Math 115 Professor K. A. Ribet

Final Exam December 16, 2006

This exam was a three-hour exam. It began at 5:00PM. There were 6 problems, for which the point counts were 6, 6, 8, 8, 10 and 7. The maximum possible score was 45.

*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 eight pages, including this cover sheet. 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.** *Establish the irrationality of the real number* $\displaystyle\sum_{n=1}^{\infty} \frac{1}{2^{n^2}}$.

This is a special case of problem 7 of page 99 of the book, which was part of HW#9, due on October 27. Aaron's solution for that problem was based on the rapid converge of the various series in question. Alternatively, we could say that a rational number has a periodic "decimal" expansion in any base. In base 2, the decimal expansion of the sum has a 1 in the first, fourth, ninth, sixteenth,... places to the right of the decimal point and 0s elsewhere. This expansion is not periodic!

**2.** *Since* $13^3 - 78 = 2119$, *13 is a cube root of 78 mod 2119. Determine the number of cube roots of 78 in* $\mathbf{Z}_{2119}$. *[It may be useful to know that the prime factorization of 2119 is* $13 \cdot 163$.*]*

In my original solution to this problem, I wrote incorrectly: "Because 78 is a cube mod 2119, the number of cube roots of 78 is the same as the number of cube roots of 1; this number is the number of elements of $\mathbf{Z}_{2119}^*$ of order dividing 3. We have to use the Chinese Remainder Theorem to view $\mathbf{Z}_{2119}^*$ as $\mathbf{Z}_{13}^* \times \mathbf{Z}_{163}^*$. The number of elements of order dividing 3 in the product is the product of the number of such elements in each factor. In $\mathbf{Z}_p^*$, the number of elements of order $d$ is $\gcd(d, p-1)$. In our case, $\gcd(3, p-1)$ is 3 for both primes $p = 13$, $p = 163$. Hence the answer is 9." In making up this problem, I chose 13 and 78 as essentially random numbers without noticing that 78 is a multiple of 13. The fact that 13 appears both as the cube root of 78 and as one of the factors of 2119 changes everything. So let's go again: the Chinese Remainder Theorem allows us to view $\mathbf{Z}_{2119}$ as $\mathbf{Z}_{13} \times \mathbf{Z}_{163}$. The number 78 is not divisible by 163, so it represents an element of $\mathbf{Z}_{163}^*$ that has a cube root (namely 13). It therefore has 3 cube roots in $\mathbf{Z}_{163}^*$, as indicated in the original version of the solution. However, 78 represents 0 in $\mathbf{Z}_{13}$. Here, 0 has a single cube root: 0. Hence there are a total of $1 \times 3 = 3$ cube roots of 78 in $\mathbf{Z}_{2119}$.

**3.** *Suppose that* $n$ *is a positive integer for which* $2^n + 1$ *is a prime. Show that* $n$ *is a power of* 2.

If $n$ is not a power of 2, there's a factorization $n = dm$ with $d$ odd and $d > 1$. Recall the algebraic factorization $x^d + 1 = (x+1)(x^{d-1} - x^{d-2} + \cdots + 1)$. Plugging in $x = 2^m$, we see that $2^n + 1$ has the non-trivial factor $2^m + 1$.

*Suppose that $n$ is a positive integer for which $2^n - 1$ is a prime. Show that $n$ is a prime number.*

This is similar. If $n = dm$ with $1 < d < n$, then $2^n - 1$ has the non-trivial factor $2^d - 1$.

**4.** *In $\mathbf{Z}[\omega]$, write $7! = 5040$ as a product of irreducible elements.*

First factor $7!$ in $\mathbf{Z}$: $7! = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. The prime numbers that are 2 mod 3, namely 2 and 5, stay prime in $\mathbf{Z}[\omega]$. The prime 3 factors as $\sqrt{-3} \cdot (-\sqrt{-3})$, which is the product of the square of $\sqrt{-3}$ and the unit $-1$. Finally, $7 = (2 + \sqrt{-3})(2 - \sqrt{-3}$ with both factors irreducible. Thus an answer is

$$5040 = 2^4 \cdot (\sqrt{-3})^4 \cdot 5 \cdot (2 + \sqrt{-3}) \cdot (2 - \sqrt{-3}).$$

The answer is not unique because you can multiply the various factors by units whose product is 1 and not change the product.

**5.** *Consider the Diophantine equation $3a^2 + b^2 = c^2$ in which $a$, $b$ and $c$ are non-zero positive integers.*

OK, it's on my radar screen.

*If $(a, b, c)$ is a solution in which at least two of the numbers $a$, $b$ and $c$ have a common factor $> 1$, show that there is a solution $(a', b', c')$ and an integer $g > 1$ so that $(a, b, c) = g \cdot (a', b', c') = (ga', gb', gc')$.*

If there's a common factor, there's a common factor that's a prime. If this prime divides two of $a$, $b$ and $c$, then its square must divide all three members of the Diophantine equation. Hence the remaining variable will be divisible by the prime. (The argument works even if the prime number is 3.) We can take $g$ to be the prime in question.

