Math 437/537—Group Work #3
Tuesday, October 1, 2024

1. Prove Hensel's lemma: Let $f(x)$ be a polynomial with integer coefficients, and let p^j be a prime power. Suppose that $a \in \mathbb{Z}$ satisfies

$$f(a) \equiv 0 \pmod{p^j} \text{ and } f'(a) \not\equiv 0 \pmod{p}.$$

Prove that there exists a unique integer t with $0 \le t < p$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$. Find a formula for that integer t. You may use the statements in #2(a) and #2(b) below.

Using equation (1) below with $h = tp^j$,

$$f(a + tp^j) = \sum_{k=0}^{d} (tp^j)^k \frac{f^{(k)}(a)}{k!} = f(a) + tp^j f'(a) + \sum_{k=2}^{d} (tp^j)^k \frac{f^{(k)}(a)}{k!}$$
$$\equiv f(a) + tp^j f'(a) \pmod{p^{j+1}},$$

since each remaining summand is a multiple of p^{2j} and hence of p^{j+1} (since $j \ge 1$). To have $f(a+tp^j) \equiv 0 \pmod{p^{j+1}}$, we must therefore have $f(a)+tp^j f'(a) \equiv 0 \pmod{p^{j+1}}$, or equivalently

$$\frac{f(a)}{p^j} + tf'(a) \equiv 0 \left(\text{mod } \frac{p^{j+1}}{p^j}\right)$$

by Theorem 2.3(1); note that we are assuming that $\frac{f(a)}{p^j}$ is an integer. Since we are also assuming that $f'(a) \not\equiv 0 \pmod{p}$, the integer $f'(a)$ is relatively prime to p (since p is prime) and therefore invertible modulo p, and we can solve for t:

$$t \equiv -(f'(a))^{-1} \frac{f(a)}{p^j} \pmod{p}.$$

All of our manipulations were equivalences, so this t is a solution and is the only solution modulo p.

[Side observation: starting from the root $a \pmod{p^j}$, the root $\pmod{p^{j+1}}$ that we construct is

$$a + tp^j = a - (f'(a))^{-1} \frac{f(a)}{p^j} p^j = a - (f'(a))^{-1} f(a).$$

Note that this is the exact same formula as in Newton's method for improving approximations of roots of differentiable functions! There's a sense in which Hensel's lemma truly is the same as Newton's method, but over the p-adic numbers rather than over the real numbers.]

(continued on next page)

2. *Concerning polynomials with integer coefficients:*

(a) *Let $f(x) \in \mathbb{Z}[x]$ have degree d. Then for any $a, h \in \mathbb{Z}$, prove that*

$$f(a+h) = f(a) + hf'(a) + h^2\frac{f''(a)}{2!} + \cdots + h^d\frac{f^{(d)}(a)}{d!}. \tag{1}$$

(Hint: with a fixed, consider both sides as polynomials in the variable h.)

(b) *Let $f(x) \in \mathbb{Z}[x]$, and let $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. Show that $\dfrac{f^{(k)}(a)}{k!}$ is an integer. You may use the statement in #2(c) below.*

(c) *Prove that the product of any k consecutive integers is a multiple of $k!$. (Note that the following is* not *a valid proof: each individual integer between 1 and k divides the product of k consecutive integers, and thus $1 \cdot 2 \cdots k$ must as well. Why is this proof invalid?) Hint for one possible proof: for any prime p, compare the power of p dividing $k!$ with the power of p dividing the product of consecutive integers.*

(a) Let $g_a(h)$ denote the polynomial on the right-hand side of equation (1); we want to prove that $f(a+h) = g_a(h)$. We easily see that $f(a+0) = f(a) = g_a(0)$. Also, note that $g_a'(h) = f'(a) + h(\text{something})$, and so $g_a'(0) = f'(a) = f'(a+h)$. More generally, for any $j \le d$, the first j terms on the right-hand side vanish when we take the dth derivative; thus

$$\begin{aligned} g_a^{(j)}(h) &= \sum_{k=j}^{d} k(k-1)\cdots(k-j+1)h^{k-j}\frac{f^{(k)}(a)}{k!} \\ &= \frac{f^{(j)}(a)}{j!} + h\sum_{k=j+1}^{d} h^{k-j-1}\frac{f^{(k)}(a)}{(k-j)!} \end{aligned}$$

and so $g_a^{(j)}(0) = f^{(j)}(a) = f^{(j)}(a+0)$. In other words, the two polynomials degree-d polynomials $g_a(h)$ and $f(a+h)$ are equal at $h=0$ and have equal 1st, 2nd, ..., dth derivatives at $h=0$, which implies that they are the same polynomial.

