ANALOGIES BETWEEN Z AND $F[T]$: HOMEWORK 5

KEITH CONRAD

The Mason–Stothers theorem and the *abc* conjecture.

1. Let $f, g \in \mathbf{C}[T]$ be nonconstant and relatively prime.

a) If $f^3 - g^2 \neq 0$, show $\deg(f^3 - g^2) \geq (1/2)\deg f + 1$, or equivalently $\deg f \leq 2(\deg(f^3 - g^2) - 1)$.

b) Find infinitely many examples where equality occurs in the conclusion of part a. Start with an example where $\deg f = 3$ and $\deg g = 2$.

c) When the hypothesis of relative primality is dropped, is part a still true?

d) Find a lower bound on $\deg(f^3 - g^2)$ in terms of $\deg g$.

2. Assume the *abc* conjecture for some ε. Show there is a constant C_ε such that, for each integer $d \neq 0$, any solution to the equation $y^2 = x^3 + d$ in relatively prime integers x and y has $|x| \leq C_\varepsilon |d|^{2(1+\varepsilon)/(1-5\varepsilon)}$ and $|y| \leq C_\varepsilon |d|^{3(1+\varepsilon)/(1-5\varepsilon)}$. Of course, C_ε depends on ε, but it does not depend on d. (The exponents can be written more simply as $2(1+\varepsilon')$ and $3(1+\varepsilon')$, but ε' is not the ε for which we are assuming the *abc* conjecture.) Can you remove the condition that x and y are relatively prime?

3. Show $\varepsilon = 0$ does not work in the *abc*-conjecture by considering $a = 3^{2^n} - 1$, $b = 1$, and $c = 3^{2^n}$ for large n, or by considering $a = 2^{p(p-1)} - 1$, $b = 1$, and $c = 2^{p(p-1)}$ for large primes p. To start, show $a \equiv 0 \bmod 2^n$ in the first case and $a \equiv 0 \bmod p^2$ in the second case. After showing the need for ε in the *abc* conjecture, use either of these examples to show $\kappa_\varepsilon \to \infty$ as $\varepsilon \to 0$.

4. For relatively prime $a, b \geq 1$, set $c = a + b$ and

$$L(a,b) = \frac{\log c}{\log(\mathrm{rad}(abc))}.$$

For example, $L(23, 25) = \log(48)/\log(690) \approx .59226$ and $L(3, 125) = \log(128)/\log(30) \approx 1.42657$.

a) Show the *abc* conjecture is equivalent to: for any $t > 1$, there are only finitely many relatively prime integers $a, b \geq 1$ such that $L(a, b) > t$.

In particular, this means there is a largest value of $L(a, b)$ when $(a, b) = 1$. The largest known value is due to Eric Reyssat (1987): $L(2, 3^{10} \cdot 109) \approx 1.62991$. (What is the factorization of c?)

b) If you have had an analysis course, use either family of examples in exercise 3 to prove

$$\varlimsup_{\substack{\gcd(a,b)=1 \\ a,b \geq 1}} L(a,b) \geq 1,$$

where $\varlimsup$ means "lim sup." Then prove the *abc* conjecture is equivalent to

$$\varlimsup_{\substack{\gcd(a,b)=1 \\ a,b \geq 1}} L(a,b) = 1.$$

5. Use the Mason–Stothers theorem to show $u^2 - (T^4 + T^3)v^2 = 1$ has no nontrivial solutions u, v in $\mathbf{Q}[T]$. Can there be solutions in $\mathbf{C}[T]$? What does the Mason–Stothers theorem tell you about nontrivial solutions in $\mathbf{F}_5[T]$? You found a nontrivial solution in Homework 3.

6. Let S be a finite nonempty set of (monic) irreducibles in $F[T]$. We will say a polynomial in $F[T]$ is *supported* in S if its prime factors all lie in S. For example, $T^3 - T^2$ is supported in S when T and $T - 1$ are in S. Any nonzero constant is supported in S, for any S.

