Math 5248 Cryptology and number theory
Fall 2006, Vic Reiner
Final exam - Due Wednesday December 13, in class

Instructions: This is an open book, open library, open notes, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult. Explain your reasoning- answers without justification or proof (where appropriate) will receive **no credit**.

1. (20 points total) Check whether or not $n = 289(= 17^2)$ is a pseudoprime for the base $b = 38$ with respect to each of these primality tests:

(a)(6 points) Fermat.

(b)(7 points) Solovay-Strassen.

(c)(7 points) Miller-Rabin.

2. (25 points) Find any solution to the equation

$$\overline{5}x^2 - \overline{9796} = \overline{0}$$

in $\mathbb{Z}/19 \cdot 23^2 = \mathbb{Z}/10051$, using no brute force, but rather using the following tools (in this order): multiplicative inverses, principal square roots, Hensel's Lemma, and Sun Ze's theorem.

3. (20 points total) Assume that $n = 407$ is published as an RSA modulus. Factor it as a product $n = pq$ using the following methods. (No credit will be given for using brute force in any of these parts.)

(a) (7 points) Factor it using Pollard's ρ method with the function $f(x) = x^2 + 2$ and seed value x, so that you begin with the pair $(x, y) = (2, f(2)) = (2, 6)$.

(b)(7 points) Someone tells you that n has a prime factor p for which $p - 1$ is $\{2, 3\}$-smooth. Use Pollard's $p - 1$ method to find this prime p and factor n.

(c)(6 points) You happen to have lying around a square-root oracle, and when you feed it the perfect square $\overline{25}(= \overline{5}^2)$ in $\mathbb{Z}/n$, it informs you that $\overline{116}$ is another square-root of $\overline{25}$ in $\mathbb{Z}/n$. Use this answer to factor n.

4. (15 points total) The *Twin Prime Conjecture* asserts that there should be infinitely many positive integers p for which $p, p+2$ are both prime. At the moment, there is no proof of this conjecture, so it remains an open question. However, you don't need to know anything about this to answer the following two questions– we mention it here only as background and motivation.

(a)(5 points) Show that there are *no* positive integers $p > 2$ for which $p, p+1$ are both primes. (Hint: think mod 2).

(b)(10 points) Show that there are no positive integers $p > 3$ for which $p, p+2, p+4$ are all three primes. (Hint: think mod 3).

5. (20 points total) Let p be prime, and let H be the subset of perfect squares in $(\mathbb{Z}/p)^\times$:

$$H := \{\overline{x} \in (\mathbb{Z}/p)^\times : \text{ there exists } \overline{z} \text{ in } (\mathbb{Z}/p)^\times \text{ with } \overline{x} = \overline{z}^2\}.$$

Consider the *squaring map*

$$\begin{array}{rccc} f: & H & \to & H \\ & f(\overline{x}) & = & \overline{x}^2. \end{array}$$

(a)(10 points) Prove that if $p \equiv 3 \mod 4$ then f is a bijection from H to H, that is, f is one-to-one and onto (or injective and surjective, or a one-to-one correspondence).

(b)(5 points) Give an example of a prime $p \equiv 1 \mod 4$ for which f is not a bijection, and illustrate why it is not.

(c)(5 points) Prove that for *any* $p \equiv 1 \mod 4$, the map f is *never* a bijection. (Hint: Take a look at $\overline{\pm 1}$.)