Math 115 Professor K. A. Ribet

Final Exam December 13, 2000

This is a closed-book exam: no notes, books or calculators are allowed. Explain your answers as clearly and as completely as you possibly can. The blue book that you hand in at the end of the exam is your only representative when the exam is graded.

1 *(4 points). Find an integer x such that $x \equiv 7$ mod 37 and $x^2 \equiv 12$ mod 37^2.*

This is a Hensel-type problem, which we can do by hand by writing $x = 7 + 37t$, expanding x^2 mod 37^2, and solving for t mod 37. The good value of t is -8; alternatively we can take $t = 29$. The value of x corresponding to $t = 29$ is 1080. Of course, you need not simplify all the arithmetic.

2 *(5 points). Let n be an odd positive integer. Show that n is a perfect square if and only if $\left(\frac{b}{n}\right) = 1$ for all integers b prime to n.*

We did this in class quite recently. If n is not a perfect square, there's a prime p that divides n to an odd power: say $n = mp^e$ with e odd and m prime to p. There are non-squares mod p. Using the Chinese Remainder Theorem, we take b to be congruent to a non-square mod p and to 1 mod m.

3 *(5 points). Express the infinite continued fraction $[\overline{1,2,3}]$ in the form $\dfrac{a+\sqrt{b}}{c}$ with a, b and c integers.*

If x is the indicated continued fraction, then we have $x = [1, 2, 3, x]$, an expression that simplifies to $\dfrac{10x+3}{7x+2}$. After cross multiplying, we get that $7x^2 - 8x - 3 = 0$. The quadratic formula shows that x is either negative (which it isn't!) or is equal to $\dfrac{4+\sqrt{37}}{7}$. This checks with the numerical value of the continued fraction, which is $1.44039\ldots$.

4 *(6 points). Find a positive integer f so that $x^{271f} \equiv x$ mod $29 \cdot 31$ for all x prime to $29 \cdot 31$.*

This is an "RSA problem" with the cryptography suppressed. We want f so that $271f \equiv 1$ mod $\phi(29 \cdot 31)$. The ϕ-value is $28 \cdot 30 = 840$. On doing a couple of quick divisions, we see that an inverse for 271 mod 840 is 31.

5 *(4 points). Decide whether or not 263 is a square mod 331. (Both numbers are primes.)*

Both 263 and 331 are 3 mod 4. Thus $\left(\frac{263}{331}\right) = -\left(\frac{331}{263}\right) = -\left(\frac{68}{263}\right) = -\left(\frac{17}{263}\right)$, with the latter equality coming from the fact that $68 = 17 \cdot 4$. Similarly,

$$\left(\frac{17}{263}\right) = \left(\frac{263}{17}\right) = \left(\frac{8}{17}\right) = \left(\frac{2}{17}\right) = +1;$$

note that 2 is a square mod 17 because $17 \equiv 1$ mod 8. Thus the answer is "-1".

6 *(5 points). Use the equations*

$$3469 = 2 \cdot 1298 + 873$$
$$1298 = 1 \cdot 873 + 425$$
$$873 = 2 \cdot 425 + 23$$
$$425 = 18 \cdot 23 + 11$$

to write 3469/1298 *as a simple continued fraction.*

We need to continue these Euclidean equations, dividing 11 into 23 to get the quotient 2 and remainder 1 and dividing 1 into 11 to get the quotient 11 and remainder 0. The continued fraction we seek has its a_i equal to the sequence of quotients. It is thus $[2, 1, 2, 18, 2, 11]$.

7 *(6 points). Let p be a prime that is congruent to 1 mod 4. View the quadratic residues (i.e., squares) mod p as integers between 0 and $p-1$. Show that the sum of these integers is $p(\frac{p-1}{4})$. [Example: when p is 5, the residues are 1 and 4. Their sum is 5.]*

The main point is that -1 is a square mod p. Thus if a is a square (or quadratic residue), so is $-a \equiv p-a$. Hence the squares come in pairs, with a paired up with $p-a$. (We don't have $a \equiv p-a$ because then $2a \equiv 0$ and $a \equiv 0$.) Each pair sums to p and there are $\frac{p-1}{4}$ pairs because there are $\frac{p-1}{2}$ residues.

8 *(4 points). If eggs in a basket are taken out 2, 3, 4, 5 and 6 at a time, there are 1, 2, 3, 4 and 5 eggs left over, respectively. If they are taken out 7 at a time, there are no eggs left over. What is the least number of eggs that can be in the basket?*

If x is the number of eggs, then x must be congruent to -1 mod each of 2, 3, 4, 5 and 6. Thus x must be congruent to -1 mod the least common multiple of these numbers. That l.c.m. is 60. On the other hand, x needs to be a multiple of 7. As it happens, $119 = 2 \cdot 60 - 1$ is a multiple of 7. And that's the answer.

9 *(5 points). Show that a positive integer n is a perfect number if and only if $\sum_{d|n} \frac{1}{d} = 2$. If n is a perfect number, show that tn is not a perfect number when $t > 1$.*

The number n is perfect if $2n = \sum_{d|n} d$, i.e., if $2 = \sum_{d|n} \frac{d}{n}$. As d runs over the set of divisors of n, so does n/d. On the other hand, $\frac{n/d}{n} = \frac{1}{d}$. Thus the condition is as stated. Now the divisors of tn include the divisors of n as well as tn. This latter number is not a divisor of n when $t > 1$. Hence the sum for tn is bigger than the sum for n. If the latter sum is 2, the former sum can't be 2 as well.

10 *(6 points). Let n be a positive integer. Suppose that the Fermat number $p = 2^{2^n} + 1$ is prime. Prove that $3^{(p-1)/2} \equiv -1$ mod p.*

The congruence means that 3 is a non-square mod p. Since p is 1 mod 4, quadratic reciprocity translates this condition into the condition that p is a non-square mod 3. Now p is the sum of 1 and an even power of 2; thus $p \equiv 2$ mod 3. This congruence shows that p is a non-square mod 3, as required.