Homework 1

CPSC 629, Spring 2005

The homework is due on Wednesday, February 2, before class.

Name (print): ________________________________ UIN ________________

Problem 1 Calculating the remainder $c = a \bmod b$ by long division has a bit complexity of $O((n_a - n_b)n_b) = O(n_a n_b - n_b^2) = O(n_a n_b - n_a n_c)$ if the integers a, b, and c are respectively represented by n_a, n_b, and n_b bits. Show that if the Euclidean algorithm is implemented with a multiprecision library that represents an integer a with $O(n_a)$ bits, then the Euclidean algorithm takes $O(n_a n_b)$ steps to calculate $\gcd(a, b)$. [Hint: Consider the sequence $a_0 = a$, $a_1 = b$, $a_2 = a_0 \bmod a_1$, $a_3 = a_1 \bmod a_2$, $\ldots$]

Problem 2 Suppose that a, b, and c are integers such that $\gcd(a, b) = 1$, and that a divides the product bc. Prove that a divides c.

Problem 3 Suppose that $a_1, \ldots, a_k$ are integers and p is a prime that divides the product $a_1 \cdots a_k$. Show that p divides a_j for some some j in $1 \leq j \leq k$.

Problem 4 Find an integer x such that

$$x \equiv 5 \bmod 31$$
$$x \equiv 7 \bmod 37$$

using the method that we have discussed in class. Show all the steps of the extended GCD calculation.

Problem 5 RSA. Suppose that Alice has the public key (e, n) and evil Eve obtained the secret exponent d. Show that Eve can use a randomized algorithm to factor Alice's modulus n in $O(\text{poly}(\log n))$ time.
[We will give some hints in class]