We consider the equation

$$f(T) + g(T) = h(T)$$

where $f, g, h \in F[T]$ are supported in S. That is, we restrict the possible irreducible factors of f, g, and h, but we do not restrict the multiplicities of these factors.

a) When $F = \mathbf{F}_p$, show there are only finitely many relatively prime solutions to the above equation which are supported in S and are *not* p-th powers. (Hint: Bound the degrees.) Note that for $r \geq 0$, the choice $f_r = T^{p^r}$, $g_r = 1 - T^{p^r} = (1-T)^{p^r}$, and $h_r = 1$, with $S \supset \{T, T-1\}$, gives infinitely many relatively prime solutions with support in S, but they are p-th powers if $r > 0$.

b) Show there are only finitely many nonconstant relatively prime solutions in $\mathbf{Q}[T]$ to the above equation which are supported in S. (Bound the degrees as a first step, but more is needed since there are infinitely many polynomials with a given degree in $\mathbf{Q}[T]$.)

c) Formulate an analogue with $\mathbf{Z}$ in place of $F[T]$, and draw consequences from the *abc* conjecture.

7. We consider the equation $a(T) + b(T) = c(T)$ in $F[T]$ in the special case where $c(T) = c$ is a nonzero constant. This forces $a(T), b(T)$, and c to be relatively prime.

By the Mason–Stothers theorem, if $a(T)$ (or equivalently, $b(T)$) has *nonzero* derivative, then

$$\deg a(T) \leq N_0(a(T)) + N_0(c - a(T)) - 1.$$

This inequality is sometimes an equality, *e.g.*, $a(T) = 1 - rT^n$, $b(T) = rT^n$, $c = 1$, where $r \in F^\times$.

a) When F has characteristic 0, show the inequality is an equality if and only if $a(T)$ equals 0 or c at the roots of $a'(T)$. Symbolically, this says $a'(\alpha) = 0 \Longrightarrow a(\alpha) \in \{0, c\}$. The roots α may not lie in F. (Hint: First normalize c to 1 by division. Then think about the factorization of $a'(T)$, more specifically how the divisibility of $a(T) - a(\alpha)$ by $T - \alpha$ affects the divisibility of $a'(T)$ by $T - \alpha$.)

b) In $\mathbf{F}_p[T]$, show $a(T) = T^p - T - 1$ and $a(T) = T^{p+1} - T^p$, with $b(T) = 1 - a(T)$ and $c = 1$ in both cases, satisfy the derivative condition in part a but the inequality is strict.

c) When F has characteristic p, show the inequality is an equality if and only if the following conditions hold: (1) $a'(\alpha) = 0 \Longrightarrow a(\alpha) \in \{0, c\}$, (2) $(p, \deg a(T)) = 1$ (*i.e.*, $\deg a'(T) = \deg a(T) - 1$), (3) every root of $a(T)$ has multiplicity prime to p. Which of these conditions fail in part b?

Reciprocity laws.

8. Let $\pi \in \mathbf{F}_2[T]$ be irreducible with degree d and $f \in \mathbf{F}_2[T]$. Write

$$f(T)\pi'(T) \equiv a_0 + a_1 T + \cdots + a_{d-1}T^{d-1} \bmod \pi,$$

where $a_j \in \mathbf{F}_2$. Prove $[f, \pi) = a_{d-1}$. (This generalizes the computational formula for $[T, \pi)$.) Test this formula in cases where you already computed $[f, \pi)$. Does such a formula work for $[f, g)$?

9. For an odd prime p and irreducible $\pi \in \mathbf{F}_p[T]$, introduce a symbol $[f, \pi)_p \in \mathbf{F}_p$ related to the equation $x^p - x \equiv f \bmod \pi$. Compute examples and prove a reciprocity law for this symbol.

Reversing reduction maps.

10. Since $a \equiv b \bmod p^k \Longrightarrow a \equiv b \bmod p$, there is a natural reduction map $\mathbf{Z}/p^k \to \mathbf{Z}/p$, which is a ring homomorphism.

a) Show there is no ring homomorphism $\mathbf{Z}/p \to \mathbf{Z}/p^k$ when $k > 1$.

b) Show $a \equiv b \bmod p \Longrightarrow a^{p^{k-1}} \equiv b^{p^{k-1}} \bmod p^k$. Deduce that $u \bmod p \mapsto u^{p^{k-1}} \bmod p^k$ is an injective *group* homomorphism $(\mathbf{Z}/p)^\times \to (\mathbf{Z}/p^k)^\times$. What is the image (i.e., range) of this homomorphism when $p = 5$ and $k = 3$? Check the image is a cyclic group explicitly.

11. For irreducible π in $\mathbf{F}_p[T]$, show $f \bmod \pi \to f^{\mathrm{N}\pi^{k-1}} \bmod \pi^k$ is well-defined, and provides an injective *ring* homomorphism $\mathbf{F}_p[T]/\pi \to \mathbf{F}_p[T]/\pi^k$. What is the image of this homomorphism when $p = 2$, $\pi = T^2 + T + 1$, and $k = 2$? Check the image is a field of size 4.

