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 knows 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 $a \not| b$.

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 $f(x) \equiv x + 4 \mod 26$. 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 $a \equiv b \mod n$ (we say a is congruent to b mod n) when $a - b$ is a multiple of n. When we write $a \equiv b \mod n$ and if $0 \leq b < n$ then b is called the **residue** of $a \mod n$. To demonstrate the idea of modular arithmetic let's look at our first example above. We have $10 + 7 \equiv 5 \mod 12$ 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 $17 \mod 12$.

In example 3 above we have $8 + 1984604 \equiv 4 \mod 12$ 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 $a \equiv b \mod n$, then $b \equiv a \mod n$.
Property 2: If a, b, and n are integers, and if $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$.

These properies 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 $17 \equiv 2 \mod 5$ and $14 \equiv 4 \mod 5$, find $17 + 14 \mod 5$.

Solution. □

Example 8. Solve for x in the equation $x - 8 \equiv 3 \mod 13$.

Solution. □

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

Exercise 2. Fill in the missing residue numbers:

1. $19 \equiv$ ____ mod 6
2. $20568 \equiv$ ____ mod 19
3. $-3 \equiv$ ____ mod 11

Exercise 3. Solve for x in the equation $3 - x \equiv 7 \mod 8$.

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 $f(x) = x + 2 \mod 5$. Compute the following:

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

Exercise 6. Now suppose we are given that $g(x) = x - 2 \mod 5$. (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 $\mod 5$ is, and we see it is 3, or rather any number $\equiv 3 \mod 5$. Hence another form of $g(x)$ could be $g(x) = x + 3 \mod 5$ or even $g(x) = x + 28 \mod 5$. Check for yourself that we get the same values.

Exercise 8. Find the additive inverses of the following:

1. $3 \mod 39$
2. $18 \mod 56$
3. $-4 \mod 20$