Math 116

PROFESSOR KENNETH A. RIBET

First Midterm Examination

February 19, 2009

11:10AM–12:30 PM, 3 Evans Hall

Please put away all books, calculators, and other portable electronic devices—anything with an ON/OFF switch. You may refer to a single 2-sided sheet of notes. For numerical questions, *show your work* but do not worry about simplifying answers. For proofs, write your arguments in complete sentences that explain what you are doing. Remember that your paper becomes your only representative after the exam is over.

Problem	Your score	Possible points
1		6 points
2		6 points
3		4 points
4		9 points
5		5 points
Total:		30 points

1. a. Using the equations

$$692 = 7 \cdot 97 + 13$$
$$97 = 7 \cdot 13 + 6$$
$$13 = 2 \cdot 6 + 1,$$

find the gcd g of 692 and 97 and exhibit integers u and v such that $u692 + v97 = g$.

The gcd *is 1, and we have* $1 = 15 \cdot 692 - 107 \cdot 97$.

b. Use the equation $1 = 62 \cdot 61728 - 97 \cdot 39455$ to solve the simultaneous congruences

$$x \equiv \begin{cases} 15 \pmod{61728} \\ 123 \pmod{39455}. \end{cases}$$

People are solving this problem by adding a suitable multiple of 61728 *to* 15. *The multiple that works is* $61728 \cdot 6696$.

2. a. Find an expression for 5^{1234} mod 144169 as a product of some of the quantities

$$a_i := 5^{2^i} \bmod 144169.$$

As most of you knew, the aim is to find the binary expansion of 1234*; this number is the sum of* 1024, 128, 64, 16 *and* 2. *The number* 5^{1234} *is then the product of the corresponding powers of* 5.

b. Compute the remainder when $11^{100000002}$ is divided by the prime number 101.

The point is that $11^{100} \equiv 1$ *mod* 101 *by Fermat's little theorem. Thus* $11^{100000002} \equiv 11^2 = 121 \equiv 20$ *mod* 101.

3. The prime factorization of N is $1729 = 7 \cdot 13 \cdot 19$. Show that we have $a^{(N-1)/2} \equiv 1 \bmod N$ for all integers a such that $\gcd(a, N) = 1$.

This is like the 561 *Carmichael problem that we did in class. It's enough to show that* $a^{(N-1)/2} \equiv 1$ *mod* p *for* $p = 7, 13, 19$. *In each case, by Fermat's little theorem, all one needs to show is that the exponent* $864 = (N-1)/2$ *is divisible by* $p - 1$. *So one needs to check that* 864 *is divisible by each of* 6, 12 *and* 18. *This is really true; in fact* $864 = 2^5 3^3$.

The number $N = 1729$ is famous because it may be written both as $12^3 + 1$ and $10^3 + 9^3$; it is the smallest integer that can be decomposed in two ways as the sum of two perfect positive cubes! Indeed, see `http://en.wikipedia.org/wiki/1729_(number)` for more on this.

4. Give a clear, concise description of each of the following:

a. The discrete log problem for $(\mathbf{Z}/p\mathbf{Z})^*$.

It's the problem of finding x *when one is given* $g \in (\mathbf{Z}/p\mathbf{Z})^*$ *along with a number of the form* g^x.

b. The Diffie–Hellman problem for $(\mathbf{Z}/p\mathbf{Z})^*$.

Given g, g^a *and* g^b *in* $(\mathbf{Z}/p\mathbf{Z})^*$, *we want to find* g^{ab}.

c. The RSA crpytosystem.

I'll defer to our textbook on this one.

5. Suppose that $m = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. How many numbers x mod m satisfy $x^2 \equiv 1 \bmod m$? List three of these numbers.

By the Chinese remainder theorem, the number of x *is the product of the numbers of square roots of 1 mod each of the four primes* 2, 3, 5 *and* 7. *There are two square roots mod each of the odd primes but only one square root (namely,* 1*) mod* 2. *Hence the number of solutions* x *is* $2 \times 2 \times 2 = 8$. *The natural answer for the "list three" question is to cite* 1, -1 *and some "exotic" square root of* 1. *For example, we could take a root that's* -1 *mod* 3 *and* 1 *mod* 70*; hmm, how about* 71*?*