18.781 Problem Set 4 part 2

Thursday March 15, with the rest of Problem Set 4.

Collaboration is allowed and encouraged. However, your writeups should be your own, and you must note on the front the names of the students you worked with.

Extensions will only be given for extenuating circumstances.

1. (a) Find a primitive root modulo 23 and modulo 23^3.

   (b) Show that $3^8 \equiv -1 \pmod{17}$. Explain why this implies 3 is a primitive root mod 17.

2. Let m and n be positive integers, with m odd. Show that $(2^m - 1, 2^n + 1) = 1$.

3. Show that if $a^k + 1$ is prime and $a > 1$ then k is a power of 2. Show that if $p | (a^{2^n} + 1)$ then $p = 2$ or $p \equiv 1 \pmod{2^{n+1}}$.

4. Let a and $n > 1$ be any integers such that $a^{n-1} \equiv 1 \pmod{n}$, but $a^d \not\equiv 1 \pmod{n}$ for every proper divisor d of $n - 1$. Prove that n is prime.

5. Show that the sequence $1^1, 2^2, 3^3, \ldots$ considered modulo p is periodic with smallest period $p(p-1)$.

6. Suppose $(10a, q) = 1$, and that k is the order of $10 \pmod{q}$. Show that the decimal expansion of the rational number a/q is periodic with smallest period k.