MAT 3343, APPLIED ALGEBRA, FALL 2003

Problem Set 3, due Oct 10, 2003

Peter Selinger

Problem 1. My public RSA key is $\langle N, e\rangle = \langle 11639, 65\rangle$. Send me an encrypted message. Encode each 2-letter pair as a 4-digit decimal number with Space=00, A=01, B=02, etc. For instance, the message "Hello" would be encoded in plaintext as the sequence of numbers 0805 1212 1500. (Calculators are allowed for this problem!)

Problem 2. Suppose that $N = pq$ is the product of two distinct primes, possibly very large. Suppose p, q are unknown, but N is known. Further, assume given an element $x \in \mathbb{Z}_N$ such that $x^2 = x$, but $x \neq 0, 1$. Show that from this information, one can efficiently compute p and q.

Problem 3. State and prove the generalized Chinese Remainder Theorem (see Exercise 1.1, Handout 3 or Problem 34, p.114)

Problem 4. Suppose $N = pqr$ is the product of three distinct odd primes.

(a) How many square roots of unity are there in $\mathbb{Z}_N$?

(b) Show that the set of such square roots can be computed efficiently if p, q, r are known.

(c) Compute the set of square roots of unity for $N = pqr$ where $p = 7$, $q = 11$, and $r = 13$.

(d) Suppose p, q, r are not known, but some square root of unity $x \in \mathbb{Z}_N$ is known such that $x \neq \pm 1$. What information, if any, can be gained about the prime factorization of N? (Hint: use a similar idea as in the first paragraph of the proof of Theorem 3.2, Handout 3).

Problem 5. (a) Use the Fermat pseudoprime test (Algorithm 1.3, Handout 4) to show that the number 119 is not prime. In particular, find some b such that the number 119 fails the Fermat pseudoprime test at base b.

(b) Use the Miller-Rabin primality test (Algorithm 3.4, Handout 4) to show that 561 is not prime. (In particular, find some b such that the number 561 fails the strong pseudoprime test at base b).