Introduction to Number Theory

So far in this course, we have used the natural numbers to solve problems. This was the right set of numbers to work with in discrete mathematics because we always dealt with a whole number of things. The natural numbers have been a tool. Now let's take a moment to inspect that tool. What mathematical discoveries can we make *about* the natural numbers themselves?

This is the main question of number theory, a huge, ancient, complex, and above all, beautiful branch of mathematics. Historically, number theory was known as the Queen of Mathematics - it was very much a branch of *pure* mathematics, studied for its own sake instead of as a means to understanding real world applications. However, this has changed in recent years, as applications of number theory have been unearthed. Probably the most well known example of this is RSA cryptography, one of the methods used in encrypt data on the internet. It is number theory that makes this possible.

So what sorts of questions belong to the realm of number theory? Here is a motivating example. Recall in our study of induction, we asked:

> Which amounts of postage can be made exactly using just 5-cent and 8-cent stamps?

We were able to prove that *any* amount greater than 27 cents could be made. You might wonder what would happen if we changed the denomination of the stamps. What if we instead had 4- and 9-cent stamps? Would there be some amount after which all amounts would be possible? Well, again, we could replace two 4-cent stamps with a 9-cent stamp, or three 9-cent stamps with seven 4-cent stamps. In each case we can create one more cent of postage. Using this as the inductive case would allow us to prove that any amount of postage greater than 23 cents can be made.

What if we had 2-cent and 4-cent stamps. Here it looks less promising. If we take some number of 2-cent stamps and some number of 4-cent stamps, what can we say about the total? Could it ever be odd? Doesn't look like it.

So *why* does 5 and 8 work, 4 and 9 work, but 2 and 4 not work? What is it about these numbers? If I gave you a pair of numbers, could you tell me right away if they would work or not? We will answer these questions, and more, after first investigating some simpler properties of numbers themselves.

1 Divisibility

It is easy to add and multiply natural numbers. If we extend our focus to all integers, then subtraction is also easy (we need the negative numbers so we can subtract any number from any other numbers, even larger from smaller). Division is the first operation that presents a challenge. If we wanted to extend our set of numbers so any division would be possible (maybe excluding division by 0) we would need to look at the rational numbers - the set of all numbers which can be written as fractions. This would be going too far, so we will refuse this option.

In fact, it is a good thing that not every number can be divided by other numbers. This helps us understand the structure of the natural numbers and opens the door to many interesting questions and applications.

If given numbers a and b, it is possible that $a \div b$ gives a whole number. In this case, we say that b *divides* a, in symbols, we write $b \mid a$. If this holds, then b is a divisor or factor of a, and a is a multiple of b. This also means that if $b \mid a$, then $a = bk$ for some integer k (this is saying a is some multiple of b).

The Divisibility Relation

Given integers m and n, we say,

$$m \mid n \qquad \text{“}m \textit{ divides } n\text{”}$$

provided $n \div m$ is an integer. Thus the following assertions mean the same thing:

1. $m \mid n$
2. $n = mk$ for some integer k
3. m is a factor (or divisor) of n
4. n is a multiple of m.

Notice that $m \mid n$ is a statement - it is either true or false. On the other hand, $n \div m = n/m$ is some number. If we want to claim that n/m is not an integer, so m does not divide n, then we can write $m \nmid n$.

Example: Decide whether each of the statements below are true or false.

1. $4 \mid 20$
2. $20 \mid 4$
3. $0 \mid 5$
4. $5 \mid 0$
5. $7 \mid 7$
6. $1 \mid 37$
7. $-3 \mid 12$
8. $8 \mid 12$
9. $1642 \mid 136299$

Solution:

1. True. 4 “goes into” 20 five times without remainder. In other words, $20 \div 4 = 5$, an integer. We could also justify this by saying that 20 is a multiple of 4: $20 = 4 \cdot 5$.
2. False. While 20 is a multiple of 4, it is false that 4 is a multiple of 20.
3. False. $5 \div 0$ is not even defined, let alone an integer.
4. True. In fact, $x \mid 0$ is true for all x. This is because 0 is a multiple of every number: $0 = x \cdot 0$.
5. True. In fact, $x \mid x$ is true for all x.
6. True. 1 divides every number (other than 0).
7. True. Negative numbers work just fine for the divisibility relation. Here $12 = -3 \cdot 4$. It is also true that $3 \mid -12$ and that $-3 \mid -12$.

