Mathematics 115 Professor K. A. Ribet

Final Examination December 14, 2012

Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in *complete sentences*. Be careful to explain what you are doing since your exam book is your only representative while you are snowboarding.

(6 pts.) **1.** Find the number of primitive roots mod 101^4.

First of all, it's helpful to know that 101 is a prime number. I am hoping that you will either recognize 101 as a prime or else notice that 101 isn't divisible by any of the 2, 3, 5, 7. (This suffices as a check because $11 > \sqrt{101}$.) When p is an odd prime, the number of primitive roots mod p is $\varphi(p-1)$; the number of primitive roots mod p^2 is $(p-1)\varphi(p-1)$. The number of primitive roots mod p^n ($n \geq 2$) is $p^{n-2}(p-1)\varphi(p-1)$. In our case, $n = 4$, $p - 1 = 100$, $\varphi(p-1) = 40$; the answer seems to be $101^2 \cdot 100 \cdot 40$. There is no need to multiply out this product. If you do, odds are that you'll get 40804000. By the way, this number is $\varphi(\varphi(101^4))$.

(8 pts.) **2.** Prove that there are infinitely many primes congruent to 2 mod 3.

It's perhaps easier to prove that there are infinitely many *odd* primes congruent to 2 mod 3. The argument is a variant of Euclid's: Assume that $p_1, ..., p_t$ are such primes and consider

$$P = 3p_1 \cdots p_t + 2,$$

which is not divisible by 2, 3 or any of the p_i. It's 2 mod 3 and therefore must be divisible by an odd number of primes $\equiv 2$ mod 3. We can add the smallest such prime factor of P to our list. Since we can go on like this forever, there are an infinite number of odd primes that are congruent to 2 mod 3. To illustrate the argument numerically, we take 2, 5, 11, 17, 23, 29, 41, 47, 53 and 59 as our primes $p_1, \ldots, p_t$ and get $P = 11273747286617 = 719027 \cdot 15679171$. The first factor is 2 mod 3, while the second is 1 mod 3. We add 719027 to the list 2, 5, 11, 17, 23, 29, 41, 47, 53 and 59 and go back to the formation of the product.

(8 pts.) **3.** Let p be the nth Fermat number $2^{2^n} + 1$. Show that $2^p \equiv 2$ mod p.

Mod p, we have $2^{2^n} \equiv -1$; squaring both sides, we get $2^{2^{n+1}} \equiv 1$ mod p. We are asked to prove $2^{p-1} \equiv 1$ mod p, so it's enough to see that $p-1$ is a multiple of 2^{n+1}, i.e., that $p \equiv 1$ mod 2^{n+1}. But we know $p \equiv 1$ mod 2^{2^n}, so it suffices to check that 2^{n+1} divides 2^{2^n}. The divisibility amounts to the inequality $n + 1 \leq 2^n$, which one can check in various ways, for example by writing $2^n = (1+1)^n$ as a sum of $n+1$ binomial coefficients, all ≥ 1.

This problem gave students a lot of trouble. It's not a good idea to try to prove that p is prime because the fifth number $2^{32} + 1$ is divisible by 641. It's also not fruitful to use induction since different Fermat numbers are relatively prime. (You can't deduce a divisibility by 17 from a divisibility by 5, for instance.)

(5 pts.) **4.** Determine whether or not 1097 is a square modulo the prime number 1103.

Because 1103 is a prime, 1097 is a square modulo 1103 if and only if $\left(\frac{1097}{1103}\right) = 1$. (Note: it turns out that $\left(\frac{1097}{1103}\right) = -1$. We can of course infer from this that 1097 is *not* a square mod 1103 without the information that 1103 is prime.) Since 1097 is 1 mod 4,

$$\left(\frac{1097}{1103}\right) = \left(\frac{1103}{1097}\right) = \left(\frac{6}{1097}\right) = \left(\frac{2}{1097}\right)\left(\frac{3}{1097}\right).$$

Because $1097 \equiv 1 \bmod 8$, the first factor is 1. By quadratic reciprocity, we can switch the "numerator" and "denominator" in the second factor. The second factor is thus seen to be -1 because $1097 \equiv 2 \bmod 3$. Hence the product is -1 and we conclude that 1097 is *not* a square mod 1103.

