Math 126 Number Theory

Prof. D. Joyce, Clark University

27 Feb 2006

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

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

Last time. Linear congruences and the Chinese remainder theorem. We proved two important theorems.

Theorem. The linear 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.

Chinese remainder theorem. If n_1, n_2, $\ldots n_k$ are k pairwise relatively prime numbers, then the system of k linear congruences

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad\vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

has a unique solution modulo the product $n_1 n_2 \ldots n_k$.

Next time. Pseudoprimes. Multiplicativity of Euler's ϕ function. Evaluating Euler's ϕ function.

Today. We'll discuss a couple more things from the section on congruences before going on to discuss Euler's phi function, also called Euler's totient function.

Interpretation of the Chinese remainder theorem as an isomorphism of rings. That's in the notes from last time, but we didn't have time to discuss it.

Systems of linear congruences with the same modulus. The Chinese remainder theorem deals with linear systems when the moduli are relatively prime. When the congruences have the same modulus n, it's easier to solve them. Since $\mathbf{Z}_k$ is a ring, you can use all the usual techniques you would use for simultaneous equations, so long as those techniques only involve addition, subtraction, and multiplication. You can also use division, but you have to be careful, that is, if you want to divide a congruence by a, make sure a is relatively prime to n.

For example, to simplify the congruence

$$6x + 10y \equiv -14 \pmod{3},$$

you can divide it by 2 since 2 is relatively prime to 3 and that yields the congruence

$$3x + 56 \equiv -7 \pmod{3}.$$

Sometimes you'll have to find the inverse of a modulo n before dividing. Suppose, for example, you wanted to divide the congruence

$$7x - 21y \equiv 8 \pmod{11}$$

by 7. You'll need to do something special because 7 doesn't easily divide 8, but it does modulo 11. A general method that works is to find the reciprocal of 7 modulo 11, that is, solve the equation $7x \equiv 1 \pmod{11}$. That gives $x = 8$ since 56 is one more than a multiple of 11. The above congruence becomes

$$x - 3y \equiv 8 \cdot 8 \equiv 9 \pmod{11}.$$

Even when you want to divide an equation by a not relatively prime to n, you can do that, but it will change the modulus. The first theorem quoted above from last meeting applies. For example, to simplify the congruence

$$28x - 14y \equiv 14 \pmod{35},$$

you would like to divide by $a = 14$, but 14 and $n = 35$ aren't relatively prime; their greatest common divisor is $d = 7$. The solution will be unique modulo $n/d = 5$, so after dividing by 14, we get the congruence

$$2x - y \equiv 2 \pmod{5}.$$

If that was just one of several congruences in a system, this change of modulus will make it more difficult to complete the solution because now not all the congruences have the same modulus.

Euler's phi function. This function is defined by setting $\phi(n)$ to the number of positive integers less than n which are relatively prime to n. It's called *Euler's ϕ function* or *Euler's totient function.* Euler didn't call it a totient function; he didn't even use the letter phi; Gauss introducted that notation. Apparently, it wasn't until 1879 that Sylvester called a positive integer smaller than n but relatively prime to n a totative, and since Euler's ϕ function counted totatives, it was called a totient function. Why Sylvester used the word totative is unclear. It seems to be made up from the Latin stem *tot* meaning "so many" and the ending -itive.

Anyway, these totatives are the elements of the ring $\mathbf{Z}_n$ that have reciprocals, and that's what makes them important.

As Stark does in the text, you don't have to represent $\mathbf{Z}_N$ by the standard complete residue system modulo n, namely the set $\{0, 1, \ldots, n-1\}$; you could use any complete residue system. And if you do that, then the elements that have reciprocals form what is called a *reduced residue system.* That's sort of clumsy to do, so we'll stick to $\{0, 1, \ldots, n-1\}$.

Examples. Let n=10. What are the positive integers less than 10 but relatively prime to 10, that is the totatives? They're 1, 3, 7, and 9. Therefore $\phi(10) = 4$. What are the reciprocals of these totatives modulo 10? We'll put them in a table.

k	1	3	7	9
k^{-1}	1	7	3	9

We'll work out a larger example in class.

Fermat's little theorem and Euler's theorem. Back in the 1640 Fermat noticed that when p is a prime, then $a^p \equiv a \pmod{p}$, and if $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$.

In 1760 Euler generalized this using his ϕ function. After the statement of Euler's theorem, we'll look at an example or two, prove it, then derive Fermat's little theorem from Euler's theorem.

Euler's Theorem: If a is relatively prime to n, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Example. Let $n = 10$. We can take any of the four totatives 1, 3, 7, or 9 for a. Let's take $a = 7$. Then Euler's theorem says $7^4 \equiv 1 \pmod{10}$. That's easy to verify since $7^2 \equiv -1 \pmod{10}$.

Proof of Euler's therem. Consider what multiplying by a modulo n does to the set of totatives

$$T = \{a_1, a_2, \ldots, a_{\phi(n)}\}.$$

Take one of the totatives a_i. Both a and a_i are relatively prime to n, therefore their product aa_i is also relatively prime to n, and when aa_i is reduced modulo n to a positive integer less than n, it's still relatively prime to n, and, therefore, another totative. Thus, multiplication by a is a function from the set of totatives to itself, $T \to T$. But a has an inverse modulo n, a^{-1}, and multiplication by a^{-1} is inverse to multiplication by a, so every totative a_j is of the form aa_i for exactly one i.

Now consider two products, the first product $a_1 a_2 \ldots a_{\phi(n)}$ being of all the totatives, and the second product of all the totatives multiplied by a, that is $(aa_1)(aa_2)\ldots(aa_{\phi(n)})$. These two products

have all the same terms since every totative a_j is aa_i for exactly one i. Therefore

$$a_1 a_2 \dots a_{\phi(n)} \equiv (aa_1)(aa_2)\dots(aa_{\phi(n)}) \pmod{n}.$$

We can divide this congruence by each totative a_i since it's relatively prime to n, and that gives us

$$1 \equiv a^{\phi(n)} \pmod{n}. \qquad \text{Q.E.D.}$$

Fermat's little theorem. If p is prime, then

$$a^p \equiv a \pmod{p}.$$

Furthermore, if $a \not\equiv 0 \pmod{p}$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(We'll prove this in class.)