Dartmouth College
Mathematics 25

Assignment 7
due Friday, November 13

1. Set up public and private keys for an RSA system using the primes 17 and 23.

2. Show that 3 is a primitive root modulo 17^5.

3. How many primitive roots exist modulo 101^{10}? Express your answer as an integer or the product of integers.

4. Suppose that n is a positive integer with $a^h \equiv a^k \equiv 1 \pmod{n}$. Show that $a^g \equiv 1 \pmod{n}$ where $g = \gcd(h, k)$.

5. Let $n > 1$ be an integer, and suppose that

   (a) $a^{n-1} \equiv 1 \pmod{n}$, and

   (b) $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all primes $q \mid n - 1$.

   Show that n must be prime.

6. Let $a, b \in U_n$ have orders h and k respectively, and suppose that h and k are coprime. Show that ab has order hk.

7. Let $a, b \in U_n$.

   (a) Show that $\operatorname{ord}_n(ab) \mid \operatorname{lcm}(\operatorname{ord}_n a, \operatorname{ord}_n b)$.

   (b) Proof or counterexample: $\operatorname{ord}_n(ab) = \operatorname{lcm}(\operatorname{ord}_n a, \operatorname{ord}_n b)$.