Math 5248 Cryptology and number theory
Fall 2006, Vic Reiner
Midterm exam 2- Due Wednesday November 15, 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**. You are also allowed to use Garrett's fast modular exponentiation calculator (linked from our syllabus), as long as you say where you used it.

1. (20 points total) Alice wishes to establish an RSA cipher with Bob, and starts by publishing the modulus $n = 1457$.

(a) (10 points) Why can't she choose $e = 3$ as the encryption exponent?

(b) (10 points) Assume she chooses to publish the encryption exponent $e = 7$, and Bob then sends her the ciphertext $y = 803$. How does Alice decrypt it, and what plaintext x does she recover?

2. (20 points total)

(a)(10 points) Let p be a prime and $k \equiv 1 \mod p-1$. Prove the following generalization of Fermat's Little Theorem: for *any* element $\bar{x} \in \mathbb{Z}/p$, regardless of whether or not $\bar{x}$ has a multiplicative inverse, one has

$$\bar{x}^k = \bar{x} \text{ in } \mathbb{Z}/p.$$

(b)(10 points) Let p, q be distinct primes and $k \equiv 1 \mod (p-1)(q-1)$ (e.g. if $k = de$ when d, e, are the encryption, decryption exponents in RSA). Prove the following important fact, alluded to in lecture: for *any* element $\bar{x} \in \mathbb{Z}/pq$, regardless of whether or not $\bar{x}$ has a multiplicative inverse, one has

$$\bar{x}^k = \bar{x} \text{ in } \mathbb{Z}/pq.$$

(Why is this important for RSA? It means Alice doesn't need to worry about whether Bob's plaintext $\bar{x}$ has a multiplicative inverse in $\mathbb{Z}/pq$; she'll still be able to decrypt it correctly.)

3. (20 points total)

(a)(10 points) Find a square root $\bar{x}$ of $\bar{2}$ in $\mathbb{Z}/23$ such that $\bar{x}$ is *not* itself a perfect square in $\mathbb{Z}/23$, using no brute force.

(b)(10 points) Find a square root $\bar{x}$ of $\bar{2}$ in $\mathbb{Z}/23^3$ using Hensel's Lemma.

4. (20 points total)

(a)(7 points) Prove that there can be at most 8 different square roots of an element $\bar{a}$ in $\mathbb{Z}/pqr$ if p, q, r are distinct primes.

(b)(7 points) Find 8 different square roots of $\bar{1}$ in $\mathbb{Z}/105$ using Sun Ze's Theorem, and no brute force.

(c)(6 points) Find 4 *different* ways to factor $f(x) = x^2 - \bar{1}$ in $\mathbb{Z}/105[x]$ into two linear factors.

5. (20 points total)

(a)(10 points) Prove that there are no elements of order 5 in the group $(\mathbb{Z}/1009)^\times$ (where the group operation is multiplication).

(b)(10 points) Prove that there *are* some elements of order 2, some of order 3, and some of order 7 in the group $(\mathbb{Z}/1009)^\times$. (You do not need to write down explicit elements of these orders.)