8. False. Both 8 and 12 are divisible by 4, but this does not mean that 12 is divisible by 8.
9. False.

This last example raises a question: how might one decide whether $m \mid n$? Of course, if you had a trusted calculator, you could ask it for the value of $n \div m$ - if it spits out anything other than an integer, you know $m \nmid n$. This seems a little like cheating though: we don't have division, so should we really use division to check divisibility?

While we don't really know how to divide, we do know how to multiply. So we might try multiplying m by larger and larger numbers until we get close to n. How close? Well, we want to be sure that if we multiply m by the next larger integer, we go over n.

For example, let's try this to decide whether $1642 \mid 136299$. Start finding multiples of 1642:

$$1642 \cdot 2 = 3284 \qquad 1642 \cdot 3 = 4926 \qquad 1642 \cdot 4 = 6568 \qquad \cdots$$

All of these are well less than 136299. I suppose we can jump ahead a bit:

$$1642 \cdot 50 = 82100 \qquad 1642 \cdot 80 = 131360 \qquad 1642 \cdot 85 = 139570$$

Ah, so we need to look somewhere between 80 and 85. Try 83:

$$1642 \cdot 83 = 136286$$

Is this the best we can do? How far are we from our desired 136299? If we subtract, we get $136299 - 136286 = 13$. So we know we cannot go up to 84, that will be too much. In other words, we have found that

$$136299 = 83 \cdot 1642 + 13$$

Since $13 < 1642$, we can now safely say that $1642 \nmid 136299$.

It turns out that the process we went through above can be repeated for any pair of numbers. We can always write the number a as some multiple of the number b plus some remainder. We know this because we know about *division with remainder* from elementary school. This is just a way of saying it using multiplication. Due to the procedural nature that can be used to find the remainder, this fact is usually called the *division algorithm*:

The Division Algorithm
Given any two integers a and b, we can always find an integer q such that

$$a = qb + r$$

where r is an integer satisfying $0 \leq r < |b|$

The idea is we can always take a large enough multiple of b so that the remainder r is as small as possible. Note that we do allow the possibility of $r = 0$. In this case, we get $b \div a$.

2 Remainder Classes

The division algorithm tells us that there are only b possible remainders when dividing by b. If we fix this divisor, we can group integers by the remainder. Each group is called a *remainder class modulo b* (or sometimes *residue class*).

Example: Describe the remainder classes modulo 5.

Solution: We want to classify numbers by what their remainder would be when divided by 5. From the division algorithm, we know there will be exactly 5 remainder classes, because there are only 5 choices for what r could be $(0 \leq r < 5)$.

First consider $r = 0$. Here we are looking for all the numbers divisible by 5. In other words, the multiples of 5. We get the infinite set:

$$\{\ldots, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}$$

Notice we also include negative integers.

Next consider $r = 1$. Which integers, when divided by 5, have remainder 1? Well, certainly 1, does, as does 6, and 11. Negatives? Here we must be careful: -6 does NOT have remainder 1. We can write $-6 = -2 \cdot 5 + 4$ or $-6 = -1 \cdot 5 - 1$, but only one of these is a "correct" instance of the division algorithm: $r = 4$ since we need r to be non-negative. So in fact, to get $r = 1$, we would could have -4, or -9, etc. Thus we get the remainder class:

$$\{\ldots, -14, -9, -4, 1, 6, 11, 16, 21, \ldots$$

There are three more to go. The remainder classes for 2, 3, and 4 are, respectively:

$$\{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}$$
$$\{\ldots, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\}$$
$$\{\ldots, -11, -6, -1, 4, 9, 14, 19, 24, \ldots\}$$

Note that in the example above, *every* integer is in exactly one remainder class. The technical way to say this is that the remainder classes modulo b form a *partition* of the integers.[1] The most important fact about partitions, is that it is possible to define an *equivalence relation* from a partition: this is a relationship between pairs of numbers which acts in all the important ways like the "equals" relationship.[2]

All fun technical language aside, the idea is really simple. If two numbers belong to the same remainder class, then in some way, they are the same. That is, they are the same *up*

[1] It is possible to develop a mathematical theory of partitions, prove statements about all partitions in general and then apply those observations to our case here.

