Homework 5
Due at the beginning of class on Nov. 15

When you are asked to compute a result “by hand”, you may use a calculator to perform multiplication/division but you may not use a special-purpose computer program.

1. The following exercises concern modular arithmetic. Answer them by hand:
   (a) Compute $[46^{-1} \mod 51]$, using the extended Euclidean algorithm.
   (b) Solve for $x$ in the following equation: $46x = 49 \mod 51$.
   (c) Compute gcd(45, 51) using the Euclidean algorithm. Does 45 have an inverse modulo 51?
   (d) The equation $45x = 39 \mod 51$ has the solution $x = 2$. Does this contradict your result from part (c)?

2. Let $N = 55 = 5 \cdot 11$. Answer the following by hand:
   (a) What is $\varphi(N)$?
   (b) Say $e = 3$. Find $d$ such that $(x^e)^d = x \mod N$ for all $x \in \mathbb{Z}_N^*$. 
   (c) Find an $x \in \mathbb{Z}_N^*$ such that $x^e = 2 \mod N$. How many $x \in \mathbb{Z}_N^*$ satisfy this equation?

3. The following exercises concern the group $\mathbb{Z}^*_17$. Answer them by hand.
   (a) Prove that 2 is not a generator of $\mathbb{Z}^*_17$.
   (b) Show that 3 is a generator of $\mathbb{Z}^*_17$.
   (c) Compute $\log_3 10$.

4. (cf. Exercise 7.13.)
   (a) Let $N = pq$ be a product of two primes. Show that if $N$ and $\varphi(N)$ are known, then it is possible to efficiently compute $p, q$. (Hint: derive a quadratic equation [over the integers] for $p, q$.)
   (b) Say $N = 18,830,129$ and $\varphi(N) = 18,819,060$. Solve for $p$ and $q$. (You may use a calculator, but not a factoring program. Show your work.)