Modular Arithmetic II

The last worksheet ended with some remarks about solving equations $ax = \overline{1}$ with modulus m. To understand those remarks we begin with a very familiar concept.

Definition 1 *Let a and n be integers. We say that n divides a (or a is divisible by n) if $a = nb$ for some integer b.*

So 3 divides 6 but 3 doesn't divide 7.

Definition 2 *Let n be a positive integer. We say that two integers a and b are congruent modulo n if $b - a$ is divisible by n. When this occurs, we write $a \equiv b \bmod n$.*

Example 3 $3 \equiv 8 \bmod 5$ *because* $8 - 3 = 5$ *is divisible by* 5. *More precisely,* $3 \equiv 8 \bmod 5$ *because* $3 - 8 = -5 = 5(-1)$.

Example 4 $123 \equiv 2 \bmod 11$ *because* $123 - 2 = 121 = 11^2$.

Example 5 $-17 \equiv 3 \bmod 4$ *because* $-17 - 3 = -20 = 4(-5)$.

Note that $8 \equiv 3 \bmod 5$ because $3 - 8 = -5$ is also divisible by 5. So we can always say that if $a \equiv b \bmod n$ then $b \equiv a \bmod n$ also.

Example 6 $3 = -17 + 4(5)$ *expresses shows* $3 \equiv -17 \bmod 4$ *in this way.*

Example 7 $123 \equiv 24 \bmod 11$ *because* $123 = 2 + 11(11)$ *and* $24 = 2 + 2(11)$. *Both have remainder equal to* 2 *when you divide by* 11.

Exercise 8 *Find three distinct integers that are conjugate to* 5 mod 7.

Two numbers are congruent modulo n if they give you the same time on a clock with n hours. Think military time:

Example 9 13 *hours is* 1*PM,* $13 \equiv 1 \bmod 12$, *and* 22 *hours is* 10 *PM,* $22 \equiv 10 \bmod 12$.

Another way to look at these examples is in terms of remainders when you divide by n. The remainder of 13 when you divide by 12 is 1, the remainder of 22 is 10. Another example from above is $123 = 11 \times 11 + 2$ i.e. the remainder of 123 upon division by 11 is 2. In fact two integers are congruent modulo n if and only if they have exactly the same remainder upon division by n. Notice that $35 = 3 \times 11 + 2$ also has a remainder of 2 and $123 - 35 = 88$ is divisible by 11 so $123 \equiv 35 \bmod 11$.

In general to say that the integer a has remainder r upon division by n means $a = qn + r$ where q is some integer and r is an integer between 0 and n (r could be 0, but we don't want the remainder to be n). So suppose that $a \equiv b \bmod n$

so that n divides $b-a$. Now write a and b in terms of n with remainders r_1 and r_2:

$$\begin{aligned} a &= q_1 n + r_1 \\ b &= q_2 n + r_2. \end{aligned}$$

Remember both, $0 \leq r_1 < n$ and $0 \leq r_2 < n$. Pretend $r_1 \leq r_2$ and subtract the first equation from the second to get

$$b - a = (q_2 - q_1)n + r_2 - r_1.$$

Because both $r_1 < n$ and $r_2 < n$ the only way n divides $b-a$ is if $r_2 - r_1 = 0$, i.e. a and b have the same remainder.

If a and b have the same remainder r then our equations are

$$\begin{aligned} a &= q_1 n + r \\ b &= q_2 n + r. \end{aligned}$$

and when we subtract, the r's cancel so it's clear that n divides $b-a$.

The symbol $\overline{a}$ represents all those integers which have the same remainder upon division by m as a. as One you fix a modulus m, modular arithmetic is is just ordinary arithmetic on the remainders after dividing by m :

Example 10 *Take* $m = 7$. *Then* $\overline{1} = \overline{8} = \overline{15}$ *and* $\overline{4} = \overline{11} = \overline{18}$. *Adding* $\overline{1}+\overline{4} = \overline{5}$ *produces the same result as adding* $\overline{8} + \overline{11} = \overline{19} = \overline{5}$ *because* $19 = 2(7) + 5$.

Example 11 *Again with* $m = 7$, $\overline{1} \times \overline{4} = \overline{4}$ *and* $\overline{15} \times \overline{18} = \overline{270}$. *But* $270 = 38 \times 7 + 4$ *so that* $\overline{270} = \overline{4}$ *and we get the same result as if we had started out by replacing* $\overline{15}$ *with* $\overline{1}$ *and* $\overline{18}$ *with* $\overline{4}$.

