The simplest equation to solve in a basic algebra class is the equation $ax = b$, with solution $x = \frac{b}{a}$, provided $a \neq 0$. The simplest congruence to solve is the linear congruence, $ax \equiv b \pmod{m}$. In this case, we expect the solution to be a congruence as well. For example, if $5x \equiv 7 \pmod{12}$, then one solution is $x = 11$ since $5 \times 11 - 7 = 48$, which is divisible by 12. But $x = 23$ is also a solution as is $x = -13$. More generally, $x = 11 + 12k$ works for any $k$. In fact, if $x_0$ is a solution to $ax \equiv b \pmod{m}$, then $ax_0 - b$ is divisible by $m$. Consequently, $a(x_0 + km) - b = ax_0 - b + km$ is also divisible by $m$ for any value of $k$. This means any $x \equiv x_0 \pmod{m}$ is a solution. In fact, a little more is true.

**Theorem 1** The congruence $ax \equiv b \pmod{m}$ has a solution if and only if the greatest common divisor of $a$ and $m$ is a divisor of $b$. That is, if $d = \gcd(a, m)$, then the congruence has a solution if and only if $d \mid b$. If there is a solution, $x_0$, then the set of all solutions is the set of all $x$ with $x \equiv x_0 \pmod{m/d}$.

**Proof:** The congruence $ax \equiv b \pmod{m}$ has a solution if and only if there are integers $x$ and $k$ for which $ax - b = km$. Letting $y = -k$, this can be written $ax + my = b$. That is, the congruence is equivalent to a linear Diophantine equation. From a previous set of notes, we know that this equation only has a solution if $d = \gcd(a, m)$ is a divisor of $b$. Moreover, if the equation has a solution $(x_0, y_0)$, then the general solution has the form $x = x_0 + \frac{m}{d}t$, $y = y_0 - \frac{a}{d}t$. We actually do not care about $y$. What is important is that all solutions $x$ have the form $x = x_0 + \frac{m}{d}t$, which is to say $x \equiv x_0 \pmod{m/d}$.

The proof also tells us how to solve the congruence $ax \equiv b \pmod{m}$. We convert to a linear Diophantine equation, and use the Euclidean algorithm or Euler’s algorithm. For example, suppose we wish to solve $15x \equiv 33 \pmod{69}$. Since $\gcd(15, 69) = 3$ and $3 \mid 33$ we know there is a solution, and the linear Diophantine equation to solve is $15x + 69y = 33$. Again, we don’t even care about $y$ except that it helps us get $x$. Using Euler’s method, $x = \frac{33 - 69y}{15} = 2 - 4y + \frac{3 - 9y}{15} \to 15z + 9y = 3 \to y = \frac{3 - 15z}{9} = -z + \frac{3 - 6z}{9} \to 9w + 6z = 3$, which has obvious solution $w = 1$, $z = -1 \to y = 2 \to x = -7$. The Diophantine equation has $(x)$ solution $x = -7 + 23t$, so the congruence has solution $x \equiv -7 \pmod{23}$, which is the same as $x \equiv 16 \pmod{23}$.

Suppose, for some reason, we wish to solve the more complicated congruence $5x^2 + 6x + 7 \equiv 0 \pmod{35}$. This again has congruences for solutions. That is, if $5a^2 + 6a + 7 \equiv 0 \pmod{35}$, this means that 35 is a divisor of $5a^2 + 6a + 7$, and since $5(a + 35k)^2 + 6(a + 35k) + 7 = 5a^2 + 6a + 7 + 35(10ka + 175k^2 + 6k)$, if $a$ satisfies the congruence, so does $a + 35k$ for any integer $k$. This works for any polynomial congruence $P(x) \equiv 0 \pmod{m}$, by the way. Solutions are congruences modulo $m$.