*Show that there are no solutions to the equation with $a$ odd and $b$ even. Find one solution with $a$ and $b$ both odd, and another solution with $a$ even and $b$ odd.*

If $a$ is odd and $b$ even, then $3a^2 + b^2 \equiv 3 \bmod 4$. However, a square must be 0 or 1 mod 4. Thus there are no solutions with $a$ odd and $b$ even. The solution $(1, 1, 2)$ has $a$ and $b$ both odd. The solution $(2, 5, 13)$ has $a$ even and $b$ odd.

*Suppose that $3a^2 + b^2 = c^2$ with $a$, $b$ and $c$ pairwise relatively prime in the sense that no two of them have a common factor $> 1$. Assume further that $a$ and $b$ are odd. Using the*

*factorization* $3a^2 = (c-b)(c+b)$, *show that there are odd positive integers* $n$ *and* $m$ *so that* $a = mn$, $c = \dfrac{n^2+3m^2}{2}$ *and* $b = \left|\dfrac{m^2-3n^2}{2}\right|$.

In the indicated factorization, the two factors on the right-hand side are both positive because $c$ and $b$ are positive and the product is a square. By the standard arguments we used in class, the gcd of $c-b$ and $c+b$ divides 2 since $b$ and $c$ are relatively prime. However, $b$ and $c$ have opposite parity, so $c-b$ and $c+b$ are both odd. Thus the gcd is 1. By unique factorization in $\mathbf{Z}$, one of $c-b$ and $c+b$ is a square and the other is 3 times a square. Say $c-b = n^2$, $c+b = 3m^2$ with $n$ and $m$ positive integers. Then solving for $c$ gives $c = \dfrac{n^2+3m^2}{2}$, as desired. Solving for $b$ gives $b = \dfrac{3m^2-n^2}{2}$, which we can write also as $b = \left|\dfrac{3m^2-n^2}{2}\right|$, since $b$ is positive. We learn also from this investigation that there was a misprint in the problem; good to catch it now, before the exam! Now $a^2 = (c-b)(c+b)/3 = n^2m^2$. Since $a$, $n$ and $m$ are positive, we have $a = nm$. Note also that $n$ and $m$ are odd because $a$ was assumed to be odd going in. The case where $c-b = 3m^2$, $c+b = n^2$ is similar. This time we get that $b = \dfrac{n^2-3m^2}{2}$ rather than $b = \dfrac{3m^2-n^2}{2}$. The absolute value signs were designed to put everything under one roof.

**6.** *Suppose that* $p$ *is an odd prime number and that* $a$ *is an integer prime to* $p$ *which is known to be a square mod* $p$. *For example, we might happen to know that 23 is a square mod the prime 15101. In this situation, one is often interested in finding a square root of* $a$ *mod* $p$. *If* $p \equiv 3$ *mod 4, show that* $a \equiv x^2$ *mod* $p$, *where* $x = a^{(p+1)/4}$.

Work mod $p$: $x^2 \equiv a^{p+1/2} = a^{p-1/2} \cdot a \equiv 1 \cdot a = a$. We know that $a^{p-1/2} \equiv 1$ because $a$ is assumed to be a square.

*Suppose again that* $a$ *is a square mod* $p$, *but assume this time that we have* $p \equiv 5$ *mod 8. Explain why we have the congruences*

$$a^{(p-1)/4} \equiv \pm 1 \pmod{p}, \quad 2^{(p-1)/2} \equiv -1 \pmod{p}.$$

The second congruence says that 2 is a non-square mod $p$. We know that (for $p$ odd), 2 is a square mod $p$ if and only if $p \equiv \pm 1$ mod 8. Because $p$ is 5 mod 8, 2 is indeed a non-square mod $p$. For the second congruence, we note again that $a^{(p-1)/2} \equiv 1$ mod $p$. Hence $a^{(p-1)/4}$ is a number mod $p$ whose square is 1. Hence $a^{(p-1)/4}$ must be $\pm 1$.

*Show that* $a \equiv x^2$ *mod* $p$ *where* $x$ *is either* $a^{(p+3)/8}$ *or* $2a \cdot (4a)^{(p-5)/8}$.

Assume first that $a^{(p-1)/4} \equiv 1$ mod $p$; this is one of two alternatives. The square of $a^{(p+3)/8}$ is $a^{(p+3)/4} = a \cdot a^{(p-1)/4} \equiv a$, so we win in this case. Assume now that $a^{(p-1)/4} \equiv -1$ mod $p$; this is the other alternative. The square of $2a \cdot (4a)^{(p-5)/8}$ is $2^2a^2 2^{(p-5)/2} a^{(p-5)/4} = 2^{(p-1)/2} a^{(p+3)/4}$. Now $2^{(p-1)/2} \equiv -1$ and $a^{(p+3)/4} = a \cdot a^{(p-1)/4} \equiv -a$. Thus $2^{(p-1)/2} a^{(p+3)/4} \equiv a$, as desired.