[2] Again, there is a mathematical theory of equivalence relations which applies in many more instances than the one we look at here.

to division by b. In the case where $b = 5$ above, the numbers 8 and 23, while not the same number, are the same when it comes to dividing by 5, because both have remainder 3.

It matters what the divisor is: 8 and 23 are the same up to division by 5, but not up to division by 7, since 8 has remainder of 1 when divided by 7 while 23 has a remainder of 2.

With all this in mind, let's introduce some notation. We want to say that 8 and 23 are basically the same, even though they are not equal. So it would be wrong to say $8 = 23$. Instead, we write $8 \equiv 23$. But this is not always true - it works if we are thinking division by 5, so that needs to be there as well. So what we will actually write is this:

$$8 \equiv 23 \pmod{5}$$

which is read, "8 is congruent to 23 modulo 5." Of course then we could observe that

$$8 \not\equiv 23 \pmod{7}$$

Congruence Modulo n

We say *a is congruent to b modulo n*, and write,

$$a \equiv b \pmod{n}$$

provided a and b have the same remainder when divided by n. In other words, provided a and b belong to the same remainder class modulo n.

Many books define congruence modulo n slightly differently. They say that $a \equiv b \pmod{n}$ if and only if $n \mid a - b$. In other words, two numbers are congruent modulo n, if their difference is a multiple of n. So which definition is correct? Turns out, it doesn't matter - they are equivalent.

To see why, consider two numbers a and b which are congruent modulo n. Then a and b have the same remainder when divided by n. So we have:

$$a = q_1 n + r \qquad\qquad b = q_2 n + r$$

Here the two r's really are the same. Consider what we get when we take the difference of a and b:

$$a - b = q_1 n + r - (q_2 n + r) = q_1 n - q_2 n = (q_1 - q_2)n$$

So $a - b$ is a multiple of n, or equivalently, $n \mid a - b$.

On the other hand, if we assume first that $n \mid a - b$, so $a - b = kn$, then consider what happens if we divide each term by n. Dividing a by n will leave some remainder, as will dividing b by n. However, dividing kn by n will leave 0 remainder. So the remainders on the left hand side must cancel out. That is, the remainders must be the same.

Thus we have:

Congruence and Divisibility
For any integers a, b, and n, we have

$$a \equiv b \pmod{n} \qquad \text{if and only if} \qquad n \mid a - b$$

It will also be useful to switch back and forth between congruences and regular equations. The above fact helps with this. We know that $a \equiv b \pmod{n}$ if and only if $n \mid a - b$, if and only if $a - b = kn$ for some integer k. Rearranging that equation, we get $a = b + kn$. In other words, if a and b are congruent modulo n, then a is b more than some multiple of n. This conforms with our earlier observation that all the numbers in a particular remainder class are the same amount larger than the multiples of n.

Congruence and Equality
For any integers a, b, and n, we have

$$a \equiv b \pmod{n} \qquad \text{if and only if} \qquad a = b + kn \text{ for some integer } k$$

3 Properties of Congruence

We said earlier that congruence modulo n behaves in many important ways the same way equality does. Specifically, we could prove that congruence modulo n is an *equivalence relation*, which would require checking the following three facts:

Congruence Modulo n is an Equivalence Relation
Given any integers a, b, c, and n, the following hold:

1. $a \equiv a \pmod{n}$
2. If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

In other words, congruence modulo n is reflexive, symmetric, and transitive, so is an equivalence relation.

You should take a minute to convince yourself that each of the properties above actually hold of congruence. Try explaining each using both the remainder and divisibility definitions.

Next let's consider how congruence behaves when doing basic arithmetic. We already know that if you subtract two congruent numbers, the result will be congruent to 0 (be a multiple of n). What if we add something congruent to 1 to something congruent to 2? Will we get something congruent to 3?