Alternately, one may proceed by induction on d, the case $d=0$ being trivial. If the statement is true for degree-d polynomials, let $F(x)$ be a degree-$(d+1)$ polynomial, and write $G_a(h)$ for the right-hand side of equation (1) with f replaced by F. Then $G_a(0) = F(a) = F(a+0)$ as before. Moreover, if we set $f(x) = F'(x)$ and $g_a(h)$ to be the polynomial on the right-hand side of equation (1) (for f) as above, then one can check that $G_a'(h) = g_a(h)$. By the induction hypothesis, equation (1) holds for $f(a+h)$ and $g_a(h)$. Therefore we see that $F(a+h)$ and $G_a(h)$ have the same value at $h=0$ and have the same polynomial as their derivatives, hence must be equal. (In fact, this is really the same proof as above, phrased in terms of induction.)

(b) If $f(x) = \sum_{k=0}^{d} c_k x^k$ for some integers c_k, then

$$\frac{f^{(j)}(a)}{j!} = \sum_{k=j}^{d} c_k\frac{k(k-1)\cdots(k-j+1)}{j!}a^{k-j};$$

the fractions inside the sum are all integers by part (c), and so each $\frac{f^{(j)}(a)}{j!}$ is an integer.

(continued on next page)

(c) (The parenthetical proof is invalid because we cannot conclude, from the fact that a and b both divide m, that their product ab automatically divides m. We would need $(a, b) = 1$ to make this deduction. Since the numbers $1, 2, \ldots, k$ are not pairwise relatively prime for $k \geq 4$, this proof isn't valid.)

Given k consecutive integers, which we write as $n+1, n+2, \ldots, n+k$, let $G = (n+1)(n+2)\cdots(n+k)$ denote their product. To prove that $k! \mid G$, it suffices to show that $v_p(k!) \leq v_p(G)$ for every prime p, where v_p was defined in problem #3 of Homework 1. (Verify that in fact $a \mid b$ if and only if $v_p(a) \mid v_p(b)$ for all primes p.) On Homework 1, you learned that

$$v_p(k!) = \sum_{j=1}^{\infty} \left\lfloor \frac{k}{p^j} \right\rfloor.$$

(In fact you can truncate this "infinite" sum explicitly, but since all but finitely many terms equal 0, this form is also fine.) This implies that

$$v_p(G) = v_p\left(\frac{(n+k)!}{n!}\right) = v_p((n+k)!) - v_p(n!) = \sum_{j=1}^{\infty} \left(\left\lfloor \frac{n+k}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^j} \right\rfloor \right).$$

Therefore, to show that $v_p(k!) \leq v_p(G)$ it suffices to show that for every prime p,

$$\left\lfloor \frac{k}{p^j} \right\rfloor \leq \left\lfloor \frac{n+k}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^j} \right\rfloor.$$

But this isn't too hard: note that

$$\left\lfloor \frac{k}{p^j} \right\rfloor + \left\lfloor \frac{n}{p^j} \right\rfloor \leq \frac{k}{p^j} + \frac{n}{p^j} = \frac{n+k}{p^j};$$

and since the left-hand side is an integer, it must be less than or equal to the greatest integer less than or equal to the right-hand side—that is,

$$\left\lfloor \frac{k}{p^j} \right\rfloor + \left\lfloor \frac{n}{p^j} \right\rfloor \leq \left\lfloor \frac{n+k}{p^j} \right\rfloor,$$

which is what we need.

(Now, after all that, let me surprise you with a one-line proof: $k!$ divides G because the binomial coefficient $\binom{n+k}{k} = \frac{G}{k!}$ is always an integer!)