Math 126 Number Theory

Prof. D. Joyce, Clark University

24 Feb 2006

Return first test.

Due Wednesday. Asmt. 8, , from page 76, exercises 1–3, 7–9, 11–13, 17, 20.

Due next Friday. Asmt. 9, from page 82, exercises 1, 2, 4, 10; and from page 86, exercises 1, 2, 6, 7

For next time. We'll discuss Euler's phi function (also called Euler's totient function). This is discussed in section 3.4 and 3.5 in the text.

Today. Linear congruences and the Chinese remainder theorem.

Linear congruences. The easiest sort of congruence equation to solve is a linear congruence, one of the form

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

It's easy because we've really already solved it. Suppose we have a solution x. Since $ax \equiv b \pmod{n}$, therefore $n|ax-b$, so there is some number y such that $ny = ax - b$, in other words,

$$ax - ny = b.$$

That's just a linear equation in two unknowns, and we know how to find all it's solutions. Namely, let $d = (a, n)$. If $d \not| b$, then there are no solutions. Otherwise the Euclidean algorithm gives us one solution, and then we can find the rest.

Let's record this as a theorem, and supply the details in a proof.

Theorem. The congruence

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

has a solution if and only if $d|b$ where $d = (a, n)$. When $d|b$, then the solution is unique modulo n/d. Thus, if $(a, n) = 1$, the congruence $ax \equiv b \pmod{n}$ always has a unique solution.

Proof: As mentioned just above, the congruence $ax \equiv b \pmod{n}$ has a solution if and only if the equation $ax - ny = b$ has a solution. More precisely, if (x, y) is a solution to the equation, then x is a solution to the congruence. (Thus, a solution to the congruence is part of a solution to the equation.) The equation has a solution if and only if $d|b$, therefore the congruence has a solution if and only if $d|b$.

Let's suppose now that $d|b$. We've seen that every solution to the equation $ax - ny = b$ is of the form

$$x = x_0 + t(n/d), \quad y = y_0 + t(n/d)$$

where (x_0, y_0) is a particular solution (which we can find with the help of the Euclidean algorithm), and t is any integer. Therefore, every solution to the congruence $ax \equiv b \pmod{n}$ is of the form

$$x = x_0 + t(n/d).$$

But

$$x_0 + t(n/d) \equiv x_0 \pmod{n/d},$$

so the congruence has a unique solution modulo n/d. Q.E.D.

Simultaneous linear congruences with different moduli. We'll start this discussion with an example.

Solve the pair of linear congruences

$$\begin{cases} x \equiv 7 \pmod{10} \\ x \equiv 4 \pmod{11} \end{cases}$$

We could search for an answer. The congruence $x \equiv 7 \pmod{10}$ says that when x is written decimally, its last digit is 7. So, look among those numbers congruent to 4 modulo 11 for one whose last digit is 7.

$$4, 15, 26, 37 \text{ Aha!}$$

What other values besides $x = 37$ are solutions? If we go 10 more numbers past 37 in the list of numbers congruent to 4 modulo 11, then we'll find another, namely 147. In fact, any number congruent to 37 modulo 110 will be a solution.

Let's take this same pair of linear congruences and find a method we can use in general. To satisfy the congruence $x \equiv 4 \pmod{11}$, we need x to be of the form

$$x = 4 + 11t$$

for an arbitrary integer t. Put $4 + 11t$ in for x in the first congruence to get

$$4 + 11t \equiv 7 \pmod{10}$$

which simplifies to

$$t \equiv 3 \pmod{10}.$$

Thus, $t = 3 + 10u$ where u is an arbitrary integer. Thus, the general solution to the pair of congruences is

$$\begin{array}{rcl} t & = & 4 + 11t \\ & = & 4 + 11(3 + 10u) \\ & = & 37 + 110u \end{array}$$

That is, $x \equiv 37 \pmod{110}$.

The Chinese remainder theorem. We can extract a theorem from our work above. We'll get what's called the Chinese remainder theorem for a pair of congruences.

Chinese remainder theorem. If m and n are relatively prime, then the pair of linear congruences

$$\left\{ \begin{array}{rcll} x & \equiv & a & \pmod{m} \\ x & \equiv & b & \pmod{n} \end{array} \right.$$

has a unique solution modulo the product mn.

We'll work out the proof in class based on the example above. At one point we need to invoke the theorem we proved above about the uniqueness of solutions to a single linear congruence.

The Chinese remainder theorem can be interpreted as what is called an isomorphism of rings. In that interpretation $\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn}$ when m and n are relatively prime. This means that each pair (a, b) where $a \in \mathbf{Z}_m$ and $b \in \mathbf{Z}_n$ corresponds to a single element $c \in \mathbf{Z}_{mn}$, and furthermore (something that we haven't proved yet) the operations of addition, subtraction, and multiplication correspond. That goes a bit beyond a basic number theory course, but it indicates the importance of the Chinese remainder theorem in modern algebra.

The Chinese remainder theorem applies to more than just two simultaneous linear congruences. If you have k simultaneous linear congruences where the moduli are all relatively prime, then there is a unique solution modulo the product of those moduli.