Hasse derivatives.

12. In $\mathbf{F}_p[T]$, higher derivatives have a big problem: the p-th and higher derivatives are identically 0. The n-th derivative $(T^m)^{(n)}$ of T^m is

$$m(m-1)\cdots(m-n+1)T^{m-n},$$

whose vanishing for $n \geq p$ (independent of m) is due to the coefficient. On the other hand, consider the identity

$$\frac{(T^m)^{(n)}}{n!} = \binom{m}{n} T^{m-n}.$$

The left side looks bad in $\mathbf{F}_p[T]$ when $n \geq p$, because the numerator and denominator both vanish. But the right side is meaningful, since $\binom{m}{n} \in \mathbf{Z}$, and leads to a nontrivial theory of higher derivatives, as follows.

Let F be any field. For $n \geq 0$, define the nth *Hasse derivative* $\mathcal{D}^{(n)} \colon F[T] \to F[T]$ by

$$\mathcal{D}^{(n)}\left(\sum_{m=0}^{d} a_m T^m\right) = \sum_{m=0}^{d} \binom{m}{n} a_m T^{m-n}.$$

In particular, $\mathcal{D}^{(1)}(T^m) = mT^{m-1}$ (so $\mathcal{D}^{(1)}$ is ordinary differentiation) and $\mathcal{D}^{(2)}(T^m) = \binom{m}{2}T^{m-2}$. When F has characteristic 0, then $\mathcal{D}^{(n)}$ is $1/n!$ times the nth derivative, but when F has characteristic p there is no connection between $\mathcal{D}^{(n)}$ and ordinary n-th derivatives for $n \geq p$.

a) What is $\mathcal{D}^{(0)}$? Show $\mathcal{D}^{(n)}(T^m) = 0$ for $0 \leq m < n$. What is $\mathcal{D}^{(n)}(T^n)$?

b) Prove $\mathcal{D}^{(n)}(f+g) = \mathcal{D}^{(n)}(f) + \mathcal{D}^{(n)}(g)$ and $\mathcal{D}^{(n)}(fg) = \sum_{k=0}^{n} (\mathcal{D}^{(k)}f)(\mathcal{D}^{(n-k)}g)$ for $f, g \in F[T]$. What is the formula for the n-th (ordinary) derivative of a product?

c) In $\mathbf{F}_3[T]$, compute $\mathcal{D}^{(3)}(T^9 + 2T^7 + 2T^3 + T + 1)$.

d) Compute all Hasse derivatives of $T^p - 1 = (T-1)^p$ in $\mathbf{F}_p[T]$.

d) For $n > 1$, prove $\mathcal{D}^{(n)}$ is not an iterate of $\mathcal{D}^{(1)}$.

e) Devise a test for counting root multiplicities of polynomials using Hasse derivatives. Apply this test to determine the order of 1 as a root of $T^7 + T^6 + T + 1$ in $\mathbf{F}_2[T]$ without factoring.

13. (Hasse derivatives of rational functions)

a) For $f(T) \in F[T]$, show

$$f(T+X) = \sum_{n \geq 0} (\mathcal{D}^{(n)}f)(X)T^n.$$

The sum is finite, since $\mathcal{D}^{(n)}f = 0$ for $n > \deg f$.

For example, with $f(T) = T^4 + 2T + 1 \in \mathbf{F}_3[T]$,

$$f(T+X) = (X^4 + 2X + 1) + (X^3 + 2)T + XT^3 + T^4.$$

b) Show the map $F[T] \to F[T][X]$ given by

$$f \mapsto \sum_{n \geq 0} (\mathcal{D}^{(n)}f)(T)X^n$$

is a ring homomorphism. For example, $T^4 + 2T + 1$ gets sent to $(T^4 + 2T + 1) + (T^3 + 2)X + TX^3 + X^4$ when $F = \mathbf{F}_3$. Observe that the product rule in part b of the previous exercise is related to the homomorphism property.

c) Extend the operators $\mathcal{D}^{(n)}$ from $F[T]$ to all of $F(T)$, preserving as many properties as you can. (If you have had calculus, then you already know how to extend $\mathcal{D}^{(1)}$ to $F(T)$, but $\mathcal{D}^{(n)}$ is not an iterate of $\mathcal{D}^{(1)}$, so you really need to work to extend all of the $\mathcal{D}^{(n)}$'s.) Does the equation $\mathcal{D}^{(n)}(T^m) = \binom{m}{n}T^{m-n}$, which was a definition when $m \geq 0$, also hold for $m < 0$? The binomial coefficient $\binom{m}{n}$ for $m < 0$ is defined as the value at $X = m$ of the polynomial $\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}$. Do the formulas in part b of the previous exercise hold for $f, g \in F(T)$?

