MODULAR ARITHMETIC AND CIPHERS

BEGINNERS NOVEMBER 1, 2015

Warm Up Problem

Two non-zero numbers p and q are **multiplicative inverses** of each other if $p \cdot q = 1$.
In the usual arithmetic, these are easy to find:

(1) Find the multiplicative inverse of
   (a) 2
   1/2

   (b) 100
   1/100

   (c) 1/7
   7

(2) Notice how multiplying a value by a number and then by its multiplicative inverse returns the original number. (In other words, multiplying by the inverse of a number "undoes" multiplication by the number)

   (a) Pick a number. Let's call this number n.

   $n =$ 5 (any number works)

   (b) Pick another number, p, and find its inverse, q.

   $p =$ 7

   $q =$ 1/7

   (c) What is $n \cdot p \cdot q$? Can you explain why $n \cdot p \cdot q = n$?
   $5 \times 7 \times 1/7 = 5 \times (7 \times 1/7) = 5 \times 1 = 5$

   (d) What is the inverse of q? 7

In modular arithmetic, multiplicative inverses are a bit different and a lot harder to find. We can use a multiplication table to help us find multiplicative inverses in modular arithmetic. Fill out the multiplication table in modulo 10 below. Part of the table is already filled out.

·	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

(1) Using the table above, find the multiplicative inverses of the following numbers in mod 10 arithmetic:

(a) 1

1

(b) 3

7

(c) 9

9

(d) 2? It doesn't exist.

Here is a cipher key. You will need this later for the rest of the handout.

Letter	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
Number	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

Caesar Cipher

Suppose that Alice and Bob are trying to send secret letters to each other in the mail. In order for the letters to stay a secret, they want to think of a way to send the messages in a "secret code" so that anybody who tries to intercept the message wouldn't be able to read it even if they managed to intercept it. One way they can do this is using a Caesar Cipher. In a Caesar cipher, the alphabet is shifted a certain number of places and each letter is replaced by the corresponding letter.

For example, say Alice and Bob agree that they want to shift the letters by three:

TO ENCRYPT

(1) Using the cipher key, they would first convert the letters in their message to their corresponding numbers to get a numerical message:

Letter Message	M	E	E	T		M	E		A	T		T	H	E		Z	O	O
Numerical Message	12	4	4	19		12	4		0	19		19	7	4		25	14	14

(2) Then they would then shift all the numbers in their message up by three:

Unshifted Numerical Message	12	4	4	19		12	4		0	19		19	7	4		25	14	14
Shifted Numerical Message	15	7	7	22		15	7		3	22		22	10	7		2	17	17

(a) Can we have numbers greater than 25 in our shifted numerical message? Why or why not?

No, there isn't a number which corresponds to a number greater than 25 in our cipher key.

(b) What do we do if a numbers in the numerical message is greater than 25?

After shifting by 3, we subtract 26 from it.

(c) Explain how this is similar to modular arithmetic.
The numbers "cycle" around like in a clock.

(d) If d is a number in our decrypted numerical message (our numerical message before we have performed the shift) and e is a number in our numerical encrypted message (our numerical message after we have performed the shift) what would the relationship between d and e be if we were shifting by 3?

$$e = d + \underline{3} \ (mod \ \underline{26})$$

(3) Then, using the cipher key, they would convert the resulting numerical message into a letter message.

Shifted Numerical Message	15	7	7	22		15	7		3	22		22	10	7		2	17	17
Encrypted Letter Message	P	H	H	W		P	H		D	W		W	K	H		C	R	R

TO DECRYPT

(1) Using the cipher key, they would first convert the letters in their message to their corresponding numbers to get a numerical message:

Encrypted Letter Message	R	N		V	H	H		B	R	X		W	K	H	Q
Numerical Message	17	13		21	7	7		1	17	23		22	10	7	16

(2) Then they would then shift all the numbers in their message down by three:

Unshifted Numerical Message	17	13		21	7	7		1	17	23		22	10	7	16
Shifted Numerical Message	14	10		18	4	4		24	14	20		19	7	4	13

(a) What do we do if a number in the numerical message is less than 0?

