p. 1: You wrote: Riemann alluded to returning to this matter later by “setting it aside for the time being.” I don’t think you’ve said what you meant here—it wasn’t the actual setting aside that was the allusion, it was his statement that he was setting it aside. So I think you meant something like this: Riemann alluded to returning to this matter later by saying that he was “setting it aside for the time being.”

You are a little inconsistent about whether the word “hypothesis” is capitalized in the phrase “Riemann hypothesis.” In the first paragraph it is, and then in the second paragraph it isn’t. In later pages it is occasionally capitalized, but usually it isn’t. You should be consistent; my preference would be not to capitalize it.

The grammar of the sentence “After laying out the statement of this result in §2 below, the main purpose . . . ” seems muddled to me, because the subject of “laying out” is missing from the sentence. You could say: “After laying out the statement of this result in Section 2 below, we turn to the main purpose of this article, which is twofold: . . . ” Feel free to try to come up with a different wording if you find this one awkward. (By the way, Monthly articles usually write “Section 2” rather than “§2”. You may want to change other instances of the symbol § as well.)

On p. 2, the first use of the phrase “Basic Identity” seems a little strange, since the identity hasn’t been defined yet. You might say something like “. . . except for an appeal to an identity that we will call the Basic Identity.”

Readers will surely be puzzled by the “provisional definition” of the zeta function of an elliptic curve. Perhaps you could add a parenthetical remark saying that the relationship between this definition and the Riemann zeta function will be explained in Section 3.

p. 3: The grammar of the last paragraph of Section 2 is muddled; “the existence” (singular) appears to be the subject of “have” (plural), the word “them” (plural) appears to refer to “the Riemann hypothesis” (singular), and the structure of “allowed them . . . while remaining” is not parallel. Perhaps you mean something like this: “Broadly speaking, it is the existence of such geometric interpretations that has allowed versions of the Riemann hypothesis for zeta functions in algebraic geometry to be proved, while the version involving Riemann’s original zeta function has remained so intractable.”

p. 4: In the first line of Section 3.1, you should define $K^\times$.

p. 7, Section 3.4: The referee is right that you need to say something about where the points of $C$ lie. The referee suggests saying that the coordinates are in the algebraic closure of $\mathbb{F}_q$, but I think it might be simpler to just say that they lie in a field that extends $\mathbb{F}_q$. (On the next page, you consider the case of points with coordinates in $\mathbb{F}_{q^m}$, but you don’t explicitly talk about the algebraic closure.) You say that the elements of $K$ are rational functions on $C$, but I think this requires a bit of explanation. As I understand it, the elements are really fractions $A/B$, where $A$ and $B$ are cosets in the quotient $\mathbb{F}_q[x, y]/(F(x, y))$. You seem to be identifying $A/B$ with the rational function $g/h$, where $g$ and $h$ are representatives of the two cosets. This makes sense because for $P \in C$, $F(P) = 0$, and therefore different representatives of the same coset will have the same value at $P$. This isn’t really hard to understand, but for people who have never seen it before a brief explanation would be helpful. Also, you talk about obtaining a one-to-one correspondence, but you don’t say between what and what. Is it between points and valuations? Do you ever actually get a
one-to-one correspondence? I don’t see that you do, so this sentence seems misleading to me.

p. 8: Example 3 requires a much better explanation. What does this have to do with the situation described at the bottom of p. 7? What is the affine line? In what sense does \( K = \mathbb{F}_3(x) \) correspond to it? Here’s what I think is going on here: You are considering the case \( q = 3 \) and \( F(x, y) = y \), so the curve \( C \) is given by the equation \( y = 0 \). (Is this curve \( C \) what you are calling the affine line?) This means each coset in \( \mathbb{F}_3[x, y]/(F(x, y)) \) has a unique representative that is just a polynomial in \( x \), so \( \mathbb{F}_3[x, y]/(F(x, y)) \) is isomorphic to \( \mathbb{F}_3(x) \), the field of rational functions of \( x \) with coefficients in \( \mathbb{F}_3 \). You are then taking points on the curve \( C \) with coordinates in the extension \( \mathbb{F}_3[i] \) of \( \mathbb{F}_3 \). Now you can apply the method from the bottom of p. 7 to get a valuation for each point on the curve. You need to explain this example in the language that was introduced on p. 7, otherwise readers won’t understand.

Later on this page, you use the notation \( \mathbb{P}^1_{\mathbb{F}_q} \). Is that the curve \( y = 0 \) that was discussed earlier? Does “points over \( \mathbb{F}_{q^m} \)” mean “points whose coordinates lie in \( \mathbb{F}_{q^m} \)”? So are you saying that for this \( C \), \( N_m(C) = (q^{2m} - 1)/(q^m - 1) \)?

p. 10: It might be a good idea to say that \( O \) is the zero of the group (that’s right, isn’t it?), and explain how to compute \(-P\) (since this comes up on p. 13).

I found the sentence “By the change of variable \( y = \sqrt{\lambda}y, \ldots \)” confusing, partly because I don’t see how \( y \) can be equal to \( \sqrt{\lambda}y \) (maybe this is the way experts write a change of variables, but something like \( y \rightarrow \sqrt{\lambda}y \) or \( y' = \sqrt{\lambda}y \) would make more sense to me) and partly because I don’t know what “represent the same elliptic curve” means. I wonder if this sentence is saying something that will be obvious to experts and confusing to nonexperts. If so, you might consider dropping it—as far as I can tell, this idea is never used in the rest of the proof.

p. 11: In the first sentence of Section 4.2, “A crucial ingredient” (singular) is the subject of “are” (plural), so something needs to be changed. I think some of the material in the rest of this paragraph should come earlier in the paper, and some should be cut. The field \( \mathbb{F}_q \) first comes up p. 2, and extensions of the form \( \mathbb{F}_{q^m} \) come up on p. 8, so I think it makes sense to discuss these ideas earlier. As far as I can tell, the relationships among \( \mathbb{F}_{p^r}, \mathbb{F}_{p^s}, \mathbb{F}_{p^rs} \), and \( \overline{\mathbb{F}}_q \) are never used; in fact, the algebraic closure is never mentioned again. Is there any need to talk about these things? I found the sentence beginning “Thus” confusing, because I don’t see how it follows from the previous sentence.

p. 12: The phrase “the binomial coefficient” in the middle of the page is confusing, because what follows this phrase is not a binomial coefficient but rather a displayed equation involving the binomial coefficient. You can either cut the phrase, or change it to something like “the binomial coefficient \( \binom{j}{k} \) satisfies”.

p. 13: The introduction of the degree function is a little confusing, because you describe it as a quadratic polynomial, but that’s not what the definition says. The reader may be a little unsure whether the degree function you are referring to is the function \( d \). We don’t find out that \( d \) can be expressed as a quadratic polynomial until p. 15.

p. 14: I found the argument here slightly confusing. The fraction we want to reduce to lowest form is of course the last one on p. 13, not the previous one. If we reduce the previous one, then one might think that the last step on p. 13 is no longer relevant. I would find it slightly clearer to phrase it like this: We want to reduce the last fraction to lowest form,
so we must determine which factors of the denominator will be canceled. Since the term $(t^9 + t)$ has no denominator, the factors that will cancel in the last fraction are the same as the factors that will cancel in the previous one, so it suffices to determine which factors will cancel in the previous one.