To say this systematically: if $a = q_1 b + r_1$ and $b = q_2 b + r_2$ all integers, then

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} = \overline{r_1} + \overline{r_2} = \overline{r_1 + r_2} \\ \overline{a} \times \overline{b} &= \overline{a \times b} = \overline{r_1} \times \overline{r_2} = \overline{r_1 \times r_2}. \end{aligned}$$

1 The Division Algorithm

Now for a different take on something very familiar. To write $\frac{33}{7}$ as a proper fraction, divide 33 by 7 to get 4 with a remainder of 5. $\frac{33}{7} = 4\frac{5}{7}$. Alternatively, write $33 = 4(7) + 5$ and divide both sides by 7 :

$$\begin{aligned} \frac{33}{7} &= \frac{4(7)+5}{7} \\ &= 4 + \frac{5}{7}. \end{aligned}$$

The proper fraction notation captures the remainder upon division by 7 and the multiplier of 7 that gets you closest to 33.

Example 12 $\frac{145}{13} = 11\frac{2}{13}$ *because* $145 = 143 + 2 = 13 \times 11 + 2$. *Note that* $145 \equiv 2 \bmod 13$.

The Division Algorithm is the mathematical theorem that says that you can always write an improper fraction as a proper fraction in one and only one way.

Theorem 13 *Let a and n be integers with n positive. Then there are unique integers q and r with $a = qn + r$ and $0 \leq r < n$.*

In a previous example, we had $a = 33, n = 7, q = 4$, and $r = 5$. The proof of this theorem probably goes back to Euclid. While the result is intuitively clear and it is easy to find q and r in any example, to actually **prove** their existence for all possible $a's$ and $n's$ requires some work!

We use the *well ordering* property of the integers that says any nonempty subset of the nonnegative integers has a smallest element. Why is this true? If $\mathcal{S}$ is a collection of nonnegative integers, choose one from S and call it s. Now check which, if any, of $s-1, s-2, ..., 1$ is in $\mathcal{S}$. If none is, then s was the smallest. Otherwise you would find the smallest among $s-1, s-2, ..., 1$.

To see how we use this property, look again at our $a = 33, n = 7$ example. We want to see that we can express $33 = 7q + r$ with $r = 33 - 7q$ between 0 and 6. So its natural to look at the possible nonnegative values of $r = 33 - 7q$ for various values of q. When

- $q = 0$, $r = 33$
- $q = 1, r = 26$
- $q = 2$,$r = 19$
- $q = 3$,$r = 12$
- $q = 4$,$r = 5$
- $q = 5$,$r = -2$

So $r = 5$ (with $q = 4$) is the smallest nonnegative integer among the integers $33 - 7q$. The result of the Division Algorithm is therefore our expression $33 = 4(7) + 5$.

For arbitrary but fixed a and n we do the same thing. Set S to be the set of all nonnegative integers that can be written as $a - qn$ with q some integer. Is there anything in S? Certainly yes if $a \geq 0$, because $a = a - 0 \cdot n$ is then in $\mathcal{S}$. If $a < 0$, then $a - an = a(1 - n) \geq 0$ since n is positive. Therefore, $a - an \in \mathcal{S}$. In either case, we see that $\mathcal{S}$ is nonempty. Now the well ordering property tells us that $\mathcal{S}$ contains a smallest element which will be our r. Since r is in S it can be written as

$$r = a - qn$$

which we can write as $a = qn + r$ proving one part of the theorem.

To show that $0 \leq r < n$, we have by design that $r \geq 0$. Pretend that $r \geq n$, so that then $r - n \geq 0$. = But $r - n = a - (q+1)n \geq r \geq 0$ .so $r - n$ is also in S and is smaller than r (which was smallest in S). This is impossible, so it must be that $r < n$.

Thus we have produced integers q and r with $a = qn + r$ and $0 \leq r < n$. Next, we need to prove uniqueness of q and r, i.e. there is only one way to write a like this. Suppose that q' and r' are a second pair of integers with $a = q'n + r'$ and $0 \leq r' < n$. If $r \neq r'$ pretend $r > r'$. Then $q'n + r' = qn + r$, so $(q' - q)n = r - r'$.Since r and r' are both between 0 and n,

$$_____0_____r'_____r_____n$$

their difference can't be a multiple of n unless it's 0, i.e. $r' = r$. But then $(q' - q)n = 0$ so $q' = q$.