Congruence and Arithmetic
Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then the following hold:

1. $a + c \equiv b + d \pmod{n}$
2. $a - c \equiv b - d \pmod{n}$
3. $ac \equiv bd \pmod{n}$

The above facts might be written a little strangely, but the idea is simple. If we have a true congruence, and we add the same thing to both sides, the result is still a true congruence. This sounds like we are saying:

If $a \equiv b \pmod{n}$ then $a + c \equiv b + c \pmod{n}$.

Of course that is true as well - it is the special case where $c = d$. But what we have works in more generality. Think of congruence as being "basically equal." If we have two numbers which are basically equal, and we add basically the same thing to both sides, the result will basically be equal.

This seems reasonable. Is it really true? Let's prove the first fact.

Proof. Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. That means $a = b + kn$ and $c = d + jn$ for integers k and j. Add these equations:

$$a + c = b + d + kn + jn.$$

But $kn + jn = (k + j)n$, which is just a multiple of n. So $a + c = b + d + (j + k)n$, or in other words, $a + c \equiv b + d \pmod{n}$ QED

The other two facts can be proved in a similar way.

One of the important consequences of these facts about congruences, is that we can basically replace any number in a congruence with any other number it is congruent to. Here are some examples to see how (and why) that works:

Example: Find the remainder of 3491 divided by 9.

Solution: We could do long division, but there is another way. We want to find x such that $x \equiv 3491 \pmod{9}$. Now $3491 = 3000 + 400 + 90 + 1$. Of course $90 \equiv 0 \pmod{9}$, so we can replace the 90 in the sum with 0. Why is this okay? We are actually subtracting the "same" thing from both sides:

$$\begin{array}{rl} & x \equiv 3000 + 400 + 90 + 1 \pmod{9} \\ - & 0 \equiv 90 \pmod{9} \\ \hline & x \equiv 3000 + 400 + 0 + 1 \pmod{9} \end{array}$$

Next, note that $400 = 4 \cdot 100$, and $100 \equiv 1 \pmod{9}$ (since $9 \mid 99$). So we can in fact replace the 400 with simply a 4. Again, we are appealing to our claim that we can replace congruent elements, but we are really appealing to property 3 about the arithmetic of congruence: we know $100 \equiv 1 \pmod{9}$, so if we multiply both sides by 4, we get $400 \equiv 4 \pmod{9}$.

Similarly, we can replace 3000 with 3, since $1000 = 1 + 999 \equiv 1 \pmod{9}$. So our original congruence becomes

$$x \equiv 3 + 4 + 0 + 1 \pmod{9}$$

$$x \equiv 8 \pmod{9}$$

Therefore 3491 divided by 9 has remainder 8.

The above example should convince you that the well known divisibility test for 9 is true: the sum of the digits of a number is divisible by 9 if and only if the original number is divisible by 9. In fact, we now know something more: any number is congruent to the sum of its digits, modulo 9.[3]

Let's try another.

Example: Find the remainder when 3^{123} is divided by 7.

Solution: Of course, we are working with congruence because we want to find the smallest positive x such that $x \equiv 3^{123} \pmod{7}$. Now first write $3^{123} = (3^3)^{41}$. We have:

$$3^{123} = 27^{41} \equiv 6^{41} \pmod{7}$$

since $27 \equiv 6 \pmod{7}$. Notice further that $6^2 = 36$ is congruent to 1 modulo 7. Thus we can simplify further:

$$6^{41} = 6 \cdot (6^2)^{20} \equiv 6 \cdot 1^{20} \pmod{7}$$

But $1^{20} = 1$, so we are done:

$$3^{123} \equiv 6 \pmod{7}$$

The above example works. We are using the fact that if $a \equiv b \pmod{n}$, then $a^p \equiv b^p \pmod{n}$. This is just applying property 3 a bunch of times.

So far we have seen how to add, subtract and multiply with congruences. What about division? There is a reason we have waited to discuss it. It turns out that we cannot simply divide. In other words, even if $ad \equiv bd \pmod{n}$, we do not know that $a \equiv b \pmod{n}$. Consider, for example:

$$18 \equiv 42 \pmod{8}$$

[3] This works for 3 as well, but definitely not for any modulus in general.

