

Math 115
Final Exam

Professor K. A. Ribet
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.

Note: I compiled this answer sheet by working with an early draft of the exam. As you will note, the order of the questions and the wording of some questions was different in the “release version” of the exam.

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

There are two solutions to $x^2 \equiv x \pmod{p^n}$ (p prime, $n \geq 1$), namely $x = 0$ and $x = 1$. Indeed, these are the only solutions mod p . Further, if x is a mod p^n solution that is 0 mod p , then p is prime to $x - 1$. Since p^n divides $x^2 - x = x(x - 1)$ and is prime to $x - 1$, p^n divides x , so x is 0 mod p^n . Similarly, if x is a solution that is 1 mod p , then x is 1 mod p^n . Once we know what’s going on mod prime powers, we can finish things off by invoking the Chinese Remainder Theorem. In our case, there are five prime powers, so the correct answer should be $2^5 = 32$.

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

Since p is 1 mod 4 and 5 mod 8, $\left(\frac{-30}{p}\right) = -\left(\frac{15}{101}\right)$. Also, the multiplicativity of the Legendre symbol gives $\left(\frac{15}{101}\right) = \left(\frac{5}{101}\right)\left(\frac{3}{101}\right)$. By quadratic reciprocity, the second factor is +1 and the first factor is -1. Thus $\left(\frac{-30}{101}\right) = +1$.

3. Find the continued fraction expansion of $2 + \sqrt{8}$.

Using the definition, you should find $\langle 4, 1, 4, 1, \dots \rangle$.

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

We proved in class that the answer is always $(p-1)\phi(p-1)$. Here we have $256 \cdot 128 = 32768$.

5. 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 $an + b(p-1) = 1$.

The numbers n and $p-1$ are relatively prime. Indeed, if q is a prime dividing $p-1$, then q is smaller than p . Since p is the smallest prime dividing n , q cannot divide n . The

existence of a and b with the required properties follows from the relative primality and the Euclidean algorithm.

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

The numbers 91 and 27 are visibly relatively prime because of the given identity. Thus the answer consists of a single congruence class mod $27 \cdot 91 = 2457$. The number 27^2 is 1 mod 91 and 0 mod 27. The number $-8 \cdot 91$ is 1 mod 27 and 0 mod 91. Hence we want $-8 \cdot 18 \cdot 91 + 35 \cdot 27^2$, which is 126 mod 2457. Needless to say, there's no need to simplify answers in this problem.

7. Let n be an integer greater than 1. Prove that the congruence $2^n \equiv 1 \pmod{n}$ is false.

Suppose that the congruence is true. Then n is clearly odd—since it divides the odd number $2^n - 1$. Let p be the smallest prime factor of n . Then $2^n \equiv 1 \pmod{p}$. Further, p is odd, so $2^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. Since one can express 1 in terms of n and $p - 1$ (as in a previous problem), we have $2^1 \equiv 1 \pmod{p}$. This is impossible.

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

If x is the indicated continued fraction, I find that $x^2 - 6x - 1 = 0$. Thus $x = 3 + \sqrt{10}$.

9. 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.)

Since p is 1 mod 4, we have $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{b^2}{a}\right) = 1$. I guess that I like this problem: I put it on the final exam the last time I taught the course, and I did it out in class this year.

10. 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.

If $n = x^2 - y^2$, then x^2 and y^2 are both either 1 or 0 mod 4. Hence n can be 0 or ± 1 mod 4, but it can't be 2 mod 4. This gives one direction. If $n = 2m + 1$ is odd, then $n = (m + 1)^2 - m^2$. If $n = 4t$ is a multiple of 4, then $n = (t + 1)^2 - (t - 1)^2$.

Hey: this has been a great class! I hope that you all enjoyed it. (I'll find out by reading the course evaluations after I turn in the grade sheets.) Happy Holidays to all—see you soon.