Math 115 Professor K. A. Ribet
First Midterm Exam February 25, 1998

☞ Answer question #2 and three other questions.

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

There are no solutions. Indeed, if x satisfies the congruence, then $x^2 \equiv 0 \bmod p$. Thus p divides x^2, so p divides x and thus p^2 divides x^2. Since we then have $x^2 \equiv 0 \bmod p^2$, we do not have $x^2 \equiv p \bmod p^2$. (Hensel's lemma has nothing to do with this problem: it doesn't apply, so it gives no information.)

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

This is the question that you were more or less promised. I would take x to be $123 \cdot (-3) \cdot 1234 + 321 \cdot 7 \cdot 529$, or 733317; you can reduce this mod 652786, getting 80531 instead. Take y to be 529.

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?*

This was a "frequently omitted" question, but it's reasonably easy. First proof: The formula $\displaystyle\binom{p+1}{k} = \frac{(p+1)!}{k!(p+1-k)!}$ displays $\binom{p+1}{k}$ as a fraction whose numerator is divisible by p but not by p^2 and whose denominator is divisible by p only when k or $p+1-k$ is one of the two numbers p, $p+1$. Hence the coefficient is divisible by p for all k except the values 0, 1, p, $p+1$. Among the $p+2$ numbers in question, $p-2$ of them are divisible by p. Second proof: Think about Pascal's triangle and the fact that all the numbers in the pth row are divisible by p (except for the two 1's at the ends).

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 $b \equiv a$ mod p and $b^{p-1} \equiv 1$ mod p^{n+1}.*

If a is as in the problem, then $a^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem. Thus a is a root mod p of $f(x) = x^{p-1} - 1$. Since $f'(a)$ is then prime to p, a can be refined in exactly one way to a root of $f(x)$ mod p^{n+1}. In other words, there exists a unique b mod p^{n+1} which satisfies $b^{p-1} \equiv 1 \bmod p^{n+1}$ and $b \equiv a$ mod p. The point of this problem is that you can actually exhibit a b that works. Namely, using Fermat's congruence $a^p \equiv a \bmod p$, you easily prove $a^{p^n} \equiv a \bmod p$ by induction. Thus b is indeed the same as a mod p. Also, a is prime to p^{n+1}, so $a^{\phi(p^{n+1})} \equiv 1 \bmod p^{n+1}$. Since $\phi(p^{n+1}) = (p-1)p^n$, this yields $b^{p-1} \equiv 1$ mod p^{n+1}.

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

I added this problem at the last minute, just taking it from the book (problem 33 on page 32). If you calculate two or three of these numbers, you see that they are composite but are not systematically divisible by any particular number. This suggests an algebraic factorization. The point turns out to be that $n^4 + n^2 + 1 = (n^4 + 2n^2 + 1) - n^2$ is a difference of two squares. It's thus the product $\left(n^2 + 1 + n\right)\left(n^2 + 1 - n\right)$. To prove that this is a non-trivial factorization, you have to see that $n^2 - n + 1$ is bigger than 1, but this is easy (graph it, or something).