Math 5330 Notes
Spring 2009 Number 6 in the series

The Chinese Remainder Theorem

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 $ax \equiv b \pmod{m}$, where the solution is again a congruence. That is, if x_0 is a number such that $ax_0 \equiv b \pmod{m}$, then x_0 has the property that $ax_0 - b$ is divisible by m. In this case $x_0 + km$ also has that property for any k, so we might say $x \equiv x_0 \pmod{m}$ is a solution. Actually, a little more could be true, as the following theorem shows.

Theorem. 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 $d = (a, m)$, 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 such that $x \equiv x_0 \pmod{m/d}$.

Proof. The congruence $ax \equiv b \pmod{m}$ has a solution if and only if there are integers x and k such that $ax - b = km$. Letting $y = -k$, this can be rewritten

$$ax + my = b.$$

From a previous set of notes, we know that this equation has a solution if and only if $(a, m) \mid b$. Moreover, if it has a solution (x_0, y_0), then the set of all solutions is $\left\{\left(x_0 + k\frac{m}{d}, y_0 - k\frac{a}{d}\right) \mid k \text{ is an integer.}\right\}$ That is, the solution x is determined modulo multiples of $\frac{m}{d}$, which is what was to be shown.

Thus, we know how to solve the congruence $ax \equiv b \pmod{m}$, we can use the Euclidean Algorithm. For example, suppose we wish to solve $15x \equiv 28 \pmod{103}$. We, instead, solve the equation $15x + 103y = 28$. Since 15 and 103 are relatively prime, we first solve $15x + 103y = 1$: $103 = 6 \cdot 15 + 13$, $15 = 1 \cdot 13 + 2$, $13 = 6 \cdot 2 + 1$. Backtracking, $1 = 13 - 6 \cdot 2 = 13 - 6(15 - 13)$, so $1 = 7 \cdot 13 - 6 \cdot 15 = 7(103 - 6 \cdot 15) - 6 \cdot 15$, giving $1 = 7 \cdot 103 - 48 \cdot 15$. As a consequence of this, -48 is a solution to the congruence $15x \equiv 1 \pmod{103}$. If we like positive solutions, then $103 - 48 = 55$ is also a solution. Finally, to get a solution to $15x \equiv 28 \pmod{103}$, we let $x \equiv 28 \cdot 55 \pmod{103}$, so, for example, $x = 98$ works, and the general solution is $\{98 + 103k\}$.

Suppose, for some reason, we wish to solve the congruence $23x \equiv 15 \pmod{70}$, and we don't want our numbers to get too big. Here is one possible approach: Since $23x - 15$ is divisible by 70, it must be divisible by both 10 and 7. So we look at these two problems separately: $23x \equiv 15 \pmod 7$ is equivalent to $2x \equiv 1 \pmod 7$, which has the solution $x \equiv 4 \pmod 7$. $23x \equiv 15 \pmod{10}$ can be converted to $3x \equiv 5 \pmod{10}$, for which we can spot a solution $x \equiv 5 \pmod{10}$. Thus, we need an x with the property that $x \equiv 4 \pmod 7$ and $x \equiv 5 \pmod{10}$. One possible approach to finding such an x is to take the two arithmetic progressions and look for their intersection. In this case, $x \equiv 4 \pmod 7$ has solutions among positive x: 4, 11, 18, 25, 32, 39, 46, $\cdots$ while $x \equiv 5 \pmod{10}$ has 5, 15, 25, 35, 45, $\cdots$. Comparing, we find $x = 25$. We can check that $x = 25$ is, in fact, a solution to the congruence $23x \equiv 15 \pmod{70}$.

It is conceivable that putting congruences together as above might come in handy. If so, it would be nice to have a systematic method for doing such. The theorem below, the Chinese Remainder Theorem, does this. It gets its name from the fact that the earliest references to the problem come from China. The oldest known problem in this area appears in the writings of Sun Tsu, who posed the problem of finding a number which when divided by 3 leaves a remainder of 2, when divided by 5 leaves a remainder of 3, and when divided by 7 has a remainder of 2. In our notation, this is asking for a solution to the system of congruences:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7.$$

Theorem (The Chinese Remainder Theorem) Let $m_1, m_2, \cdots, m_k$ be pairwise relatively prime positive integers. (That is, no m has any factors in common with any other m.) Let $a_1, a_2, \cdots, a_k$ be arbitrary integers. Then there exists an integer x such that

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_k \pmod{m_k}.$$

Moreover, if $M = m_1 m_2 \cdots m_k$, then x is unique modulo M.

Proof. We will actually give a way of constructing the solution x. For each i, let

$M_i = (M/m_i)^{\varphi(m_i)}$. By Euler's theorem, $M_i \equiv 1 \pmod{m_i}$. Moreover, if $j \neq i$, then $M_i \equiv 0 \pmod{m_j}$. The solution is now $x = a_1M_1 + a_2M_2 + \cdots + a_kM_k$.