Carlitz polynomials.

14. This exercise describes an interesting analogue in $\mathbf{F}_p[T][X]$ of the polynomials $X^m - 1 \in \mathbf{Z}[X]$. (Just reducing $X^m - 1$ modulo p is a somewhat cheap analogue, since, as a polynomial in $\mathbf{F}_p[T][X]$, its X-coefficients are constants in $\mathbf{F}_p$ rather than honest polynomials in T.)

Rather than a multiplicative theory based on roots of unity, we develop an *additive* theory. Here p can be any prime.

We start with powers. For $n \geq 1$, define $[T^n](X) \in \mathbf{F}_p[T][X]$ recursively by

$$[T](X) := X^p + TX, \quad [T^n](X) := [T]([T^{n-1}](X))$$

for $n \geq 2$. For a general polynomial $M = c_n T^n + \cdots + c_1 T + c_0$ in $\mathbf{F}_p[T]$, define the *Carlitz polynomial* associated to M to be

$$[M](X) := c_n[T^n](X) + \cdots + c_1[T](X) + c_0 X \in \mathbf{F}_p[T][X].$$

Note $[c](X) = cX$ for any constant $c \in \mathbf{F}_p$. The polynomials $[M](X)$ are analogous to $X^m - 1$ (*more accurately*, to $(1+X)^m - 1$). (Our use of square brackets in $[M](X)$ should not be confused with its meaning in the notation $\mathbf{Z}[T]$, just as the dual use of parentheses in a polynomial $f(T)$ and in the field $\mathbf{Q}(T)$ causes no confusion.)

Recall $\mathrm{N}(M) = \#(\mathbf{F}_p[T]/M) = p^{\deg M}$ denotes the norm of M.

a) Compute $[T^2](X)$ and $[T^3 - T](X)$ in $\mathbf{F}_p[T][X]$. In $\mathbf{F}_3[T][X]$, compute $[2T^3 + T + 2](X)$.

b) Show $[M](X)$ has X-degree $p^{\deg M} = \mathrm{N}(M)$. Moreover, show that as a polynomial in X, $[M](X)$ is a "p-polynomial":

$$[M](X) = \sum_{j=0}^{\deg M} a_{j,M}(T) X^{p^j},$$

(note X^{p^j}, not X^j), with coefficients $a_{j,M}(T) \in \mathbf{F}_p[T]$. In particular, show $a_{0,M}(T) = M$ and $a_{\deg M, M}(T)$ is the leading coefficient of M. Note $[M](X)$ has constant term 0.

c) Show $[M](X+Y) = [M](X) + [M](Y)$ and $[M](cX) = c[M](X)$ for any c in $\mathbf{F}_p$.

d) For M_1, M_2 in $\mathbf{F}_p[T]$, show

$$[M_1 + M_2](X) = [M_1](X) + [M_2](X), \quad [M_1 M_2](X) = [M_1]([M_2](X)).$$

The second equation has an analogue for the polynomials $(1+X)^m - 1$ in $\mathbf{Z}[X]$ (what is it?).

e) For $M \in \mathbf{F}_p[T]$, prove $a_{1,M} = (M^p - M)/(T^p - T)$.

f) For $1 \leq j \leq \deg M$, prove the recursion

$$a_{j,M} = \frac{a_{j-1,M}^p - a_{j-1,M}}{T^{p^j} - T}$$

and then derive that $a_{j,M}$ is a polynomial function of M (like $\binom{m}{n}$ as a function of m):

$$a_{j,M}(T) = \frac{\prod_{\deg h < j}(M - h)}{D_j}, \quad D_j := \prod_{\substack{h \text{ monic} \\ \deg h = j}} h.$$

(Note h in the numerator of $a_{j,M}$ runs over all polynomials of degree less than j, including $h = 0$, while h in the denominator D_j runs over all monics of degree exactly j.)