After we have shifted down by three, add 26.

(b) If e is a number in our encrypted numerical message (our numerical message before we have performed the shift) and d is a number in our decrypted numerical message (our numerical message after we have performed the shift) what would the relationship between d and e be?

$$d = e - \underline{3} \ (mod \ \underline{26})$$

(3) Then, using the cipher key, they would convert the resulting numerical message into a letter message.

Shifted Numerical Message	14	10		18	4	4		24	14	20		19	7	4	13
Decrypted Letter Message	O	K		S	E	E		Y	O	U		T	H	E	N

Cracking the Caesar Cipher

As you can see, encrypting and decrypting is very easy in the Caesar cipher. However the Caesar cipher is not very safe. In fact, a computer program can crack a short Caesar cipher in less than a second!

(1) Suppose we want to shift our alphabet forward by p places to encrypt, where $p < 26$. If e is a number in our encrypted numerical message (our numerical message after we have performed the shift) and d is the corresponding number in our decrypted numerical message (our numerical message before we have performed the shift) what would the relationship between e and d be?

$e = d + p \pmod{26}$

(2) Suppose the alphabet contained m letters and we wanted to shift the alphabet forward by 15 places. $(m > 15)$ If e is a number in our encrypted numerical message (our numerical message before we have performed the shift) and d is the corresponding number in our decrypted numerical message (our numerical message after we have performed the shift) what would the relationship between d and e be?

$e = d + 15 \pmod{m}$

(3) How many possible values can we choose to shift our 26 letter alphabet by? How many possible ways can a message be encrypted?

If we count shifting by zero as one way to encrypt, then 26. If not, then 25.

(4) To crack a Caesar cipher in our 26 letter alphabet, how many tries do we need before we're guaranteed to crack a message?

26 or 25, depending on the last answer.
We crack the Caesar cipher by shifting the message by 1, 2, ..., 25 until we see a message that is readable.

Improving the Caesar Cipher

Encrypting Using Multiplicative Encoders

Alice and Bob realize that the Caesar Cipher isn't very safe, so they decide to try and come up with a different cipher. However, they want to keep the idea of using modular arithmetic. Instead of adding p to each number in modular arithmetic to encrypt messages, they want to try multiplying each number by p to encrypt messages. In order to test this method they will start with messages consisting of numbers.

(1) They first want to try to encrypt the numbers 0 to 9 by multiplying them by $p = 7$ in modulo 10. In other words, $e = d \cdot 7 \ (mod\ 10)$. Fill out the chart below:

d: Unencrypted Number	e: Encrypted Number (Multiplying by 7 in Modulo 10)
0	$0 \times 7 = 0 \ (mod\ 10)$
1	7
2	4
3	1
4	8
5	5
6	2
7	9
8	6
9	3

(2) Do you think that 7 is a good choice of a number to multiply by for encrypting? Why or why not?

Yes. Every number is encrypted to a unique number.

(3) Next, they want to see if they can use a different value of p to encrypt encrypt the numbers 0 to 9. Bob decides that he wants to try multiplying them by $p = 5$ in modulo 10. In other words, $e = d \cdot 5 \ (mod\ 10)$. Fill out the chart below:

d: Unencrypted Number	e: Encrypted Number (Multiplying by 5 in Modulo 10)
0	$0 \times 5 = 0 \ (mod\ 10)$
1	5
2	0
3	5
4	0
5	5
6	0
7	5
8	0
9	5

(4) Do you think that 5 is a good choice of a number to multiply by for encrypting? Why or why not?

NO, all the numbers get encrypted to either a zero or five. This would not work because if we get a message like "50", we would not be able to determine if it gets decrypted to "32" or "94" or "16", etc.

(5) As you can see, not all numbers make good choices for p. We will call the numbers that are good choices **multiplicative encoders**.

(a) List all the numbers between 2 and 9 that are multiplicative encoders in modulo 10. For each multiplicative encoder, 10, find $\gcd(p, 10)$, i.e., the greatest common divisor of p and 10.

