Mathematics 115 Professor K. A. Ribet

Yet Another Midterm Exam October 27, 2011

Please put away all calculators, cell phones, books, iPads, iPods, laptops, etc., etc. You may consult a single two-sided sheet of notes. Please write carefully and clearly in complete sentences. Take pains to explain what you are doing since the grader cannot read your mind.

The problems have equal weight (6 points each).

This document contains some quick and dirty "answers" written by Ribet. The intention is not to write up model solutions but rather to give a sense of how things should go.

1. Prove that there are infinitely many prime numbers of the form $4k-1$.

This problem is similar to one on the homework due October 27. The idea is to adapt Euclid's proof that there are infinitely many primes. Suppose that we have a bunch of primes p_1, p_2,…, p_t, all congruent to 3 mod 4. To fix ideas, imagine that the sequence is already pretty healthy: let's say that we have $p_1 = 3$, $p_2 = 7$, $p_3 = 11$ and $t \geq 3$. Consider the number

$$N = 4p_1 \cdots p_t - 1,$$

which is congruent to 3 mod 4 and which is divisible by none of the p_i. Let's factor this odd number: $N = q_1 q_2 \cdots q_s$. The primes q_i are all odd, so they are congruent to ± 1 mod 4. They can't all be congruent to $+1$ because then N would be $+1$ mod 4, which it isn't. Thus one of the primes, say q_j, is 3 mod 4. Since N is not divisible by any of the p_i, q_j must be distinct from all the p_i. Therefore it's a new prime that's congruent to 3 mod 4, and we can append it to the list of p_i. We can continue in this manner indefinitely and make an arbitrarily long string of primes that are 3 mod 4. Accordingly, there are infinitely many such primes.

2. Identify the smallest positive integer that is a non-square modulo the prime number $9000000001 = 9 \times 10^9 + 1$.

Let $p = 9000000001 = 9 \times 10^9 + 1$. Since $p \equiv 1$ mod 8, 2 is a square mod p. (So is 1, by the way.) If q is an odd prime, we know that q is a square mod p if and only if p is a square mod q; this follows from the fact that p is 1 mod 4. Clearly p is 1 mod 3 and p is 1 mod 5. Hence all positive integers ≤ 6 are squares mod p. We have

$$\left(\frac{p}{7}\right) = \left(\frac{2 \times 3^9 + 1}{7}\right) = \left(\frac{2 \times 3^3 + 1}{7}\right) = \left(\frac{-1}{7}\right) = -1.$$

Hence 7 is the smallest positive non-square mod p.

3. Let p be the prime number $101 = 10^2 + 1$. Find all square roots of -1 mod p^2.

Since $p = 10^2 + 1$, 10 and -10 are square roots of -1 mod! p. They are *the* square roots because the polynomial $f(x) = x^2 + 1$ can have only two square roots mod p. Because $f'(10) = 20$ and $f'(-10) = -20$ are non-zero mod p, each of the two roots of $f(x)$ lifts uniquely to a root of $f(x)$ mod p^2. Clearly these two lifts are negatives of each other because $-r$ is a root of $f(x)$ (mod anything) if and only if r is a root of $f(x)$ modulo the same number. We just have to find the square root of -1 mod p^2 that lifts 10 and then negate this answer to get the second square root of -1.

The general formula (à la Hensel) is that

$$a - \frac{f(a)}{f'(a)}$$

is a root of $f(x)$ mod p^2 lifting a mod p as long as $f(a) \equiv 0$ mod p and $f'(a) \not\equiv 0$ mod p. These conditions are satisfied when $f(x) = x^2 + 1$ and $a = 10$. We have in this case $f(a) = p$ and $1/f'(a) = 1/20 = -5$; this reciprocal needs to be calculated only mod p. If I'm not mistaken,

$$a - \frac{f(a)}{f'(a)} = 515$$

in our case. This seems to be correct since $515^2 + 1 = 2 \cdot 13 \cdot 101^2$. Summary: the two square roots of -1 mod p^2 are ± 515.

4. Let $N = 259 = 7 \times 37$. How many roots does the polynomial $x^{36} - 1$ have modulo N? How many roots does the polynomial $x^9 - 1$ have modulo N?

If a positive power of a number a mod N is 1, then a is invertible mod N. So this problem is really about $(\mathbf{Z}/\mathbf{NZ})^*$, which can (and almost certainly should) be viewed as $(\mathbf{Z}/\mathbf{7Z})^* \times (\mathbf{Z}/\mathbf{37Z})^*$. In other words, I hope that you brought the Chinese Remainder Theorem into the exam room with you. When we think of elements of $(\mathbf{Z}/\mathbf{NZ})^*$ as pairs (a, b) with $a \in (\mathbf{Z}/\mathbf{7Z})^*$ and $b \in (\mathbf{Z}/\mathbf{37Z})^*$, we see that the number of solutions to $x^{36} = 1$ (for instance) in $\mathbf{Z}/\mathbf{NZ}$ is the product of the number of a such that $a^{36} = 1$ and the number of b such that $b^{36} = 1$. In fact, by Fermat's little theorem, $a^6 = 1$ for all a and $b^{36} = 1$ for all b. Hence $x^{36} - 1$ has $(7 - 1)(37 - 1) = 216$ roots mod N. Now how many a satisfy $a^9 = 1$? These are the a such that $a^3 = 1$; such a are exactly the squares mod 7, and there are three of them. How many b satisfy $b^9 = 1$? There are 9 such b, as we can see in various ways, for example by Corollary 2.42 on page 104 of the textbook. (The b in question are the powers of g^4, where g is a generator mod 37.) The number of 9th roots of 1 mod N is $3 \times 9 = 27$.

5. Suppose $p > 3$ is a prime $\equiv 3 \bmod 4$ for which $P = 2p + 1$ is also a prime; for example, we could have $p = 11$ or $p = 23$ (so that P would be 23 or 47).

a. Explain why we have $2^{(P-1)/2} \equiv 1 \bmod P$.

The congruence means that 2 is a square mod P (Euler's criterion). We know that 2 is a square mod an odd prime if and only if the prime is ±1 mod 8. Our P is 7 mod 8, so it qualifies.

b. Deduce that $2^p - 1$ is not prime.

By part (a), $2^p - 1 = 2^{(P-1)/2} - 1$ is divisible by P. Thus we will know that $2^p - 1$ is composite as soon as we know that $(2^p - 1)/P \neq 1$. The equality $(2^p - 1)/P = 1$ would translate to

$$2p + 1 = 2^p - 1,$$

which looks kind of absurd. It is correct for $p = 3$ (which we excluded), in which case both sides of the equation are 7. To get a contradition, it would be enough to prove $2^n > n + 2$ for $n \geq 3$ because we could plug in $p - 1$ for n and get $2^{p-1} > p + 1$, $2^p > 2p + 2$ and then $2^p - 1 > 2p + 1$. I checked quickly that $2^n > n + 2$ comes easily by induction on n.