1. Some basics

1.1. **Multiplicity.** Let k be a field of arbitrary characteristic, and consider f in $\mathsf{k}[x_1, \ldots, x_n]$.

(1) If $\mathfrak{m}$ is the ideal of $\mathsf{k}[x_1, \ldots, x_n]$ generated by the variables, describe canonical generators for the ideal $\mathfrak{m}^t$ where t is a positive integer.
(2) Verify that $f \in \mathfrak{m}$ if and only if $f(\mathbf{0}) = 0$, where $\mathbf{0} = (0, \ldots, 0) \in \mathsf{k}^n$ is the origin.
(3) Make sense of the term "lowest degree component of f" and describe what it means for f to be in $\mathfrak{m}^t$ in terms of its lowest degree component.
(4) When describing what it meant for the origin $\mathbf{0}$ to be a singular point of f, we used the fact that we can always write $f = L + G$ where $L = f(\mathbf{0}) + \frac{\partial f}{\partial x_1}(\mathbf{0}) \cdot x_1 + \cdots + \frac{\partial f}{\partial x_n}(\mathbf{0}) \cdot x_n$ and $G \in \mathfrak{m}^2$. Verify this, and make sure your argument works for every k.
(5) Next, suppose, in addition, that f vanishes at the origin $\mathbf{0} \in \mathsf{k}^n$. Algebraically, this means that f lies in the ideal $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$, the ideal of $\mathsf{k}[x_1, \ldots, x_n]$ generated by the variables. In Lecture 1, we stated that if $\mathbf{a} = (a_1, \ldots, a_n) \in \mathsf{k}^n$ is a nonzero point, then
$$\ell = \{\mathbf{a}t : t \in \mathsf{k}^n\}$$
which is the line through the origin determined by this point, is *tangent* to the hypersurface $\mathsf{V} = \mathbb{V}(f)$ if and only if $t^2 | f(\mathbf{a}t)$, which is a polynomial over k in the single variable t. Think about why this is a good definition, and is consistent with the situation from calculus.
(6) In Lecture 1, we saw that the following are equivalent for f vanishing at the origin.
- L as above is the zero polynomial
- $f(\mathbf{0}) = \partial f/\partial x_1(\mathbf{0}) = \cdots = \partial f/\partial x_n(\mathbf{0}) = 0$
- $f \in \mathfrak{m}^2$

We then defined f to be *singular at the origin* if any of these conditions holds. Note that in this case, f lies in both $\mathfrak{m}$ and $\mathfrak{m}^2$, and so it might be reasonable to think about the largest power of $\mathfrak{m}$ that contains f. Prove that this makes sense, as long as the original f that we started with was nonzero (which it always should be in this lecture series).
Hint: What you are being asked to show is that $\cap_{t=1}^{\infty} \mathfrak{m}^t = 0$.
(7) The last problem shows that the following number is well-defined.

> **Definition**: The multiplicity of f at $\mathbf{0}$ is $\text{mult}(f) = \text{mult}_{\mathbf{0}}(f) = \max\{t : f \in \mathfrak{m}^t\}$.

Describe why this is a good first start towards our goal of describing how singular a hypersurface can be at the origin. Are there any reasons why this approach isn't so great?
(8) Prove that the inverse of the multiplicity may be characterized in the following way:
$$\frac{1}{\text{mult}(f)} = \sup\left\{\frac{i}{q} : i, q \in \mathbb{N}, q \neq 0, \text{ and } f^i \notin \mathfrak{m}^q\right\}$$
Hint: Why can you write $f = f_M + f_{M+1} + \cdots + f_N$ for some positive integers $M \leq N$, where each f_i is a k-linear combination of monomials of degree i, and $f_M \neq 0$? What is M? What is the "lowest degree component" of f^i, and what does this have to do with a noncontainment of the form $f^i \notin \mathfrak{m}^q$?

1.2. **Finite and free extensions.** An arbitrary extension of rings $\mathsf{A} \subseteq \mathsf{B}$ is called *finite and free* if there exists a finite collection of elements $b_1, \ldots, b_t$ of B satisfying the following conditions:

- Every element of B can be written as an A-linear combination of $b_1, \ldots, b_t$. That is, for every $b \in \mathsf{B}$, there exist $a_1, \ldots, a_t \in \mathsf{A}$ such that $b = a_1 b_1 + \ldots + a_t b_t$.
- The $b_1, \cdots, b_t$ are linearly independent over A. That is, if $0 = a_1 b_1 + \cdots + a_t b_t$ for some $a_1, \cdots, a_t \in \mathsf{A}$, then $a_1 = \cdots = a_t = 0$.

