Math 126 Number Theory

Prof. D. Joyce, Clark University

13 Mar 2006

Due Friday. Asmt. 10. From page 106: 2, 4, 5, 9; and from page 108 Misc. exercises: 8, 15. Treat these last two as challenge problems. We'll have time on Wednesday for hints if you want them.

Next time. After we finish the discussion on primitive roots, we'll start on higher degree Diophantine equations in chapter 5. We've already completed the general theory of linear Diophantine equations. In chapter 5 we'll look at Pythagorean triples—mentioned in the introduction to the course—in more detail. We'll also consider the Fermat/Wiles theorem, at least the statement of it and some low degree cases of it, and discuss the Pell equation.

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

Today. Primitive roots.

The group of totatives. Recall that a totative modulo n is an element of $\mathbf{Z}_n$ relatively prime to n, that is, a number a less than or equal to n but relatively prime to n. We've seen that the number of totatives is the value of the Euler phi function, $\phi(n)$.

The set of totatives modulo n forms a mathematical structure called an Abelian group. An *Abelian group* is a set equipped with a binary operation, here denoted as multication, satisfying the following axioms

1. Associativity. $(ab)c = a(bc)$ for all elements a, b, and c.
2. Commutativity. $ab = ba$ for all elements a and b.
3. Identity. There is an element 1 such that $1a = a$ for all a.
4. Inverses. For each element a there is another element, denoted a^{-1} such that $aa^{-1} = 1$.

Although the axioms don't state it, the element 1 is unique. Also, each element a has a unique inverse. These two statements of uniqueness can be proved from the axioms, in fact, commutativity is not required. By the way, a *group* has the same axioms as an Abelian group except commutativity is not required.

The set of totatives modulo n is an Abelian group because (1) the product of two totatives is another so that the binary operation of multiplications is defined on the set of totatives, (2) multiplication is, of course, associative and commutative, (3) 1 is a totative, and (4) totatives have inverses modulo n.

The order of a totative. The *order* of an element a in a group is the smallest positive power of a that is the identity 1. Thus, the order of a totative a is the smallest positive b such that

$$a^b \equiv 1 \pmod{n}.$$

The order of a is denoted $\mathrm{ord}_n(a)$.

Example. Let's make a table of powers of totatives modulo $n = 20$ listing all the totatives a and their powers until some power becomes 1.

a	1	3	7	9	11	13	17	19
a^2		9	9	1	1	9	9	1
a^3		7	3			17	13	
a^4		1	1			1	1	
$\mathrm{ord}_n(a)$	1	4	4	2	2	4	4	2

Note that the orders of the 8 totatives are numbers which divide 8, but none of them happen to equal 8.

Example. Let's do another one when n is a prime number, say $n = 11$

k	1	2	3	4	5	6	7	8	9	10
k^2		4	9	5	3	3	5	9	4	1
k^3		8	5	9	4	7	2	6	3	
k^4		5	4	3	9	9	3	4	5	
k^5		10	1	1	1	10	10	10	1	
k^6		9				5	4	3		
k^7		7				8	6	2		
k^8		3				4	9	5		
k^9		6				2	8	7		
k^{10}		1				1	1	1		
$\mathrm{ord}_n(k)$	1	10	5	5	5	10	10	10	5	2

Note that the orders of the 10 totatives are numbers which divide 10, and some of them do happen to equal 10. We'll call those primitive roots.

Primitive roots. A *primitive root* modulo n is a totative k whose order is $\phi(n)$, that is,

$$\mathrm{ord}_n(k) = \phi(n).$$

In the last two examples, we found that there were no primitive roots modulo 20, but there were four primitive roots modulo 11, namely, 2, 6, 7, and 8.

One nice thing about primitive roots is that every totative is a power of each primitive root. For instance, the powers of the primitive root 2 modulo 11 are the 10 totatives modulo 11.

In the next couple of theorems, we'll develop some properties of orders and primitive roots. Two important theorems are that the order of a totative always divides $\phi(n)$ and that there are always primitive roots modulo primes. The proofs of these theorems take time to develop, so we'll follow Stark's well-prepared presentation. Even so, we'll omit the proofs of the later theorems.

Since in these theorems there is a fixed value of n, let's omit the $\pmod n$ in all the congruences except in the statements of the theorems.

