

Clock Arithmetic and Euclid's Algorithm

Earlier we discussed Caesar Shifts and other substitution ciphers, and we saw how easy it was to break these ciphers by using frequency analysis. The next breakthrough in cryptography came with the invention of computers. Since computers only deal with strings of 0's and 1's, each letter in a message is replaced by its ASCII binary number, and that long string of numbers is scrambled, sent, and then descrambled and read. In the 1970's, Horst Feistel developed the Lucifer system which encrypts messages according to a scrambling operation. The only problem with this system was that the sender and receiver must first agree on a key which is the scrambling algorithm.

This problem of key distribution was a main concern for cryptographers. But in 1977 Ronald Rivest, Adi Shamir and Leonard Adleman solved that problem with the encryption method known as RSA. This idea is based on the fact that it is easy to multiply numbers, but it is difficult to factor a number into primes. Before we can fully explain their method, we need to learn some stuff about numbers.

Definitions

Here are some words which will occur in our discussion today.

Definition 1. An integer b is **divisible** by an integer a , not zero, if there is an integer x such that $b = ax$, and we write $a|b$. If b is not divisible by a , we write $a \nmid b$.

Example 1. 14 is divisible by 7 because $14 = 7 \times 2$, and we write $7|14$.

Definition 2. The integer a is a **common divisor** of b and c if $a|b$ and $a|c$. Since there is a finite number of common divisors, the greatest one is called the **greatest common divisor** of b and c and is denoted by (b, c) or by $\gcd(b, c)$.

Example 2. 6 is a common divisor of 24 and 120, but 24 is their greatest common divisor, i.e., $(24, 120) = 24$.

Definition 3. We say that a and b are **relatively prime** if $(a, b) = 1$.

Definition 4. An integer $p > 1$ is called a **prime number** or a **prime** if there is no divisor d of p satisfying $1 < d < p$. If an integer $a > 1$ is not a prime, it is a **composite number**.

Clock Arithmetic

Addition

I think the best way to first explain this type of arithmetic is through an example.

Example 3. If it is 10 o'clock (we don't care about am and pm) and Josh is picking you up in 7 hours, assuming he is on time, what time will he be there?

Solution.

□

This is a simple problem, one that we have done since about 2nd grade. But what is really going on here? We add the numbers together, but we don't care about how many revolutions are made, just about what is left over. For small numbers like these, we see that it is easy enough to add and figure out the correct number, but for large numbers can you figure out a fast way to do this?

Example 4. If it is 5 o'clock and you have to leave for the airport in 39 hours, what time do you need to leave?

Solution.

□

Example 5. If it is 8 o'clock, and you have an appointment in 1984604 hours, what time is your appointment?

Solution.

□

Example 6. Let's do an example dealing with encryption. First we will assign a number value to each letter in the alphabet according to the table below. Now we want to send the message "REPLY" to someone using a clock arithmetic Caesar shift. For each letter in the message, replace it with its number value. Put each of those values in our encrypting function $f(x) = x + 4 \pmod{26}$. Find the corresponding letter for the new numbers. What is your encrypted message?

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

Solution.

□

The fancy math term for this type of arithmetic is called **modular arithmetic**, and we write $a \equiv b \pmod{n}$ (we say a is congruent to $b \pmod{n}$) when $a - b$ is a multiple of n . When we write $a \equiv b \pmod{n}$ and if $0 \leq b < n$ then b is called the **residue** of $a \pmod{n}$. To demonstrate the idea of modular arithmetic let's look at example 3 above. We have $10 + 7 \equiv 5 \pmod{12}$ because $10 + 7 - 5$ is a multiple of 12, or equivalently, $10 + 7$ divided by 12 has a remainder of 5. And we can say that 5 is the residue of $17 \pmod{12}$.

In example 5 above we have $8 + 1984604 \equiv 4 \pmod{12}$ since $8 + 1984604$ divided by 12 has a remainder of 4, or $8 + 1984604 - 4$ is a multiple of 12.

