Mathematics 115 | Professor K. A. Ribet

Final Examination | December 13, 2011

Please put away all calculators, cell phones and other electronic devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in complete sentences. Take pains to explain what you are doing since the grader cannot read your mind.

(6 pts.) **1.** Calculate the number of solutions to the congruence $x^3 \equiv 8 \bmod n$, where $n = 2^4 \cdot 3^2 \cdot 5 \cdot 7$.

Let $N(i)$ be the number of solutions to the congruence mod i. By the Chinese Remainder Theorem, $N(n) = N(2^4)N(3^2)N(5)N(7)$. One can see in various ways that $N(16) = 4$; the solutions to the congruence are $x = 2$, $x = 6$, $x = 10$ and $x = 14$. Similarly, $N(9) = 3$, $N(5) = 1$, $N(7) = 3$. Hence $N(n) = 4 \cdot 3 \cdot 1 \cdot 3 = 36$.

(8 pts.) **2.** Let n and d be positive integers. Assume that d^2n is the sum of two integral squares. Prove that n is also the sum of two integral squares. Further, suppose that n is the sum of the squares of two *rational* numbers. Prove that n is the sum of the squares of two integers.

If m is a positive integer, we learned during the semester that m is the sum of two integral squares if and only if $\operatorname{ord}_p(m)$ is even for each prime $p \equiv 3 \bmod 4$. Here $\operatorname{ord}_p(m)$ is the exponent of the highest power of p that divides m. For each relevant p, we have $\operatorname{ord}_p(d^2n) = \operatorname{ord}_p(n) + 2\operatorname{ord}_p(d)$. Hence $\operatorname{ord}_p(d^2n)$ is even if and only if $\operatorname{ord}_p(n)$ is even. Hence n is a sum of two squares if and only if d^2n is such a sum; this proves the first assertion. Note, by the way that it is not true (as some of you are writing) that a and b have to be divisible by d when $d^2n = a^2 + b^2$. For a specific example, take $n = 2$ and $d = 5$; then $50 = 7^2 + 1^2$ but the integers 7 and 1 are not divisible by 5.

For the second, we take d to be a common denominator for the two rational numbers. Then d^2n is the sum of the squares of two integers; the analogous statement holds for n by the first part of the problem.

(6 pts.) **3.** Find an integer n so that $n^2 \equiv 5 \bmod 59^2$ and $n \equiv 8 \bmod 59$.

You were expecting a Hensel Lemma problem, so you got one! The number 8 is a root of $f(x) = x^2 - 5 \bmod p$, where p is the prime 59. A refinement of this root mod 59^2 is given by the formula $8 - f(8)/f'(8)$, where the inverse to $f'(8)$ needs to be computed only mod 59. We have $f(8) = 59$, $f'(8) = 16$. A quick computation (e.g., using the Euclidean algorithm) shows that an inverse to 16 mod 59 is -11. (Indeed, $-11 \cdot 16 - 1 = -177 = (-3) \cdot 59$.) Hence we can take $n = 8 + 11 \cdot 59$. You can stop there or perhaps go on to compute the value $n = 657$. We have $f(n) = 431644 = 124 \cdot 59^2$.

(6 pts.) **4.** Let $\zeta = e^{2\pi i/p}$, where $p \geq 3$ is prime. Show that $\displaystyle\sum_{a \bmod p} \left(\frac{a}{p}\right)\zeta^a = \sum_{a \bmod p} \zeta^{a^2}$.

Let S be the sum of the ζ^a for a a non-zero square mod p. Let N be the corresponding sum over the non-squares a. There is only one remaining a, namely $a = 0$. The quantity ζ^0 is 1. In the formula to be proved, the left-hand side is $S - N$ and the right-hand side is $1 + 2S$. The two sides are equal if $S - N = 1 + 2S$, i.e., if $0 = 1 + S + N$. Because zeta is a root of the polynomial $1 + x + x^2 + \cdots + x^{p-1}$, we do have $S + N + 1 = 0$.