- 3 : gcd (3, 10) = 1
- 7 : gcd (7, 10) = 1
- 9 : gcd (9, 10) = 1

(b) List all the numbers between 2 and 9 that are not multiplicative encoders in modulo 10. For each non-multiplicative inverse, n, find $\gcd(n, 10)$.

- 2 : gcd (2, 10) = 2
- 4 : gcd (4, 10) = 2
- 5 : gcd (5, 10) = 5
- 6 : gcd (6, 10) = 2
- 8 : gcd (8, 10) = 2

(c) We say that 1 **is** a multiplicative encoder because every number will be encoded to a unique number. However, it would be a better idea to choose a different multiplicative encoder in modulo 10. Why?

A message encrypted with the multiplicative encoder 1 would look the same as the original message. This isn't very good for keeping the message a secret!

(6) Choosing a different modulus (other than 10) makes things more interesting.

(a) List all the numbers between 2 and 6 that are multiplicative encoders in modulo 7. For each multiplicative encoder, p, find $\gcd(p, 7)$.

- 2 : gcd(2,7)=1
- 3 : gcd(3,7)=1
- 4 : gcd(4,7)=1
- 5 : gcd(5,7)=1
- 6 : gcd(6,7)=1

(b) List all the numbers between 2 and 6 that are not multiplicative encoders in modulo 7. For each number n which is not a multiplicative encoder find $\gcd(n, 7)$.

None !

Decrypting With Multiplicative Inverses

(1) Do you notice any patterns for which numbers are multiplicative encoders and which numbers are not?
Multiplicative encoders don't have any common denominators with the modulus aside from 1.

(2) Two numbers p and m are called **co-prime** if the greatest common divisor of p and m is 1. For a given modulus m, any number $p < m$ that is coprime with m is a multiplicative encoder.

(3) Furthermore, if p and m are co-primes, then there exists another number less than m called q such that $p \cdot q = 1 \ (mod\ m)$. We call q the **multiplicative inverse** of p.

(a) Suppose we are working in modulo 12. Determine whether the following numbers are coprime to 12. If they are coprime to 12, find their multiplicative inverse. If they are not coprime to 12, explain why.

(i) 4 No, because $\gcd(4,12) = 4 \neq 1$.

(ii) 11 Yes, $11 \times 11 = 121 \equiv 1 \pmod{12}$

(iii) 1 Yes, $1 \times 1 = 1 \equiv 1 \pmod{12}$

(b) Now suppose we are working in modulo 9. For each number, determine whether it is coprime to 9. If it is coprime, find its multiplicative inverse. If not, explain why not.

(i) 7 Yes, $4 \times 7 = 28 \equiv 1 \pmod 9$

(ii) 4 Yes, $7 \times 4 = 28 \equiv 1 \pmod 9$

(iii) 3 No, $\gcd(3,9) = 3 \neq 1$

(iv) 8 Yes, $8 \times 8 = 64 \equiv 1 \pmod 9$

(v) 2 Yes, $5 \times 2 = 10 \equiv 1 \pmod 9$

Alice believes that we can use the idea of multiplicative inverses to decrypt our messages without having to refer to the chart we made on Page 8. After all, if we can undo addition in the Caesar cipher by performing subtraction, then we should be able to undo the multiplication like we did during the warm up!

(1) Find the multiplicative inverse of $p = 7$ in modulo 10. Let this be q. (Hint: use the multiplication table from the warmup.)

$q =$ 3

(2) Let's try to decrypt the encrypted numbers from 0 to 9:

Unencrypted Number	Encrypted Number (Multiplying the Unencrypted Number by p in Modulo 10)	Decrypted Number (Multiplying the Encrypted Number by q in Modulo 10)
0	$0 \times p = 0 \pmod{10}$	$0 \times q = 0 \pmod{10}$
1	7	$7 \times 3 = 21 \equiv 1$
2	4	$4 \times 3 = 12 \equiv 2$
3	1	$1 \times 3 = 3 \equiv 3$
4	8	$8 \times 3 = 24 \equiv 4$
5	5	$5 \times 3 = 15 \equiv 5$
6	2	$2 \times 3 = 6 \equiv 6$
7	9	$9 \times 3 = 27 \equiv 7$
8	6	$6 \times 3 = 18 \equiv 8$
9	3	$3 \times 3 = 9 \equiv 9$

(3) Were we able to successfully encrypt and decrypt the message using p and q?

