3 Congruence

Congruences are an important and useful tool for the study of divisibility. As we shall see, they are also critical in the art of cryptography.

Definition 3.1 *If a and b are integers and $n > 0$, we write*

$$a \equiv b \bmod n$$

to mean $n|(b-a)$. We read this as "a is congruent to b modulo (or mod) n.

For example, $29 \equiv 8 \bmod 7$, and $60 \equiv 0 \bmod 15$.

The notation is used because the properties of congruence "$\equiv$" are very similar to the properties of equality "$=$". The next few result make this clear.

Theorem 3.2 *For any integers a and b, and positive integer n, we have:*
1. $a \equiv a \bmod n$.
2. If $a \equiv b \bmod n$ then $b \equiv a \bmod n$.
3. If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$

These results are classically called: 1. Reflexivity; 2. Symmetry; and 3. Transitivity. The proof is as follows:
1. $n|(a-a)$ since 0 is divisible by any integer. Therefore $a \equiv a \bmod n$.
2. If $a \equiv b \bmod n$ then $n|(b-a)$. Therefore, $n|(-1)(b-a)$ or $n|(a-b)$. Therefore, $b \equiv a \bmod n$.
3. If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $n|(b-a)$ and $n|(c-b)$. Using the linear combination theorem, we have $n|(b-a+c-b)$ or $n|(c-a)$. Thus, $a \equiv c \bmod n$.

The following result gives an equivalent way of looking at congruence. It replaces the congruence sign with an equality.

Theorem 3.3 *If $a \equiv b \bmod n$ then $b = a + nq$ for some integer q, and conversely.*

Proof: If $a \equiv b \bmod n$ then by definition $n|(b-a)$. Therefore, $b-a = nq$ for some q. Thus $b = a+nq$. Conversely if $b = a+nq$, then $b-a = nq$ and so $n|(b-a)$ and hence $a \equiv b \bmod n$ then $b = a + nq$.

We will use often this theorem for calculations. Thus, we can write $15 \equiv -2 \bmod 17$ by subtracting 17 from 15: $-2 = 15 + (-1) \cdot 17$. Similarly, $52 \equiv 12 \bmod 20$. Just subtract 40 (2 times 20) from 52.

A simple consequence is this: Any number is congruent mod n to its remainder when divided by n. For if $a = nq + r$, the above result shows that $a \equiv r \bmod n$. Thus for example, $23 \equiv 2 \bmod 7$ and $103 \equiv 3 \bmod 10$. For this reason, the remainder of a number a when divided by n is called $a \bmod n$. In EXCEL, as in many spreadsheets, this is written "MOD(a,n)." If you put the expression =MOD(23,7) in a cell, the readout will be simply 2. Try it!

Another way of relating congruence to remainders is as follows.

Theorem 3.4 *If $a \equiv b \bmod n$ then a and b leave the same remainder when divided by n. Conversely if a and b leave the same remainder when divided by n, then $a \equiv b \bmod n$.*

Proof: Suppose $a \equiv b \bmod n$. Then by Theorem 3.3, $b = a + nq$. If a leaves the remainder r when divided by n, we have $a = nQ + r$ with $0 \leq r < n$. Therefore, $b = a + nq = nQ + r + nq = n(Q + r) + r$, and so b leaves the same remainder when divided by n. The converse is straightforward and we omit the proof.

We can now show some useful algebraic properties of congruences. Briefly, congruences can be added and multiplied.

Theorem 3.5 *If $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then*
1. $a + c \equiv b + d \bmod n$.
2. $ac \equiv bd \bmod n$.

Proof: Write $b = a + nq_1$ and $d = c + nq_2$, using Theorem 3.3. Then adding equalities, we get $b + d = a + c + nq_1 + nq_2 = a + c + n(q_1 + q_2)$. This shows that $a + c \equiv b + d \bmod n$ by Theorem 3.3.

Similarly, multiplying, we get $bd = (a + nq_1)(c + nq_2) = ac + naq_2 + ncq_1 + n^2q_1q_2$. Thus, $bd = ac + n(aq_2 + cq_1 + nq_1q_2$, and so $ac \equiv bd \bmod n$, again by Theorem 3.3.

Some Examples.
We have noted that $23 \equiv 2 \bmod 7$. We can square this (i.e. multiply this congruence by itself) to get $23^2 \equiv 4 \bmod 7$. What a nice way to find the remainder of 23^2 when it is divided by 7! Multiply again by $23 \equiv 2 \bmod 7$, to get

$$23^3 \equiv 8 \equiv 1 \bmod 7$$

(This string of congruences is similar to a string of inequalities. It is read 23^3 is congruent to 8 which is congruent to 1 mod 7. By transitivity (Theorem 3.2) this implies that 23^3 is congruent to 1 mod 7.) Once we know that $23^3 \equiv 1 \bmod 7$, we can raise to the 5th power (i.e. multiply this by itself 5 times) to get $23^{15} \equiv 1 \bmod 7$. The application of a few theorems and we have found remainders of huge numbers rather easily!