Back to the given problem, we can’t use the quadratic formula because square roots are problematic with modular arithmetic (we need integers). A simpleminded approach is to just try $x = 0, x = 1, x = 2, \ldots, x = 34$, all modulo 35. That is, plug in $x = 0, x = 1, \ldots$ looking for numbers divisible by 35. Trying to be more sophisticated, we could try to simplify the
problem: If $5x^2 + 6x + 7$ is divisible by 35, then it must be divisible by both 5 and 7. Rather than a congruence modulo 35, let’s look at two congruences: $5x^2 + 6x + 7 \equiv 0 \pmod{5}$ and $5x^2 + 6x + 7 \equiv 0 \pmod{7}$. The first congruence is the same as $x + 2 \equiv 0 \pmod{5}$, or $x \equiv 3 \pmod{5}$. The second is equivalent to $5x^2 + 6x \equiv 0 \pmod{7}$. This has an obvious solution $x \equiv 0 \pmod{7}$ and another not quite as obvious solution $x \equiv 3 \pmod{7}$. How do we use these to get solutions to the original problem? What we need are numbers that are congruent to 3 modulo 5, and to either 0 or 3 modulo 7. Here is a simple way to find such numbers: If we are 3 modulo 5, then we belong to the arithmetic sequence 3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58, 63, 68, 73, 78, . . . . Numbers that are 0 modulo 7 belong to the sequence 0, 7, 14, 21, 28, 35, 42, 49, 56, 63, 70, . . . . If we look for overlap, we notice 28 and 63. Since solutions are supposed to be determined modulo 35, this must mean $x \equiv 28 \pmod{35}$ is a solution. In fact, all we needed was to calculate that part of the progressions between 0 and 35 to see the matches. Similarly, if $x \equiv 3 \pmod{7}$ then $x$ belongs to the progression 3, 10, 17, 24, 31, . . . , and we get a second solution $x \equiv 3 \pmod{35}$. These are both easy to check, of course, $5 \cdot 28^2 + 6 \cdot 28 + 7 = 4095 = 117 \cdot 35$, for example.

It would be nice if we could stitch smaller congruences together to get bigger ones by something nicer than the approach above. For example, suppose we had the congruence $71x^2 + 72x + 73 \equiv 0 \pmod{5183}$. Here, 5183 = 71 \cdot 73, so this is very similar to the example above, just bigger. If we look modulo 71, we get $x + 2 \equiv 0 \pmod{71}$, or $x \equiv 69 \pmod{71}$. (Actually, this is probably better written $x \equiv -2 \pmod{71}$.) The second congruence is $71x^2 + 72x \equiv 0 \pmod{73}$, which again has obvious solution $x \equiv 0 \pmod{73}$. In fact, we can find a second solution as well: if $x \equiv 0 \pmod{73}$, then we can cancel an $x$ to get $71x + 72 \equiv 0 \pmod{73}$. If I were to solve this, I would write it as $-2x - 1 \equiv 0 \pmod{73}$, or $2x \equiv -1 \equiv 72 \pmod{73}$, so $x \equiv 36 \pmod{73}$. What we need: A number $x$ for which $x \equiv -2 \pmod{71}$ and $x \equiv 0 \pmod{73}$ and a second $x$ with $x \equiv -2 \pmod{71}$ and $x \equiv 36 \pmod{73}$. Looking for the intersection of arithmetic progressions would be tedious, at least for a human.

There is a systematic approach to this problem, called the Chinese Remainder Theorem. The reason for the name is that a very early reference to this kind of problem comes from China. In the writings of Sun Tsu, he posesses the question of finding a number which leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5 and a remainder of 2 again when divided by 7. In the notation of congruences, he asked for numbers $x$ simultaneously satisfying the system of congruences

\[
\begin{align*}
x &\equiv 2 \pmod{3} \\
x &\equiv 3 \pmod{5} \\
x &\equiv 2 \pmod{7}.
\end{align*}
\]
Theorem 2 (The Chinese Remainder Theorem) Let \( m_1, m_2, \ldots, m_k \) be pairwise relatively prime positive integers. That is, no \( m \) has any factors in common with any other \( m \). Let \( a_1, a_2, \ldots, a_k \) be any set of integers. Then there is an integer \( x \) such that

\[
\begin{align*}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\vdots \\
x &\equiv a_k \pmod{m_k}.
\end{align*}
\]

Moreover, if \( M = m_1m_2 \cdots m_k \), then \( x \) is unique modulo \( M \).

