Math 115 Professor K. A. Ribet
Final Exam May 18, 1998

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.*

This was like a homework problem that you had early in the course. Try $n = 3^a 2^b 5^c$ and look for congruences that are imposed on the three exponents. For example, a has to be 1 mod 3 and 0 mod 4 and mod 5; so a could be 40 (Chinese remainder situation). One answer to the question is $3^{40}2^{30}5^{36}$, or 18996352279776451251562500000000000000000000000000000.

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

This is like one of the questions on the "practice final" from 1986. Work mod 31: It's clear that y can't be divisible by 31, because then both x and y would be, and the LHS would be divisible by 31^2. Hence if there's a solution, we find that 15 is a square mod 31. It's not, for instance from the point of view of the Jacobi symbol—since both 15 and 31 are 3 mod 4, we have $\left(\dfrac{15}{31}\right) = -\left(\dfrac{31}{15}\right) = -1$.

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

This is a standard problem like that on the second midterm. You multiply the number of solutions mod 8, which is 4, by the number of solutions mod 11^2, which you find by Hensel's lemma. The latter number is 2, so the answer is 8.

4 *(7 points). Which positive integers m have the property that there is 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 $(257)^2$, $4 \cdot 661$, $257 \cdot 661$, $\ldots$.)*

First, recall the situation when m is a power of a prime: If $m = p^t$ with p odd, then there's always a primitive root mod m. If $m = 2^t$, then there's no primitive root for $t > 2$, but there is a primitive root if $t = 1$ or $t = 2$. If m is not a prime power, then there's never a primitive root mod m except when m has the form $2p^t$ with p odd. The reason is as follows. Suppose that $m = ab$, with a and b relatively prime and $a, b > 1$. A primitive root is a number mod m whose order is $\phi(m) = \phi(a)\phi(b)$. You can think of the number as a pair (x, y) with x mod a and y mod b. The order of (x, y) is the lcm of the orders of x and y, so it's at most $\operatorname{lcm}(\phi(a), \phi(b))$. In order that this order (sorry for pun) be $\phi(a)\phi(b)$, you need $\phi(a)$ and $\phi(b)$ to be relatively prime. This happens almost never, since $\phi(n)$ is even unless it's 1. In the case where $\phi(a)$, say, is 1, we clearly have $a = 2$. In this case, i.e., $m = 2b$ with b odd, it's easy to see that there's a primitive root mod m is there is one mod b. (By the Chinese Remainder Theorem, the system of invertible numbers mod m is the same as the system mod b.)

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.*

Well, we must have $2^{37} \equiv 1 \bmod p$. Thus the order of 2 mod p is 37. This implies that 37 divides $p - 1$, so that p is 1 mod 37. The multiples of 37 in the relevant range are 222, 259, and 296. Hence

p must be one of 223, 260, 297. The last two numbers are visibly not prime; the third, for instance, is a multiple of 3. Hence p must be 223, which it is.

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

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

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

We have $(h, k) = (h_{99}, k_{99})$. A useful formula here is $h_n^2 - dk_n^2 = (-1)^{n+1} q_{n+1}$, which we apply with $n = 99$ and $d = 5$. The answer is that $h^2 - 5k^2$ is q_{100}. After some head-scratching, we remember that $q_n = 1$ precisely when n is a multiple of the period of the continued fraction, which is 1 in this case. So $h^2 - 5k^2 = 1$.

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

We discussed stuff like this in class. If $p_1, \ldots, p_t$ are primes different from 3 which are 3 mod 4, we consider $N = 4p_1 \cdots p_t + 3$. This odd number is divisible by none of the p_i and is prime to 3. The primes which divide it cannot all be 1 mod 4, since then N would be 1 mod 4. Hence N is divisible by some prime which is 3 mod 4 (and different from 3), and we can use this prime to augment our list of such primes.

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.)*

I liked this problem when I saw it discussed in office hours, some weeks back. The point is that $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{b^2}{a}\right)$, the first equality because p is 1 mod 4 and the second because p is b^2 mod a.

9 *(8 points). Let* a *and* b *be positive integers. Show that* $\phi(ab)\phi(\gcd(a, b)) = \phi(a)\phi(b)\gcd(a, b)$*. (Example: If* $a = 12$ *and* $b = 8$*, the equation reads* $32 \cdot 2 = 4 \cdot 4 \cdot 4$*.)*

This is a somewhat ugly problem, for which I semi-apologize. Maybe it's best to realize that both sides are multiplicative in a and b separately, so we can assume that $a = p^n$ and $b = q^m$ are prime powers. If $q \neq p$, then the two sides are both obviously $\phi(a)\phi(b)$. Hence we can assume that $q = p$ and just calculate! By symmetry, we can assume that $n \leq m$, so that $\gcd(a, b) = p^n$. The LHS is then $(p-1)p^{n+m-1} \cdot (p-1)p^{n-1}$, while the RHS is $(p-1)p^{n-1} \cdot (p-1)p^{m-1} \cdot p^n$. If I did this correctly, the two sides are equal.

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

This is a very elementary question. Just write $36 = (z - y)(z + y)$. Clearly, $(z - y)$ and $(z + y)$ are complementary factors of 36; given such factors a and $b = 36/a$, we can solve for y and z—provided that a and b have the same parity. Indeed, if $z - y = a$ and $z + y = b$, then $z = \dfrac{a+b}{2}$ and $y = \dfrac{b-a}{2}$. The possibilities for a seem to be ± 2, ± 6, ± 18. Thus, there should be 6 pairs (y, z). These are $(\pm 8, \pm 10)$, where the signs can be taken independently (4 poss. here), together with $(0, \pm 6)$.