Example 3.6 *Find* $17^{341} \bmod 5$. As explained on page 26, this is the remainder when 17^{341} is divided by 5.

Method. We have

$$17 \equiv 2 \bmod 5$$

Squaring, we have

$$17^2 \equiv 4 \equiv -1 \bmod 5$$

Squaring again, we find

$$17^4 \equiv 1 \bmod 5$$

Now, 1 to any power is 1, so we raise this last congruence to the 85th power. Why 85? Just wait a moment to find out. We then find

$$17^{340} \equiv 1 \bmod 5$$

Finally, multiply by the first congruence to obtain

$$17^{341} \equiv 2 \bmod 5$$

So the required remainder is 2.

The strategy is to find some power of 17 to be 1 mod 5. Here, the power 4 worked. The we divided 4 into 341 to get a quotient 85, and this is the power we used on the congruence $17^4 \equiv 1 \bmod 5$. Note also the little trick of replacing 4 by $-1 \bmod 5$. This gives an easier number to square.

Example 3.7 *Solve for* x : $5x \equiv 1 \bmod 12$.

One method is as follows. We know that $\gcd(5, 12) = 1$, so some linear combination of 5 and 12 is equal to 1. In Section 1 we had a general method for doing this, and we also had a spreadsheet approach. However, we can simply note by observation that

$$1 = 5 \cdot 5 + (-2) \cdot 12$$

So both sides of this equality are congruent to each other mod 12. Hence

$$1 \equiv 5 \cdot 5 + (-2) \cdot 12 \equiv 5 \cdot 5 \bmod 12$$

So one solution is $x = 5$. More generally, if $x \equiv 5 \bmod 12$ then

$$5x \equiv 25 \equiv 1 \bmod 12$$

Here is another approach: Start with the equation $5x \equiv 1 \bmod 12$. If this were an equality, we would simply divide by 5 to get $x = 1/5$. But we are in the realm of integers so this won't work. Instead we *multiply* by 5 to get $25x \equiv 5 \bmod 12$ or $x \equiv 5 \bmod 12$. Note that we multiplied by 5 to get a coefficient of 1: $5 \cdot 5 \equiv 1 \bmod 12$.

The algebra of congruences is sometime referred to as "clock arithmetic." This example illustrates this. Imagine you are a mouse and that each day you travel clockwise around a clock, passing through 25 minutes on the clock. You start at 12 o'clock. Here is what you journey will look like:

Start	Day 1	Day 2	Day 3	Day 4	Day 5
12 Midnight	5 o'clock	10 o'clock	3 o'clock	8 o'clock	1 o'clock

Note that the transition from 10 o'clock was not to 15 o'clock, but (working mod 12) to 15 mod 12 or 3 o'clock. In terms of clocks, we asked when the mouse would land at the 1 o'clock spot on the clock.

We can quickly find when the mouse will land at 4 o'clock. The equation is

$$5x \equiv 4 \bmod 12$$

Multiply by 5 to get $25x \equiv 20 \bmod 12$ or simply $x \equiv 8 \bmod 12$. It take 8 days.

Example 3.8 *Same clock, different mouse. This mouse goes 23 minutes a day and starts at 12 o'clock. How many days before she reaches 9 minutes before 12?*

The appropriate congruence is $23x \equiv -9 \bmod 60$. We'll use the gcd method and find 1 as a linear combination of 23 and 60. A spreadsheet calculation gives

$$1 = -13 \cdot 23 + 5 \cdot 60$$

Taking this mod 60, we find

$$23(-13) \equiv 1 \bmod 60.$$

Multiply by -9 to get

$$23(117) \equiv -9 \bmod 60.$$

But $117 \equiv 57 \bmod 60$. And so the mouse must travel 57 days to reach 9 minutes before the hour. Note that $57 \equiv -3 \bmod 60$ so the mouse will take 3 days if she goes in the other direction.

Up to now, all of our congruences have been modulo one fixed n. The following results show how to change the modulus in certain situations.

Theorem 3.9 *If $a \equiv b \bmod n$, and c is a positive integer, then $ca \equiv cb \bmod cn$*

Proof: This is little more than a divisibility theorem. Since $n|(b-a)$, we have $cn|c(b-a)$ or $cn|(cb-ca)$, and this is the result.

