

## Review of “A $p$ -adic Euclidean Algorithm,” by Courtney Lager

This paper presents an analog of the Euclidean Algorithm over the  $p$ -adic rationals, inspired by Browkin’s continued fraction algorithm for  $p$ -adic numbers. It incorporates some nice ideas accessible to undergraduates, most notably the  $p$ -adics, and it is a good example of a construction in a new setting to parallel a classical object. From what I understand about the RHIT Undergraduate Journal, this paper should be a good fit for the journal, and I recommend it for publication.

I have a few structural comments and then a lot of minor comments. Most of them are recommendations, not requirements, leaving the option to the author.

---

### Structural:

–The paper needs a proper introduction. Most of Section 1 should be moved to a (new) second section. The first section should be pure introduction, saying what is going to be done in the paper. So for example, most of (an appropriately edited version of) the first paragraph of Section 4 should be moved to the beginning of the paper, rather than the end. (Math papers traditionally say what they are going to do in the first few pages and then **do not** say what they have done at the end.) This new first section should also say that there are other ways than the reals to complete the rational numbers, but probably **not** go into the discussion of  $p$ -adic absolute values and  $p$ -adic numbers. (Leave that for the new second section.) It should also lay out the rest of the paper. Something like: “In Section 2, we will describe the  $p$ -adic numbers, and in Section 3 we will present our  $p$ -adic Division Algorithm and Euclidean Algorithm. In Section 4 we will present some applications, including a connection to Browkin’s  $p$ -adic continued fractions, which motivated our investigations in the first place. Finally, in Section 5, we will present some open questions for further study.”

–The current first few sentences of the current paper should probably be scrapped. I think the author is trying too hard to go quickly from mentioning the Euclidean algorithm to the reals, and then to motivate the  $p$ -adics. But the Euclidean algorithm is really not related to the reals. (Or if it is, the author should make that case very clearly and explicitly.) Instead, I’d recommend saying just a bit more about the Euclidean algorithm itself (avoiding vague phrases like “tell us important things”) and then **separately** mention that there is this other number system  $\mathbb{Q}_p$  containing the rationals. Then say that the goal of the paper is to present and discuss a  $p$ -adic version of the classical algorithm.

### Other Comments:

–Since we have multiple absolute values in this paper, the usual absolute value should **always** be referred to as “the standard absolute value” or “the familiar absolute value” or “the usual absolute value,” and **not** simply “the absolute value,” to be absolutely clear what we are talking about. Similarly, the notation  $|\cdot|$  should be avoided for the same reason. Number theorists dealing with both the standard and  $p$ -adic absolute values settle this by using the notation  $|\cdot|_\infty$  for the usual absolute value. This can be introduced by a sentence early on like, “Since we will use different absolute value functions in this paper, to avoid confusion, we will denote the standard absolute value as  $|\cdot|_\infty$  rather than  $|\cdot|$ .” Then change **all** subsequent appearances of  $|\cdot|$  to  $|\cdot|_\infty$ .

–I would recommend against calling an absolute value a “norm.” (The term “norm” is weaker, as it does not include any requirements on what  $|ab|$  is in relation to  $|a|$  and  $|b|$ .)

Instead, the current fourth sentence of the paper should be rephrased more like, “However, there are other absolute values on the rationals besides the standard one.”

–When  $|\cdot|_p$  is introduced, it should be written as  $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}$ , so we know what we’re talking about. (Otherwise, a reader who has never seen it before might think one can take the  $p$ -adic absolute value of any **real** number, too, which of course we can’t.) Also, the definition given only works for nonzero numbers; the clause “and  $|0|_p = 0$ ” needs to be added.

–The specification that  $p$  is odd throughout the paper is only said once, and it’s hidden in the middle of an obscure paragraph. This hypothesis needs to be more clearly advertized. For example, it should be repeated in the statements of Theorem 1 and Definition 2. (“Let  $p$  be an odd prime.”)

–In Definition 1,  $\zeta$  is a **Laurent** series in  $p$ , not a power series. (Same change to be made on the first line of the current page 2.)

–p2, l2: To make the sentence not a run-on, change “however” to “although”.