g) Prove, for $j \geq 1$, that $D_j = (T^{p^j} - T) D_{j-1}^p$. Thus,

$$D_0 = 1, \quad D_1 = T^p - T, \quad D_2 = (T^{p^2} - T)(T^p - T)^p, \quad D_3 = (T^{p^3} - T)(T^{p^2} - T)^p (T^p - T)^{p^2}.$$

h) For primes p, you know $p \mid \binom{p}{k}$ for $1 \leq k \leq p-1$. This says the intermediate coefficients of $(1+X)^p$ are multiples of p. Prove an analogue for the X-coefficients of $[\pi](X)$ when π is irreducible in $\mathbf{F}_p[T]$.

i) For $f \in \mathbf{F}_p[T][X]$ and monic irreducible $\pi \in \mathbf{F}_p[T]$, show $f([\pi](X)) = f(X)^{\mathrm{N}\pi}$ in $(\mathbf{F}_p[T]/\pi)[X]$. This is the analogue of $f(X^p) = f(X)^p$ in $(\mathbf{Z}/p)[X]$ for any f in $\mathbf{Z}[X]$.

15. (Carlitz actions) For nonzero $m \in \mathbf{Z}$, the units mod m are a group under multiplication. We can raise units to powers and see whether some unit generates the whole group.

On Homework 1 you found that, while $(\mathbf{Z}/p^2)^\times$ is a cyclic group for any p, $(\mathbf{F}_p[T]/\pi^2)^\times$ is not a cyclic group for $\deg \pi > 1$. With the help of Carlitz polynomials, we can repair this nonanalogy between $\mathbf{Z}$ and $\mathbf{F}_p[T]$.

The key idea is to think additively: let the $\mathbf{F}_p[T]$-analogue of the multiplicative group $(\mathbf{Z}/m)^\times$ be the additive group $\mathbf{F}_p[T]/M$, and "powers" on $\mathbf{F}_p[T]/M$ will be interpreted as the effect of Carlitz polynomials. In other words, the power u^k, for $u \in (\mathbf{Z}/m)^\times$ and $k \in \mathbf{Z}$, will be replaced by the "Carlitz power" $[g](a)$, for $a \in \mathbf{F}_p[T]/M$ and $g \in \mathbf{F}_p[T]$. Here $[g](a)$ is the value of the $[g](X) \in \mathbf{F}_p[T][X]$ at $X = a$. (To write a^g instead of $[g](a)$ would be a horrible abuse of notation, but it would convey the intent more bluntly.)

a) For $a \in \mathbf{F}_p[T]/M$, show there is some monic $g \in \mathbf{F}_p[T]$ such that $[g](a) \equiv 0 \bmod M$. (Hint: pigeonhole)

b) Show that 1 is a "Carlitz generator" of $\mathbf{F}_3[T]/(T^2+1)$. That is,

$$\{[g](1) \bmod T^2+1 : g \in \mathbf{F}_3[T]\} = \mathbf{F}_3[T]/(T^2+1).$$

On the other hand, show $T+1 \in \mathbf{F}_3[T]/(T^2+1)$ is not a Carlitz generator.

c) Show 1 is a Carlitz generator of $\mathbf{F}_2[T]/(T^2)$ and also of $\mathbf{F}_2[T]/(T^2+T+1)$.

d) Show 1 is *not* a Carlitz generator of $\mathbf{F}_{23}[T]/M$, where $M = T^3+9T^2+13T+1$. In fact, show

$$\{[g](1) \bmod M : g \in \mathbf{F}_{23}[T]\} = \{c_1T + c_0 \bmod M : c_0, c_1 \in \mathbf{F}_{23}\},$$

so the Carlitz powers of 1 mod M are the residue classes where the coefficient of T^2 is 0.

For $a \in \mathbf{F}_p[T]/M$, its "Carlitz order" is defined to be the least degree monic g in $\mathbf{F}_p[T]$ such that $[g](a) \equiv 0 \bmod M$. (At least one such g exists by part a.) For example, the Carlitz order of $1 \in \mathbf{F}_3[T]/(T^2+1)$ is T^2 and the Carlitz order of $T+1 \in \mathbf{F}_3[T]/(T^2+1)$ is T. Note Carlitz orders are polynomials, not integers. We are not doing group theory.

e) Compute the Carlitz order of 1 mod M in part d.

f) For $a \in \mathbf{F}_p[T]/M$, show any g which satisfies $[g](a) \equiv 0 \bmod M$ is divisible by the Carlitz order of a. If the Carlitz orders of two elements are relatively prime, prove the Carlitz order of their *sum* is the product of their Carlitz orders.

