each of the 4 boxes is assigned a color. For example, one possible outcome of this experiment might be the one where box 1 is colored red, box 2 is colored blue, box 3 is colored green, and box 4 is colored blue.

1. How many possible outcomes are there?

   The answer is $8^4 = 70$ outcomes. We can assign any of the 8 colors to box 1, any of the 8 colors to box 2, any of the 8 colors to box 3, and any of the 8 colors to box 4.

2. How many outcomes are in the event "no two boxes have the same color?"

   The answer is $8 \cdot 7 \cdot 6 \cdot 5 = 1680$. Once we pick a color, we can no longer use that color for the next box.

(Exercise.) Suppose you have k boxes and you have n colors available. Consider again the same experiment where each of the k boxes is assigned one of the n colors "at random" (i.e., construct a uniform probability space).

1. What is the probability of the event that no two boxes have the same color?

   Note that the number of outcomes such that no two boxes have the same color is given by $n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot \ldots \cdot (n-k+1)$. The total number of outcomes is n^k. The probability is given by

   $$\frac{n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot \ldots \cdot (n-k+1)}{n^k}.$$

2. What is the probability that there are at least two boxes of the same color?

Note that the event that at least two boxes have the same colors is the opposite of the event that no two boxes have the same colors. In other words,

$$\mathbb{P}(\geq 2 \text{ Boxes Have Same Color}) = 1 - \mathbb{P}(\text{No Two Boxes Have Same Color}).$$

This gives us

$$\mathbb{P}(\geq 2 \text{ Boxes Have Same Color}) = 1 - \frac{n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot \ldots \cdot (n-k+1)}{n^k}.$$

3. Find expressions in terms of n and k.

Notice that

$$n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot \ldots \cdot (n-k+1) = (n)_k = \frac{n!}{(n-k)!}.$$

This is known as a falling factorial. So,

(a) $\frac{\frac{n!}{(n-k)!}}{n^k}$.

(b) $1 - \frac{\frac{n!}{(n-k)!}}{n^k}$.

3.2.2 Random Variables

A common way that events show up is through **random variables**. We can think of random variables as representations of making an observation (or taking a measurement) on the outcome of an experiment. A random variable has a set of possible values that it can take. Letters like X or Y can be used to denote random variables.

Definition 3.4: Random Variable

Fix a probability space Ω. A **random variable** is a function with domain Ω and its set of *possible* values is the range of this function.

(Example.) Consider the "multi-part" experiment discussed earlier (with the coin being flipped twice). We can make the observation that the first coin flip can be thought of as a random variable, which we can call X. X can take the value "heads" or "tails." Then, we can write things like $X = H$ to refer to the event that the first coin flip landed heads. In other words, in the sample space

$$\Omega = \{HH, HT, TH, TT\},$$

the notation $X = H$ describes the event $\{HH, HT\}$ and we have

$$\mathbb{P}[X = H] = \mathbb{P}[HH] + \mathbb{P}[HT] = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

(Example.) Suppose we're interested in the number of heads. We can define another random variable Y that can take values 0, 1, or 2. The notation $Y = n$ for either $n = 0, 1, 2$ describes the event that we observe n heads out of the two coin flips. So, for $Y = 1$, we have the event $\{HT, TH\}$ and

$$\mathbb{P}[Y = 1] = \mathbb{P}[HT] = \mathbb{P}[TH] = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

However, for $Y = 0$, we have the event $\{TT\}$ and

$$\mathbb{P}[Y = 0] = \mathbb{P}[TT] = \frac{1}{4}.$$

Definition 3.5: Uniform Random Variable

A random variable is **uniform** if all of its values have equal probability.

In the previous two examples, X is uniform (it can either take heads or tails, i.e., $X = H$ or $X = T$, both of which have probabilities $1/2$) whereas Y is not uniform.

Definition 3.6: Expected Value

Suppose X is a random variable whose values are real numbers. The **expected value**, known as the expectation, of X, denoted $\mathbb{E}[X]$, is defined by

$$\mathbb{E}[X] = \sum_{\text{values } a} a \cdot \mathbb{P}[X = a].$$

(Example.) In the experiment involving two coin flips, the random variable Y which counts the number of heads has real number values (0, 1, 2). Its expectation is given by

$$\mathbb{E}[Y] = 0 \cdot \frac{1}{4} + 1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} = 1.$$

(Exercise.) Consider the experiment where you roll a pair of fair dice. Let the random variable X denote the sum of the dice rolls.

