MATH 445, HOMEWORK 6

Note: Although most of the problems on this homework assignment can be done easily by computer, I am asking you to do them by hand. The point of this assignment is to make sure you have understood and internalized the algorithms and methods involved in these computations.

1. Compute $\mathrm{GCD}(273, 1870)$ and $\mathrm{GCD}(1365, 4004)$.

2. Write $\mathrm{GCD}(273, 1870)$ in the form $273a + 1870b$ with a, b integers. Write $\mathrm{GCD}(1365, 4004)$ in the form $1365a + 4004b$ with a, b integers.

3. Verify that $\mathrm{GCD}(170, 1001) = 1$ and determine $170^{-1} \pmod{1001}$.

4. Compute $3^{784} \pmod{42943}$. (On this problem you should feel free to use a calculator to help with repeated squaring mod 42943.)

5. If $(a, n) = 1$, the *order* of a mod n is the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$. Prove that $d \mid \phi(n)$. (Hint: divide $\phi(n)$ by d.)