Math 115 Professor K. A. Ribet
Second Midterm Exam April 8, 1998

☞ The numbers 257 and 661 are prime.

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

By the Chinese Remainder Theorem, the answer is the product of the numbers of solutions modulo the three factors 3, 11^2, 13^3. Mod 3, there is clearly only the solution 0. Mod 11, there are two solutions to the equation $x^2 = 9$, namely ± 3. By Hensel's Lemma, each solution lifts to a unique solution mod 11^2. A similar reasoning shows that there are two solutions mod 13^3. In summary, then, the number of square roots is $1 \cdot 2 \cdot 2 = 4$.

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

We want to compute $\left(\frac{116}{661}\right) = \left(\frac{4 \cdot 29}{661}\right) = \left(\frac{29}{661}\right)$. By quadratic reciprocity, we can write this as $\left(\frac{661}{29}\right)$. The value of this Legendre symbol is unchanged if we replace 661 by any number congruent to it mod 29. It's natural to substract off $29 \cdot 20 = 580$ from 661 to get going. But $661 - 580 = 81$, and 81 is a perfect square. So $\left(\frac{661}{29}\right) = +1$, and 116 is indeed a square mod 661.

3 *(5 points). Determine whether or not 116 is a cube modulo 661. Whoops! I meant to ask something easy here. Let's change the problem: determine whether or not 116 is a seventh power modulo 661.*

Since 7 is prime to $661 - 1 = 660 = 2^2 \cdot 3 \cdot 5 \cdot 11$, all elements of $\mathbf{Z}_{661}$ are seventh powers mod 661.

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

Perhaps this is a dumb question. The number of primitive roots mod p is $\phi(p-1)$. The number of primitive roots mod p^2 is $(p-1)\phi(p-1)$. In this case, $p - 1 = 256 = 2^8$ and $\phi(p-1) = 2^7$, so the answer is 2^{15}. If you say basically this you will get full credit. Saying something more, as long as it's correct, is obviously a bit better.

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

I hope that the negative rational number won't throw you. The a_0 is still $[-15/47] = -1$, and then $\xi - a_0 = \dfrac{32}{47}$, so $\xi_1 = 47/32$, and then you just go on autopilot. The answer is apparently $\langle -1, 1, 2, 7, 2\rangle$.

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

This was the first bit of a homework problem. If p divides $x^2 + 1$, then -1 is a square mod p, so p is either 2 or a prime congruent to 1 mod 4. Since x is even, though, $x^2 + 1$ is odd, so p can't be 2. To show that there are an infinite number of ps which are 1 mod 4, you suppose that you have a bunch of them already: $p_1, \ldots, p_t$. Take $x = 2p_1 \cdots p_t$ and form $x^2 + 1$. Any prime which divides this number (which is bigger than 1, so divisible by some prime) will be 1 mod 4 and distinct from $p_1, \ldots, p_t$.