This is true. Now 18 and 42 are both divisible by 6. However,

$$3 \not\equiv 7 \pmod 8$$

While this doesn't work, note that $3 \equiv 7 \pmod 4$. We cannot divide 8 by 6, but we can divide 8 by the greatest common factor of 8 and 6. Will this always work?

Suppose $ad \equiv bd \pmod n$ In other words, we have $ad = bd + kn$ for some integer k. Of course ad is divisible by d, as is bd. So kn must also be divisible by d. Now if n and d have no common factors (other than 1), then we must have $d \mid k$. But in general, if we try to divide kn by d, we don't know that we will get an integer multiple of n. Some of the n might get divided as well. To be safe, let's divide as much of n as we can. Take the largest factor of both d and n, and cancel that out from n. The rest of the factors of d will come from k, no problem.

We will call the largest factor of both d and n, the $\gcd(d,n)$, for greatest common divisor. In our example above, $\gcd(6,8) = 2$ since the greatest divisor common to 6 and 8 is 2.

Congruence and Division

Suppose $ad \equiv bd \pmod n$. Then $a \equiv b \pmod{\frac{n}{\gcd(d,n)}}$

If d and n have no common factors[4] then $\gcd(d,n) = 1$, so $a \equiv b \pmod n$.

Example: Simplify the following congruences using division: (a) $24 \equiv 39 \pmod 5$ and (b) $24 \equiv 39 \pmod{15}$.

Solution: (a) Both 24 and 39 are divisible by 3, and 3 and 5 have no common factors, so we get

$$8 \equiv 13 \pmod 5$$

(b) Again, we can divide by 3. However, if doing so blindly gives us $8 \equiv 13 \pmod{15}$ which is no longer true. Instead, we must also divide the modulus 15 by the greatest common factor of 3 and 15, which is 3. Again we get

$$8 \equiv 13 \pmod 5$$

4 Solving Congruences

Now that we have some algebraic rules to govern congruence relations, we can attempt to solve for an unknown in a congruence. For example, is there a value of x that satisfies,

$$3x + 2 \equiv 4 \pmod 5,$$

and if so, what is it?

In this example, since the modulus is small, we could simply try every possible value for x. There are really one 5 to consider, since any integer that satisfied the congruence could be replaced with any other integer it was congruent to modulo 5. Here, $x = 4$ gives 14 which is indeed congruent to 4 modulo 5. This means that $x = 9$ and $x = 14$ and $x = 19$ and so on will each also be a solution because as we saw above, replacing any number in a congruence with a congruent number does not change the truth of the congruence.

So in this example, simply compute $3x + 2$ for values of $x \in \{0, 1, 2, 3, 4\}$. This gives 2, 5, 8, 11, and 14 respectively, for which only 14 is congruent to 4.

Let's also see how you could solve this using our rules for algebra of congruences. Such an approach would be much simpler that the trail and error tactic if the modulus was larger. First, we know we can subtract 2 from both sides:

$$3x \equiv 2 \pmod{5}.$$

Then to divide both sides by 3, we first add 0 to both sides. Of course, on the right hand side, we want that 0 to be a 10 (yes, 10 really is 0 - they are congruent modulo 5). This gives,

$$3x \equiv 12 \pmod{5}.$$

Now divide both sides by 3. Since $\gcd 3, 5 = 1$, we do not need to change the modulus:

$$x \equiv 4 \pmod{5}.$$

Notice that this in fact gives the *general solution*: not only can $x = 4$, but x can be any number which is congruent to 4. We can leave it like this, or write "$x = 4 + 5k$ for any integer k."

Here are a few of more examples of this process.

Example: Solve the following congruences for x.

1. $7x \equiv 12 \pmod{13}$
2. $84x - 38 \equiv 79 \pmod{15}$
3. $20x \equiv 23 \pmod{14}$

Solution:

1. All we need to do here is divide both sides by 7. We add 13 to the right hand side repeatedly until we get a multiple of 7 (adding 13 is the same as adding 0, so this is legal). We get 25, 38, 51, 64, 77 - got it. So we have:

$$\begin{aligned} 7x &\equiv 12 \pmod{13} \\ 7x &\equiv 77 \pmod{13} \\ x &\equiv 11 \pmod{13} \end{aligned}$$

