

# Clock Arithmetic and Euclid's Algorithm

Lecture notes for Access 2008 by Erin Chamberlain.

Earlier we discussed Caesar Shifts and other substitution ciphers, and we saw how easy it was to break these ciphers by using frequency analysis. If Mary Queen of Scots had known this, perhaps she would not have been executed. People came up with more complicated substitution ciphers like using the Vigenère square. The Great Cipher of France baffled people for quite a while until Bazeries after three years figured it out, and possibly found the true identity of the Man in the Iron Mask, one of the great mysteries of the seventeenth century. Edgar Allan Poe and Sir Arthur Conan Doyle even dabbled in cryptanalysis. Secrecy was still a problem though because the key needed to be sent, and with the key anyone could encrypt and decrypt the messages. Also frequency analysis was used to break all of these codes. In 1918 Scherbius invented his Enigma machine, but Alan Turing's machine helped in figuring out that supposedly unbreakable code. Americans in the second world war used code talkers, but there were many cases of friendly fire when the code talker was killed. 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.

The beauty of these encryption methods is we can write mathematical formulas to represent the substitution ciphers and RSA. Let's look at an example:

**Example 1.** 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 Caesar shift. For each letter in the message, replace it with its number value. Put each of those values in our encrypting function  $f(x) = x + 4$  but cycle around the alphabet when you need to. For example,  $f(X) = f(23) = 23 + 4 = 27$  which is the same as  $1 = B$ . 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.* REPLY = 17 - 4 - 15 - 11 - 24.  $f(17 - 4 - 15 - 11 - 24) = 21 - 8 - 19 - 15 - 28$  which is equivalent to  $21 - 8 - 19 - 15 - 2 = VITPC$ .  $\square$

Before we can fully explain the method for RSA, 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 2.** 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 3.** 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**.

**Definition 5.** The integer  $a$  is a **common multiple** of  $b$  and  $c$  if  $b|a$  and  $c|a$ . The smallest common multiple of  $b$  and  $c$  is called the **least common multiple** and is denoted by  $lcm(b, c)$ .

**Example 4.**  $(60)(84) = 5040$  is a common multiple of 60 and 84, but  $(12)(7)(5) = 420$  is their least common multiple;  $lcm(60, 84) = 420$ . Using prime factorizations it is easy to see that

$$lcm(b, c) = \frac{bc}{gcd(b, c)}.$$

In our example with  $b = 60$  and  $c = 84$ , we have  $gcd(60, 84) = 12$ , so  $lcm(60, 84) = (12)(7)(5) = \frac{(60)(84)}{12}$ .

## Clock Arithmetic

### Addition

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

**Example 5.** 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.*  $10 + 7 = 17$ , but we need to subtract off 12 to find out the correct time, so  $17 - 12 = 5$ , so Josh will be there at 5 o'clock.  $\square$

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 6.** 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.*  $5 + 39 = 44$  but we don't care about the multiples of 12, so let's divide and find the remainder.  $44 \div 12 = 3.66666\dots$ , so to calculate what the remainder is we do the following:  $44 - 12 \times 3 = 8$ , so you should leave for the airport at 8 o'clock.  $\square$

**Example 7.** If it is 8 o'clock, and you have an appointment in 1984604 hours, what time is your appointment?

*Solution.* Once again we need to find the remainder of  $8 + 1984604 = 1984612$  divided by 12. This is a two step process. First we find out how many times 12 goes into 1984612. Using a calculator or a computer we see that  $1984612 \div 12 = 165384.333\dots$ . The next step is to find the remainder as follows:  $1984612 - 12 \times 165384 = 4$ . So the appointment is at 4 o'clock.  $\square$

The fancy math term for this type of arithmetic we used in example 1 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 4 above.

We will look at this problem in two different but equivalent ways. First, we have  $10 + 7 = 17$ , and to get a multiple of 12, we need to subtract 5, so  $10 + 7 \equiv 5 \pmod{12}$  because  $10 + 7 - 5$  is a multiple of 12. We can equate this to our definition with  $10 + 7 = a$ ,  $5 = b$ , and  $12 = n$ .

The equivalent and probably more useful way of thinking of this is by using remainders. We have  $10 + 7 = 17$ , and 17 divided by 12 has a remainder of 5. Remember that a remainder just means how far away our number 17 is from being a multiple of 12. So  $10 + 7 \equiv 5 \pmod{12}$ . And we can say that 5 is the residue of  $17 \pmod{12}$ .