1. What are the possible values of X?

   The possible values are
   $$\{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.$$

2. What is $\mathbb{P}[X = 7]$?

   Note that the pair of fair dice will have sum 7 if we get
   $$\{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1).\}$$
   Therefore,
   $$\mathbb{P}[X = 7] = \frac{6}{36} = \frac{1}{6}.$$

3. What is $\mathbb{P}[X = 7 \text{ or } 11]$?

Note that the paur of fair dice will have 11 if we get

$$\{(6,5),(5,6)\}.$$

Combining this with this previous part, we have 8 possible combinations. This gives us

$$\mathbb{P}[X = 7 \text{ or } 11] = \frac{8}{36} = \frac{2}{9}.$$

4. What is $\mathbb{E}[X]$?

Note that

- For sum 2, there is only 1 possible combination.
- For sum 3, there are 2 possible combinations.
- For sum 4, there are 3 possible combinations.
- For sum 5, there are 4 possible combinations.
- For sum 6, there are 5 possible combinations.
- For sum 7, there are 6 possible combinations.
- For sum 8, there are 5 possible combinations.
- For sum 9, there are 4 possible combinations.
- For sum 10, there are 3 possible combinations.
- For sum 11, there are 2 possible combinations.
- For sum 12, there are 1 possible combinations.

Therefore, the expected value is

$$\begin{aligned}\mathbb{E}[X] &= 2\frac{1}{36} + 3\frac{2}{36} + 4\frac{3}{36} + 5\frac{4}{36} + 6\frac{5}{36} + 7\frac{6}{36} + 8\frac{5}{36} + 9\frac{4}{36} + 10\frac{3}{36} + 11\frac{2}{36} + 12\frac{1}{36} \\ &= 7.\end{aligned}$$

3.3 Interlude: G-Test

Suppose that every registered voters in an imaginary county in the United States is classified into the mutually exclusive and exhaustive racial groups "White," "Black," "Hispanic," and "Other." Suppose that, by inspecting the voter rolls, we find that the racial distribution of this county is

	White	Black	Hispanic	Other	Total
Distribution	72%	7%	12%	9%	100%

Since jurors are supposed to be drawn from the list of registered voters, we might hope that a random sample of jurors would follow this same racial distribution. Suppose we sample 275 jurors and observe the racial distribution displayed in the second row:

	White	Black	Hispanic	Other	Total
Distribution	72%	7%	12%	9%	100%
Observed	210	10	20	35	275
Expected	198	19.25	33	24.75	275

Now, if our random sample of jurors followed the overall racial distribution of registered voters, we would expect that 72% of them would be White, which would be $0.72 \cdot 275 = 198$ people. We can calculate the expected numbers of jurors in the other groups similarly to fill in the third row above.

Note that we can, and should, expect *some* deviation from the expected counts. Remembering that our categories are mutually exclusive, so we could not possibly observe a sample of 19.25 Black jurors. However, if we had expected something like 198 White jurors, 19 Black jurors, 33 Hispanic jurors, and 25 Other jurors – or something close to that – we probably would not be surprised with our results.

Stated differently, *the data we collected would feel consistent with the hypothesis that the racial distribution of jurors matches the racial distribution of the electorate.* However, what we observed was pretty far from the expected counts. **How do we quantify and make sense of this observation?**

3.3.1 The G-Test

The idea is to introduce a number that measures the difference between the observed and expected rows. There are a variety of numbers that can be used, but let us consider one that is often denoted G. It is defined as follows:

Definition 3.7

Suppose X is a random variable with finitely many values $a_1, \dots, a_n$ and let $p_i = \mathbb{P}[X = a_i]$. Suppose we make N observations of the values $a_1, \dots, a_n$ and that O_i is the number of observations of a_i that we made. Let $E_i = Np_i$ and then define

$$G = 2\sum_i O_i \ln\left(\frac{O_i}{E_i}\right).$$

If $O_i = 0$ for some i, we set the corresponding summand $O_i\left(\frac{O_i}{E_i}\right) = 0$. If there exists an i such that $E_i = 0$ but $O_i \neq 0$, set $G = \infty$.