The converse is also valid. Thus, if $ca \equiv cb \bmod cn$ with $c > 0$ then $a \equiv b \bmod n$.

These results can be stated: A congruence can by multiplied through (including the modulus) and similarly, it can be divided by a common divisor.

Finally, we can mention that if $a \equiv b \bmod n$ and if $d|n$, then $a \equiv b \bmod d$. We leave the proof to the reader.

We can now tackle the general question of solving a linear congruence $ax \equiv b \bmod n$. We will find when this congruence has a solution, and how many solutions it has. We first consider the case $\gcd(a, n) = 1$. (In the examples above, this was the situation.) The following theorem answers this question and also shows how to find the solution.

Theorem 3.10 *If $\gcd(a, n) = 1$, then the congruence $ax \equiv b \bmod n$ has a solution $x = c$. In this case, the general solution of the congruence is given by $x \equiv c \bmod n$.*

Proof: Since a and n are relative prime, we can express 1 as a linear combination of them:

$$ar + ns = 1$$

Multiply this by b to get $abr + nbs = b$. Take this mod n to get

$$abr + nbs \equiv b \bmod n \text{ or } abr \equiv b \bmod n$$

Thus $c = br$ is a solution of the congruence $ax \equiv b \bmod n$. In general, if $x \equiv c \bmod n$ we have $ax \equiv ac \equiv b \bmod n$.

We now claim that *any* solution of $ax \equiv b \bmod n$ is necessarily congruent to $c \bmod n$. For suppose $ax \equiv b \bmod n$. We already know that $ac \equiv b \bmod n$. Subtract to get

$$ax - ac \equiv 0 \bmod n \text{ or } a(x-c) \equiv 0 \bmod n$$

But this means that $n|a(x-br)$. But since a and n are relatively prime, this implies that $n|(x-c)$ and $x \equiv c \bmod n$. This completes the proof.

An important special case occurs when n is a prime p.

Corollary 3.11 *If p is a prime, the congruence $ax \equiv b \bmod p$ has a unique solution $x \bmod p$ provided $a \not\equiv 0 \bmod p$.*

The reason we single this case out is that this result is almost exactly like the similar result in high school algebra: The equation $ax = b$ has a unique solution provided $a \neq 0$. We shall soon delve further into this analogy. The reason this is true is that if an integer a is not divisible by p, it is relatively prime to p. Thus, if $a \not\equiv 0 \bmod p$, then a and p are relatively prime.

During the course of the proof of theorem 3.10 , we proved the following useful result.

Theorem 3.12 *If $ab \equiv ac \bmod n$ and if $\gcd(a, n) = 1$, then we have $b \equiv c \bmod n$.*

In short, we can cancel the factor a from both sides of the congruence so long as $\gcd(a, n) = 1$. In algebra, we learn that we "can divide an equation $ax = ay$ by a" if $a \neq 0$. Here we can "cancel the factor a from both sides of the congruence $ax \equiv ay \bmod n$" if a and n are relatively prime. This theorem is sometimes called the cancelation law for congruences.

Now suppose that we wish to solve the congruence $ax \equiv b \bmod n$ where $d = \gcd(a, n) > 1$. For example, consider the congruence $18x \equiv 12 \bmod 24$. Here $d = \gcd(18, 24) = 6$. We can divide this congruence by 6 to get the equivalent[15] congruence $3x \equiv 2 \bmod 4$. So we end up with the congruence $3x \equiv 2 \bmod 4$, in which $\gcd(3, 4) = 1$ and which has general solution $x \equiv 2 \bmod 4$. So this is the solution of the original congruence $18x \equiv 12 \bmod 24$. This worked because the gcd also divided the constant term 12. If it didn't there would be no solution. This is the content of the following theorem which generalizes this problem.

Theorem 3.13 *Given the congruence $ax \equiv b \bmod n$. Let $d = gcd(a, n)$. Then*
1. If d does not divide b, the congruence has no solution.
2. If $d|b$ then the congruence is equivalent to the congruence $(a/d)x \equiv (b/d) \bmod (n/d)$ which has a unique solution mod n/d.

Proof: Suppose there were a solution of $ax \equiv b \bmod n$. Then we would have $ax \equiv b \bmod d$. But $a \equiv 0 \bmod d$ since $d|a$. So we would have $0 \equiv b \bmod d$ or $d|b$. So a necessary condition for a solution is that $d|b$. This prove part 1. As for part 2, divide the entire congruence by d as in the above example. The reduced congruence has a unique solution mod n/d since a/d and n/d are relatively prime.