2 Euclidean Algorithm

The Euclidean Algorithm (EA for short) is the key to understanding the existence of multiplicative inverses $\bmod n$ (and many other things). While most of us learned to find the greatest common divisor by factoring, that method is the worst possible for large integers like those that are used in cryptography. The Euclidean Algorithm is easy and fast to perform on a computer. There are several reasons why I'm spending a lot of time on the EA. One is that I find it to be very beautiful mathematics. Another is that it has important implications for our applications to information security..And it also is the gateway to the fascinating area of mathematics known as number theory. Most likely you were taught to find the greatest common divisor (gcd) of to integers by factoring. The EA uses the Division Algorithm instead.

Here is an example of the EA to calculate $\gcd(10, 14)$:

1. Use the Division Algorithm with $b = 14, a = 10$ to write

$$14 = 1(10) + 4$$

   Note that $0 \leq 4 < 10$.

2. Use the Division Algorithm with $b = 10, a = 4$ to write

$$10 = 2(4) + 2$$

3. Use the Division Algorithm with $b = 4, a = 2$ to write

$$4 = 2(2) + 0$$

4. The last nonzero remainder, 2, is the $\gcd(10, 14)$.

Of course this example is done more quickly by factoring:

$$\begin{aligned} 10 &= 2 \times 5 \\ 14 &= 2 \times 7. \end{aligned}$$

Thus the prime factorization of $\gcd(10, 14)$ is just 2. But for larger numbers, the inherent difficulty in factoring makes this method unpleasant.

Example 14 *To calculate* $\gcd(12342, 2738470)$*, we list the divisions with remainder we need to perform to calculate the* gcd.

$$\begin{aligned} &b = 2738470,\ a = 12342;\ 2738470 = 221 \cdot 12342 + 10888 \\ &b = 12342,\ a = 10888;\ 12342 = 1 \cdot 10888 + 1454 \\ &b = 10888,\ a = 1454;\ 10888 = 7 \cdot 1454 + 710 \\ &b = 1454,\ a = 710;\ 1454 = 2 \cdot 710 + 34 \\ &b = 710,\ a = 34;\ 710 = 20 \cdot 34 + 30 \\ &b = 34,\ a = 30;\ 34 = 1 \cdot 30 + 4 \\ &b = 30,\ a = 4;\ 30 = 7 \cdot 4 + 2 \\ &b = 4,\ a = 2;\ 4 = 2 \cdot 2 + 0. \end{aligned}$$

The last nonzero remainder is 2*, so* $2 = \gcd(12342, 2738470)$.

It would be much more laborious to attempt to calculate $\gcd(12342, 2738470)$ by factoring.

Here is the general procedure to calculate $\gcd(a, b)$ by the EA. Let's assume that $b > a$:

Algorithm 15 *Euclidean Algorithm*

1. Use the Division Algorithm to express

$$b = q_1 a + r_1 \text{ with } 0 \leq r_1 < a.$$

2. Use the Division Algorithm to express

$$a = q_2 r_1 + r_2 \text{ with } 0 \leq r_2 < r_1.$$

3. Use the Division Algorithm to express

$$r_1 = q_3 r_2 + r_3 \text{ with } 0 \leq r_3 < r_2.$$

4. Use the Division Algorithm to express

$$r_2 = q_4 r_3 + r_4 \text{ with } 0 \leq r_4 < r_3$$

5. Proceed until a remainder is equal to 0:

$$r_{n-2} = q_n r_{n-1} + r_n \text{ with } 0 \leq r_n < r_{n-1},$$

$$r_{n-1} = q_{n+1} r_n + 0.$$

Then r_n, the last nonzero remainder, is the $\gcd(a, b)$.

Two questions should immediately arise?

1. Why does the procedure stop, i.e. why must a remainder eventually be 0?
2. Why is the last nonzero remainder equal to the gcd?

Instead of answering these questions now, let's look at some more examples.

Example 16 *To calculate* $\gcd(30, 132)$,*we do the following arithmetic.*

$$\begin{aligned} 132 &= 4(30) + 12 \\ 30 &= 2(12) + 6 \\ 12 &= 2(6) + 0 \end{aligned}$$

Since the final nonzero remainder is 6*, we have* $6 = \gcd(30, 132)$.