We call such a collection of elements $b_1, \ldots, b_t$ a *free basis* for B over A. **Note**: In the language of module theory, this is simply saying that B is finitely-generated and free when regarded as an A-module via the inclusion of A into B.

(1) Verify that if $\mathsf{A} = \mathbb{Q}[x]$ and $\mathsf{B} = \mathbb{Q}[x,y]/\langle y^3 - x^2y^2 + 7xy - 11x^{100}\rangle$, then the natural inclusion $\mathsf{A} \hookrightarrow \mathsf{B}$ is finite and free. Can you generalize this example?
(2) Specialize to the characteristic p case: If R is the polynomial ring $\mathbb{F}_p[x]$ over $\mathbb{F}_p$ in the variable x, and R^p is the polynomial ring $\mathbb{F}_p[x^p]$ over $\mathbb{F}_p$ in the p-th power x^p, then the natural inclusion $\mathsf{R}^p \subseteq \mathsf{R}$ is finite and free. What is a canonical free basis for R over R^p?
(3) If you feel like it, generalize the above to cover the case that $\mathsf{R} = \mathbb{F}_p[x,y]$.
(4) As in linear algebra, verify that $b_1, \ldots, b_t$ is a free basis for B over A if and only if every element of B can be expressed as an A-linear combination of $b_1, \ldots, b_t$ in a *unique* way.
(5) Suppose that $b_1, \ldots, b_t$ is a free basis for B over A, and fix an element $b \in \mathsf{B}$. Prove that, if in the unique expression of $b = a_1b_1 + \cdots + a_tb_t$ with each $a_i \in \mathsf{A}$, some a_s is a unit in A, then one may replace b_s with b to obtain another free basis for B over A.
(6) Suppose that $b_1, \ldots, b_t$ is a free basis for B over A. If we fix some b_i, prove that there exists a map $\phi : \mathsf{B} \to \mathsf{A}$ satisfying the following conditions:
   (a) ϕ is a map of abelian groups: $\phi(f+g) = \phi(f) + \phi(g)$ for every $f, g \in \mathsf{B}$.
   (b) ϕ is A-linear: $\phi(ab) = a\phi(b)$ for every $a \in \mathsf{A}$ and $b \in \mathsf{B}$.
   (c) $\phi(b_i) = 1$.

2. Some standard Frobenius stuff

2.1. **Frobenius powers of ideals.** Let R be a ring of characteristic p, and let I be an ideal of R.

(1) Prove that, as elements of R, the binomial coefficient $\binom{p}{i}$ is zero if $1 \leq i \leq p-1$. Apply the binomial theorem to remind yourself that, as a consequence of this fact, the map $F : \mathsf{R} \to \mathsf{R}$ defined by $F(f) = f^p$ is a map of rings. We call this map the *Frobenius map* on R.
(2) Recall the definition of the p-th Frobenius power of I.

> **Definition**: The p-th Frobenius power of I is the ideal $I^{[p]}$ of R generated by the p-th powers of all elements in I. That is, $I^{[p]} = \langle f^p : f \in I\rangle$

Suppose that $\mathcal{G}$ is a finite generating set for I, i.e., every element of I is an R-linear combination of elements of $\mathcal{G}$. Prove that $I^{[p]}$ is generated by the p-th powers of the elements in $\mathcal{G}$. In other words, if $I = \langle f : f \in \mathcal{G}\rangle$, then $I^{[p]} = \langle f^p : f \in \mathcal{G}\rangle$. In particular, if $\mathcal{H}$ is another generating set for I, then $\langle f^p : f \in \mathcal{G}\rangle = I^{[p]} = \langle f^p : f \in \mathcal{H}\rangle$. Make certain to note when you are using the assumption that R has characteristic p.
(3) Contrast this with similar possible constructions in characteristic zero, which are not as well-behaved. For example, consider the ideal $I = \langle x, y\rangle$ of the polynomial ring $\mathbb{Q}[x,y]$. By definition, $\mathcal{G} = \{x, y\}$ is a generating set for I, and clearly, so is $\mathcal{H} = \{x, x+y\}$. Unfortunately, as you should verify, $\langle x^2, y^2\rangle = \langle f^2 : f \in \mathcal{G}\rangle \neq \langle f^2 : f \in \mathcal{H}\rangle = \langle x^2, (x+y)^2\rangle$.
(4) Recall that if $\varphi : \mathsf{A} \to \mathsf{B}$ is a map of commutative rings, then the expansion of an ideal $\mathfrak{a}$ of A to B is the ideal of B generated by $\varphi(\mathfrak{a})$ (NB: The image $\varphi(\mathfrak{a})$ itself need not be an ideal; come up with an example.) Verify that if $\mathsf{A} = \mathsf{B} = \mathsf{R}$ and φ is the Frobenius map $F : \mathsf{R} \to \mathsf{R}$ given by $F(g) = g^p$, then the expansion of I is precisely $I^{[p]}$. This shows that forming the p-th Frobenius power $I^{[p]}$ of I is a canonical thing to do, at least in characteristic p.
(5) Iterate this construction, and define the p^e-th Frobenius power $I^{[p^e]}$ of an ideal I of R for every positive integer exponent e.

