Modular Arithmetic continued

Lecture notes for Access 2010 by Erin Chamberlain and Nick Korevaar

Number theory refresher

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 by $gcd(b, c)$.

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

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

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 3. $(60)(84) = 5040$ 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 $lcm(60, 84) = (12)(7)(5) = \frac{(60)(84)}{12}$.

Functions in modular arithmetic

Example 4. In the example from yesterday we used

$$f(x) = x + 4 \mod 26$$

to encrypt a message. The domain and range for this function is the collection or residue numbers $\{0, 1, 2, \ldots 25\} \mod 25$, which we have identified with the 26 letter alphabet. Our function described a Caesar shift by 4 letters. The inverse (decryption) function is

$$g(x) = x - 4 \mod 26$$

.

We will eventually be encrypting long packets of numbers corresponding to long strings of letters and punctuation, and we will be using power functions in modular arithmetic with very large moduli. In this set of notes we're focusing on addition an multiplication, and encryption functions, like the example above, which use these two operations. Our example moduli will be small numbers we can work with by hand.

Example 5. For small moduli it's sometimes helpful to use addition or multiplication tables. Here is 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 1. Suppose we had a function $f(x) = x + 2 \mod 5$. Compute the following:

1. $f(3)$

2. $f(1)$

3. $f(2)$

What row(s) of the addition table could you look at to show how $f(x)$ permutes the residue values?

Exercise 2. Now suppose we are given that $g(x) = x - 2 \mod 5$. (The inverse or "undo" function of $f(x)$.) Compute the following, and compare this to the previous exercise.

1. $g(0)$

2. $g(3)$

3. $g(4)$

Exercise 3. Can you think of another formula, one which uses addition rather than subtraction, that yields the same inverse function $g(x)$? Can you illustrate how $f(x)$ and $g(x)$ are inverse functions, using the addition table?

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 $g(x) \equiv x + 3 \mod 5$ or even $g(x) \equiv x + 28 \mod 5$. Check for yourself that we get the same values.

Exercise 4. Find the residue numbers which are additive inverses of the following:

1. $3 \mod 39$

2. $18 \mod 56$

3. $-4 \mod 20$

Example 6. Find the residue number solution x to the equation $3 - x \equiv 7 \mod 8$.

Solution. We solve this equation the same way we would solve $3 - x = 7$. If we subtract 3 from both sides of this equation we get $-x \equiv 4 \mod 8$. Multiply by -1 to get $x \equiv -4 \mod 8$. Thus $x = -4 \mod 8$, so $x = 4$. □

Exercise 5. Find a residue number solution x for $7 - x \equiv 21 \mod 24$.

Now lets consider multiplication, and multiplication functions. Here is the multiplication table for modulo 5. Make sure to check some of the entries to see that you agree:

$\times$	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 6. Let $f(x) = 2x \mod 5$. 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 7. Compute the following with $g(x) = 3x \mod 5$ and compare this problem with the previous exercise.

1. $g(1)$

2. $g(2)$

3. $g(4)$

Exercise 8. Using the same table as yesterday (repeated below), encrypt the message "ATTACK AT DAWN" using the function $f(x) = 5x \mod 26$.

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

Exercise 9. Can you find the inverse function needed to decrypt your message from the previous exercise?

Finding Multiplicative Inverses

Example 7. Make a multiplication table for mod 15, and then make a table of multiplicative inverses.

Here are the tables:

×	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 10. List the numbers which have inverses. How do these numbers relate to 15?

Exercise 11. List the numbers which do not have inverses. How do these numbers relate to 15?

Exercise 12. 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 $0, 1, 2, \ldots n-1$. Furthermore, a does not have a multiplicative inverse mod n if and only if $az \equiv 0 \mod n$ for some $0 < z < n$.

Proof. If a has a multiplicative inverse mod n, then both sides of the equation $ax \equiv ay \mod n$ may be multiplied by a^{-1} to deduce $x \equiv y \mod n$. 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 $ax \equiv ay$, 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 $az \equiv 0$ 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 and n are relatively prime, i.e. $gcd(a, n) = 1$.

Proof. We will check the logically equivalent statement that a does not have a multiplicative inverse if and only if $gcd(a, n) = b > 1$: If a does not have a multiplicative inverse then pick the smallest $0 < z < n$ so that $az \equiv 0 \mod n$, 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 $az \equiv 0 \mod n$ we are choosing the smallest postive z so that az has n as a factor. Since $z < n$ we also have $az < an$. But $az = lcm(a, n) = \frac{an}{gcd(a,n)}$, so it must be that $gcd(a, n) > 1$.

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

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 example 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 8. Find the multiplicative inverse of $8 \mod 11$.

Solution. We have already seen that we can find the multiplicative inverse by making a multiplication table, but we want to make that big of a table from scratch. We could try to find the inverse by just going through the multiples of 8 until one of them is congruent to 1. Here's a third way: we need a number b such that $8b \equiv 1 \mod 11$. 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 mod 11 is 7. □

Exercise 13. Solve $8x \equiv 3 \mod 11$ for a residue number x.