2. Here, since we have numbers larger than the modulus, we can reduce them prior to applying any algebra. We have $84 \equiv 9$, $38 \equiv 8$ and $79 \equiv 4$. Thus,

$$\begin{aligned} 84x - 38 &\equiv 79 \pmod{15} \\ 9x - 8 &\equiv 4 \pmod{15} \\ 9x &\equiv 12 \pmod{15} \\ 9x &\equiv 72 \pmod{15} \end{aligned}$$

We got the 72 by adding $0 \equiv 60 \pmod{15}$ to both sides of the congruence. Now divide both sides by 9. However, since $\gcd 9, 15 = 3$, we must divide the modulus by 3 as well:

$$x \equiv 8 \pmod{5}$$

So the solutions are those values which are congruent to 8, or equivalently 3, modulo 5. This means that in some sense there are 3 solutions modulo 15: 3, 8, and 13. We can write the solution:

$$x \equiv 3 \pmod{15}; \quad x \equiv 8 \pmod{15}; \quad x \equiv 13 \pmod{15}$$

3. First reduce modulo 14:

$$6x \equiv 9 \pmod{14}$$

We could now divide both sides by 3, or try to increase 9 by a multiple of 14 to get a multiple of 6. If we divide by 3, we get,

$$2x \equiv 3 \pmod{14}$$

Now try adding multiples of 14 to 3, in hopes of getting a number we can divide by 2. This will not work! Every time we add 14 to the right side, the result will still be odd. We will never get an even number, so we will never be able to divide by 2. Thus there are no solutions to the congruence.

The last congruence above illustrates the way in which congruences might not have solutions. We could have seen this immediately in fact. Look at the original congruence:

$$20x \equiv 23 \pmod{14}$$

If we write this as an equation, we get

$$20x = 23 + 14k$$

or equivalently $20x - 14k = 23$. This is a linear Diophantine equation, and one for which we can easily see there will be no solution. The left hand side will always be even, but the right hand side is odd. A similar problem would occur if the right hand side was divisible by *any* number the left hand side was not.

So in general, given the congruence

$$ax \equiv b \pmod{n},$$

if a and n are divisible by a number which b is not divisible by, then there will be no solutions. In fact, we really only need to check one divisor of a and n: the greatest common divisor. Thus, a more compact way to say this is:

Congruences with no solutions
If $\gcd(a,n) \nmid b$, then $ax \equiv b \pmod{n}$ has no solutions.

5 Solving Linear Diophantine Equations

We now have the tools need to solve linear Diophantine equations such as

$$51x + 87y = 123.$$

The general strategy will be to convert the equation to a congruence, then solve that congruence.[5] Let's work this particular example to see how this might go.

First, check if perhaps there are no solutions because a divisor of 51 and 87 is not a divisor of 123. Really, we just need to check whether $\gcd(51, 87) \mid 123$. This greatest common divisor is 3, and yes $3 \mid 123$. At this point, we might as well factor out this greatest common divisor. So instead, we will solve:

$$17x + 29y = 41$$

Now observe that if there are going to be solutions, then for those values of x and y, the two sides of the equation must have the same remainder as each other, no matter what we divide by. In particular, if we divide both sides by 17, we must get the same remainder. Thus we can safely write,

$$17x + 29y \equiv 41 \pmod{17}$$

We choose 17 because $17x$ will have remainder 0. This will allow us to reduce the congruence to just one variable. We could have also moved to a congruence modulo 29, although there is usually a good reason to select the smaller choice, as this will allow us to reduce the other coefficient. In our case, we reduce the congruence as follows:

$$\begin{aligned}
17x + 29y &\equiv 41 \pmod{17}\\
0x + 12y &\equiv 7 \pmod{17}\\
12y &\equiv 24 \pmod{17}\\
y &\equiv 2 \pmod{17}
\end{aligned}$$

Now at this point we know $y = 2 + 17k$ will work for any integer k. If we haven't made a mistake, we should be able to plug this back into our original Diophantine equation to find x:

$$\begin{aligned}
17x + 29(2 + 17k) &= 41\\
17x &= -17 - 29 \cdot 17k\\
x &= -1 - 29k
\end{aligned}$$

We have now found all solutions to the Diophantine equation. For each k, $x = -1 - 29k$ and $y = 2 + 17k$ will satisfy the equation. We could check this for a few cases. If $k = 0$, the

[5] This is certainly not the only way to proceed. A more common technique would be to apply the *Euclidean algorithm*. Our way can be a little faster, and is presented here primarily for variety.

solution is $(-1, 2)$, and yes, $-17 + 2 \cdot 29 = 41$. If $k = 3$, the solution is $(-88, 53)$. If $k = -2$, we get $(57, -32)$.