(6) It should be clear that the Frobenius power $I^{[p]}$ is contained in the regular power I^p; if it isn't, please convince yourself! Prove that if I can be generated by t elements, then we have the string of inclusions $I^{tp} \subseteq I^{[p]} \subseteq I^p$. Finally, verify that all of this still works when replacing p by p^e for some positive integer exponent e.
Hint: Look at the generators for I^{tp}, and apply the Pigeonhole Principle.

2.2. **The Frobenius fractal associated to a polynomial ring.** In this section, let $\mathsf{R} = \mathbb{F}_p[x_1, \ldots, x_n]$. In Lecture 2, we saw that the Frobenius fractal in this case is the chain of rings

$$\ldots \subseteq \mathsf{R}^{p^e} \subseteq \ldots \subseteq \mathsf{R}^{p^2} \subseteq \mathsf{R}^p \subseteq \mathsf{R}$$

where each ring R^{p^e} is defined as $\mathsf{R}^{p^e} := F^e(\mathsf{R}) = \{f^{p^e} : f \in \mathsf{R}\} = \mathbb{F}_p[x_1^{p^e}, \ldots, x_n^{p^e}]$, where

$$F^e = F \circ F \circ F \cdots \circ F$$

is the Frobenius map on R composed with itself e times.

Thus, each term in this chain is simply a polynomial ring over $\mathbb{F}_p$ in n variables, and hence, they are all isomorphic as rings. Furthermore, in lecture, and/or in the problems above, we have seen that every extension of rings $\mathsf{R}^{p^e} \subseteq \mathsf{R}$ in this chain is finite and free.

(1) In Lecture 2, we showed that $\mathsf{R}^p = F(\mathsf{R})$ is contained in $\mathbb{F}_p[x_1^p, \ldots, x_n^p]$, but as was pointed out to me by an observant participant after the talk, we did not establish the opposite containment. Correct this oversight by verifying that $F(\mathsf{R})$ actually equals $\mathbb{F}_p[x_1^p, \ldots, x_n^p]$, and convince yourself that the same argument shows that $F^e(\mathsf{R}) = \mathbb{F}_p[x_1^{p^e}, \ldots, x_n^{p^e}]$.
(2) In Lecture 2, we verifed that $R^p \subseteq R$ is finite and free, and you may have also done this yourself if you worked out all parts of Problem 1.2. This result, along with the fractal nature of this chain, suggests that *every* possible extension of rings in this chain should be finite and free. To test your understanding, verify this by showing that if $e > s$, then the extension $\mathsf{R}^{p^e} \subseteq \mathsf{R}^{p^s}$ is finite and free by exhibiting a finite set of free generators.
(3) Verify that every inclusion of rings $\mathsf{R}^{p^e} \subseteq \mathsf{R}$ in this chain *splits*. In other words, show that there exists a map $\phi : \mathsf{R} \to \mathsf{R}^{p^e}$ with the following properties:
   (a) ϕ is a map of abelian groups, i.e., $\phi(f+g) = \phi(f) + \phi(g)$ for every $f, g \in \mathsf{R}$.
   (b) ϕ is linear over R^{p^e}, i.e., $\phi(f^{p^e} g) = f^{p^e} \phi(g)$ for every $f \in \mathsf{R}$.
   (c) $\phi(1) = 1$.
   Note: The last two points imply that $\phi(f^{p^e}) = f^{p^e}$ for every $f \in \mathsf{R}$. Thus, the map ϕ, which is typically called a splitting of the inclusion $\mathsf{R}^{p^e} \subseteq \mathsf{R}$, or a *Frobenius splitting*, can be thought of as a way to turn every element of R into a p^e-power power in such a way that respects addition, and does not alter an element of R that was already a p^e-power.
   Hint: We know that R is finite and free over R^{p^e}, and in fact, the free basis that we described in lecture (or you produced in an earlier problem) contains the element 1.
(4) Let I be an arbitrary ideal of R. Prove that if $f \in \mathsf{R}$, then $f^p \in I^{[p]}$, as defined in the previous sets of problems, if and only if $f \in I$. **Hint**: One direction is easy. For the other, write out what it means for f^p to be in $I^{[p]}$ using elements, and then apply the map ϕ that you constructed above.