g) Let π be monic irreducible in $\mathbf{F}_p[T]$. Use exercise 14h to show $[\pi - 1](a) \equiv 0 \bmod \pi$ for all $a \in \mathbf{F}_p[T]$. In particular, every element of $\mathbf{F}_p[T]/\pi$ has Carlitz order dividing $\pi - 1$. (Sound familiar to something classical?)

h) Prove $\mathbf{F}_p[T]/\pi$ (additive!) is cyclic in the Carlitz sense: it contains an element whose Carlitz powers fill up all of $\mathbf{F}_p[T]/\pi$.

i) Prove $\mathbf{F}_p[T]/\pi^2$ is cyclic in the Carlitz sense. This is the right analogue of $(\mathbf{Z}/p^2)^\times$ being cyclic for all p.

j) It is known that $(\mathbf{Z}/p^k)^\times$ is cyclic, unless $p = 2$ and $k \geq 3$. Using a proof of this classical result, can you devise a Carlitz analogue for $\mathbf{F}_p[T]/\pi^k$?

16. (Carlitz coefficient functions) Pursuing the analogy between $[M](X)$ and $(1+X)^m - 1$, we look at their expansion coefficients:

$$(1+X)^m - 1 = \sum_{n=1}^{m} \binom{m}{n} X^n, \quad [M](X) = \sum_{j=0}^{\deg M} a_{j,M}(T) X^{p^j}.$$

From the expansion, we know $\binom{m}{n} \in \mathbf{Z}$ when $0 \leq n \leq m$. (We do not need $\binom{m}{0}$ here, but we know this is 1.) From the factorization formula

$$\binom{m}{n} = \frac{m(m-1)\cdots(m-n+1)}{n!}$$

for $n \geq 0$, we see $\binom{m}{n}$ is a polynomial function in m with rational coefficients.

Writing this polynomial as $\binom{X}{n}$ extends the meaning of $\binom{m}{n}$ to all integers m (including negatives) by substitution into the polynomial. It is not hard to check $\binom{-X}{n} = (-1)^n\binom{X+n-1}{n}$, which shows $\binom{m}{n} \in \mathbf{Z}$ for all integers m. Note $\deg\binom{X}{n} = n$.

a) Inspired by the formula in exercise 14f, define for $j \geq 1$

$$E_j(X) := \frac{\prod_{\deg h<j}(X-h)}{D_j} \in \mathbf{F}_p(T)[X].$$

Note $h = 0$ is included in the product. Set $E_0(X) = X$.

As an example, $E_1(X) = (X^p - X)/(T^p - T)$. Prove $E_j(M) \in \mathbf{F}_p[T]$ for every M in $\mathbf{F}_p[T]$, and also

$$E_j(X) = \frac{X\prod_{\substack{\text{monic } h\\ \deg h<j}}(X^{p-1} - h^{p-1})}{D_j}.$$

(Hint: $X^{p-1} - h^{p-1} = \prod_{c\in\mathbf{F}_p^\times}(X - ch)$.)

b) For all j, prove $E_j(X+Y) = E_j(X) + E_j(Y)$ and $E_j(cX) = cE_j(X)$ where $c \in \mathbf{F}_p$.

c) For $j \geq 1$, show

$$E_j(TX) - TE_j(X) = E_{j-1}(X)^p, \quad (T^{p^j} - T)E_j(X) = E_{j-1}(X)^p - E_{j-1}(X).$$

d) When M is monic with $\deg M = j$, prove $E_j(M) = 1$. (What if M is not monic?) Setting $Y = T^j$ in part b, conclude

$$E_j(X) + 1 = \frac{\prod_{\substack{\text{monic } h\\ \deg h=j}}(X+h)}{D_j}.$$

Note the + sign in the numerator.

e) Let $L_j = (T^p - T)(T^{p^2} - T)\cdots(T^{p^j} - T)$. Show

$$E_j(X) = \sum_{i=0}^{j}\frac{(-1)^{j-i}X^{p^i}}{D_iL_{j-i}}.$$

Compute the Hasse derivatives (exercise 12) of $E_j(X)$, with respect to X.

f) Because $[M](X)$ is a p-polynomial in X (meaning the only terms are those involving X^{p^j}), it is best to consider $E_j(X)$ (the polynomial derived from $a_{j,M}$ as a function of M) to be analogous not to $\binom{X}{j}$, but to $\binom{X}{p^j}$. (For example, $E_0(X) = X = \binom{X}{0}$ and $E_j(X)$ has X-degree p^j.) We fill out the sequence E_j to a larger family of polynomials using base p digit expansions, as follows.

