Homework

due on Thursday, July 22

Read carefully Chapter 10 and the notes about order modulo m posted on the course web page. Solve the following problems:

Problem 1. Let $a > 1$, $n > 0$ be integers. Find the order of a modulo $a^n - 1$. Use it to show that $n|\phi(a^n - 1)$, where ϕ is the Euler's function.

Problem 2. Is there a prime number p such that each of the numbers $2, 3, 6$ is a primitive root modulo p? Justify your answer. Hint: Can an even power of a primitive root be a primitive root?

Problem 3. Let p be a prime and a an integer not divisible by p. Suppose that for every prime divisor q of $p - 1$ we have $a^{(p-1)/q} \not\equiv 1 \pmod{p}$. Prove that a is a primitive root modulo p.