To see that x is unique (mod M), suppose that y is also a solution. Then for each i, $x \equiv y \pmod{m_i}$. This means that $m_i \mid (x - y)$. Since this is true for each m_i and since the m_i are pairwise relatively prime, it follows that $M \mid (x - y)$, so $x \equiv y \pmod{M}$. This concludes the proof.

If we now attempt to solve Sun Tsu's problem, we may proceed as follows: since $\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(7) = 6$, we let $M_1 = (5\cdot7)^2$, $M_2 = (3\cdot7)^4$, and $M_3 = (3\cdot5)^6$, and set $x = 2M_1 + 3M_2 + 2M_3 = 2\cdot1225 + 3\cdot944{,}481 + 2\cdot11{,}390{,}625 = 23{,}367{,}143$. Obviously, a drawback to this method is that it produces large solutions. One way to keep the calculations smaller is to do the calculations module $M = m_1m_2\cdots m_n$, since the solution is only determined up to congruence module M anyway. In this case, we can let $M_1, \cdots, M_n$ be their least residues module M. For the preceding problem, M = 105, $M_1 = 70$, $M_2 = 21$, $M_3 = 15$, and $x = 2\cdot70 + 3\cdot21 + 2\cdot15 = 233$. Finally, we may take the least residue of x module M, in this case, $x \equiv 23 \pmod{105}$. The solution x = 23 is what Sun Tsu gave as the answer.

As a second example, suppose $m_1 = 5$, $m_2 = 7$, $m_3 = 9$. Then $\varphi(5) = 4$, $\varphi(7) = 6$, $\varphi(9) = 6$, so $M_1 = 63^4$, $M_2 = 45^6$, $M_3 = 35^6$. We can actually restrict the M's to be numbers mod $M = 315$, 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, $x = 3\cdot126 + 2\cdot225 + 3\cdot280 = 1668 \equiv 93$ will work.

There is another approach to solving systems of congruences. Again, suppose we wish to solve $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$, $x \equiv 3 \pmod 9$. We proceed as follows: If $x \equiv 3 \pmod 5$, then $x = 3 + 5k$ for some k. Now $3 + 5k \equiv 2 \pmod 7$. We try to solve this for k: $3 + 5k \equiv 2 \pmod 7 \rightarrow 5k \equiv 6 \pmod 7$. Since $3\cdot5 = 15 \equiv 1 \pmod 7$, if we multiply both sides by 3, we have $k \equiv 18 \equiv 4 \pmod 7$. This means that $x = 3 + 5\cdot(4 + 7j) = 23 + 35j$ is the solution to both $x \equiv 3 \pmod 5$ and $x \equiv 2 \pmod 7$. We now seek j so that $23 + 35j \equiv 3 \pmod 9$. Reducing everything modulo 9 gives $5 + 8j \equiv 3 \pmod 9$ or $8j \equiv 7 \pmod 9$. Since $8 \equiv -1 \pmod 9$, we have $-j \equiv 7 \pmod 9$, or $j \equiv -7 \equiv 2 \pmod 9$. So $x = 23 + 35\cdot(2 + 9k) = 93 + 315k$ is the general solution to

the system. Suppose we use the same method, but with a slight bit more insight: The order of the congruences does not matter, so solve $x \equiv 3 \pmod 5$, $x \equiv 3 \pmod 9$, $x \equiv 2 \pmod 7$. The point is that the first two can be solved instantly: $x \equiv 3 \pmod{45}$. (If we want $5 \mid x - 3$ and $9 \mid x - 3$, then we need $45 \mid x - 3$.) We now combine this with the last congruence as before: $x = 3 + 45k$, so we want $3 + 45k \equiv 2 \pmod 7$, or $3k \equiv 6 \pmod 7$. Obviously, we need $k \equiv 2 \pmod 7$ and get solution $x = 3 + 45(2 + 7j)$, or $x = 93 + 315j$, or just $x \equiv 93 \pmod{315}$.

The second approach to solving Chinese Remainder problems works because the a's that arise in solving $ax \equiv b \pmod m$ are always products of some of the m's, and these are always relatively prime to the other m's. I won't give a full discussion of what happens if some of the m's are not relatively prime. I will, however, give an example. Suppose we wish to solve the systems

$$\left.\begin{aligned} x &\equiv 8 \pmod{12}, \\ x &\equiv 5 \pmod 9, \\ x &\equiv 14 \pmod{15}. \end{aligned}\right\} \quad \text{and} \quad \left.\begin{aligned} x &\equiv 4 \pmod{12}, \\ x &\equiv 5 \pmod 9, \\ x &\equiv 13 \pmod{15}. \end{aligned}\right\}.$$