(Example.) Consider the motivating example with the voters. Define

- The random variable X represents observing the race of a randomly drawn voter from our county. It has 4 possible values (White, Black, Hispanic, Other), so $n = 4$.
- The values p_i are the percentages of the electorate in each racial group.
- The values O_i are the observed counts.
- The values E_i are the expected counts.
- For fun, $N = 275$ (we have 275 total observations across a_1, a_2, a_3, a_4).

Then,

$$G = 2\left(210\ln\left(\frac{210}{198}\right) + 10\ln\left(\frac{10}{19.25}\right) + 20\ln\left(\frac{20}{33}\right) + 35\ln\left(\frac{35}{24.75}\right)\right) \approx 15.84.$$

Remark: If you're inclined to see why $E_i = Np_i$, note that $N = 275$ (that's the number of observations of all the values) and p_i is the percent of the electorate in the racial group i. So, for Black, $E = 275 \cdot 0.07 = 19.25$.

Theorem 3.1: Gibbs' Inequality

We always have $G \geq 0$. Moreover, $G = 0$ if and only if $O_i = E_i$ for all $i = 1, \dots, n$.

The question is simply, how big is "big?" In particular, in our example, can we say 15.84 is a "*big*" value of G? The answer to this question is provided by the following theorem, which we'll state slightly imprecisely and explain in a bit more detail later.

Theorem 3.2: Wilks' Theorem

Suppose the N observations of the values $a_1, \ldots, a_n$ that we make are in fact independent observations of the random variable X. For large values of N, the values of G are well-approximated by a chi-square distribution with $n-1$ degrees of freedom.

There are several points of explanation to make.

- A "chi-square distribution with k degrees of freedom" is a certain function f_k defined on $[0, \infty)$ and taking non-negative values everywhere with total integral equal to 1. In other words, we have $f_k(x) \geq 0$ for all $x \geq 0$ and
$$\int_0^\infty f_k(x)dx = 1.$$
The formula for $f_k(x)$ is complicated and also unimportant for our purposes.

- To say that "the values of G are well-approximated by a chi-square distribution with $n-1$ degrees of freedom" is to say that, for any (not necessarily finite) interval (a, b), the probability that G lands inside the interval (a, b) is approximately
$$\int_a^b f_k(x)dx.$$

(Example.) Notice that
$$\int_0^{15.84} f_3(x)dx \approx 0.999.$$
It follows that
$$\int_{15.84}^\infty f_3(x)dx = 1 - \int_0^{15.84} f_3(x) \approx 1 - 0.999 = 0.001.$$
The number 0.001 is our p-value, and it means that the probability of observing a value of G that is bigger than 15.84 is only about 0.1%. That is quite a small probability, so our calculation suggests that the value of G that we saw is in fact quite large.

Stated differently, with a p-value of 0.001, this indicates that if jurors in this county were truly representative of the county's electorate, there would only be roughly a 0.1% chance of seeing a sample that deviated at least as much from the expected counts as the data that we saw. Because that's such a small probability, this suggests that it's very unlikely that our sample of jurors is actually representative of the county's electorate. We have quantified the observation we made informally above.

- Another thing to look at is "for large values of N." In particular, that this theorem would only work for large values of N. Was $N = 275$ large enough to justify what we did? The answer *depends* on how well you want the values of G to be approximated by a chi-square distribution. The better an approximation you want, the higher a value of N you need. That being said, the following heuristic generally works well.

Theorem 3.3: Heuristic Addendum to Wilks' Theorem

The approximation of G by a chi-square distribution with $n-1$ degrees of freedom is "good enough" as long as the vast majority of the expected counts $E_1, \ldots, E_n$ are all at least 5.

Because all of our expected counts are well above 5, we do not need to worry.

The process (computing expected counts, finding an observed value of G, using a chi-square approximation to find a p-value, i.e., the probability of observing a larger value of G than what we observed if the observations do in fact come from the theoretical distribution) is called a **G-test**. It's a useful technique for a lot of problems in statistics and can be used in codebreaking.

(Exercise.) A professor using an open source introductory statistics book predicts that 60% of the students will purchase a hard copy of the book, 25% will print it out from the web, and 15% will read it online. At the end of the semester she asks her students to complete a survey where they indicate what format of the book they used. Of the 126 students, 71 said they bought a hard copy of the book, 30 said they printed it out from the web, and 25 said they read it online. How well does this data fit the professor's predictions? Run a G-test to find out!

Similar to the introduction of this section, we can create a table.