Here are some important properties of modular arithmetic:

Property 1: If a, b , and n are integers, and if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

Property 2: If a, b , and n are integers, and if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

These properties just demonstrate that this type of arithmetic behaves like we want it to. But let's look at some examples.

Example 7. We know that $17 \equiv 2 \pmod{5}$ and $14 \equiv 4 \pmod{5}$, find $17 + 14 \pmod{5}$.

Solution.

□

Example 8. Solve for x in the equation $x - 8 \equiv 3 \pmod{13}$.

Solution.

□

Exercise 1. List all of the integers x between 1 and 50 which satisfy $x \equiv 7 \pmod{17}$.

Exercise 2. Fill in the missing residue numbers:

1. $19 \equiv \underline{\hspace{1cm}} \pmod{6}$
2. $20568 \equiv \underline{\hspace{1cm}} \pmod{19}$
3. $-3 \equiv \underline{\hspace{1cm}} \pmod{11}$

Exercise 3. Solve for x in the equation $3 - x \equiv 7 \pmod{8}$.

Exercise 4. What function would we use to decrypt our message in Example 6?

Let's look at the addition table for modulus 5:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Note that if n were large it would not be profitable to make a huge addition table.

Exercise 5. Suppose we had a function $f(x) = x + 2 \pmod{5}$. Compute the following:

1. $f(3)$
2. $f(1)$
3. $f(2)$

Exercise 6. Now suppose we are given that $g(x) = x - 2 \pmod{5}$. (The inverse or "undo" function of $f(x)$.) Compute the following:

1. $g(0)$
2. $g(3)$
3. $g(4)$

Exercise 7. Can you think of another formula which would give you $g(x)$, the inverse function of $f(x)$?

There are some subtleties happening with $g(x)$. How did we find $g(x)$? Simple, we just needed to find out how to undo whatever happened in $f(x)$. Since we added 2 to our value in $f(x)$, then we would just need to subtract 2 (or add -2) to get $g(x)$. What we are really doing is finding the additive inverse for 2. If we have a number a , then its **additive inverse** is a number b such that $a + b \equiv 0$. Now we can look at our addition table above to see what the additive inverse of $2 \pmod{5}$ is, and we see it is 3, or rather any number $\equiv 3 \pmod{5}$. Hence another form of $g(x)$ could be $g(x) = x + 3 \pmod{5}$ or even $g(x) = x + 28 \pmod{5}$. Check for yourself that we get the same values.

Exercise 8. Find the additive inverses of the following:

1. $3 \pmod{39}$
2. $18 \pmod{56}$
3. $-4 \pmod{20}$

Multiplication

Multiplication also behaves like we want as the next property says.

Property 3: If a, b , and n are integers, and if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Example 9. What is $3 \times 7 \times 9 \pmod{5}$.

Solution.

□

Example 10. Find $7^5 \pmod{9}$.

Solution.

□

Exercise 9. Fill in the missing residue numbers:

1. $2^{10} \equiv \underline{\hspace{1cm}} \pmod{7}$

2. $4^{20} \equiv \underline{\hspace{1cm}} \pmod{5}$

Here is the multiplication table for modulo 5.

\times	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Exercise 10. Let $f(x) = 2x \pmod{5}$. Compute the following:

1. $f(3)$

2. $f(1)$

3. $f(2)$

What is the inverse of this function? Is it $g(x) = \frac{x}{2}$? If it were then $g(1) = \frac{1}{2}$ which is not possible. So how do we find $g(x)$?

To answer this question we need to find the multiplicative inverse of 2. If we have a number a , its **multiplicative inverse** is a number c such that $ac \equiv 1$. Now we can look at our multiplication table to find the multiplicative inverse of 2, which we see is 3.

Exercise 11. Compute the following with $g(x) = 3x \pmod{5}$.

1. $g(1)$
2. $g(2)$
3. $g(4)$

Exercise 12. Using the same table in example 6, encrypt the message "ATTACK AT DAWN" using the function $f(x) = 5x \pmod{26}$

Exercise 13. Can you find the inverse function needed to decrypt your message from exercise 12?

Finding Multiplicative Inverses

Example 11. Make a multiplication table for mod 6, and then make a table of multiplicative inverses.