We will give a proof that though constructive, is mostly of theoretical interest. That is, it can be used to find solutions but the numbers involved tend to be large. First, a linear algebra digression. Suppose we define three vectors by

\[
e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.
\]

Then given any three numbers \( a_1, a_2, a_3 \), we can write the vector \( \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \) as a combination of these three, namely

\[
\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = a_1e_1 + a_2e_2 + a_3e_3.
\]

This same idea can be used in many different areas of mathematics. For example, suppose we want a polynomial \( p(x) \) to have the following properties: \( p(1) = 2, p(3) = 5, p(6) = 3 \). One way is to find three polynomials, \( p_1(x), p_2(x), p_3(x) \) for which

\[
\begin{align*}
p_1(1) &= 1, \quad p_1(3) = 0, \quad p_1(6) = 0, \\
p_2(1) &= 0, \quad p_2(3) = 1, \quad p_2(6) = 0, \\
p_3(1) &= 0, \quad p_3(3) = 0, \quad p_3(6) = 1,
\end{align*}
\]

and let \( p(x) = 2p_1(x) + 5p_2(x) + 3p_3(x) \). How do we find these polynomials? As usual, there is a trick. First, we consider the polynomial \( q(x) = (x - 1)(x - 3)(x - 6) \). To get \( p_1, p_2 \) and \( p_3 \) we delete various factors and plug in values for \( x \). Specifically,

\[
\begin{align*}
p_1(x) &= \frac{(x - 3)(x - 6)}{(1 - 3)(1 - 6)}, \\
p_2(x) &= \frac{(x - 1)(x - 6)}{(3 - 1)(3 - 6)}, \\
p_3(x) &= \frac{(x - 1)(x - 3)}{(6 - 1)(6 - 3)},
\end{align*}
\]

or

\[
\begin{align*}
p_1(x) &= \frac{1}{10}(x - 3)(x - 6), \\
p_2(x) &= -\frac{1}{6}(x - 1)(x - 6), \\
p_3(x) &= \frac{1}{15}(x - 1)(x - 3),
\end{align*}
\]
and the desired polynomial is \( p(x) = \frac{1}{6}(x - 3)(x - 6) - \frac{5}{6}(x - 1)(x - 6) + \frac{1}{6}(x - 1)(x - 3) = -\frac{13}{30}x^2 + \frac{97}{30}x + \frac{2}{5}. \)

**Proof:** After this long digression, here is the proof. We first seek numbers \( M_1, M_2, \ldots, M_k \) with the property that \( M_1 \equiv 1 \pmod{m_1}, M_1 \equiv 0 \pmod{m_j} \) for each \( j > 1 \), and in general, for each \( i, M_i \equiv 1 \pmod{m_i}, M_i \equiv 0 \pmod{m_j} \) for each \( j \neq i \). If we can find such \( M \)'s then a solution would be \( x = a_1 M_1 + a_2 M_2 + \cdots + a_k M_k \). In fact, it is easy to give a formula for the \( M \)'s. We have

\[
M_1 = \left( \frac{M}{m_1} \right)^{\phi(m_1)}, \quad \left( \frac{M}{m_2} \right)^{\phi(m_2)}, \quad \ldots, \quad \left( \frac{M}{m_k} \right)^{\phi(m_k)}.
\]

Why do these have the desired properties? First, since the \( m \)'s are relatively prime, \( \frac{M}{m_1} \) is relatively prime to \( m_1 \), but it is divisible by \( m_2, \ldots, m_k \). This means that \( M_1 \) is divisible by \( m_2, \ldots, m_k \), so \( M_1 \equiv 0 \pmod{m_j} \) for each \( j > 1 \). By Euler’s theorem, \( M_1 \equiv 1 \pmod{m_1} \), and this argument can be used on each of the other \( M \)'s.