Write $n > 0$ as $n = b_0 + b_1p + \cdots + b_sp^s$, where $0 \leq b_j \leq p-1$. Define

$$G_n(X) := \prod_{j=0}^{s}E_j(X)^{b_j} \in \mathbf{F}_p(T)[X].$$

The effect of n on the right side is in the exponents, which are its base p digits. Set $G_0(X) = 1$. As an example, $2p - 1 = p - 1 + 1\cdot p$, so $G_{2p-1}(X) = E_0(X)^{p-1}E_1(X)^1 = X^{p-1}E_1(X)$. Note $\deg G_n = n$.

Explicitly compute $G_n(X)$ for $0 \leq n \leq 2p-1$.

g) Prove $G_n(X+Y) = \sum_{k=0}^{n}\binom{n}{k}G_k(X)G_{n-k}(Y)$ and $G_n(cX) = c^nG_n(X)$, where $c \in \mathbf{F}_p$.

h) (Sinnott) The denominator of $G_n(X)$ is $\prod_{j=0}^{s}D_j^{b_j} \in \mathbf{F}_p[T]$. Denote this denominator as $\Pi(n)$. Comparing $G_n(X)$ with $\binom{X}{n}$ suggests $\Pi(n)$ is an $\mathbf{F}_p[T]$-analogue of $n!$. Show the highest power of an irreducible $\pi \in \mathbf{F}_p[T]$ that divides $\Pi(n)$ is

$$\sum_{k\geq 1}\left\lfloor\frac{n}{\mathrm{N}\pi^k}\right\rfloor,$$

where $\lfloor\cdot\rfloor$ is the usual greatest integer function. This resembles the classical formula $\sum_{k\geq1}\lfloor n/p^k\rfloor$ for the highest power of p dividing $n!$.

17. Here is a striking analogy between the families $\binom{X}{n} \in \mathbf{Q}[X]$ and $G_n(X) \in \mathbf{F}_p(T)[X]$.

a) Using the formula $\deg \binom{X}{n} = n$, prove any polynomial $f(X) \in \mathbf{Q}[X]$ of degree d (say) can be written in a unique manner as a finite sum of the form

$$f(X) = \sum_{n=0}^{d} c_n \binom{X}{n},$$

with $c_n \in \mathbf{Q}$.

b) What is this expansion for $(X^3 - X)/2$? For $X^2 + X/4 - 1$?

c) Prove $f(\mathbf{Z}) \subset \mathbf{Z} \Longleftrightarrow c_n \in \mathbf{Z}$ for all n.

d) Prove any polynomial $f \in \mathbf{F}_p(T)[X]$ of X-degree d (say) can be written uniquely in the form

$$f(X) = \sum_{n=0}^{d} c_n G_n(X),$$

where $c_n \in \mathbf{F}_p(T)$, and $f(\mathbf{F}_p[T]) \subset \mathbf{F}_p[T] \Longleftrightarrow c_n \in \mathbf{F}_p[T]$ for all n.

18. (Cyclotomic polynomials) The mth *cyclotomic polynomial*, $\Phi_m(X)$, is defined to be the polynomial whose roots are the different complex roots of unity of *exact* order m (called *primitive* m-th roots of unity):

$$\Phi_m(X) := \prod (X - \omega),$$

where ω runs over the primitive mth roots of unity in $\mathbf{C}$. For example,

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1, \quad \Phi_4(X) = X^2 + 1.$$

Collecting the mth roots of unity according to their exact order, we have the basic identity

$$X^m - 1 = \prod_{d|m} \Phi_d(X).$$

a) Prove $\Phi_m(0) = 1$ for $m \geq 2$. What is $\Phi_m(1)$?

b) As the examples suggest, $\Phi_m(X)$ has integer coefficients. This is not evident from its definition, which only gives $\Phi_m(X) \in \mathbf{C}[X]$. Prove $\Phi_m(X) \in \mathbf{Z}[X]$ by induction on m and Gauss' lemma.

c) Are the coefficients of $\Phi_m(X)$ equal to 0 or ± 1 for all m?