(7 pts.) **5.** Let p and q be odd primes, and let M be the Mersenne number $2^q - 1$.

a. If p divides M, prove that we have $p \equiv 1 \bmod 2q$.

If p divides M, we have $2^q \equiv 1 \bmod p$, which means that the order of 2 mod p is q. This order a priori divides $p - 1$, so q divides $p - 1$. Equivalently, $p \equiv 1 \bmod q$. Since p and q are odd, it follows that $p \equiv 1 \bmod 2q$.

b. Assume that p^2 divides M. Show that $2^{(p-1)/2} \equiv 1 \bmod p^2$.

By the first part of the problem, $(p - 1)/2$ is a multiple of q, so it suffices to show that $2^q \equiv 1 \bmod p^2$. But trivially we have $2^q \equiv 1 \bmod M$ and p^2 is a divisor of M.

If $2^{(p-1)/2} \equiv 1 \bmod p^2$, then $2^{(p-1)} \equiv 1 \bmod p^2$, so that p is a *Wieferich prime*. There are only two Wieferich primes known, namely 1093 and 3511. For neither of these is it true that $2^{(p-1)/2} \equiv 1 \bmod p^2$. In other words, one knows no prime p for which $2^{(p-1)/2} \equiv 1 \bmod p^2$ and therefore (by the problem) no situation where a Mersenne number is divisible by the square of a prime. In other words, one knows no Mersenne number that is not square free. Are all Mersenne numbers actually square free? No one knows.

(8 pts.) **6.** Here are two formulas involving the Jacobi symbol:

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right), \qquad \left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \bmod 8, \\ -1 & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

In the first, m and n are odd, positive and not both 3 mod 4. In the second, p is odd and positive (but not necessarily prime). Show that the first formula implies the second:

a. Suppose that p is an odd integer greater than 8. Using the first of the two formulas, justify each of the four numbered equalities

$$\left(\frac{2}{p}\right) \overset{(i)}{=} \left(\frac{8-p}{p}\right) \overset{(ii)}{=} \left(\frac{p}{p-8}\right) \overset{(iii)}{=} \left(\frac{8}{p-8}\right) \overset{(iv)}{=} \left(\frac{2}{p-8}\right),$$

thereby obtaining $\left(\frac{2}{p}\right) = \left(\frac{2}{p-8}\right)$.

Clearly $\left(\frac{2}{p}\right) = \left(\frac{8}{p}\right)$ because $8 = 2^2 \cdot 2$. Also $8 - p \equiv 8 \bmod p$, so $\left(\frac{8}{p}\right) = \left(\frac{8-p}{p}\right)$; this gives (i). We get (iv) simply because $8 = 2^2 \cdot 2$. For (iii), we note that $p \equiv 8 \bmod (p - 8)$.

The equality (ii) is slightly more complicated than I thought, so I will change the wording of the problem for the exam. If p is 1 mod 4, then $\left(\frac{8-p}{p}\right) = \left(\frac{p-8}{p}\right)$; the numerator and denominator are both 1 mod 4, so we can swap them and get the right-hand side of (ii). If p is 3 mod 4, then $\left(\frac{8-p}{p}\right) = -\left(\frac{p-8}{p}\right)$, but both numerator and denominator are now 3 mod 4 and we get a second minus sign when we swap them to get the right-hand side of (ii).

b. Using the result of part (a) and computing the values $\left(\dfrac{2}{p}\right)$ for $p \le 7$, establish the second of the two formulas for the Jacobi symbol.

I leave you to compute the values for $p = 1$, $p = 3$, $p = 5$ and $p = 7$. They are $+1$, -1, -1, $+1$. Once you know them and have done part (a), you get the second formula of the problem by a sort of induction: just keep substracting 8 until you get in the range where you have computed things by hand.