	Hard Copy	Web	Online	Total
Distribution	60%	25%	15%	
Observed	71	30	25	126
Expected	75.6	31.5	18.9	126

Note that

- X represents observing whether a person reads from a hard copy, web, or online. Therefore, $n = 3$.
- The values p_i represents the percentages that a person chooses to either purchase a hard copy, or print it out, or read it online.
- The values O_i are the observed counts.
- The values E_i are the expected counts.

Calculating the G value, we have

$$G = 2\left(71\ln\left(\frac{71}{75.6}\right) + 30\ln\left(\frac{30}{31.5}\right) + 25\ln\left(\frac{25}{18.9}\right)\right) \approx 2.14403.$$

We now want to see what the probability is of observing a value of G that is bigger than 2.14403. To do this, note that

$$\int_{2.14403}^{\infty} f_2(x) = 1 - \int_0^{2.14403} f_2(x) \approx 1 - 0.65768194886549 = 0.342318.$$

So, 0.342318 is our p-value, and it follows that the probability that we find a higher G value is about 34.23%. In other words, there would be a 34.23% chance of seeing a sample that deviated as least as much from the expected counts as the data we just saw.

3.4 Breaking Rectangular Transposition

Suppose you're given a long passage of ciphertext (with 2808 characters) that is known to be encrypted using rectangular transposition. How do we break the code? We'll talk about a strategy for breaking the code.

1. First, start by making an arbitrary guess for the "period," i.e., the length of the key word. We know that the period has to be a *divisor* of the length of the ciphertext. Note that 2808 has 32 possible divisors:

$$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 18, 24, 26, 27, \ldots, 234, 312, 351, 468, 702, 936, 1404, 2808\}.$$

Since there are only 26 characters in the English alphabet, the period can be at most 26. This means that the period must be one of the following:

$$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 18, 24, 26\}.$$

Suppose we guess that the period is 6.

2. Next, we can arrange our ciphertext into a rectangle of length 6 (the period we guessed). Note that our rectangle will have height $N = \frac{2808}{6} = 468$, so for the sake of being concise only the first few rows will be shown:

```
OIPWMJ
ALWSLE
LJLYEA
MENUAB
IHSDAC
ESRTIE
EMKHAO
AMNPAI
IELNAP
   .
   .
   .
```

3. For every pair of numbers $i \neq j$ between 1 and 6 (the period we guessed), we consider the tall column of width 2 we would get by placing the ith and jth column of the above rectangle next to each other. For example, if $i = 4$ and $j = 2$, we would get the following 468×2 rectangle:

```
WI
SL
YJ
UE
DH
TS
HM
PM
NE
.
.
.
```

4. We can think of this as 468 observations of a pair of English letters *if* the columns i and j were consecutive in the plaintext.In particular, for every pair of letters α and β, we count the number of times that we see the sequence $\alpha\beta$ appearing in this column. Let $O^{(i,j)}_{\alpha\beta}$ be this number. In our truncated example above (in step 3), notice that $O^{(4,2)}_{\text{WI}}$, $O^{(4,2)}_{\text{SL}}$, etc. are all at least 1.

   On the other hand, we can use a large sample of English to calculate the probability $p_{\alpha\beta}$ of the pair $\alpha\beta$ occurring in the English text. We can use these to calculate the expected counts $E_{\alpha\beta} = Np_{\alpha\beta} = 468p_{\alpha\beta}$ and then calculate a corresponding value of G using the observed counts $O^{(i,j)}_{\alpha\beta}$. We can call this $G^{(i,j)}$; in other words,

$$G^{(i,j)} = \sum_{\alpha\beta} O^{(i,j)}_{\alpha\beta} \ln\left(\frac{O^{(i,j)}_{\alpha\beta}}{E_{\alpha\beta}}\right).$$

We can then assemble all of these values[6] of $G^{(i,j)}$ as $i \neq j$ varies into a box of numbers:

$$\begin{bmatrix} \infty & G^{(1,2)} & G^{(1,3)} & G^{(1,4)} & G^{(1,5)} & G^{(1,6)} \\ G^{(2,1)} & \infty & G^{(2,3)} & G^{(2,4)} & G^{(2,5)} & G^{(2,6)} \\ G^{(3,1)} & G^{(3,2)} & \infty & G^{(3,4)} & G^{(3,5)} & G^{(3,6)} \\ G^{(4,1)} & G^{(4,2)} & G^{(4,3)} & \infty & G^{(4,5)} & G^{(4,6)} \\ G^{(5,1)} & G^{(5,2)} & G^{(5,3)} & G^{(5,4)} & \infty & G^{(5,6)} \\ G^{(6,1)} & G^{(6,2)} & G^{(6,3)} & G^{(6,4)} & G^{(6,5)} & \infty \end{bmatrix}.$$