Here are the tables:

\times	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

a	b
0	
1	
2	
3	
4	
5	

We notice that not all of the values have inverses. Can you find a reason why some have an inverse and some do not? Is there any kind of pattern you notice in the multiplication table?

If we look at the table, we notice that not all of the rows have every number represented, and the only rows that have all of the numbers represented are the rows with inverses. Also the rows without all of the numbers represented have a repeating pattern to them.

Theorem 1. Let a and n be integers with $0 < a < n$, and suppose they share a common divisor. Then a does not have a multiplicative inverse mod n .

Proof. Let b be the common divisor of a and n . In other words we can factor a and n and get two integers c, m with $a = bc$ and $n = bm$. Suppose also that a does have a multiplicative inverse, and call it d . Then $ad \equiv bcd \equiv 1 \pmod{n}$, so by multiplying both sides by m , we have $bcdm \equiv m \pmod{n}$. But $bm = n$ which implies that $bcdm \equiv 0 \pmod{n}$, which is a contradiction. Therefore a does not have a multiplicative inverse. \square

We will see that a number a has a multiplicative inverse mod n if and only if the gcd of a and n is 1, i.e. $(a, n) = 1$.

Note that primes are special because all nonzero numbers mod p have a multiplicative inverse.

Example 12. Find the multiplicative inverse of 8 mod 11.

Solution.

□

Exercise 14. Solve $8x \equiv 3 \pmod{11}$.

Exercise 15. Find $5^{-1} \pmod{26}$.

Exercise 16. Using your answer from exercise 15, decrypt your message you made in exercise 12.

Euclid's Algorithm

If our numbers are large, then it would usually take too long to try to guess what the correct inverse value is. So we have something called Euclid's Algorithm to help us find the inverses. Recall that an algorithm is a set of instructions that you repeat until you finish your task. Euclid's Algorithm actually is used to find the gcd (greatest common divisor) of two integers, but we can also use it to find inverses.

There is another important algorithm associated to Euclid's algorithm called the Division Algorithm.

Theorem 2 (The Division Algorithm). Given any integers a and b , with $a > 0$, there exist unique integers q and r such that $b = qa + r$, $0 \leq r < a$. If $a \nmid b$, then r satisfies the stronger inequalities $0 < r < a$.

The division algorithm is most likely something that you are already familiar with, but it is a powerful tool and necessary to understand in order to find multiplicative inverses.

Let's first demonstrate Euclid's algorithm with our previous exercise, and then we will formulate the algorithm exactly.

We want to find the inverse of $8 \pmod{11}$.

1. Divide one number into the other, $11 \div 8 = 1$ with a remainder of 3. We will now rewrite this as $11 = 8 \times 1 + 3$.
2. Now instead of concentrating on 8 and 11, focus on 8 and 3, and do the same step. $8 \div 3 = 2$ with a remainder of 2, so we write $8 = 3 \times 2 + 2$.
3. Continue now with 3 and 2. $3 \div 2 = 1$ with a remainder of 1, so we write $3 = 2 \times 1 + 1$.
4. Now we do the same with 2 and 1. $2 \div 1 = 2$ with a remainder of 0, so we write $2 = 1 \times 2 + 0$, and we stop since we now have a remainder of 0.

This algorithm has told us right now that the gcd of 8 and 11 is 1 because that is the last nonzero remainder value that we have. The second part of the algorithm is a method to write $1 = 8x + 11y$ for some integers x and y . To do this we work backwards from the above equations.

- 3'. We have $3 = 2 \times 1 + 1$, so we re-write this equation to be $1 = 3 - 2 \times 1$.
- 2'. We write $2 = 8 - 3 \times 2$ from step 2 above and substitute this into our equation from 3' to get $1 = 3 - (8 - 3 \times 2) \times 1 = 3 - (8 - 3 \times 2)$. We can do some combining of like terms to get $1 = 3 \times 3 - 8$.
- 1'. We write $3 = 11 - 8 \times 1$ from step 1 above and substitute this into our equation from 2' to get $1 = (11 - 8 \times 1) \times 3 - 8$. Now we combine like terms until we have the form $1 = 8x + 11y$. Our answer is $1 = 8 \times -4 + 11 \times 3$ which we can easily check.