Algebra on a Small Scale.
Corollary 3.11 has an interesting interpretation–if p is a prime and we work mod p, the integers mod p behave algebraically like the real numbers. In the real number system the equation $ax = b$ has a solution $x = b/a = ba^{-1}$ where $a^{-1} = 1/a$ is the reciprocal of a and is the solution of the equation $ax = 1$. What is the situation if we try to do this mod p?

[15] It is equivalent, since we can multiply the resulting congruence by 6 to get back the original congruence.

Example 3.14 *What is the value of* $5^{-1} \bmod 7$*?*

Method. It is required to find the solution of $5x \equiv 1 \bmod 7$. We can do this using the method of Example 3. Since

$$3 \cdot 5 + (-2)7 = 1$$

be observation, we have

$$3 \cdot 5 \equiv 1 \bmod 7$$

So $5^{-1} \equiv 3 \bmod 7$, or simply $5^{-1} = 3 \bmod 7$, where equality if used because it is understood that we are working mod 7.

Since we are working mod 7, there are only 7 different numbers mod 7, namely the remainders 0 through 6 when a number is divided by 7. So the algebra of numbers mod 7 is a strictly finite algebra. Here is the multiplication table for these numbers mod 7. We omit 0.

$\times$	1	2	3	4	5	6
1	$\underline{1}$	2	3	4	5	6
2	2	4	6	$\underline{1}$	3	5
3	3	6	2	5	$\underline{1}$	4
4	4	$\underline{1}$	5	2	6	3
5	5	3	$\underline{1}$	6	4	2
6	6	5	4	3	2	$\underline{1}$

Multiplication Table mod 7

The number 1 is underlined in the body of the table. The row and column where a 1 appears are inverses, because the product is 1. By observation, we can see that 2 and 4 are inverses mod 7, as are 3 and 5. Both 1 and 6 are self inverses. (Note that $6 = -1 \bmod 7$, and so it is not surprising that 6 is its own inverse: $(-1)^{-1} = -1$.

Let us go one step further with the analogy with ordinary algebra.

Example 3.15 *Solve the congruence* $8x \equiv 13 \bmod 29$*.*

First method. In analogy with algebra we expect the solution $x \equiv 13 \cdot 8^{-1} \bmod 29$. So we first compute $8^{-1} \bmod 29$. We express 1 as a linear combination of 8 and 29 by the method given in section 1, or using a spreadsheet. A possible result is

$$1 = 11 \cdot 8 - 3 \cdot 29$$

Taking this mod 29, we find $8^{-1} \equiv 11 \bmod 29$. So, solving for x, we find

$$x \equiv 13 \cdot 8^{-1} \equiv 13 \cdot 11 = 143 \equiv 27 \bmod 29$$

Second method. Using fractions, we write

$$x \equiv \frac{13}{8} \bmod 29$$

Ordinarily, we cancel factors in the numerator and denominator. We can't do this here, but we can *multiply* numerator and denominator by the same (non-zero) number. We choose 4, because this gets the denominator close to the modulus 29, making the quotient simpler. Thus

$$x \equiv \frac{13}{8} \equiv \frac{52}{32} \equiv \frac{23}{3} \bmod 29$$

Now do it again, using a factor 10:

$$\frac{23}{3} \equiv \frac{230}{30} \equiv \frac{27}{1} \equiv 27 \bmod 29$$

This is the same answer, of course. Here's the way the full solution works in one line:

$$x \equiv \frac{13}{8} \equiv \frac{52}{32} \equiv \frac{23}{3} \equiv \frac{230}{30} \equiv \frac{27}{1} \equiv 27 \bmod 29$$

Third method. When we write $x \equiv \frac{13}{8} \bmod 29$, we can cancel at least one factor 2, if we *add* 29 to the numerator. Thus,

$$x \equiv \frac{13}{8} \equiv \frac{42}{8} \equiv \frac{21}{4} \equiv \frac{50}{4} \equiv \frac{25}{2} \equiv \frac{54}{2} \equiv \frac{27}{1} \equiv 27 \bmod 29$$

We don't necessarily recommend this method, but we use it to illustrate that there are often many ways to attack a problem and to show the inner consistency of our small scale arithmetic.

Divisibility Tricks. The number 345,546,711 is divisible by 3. In fact it is divisible by 9. We can discover this easily using the following trick, which we shall prove.

A number is congruent mod 9 *to the sum of the digits in that number.*

Here we have

$$345,546,711 \equiv 3+4+5+5+4+6+7+1+1 = 36 \equiv 3+6 = 9 \equiv 0 \bmod 9$$

In fact, using this result, it is not even necessary to find the sum. There are short cuts. For example $3+4+5 = 12$ which is congruent to *its* digit sum $1+2 = 3 \bmod 9$. Continuing, add $5+5 = 10 \equiv 1$, so we add 1 to 3 to get 4. And so on. This is a lot easier to do than to explain. Briefly, any time you get a two digit answer, replace it by its digit sum.

