Math 250A, Fall 2004
Homework Assignment #9
Problems due November 16, 2004

The assignment consisted of five problems from Lang's Chapter IV. I hope that you were all OK with these problems. They are not easy, in the main, but they were intended to be instructive.

3. Think about how to prove Taylor's theorem for polynomials in the context of Math 1A. Suppose that a is a constant and x is a variable, and let f be a polynomial. We have $f(x+a) = \sum_i c_i x^i$, and we want to determine the c_i. We differentiate repeatedly with respect to x and set $x = 0$ each time. If we differentiate zero times, and just set $x = 0$, we find that $f(a) = c_0$. If we differentiate once and set $x = 0$, we get that $f'(a) = 1 \times c_1$. At the kth stage, we get that $f^{(k)}(a) = k! c_k$. A problem is that we need to know that the kth derivative of $f(x+a)$ is really $f^{(k)}(x+a)$. In calculus, we might see this by invoking the chain rule. For polynomials, we can check directly that differentiation with respect to x commutes with translation by a. For this, by linearity we can assume that the polynomial is x^n and check use the binomial theorem to check that the derivative with respect to x of $(x+a)^n$ is really n times the polynomial $(x+a)^{n-1}$.

In our context, we think of the coefficient ring as $k[y]$ and apply what I said in the paragraph above. We have $f(x+y) = \sum_i c_i(y) x^i$ and will discover that $i! c_i(y) = f^{(i)}(y)$. This is the formula of the problem, except that Lang uses upper-case letters X and Y and has the two variables permuted. In other words, his Y is my x and his X is my y.

5. If $f(x) = x^4 + 1$, then $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ is Eisenstein at 2 and is therefore irreducible. Thus $f(x)$ is irreducible as well. Similarly, $(x+1)^6 + (x+1)^3 + 1 = 3 + 9x + 18x^2 + 21x^3 + 15x^4 + 6x^5 + x^6$ is Eisenstein at 3. A cubic polynominal has a factor of degree 1 if it has a non-trivial factor; but factors of degree 1 yield roots! The only possible roots of $x^3 - 5x^2 + 1$ are ± 1 by what Lang calls the integral root test (p. 185). Since these are not in fact roots (even mod 2), the polynomial is irreducible.

I see that I'm using a lower-case x instead of Lang's X; sorry.

For $X^2 + Y^2 - 1$ over $\mathbf{C}$, it is helpful to regard $\mathbf{C}[X,Y]$ as the ring of polynomials in X over $\mathbf{C}[Y]$. The quadratic polynomial $X^2 + (Y^2 - 1)$, which I view as having coefficients in $\mathbf{C}[Y]$, has content 1: there is no non-constant polynomial in Y that divides both 1 and $Y^2 - 1$! Also, it is irreducible as a polynomial over the field $\mathbf{C}(Y)$ because it is Eisenstein at the prime $Y - 1$. Hence it is irreducible in $\mathbf{C}[X,Y]$.

6. Look at the bottom of page 185. If b/d is a root of $f(X)$, then

$$a_n b^n + a_{n-1} b^{n-1} d + \cdots + a_0 d^n = 0.$$

It follows that b divides $a_0 d^n$. If b is prime to d, then b divides a_0. Similarly, d divides a_n.

7. Prelude on notation: k is a finite field in this problem. Let p be the characteristic of k. Then the number of elements in k is some power of p. The letter "q" is a traditional symbol for this power of p.

