Math 115 — Professor K. A. Ribet

Fall Semester, 1999

First Midterm Exam — September 23, 1999

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.

1 *(4 points).* Find the remainder when 2^{33} is divided by 31.

2 *(4 points).* Use the identity $27^2 - 8 \cdot 91 = 1$ to find an integer x such that $27x = 14 \bmod 91$.

3 *(4 points).* Find all prime numbers p such that $p^2 + 2$ is prime.

4 *(5 points).* Suppose that $ax + by = 17$, where a, b, x and y are integers. Show that the numbers $\gcd(a, b)$ and $\gcd(x, y)$ are divisors of 17. Decide which, if any, of the following four possibilities can occur:
(i) $\gcd(a, b) = \gcd(x, y) = 1$;
(ii) $\gcd(a, b) = 17$ and $\gcd(x, y) = 1$;
(iii) $\gcd(a, b) = 1$ and $\gcd(x, y) = 17$;
(iv) $\gcd(a, b) = \gcd(x, y) = 17$.

5 *(6 points).* Suppose that n is composite: an integer greater than 1 that is not prime. Show that $(n-1)!$ and n are not relatively prime. Prove that the congruence $(n-1)! \equiv -1 \bmod n$ is false.

6 *(6 points).* Prove that -1 is not a square modulo the prime p if $p \equiv 3 \bmod 4$.

7 *(6 points).* Show that $x^8 \equiv 1 \bmod 20$ if x is an integer that is prime to 20. Find the integer t such that $t^9 = 760231058654565217 \approx 7.60231 \times 10^{17}$.

Second Midterm Exam — October 28, 1999

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. Don't worry too much about simplifying arithmetical expressions; "$3 \cdot 5 + 1$" is the same answer as "16" in most contexts.

1 *(5 points).* Suppose that n and m are positive integers, that p is a prime and that α is a non-negative integer. Assume that n is divisible by p^α, that m is prime to p and that $F = \dfrac{n}{m}$ is an integer. Show that F is divisible by p^α.

2 *(6 points).* Let $f(x)$ be a polynomial with integer coefficients that satisfies $f(1) = f'(1) = 3$. Calculate the remainder when $f(-18)$ is divided by 19^2.

3 *(5 points).* Determine the number of solutions to the congruence $x^2 + x + 1 \equiv 0 \bmod 7^{11}$.

4 *(6 points).* Find an integer $n \geq 1$ so that $a^{3n} \equiv a \bmod 85$ for all integers a that are divisible neither by 5 nor by 17.

5 *(6 points)*. Find the number of solutions mod 120 to the system of congruences $x \equiv \begin{cases} 2 & \text{mod } 4 \\ 3 & \text{mod } 5 \\ 4 & \text{mod } 6 \end{cases}$.

6 *(7 points)*. If $m = 15709$, we have $2^{(m-1)/2} \equiv 1 \bmod m$ and $2^{(m-1)/4} \equiv 2048 \bmod m$. With the aid of these congruences, one can find quite easily a positive divisor of m that is neither 1 nor m. Explain concisely: how to find such a divisor, and why your method works.

Final Exam — December 14, 1999

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.

Each question is worth 6 points.

1. Let n be an integer greater than 1. Let p be the smallest prime factor of n. Show that there are integers a and b so that $an + b(p-1) = 1$.

2. Using the identity $27^2 - 8 \cdot 91 = 1$, describe the set of all integers x that satisfy the two congruences $x \equiv \begin{cases} 35 & \text{mod } 91 \\ 18 & \text{mod } 27 \end{cases}$.

3. Let $m = 2^2 3^3 5^5 7^7 11^{11}$. Find the number of solutions to $x^2 \equiv x \bmod m$.

4. Calculate $\left(\frac{-30}{p}\right)$, where p is the prime 101. Justify each equality that you use.

5. Write $2 + \sqrt{8}$ as an infinite simple continued fraction.

6. Find the number of primitive roots mod p^2 when p is the prime 257.

7. Express the continued fraction $\langle 6, 6, 6, \ldots \rangle$ in the form $a + b\sqrt{d}$, with a and b rational numbers and d a positive non-square integer.

8. Suppose that $p = a^2 + b^2$, where p is an odd prime number and a is odd. Show that $\left(\frac{a}{p}\right) = +1$. (Use the Jacobi symbol.)

9. Let n be an integer. Show that n is a difference of two squares (i.e., $n = x^2 - y^2$ for some $x, y \in \mathbf{Z}$) if and only if n is either odd or divisible by 4.

10. Let n be an integer greater than 1. Prove that 2^n is not congruent to 1 mod n.