Math 126 Number Theory

Prof. D. Joyce, Clark University

3 Mar 2006

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

Next time. Primitive roots, Section3.7.

Last time. Totatives and Euler's ϕ function.

Today. Fermat's little theorem and Euler's theorem. Pseudoprimes. Multiplicativity of Euler's ϕ function.

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.

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

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

Proof: 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

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

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

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

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.)

Pseudoprimes. Fermat's theorem says that if p is prime, then $a^p \equiv a \pmod{p}$. But do any other numbers have this property that aren't prime? Yes. We'll look at the case when $a = 2$ and call a nonprime integer n satisfying the condition

$$2^n \equiv 2 \pmod{n}$$

a *pseudoprime with respect to* 2 or more simply, just a pseudoprime. An example of a pseudoprime is $n = 341$.

Multiplicativity of Euler's ϕ function. We've seen two multiplicative functions already, $d(n)$ the number of divisors of n, and $\sigma(n)$ the sum of the divisors of n. We'll show that $\phi(n)$ is another multiplicative function. Recall the defintion of multiplicative function.

Definition. A function f defined on the natural numbers $\mathbf{N}$ is said to be *multiplicative* if $f(mn) = f(m)f(n)$ whenever m and n are relatively prime.

We won't formally prove that ϕ is multiplicative, but we'll look at an example that is sufficiently generic so that we could extract a proof from the example.

Once we know ϕ is multiplicative, it's fairly easy to evaluate $\phi(n)$ given a prime factorization of n. Suppose that prime factorization is

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Then

$$\phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k}).$$

So, to complete the evaluation of $\phi(n)$, all we have to know is how to evaluate ϕ at at prime power p^e. The positive integers less than p^e that are not relatively prime to p^e are

$$p, 2p, 3p, \ldots, (p^{e-1} - 1)p.$$

Since there are p^{e-1} of them not relatively prime to p^e, therefore there are $p^e - p^{e-1}$ that are relatively prime to p^e. Thus,

$$\phi(p^e) = p^e - p^{e-1}.$$

Example: Evaluate $\phi(100000)$. We're computing the number of positive integers less than a million relatively prime to a million.

$$\begin{aligned} \phi(1000000) &= \phi(2^6 5^6) = \phi(2^6)\phi(5^6) \\ &= (64 - 32)(15625 - 3125) \\ &= 400000 \end{aligned}$$