If we guessed the period correctly, then we should find that every row except *one of them* has *one* number that's much smaller than all the others. This tells us something about how to permute the letters to find the plaintext. For example, if we find in the first row that $G^{(1,4)}$ is *much* smaller than the other numbers, that tells us that rows 1 and 4 are likely to be *consecutive* in the plaintext, because the frequency distribution of the pairs that occur in the long 468×2 rectangle displayed earlier is close to the frequency distribution of pairs that occur in the English plaintext.

Note that there are *many* calculations to do by hand. Therefore, we will make use of a compute to do these calculations for us.

(Example.) Suppose our "G-box" is

$$\begin{bmatrix} \infty & 1151.3 & 1090.2 & \underline{\mathbf{485.5}} & 1069.3 & 1005.0 \\ 1234.4 & \infty & 1228.3 & 1049.6 & \underline{\mathbf{440.2}} & 1148.6 \\ \underline{\mathbf{437.5}} & 1044.1 & \infty & 1004.1 & 1164.5 & 933.4 \\ 1154.7 & 1088.6 & 977.3 & \infty & 1115.7 & 1023.6 \\ 1137.2 & 1221.9 & \underline{\mathbf{425.9}} & 1100.0 & \infty & 1070.0 \\ 1003.7 & \underline{\mathbf{442.3}} & 944.9 & 1021.6 & 1086.1 & \infty \end{bmatrix}.$$

The numbers themselves are not very important. *However*, what's important is how every row except one has a number that's significantly smaller than the other numbers on that row. The numbers that are smaller than the others on the same row are bolded and underlined. Notice that every row except the fourth row has a bolded/underlined entry. Now,

- the fact that, in row 1, the 4th column is much smaller than the other entries in that row suggests that columns 1 and 4 in our 468×6 rectangle are consecutive.
- notice that, in row 2, the 5th column is much smaller than the other entries suggests that columns 2 and 5 are consecutive.
- the 4th row not having an entry that's much smaller than the others corresponds to the fact that the 4th column gets reordered to the end.

Observing all the relations this way, and then putting them together, we find that the above G-box leads us to think that the ordering of the columns is $\boxed{6, 2, 5, 3, 1, 4}$.

To clarify how the ordering was obtained, notice how

- in row 1, the smallest number is in column 4.
- in row 2, the smallest number is in column 5.
- in row 3, the smallest number is in column 1.
- in row 4, no number is significantly smaller, so we can assume that the 4th column was reordered to the end.

[6] Note that all the diagonal entries of this box are set to ∞ since we only compute $G^{(i,j)}$ when $i \neq j$. This is an arbitrary convention and the diagonal entries should just be ignored.

- in row 5, the smallest number is in column 3.
- in row 6, the smallest number is in column 2.

With this in mind, notice how we have pairs $(1, 4)$, $(2, 5)$, $(3, 1)$, $(5, 3)$, and $(6, 2)$. If we "connect" the pairs, we end up with

$$(6, 2), (2, 5), (5, 3), (3, 1), (1, 4).$$

Removing the connecting duplicate numbers yields

$$6, 2, 5, 3, 1, 4.$$

(Exercise.) Suppose that, when trying to break rectangular transposition, you find "G-boxes" of the following forms, where the exclamation mark indicates an entry that is much smaller than every other entry on its row. Write down the corresponding decrypting permutation (i.e., the ordering of the columns in the plaintext) that this configuration of values suggests.

(a) $\begin{bmatrix} . & . & . & ! & . \\ . & . & . & . & ! \\ . & . & . & . & . \\ . & ! & . & . & . \\ . & . & ! & . & . \end{bmatrix}$

Notice how

- in row 1, the exclamation mark is in column 4.
- in row 2, the exclamation mark is in column 5.
- in row 3, no exclamation mark exists, implying that 3 will be at the end of the ordering.
- in row 4, the exclamation mark is in column 2.
- in row 5, the exclamation mark is in column 3.