To see that \( x \) is unique modulo \( M \), suppose that \( y \) is also a solution. Then \( x \equiv a_1 \pmod{m_1} \) and \( y \equiv a_1 \pmod{m_1} \), so \( x = y \pmod{m_1} \). Similarly, \( x \equiv y \pmod{m_i} \) for each \( i \). This means that \( x - y \) is divisible by each of \( m_1, m_2, \ldots, m_k \). Since the \( m \)'s are relatively prime, \( x - y \) is divisible by \( m_1 m_2 \cdots m_k \). That is, \( x - y \) is divisible by \( M \) so \( x \equiv y \pmod{M} \). }

As an example, let’s solve Sun Tzu’s problem. In this case, \( m_1 = 3, m_2 = 5, m_3 = 7, M = 3 \cdot 5 \cdot 7 = 105 \). Also, \( \phi(3) = 2, \phi(5) = 4, \phi(7) = 6 \). With all this, \( M_1 = (5 \cdot 7)^2 = 1225, M_2 = (3 \cdot 7)^4 = 194,481, M_3 = (3 \cdot 5)^6 = 11,390,625 \). Finally, this means that one solution is \( x = 2M_1 + 3M_2 + 2M_3 = 23,367,143 \). Obviously, a drawback to this method is that it gives very large solutions. One way to keep the calculations smaller is to reduce things modulo \( M \). In particular, rather than \( M_1 = 1225 \), we can reduce this modulo 105 and instead let \( M_1 = 70 \). Similarly, we can let \( M_2 = 21, M_3 = 15 \) so \( x = 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233 \). Again, we can reduce modulo 105. The solution is \( x \equiv 23 \pmod{105} \). The solution \( x = 23 \) was what Sun Tzu gave as the answer.

As a second example, suppose \( m_1 = 5, m_2 = 7, m_3 = 9 \). Then \( \phi(5) = 4, \phi(7) = 6, \phi(9) = 6 \), so \( M_1 = 63^4, M_2 = 45^6, M_3 = 35^6 \). As before, we can restrict the \( M \)'s to be numbers modulo \( M = 315 \), so we can let \( M_1 = 126, M_2 = 225, M_3 = 280 \). Now suppose we wish to solve the system \( x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}, x \equiv 3 \pmod{9} \). Then by the proof of the theorem, \( x = 3 \cdot 126 + 2 \cdot 225 + 3 \cdot 280 = 1668 \) will work. reducing modulo 315, we have \( x \equiv 93 \pmod{315} \).

There is another approach to solving systems of congruences. Again, suppose we wish to solve the system \( x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}, x \equiv 3 \pmod{9} \). We build up the solution congruence by congruence, as follows. From \( x \equiv 3 \pmod{5} \) we know \( x = 3 + 5k \) for some integer \( k \). We substitute this into the second congruence to get \( 3 + 5k \equiv 2 \pmod{7} \), and try to solve this for \( k \). Adding 4 to each side (using \( 7 \equiv 0 \pmod{7} \)), we have \( 5k \equiv 6 \pmod{7} \).
This is a standard linear congruence as described at the beginning of this set of notes. We could convert to a linear Diophantine equation or just note that $3 \cdot 5 = 15 \equiv 1 \pmod{7}$. Using this, multiply the congruence by 3 to get $k \equiv 18 \equiv 4 \pmod{7}$. This means $k = 4 + 7j$ for some integer $j$, so $x = 3 + 5k = 3 + 5(4 + 7j) = 23 + 35j$. We now know that the solution to the system of two congruences $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$ is $x \equiv 23 \pmod{35}$. We now go to the third congruence, with $23 + 35j \equiv 3 \pmod{9}$. We reduce modulo 9 to get $5 + 8j \equiv 3 \pmod{9}$. The quickest way to solve this is to write $8 \equiv -1 \pmod{9}$ so $-j \equiv -2 \pmod{9}$ or $j \equiv 2 \pmod{9}$. Writing $j = 2 + 9m$ we have $x = 23 + 35(2 + 9m) = 93 + 315m$, so $x \equiv 93 \pmod{315}$, as before. I usually use this second method to solve congruences.