(9 pts.) **7.** Suppose that p is a prime congruent to 1 mod 4 and that u is a square root of -1 mod p satisfying $1 \le u < p/2$. You demonstrated on November 22 that the continued fraction expansion of u/p may be written $\langle 0, a_1, \ldots, a_n, a_n, \ldots a_1\rangle$; this means that the string following the initial 0 is palindromic of even length. As usual, let h_i/k_i $(i = 0, \ldots, 2n)$ be the convergents belonging to this continued fraction. For instance, if $p = 73$ and $u = 27$, then $u/p = \langle 0, 2, 1, 2, 2, 1, 2\rangle$ has convergents $\frac{0}{1}, \frac{1}{2}, \frac{1}{3}, \frac{3}{8}, \frac{7}{19}, \frac{10}{27}, \frac{27}{73}$.

a. Using the formula $\dfrac{k_n}{k_{n-1}} = \langle a_n, \ldots, a_2, a_1\rangle$ of HW13, prove

$$\frac{u}{p} = \langle 0, a_1, \ldots, a_n, k_n/k_{n-1}\rangle = \frac{h_n k_n + h_{n-1}k_{n-1}}{k_n^2 + k_{n-1}^2}.$$

My idea here is that $u/p = \langle 0, a_1, \ldots, a_n; a_n, a_{n-1}, \ldots, a_1\rangle$ by what was proved in the homework. We replace the last n terms by k_n/k_{n-1} (also using the homework) and then exploit the formula $\langle 0, a_1, \ldots, a_n, \xi\rangle = \dfrac{\xi h_n + h_{n-1}}{\xi k_n + k_{n-1}}$ with $\xi = k_n/k_{n-1}$. If you simplify the expression by multiplying numerator and denominator by k_n, you should get the desired expression for u/p. Of course, we don't know that the fraction $\dfrac{h_n k_n + h_{n-1}k_{n-1}}{k_n^2 + k_{n-1}^2}$ is in lowest terms, so we don't yet know that $p = k_n^2 + k_{n-1}^2$. If we can prove that $k_n^2 + k_{n-1}^2$ is less than $2p$, we will be able to conclude that $k_n^2 + k_{n-1}^2$ must be p, rather than a non-trivial positive multiple of p.

b. (Omitted. The problem was to show that $p = k_n^2 + k_{n-1}^2$. Extra credit if you can do this! Note that in the example with $p = 73$, we have $73 = 3^2 + 8^2$.)

OK, someone solved the problem; here's the student's solution. The aim is to show that $\dfrac{h_n k_n + h_{n-1}k_{n-1}}{k_n^2 + k_{n-1}^2}$ is in lowest terms, as was stated above. Let $g = \gcd(\text{num.}, \text{denom.})$; we wish to show $g = 1$. Consider $k_{n-1}(h_n k_n + h_{n-1}k_{n-1}) - h_{n-1}(k_n^2 + k_{n-1}^2)$. This works out to be $k_{n-1}h_n k_n - h_{n-1}k_n k_n = (k_{n-1}h_n - k_n h_{n-1})k_n = \pm k_n$. For example, when $p = 73$, $u = 27$, we have $(h_n, k_n) = (3, 8)$, $(h_{n-1}, k_{n-1}) = (1, 3)$ and $k_{n-1}(h_n k_n + h_{n-1}k_{n-1}) - h_{n-1}(k_n^2 + k_{n-1}^2) = 3 \cdot 27 - 1 \cdot 73 = 8 = k_n$. Since g divides the numerator and denominator of the fraction, g divides k_n and hence also k_n^2. Looking at the denominator, we see that g divides k_{n-1}^2 as well. On the other hand, we remember that k_n and k_{n-1} are relatively prime because of the formula $h_{n-1}k_n - h_n k_{n-1} = \pm 1$. Therefore, k_n^2 and k_{n-1}^2 are relatively prime and we conclude that $g = 1$.