–p2, l5: “naively” makes it sound like the calculation that follows is not on stable footing. But the **same** proof of the geometric series rule, using the  $p$ -adic rather than the standard absolute value, gives the result. I’d recommend deleting the word “naively,” and possibly saying briefly that the geometric series test still applies to the  $p$ -adic absolute value and to convergence in  $\mathbb{Q}_p$ .

–p2, l10: **NOT** every  $\zeta \in \mathbb{Q}_p$  can be written as claimed. Instead, every  $\zeta \in \mathbb{Q}_p \setminus \{0\}$  can be written that way. (This also needs to be corrected numerous places later in the paper.)

–p2, l11: “non-archmedian” should be “non-archimedean.”

–p2, l12: Later, in the proof of Theorem 2, we use (implicitly) the fact that the non-archimedean triangle inequality gives equality if  $|\zeta_1|_p \neq |\zeta_2|_p$ . So that fact should be stated explicitly here.

–p2, l18: I’d recommend adding “; that is, it is a subring of  $\mathbb{Q}$ ” to the end of the sentence noting that  $\mathbb{Z}[\frac{1}{p}]$  is closed under addition and multiplication. (Maybe “in fact” instead of “that is”, since we never explicitly said it was nonempty and also closed under negatives.)

–p2, Theorem 1: The hypothesis that  $\tau \neq 0$  **must** be added, or else the statement is false. (Note that we use this hypothesis in the proof, when writing  $\tau = tp^{v(\tau)}$ . It is not needed for  $\sigma$ , because at that point in the proof, we have  $|\sigma|_p \geq |\tau|_p > 0$ .) Also, as noted earlier, begin with “Let  $p$  be an odd prime.”

–p2, l-11,-10:  $s$  and  $t$  are elements of  $\mathbb{Q}_p$ , so it is a little inappropriate to write  $p \nmid s, t$ . Instead, write  $|s|_p = |t|_p = 1$ , as on line 10 of this page.

–p2, l-7: here, when introducing  $\eta$ , write “Then let  $\eta = \dots$ ” instead of “Then  $\eta = \dots$ ”.

–p2, l-7: again, the statement  $p^{v(\tau)+1}|\eta$  is inappropriate, because  $\eta \in \mathbb{Q}_p$ , and (if  $v(\tau) \leq -2$ )  $p^{v(\tau)+1}$  could be a non-integer rational number. Instead, say that  $v(\tau) + 1 \leq v(\eta)$ , and therefore  $|\eta|_p < |\tau|_p$ , perhaps.

–p2, l-3,-2: The phrasing flows more smoothly if the big displayed equation ends with a comma (instead of a period), and “This implies” is changed to “which implies”.

–p3, Definition 2. “p-adic” should be “ $p$ -adic” (note math mode). As previously noted, add the sentence, “Let  $p$  be an odd prime.” Also, add the specification that  $\tau \neq 0$ .

–p4, l2: A period is needed at the end of this displayed equation.

–p4, Theorem 2: again, specify  $p$  is an odd prime and  $\tau \neq 0$ .

–p4, l9: In this first sentence of the proof, things need to be introduced and stated more carefully. First of all, add words like, “For all  $i$  such that  $q_i, \eta_i \neq 0$ , write” at the start, or else the rest of the sentence is impossible. Second, specify explicitly that  $\epsilon_i = v(\eta_i)$ ,  $\delta_i = v(q_i)$ ,

and  $|h_i|_p = |c_i|_p = 1$ . (You may even wish to eliminate the  $\epsilon_i$  and  $\delta_i$  notation entirely and write  $v(\eta_i)$  and  $v(q_i)$ , but that is your choice.) Also, delete the word “information” at the end of the line.

–p4, l10: Point (i) is **not** obvious from the **statement** of Theorem 1. It relies first on the equality version of the non-archimedean triangle inequality (see my earlier comment), but more importantly, we need to know not only that  $|\eta_i|_p < |\eta_{i-1}|_p$  (which does indeed follow from Theorem 1 but bears explicit repeating) but also that  $|q_i|_p \geq 1$ , which follows from the **proof** of Theorem 1. (Incidentally, we also need the assumption I added above, that that  $q_i \neq 0$ , to conclude that  $|q_i|_p \geq 1$ .)