Now how does this help us find our inverse? Well, now we take that equation mod 11. $8 \times -4 + 11 \times 3 \equiv 1 \pmod{11}$, but $11 \times 3 \equiv 0 \pmod{11}$, so $8 \times -4 \equiv 1 \pmod{11}$ and -4 is our inverse. Usually we like to write the inverse as a positive number, so now we need to find out what $-4 \pmod{11}$ is. But we know $-4 \equiv 7 \pmod{11}$, so the multiplicative inverse of $8 \pmod{11}$ is 7 .

Let's do the same example but organize the information so we can see it easier.

We are going to compute $8^{-1} \pmod{11}$.

$$\begin{array}{l|l} \mathbf{11} = \mathbf{8}(1) + \mathbf{3} & 3 = 11 - 8(1) \\ \mathbf{8} = \mathbf{3}(2) + \mathbf{2} & 2 = 8 - 3(2) \\ \mathbf{3} = \mathbf{2}(1) + \mathbf{1} & 1 = 3 - 2(1) \\ \mathbf{2} = \mathbf{1}(2) & \end{array}$$

Now reverse the process using the equations on the right.

$$\begin{aligned} 1 &= 3 - 2(1) \\ 1 &= 3 - (8 - 3(2)) = 3(3) - 8 \\ 1 &= (11 - 8(1))(3) - 8 = 11(3) - 8(4) = 11(3) + 8(-4) \end{aligned}$$

Be careful about the order of the numbers. We do not want to accidentally switch the bolded numbers with the non-bolded numbers.

Here is the exact formulation of Euclid's Algorithm:

Theorem 3 (The Euclid Algorithm). Given integers b and $c > 0$, we make a repeated application of the division algorithm to obtain a series of equations

$$\begin{aligned} b &= cq_1 + r_1, 0 < r_1 < c, \\ c &= r_1q_2 + r_2, 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, 0 < r_3 < r_2, \\ &\dots \\ r_{j-2} &= r_{j-1}q_j + r_j, 0 < r_j < r_{j-1} \\ r_{j-1} &= r_jq_{j+1}. \end{aligned}$$

The greatest common divisor (b, c) of b and c is r_j , the last nonzero remainder in the division process. Values of x_0 and y_0 in $(b, c) = bx_0 + cy_0$ can be obtained by writing each r_i as a linear combination of b and c .

Let's look at another example because this algorithm requires some practice to become familiar with it.

Example 13. Find the gcd of 42823 and 6409.

Solution.

□

How does this algorithm actually give the gcd? It seems kind of strange that we can get the gcd of two numbers a and b by looking at the gcd's of the subsequent remainder values. Notice that the division algorithm gives us the equation $a = bq_1 + r_1$, and since the gcd divides a and b it must divide r_1 . Similarly in the next equation $b = r_1q_2 + r_2$, the gcd divides b and r_1 , so it must also divide r_2 . Going the other direction, we notice that if some number divides r_1 and r_2 , then it must divide b and hence then also a . Therefore this algorithm does give us the gcd of a and b . But enough of these explanations, let's get back to some examples and exercises.

Example 14. Find integers x and y to satisfy

$$42823x + 6409y = 17.$$

Solution.

□

Exercise 17. Find the gcd of:

1. 7469 and 2464

2. 2689 and 4001

3. 2947 and 3997

4. 1109 and 4999

Exercise 18. Find the greatest common divisor g of the numbers 1819 and 3587, and then find integers x and y to satisfy

$$1819x + 3587y = g$$

Exercise 19. Find the multiplicative inverses of the following:

1. $50 \pmod{71}$

2. $43 \pmod{64}$

Exercise 20. Using the information from the previous exercise, solve the following equation for x and check your answer.

$$50x \equiv 63 \pmod{71}.$$

Exercise 21. Solve $12345x \equiv 6 \pmod{54321}$. Hint: First find the gcd.