Exercise Set 4:
Applications of the Integers Modulo n

Math 414, Winter 2010, University of Washington

Due Friday, February 5, 2010

1. Let a, m, n be random integers with about 10000 digits each. How long does it take Sage to compute $a^m \pmod{n}$? What if they have 100000 digits each? 1000000 digits each?

2. Let φ be the Euler phi function. For what values of n is $\varphi(n)$ even?

3. Explicitly find a primitive root modulo 49.

4. Prove that if $a, b \in (\mathbb{Z}/k\mathbb{Z})^*$ have multiplicative orders n, m, with $\gcd(n, m) = 1$, then ab has multiplicative order nm.

5. (*) Let p be an odd prime. Prove that there is a primitive root modulo p^2. (Hint: Use the result of the previous exercise.)

6. Is the number $n = 3^{2011} - 40$ prime? You may **not** directly use the `is_prime` function in Sage to solve this problem.