2.3. **The localized Frobenius fractal.** Let R be the polynomial ring $\mathbb{F}_p[x_1, \ldots, x_n]$, and let $\mathfrak{m}$ be the ideal of this ring generated by the variables. Let S be the localization of R at the origin/at the maximal ideal $\mathfrak{m}$. In more concrete terms, S is the subset of the fraction field of R consisting of all fractions of the form fg^{-1}, where $f, g \in \mathsf{R}$, and $g(\mathbf{0}) \neq 0$, i.e., $g \notin \mathfrak{m}$.

(1) Verify that S is a subring of the fraction field of R, and that R is a subring of S.
   Hint: The main thing to do is show that S is closed under taking sums and products.
(2) Above, you showed that there is an inclusion $\mathsf{R} \subseteq \mathsf{S}$. Under this inclusion, which elements of R that are *not* units in R become units when regarded as elements of S?

(3) Note that S has its own Frobenius map $F : \mathsf{S} \to \mathsf{S}$, and so the Frobenius fractal for S is simply the chain of rings

$$\ldots \subseteq \mathsf{S}^{p^e} \subseteq \ldots \subseteq \mathsf{S}^{p^2} \subseteq \mathsf{S}^p \subseteq \mathsf{S}$$

where each ring S^{p^e} is defined as $\mathsf{S}^{p^e} := F^e(\mathsf{S}) = \{f^{p^e} g^{-p^e} : f, g \in \mathsf{R}, g \notin \mathfrak{m}\}$.

Prove that every extension of rings $\mathsf{S}^{p^e} \subseteq \mathsf{S}$ is finite and free. In fact, prove the stronger assertion that every free basis for R over R^{p^e} becomes a free basis for S over S^{p^e}, when we interpret the terms of this free basis as elements of S via the canonical inclusion $\mathsf{R} \hookrightarrow \mathsf{S}$.

(4) At this point, we have shown that $\mathsf{S}^{p^e} \subseteq \mathsf{S}$ is finite and free by exhibiting a free basis for this extension. Of course, as in linear algebra, where each finite-dimensional vector space has lots of bases, there are lots of free bases for S over S^{p^e}. Our goal now is to prove the following result that is related to this, which motivates the definition of the Frobenius index of singularities (in the literature, we call this the F-pure threshold) that we considered/will consider soon.

> **Lemma**: Let g be a polynomial in R vanishing at the origin, i.e., g is contained in $\mathfrak{m}$. Prove that there exists a free basis $g_1, \ldots, g_t$ for S over S^{p^e} with one of the g_i equaling g if and only if $g \notin \mathfrak{m}^{[p^e]} = \langle x_1^{p^e}, \ldots, x_n^{p^e} \rangle$. Note that the former condition concerns a basis for S, but the latter is a condition on an element and ideal of R.

- Step 0: For simplicity, let's only consider the case that $e = 1$. Once you are done, go back and see that you can simply replace p with p^e everywhere to get the general case.
- Step 1: Prove that if $g \notin \mathfrak{m}^{[p]}$, then g is part of some free basis for S over S^p.
  Hint: We already know that there is a free basis $h_1, \ldots, h_t$ for R over R^p, and by the previous problem, this remains a free basis for S over S^p. Thus, we may write $g = \ell_1^p h_1 + \ldots + \ell_t^p h_t$ for some $\ell_i \in \mathsf{R}$. What does $g \notin \mathfrak{m}^{[p]}$ tell us about the ℓ_i?
- Step 2: Prove that if $g \in \mathfrak{m}^{[p]}$, then g cannot be part of any free basis for S over S^p.
  Hint: By contradiction, suppose that $g \in \mathfrak{m}^{[p]}$, and somehow, that there is a free basis $g = g_1, g_2, \ldots, g_t$ for S over S^p. As in an earlier problem, use this to construct an S^p-linear map $\pi : \mathsf{S} \to \mathsf{S}^p$ that sends g to 1. However, write out what the containment $g \in \mathfrak{m}^{[p]}$ in terms of elements, and see that $\pi(g)$ could never equal to 1.