We factor the moduli into primes or prime powers. For example, $12 = 3 \cdot 4$, $9 = 9$, $15 = 3 \cdot 5$. Next, by the Chinese Remainder Theorem, $x \equiv a \pmod{mn}$ has the same solution as the system $x \equiv a \pmod m$, $x \equiv a \pmod n$ if m and n are relatively prime, so we can expand the systems into:

$$\left.\begin{aligned} x &\equiv 8 \pmod 3, \\ x &\equiv 8 \pmod 4, \\ x &\equiv 5 \pmod 9, \\ x &\equiv 14 \pmod 3, \\ x &\equiv 14 \pmod 5. \end{aligned}\right\} \quad \text{and} \quad \left.\begin{aligned} x &\equiv 4 \pmod 3, \\ x &\equiv 4 \pmod 4, \\ x &\equiv 5 \pmod 9, \\ x &\equiv 13 \pmod 3, \\ x &\equiv 13 \pmod 5. \end{aligned}\right\}$$

If we reorder the congruences and reduce to least residues, we get

$$\left.\begin{aligned} x &\equiv 2 \pmod 3, \\ x &\equiv 2 \pmod 3, \\ x &\equiv 0 \pmod 4, \\ x &\equiv 4 \pmod 5, \\ x &\equiv 5 \pmod 9. \end{aligned}\right\} \quad \text{and} \quad \left.\begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv 1 \pmod 3, \\ x &\equiv 0 \pmod 4, \\ x &\equiv 3 \pmod 5, \\ x &\equiv 5 \pmod 9. \end{aligned}\right\}$$

Next, we look for inconsistencies. The only real problem here would be with the 3's and the 9. In each case, the 3's are fine. If one equation in a system had been $x \equiv 1 \pmod 3$ and another had been $x \equiv 2 \pmod 3$, we would have had an inconsistent system. Next, we look at 3 vs 9. In particular, if $x \equiv 5 \pmod 9$, then it must also be congruent to 5 (mod 3). Since $5 \equiv 2 \pmod 3$, the first system is consistent. However, the second will be inconsistent. Finally, in solving the first system, we may delete any redundant congruences. In this case, both 3's are redundant (covered by the congruence mod 9) so we solve the system

$$\left.\begin{aligned} x &\equiv 0 \pmod 4, \\ x &\equiv 4 \pmod 5, \\ x &\equiv 5 \pmod 9. \end{aligned}\right\}$$

We have: $x = 4i$ from the first congruence, $4i \equiv 4 \pmod 5 \Rightarrow i \equiv 1 \pmod 5$, so $i = 1 + 5j$, $x = 4(1 + 5j) = 4 + 20j \equiv 5 \pmod 9 \Rightarrow 2j \equiv 1 \pmod 9 \Rightarrow j \equiv 5 \pmod 9$. Thus, $j = 5 + 9k$, and our solution will be $x = 4 + 20(5 + 9k) = 104 + 180k$. Note that the solution is a congruence modulo 180 = LCM(12, 9, 15).

Back to Euler's φ-function. We seek an easy way to calculate $\varphi(n)$. It turns out that there is no easy way for large n: $\varphi(n)$ depends on how n factors; if factoring n is a problem, so is finding $\varphi(n)$. We can say some things, however.

Lemma. If $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof: Given any a with $1 \le a \le mn - 1$, let $x \equiv a \pmod m$ and $y \equiv a \pmod n$, where $0 \le x \le m - 1$ and $0 \le y \le n - 1$. If $(a, mn) = 1$, then $(a, m) = 1$ and $(a, n) = 1$ (why?) From this, it follows that $(x, m) = 1$ and $(y, n) = 1$. Similarly, for any x and y with $0 \le x \le m - 1$ and $0 \le y \le n - 1$, we can use the Chinese Remainder Theorem to find an a with $0 \le a \le mn - 1$ and $a \equiv x \pmod m$, $a \equiv y \pmod n$. Moreover, if $(m, x) = 1$ and $(n, y) = 1$, it follows that $(mn, a) = 1$. This means that to every a which is relatively prime to mn, there is a unique pair (x, y) with x relatively prime to m and y relatively prime to n. A counting argument now gives $\varphi(mn)$ = number of a = number of ordered pairs (x, y) = $\varphi(m)\varphi(n)$.

As an example of the proof, suppose $m = 3$, $n = 5$. We have the following correspondences:

a	(x, y)	a	(x, y)
1	(1, 1)	8	(2, 3)
2	(2, 2)	11	(2, 1)
4	(1, 4)	13	(1, 3)
7	(1, 2)	14	(2, 4)

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

Proof: Homework exercise.

With this, we can now give a formula for $\varphi(n)$, provided we know the prime factorization of n.

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

Proof: This is a simple application of the two previous lemmas.

Usually, the formula for $\varphi(n)$ is written slightly differently: Since $p-1 = p\left(1- \frac{1}{p}\right)$, we can write $p^{n-1}(p - 1)$ as $p^n\left(1 - \frac{1}{p}\right)$. If we do this with each term of the formula, then the product of the prime powers is n, so $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right)$. For example, $\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 50 \cdot \frac{4}{5} = 40$. This is how I usually calculate $\varphi(n)$ as opposed to the alternative:

$\varphi(100) = \varphi(2^2 5^2) = 2(2-1)5(5-1) = 2\cdot 5\cdot 4 = 40.$