

## MATH 465 NUMBER THEORY, SPRING 2009, PROBLEMS 10

### Primitive roots

*Return by Monday 30th March*

1. Let  $p$  be an odd prime, suppose  $p \nmid a$ , and let  $n$  be the exponent to which  $a$  belongs modulo  $p$ . Prove that if  $n > 1$ , then

$$a + a^2 + \cdots + a^{n-1} \equiv -1 \pmod{p}.$$

2. (i) Find the exponents to which 2, 3 and 5 belong modulo 23.

(ii) Find a primitive root modulo 23, construct a table of indices, and solve the congruence  $x^6 \equiv 4 \pmod{23}$ .

3. Show that  $1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$  when  $p-1 \nmid k$  and is  $\equiv -1 \pmod{p}$  when  $p-1 \mid k$ .

4. Find all the primitive roots of 7, 14, 49.

### The following questions are for amusement, not for credit

A. The numbers  $F_n = 2^{2^n} + 1$  are called Fermat numbers.  $F_0$  through  $F_4$  are prime. Fermat had conjectured that  $F_n$  is always prime. Show that  $641 \mid F_5$ . We now know that  $F_5, \dots, F_{19}$  are composite and it is now conjectured that there are no further Fermat primes!

Suppose that  $p$  is a prime with  $p \mid F_n$ . Let  $e$  denote the smallest positive integer such that  $2^e \equiv 1 \pmod{p}$ .

(i) Show that  $e$  exists and  $e \mid 2^{n+1}$ .

(ii) Show that  $e \nmid 2^n$ .

(iii) Show that  $p \equiv 1 \pmod{2^{n+1}}$ .

B. Show that every integer satisfies at least one of the following congruences;  $x \equiv 0 \pmod{2}$ ,  $x \equiv 0 \pmod{3}$ ,  $x \equiv 1 \pmod{4}$ ,  $x \equiv 1 \pmod{6}$ ,  $x \equiv 3 \pmod{8}$ ,  $x \equiv 11 \pmod{12}$ . Such a collection of congruences (with the moduli all different) is known as a covering class. Paul Erdős asked whether there are covering classes with all the moduli arbitrarily large. It is still an open question. There is a prize worth probably several thousand dollars for its solution.

C. Show that if  $n = 4^h(8k+7)$  for some non-negative integers  $h$  and  $k$ , then  $n = x^2 + y^2 + z^2$  is insoluble in integers  $x, y, z$ . If  $n$  is not of this form, then it can be shown that this equation is soluble. Legendre thought he had a proof, but Gauss pointed out a gap and provided the first complete proof.