2.4. **Generalizing/extending the Frobenius fractal.** To this point, we have only considered the Frobenius fractal associated to a (localization of) a polynomial ring over $\mathbb{F}_p$. Here, we take a closer look at the Frobenius fractal associated to an arbitrary domain of characteristic p.

Note: None of this plays a real role in this lecture series, but it is relevant in this area of math, and I think it is fun. It also addresses a question from a participant in Lecture 2, who asked whether we can extend the Frobenius fractal to infinity in the "other" direction.

Let R be a domain of characteristic p, let L be the fraction field of R, and let $\overline{\mathsf{L}}$ be the algebraic closure of L, so that $\mathsf{R} \hookrightarrow \mathsf{L} \hookrightarrow \overline{\mathsf{L}}$. In this setting, we still have a Frobenius map $F : \mathsf{R} \to \mathsf{R}$ defined by $f \mapsto f^p$, as well as its iterates $F^e = F \circ F \cdots \circ F$. It is easy to check that $\mathsf{R}^p := F(\mathsf{R}) = \{f^p : f \in \mathsf{R}\}$ is still a subring of R, and as we did in Lecture 2, we can break up $F : \mathsf{R} \to \mathsf{R}$ as

$$\mathsf{R} \xrightarrow{F} F(\mathsf{R}) \subseteq R$$

where the portion $\mathsf{R} \xrightarrow{F} F(R)$ is an isomorphism of rings. Thus, just as in the polynomial ring case, $F(\mathsf{R}) = \mathsf{R}^p$ is a subring of R that is isomorphic to R. Anyway, iterating this, we get the chain

$$\ldots \subseteq \mathsf{R}^{p^e} \subseteq \ldots \subseteq \mathsf{R}^{p^2} \subseteq \mathsf{R}^p \subseteq \mathsf{R}.$$

where we define $\mathsf{R}^{p^e} := F^e(\mathsf{R}) = \{f^{p^e} : f \in \mathsf{R}\}$. The self-similar nature of this chain should be evident. Below, we discuss how to extend this chain infinitely to the right of the initial term R.

(1) We start with the definition of a p-th root, which is what you would expect.

> **Definition**: A p-th root of $f \in \mathsf{R}$ is any $g \in \overline{\mathsf{L}}$ such that $g^p = f$.

Prove that every element of R possesses a *unique* p-th root.
Hint: For existence, consider $x^p - f \in \mathsf{L}[x]$. For uniqueness, suppose that $f \in \mathsf{R}$ has two p-th roots α and β. Write out what this means to derive a relationship between α and β, and then apply Frobenius.

(2) We may now talk of *the* p-th root of an element of $f \in \mathsf{R}$, which we denote by $f^{1/p}$.

> **Definition**: $\mathsf{R}^{1/p} = \{f^{1/p} : f \in \mathsf{R}\}$, a subset of $\overline{\mathsf{L}}$.

Prove that $\mathsf{R}^{1/p}$ is a subring of $\overline{\mathsf{L}}$ and that R is a subring of $\mathsf{R}^{1/p}$.
Hint: Show that the sum and product of p-th roots is a p-th root.

(3) Make sense of the following statement: $\mathsf{R}^{1/p}$ is to its subring R as R is to its subring R^p.

(4) Describe how to iterate this operation to obtain an increasing sequence of subrings

$$\mathsf{R} \hookrightarrow \mathsf{R}^{1/p} \hookrightarrow \mathsf{R}^{1/p^2} \hookrightarrow \cdots \hookrightarrow \mathsf{R}^{1/p^e} \hookrightarrow \cdots$$

of $\overline{\mathsf{L}}$. Use this to extend the Frobenius fractal to infinity in both directions.

(5) What is $\mathsf{R}^{1/p}$, and more generally, R^{1/p^e}, when R is a polynomial ring over $\mathbb{F}_p$?

