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 $b^{32} = a^{32}$.

Because $a^4 = a^{16}$, we know that $a^{12} = 1$. Hence $a^{36058} = a^{10} = a^2a^8 = 11 \cdot 26 = 27$. In the second question, the bs correspond to cs for which $c^{32} = 1$. To say that $c^{32} = 1$ is to say that $c^4 = 1$, since $c^{36} = 1$ by Fermat's Little Theorem. Let g be a generator, and write $c = g^i$ where i is an integer mod 36. The condition $c^4 = 1$ means that $4i \equiv 0 \bmod 36$, i.e., that i is divisible by 9. The possible values of i mod 36 are then 0, 9, 18 and 27. There are four such values. For what it's worth, the possible values of b are 10, 14, 23 and 27 mod 37. Note: Many people ignored the second question in the problem. Is this because it was a stealth question somehow or because it was hard?

(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?

The log in question is the smallest power of g that's equal to h. Since $g^{609} = g^{1238}$, we can infer that $g^{629} = 1$. The order of g must be equal to 629 because otherwise it would be a proper divisor of 629 and then would certainly be less than 609. The only significant thing going on here is that g is not a generator (even though 'g' suggests 'generator'). Since h is a power of g, the discrete log is well defined, and 609 is its value.

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

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

You do not need to simplify your answer.

Answer: $-99 \cdot 1162438012471 \cdot 504265 + 213 \cdot 1634152 \cdot 358703966558$. The value of this unpleasant expression is 14068243304608531683.

(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 $1, g, g^2, \ldots$ (the first list) with ratios $h, hg^{-n}, hg^{-2n}, \ldots$ (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?

The value of n is $\lfloor\sqrt{p-1}\rfloor + 1 = 101$; note that the square root of $p-1$ is smaller than 101 because $101^2 = 10201$. When $h = g^{456}$, we divide 456 by $n = 101$, getting the quotient 4 and the remainder 52. This means that $456 = 4n + 52$, so that $h = g^{4n+52} = g^{4n}g^{52}$. Thus $hg^{-4n} = g^{52}$, so that g^{52}, which is on the first list, also occurs as hg^{-4n} on the second list.

(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^*).

There are 9 elements in F; in general, there are p^n elements if we start with $\mathbf{F}_p$ and use an irreducible polynomial of degree n. (We know that $x^2 - x - 1$ is irreducible in this case because we are told that the quotient ring $\mathbf{F}_3[x]/(x^2 - x - 1)$ is a field.) In F, we have $a^2 = a + 1$, so that $a^4 = (a + 1)^2 = a^2 - a + 1$. (Note that $2 = -1$.) Thus $a^4 = (a+1) - a + 1 = 2 = -1$, as required. The order of a is now clearly 8 because $a^8 = 1$ and $a^4 \neq 1$. Thus a is a multiplicative generator (i.e., a primitive root).

(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 $a, b \in \mathbf{F}_2[z]$.

We have

$$\begin{aligned} f &= g + z^3 + z \\ g &= z \cdot (z^3 + z) + (z^2 + 1) \\ z^3 + z &= z(z^2 + 1). \end{aligned}$$

Hence the gcd of the two polynomials is $z^2 + 1$. Further,

$$z^2 + 1 = g + z(z^3 + z) = g + z(f + g) = (z + 1)g + zf.$$

Note, by the way that $g = (z+1)^4$ and that $z^2+1 = (z+1)^2$. Also, $f = (z+1)^4 + z(z+1)^2$.