Assume that f is zero at the origin of k^n but not elsewhere on k^n. As suggested by Lang, we look at $1 - f^{q-1}$, a polynominal of degree $d(q-1)$ that induces on k^n the characteristic function of the origin. This is the same function that we get from the product $(1 - X_1^{q-1}) \cdots (1 - X_n^{q-1})$. It follows that the two polynominals must have the same *reductions*: You get the *reduction* of a polynomial by lowering all exponents that you see until they're at most $q-1$; you do this by using that X_i^q is the same as X_i as far as values are concerned. (See page 177 of our text.) The polynomial $(1-X_1^{q-1}) \cdots (1-X_n^{q-1})$ is its own reduction; its degree is $n(q-1)$. (The degree of a monomial is the sum of the exponents in it; the degree of a non-zero polynomial is the maximum of the degrees of the monomials that appear in it.) The polynomial $1 - f^{q-1}$ has degree $d(q-1)$, where d is the degree of f. Thus the reduction of $1 - f^{q-1}$ has degree at most $d(q-1)$. We get $n(q-1) \leq d(q-1)$, which contradicts the hypothesis $n > d$. Hence f, if zero at 0, must have at least one other zero.

On to part (b). Note that $x^{q-1} = 1$ for all $x \in k^*$ by Lagrange's theorem in finite group theory. For $i > 0$, x^i is then the same thing as x^j where $j = i \pmod{q-1}$ is the remainder on dividing i by $q-1$. Thus x^j is identically 1 if j is a multiple of $q-1$, whereas x^j is not identically 1 if j is not a multiple of $q-1$. (If i is positive but less than $q-1$, $x^i - 1$ cannot have $q-1$ roots in k.) If j is a multiple of $q-1$, then $\sum_{x \in k} x^j$ is then the sum of $q-1$ 1's, so it's $q-1 = -1$ in k. If j is not a multiple of $q-1$, then there is $y \in k$ so that $y^j \neq 1$. We have $\sum_{x \in k} x^j = \sum_{x \in k} (yx)^j = y^j \sum_{x \in k} x^j$, so that $(1 - y^j) \sum_{x \in k} x^j = 0$. Since $(1 - y^j)$ is non-zero, this forces the sum to vanish. We have now gotten to the last line of page 213.

So $\psi(i)$ will now be $\sum_{x \in k} x^i$, which we have just computed to be -1 or 0. If we have a tuple of integers $(i_1, \cdots, i_n)$, when the displayed sum $\sum_{x_1, \cdots, x_n} x_1^{i_1} \cdots x_n^{i_n}$ is the product of n different single sums that we have evaluated; the value of the n-fold sum is $\psi(i_1) \cdots \psi(i_n)$, as we were required to show. Further, $f(x)^{q-1}$ is 1 if $f(x)$ is non-zero but 0 if $f(x) = 0$. Hence the sum $\sum_{x \in k^{(n)}} \left(1 - f(x)^{q-1}\right)$ does indeed count the number of zeros of f. The sum is a number in k that represents the image of N (the number of zeros of f) in k. Thus it gives us N mod p, where p is the characteristic of k. Since $\sum_{x \in k^{(n)}} 1 = q^n \equiv 0 \bmod p$, we have the simpler congruence $N \equiv -\sum f(x)^{q-1}$. To prove that p divides N, we have to show that this sum is 0 in k.

Write $f(x)^{q-1} = f(x_1, \cdots, x_n)^{q-1}$ as a polynomial $\sum_{(i_1, \cdots, i_n)} a_{i_1, \cdots, i_n} x_1^{i_1} \cdots x_n^{i_n}$. After we sum this sum over tuples $(x_1, \cdots, x_n)$, we will get essentially $\sum_{(i_1, \cdots, i_n)} a_{i_1, \cdots, i_n} \psi(i_1) \cdots \psi(i_n)$. The only wrinkle here is that the sum $\sum_{(x_1, \cdots, x_n)} x_1^{i_1} \cdots x_n^{i_n}$ is clearly 0 in k if one of the i_j is 0;

indeed, the sum becomes q times a lower-dimensional sum. Hence we can and will confine our attention to tuples $(i_1, \cdots, i_n)$ where all of the i_j are positive. Now the product $\psi(i_1) \cdots \psi(i_n)$ can be non-zero only when each i_j is divisible by $q-1$. Since the i_j are going to be positive, the divisibility implies the inequality $i_j \geq q-1$ for each index j. Since the sum of the i_j is at most the degree of f^{q-1}, which is $q-1$ times the degree of f, we can get a non-zero contribution to the sum only when the the degree of f is at least the sum of variables. We are assuming however, that $n > d$, i.e., that the number of variables is greater than the degree. Hence $\sum_x f(x)^{q-1}$ is zero in k. We are finished with part (b) now, I think.