In example 6 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 8.** We know that  $17 \equiv 2 \pmod{5}$  and  $14 \equiv 4 \pmod{5}$ , find  $17 + 14 \pmod{5}$ .

*Solution.* We did similar examples like this before by adding and then finding the remainder, but let's do this using property 2 above.  $17 + 14 \equiv 2 + 4 \pmod{5} \equiv 1 \pmod{5}$ .  $\square$

**Example 9.** Solve for  $x$  in the equation  $x - 8 \equiv 3 \pmod{13}$ .

*Solution.* We can use property 2 again by adding 8 to both sides of the equation.  $x - 8 + 8 \equiv 3 + 8 \pmod{13}$ , so  $x \equiv 11 \pmod{13}$ .  $\square$

**Example 10.** List all of the integers  $x$  between 1 and 50 which satisfy  $x \equiv 7 \pmod{17}$ .

*Solution.* We want the numbers between 1 and 50 with a remainder of 7 when we divide by 17. In other words, we want numbers of the form  $17n + 7$  for  $n$  and whole number. Letting  $n = 0, 1, 2$ , we see the numbers are 7, 24, and 41.  $\square$

**Example 11.** What is  $-3 \equiv \underline{\hspace{1cm}} \pmod{11}$ ?

*Solution.* If we think about our clock with 11 ticks, the negative 3 means we circle around the clock three ticks in the counterclockwise direction. To get the residue value, we count the ticks in the clockwise direction which is the same as the  $-3$  value. So we get  $11 - 3 = 8$ , so  $-3 \equiv 8 \pmod{11}$ . Or equivalently,  $-3 - 8 = -11$  which is a multiple of 11, so  $-3 \equiv 8 \pmod{11}$ . Or for another way of thinking of this, we can divide again. We have  $-3$  divided by 11 is  $-1$  with a remainder of 8.  $\square$

**Exercise 1.** Use the above properties to find  $21 + 83 \pmod{5}$ .

**Exercise 2.** Solve for  $x$  in the equation  $x - 14 \equiv 3 \pmod{9}$ .

**Exercise 3.** Find all of the integers  $y$  between 1 and 100 which satisfy  $x \equiv 13 \pmod{20}$ .

**Exercise 4.** Fill in the missing residue numbers:

1.  $19 \equiv \underline{\hspace{1cm}} \pmod{6}$

2.  $20568 \equiv \underline{\hspace{1cm}} \pmod{19}$

3.  $-13 \equiv \underline{\hspace{1cm}} \pmod{25}$ .

4.  $-39 \equiv \underline{\hspace{1cm}} \pmod{16}$ .

**Exercise 5.** What function would we use to decrypt our message in Example 1?

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

1.  $f(3)$

2.  $f(1)$

3.  $f(2)$

**Exercise 7.** Now suppose we are given that  $g(x) = x - 2 \pmod{5}$ . (The inverse or "undo" function of  $f(x)$ .) Compute the following, and compare this to Exercise 8.

1.  $g(0)$

2.  $g(3)$

3.  $g(4)$

**Exercise 8.** 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  $g(x) \equiv x + 3 \pmod{5}$  or even  $g(x) \equiv x + 28 \pmod{5}$ . Check for yourself that we get the same values.

**Exercise 9.** Find the residue numbers which are 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 12.** What is  $3 \times 7 \times 9 \pmod{5}$ .

*Solution.* Notice that  $7 \equiv 2 \pmod{5}$  and  $9 \equiv 4 \pmod{5}$ , so by using property 3 we have the following product.  $3 \times 2 \times 4 = 6 \times 4 \equiv 1 \times 4 \pmod{5} \equiv 4 \pmod{5}$ .  $\square$

**Example 13.** Find  $7^5 \pmod{9}$ .

*Solution.* We can use property 3 and rules of exponents to break up this multiplication.  $7^5 = (7^2)(7^2)(7) = (49)(49)(7) \equiv (4)(4)(7) = (16)(7) \equiv (7)(7) \equiv 4 \pmod{9}$ .  $\square$

**Example 14.** Solve for  $x$  in the equation  $3 - x \equiv 7 \pmod{8}$ .

*Solution.* We solve this equation the same way we would solve  $3 - x = 7$ . First we subtract 3 from both sides to get  $-x \equiv 4 \pmod{8}$ . Now multiply by  $-1$  to get  $x \equiv -4 \pmod{8}$ . Finally we use our clock argument to find the positive equivalent value for  $-4 \pmod{8}$  which is  $4 \pmod{8}$ . Therefore  $x \equiv 4 \pmod{8}$ .  $\square$

**Exercise 10.** Fill in the missing residue numbers:

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

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

**Exercise 11.** Solve  $7 - x \equiv 21 \pmod{24}$ .

Here is the multiplication table for modulo 5.

