

## HW6

This is due Monday, March 31

1. (a) Let  $m = 1111$ . Show that  $m$  is composite using Fermat theorem.  
(b) Do the same for  $m = 1111111111$ .
2. Show that 2047 is composite by applying the strong pseudoprime test.
3. Show that if  $m$  is pseudoprime but not strong pseudoprime, then the strong pseudoprime test in conjunction with the Euclidean algorithm provide an efficient means of locating a proper divisor  $d$  of  $m$ .
4. Use the Pollard rho method to locate proper divisors of the following numbers: 8131, 10277 and 199934971.
5. Show that if  $(a, m) = 1$  and  $m$  has a prime factor  $p$  such that  $(p - 1) | Q$ , then  $(a^Q - 1, m) > 1$ .