(7 pts.) **5.** If n is a positive integer, establish the congruence

$$(4n+1)^2 \equiv 1 \bmod n(2n+1).$$

Let p and q be the prime numbers 509 and 1019. Find all the square roots of 1 mod pq, explaining why your list is complete. (You can leave your answers in the form of unsimplified arithmetic expressions, things like $2 \times 3 - 17$.)

We have $(4n+1)^2 = 16n^2 + 8n + 1 = 8(n(2n+1)) + 1 \equiv 1 \bmod n(2n+1)$. Thus $4n+1$ and its negative are square roots of 1 mod $n(2n+1)$. To this list of square roots of 1, we can add 1 and -1. When $n = 509$, $2n + 1 = 1019$. These numbers are distinct primes, so there are exactly four square roots of 1 modulo $n(2n+1)$. Numerically, these square roots are ± 1 and ± 2037.

(7 pts.) **6.** If $1 \leq k \leq n$, prove that the number of partitions of n into k parts coincides with the number of partitions of n in which all parts are $\leq k$ and at least one part is equal to k.

See Theorem 10.3 on page 448 and the proof of the theorem. The point is that partitions with the first property are the conjugates of the partitions with the second property.

(6 pts.) **7.** Let p be an odd prime and let c be a non-zero integer mod p.

a. For each $a \in (\mathbf{Z}/\mathbf{pZ})^*$, show that there is exactly one such pair $(x, y) \in \mathbf{Z}/\mathbf{pZ} \times \mathbf{Z}/\mathbf{pZ}$ satisfying $x^2 - y^2 = c$ and $x - y = a$.

b. Find the number of pairs (x, y) such that $x^2 - y^2 = c$.

If $x - y = a$, to say that $x^2 - y^2 = c$ is to say that $x + y = ca^{-1}$. Using the techniques of Math 54 (or high school algebra), we can solve the pair of equations

$$x - y = a, \qquad x + y = ca^{-1}$$

to find unique values of x and y when a is given. (This works because we can divide by 2; remember that p is an odd prime.) Hence the number of possible "pairs" as in the problem is the number of possible as, namely $p-1$. What's going on here is that there are $p+1$ points on the curve $x^2 - y^2 = c$ in the *projective* plane over $\mathbf{Z}/\mathbf{pZ}$. However, two of these points are "points at infinity," so that there remain exactly $p-1$ points in the regular old affine plane. It's interesting to contrast the situation with $x^2 + y^2 = 1$, where there are again $p+1$ projective points but the number of points at infinity depends on the residue class of p mod 4.

(7 pts.) **8.** Find the sum of the points $(2,3)$ and $(-1,0)$ on the elliptic curve $y^2 = x^3 + 1$.

We find the sum by the chord and tangent process. The line joining $(2,3)$ and $(-1,0)$ has equation $y = x + 1$. If (x,y) lies both on the line and on the elliptic curve, we have $x^3+1 = y^2 = (x+1)^2 = x^2+2x+1$ and $y = x+1$. The equation $x^3+1 = x^2+2x+1$ simplifies to $x^3 - x^2 - 2x = 0$. The cubic on the left has roots -1, 0 and 2. The first and third roots correspond to the two points that were given initially, while the root 0 corresponds to $(0,1)$, which is on both the line and the curve. The sum of $(2,3)$ and $(-1,0)$ is then the point gotten by reflecting $(0,1)$ through the x-axis, which is $(0,-1)$.

Happy Holidays—have a great break! I enjoyed getting to know you; please keep in touch.