Mathematics 115 — Professor K. A. Ribet

Last Midterm Exam — October 25, 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.* Be careful to explain what you are doing since your exam book is your only representative when your work is being graded.

The problems are worth 6 points each.

1. Which numbers between 1 and 11 are quadratic residues modulo the prime 3001?

The main point is to figure out whether 2, 3, 5, 7 and 11 are squares because the remaining numbers (1, 4, 6, 8, 9, 10) are products of these five. (For example, 1 is the empty product of those five numbers.) You can calculate $\left(\frac{2}{3001}\right)$ and so on by quadratic reciprocity. This should be easy because 3001 is congruent to 1 mod lots of stuff. The end result (according to sage) is that the only non-square among the numbers between 1 and 11 is 7.

2. Find an integer a such that $\left(\frac{a}{35}\right) = +1$ but such that a is not a square modulo 35.

You need to find non-squares mod 5 and mod 7 and then combine them into a number mod 35 using the Chinese Remainder Theorem (or by inspection). The smallest non-sqaure mod 5 is 2; the smallest non-square mod 7 is 3. It looks like 17 is 2 mod 5 and 3 mod 7. You can take $a = 17$, though of course there are other answers.

3. If $f(x)$ is the polynomial $x^3 + 2x^2 + 3x + 4 \in \mathbf{Z}[x]$, one has $f(2) = 26$. Using the techniques of Hensel's lemma, find a root of $f(x)$ modulo 13^2.

The derivative of $f(x)$ is $3x^2 + 4x + 3$, and $f'(2) = 23$, which is -3 mod 13. The inverse of -3 mod 13 is 4. The general formula $a - f(a)/f'(a)$ yields $2 - 4 \cdot 26 = -102$ when $a = 2$. The quantity -102 mod 169 is the desired root of $f(x)$ modulo 13^2; we can rewrite this root as 67 mod 169 if we care to.

4. Let p be a prime number. Suppose that i is a positive integer such that $(a+i)^{a+i} \equiv a^a$ mod p for all $a = 1, 2, 3, \ldots$. Show that i is divisible by $p(p-1)$.

During the exam, one student asked me "Can we quote our homework?" Well, not really, but I hope that you remembered how to do this! First, let's prove that i is divisible by p. Consider the congruence $(p+i)^{p+i} \equiv p^p$ mod p. The right-hand side is 0 mod p, so the left-hand side must be 0 mod p as well. Hence $(p+i)^{p+i}$ is divisible by p, which implies easily that i is divisible by p.

Say $i = pj$, and take a to be a primitive root mod p. We have

$$a^a \equiv (a + pj)^{a+pj} \equiv a^{a+pj} \equiv a^a (a^p)^j \equiv a^a a^j \bmod p.$$

Hence $a^j \equiv 1 \bmod p$. Since a is a primitive root, this implies that j is divisible by $p - 1$.

5. Let p be a prime number. Prove that $\binom{p-1}{j} \equiv (-1)^j \bmod p$ for $j = 0, \ldots, p - 1$.

When $p = 2$, the two binomial coefficients in question are both 1, and indeed they are respectively congruent to $+1$ and -1 mod 2. Assume now $p > 2$, so that p is an odd number. The problem is secretly asking us to verify the equality of the two mod p polynomials $\sum_{j=0}^{p-1} \binom{p-1}{j} x^j$ and $\sum_{j=0}^{p-1} (-1)^j x^j$. By the binomial theorem, the first polynomial is $(1 + x)^{p-1}$. We can use the fact that two polynomials are equal if they become equal after multiplication by a non-zero polynomial; let's multiply by $1 + x$. The left side then becomes $(1 + x)^p = 1 + x^p$. The right side also becomes $1 + x^p$ because of the standard identity

$$x^n + 1 = (x + 1)(1 - x + x^2 - \cdots)$$

when n is an odd number.

If you did the problem that way, you're a big star. I think that most people will do the problem directly. We have to prove the mod p congruence

$$(p - 1)! \equiv (-1)^j j!(p - 1 - j)!$$

for each j. Now

$$(p - 1 - j)! = 1 \cdot 2 \cdot 3 \cdot (p - 1 - j) \equiv (p - 1)(p - 2) \cdots (j + 1)(-1)^{p-1-j}.$$

However, $(-1)^{p-1-j} = (-1)^j$ when $p-1$ is even, which we have assumed. Hence $j!(p-1-j)!$ is congruent mod p to $(-1)^j$ times $(p-1)!$, so we have established our congruence directly.

Note: this problem presents a variant of the congruence needed to do problem #14, the one with $(2^p - 2)/p$.