With this in mind, we have the pairs $(1, 4)$, $(2, 5)$, $(4, 2)$, and $(5, 3)$. If we "connect" the pairs, we end up with

$$(1, 4), (4, 2), (2, 5), (5, 3).$$

Joining the pairs (and removing the consecutive equal numbers) yields

$$1, 4, 2, 5, 3.$$

(b) $\begin{bmatrix} . & ! & . & . & . \\ . & . & . & . & . \\ ! & . & . & . & . \\ . & . & ! & . & . \\ . & . & . & ! & . \end{bmatrix}$

We have the pairs $(1, 2)$, $(3, 1)$, $(4, 3)$, and $(5, 4)$. "Connecting" them gives us

$$(5, 4), (4, 3), (3, 1), (1, 2).$$

Joining the pairs, removing the consecutive equal numbers, yields

$$5, 4, 3, 1, 2.$$

(c) $$\begin{bmatrix} . & . & . & ! & . & . & . \\ . & . & . & . & . & . & ! \\ . & ! & . & . & . & . & . \\ . & . & ! & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & ! & . & . \\ . & . & . & . & . & ! & . \end{bmatrix}$$

We have the pairs $(1,4),(2,7),(3,2),(4,3),(6,5),(7,6)$. Connecting them yields

$$(1,4),(4,3),(3,2),(2,7),(7,6),(6,5)$$

Joining the pairs, removing the consecutive equal numbers, yields

$$1,4,3,2,7,6,5.$$

3.5 Interlude: Conditional Probability

Suppose Kambili and Amaka both secretly flip two fair coins.

- Kambili announces that her second flip was heads.
- Amaka announces that she had at least one heads.

Who is more likely to have flipped two heads? In other words, if you had to make a bet about who flipped more heads, who would you bet on?

Definition 3.8: Conditional Probability

Fix a probability space. Given two events A and B, we define the **conditional probability** $\mathbb{P}[A|B]$ by

$$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \cap B]}{\mathbb{P}[B]}.$$

The intuition here is that $\mathbb{P}[A|B]$ represents how confident we are that A happens, *given that we already know* that B happens.

(Example.) Consider the example with Kambili and Amaka. Intuitively, the answer is that "both are equally likely"; that is, both Kambili and Amaka have an equal chance of getting two heads. This is not correct.

To formalize this argument, consider the following:

- The experiment that we're considering involves two coin flips, so we're working with

$$\Omega = \{HH, HT, TH, TT\}.$$

- We're interested in the event

$$A = \{HH\}.$$

In Kambili's situation, we know that her second flip was heads. So, in other words, we're restricting ourselves to the event

$$B_1 = \{HH, TH\}$$

and we have

$$\mathbb{P}[A|B_1] = \frac{\mathbb{P}[A \cap B_1]}{\mathbb{P}[B_1]} = \frac{\mathbb{P}[A]}{\mathbb{P}[B_1]} = \frac{1/4}{1/2} = \frac{1}{2}.$$

Therefore, **the probability that Kambili has two heads** is $\frac{1}{2}$. In Amaka's situation, we only know that one of her flips was heads. In other words, we have the event