For part (c), we have polynomials $f_1, \ldots, f_r$. We consider $P := (1 - f_1^{q-1}) \cdots (1 - f_r^{q-1})$ instead of $1 - f^{q-1}$. This product is 1 at a point if and only if all f_i are zero there. Hence the number of common zeros of the f_i is measured mod p by the sum $\sum_{x \in k^n} P(x)$. The argument works as before: the degree of $P(x)$ is $q-1$ times the sum of the degrees of the f_i and therefore is less than $(q-1)n$. Accordingly, when we expand out and sum as in part (b), we get 0.

For part (d), we note that the product polynomial introduced in part (a) represents the characteristic function of the origin in k^n. By replacing $(x_1, \ldots, x_n)$ by $(x_1 - a_1, \ldots, x_n - a_n)$, we can realize as a polynomial function the characteristic function of an arbitrary n-tupe $(a_1, \ldots, a_n)$ in k^n. Every function is a k-linear combination of such characteristic functions, so we can realize each function as a polynomial.

18. Let $x = X$. (It's easier to type lower-case letters.) For part (a), we could consider the polynomial $x(x-1)/2$, for example. More generally, let $\binom{x}{r}$ be the binomial polynomial defined in part (b). Then $\binom{x}{r}$ is well known to be an integer when x is a non-negative integer. This means, concretely, that $r!$ divides $i(i-1)\cdots(i-r+1)$ when i is positive. Since this divisibility only depends on i mod $r!$, it'll hold for all integers i.

For part (b), it's helpful to introduce the Δ-operator as in part (c), except I prefer the slightly different definition $(\Delta f)(n) := f(n+1) - f(n)$. (I find it forward-looking.) If $f(x) = \binom{x}{i}$, then Δf is $\binom{x}{i-1}$ for i positive, while $\Delta f = 0$ when $i = 0$.

When P is a rational polynomial of degree r, we can write

$$P(x) = c_0 \binom{x}{r} + c_1 \binom{x}{r-1} + \cdots c_r$$

as desired, except that the coefficients c_i are a priori rational numbers. (The binomial polynomials of degree $\leq d$ clearly form a basis for the $\mathbf{Q}$-vector space of rational polynomials of degree at most d.) Assume that P takes integer values on positive integers. We have $c_i = (\Delta^i P)(0)$ for each i. Since the right-hand side is an integer, $c_i \in \mathbf{Z}$. It follows

from this that P takes integral values on all integers, since $\binom{x}{i}$ has this property for all i. We've proved that a polynomial with integer values on positive integers takes integer values on all integers; from this, it follows by translating x that a polynomial that takes integer values on all sufficiently large integers must take integer values on all integers. This completes the proof of part (b).

In part (c), we know by (b) that Δf can be written (for sufficiently large n, but let's ignore this complication for the sake of simplicity) as a linear combination of binomial coefficients $\binom{x}{i}$. But $\binom{x}{i} = (\Delta F)(x)$ with $F(x) = \binom{x}{i+1}$. Hence we can write $\Delta f = \Delta G$, where G is a linear combination of binomial coefficients $\binom{x}{i+1}$ (and therefore an integral-valued polynomial). It follows by an easy argument that $f(n) - f(0) = G(n) - G(0)$ for all $n \in \mathbf{Z}$. Said differently, this equation states that f and G differ by a constant. After adding a constant to G, we get $f = G$.