To summarize this process, to solve $ax + by = c$, we,

1. Divide both sides of the equation by $\gcd a, b$ (if this does not leave the right hand side as an integer, there are no solutions). Let's assume that $ax + by = c$ has already been reduced in this way.

2. Pick the smaller of a and b (here, assume it is b), and convert to a congruence modulo b:
$$ax + by \equiv c \pmod{b}$$
This will reduce to a congruence with one variable, x:
$$ax \equiv c \pmod{b}$$

3. Solve the congruence as we did in the previous section. Write your solution as an equation, such as,
$$x = n + kb$$

4. Plug this into the original Diophantine equation, and solve for y.

5. If we want to know solutions in a particular range (for example, $0 \leq x, y \leq 20$), pick different values of k until you have all required solutions.

Here is another example.

Example: How can you make \$6.37 using just 5-cent and 8-cent stamps? What is the smallest and largest number of stamps you could use?

Solution: First we need a Diophantine equation. We will work in numbers of cents. Let x be the number of 5-cent stamps, and y be the number of 8-cent stamps. We have:
$$5x + 8y = 637.$$

Convert to a congruence and solve:

$$\begin{aligned} 8y &\equiv 367 \pmod{5} \\ 8y &\equiv 2 \pmod{5} \\ 8y &\equiv 32 \pmod{5} \\ y &\equiv 4 \pmod{5} \end{aligned}$$

Thus $y = 4 + 5k$. Then $5x + 8(4 + 5k) = 637$, so $x = 121 - 8k$.

This says that one way to make \$6.37 is to take 121 of the 5-cent stamps and 4 of the 8-cent stamps. To find the smallest and largest number of stamps, try different values of k.

k	(x, y)	Stamps
-1	(129, -1)	not possible
0	(121, 4)	125
1	(113, 9)	122
2	(105, 13)	119
$\vdots$	$\vdots$	$\vdots$

Of course this is no surprise - having the most stamps means we have as many 5-cent stamps as possible, and to get the smallest number of stamps would require have the least number of 5-cent stamps. To minimize the number of 5-cent stamps, we want to pick k so that $121 - 8k$ is as small as possible (but still positive). When $k = 15$, we have $x = 1$ and $y = 79$.

Therefore, to make $6.37, you can us as few as 80 stamps (1 5-cent stamp and 79 8-cent stamps) or as many as 125 stamps (121 5-cent stamps and 4 8-cent stamps).

Using this method, as long as you can solve linear congruences in one variable, you can solve linear Diophantine equations of two variables. There are times though that solving the linear congruence is a lot of work. For example, suppose you need to solve,

$$13x \equiv 6 \pmod{51}$$

You *could* keep adding 51 to the right side until you get a multiple of 13: You would get 57, 108, 159, 210, 261, 312, and 312 is the first of these that is divisible by 13. This works, but is really too much work. Instead we could convert *back* to a Diophantine equation:

$$13x = 6 + 51k$$

Now solve *this* like we have in this section. Write it as a congruence modulo 13:

$$\begin{aligned} 0 &\equiv 6 + 51k \pmod{13} \\ -12k &\equiv 6 \pmod{13} \\ 2k &\equiv -1 \pmod{13} \\ 2k &\equiv 12 \pmod{13} \\ k &\equiv 6 \pmod{13} \end{aligned}$$

so $k = 6 + 13j$. Now go back and figure out x:

$$\begin{aligned} 13x &= 6 + 51(6 + 13j) \\ x &= 24 + 51j \end{aligned}$$

Of course you could do this switching back and forth between congruences and Diophantine equations as many times as you like. If you *only* used this technique, you would essentially replicate the Euclidean algorithm (a more standard way to solve Diophantine equations).