First, we'll need his theorem 3.25, a technical lemma that makes the rest of the proofs much easier.

Lemma. If two positive powers b and c of a totative a are congruent to 1 modulo n, then a raised to the greatest common divisor $d = (b, c)$ is also congruent to 1 modulo n. That is, modulo n,

$$a^b \equiv 1 \text{ and } a^c \equiv 1 \text{ imply } a^{(b,c)} \equiv 1.$$

Proof: Since d is the greatest common divisor of b and c, therefore d is a linear combination of them, that is,

$$d = rb + sc$$

for some integers r and s. Therefore,

$$a^d \equiv a^{rb+sc} \equiv (a^b)^r (a^c)^s \equiv 1^4 1^s \equiv 1.$$

Note that r or s may be negative, but a totative a has negative powers modulo n, and the usual laws of exponentiation are valid even if some of the exponents are negative. Q.E.D.

Theorem. The order, $\mathrm{ord}_n(a)$, of a totative a divides b if and only if $a^b \equiv 1 \pmod n$.

Proof $\Rightarrow$: It is always the case that $a^{\mathrm{ord}_n(a)} \equiv 1$, so if $\mathrm{ord}_n(a) | b$, say $c\ \mathrm{ord}_n(a) = b$, then

$$a^b \equiv a^{c\ \mathrm{ord}_n(a)} \equiv (a^{\mathrm{ord}_n(a)})^c \equiv 1^c \equiv 1.$$

Proof $\Leftarrow$: Suppose that $a^b \equiv 1 \pmod n$. Then since $a^{\mathrm{ord}_n(a)} \equiv 1$ also, therefore, by the lemma above, $a^d \equiv 1 \pmod n$ where $d = (b, \mathrm{ord}_n(a))$. But $\mathrm{ord}_n(a)$ is the smallest power to which a can be raised so that the result is congruent to 1 modulo n, therefore, $d = \mathrm{ord}_n(a)$. But that implies $\mathrm{ord}_n(a)$ divides b. Q.E.D.

Corollary. The order of a totative a divides $\phi(n)$.

Proof: Euler's theorem says $a^{\phi(n)} = 1$. So, by the previous theorem, $\mathrm{ord}_n(a) \mid \phi(n)$. Q.E.D.

This last corollary is a special case of what is called Lagrange's theorem in group theory. Lagrange's theorem says that the number of elements in a subgroup divides the number of elements in the entire group, called the *order* of the group. That

implies that the order of a element in a group divides the order of the group. Our particular group, the group of totatives modulo n, has $\phi(n)$ elements, so that theorem translates in our case to the corollary above.

The theorems so far apply to any positive integer n. Now, we'll specialize to the case where n is a prime, and we'll denote it p instead. We'll omit the proofs and treat the remainder of this section as a survey.

Theorem. The congruence

$$x^d \equiv 1 \pmod{p}$$

has exactly d solutions when d divides $p-1$ (and none when d doesn't divide $p-1$).

Example. Refer to the example above when $p = 11$. The divisors of $p - 1 = 10$ are 1, 2, 5, and 10. All 10 totatives, 1 through 10, satisfy the congruence

$$x^{10} \equiv 1 \pmod{11}.$$

That's just Fermat's theorem. There are five solutions to the congruence

$$x^5 \equiv 1 \pmod{11},$$

namely $x \equiv 1$, 3, 4, 5, and 9. There are two solutions to the congruence

$$x^2 \equiv 1 \pmod{11},$$

namely $x \equiv 1, 10$, or, more conventionally stated, $x = \pm 1$. And the only solution to the congruence $x^1 \equiv 1 \pmod{11}$ is, of course, $x \equiv 1$.

Theorem. If d divides $p-1$, then there are exactly $\phi(d)$ totatives whose order is d. In particular, there are exactly $\phi(p-1)$ primitive roots of p.

Example. Take $p = 11$. There is $\phi(1) = 1$ totative of order 1, namely 1. There is $\phi(2) = 1$ totative of order 2, namely 10 (that is, -1). There are $\phi(5) = 4$ totatives of order 5, namely 3, 4, 5, and 9. Finally, there are $\phi(10) = 4$ totatives of order 10, namely 2, 6, 7, and 8. Those are the primitive roots modulo 11.