What happens if the $m$'s are not relatively prime? I will not give a full discussion but mention that there are a number of possibilities. First, the system of congruences might be inconsistent, with no $x$ simultaneously satisfying all the congruences. Second, the system might still be consistent, in which case the solutions $x$ will satisfy some congruences, but not modulo the product of the $m$'s. I almost always use the second method above on this problems. Here are some examples. First, consider

$$x \equiv 8 \pmod{12}$$
$$x \equiv 5 \pmod{9}$$
$$x \equiv 14 \pmod{15}.$$

We start with the first, writing $x = 8 + 12k$. Plugging into the second, $8 + 12k \equiv 5 \pmod{9} \rightarrow 3k \equiv -3 \pmod{9} \rightarrow k \equiv -1 \equiv 2 \pmod{3}$, or $k = 2 + 3j$ for some integer $j$. This means the solution to the first two congruences is $x = 8 + 12(2 + 3j) = 32 + 36j$, or $x \equiv 32 \pmod{36}$. Note that 36 is smaller than the product $12 \times 9 = 108$. This is because 12 and 9 are not relatively prime. Next, we plug into the third congruence: $32 + 36j \equiv 14 \pmod{15} \rightarrow 2 + 6j \equiv 14 \pmod{15} \rightarrow 6j \equiv 12 \pmod{15} \rightarrow j \equiv 2 \pmod{5}$, where Theorem 1 of this set of notes has been invoked. Now $j = 2 + 5m$ for some integer $m$, so $x = 32 + 36(2 + 5m) = 108 + 180m$, meaning that $x = 108$ is a solution, and solutions are unique modulo 180 (rather than $12 \times 9 \times 15 = 1620$.)

As a second example, consider

$$x \equiv 8 \pmod{12}$$
$$x \equiv 5 \pmod{9}$$
$$x \equiv 13 \pmod{15}$$

where all that changed was the last congruence. We still have $x = 32 + 36j$ from the first two. Now, however, when we plug into the third, $32 + 36j \equiv 13 \pmod{15} \rightarrow 6j \equiv 11 \pmod{15}$, and this has no solution since gcd$(6, 15) = 3$, which is not a divisor of 11. This means that this particular system of congruences is inconsistent.

I will mention a second approach to these two problems: The Chinese Remainder Theorem can be used in two different directions: two congruences can be combined into a single
congruence, but also, a single congruence can be split into two congruences. That is, if $x \equiv a \pmod{mn}$ where $m$ and $n$ are relatively prime, then $x \equiv a \pmod{m}$ and $x \equiv a \pmod{n}$. So we could take a system like

$$
\begin{align*}
  x &\equiv 8 \pmod{12} \\
  x &\equiv 5 \pmod{9} \\
  x &\equiv 14 \pmod{15}.
\end{align*}
$$

and break it into a larger system, using $12 = 3 \times 4$, $15 = 3 \times 5$:

$$
\begin{align*}
  x &\equiv 8 \pmod{3} \\
  x &\equiv 8 \pmod{4} \\
  x &\equiv 5 \pmod{9} \\
  x &\equiv 14 \pmod{3} \\
  x &\equiv 14 \pmod{5}
\end{align*} \quad \rightarrow \quad
\begin{align*}
  x &\equiv 2 \pmod{3} \\
  x &\equiv 0 \pmod{4} \\
  x &\equiv 5 \pmod{9} \\
  x &\equiv 2 \pmod{3} \\
  x &\equiv 4 \pmod{5}
\end{align*}
$$