$$B_2 = \{HH, TH, HT\}.$$

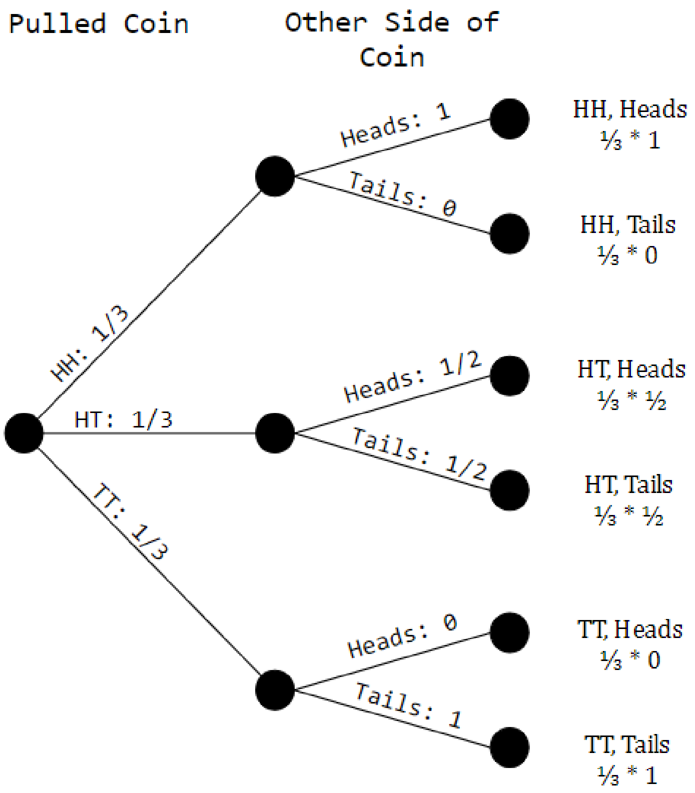
Then,

$$\mathbb{P}[A|B_2] = \frac{\mathbb{P}[A \cap B_2]}{\mathbb{P}[B_2]} = \frac{\mathbb{P}[A]}{\mathbb{P}[B_2]} = \frac{1/4}{3/4} = \frac{1}{3}.$$

Therefore, **the probability that Amaka has two heads** is $\frac{1}{3}$. In other words, Kambili is more likely to have two heads than Amaka.

(Exercise.) There are three coins in a bag. One is a normal quarter: one side is heads, the other side is tails. The second coin is almost identical except that both sides are heads; similarly, both sides of the third coin are tails. You shake the bag around to shuffle the coins. You then close your eyes, pull one coin out at random, put it down on a table, and then open your eyes. You see heads. What is the probability that the other side of the coin is also heads?

Consider the following tree diagram:



So, we want to find the probability that, given we got heads initially, the otherwise will also have heads. This gives us

$$\mathbb{P}[\text{heads}|\text{got heads}] = \frac{\mathbb{P}[\text{heads given heads}]}{\mathbb{P}[\text{got heads}]} = \frac{1/3 \cdot 1}{1/2} = \frac{2}{3}.$$

Note that one way we can think about getting heads is by thinking about the possible face we *can* get; in this case, we can either get $\{H, H, H, T, T, T\}$. We have a $\frac{3}{6} = \frac{1}{2}$ chance of getting heads.

(Exercise.) Suppose 80% of people like peanut butter, 89% like jelly, and 78% like both. Given that a randomly sampled person likes peanut butter, what's the probability that they also like jelly?

Let J be the event that someone likes jelly and B be the event that someone likes peanut butter. We know that

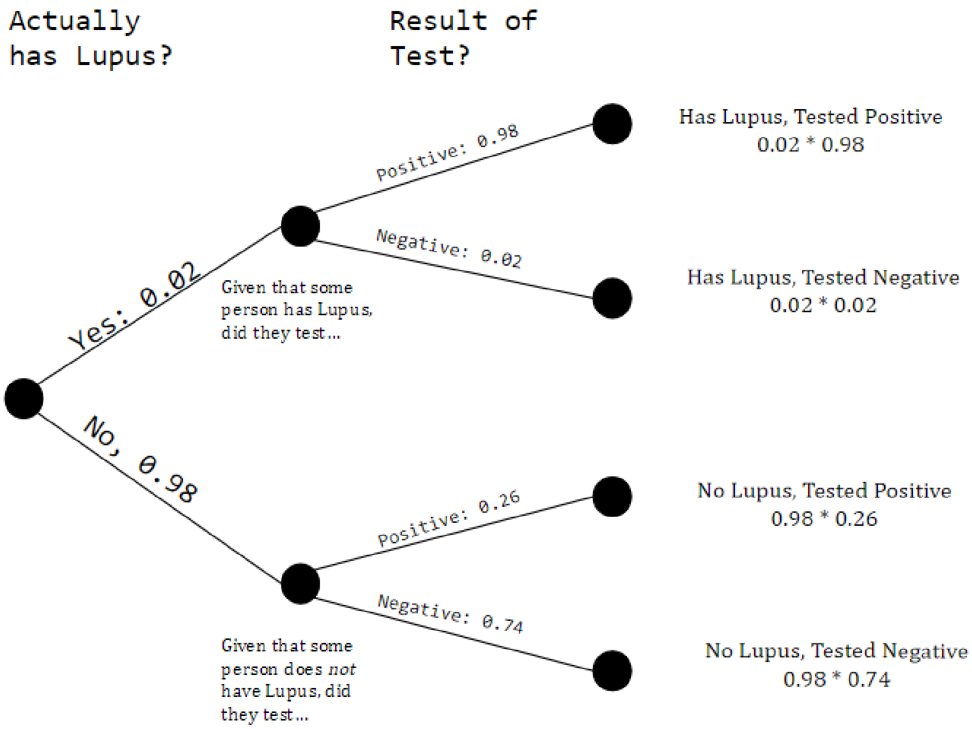
$$PR[B] = 0.80.$$

We also know that $\mathbb{P}[J \cap B] = 0.78$ since 78% of people like *both* peanut butter and jelly. So,

$$\mathbb{P}[J|B] = \frac{\mathbb{P}[J \cap B]}{\mathbb{P}[B]} = \frac{0.78}{0.80} = 0.975.$$