The proof of this trick depends on the knowledge that the digits in an expansion of a number represent coefficient of powers of 10. Thus,

$$3,412 = 3 \times 10^3 + 4 \times 10^2 + 1 \times 10^1 + 2 \times 1$$

Since $10 \equiv 1 \bmod 9$, we can square to get $10^2 \equiv 1 \bmod 9$. Similarly, by cubing we get $10^3 \equiv 1 \bmod 9$, and so on. Thus,

$$3412 = 3 \times 10^3 + 4 \times 10^2 + 1 \times 10^1 + 2 \times 1 \equiv 3 + 4 + 1 + 2 \bmod 9$$

where the latter sum is simply the sum of the digits of 3412. This generalizes to give the result. It follows that a number is congruent to its digit sum mod 3, because if $a \equiv b \bmod n$ and $d|n$ then $a \equiv b \bmod n$. (Here $n = 9$ and $d = 3$.)

This simple trick has a useful application. It is a check on possible calculation errors. For example, suppose you are given the multiplication $341 \times 167 = 56847$ and you are suspicious of this result. (Perhaps someone was sloppy or didn't copy it down correctly.) Now if this multiplication were true, it would also be true mod 9. But $341 \equiv 8 \bmod 9$ (just add the digits!) and $167 \equiv 14 \equiv 5 \bmod 9$ so $341 \times 167 \equiv 8 \times 5 = 40 \equiv 4 \bmod 9$. But the answer given us was $56847 \equiv 30 \equiv 3 \bmod 9$, and so it was in error. This method is not failsafe, but it is a quick check.[16] Incidentally, you know that the multiplication $1234567 \times 245678 = 303305951435$ is wrong. (Hint: look at the last digits.) You know it's wrong by checking the answer mod 10.

There is another simple trick to find a number mod 11 using its digits. In this case, we find the alternating sum starting with the units column. For example, to find 56744 mod 11, we compute $56743 \equiv 3 - 4 + 7 - 6 + 5 = 5 \bmod 11$. The proof is similar to the proof above, and is based on the simple congruence $10 =\equiv -1 \bmod 11$. Squaring, we get $100 =\equiv 1 \bmod 11$. Cubing, we get $1000 \equiv 1 \bmod 11$, etc. Thus,

$$56743 = 3 + 4 \times 10 + 7 \times 10^2 + 6 \times 10^3 + 5 \times 10^4 \equiv 3 - 4 + 7 - 6 + 5 = 5 \bmod 11$$

The general proof is the same.

For example, the alleged calculation $345 \times 3456 = 1129320$ can be check mod 11. We have

$$345 \times 3456 \equiv (5 - 4 + 3)(6 - 5 + 4 - 3) = 4 \times 2 = 8 \bmod 11$$

The alleged answer is $1129320 \equiv 0 - 2 + 3 - 9 + 2 - 1 + 1 = -6 \equiv 5 \not\equiv 8 \bmod 11$. The actual answer for this multiplication is 11<u>92</u>320, so the error was a simple transposition of digits, a common error. The alternating sum will catch such an error.

Exercises on Congruences.

1. If $a \equiv b \bmod 2$ show that both a and b are both odd, or they are both even.

2. Given that $a \equiv b \bmod 1$. What does this say about a and b?

[16] A personal tale: In the early grades, when I was learning simple additions and multiplications, the teacher told this trick to someone in the class (not me) who used it to check the work of the others. Naturally, this was resented by me, so giving this trick is my small revenge. Now you all know it!

3. How would you interpret the congruence $a \equiv b \bmod 0$?

4. If $a \equiv b \bmod 4$ and $a \equiv b \bmod 5$, show that $a \equiv b \bmod 20$.

5. Prove: $a \equiv b \bmod m$ and $a \equiv b \bmod n$, and $\gcd(m, n) = 1$, then $a \equiv b \bmod mn$.

6. Find $2^{501} \bmod 17$.

7. Find $3^{701} \bmod 80$.

8. Find $7^{-1} \bmod 13$.

9. Find $13^{-1} \bmod 17$.

10. Solve for x: $6x \equiv 5 \bmod 7$.

11. Solve for x: $7x \equiv 4 \bmod 11$.

12. Solve for x: $41x \equiv 5 \bmod 51$.

13. Solve for x: $62x \equiv 55 \bmod 125$.