×	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 12.** 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 13.** Compute the following with  $g(x) = 3x \pmod{5}$  and compare this problem with the previous exercise.

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

**Exercise 14.** Using the same table in example 7, encrypt the message "ATTACK AT DAWN" using the function  $f(x) = 5x \pmod{26}$

**Exercise 15.** Can you find the inverse function needed to decrypt your message from exercise 14?

## Finding Multiplicative Inverses

**Example 15.** Make a multiplication table for mod 15, and then make a table of multiplicative inverses.

Here are the tables:

$\times$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7															
8															
9															
10	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	0	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	0	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	0	14	13	12	11	10	9	8	7	6	5	4	3	2	1

a	b
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	

We notice that not all of the values have inverses.

**Exercise 16.** List the numbers which have inverses. How do these numbers relate to 15?

**Exercise 17.** List the numbers which do not have inverses. How do these numbers relate to 15?

**Exercise 18.** What do you notice about row  $a$  when  $a$  has a multiplicative inverse, as compared to when it doesn't? In rows where the pattern of products repeats, how many times does it repeat, and when does the first repetition occur?

Here's one way to answer some of these exercises:

**Lemma 1.** Let  $a$  and  $n$  be integers with  $0 < a < n$ . Then  $a$  has a multiplicative inverse mod  $n$  if and only if row  $a$  of the residue multiplication table mod  $n$  is a permutation (rearrangement) of the residue numbers  $0, 1, 2, \dots, n - 1$ . Furthermore,  $a$  does not have a multiplicative inverse mod  $n$  if and only if  $az \equiv 0 \pmod{n}$  for some  $0 < z < n$ .

*Proof.* If  $a$  has a multiplicative inverse mod  $n$ , then both sides of the equation  $ax \equiv ay \pmod{n}$  may be multiplied by  $a^{-1}$  to deduce  $x \equiv y \pmod{n}$ . Thus, if  $a^{-1}$  exists, then the residue entries of row  $a$  of the multiplication table are all distinct (different). Since there are  $n$  residue values and  $n$  entries in the row, we deduce that row  $a$  is a permutation of the  $n$  residue values. Conversely, if row  $a$  is a permutation of the residue values, then the number "1" occurs somewhere in row  $a$ , say in column  $x$ . This means  $x$  is the multiplicative inverse of  $a$ . Thus we have shown that  $a^{-1}$  exists if and only if row  $a$  is a permutation of the residue values.

If  $a$  does not have a multiplicative inverse, then the number 1 does not appear in row  $a$  of the multiplication table. Since there are  $n - 1$  residue values besides 1, and  $n$  entries to fill, at least two of the entries of row  $a$  must be the same, say  $ax \equiv ay \pmod{n}$ , with  $0 \leq x < y < n$ . Thus  $0 \equiv ay - ax \equiv a(y - x)$ ; i.e. the entry in column  $z = y - x$  of row  $a$  is zero. Conversely, if  $az \equiv 0 \pmod{n}$  for some  $0 < z < n$ , then since column 0 and column  $z$  of row  $a$  in the table both have entries 0, row  $a$  is not a permutation of the residue numbers, so by the previous paragraph we deduce  $a^{-1}$  does not exist. □

**Theorem 1.** Let  $a$  and  $n$  be integers with  $0 < a < n$ . Then  $a$  has a multiplicative inverse mod  $n$  if and only if  $(a, n) = 1$ .