d) Since $\Phi_m(X)$ has coefficients in $\mathbf{Z}$, the polynomial can be reduced mod p. That is, we can consider $\overline{\Phi}_m(X)$ in $\mathbf{F}_p[X]$. Let $K \supset \mathbf{F}_p$ be a field over which $\overline{\Phi}_m(X)$ decomposes into linear factors. Prove that when p does not divide m, the roots of $\overline{\Phi}_m(X)$ in K are primitive m-th roots of unity. (This does require proof, since we defined $\overline{\Phi}_m(X)$ as the reduction mod p of some integral polynomial, not as a polynomial having certain roots over $\mathbf{F}_p$.) What happens when $p|m$?

e) Use the factorization of $X^{p-1} - 1$ into cyclotomic polynomials to prove $(\mathbf{Z}/p)^\times$ is cyclic. This is probably not the same as your proof of this result when you were a first-year student. Does the proof extend to show the group of nonzero elements of any finite field is cyclic?

19. (Roots of Carlitz polynomials) We know by Homework 1 that there is a field $K \supset \mathbf{F}_p(T)$ in which $[M](X)$ decomposes into linear factors as a polynomial in X.

a) Show all the roots of $[M](X)$ in K are distinct. (Hint: Consider the derivative of $[M](X)$ with respect to X, trying $M = T$ to get a sense of what's going on.)

b) Let Λ_M be the set of all X-roots of $[M](X)$. For example, Λ_T contains 0 and the $(p-1)$-th roots of $-T$.

Prove Λ_M is an additive group. For $\alpha \in \Lambda_M$ and $A \in \mathbf{F}_p[T]$, show $[A](\alpha) \in \Lambda_M$. Then, for A, B in $\mathbf{F}_p[T]$, prove

$$[A](\alpha) = [B](\alpha) \text{ for all } \alpha \in \Lambda_M \Longleftrightarrow A \equiv B \bmod M.$$

This is the analogue of: $\omega^a = \omega^b$ for all mth roots of unity $\omega \in \mathbf{C}$ if and only if $a \equiv b \bmod m$.

c) For $A \in \mathbf{F}_p[T]$, show $\{[A](\alpha) : \alpha \in \Lambda_M\} = \Lambda_M$ if and only if $(A, M) = 1$. This is the analogue of: $\{\omega^a : \omega^m = 1\} = \{\omega : \omega^m = 1\}$ if and only if $(a, m) = 1$.

d) For *monic* M in $\mathbf{F}_p[T]$, set

$$\Phi_M(X) = \prod_{\substack{[M](\alpha)=0 \\ [D](\alpha)\neq 0}} (X-\alpha),$$

where the product is taken over roots α of $[M](X)$ which are not roots of $[D](X)$ for any monic proper divisor D of M. This is an analogue of the mth cyclotomic polynomial, and the roots of $\Phi_M(X)$ could be considered as "primitive" roots of $[M](X)$. What is the X-degree of $\Phi_M(X)$? Show $[M](X) = \prod_{D|M} \Phi_D(X)$, the product taken over the monic divisors D of M, and show $\Phi_M(X)$ lies in $\mathbf{F}_p[T][X]$. Compute $\Phi_1(X)$, $\Phi_T(X)$, $\Phi_{T+1}(X)$, and $\Phi_{T^2}(X)$.

e) Read a proof that $\Phi_m(X)$ is irreducible in $\mathbf{Q}[X]$, and adapt the proof to show $\Phi_M(X)$ is irreducible in $\mathbf{F}_p(T)[X]$.

f) If you know Galois theory, extend the usual proof that $\mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q}) \cong (\mathbf{Z}/m)^\times$ to give a natural proof that $\mathrm{Gal}(\mathbf{F}_p(T,\Lambda_M)/\mathbf{F}_p(T)) \cong (\mathbf{F}_p[T]/M)^\times$. (As in the classical case, it is best to start by defining a map from the units mod M to the Galois group, rather than the other way around.)

g) If you know algebraic number theory, prove an irreducible $\pi \in \mathbf{F}_p[T]$ is unramified in $\mathbf{F}_p(T,\Lambda_M)$ if and only if $(\pi, M) = 1$. If $(\pi, M) = 1$ and π is monic, prove the isomorphism in part f identifies the Frobenius at π in $\mathrm{Gal}(\mathbf{F}_p(T,\Lambda_M)/\mathbf{F}_p(T))$ with the congruence class π mod M. This is similar to the description of Frobenius elements in cyclotomic extensions of $\mathbf{Q}$.