(6) Prove that if $f \in \mathsf{R}$ and $f^{1/p} \notin \mathsf{R}$, then the polynomial $m_f(x) = x^p - f \in \mathsf{L}[x]$ is irreducible in $\mathsf{L}[x]$, and thus, is the minimal polynomial of $f^{1/p}$ over L. **Note**: This is a more involved, is not crucial to the lecture series, and is meant as practice for working in characteristic p.
Hint: By means of contradiction, suppose that m_f is reducible in $\mathsf{L}[x]$. Why does this mean that we may write $m_f = gh$ with g an irreducible polynomial with $\deg(g) < p$? Why does this bound on $\deg(g)$ imply that g', the derivative of g with respect to x, is nonzero? Differentiate both sides of $m_f = gh$ to conclude that g must divide h. Iterate this to demonstrate that, up to a nonzero unit, m_f equals a power of g. What must this power be? Equivalently, what must the degree of g be? Finally, apply the assumption that the p-th root of f does not lie in R to derive a contradiction.

3. The Frobenius index of singularities

Let f denote a polynomial in $\mathsf{R} = \mathbb{F}_p[x_1, \ldots, x_n]$ vanishing at the origin, i.e., a polynomial contained in $\mathfrak{m}$, the ideal of R generated by the variables.

In lecture, we have/will define the Frobenius index of singularity at $\mathbf{0}$ of f to be the quantity

$$\mathrm{FIS}(f) = \mathrm{FIS}_{\mathbf{0}}(f) = \sup\left\{ \frac{i}{p^e} : i, e \in \mathbb{N}, \text{ and } f^i \notin \mathfrak{m}^{[p^e]} \right\}$$

which, according to an earlier problem, is obtained from the characterization for the reciprocal of $\mathrm{mult}(f)$, except we have replaced q by p^e, and the regular power $\mathfrak{m}^q$ with the Frobenius power $\mathfrak{m}^{[p^e]}$.

3.1. **Some basic facts.**

(1) Show that the condition that $f^i \notin \mathfrak{m}^{[p^e]}$ depends only on the fraction $\lambda = i/p^e$. For example, if we write $\lambda = ip/p^{e+1}$, show that condition corresponding to the first representation of λ holds if and only if the one corresponding to the second representation of λ holds.
Hint: Invoke a result from a previous problem.

(2) Apply the last part of Problem 2.1 to show that $\frac{1}{\mathrm{mult}(f)} \leq \mathrm{FIS(f)} \leq \frac{n}{\mathrm{mult}(f)}$.
Hint: Invoke a result from a previous problem that relates $\mathfrak{m}^{p^e}$ to $\mathfrak{m}^{[p^e]}$.

3.2. **Some examples.**

(1) Prove that if $f = x_1^{a_1} \cdots x_n^{a_n}$ is a monomial, then $\mathrm{FIS}(f) = \min\{1/a_1, \ldots, 1/a_n\}$.

(2) Prove that if f vanishes at the origin, but is nonsingular there, then $\mathrm{FIS}(f) = 1$.
Hint: In this case, what is the lowest degree part of f? Alternately, what is the multiplicity of f? Would an earlier bound be useful?

(3) We seek to compute the Frobenius index of singularity associated to the cusp $f = y^2 - x^3$. First, we need to know about the behavior of binomial coefficients modulo p.

> **Lucas' Theorem**: Consider positive integers $a < b$, and write the base p expansions of these integers as
>
> $$b = b_0 + b_1 p + \cdots + b_s p^s$$
> $$a = a_0 + a_1 p + \cdots + a_s p^s$$
>
> where each b_i and a_i is a natural number less than p, and $b_s \neq 0$. Then
>
> $$\binom{b}{a} \equiv \binom{b_0}{a_0} \cdots \binom{b_s}{a_s} \bmod p$$
>
> where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is the binomial coefficient, which is zero whenever $k > n$.

Prove Lucas' Theorem.
Hint: Look at the polynomial $(1+x)^b \in \mathbb{F}_p[x]$ in two different ways. First, expand using the binomial theorem. For the second way, instead write out the base p expansion of b, apply Frobenius, and only then apply the binomial theorem.

(4) Compute the Frobenius index of singularities of the cusp $f = y^2 - x^3 \in \mathbb{F}_p[x, y]$.
Note: I consider this to be very hard, so think of this as a serious challenge problem!
Hint: Expand f^t out using the binomial theorem, and make sure to apply Lucas' Theorem when you need to know that a binomial coefficient is nonzero modulo p. Maybe start by showing that the Frobenius index of singularities in this case is at most $5/6$. At the end of

the day, the answer turns out to be

$$\mathrm{FIS}(y^2 - x^3) = \begin{cases} 1/2 & p = 2 \\ 2/3 & p = 3 \\ 5/6 & p \equiv 1 \bmod 6 \\ 5/6 - 1/(6p) & p \equiv 5 \bmod 6 \end{cases}$$