Math 115 Professor K. A. Ribet

Midterm Exam November 1, 2006

This exam was an 50-minute exam. It began at 2:10PM. There were 3 problems, for which the point counts were 8, 10 and 12. The maximum possible score was 30.

> *Please put away all books, calculators, electronic games, cell phones, pagers, .mp3 players, PDAs, and other electronic devices. You may refer to a single 2-sided sheet of notes. Your paper is your ambassador when it is graded. Correct answers without appropriate supporting work will be regarded with extreme skepticism. Incorrect answers without appropriate supporting work will receive no partial credit. This exam has four pages, including this cover sheet and a blank page at the end. Please write your name on each page. At the conclusion of the exam, please hand in your paper at the front of the room.*

1. *Determine the value of the Legendre symbol* $\left(\dfrac{71}{113}\right)$, *using quadratic reciprocity or otherwise.*

The numbers 71 and 113 are prime. (For 113, this was supposed to be obvious from the notation, since we haven't discussed Kronecker symbols in which the bottom number is not prime.) It is clear that $113 \equiv 100 \equiv 1 \bmod 4$, so $\left(\dfrac{71}{113}\right) = \left(\dfrac{113}{71}\right) = \left(\dfrac{42}{71}\right) = \left(\dfrac{2}{71}\right)\left(\dfrac{3}{71}\right)\left(\dfrac{7}{71}\right)$. The first of the three factors is $+1$ because $71 \equiv -1 \bmod 8$. By quadratic reciprocity, we have $\left(\dfrac{3}{71}\right) = -\left(\dfrac{71}{3}\right) = -\left(\dfrac{2}{3}\right) = +1$. Finally, $\left(\dfrac{7}{71}\right) = -\left(\dfrac{71}{7}\right) = -\left(\dfrac{1}{7}\right) = -1$. Thus the answer is -1.

Using the relation $1 = 22 \cdot 113 - 35 \cdot 71$, *find an integer* n *for which* $n \equiv -2$ *mod 113 and* $n \equiv 8$ *mod 71. (An answer like* $n = 91 \cdot 65 + 123 \cdot 765$ *will be fine; avoid doing a lot of arithmetic.)*

The number $22 \cdot 113$ is 0 mod 113 and 1 mod 71, whereas $-35 \cdot 71$ is 1 mod 113 and 0 mod 71. If $n = 2 \cdot 35 \cdot 71 + 8 \cdot 22 \cdot 113$, we should be in good shape.

2. *If* p *is an odd prime, show that the product of the quadratic residues mod* p *is 1 mod* p *if* $p \equiv 3$ *mod 4 and* -1 *mod* p *if* $p \equiv 1$ *mod 4. For example, the squares mod 11 are 1, 3, 4, 5, 9; their product is 1 mod 11. The squares mod 13 are 1, 3, 4, 9, 10, 12; they multiply to* -1 *mod 13.*

The quadratic residues are gotten by squaring all the integers from 1 to $(p-1)/2$, inclusive. The product of the residues is thus the square of $\left(\dfrac{p-1}{2}\right)!$. As we have discussed in class, the conclusion now follows from Wilson's theorem, which states that $(p-1)!$ is -1 mod p.

3. *Suppose that p is a prime number and n is a positive integer. Show that -1 and $+1$ are the only solutions to $x^2 \equiv 1 \bmod p^n$ when p is at least 3. (It might be useful to factor $x^2 - 1$.)*

If p^n divides $x^2 - 1$, then p divides $x^2 - 1$. Hence p divides $x - 1$ or $x + 1$. The "or" is exclusive: if p divided both, it would divide their sum, which is 2, contradicting the assumption that p is odd. To fix ideas, say p divides $x - 1$ but is prime to $x + 1$. Then p^n is prime to $x + 1$. Since p^n divides $(x - 1)(x + 1)$ but is prime to the second factor, it must divide the first factor, so that x is 1 mod p^n. Similarly if p divides $x + 1$ but not $x - 1$.

The case $p = 2$ is different: If $x \equiv \pm 1 \bmod 2^n$, where $n \geq 1$, show that $x^2 \equiv 1 \bmod 2^{n+1}$. Find a solution to $x^2 \equiv 1 \bmod 1024$ other than $\pm 1 \bmod 1024$.

If $x \equiv \pm 1 \bmod 2^n$, we can write $x = \pm 1 + t2^n$ for some integer t. Square this relation to see that $x = 1 \pm t2^{n+1} + t^2 2^{2n}$. Since n is at least 1, $2n \geq n + 1$; thus, x is 1 mod 2^{n+1}, as required. For a non-trivial solution mod 1024, we can take 511 or 513.