Lupus is a medical phenomenon where antibodies that are supposed to attack foreign cells to prevent infections instead see plasma proteins as foreign bodies, leading to a high risk of blood clotting. It is believed that 2% of the population suffers from this disease. A test for lupus is 98% accurate if a person actually has the disease, and 74% accurate if a person does not have the disease. There is a line from the Fox television show House that is often used after a patient tests positive for lupus: "It's never lupus." Do you think there is truth to this statement? Use appropriate probabilities to support your answer.

Consider the following tree diagram:


Actually has Lupus?
Result of Test?
Yes: 0.02
No, 0.98
Positive: 0.98
Negative: 0.02
Positive: 0.26
Negative: 0.74
Given that some person has Lupus, did they test...
Given that some person does *not* have Lupus, did they test...
Has Lupus, Tested Positive
0.02 * 0.98
Has Lupus, Tested Negative
0.02 * 0.02
No Lupus, Tested Positive
0.98 * 0.26
No Lupus, Tested Negative
0.98 * 0.74

Then,

$$\mathbb{P}[\text{has lupus}|\text{tested positive}] = \frac{\mathbb{P}[\text{has lupus} + \text{tested positive}]}{\mathbb{P}[\text{tested positive}]} = \frac{0.02 \cdot 0.98}{0.02 \cdot 0.98 + 0.98 \cdot 0.26} \approx 0.07142.$$

So, there is some truth to the statement since if someone tests positive for lupus, there's only 7.14% that they have lupus.

Definition 3.9: Independent Events

Fix a probability space. We say that two events A and B are independent if

$$\mathbb{P}[A \cap B] = \mathbb{P}[A]\mathbb{P}[B].$$

Often, it's convenient to reformulate this definition slightly. In the case that $\mathbb{P}[B] > 0$,

$$\mathbb{P}[A \cap B] = \mathbb{P}[A]\mathbb{P}[B] \iff \frac{\mathbb{P}[A \cap B]}{\mathbb{P}[B]} = \mathbb{P}[A].$$

However, notice that

$$\frac{\mathbb{P}[A \cap B]}{\mathbb{P}[B]} = \mathbb{P}[A|B]$$

so it follows that the independence of A and B is equivalent to asserting that

$$\mathbb{P}[A|B] = \mathbb{P}[A].$$

We could interpret this statement as follows: if A and B are independent, then our confidence in A happening does not change at all even if we're told that B happened (or did not happen). More loosely, knowing whether or not B happens tells us "nothing" about whether or not A happenes.

(Exercise.) The American Community Survey is an ongoing survey that provides data every year to give communities the current information they need to plan investments and services. The 2010 American Community Survey estimates that 14.6% of Americans live below the poverty line, 20.7% speak a language other than English at home, and 4.2% fall into both categories. Is the event that a randomly chosen American lives below the poverty line independent of the event that the person speaks a language other than English at home?

Define

$$\mathbb{P}[\text{Below Poverty Line}] = 0.146,$$

$$\mathbb{P}[\text{Speak Language Other Than English}] = 0.207,$$

$$\mathbb{P}[\text{Below Poverty Line AND Speak Language Other Than English}] = 0.042.$$

Using the formula in (3.9), notice how

$$0.042 \neq 0.146(0.207) = 0.030222.$$

(Exercise.) A bag contains 5 red marbles and 3 blue marbles. Two marbles are drawn randomly from the bag: Alejandra takes the first one and Beatrice takes the second. Is the event that Alejandra's marble is blue independent of the event that Beatrice's marble is blue?

No. If Alejandra takes the first marble and doesn't put it back, then it's possible that she took the blue marble, which affects the probability that Beatrice gets a blue marble.

Definition 3.10

Fix a probability space. Two random variables X and Y are **independent** if the events $X = a$ and $Y = b$ are independent for all pairs (a, b) where a is a value of X and b a value of Y.