T-79.5501 Cryptology
Midterm Exam 2
May 9, 2008

1. (6 pts) Solve

$$x^9 \equiv 5 \pmod{2008}.$$

   Note that $2008 = 8 \cdot 251$.

2. (6 pts) It is given that

$$2^{6!} \equiv 105226 \pmod{121939}.$$

   Attempt to find a nontrivial factor of 121939 using the $p-1$ method with $B = 6$.

3. Bob is using the *Rabin Cryptosystem*. Bob's modulus is $40741 = 131 \cdot 311$. Alice knows Bob's modulus but not its factors. Alice wants to remind Bob of a date in December and sends it to Bob encrypted. The ciphertext is 38176.

   (a) (3 pts) Show how Bob decrypts the ciphertext. One of the possible plaintexts is a date, which Bob accepts and discards the other decryptions.

   (b) (3 pts) Alice happens to see one of the decryptions discarded by Bob. It is 20669. Show how Alice can now factor Bob's modulus.

4. Let $\mathbb{F}$ be a finite field with $q$ elements and $\beta$ a primitive element in $\mathbb{F}$. Consider the function $f : \mathbb{Z}_{q-1} = \{0, 1, \ldots, q-2\} \rightarrow \mathbb{F}^*$, $f(x) = \beta^x$.

   (a) (3 pts) Show that $f$ is a bijection.

   (b) (3 pts) For $a' \in \mathbb{Z}_{q-1}$ and $b' \in \mathbb{F}$, let us denote

$$N_D(a', b') = \#\{x \in \mathbb{Z}_{q-1} | f((x + a') \bmod (q-1)) - f(x) = b'\}.$$

   Show that $N_D(a', b') = 1$, for all $a' \neq 0$ and $b' \neq 0$.