Math 115 Professor K. A. Ribet

Spring Semester, 1998

First Midterm Exam February 25, 1998

Instructions: Answer question #2 and three other questions.

1 *(6 points)*. Find all solutions to the congruence $x^2 \equiv p \bmod p^2$ when p is a prime number.

2 *(9 points)*. Using the equation $7 \cdot 529 - 3 \cdot 1234 = 1$, find an integer x which satisfies the two congruences $x \equiv \begin{cases} 123 & \bmod 529 \\ 321 & \bmod 1234 \end{cases}$ and an integer y such that $7y \equiv 1 \bmod 1234$. (No need to simplify.)

3 *(7 points)*. Suppose that p is a prime number. Which of the $p+2$ numbers $\binom{p+1}{k}$ $(0 \le k \le p+1)$ are divisible by p? [Example: The seven binomial coefficients $\binom{6}{k}$ are 1, 6, 15, 20, 15, 6, 1; the middle three are divisible by 5.]

4 *(7 points)*. Let p be a prime and let n be a non-negative integer. Suppose that a is an integer prime to p. Show that $b := a^{p^n}$ satisfies $b \equiv a \bmod p$ and $b^{p-1} \equiv 1 \bmod p^{n+1}$.

5 *(6 points)*. Show that $n^4 + n^2 + 1$ is composite for all $n \ge 2$.

Last Midterm Exam April 8, 1998

☞ The numbers 257 and 661 are prime.

1 *(5 points)*. Find the number of square roots of 9 modulo $3 \cdot 11^2 \cdot 13^3$.

2 *(5 points)*. Determine whether or not 116 is a square modulo 661.

3 *(5 points)*. Determine whether or not 116 is a cube modulo 661.

4 *(5 points)*. Calculate the number of primitive roots modulo 257^2.

5 *(7 points)*. Express $-\dfrac{15}{47}$ as a continued fraction.

6 *(8 points)*. Let p be a prime number dividing $x^2 + 1$, where x is an even integer. Show that $p \equiv 1 \bmod 4$ and that p is prime to x. Deduce that there are an infinite number of primes congruent to 1 mod 4.

Final Exam May 18, 1998

☞ The numbers 257 and 661 are prime.

1 *(6 points).* Find a positive integer n such that $n/3$ is a perfect cube, $n/4$ is a perfect fourth power, and $n/5$ is a perfect fifth power.

2 *(5 points).* Prove that there are no whole number solutions to the equation $x^2 - 15y^2 = 31$.

3 *(5 points).* Find the number of solutions to the congruence $x^2 \equiv 9 \mod 2^3 \cdot 11^2$.

4 *(7 points).* Which positive integers m have the property that there a primitive root mod m? (Summarize what we know about this question, and why we know it. Your answer should be clear enough that one could use it to decide immediately if there is a primitive root modulo $(257)^2$, $4 \cdot 661$, $257 \cdot 661$, $\ldots$.)

5 *(6 points).* Fermat showed that $2^{37} - 1$ is composite by finding a prime factor p of $2^{37} - 1$ which lies between 200 and 300. Using your knowledge of number theory, deduce the value of p.

6 *(7 points).* The continued fraction expansion of $\sqrt{5}$ is $\langle 2, 4, 4, \ldots \rangle$. If

$$\langle 2, \underbrace{4, 4, \ldots, 4}_{99\ 4'\mathrm{s}} \rangle = h/k$$

(in lowest terms), calculate $h^2 - 5k^2$.

7 *(5 points).* Prove that there are an infinite number of primes congruent to 3 mod 4.

8 *(6 points).* 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 *(8 points).* Let a and b be positive integers. Show that

$$\phi(ab)\phi(\gcd(a, b)) = \phi(a)\phi(b)\gcd(a, b), \qquad \phi = \text{Euler } \phi\text{-function.}$$

(Example: If $a = 12$ and $b = 8$, the equation reads $32 \cdot 2 = 4 \cdot 4 \cdot 4$.)

10 *(5 points).* Find all solutions in integers y and z to the equation $6^2 + y^2 = z^2$.