

### 3.1 Homework Four

These homework problems are due March 12.

1. Use the “repeated squaring algorithm” to apply the strong pseudoprime test (base 2) to the numbers 37813 and 48149. You will need to use your calculator or a program like Maple, but you should show the steps involved in the calculation. You may use a program (calculator or Maple) but you should supply the code in your solution.
2. Find the number of solutions to the equation  $a^{N-1} \equiv 1 \pmod{N}$ , when  $N = 3465$ .
3. Let  $f(x)$  be a polynomial in  $x$ , with integer coefficients. Let  $N_f(m)$  be the number of solutions to the equation  $f(x) \equiv 0 \pmod{m}$ . Prove that  $N_f(m)$  is a multiplicative function.
4. Suppose that  $N$  is a Carmichael number, so that  $a^{N-1} \equiv 1 \pmod{N}$  for all  $a$  relatively prime to  $N$ . Prove that  $a^N \equiv a \pmod{N}$  for all  $a$ , even those with a factor in common with  $N$ .
5. Prove that a Carmichael number must be squarefree.
6. (a) Fix a prime  $p$ . Let  $f(p)$  be the order of 2 mod  $p$ . Show that, if  $q$  is a prime different from  $p$ , then  $pq$  is a pseudoprime base 2 if and only if  $q \equiv 1 \pmod{f(p)}$  and  $q$  divides  $2^{p-1} - 1$ . Using this, show that, for fixed  $p$ , there are only finitely many  $q$  such that  $pq$  is a Fermat pseudoprime base 2.
  - (b) Show that if  $p=2,3,5,7$  there is no  $q$  such that  $pq$  is a pseudoprime. Show that, for  $p=11$ ,  $pq$  is a pseudoprime only if  $q=31$ . What happens for  $p=13$ ?  $p=17$ ?

**Extra Credit** What about products of three primes? See [6] for a generalization of this type of process for generating a list of all Fermat pseudoprimes.