Math 115 - Midterm 2

July 28, 2010

Answer one of 1a and 1b, one of 2a and 2b, 3, and one of 4a and 4b.

1a. Suppose p is a prime of the form $7k+1$ and suppose a is an integer not divisible by p. Show that a is a seventh power modulo p if and only if $a^{(p-1)/7} \equiv 1 \mod p$.

1b. Determine the number of solutions to the congruence $x^7 \equiv 17 \mod 101$ (note: 101 is prime).

2a. The integer $p = 2^{31} - 1$ is prime. Compute $35^{(p-1)/2} \mod p$.

2b. Determine if 35 is a square modulo $18871 = 113 \cdot 167$ (note: 113 and 167 are prime).

3. Determine if there is a positive integer k such $a^{5k} \equiv a \mod 91$ for all integers a which are not divisible by 7 or 13. If such a k exists, find it. (note: $91 = 7 \cdot 13$)

4a. Here is a table of powers of 53 modulo $n = 375871$.

k	1	2	3	4	5	6
$53^k \mod n$	53	2809	148877	373061	226941	1

Use this table to find a proper factor of n. You may leave your answer in the form of a gcd so long as you prove that the gcd is indeed a proper factor (i.e. is not equal to 1 or n).

4b. The integer $n = 375871$ is a product of two primes p and q. The order of 36 modulo n is $51 = 3 \cdot 17$. The order of 36 modulo p is strictly smaller than 51. Explain how you can use this information to quickly find p.