*Proof.* We will check the logically equivalent statement that  $a$  does not have a multiplicative inverse if and only if  $(a, n) = b > 1$ : If  $a$  does not have a multiplicative inverse then pick the smallest  $0 < z < n$  so that  $az \equiv 0 \pmod{n}$ , which we can do by applying the preceding lemma. Thus  $az$  is a multiple of  $n$ , and is in fact the least common multiple of  $a$  and

$n$  since by choosing the smallest positive  $z$  for which  $az \equiv 0 \pmod{n}$  we are choosing the smallest positive  $z$  so that  $az$  has  $n$  as a factor. Since  $z < n$  we also have  $az < an$ . But  $az = \text{lcm}(a, n) = \frac{an}{(a, n)}$ , so it must be that  $(a, n) > 1$ .

Conversely, if  $(a, n) = b > 1$ , then for  $z = \frac{n}{b}$  we have  $az = \text{lcm}(a, n)$  so  $az \equiv 0 \pmod{n}$ , i.e. column  $z$  of row  $a$  of the multiplication table is zero, so  $a^{-1}$  does not exist by the previous lemma.  $\square$

Notice that although our theorem tells us when multiplicative inverses exist in clock arithmetic, it doesn't give us an efficient algorithm to compute them if the modulus is large. In the next few examples we keep the modulus relatively small. In the next section we'll see how to find multiplicative inverses when the modulus is large.

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

**Example 16.** Find the multiplicative inverse of  $8 \pmod{11}$ .

*Solution.* We have already seen that we can find the multiplicative inverse by making a multiplication table, but I don't think we want to make that big of a table. Also we could try to find the inverse by just going through the multiples of 8. The third method is to use Euclid's Algorithm, which we will discuss next. Just for fun though, let's try to figure this one out. We need a number  $b$  such that  $8b \equiv 1 \pmod{11}$ . The numbers congruent to 1 mod 11 are 12, 23, 34, 45, 56, 67, 78, etc. Of those we need to find the one that is divisible by 8, which is  $56 = 8 \times 7$ . Thus the multiplicative inverse of  $8 \pmod{11}$  is 7.  $\square$

**Exercise 19.** Solve  $8x \equiv 3 \pmod{11}$ .

**Exercise 20.** Find  $5^{-1} \pmod{26}$ .

**Exercise 21.** Using your answer from exercise 20, decrypt your message you made in exercise 14.

## 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  $8^{-1} \pmod{11}$ .

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

Now reverse the process using the equations on the right.

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

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 17.** Find the gcd of 42823 and 6409.

$$\begin{array}{rcl}
 \mathbf{42823} & = & \mathbf{6409}(6) + \mathbf{4369} \\
 \mathbf{6409} & = & \mathbf{4369}(1) + \mathbf{2040} \\
 \textit{Solution.} \quad \mathbf{4369} & = & \mathbf{2040}(2) + \mathbf{289} \\
 \mathbf{2040} & = & \mathbf{289}(7) + \mathbf{17} \\
 \mathbf{289} & = & \mathbf{17}(17)
 \end{array}$$

Therefore  $(42823, 6409) = 17$ . □

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 18.** Find integers  $x$  and  $y$  to satisfy

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

*Solution.* We begin by writing the above equations but solving for the remainder. We have:

$$4369 = 42823 - 6409(6)$$

$$2040 = 6409 - 4369$$

$$289 = 4369 - 2040(2)$$

$$17 = 2040 - 289(7)$$

Now we do the substitutions starting with that last equation and working backwards and combining like terms along the way:

$$17 = 2040 - 289(7) = 2040 - (4369 - 2040(2))(7) = 2040(15) - 4369(7)$$

$$17 = (6409 - 4369)(15) - 4369(7) = 6409(15) - 4369(22)$$

$$17 = 6409(15) - (42823 - 6409(6))(22) = 6409(147) - 42823(22)$$

Therefore  $x = -22, y = 147$ . □

**Exercise 22.** Find the gcd of:

1. 7469 and 2464

2. 2689 and 4001

3. 2947 and 3997

4. 1109 and 4999

**Exercise 23.** 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 24.** Find the multiplicative inverses of the following:

1.  $50 \pmod{71}$

2.  $43 \pmod{64}$

**Exercise 25.** Using the information from the previous exercise, solve the following equation for  $x$  and check your answer.

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

**Exercise 26.** Solve  $12345x \equiv 6 \pmod{54321}$ . Hint: First find the gcd.

Information for these notes came from previous lecture notes of Jim Carlson, and definitions and theorems came from *An Introduction to The Theory of Numbers, fifth edition*, by Niven, Zuckerman, and Montgomery.