Mathematics 116 — Professor K. A. Ribet

First Midterm Exam — February 14, 2012

Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in *complete sentences*. Take pain to explain what you are doing since your exam book is your only representative when you work is being graded.

(6 points) **1.** Suppose that $a \in \mathbf{Z}/37\mathbf{Z}$ is such that the values of a^2, a^4, a^8, a^{16} and a^{32} are respectively 11, 10, 26, 10 and 26. Compute a^{36058}. Find the number of elements b in $\mathbf{Z}/37\mathbf{Z}$ that satisfy $b^{32} = a^{32}$.

(5 points) **2.** Consider the following sage transcript:

```
sage:  p=1259
sage:  g=Mod(1028,p)
sage:  h=g^1238
sage:  log(h,g)
609
```

Why is sage telling us that $\log(h, g)$ is 609, rather than 1238?

(5 points) **3.** Using the equation $1 = 1634152 \cdot 358703966558 - 1162438012471 \cdot 504265$, find an integer x satisfying

$$x \equiv \begin{cases} 99 & \mod 1634152 \\ 123 & \mod 1162438012471. \end{cases}$$

You do not need to simplify your answer.

(7 points) **4.** Let p be the prime 10007 and let g be the primitive root 5 mod p. Imagine that we will be using the baby-step giant-step algorithm to find the discrete logarithm of a number $h \in \mathbf{Z}/p\mathbf{Z}$ with respect to g: we will compare baby steps 1, g, g^2, ... (the first list) with ratios h, hg^{-n}, hg^{-2n}, ... (the second list). If we follow the procedure that was outlined in class, what value n will we choose and how long will each of the lists be? In the case $h = g^{456}$, for which i will g^i occur on both lists?

(8 points) **5.** Let F be the field $\mathbf{F}_3[x]/(x^2 - x - 1)$. How many elements are in F? Let

$$a = x \bmod (x^2 - x - 1)$$

be the image of x in F. Show that $a^4 = -1$ and also that a is a primitive root in F (i.e., a generator of the multiplicative group F^*).

(9 points) **6.** In the ring $\mathbf{F}_2[z]$ of polynomials over the field with two elements, let $f = z^4 + z^3 + z + 1$ and $g = z^4 + 1$. Use the extended Euclidean algorithm to find the gcd d of f and g and to write d in the form $af + bg$ with $a, b \in \mathbf{F}_2[z]$.