Yes! Multiplying the encrypted number with the inverse decrypted it.

(4) Can you think of an explanation as to why this works?

Like in the warm up, multiplying a number by p and then the inverse of p gives the number because $p \times (p \text{ inverse}) = 1$, so $n \times p \times (p \text{ inversed} = n \times 1 = n$.

Simplified RSA

One of the most popular ciphers to keep online data such as emails and credit card information safe is called RSA. It is based on the idea of using multiplicative inverses to encrypt and decrypt messages. Because RSA is a little bit more complicated than the cipher Alice and Bob have come up with, we will call their cipher "Simplified RSA". Now that we understand how simplified RSA works, let's try to encrypt and decrypt some messages!

Encrypting A Message

Alice told you that in order to send a message to her, you should use the multiplicative encoder $p = 11$ in modulo 50.

(1) You decide to send her the following message by first using the cipher key to obtain a numerical message:

Letter Message	T	E	L	L		M	E		A		J	O	K	E
Numerical Message	19	4	11	11		12	4		0		9	14	10	4

(2) Then you encrypt the numerical message by multiplying each number by 11 in modulo 50:

Unencrypted Numerical Message	19	4	11	11		12	4		0		9	14	10	4
Encrypted Numerical Message	$19\times11=209$ $=9 \pmod{50}$	44	21	21		32	44		0		49	4	10	44

(3) Because there are less than 50 letters in the English alphabet, we can just send the message in its numerical form

Decrypting a Message

Alice replied "I didn't have time to encrypt the entire message, so I only encrypted the answer to the following joke: 'What do you call a fake noodle?'".

(1) You decrypt the answer using the multiplicative inverse of 11 in modulo 50, which is 41.

Encrypted Numerical Message	0	43		38	32	15	0	48	9	0
Unencrypted Numerical Message	$0 \times 41 = 0 \pmod{50}$	13		8	12	15	0	18	19	0

(2) Then you translate the decrypted numerical message into the English alphabet using the cipher key.

Decrypted Numerical Message	0	13		8	12	15	0	18	19	0
Decrypted Letter Message	A	N		I	M	P	A	S	T	A

Cracking Simplified RSA

Alice claims "As you can see, it's very hard to find the right decryption key when we use very large numbers, even if we know what the encryption key is in simplified RSA." However Bob is concerned and asks "That might be true, but what if someone tries to crack the code by trying a lot of different decryption keys?"

Bob and Alice are both right, but let's analyze how true their statements are.

(1) Suppose a hacker knows that Alice and Bob are communicating in modulo 50. How many different encryption keys does he have to try before he is guaranteed to crack their secret message? (Assume we can use 1 as a encryption key.)

He would have to try all the keys which are multiplicative encoders of 50. (ie, are coprime to 50) These are:

1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49.

There are 20 in all so he would have to try 20 times.

(2) Suppose a hacker doesn't know that Alice and Bob are communicating in modulo 50. How would he go about trying to crack the cipher?

He would try all the encryption keys for 1, 2, ... all the way until he gets the right one. (There's a lot).

(3) Can you think of another way we can crack Simplified RSA without having to try a lot of different encryption keys?

Since Simplified RSA is basically a substitution cipher, we know that each letter will get ~~to a num~~ encrypted to another unique number. We can crack this by performing a frequency analysis on the numbers which appear in the encrypted message, and then matching those to the frequencies of the english language. For example, we know that 'E' is the most common english letter used. So if we have an encrypted message that has a lot of '49's, then there's a good chance that '49' will be decrypted to 'E'.