Math 115 Professor K. A. Ribet

Second Midterm Exam November 3, 2000

This is a closed-book exam: no notes, books or calculators are allowed. Explain your answers in complete English sentences. No credit will be given for a "correct answer" that is not explained fully. In general, there is no need to simplify numerical answers.

1 *(3 points). Calculate the number of primitive roots mod* $35035 = 5 \cdot 7^2 \cdot 11 \cdot 13$.

There aren't any because 35035 is not on the short list of moduli for which there is a primitive root.

2 *(6 points). What is the remainder when one divides the prime number* 1234567891 *by 11? What is the remainder when* $11^{1234567890}$ *is divided by 1234567891?*

The answer to the first question is "7"; for this, use the fact that 10 is -1 mod 11, so that 10^2 is 1 mod 11, 10^3 is -1 mod 11, etc. The answer to the second question is "1"; this is Fermat's Little Theorem.

3 *(5 points). Find a mod 29 inverse to the* 2×2 *matrix* $\begin{pmatrix} 1 & 2 \\ 3 & 9 \end{pmatrix}$ *mod 29.*

The determinant of this matrix is 3, and an inverse to 3 mod 29 is 10 mod 29. You have to multiply this number (i.e., 10) by the matrix $\begin{pmatrix} 9 & -2 \\ -3 & 1 \end{pmatrix}$ mod 29 to get the answer, which seems to be $\begin{pmatrix} 3 & 9 \\ 28 & 10 \end{pmatrix}$.

4 *(9 points). If p is a prime, show that all prime divisors of* $2^p - 1$ *are congruent to 1 mod p. (For example,* $2^{11} - 1 = 23 \cdot 89$ *is divisible by the primes 23 and 89 and by no others.)*

Let ℓ be a prime dividing $2^p - 1$. Then $2^p \equiv 1$ mod ℓ, and hence the order of 2 mod ℓ divides p. This order can't be 1, so the order is p. The order divides $\ell - 1$ as well; thus p divides $\ell - 1$, which is what is needed here. (If you just say that this is a theorem in the book, you will get some partial credit but not all that much.)

5 *(7 points). Let* μ *be the Möbius function, and let* τ *be the function whose value on* $n \geq 1$ *is the number of divisors of n. Explain why the function* $F(n) := \sum_{d|n} \mu(d)\tau(d)$ *satisfies the relation* $F(n_1 n_2) = F(n_1)F(n_2)$ *when* $\gcd(n_1, n_2) = 1$. *Calculate* $F(p^e)$ *when p is a prime and e is a positive integer.*

The point here is that F is the summatory function of a multiplicative function, so that F is multiplicative by a theorem that we proved in class. The relation $F(n_1 n_2) = F(n_1)F(n_2)$ is the statement that F is multiplicative! Multiplicative functions are determined by their values on prime powers. We have $F(p^e) = \mu(1)\tau(1) + \mu(p)\tau(p) = 1 + (-1)2 = -1$ when p is prime and e is positive; hope I got that right.

NB: If you find mistakes in this write-up, please let me know by e-mail and I'll make the necessary changes.