We see here that the second $x \equiv 2 \pmod{3}$ is redundant. Moreover, we have to be careful about things like $x \equiv 2 \pmod{3}$ and $x \equiv 5 \pmod{9}$. It turns out that these congruences are consistent with each other, with $x \equiv 5 \pmod{9}$ being more restrictive. That is, if $x \equiv 2 \pmod{3}$ then $x \equiv 2$ or 5 or 8 $\pmod{9}$. This means that the first $x \equiv 2 \pmod{3}$ is also redundant, so our system is equivalent to

$$
\begin{align*}
  x &\equiv 0 \pmod{4} \\
  x &\equiv 5 \pmod{9} \\
  x &\equiv 4 \pmod{5},
\end{align*}
$$

and we have reduced to the case of relatively prime moduli. Again, this tells us that there is a unique solution modulo 180, the product of 4, 9, and 5. On the other hand, in the second example, we would have had

$$
\begin{align*}
  x &\equiv 8 \pmod{3} \\
  x &\equiv 8 \pmod{4} \\
  x &\equiv 5 \pmod{9} \\
  x &\equiv 13 \pmod{3} \\
  x &\equiv 13 \pmod{5}
\end{align*} \quad \rightarrow \quad
\begin{align*}
  x &\equiv 2 \pmod{3} \\
  x &\equiv 0 \pmod{4} \\
  x &\equiv 5 \pmod{9} \\
  x &\equiv 1 \pmod{3} \\
  x &\equiv 3 \pmod{5}
\end{align*}
$$

and here we have an inconsistency: we need $x \equiv 2 \pmod{3}$ and $x \equiv 1 \pmod{3}$, and certainly $x$ can’t be both at once. If we had kept $x \equiv 14 \pmod{15}$ but changed the middle congruence to, say, $x \equiv 7 \pmod{9}$, then we would still have had problems because $x \equiv 2 \pmod{3}$ is inconsistent with $x \equiv 7 \pmod{9}$. A final comment on these types of problems: If the moduli are not relatively prime but the system is constant, then there will be a unique solution modulo the least common multiple of the moduli (instead of their product).
A formula for Euler’s phi-function

I will close this set of notes with an application of the Chinese Remainder Theorem to Euler’s phi-function. The goal is to find an easy way to calculate \( \phi(p^n) \). It turns out that there is no easy way for large \( n \) as \( \phi(n) \) depends on how \( n \) factors. If factoring \( n \) is difficult, then calculating \( \phi(p^n) \) is also hard. However, in the case where factoring \( n \) is relatively easy, we can say a lot.

Lemma 1 If \( \gcd(m,n) = 1 \) then \( \phi(mn) = \phi(m)\phi(n) \).

Proof: This will be a consequence of the Chinese Remainder Theorem. First, note that there is a one-to-one correspondence between \( x \) with \( 0 \leq x \leq mn - 1 \) and ordered pairs \((a,b)\) with \( 0 \leq a \leq m - 1 \) and \( 0 \leq b \leq n - 1 \). That is, given any such \( x \), we can pick \( a \) and \( b \) by letting \( a \equiv x \pmod{m} \) and \( b \equiv x \pmod{n} \). It is the Chinese Remainder Theorem that says we can go backwards: given \( a,b \), there must be a corresponding \( x \). And of course, there are \( mn \) possible values of \( x \) and \( mn \) possible ordered pairs \((a,b)\).