Example 17 *Calculate* $\gcd(72, 333)$.

$$\begin{aligned} 333 &= 4(72) + 45 \\ 72 &= 1(45) + 27 \\ 45 &= 1(27) + 18 \\ 27 &= 1(18) + 9 \\ 18 &= 2(9) + 0 \end{aligned}$$

Therefore $9 = \gcd(72, 333)$

Exercise 18 *Use the Euclidean Algorithm to find*

1. $\gcd(24, 54)$.
2. $\gcd(84, 315)$.
3. $\gcd(2006, 136)$

The EA does a lot more. It allows us to write $\gcd(a, b)$ in terms of a and b.

Example 19 $\gcd(24, 112) = 8$.

$$\begin{aligned} 112 &= 4 \cdot 24 + 16 \\ 24 &= 1 \cdot 16 + 8 \\ 16 &= 2 \cdot 8 + 0. \end{aligned}$$

Working backward, the second to last equation is $24 = 1 \cdot 16 + 8$, or

$$8 = 1 \cdot 24 + (-1) \cdot 16.$$

Thus, we have written the gcd 8 as a linear combination of 24 and 16. The equation before that (the first) is$112 = 4 \cdot 24 + 16$, or

$$16 = 1 \cdot 112 + (-4) \cdot 24.$$

Replacing 16 in the previous displayed equation by this expression yields

$$\begin{aligned} 8 &= 1 \cdot 24 + (-1) \cdot (1 \cdot 112 + (-4) \cdot 24) \\ &= 1 \cdot 24 - 1 \cdot 112 + 4 \cdot 24 \\ &= 5 \cdot 24 + (-1) \cdot 112, \end{aligned}$$

which is the desired representation.

A *linear combination* of two integers a and b is an expression

$$xa + yb$$

where x and y are also integers. So in

$$5 \cdot 24 + (-1) \cdot 112 = 8$$

we have $a = 24, b = 112, x = 5, y = -1$.

Exercise 20 *Find integers x and y for which* $\gcd(84, 315) = 84x + 315y$

The next observation is crucial to all that follows: *If p is a prime integer and a is an integer not divisible by p then* $\gcd(a, p) = 1$. *As a consequence there are integers x and y with $ax + py = 1$.*

Example 21 *Take $p = 17$ and $a = 9$ Then*

$$\begin{aligned} 9 \cdot 2 + 17 \cdot (-1) &= 18 - 17 = 1 \\ &= 1. \end{aligned}$$

Here $x = 2$ and $y = -1$.

Example 22 *Find integers x and y for which $14x + 23y = 1$. We'll use the Euclidean Algorithm to "find"* $\gcd(14, 23) = 1$ *and then work backwards.*

$$\begin{array}{ll} 23 = 1 \cdot 14 + 9 & 1 = 5 - 4 \\ 14 = 1 \cdot 9 + 5 & \quad = 5 - (9 - 5) \\ 9 = 1 \cdot 5 + 4 & \quad = 2 \cdot 5 - 9 \\ 5 = 1 \cdot 4 + 1 & \quad = 2(14 - 9) - 9 \\ 4 = 4 \cdot 1 + 0 & \quad = 2 \cdot 14 - 3 \cdot 9 \\ & \quad = 2 \cdot 14 - 3(23 - 14) \\ & \quad = 5 \cdot 14 - 3 \cdot 23 \end{array}$$

Read the next to last equation on the right $1 = 5 \cdot 14 - 3 \cdot 23$ modulo the prime 23 to see that $\overline{1} = \overline{5} \cdot \overline{14}$, i.e. $\overline{5}$ and $\overline{14}$ are multiplicative inverses mod 23

Exercise 23 *Use the method of the previous example to find a linear combination of* 8 *and* 19 *that is equal to* 1. *Then find the multiplicative inverse of* 8 mod 19.

If p is a prime and a is not a multiple of p the EA backwards will always find integers x and y for which $\gcd(a, p) = 1 = ax + py$.Reading this equation mod p shows that every such $\overline{a}$ has a multiplicative inverse mod p. This explains our observations from the multiplication tables mod p. It also explains why it's impossible to solve $\overline{1} = \overline{ax} \bmod m$ when $\gcd(a, m)$