What happens when we make things relatively prime? That is, there are \( \phi(mn) \) values of \( x \) with \( 0 \leq x \leq mn - 1 \) and \( \gcd(x,mn) = 1 \). There are \( \phi(m)\phi(n) \) ordered pairs \((a,b)\) satisfying \( 0 \leq a \leq m - 1 \), \( 0 \leq b \leq n - 1 \), \( \gcd(a,m) = 1 \) and \( \gcd(b,n) = 1 \). How do these \((a,b)\) relate to \( x \)? Again, given an \( x \), we can pick \( a \) and \( b \) using \( a \equiv x \pmod{m} \) and \( b \equiv x \pmod{n} \). If \( \gcd(x,mn) = 1 \) then \( \gcd(a,m) = 1 \) and \( \gcd(b,n) = 1 \). (Can you prove this?) This tells us that each relatively prime \( x \) gives us a relatively prime pair \((a,b)\), so \( \phi(mn) \leq \phi(m)\phi(n) \). Similarly, for any \( a \) and \( b \) with \( 0 \leq a \leq m - 1 \) and \( 0 \leq b \leq n - 1 \), we can use the Chinese Remainder Theorem to find an \( x \) with \( 0 \leq x \leq mn - 1 \) and \( x \equiv a \pmod{m} \), \( x \equiv b \pmod{n} \). Moreover, if \( \gcd(m,a) = 1 \) and \( \gcd(n,b) = 1 \), it follows that \( \gcd(mn,x) = 1 \). (Again, can you show this?) This gives us the other inequality, \( \phi(mn) \geq \phi(m)\phi(n) \), so these two expressions must be equal.

As an example of the proof, suppose that \( m = 3 \), \( n = 5 \). We have the following correspondences

\[
\begin{array}{c|c|c|c|c|c}
\text{\( x \)} & \text{\((a,b)\)} & \text{\( x \)} & \text{\((a,b)\)} & \text{\( x \)} & \text{\((a,b)\)} \\
\hline
1 & (1, 1) & 2 & (2, 2) & 4 & (1, 4) \\
8 & (2, 3) & 11 & (2, 1) & 13 & (1, 3) \\
14 & (2, 4) & \\
\end{array}
\]

or

\[
\begin{array}{c|c|c|c|c|c}
\text{\((a,b)\)} & \text{\( x \)} & \text{\((a,b)\)} & \text{\( x \)} & \text{\((a,b)\)} & \text{\( x \)} \\
\hline
(1, 1) & 1 & (1, 2) & 7 & (1, 3) & 13 \\
(2, 1) & 11 & (2, 2) & 2 & (2, 3) & 8 \\
& & & & & 14 \\
\end{array}
\]
We are now in a position to give a formula for $\phi(n)$. First, a special case.

**Lemma 2** If $p$ is a prime, then $\phi(p^n) = p^{n-1}(p - 1)$.

**Proof:** This was a homework exercise.

Given any $n$, we can factor it into primes, and use Lemma 1 and Lemma 2 to find $\phi(n)$. For example, if $n = 360 = 2^3 \times 3^2 \times 5$ then

$$
\phi(360) = \phi(2^3) \phi(3^2) \phi(5) = 2^2 (2 - 1) 3^1 (3 - 1) (5 - 1) = 96.
$$

Summarizing,

**Theorem 3** If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then $\phi(n) = p_1^{a_1 - 1} (p_1 - 1) p_2^{a_2 - 1} (p_2 - 1) \cdots p_k^{a_k - 1} (p_k - 1)$.

Usually, we write this a bit more compactly. Note that $p - 1 = p(1 - \frac{1}{p})$, and $p^{a-1}(p - 1) = p^a(1 - \frac{1}{p})$. If we do this with each term in the formula, then the product of the prime powers is $n$ again, so we get $\phi(n) = n \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_k} \right)$. So, for example, $\phi(360) = 360 \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{1}{3} \right) \left( 1 - \frac{1}{5} \right) = 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96$. For easy calculations, this is the way I usually calculate $\phi(n)$. More tersely, this formula for $\phi(n)$ is usually expressed as follows:

$$
\phi(n) = n \prod_{p|n} \left( 1 - \frac{1}{p} \right).
$$