Here are two possible ways to fix this. One is to restate the **statement** of Theorem 1 to add the sentence, “If  $q \neq 0$ , then  $|q|_p \geq 1$ .” (And then, of course, observe in the proof that this statement is true.) The other is to add a Remark immediately following the proof of Theorem 1, saying something like, “Note in the proof of Theorem 1 that if  $q \neq 0$ , then in fact  $p \nmid \bar{q}$ , and therefore  $v(q) = v(\sigma) - v(\tau) \leq 0$ ; that is,  $|q|_p \geq 1$ .”

Then, in this proof of Theorem 2, say that because  $|q_i|_p \geq 1$  and  $|\eta_i|_p < |\eta_{i-1}|_p$  by Theorem 1 (or by Theorem 1 and Remark 2), we have  $|q_i \eta_{i-1}|_p > |\eta_i|_p$ , and therefore  $|\eta_{i-2}|_p = |q_i \eta_i - 1|_p$ . Thus,  $\delta_i + \epsilon_{i-1} = \epsilon_{i-2}$ .

–p4, l13: insert a comma before “and” (as should be done many places in the paper), and add a word like “therefore” at the end of the line. Also, it is **crucial** to note **explicitly** that  $h_i$  (and  $c_i$ ) lie in  $\mathbb{Q}$ , and not just  $\mathbb{Q}_p$ — that is, so that it makes sense to even talk about  $|h_i|_\infty$ . (FYI: from here to the end of the proof is probably the most important place where the  $|\cdot|$ ’s should be  $|\cdot|_\infty$ ’s, but of course that change should already have been made everywhere.)

–p4, l-7: “positive sequence” is a little awkward. Perhaps, “consider the sequence  $\{|h_{i-1}|_\infty + 2|h_i|_\infty\}_i \geq 1$  of positive rational numbers.”

–p5, l3-5: Substantially shorten these sentences; just say something like, “Recall the following definition.” After all, it has been assumed earlier in the paper that the reader knows what an lcm is, so presumably the same reader already knows what a gcd is.

–p5, l3,6,13: In these three places (and possibly others), the notation  $(a,b)$  needs to be  $(a, b)$ ; that is, in math mode.

–p5, Definition 3: Rather than try to list a lot of little complaints, here is a suggested rephrasing: “Let  $a, b \in \mathbb{Z}$ , not both zero. Then the greatest common divisor, or gcd, of  $a$  and  $b$  is the unique positive integer  $g = (a, b) = \gcd(a, b)$  that satisfies the following properties:”

(The most important changes there are that  $a, b$  can’t both be zero, or else this definition collapses; and the word “unique” needs to appear somewhere. The rest of the changes are also important but merely grammatical or stylistic.)

(Also, in property (i), the comma goes **before** “and”, not after it. And in property (ii), it should be “if there exists  $f \in \mathbb{Z}$ ” (or maybe  $f \in \mathbb{Q}$ ; your choice) and not “if there exists  $f$ ”.)

–p5, l10,11: The specification that  $a/b$  and  $c/d$  are written in lowest terms is needed here. Also, the notation  $(a/b, c/d)$  is used here, but a few lines later (in Theorem 3) it is  $\gcd(a/b, c/d)$ ; the notation should be consistent.

More importantly, some justification needs to be given that this new definition deserves to be called a gcd. In particular, thinking ahead to the proof of Theorem 3, it should be stated (probably as a proposition or lemma or something) that the gcd of two rational numbers (again, not both zero) satisfies some appropriate (and again, **explicitly written out**) analog of Definition 3. Then, of course, either a proof should be given of this new

proposition/lemma, or it should be referenced to a result in some textbook or published paper. Otherwise, the proof of Theorem 3 has a gap.

–p5, Theorem 3: Again, the specification that  $\sigma$  and  $\tau$  are nonzero needs to be added here. (Otherwise,  $s$  and  $t$  cannot be defined.) Oh, and “ $k$ -steps” shouldn’t have a hyphen.

Also, the specification that  $\epsilon_i = v(\eta_i)$  needs to be made when that notation is introduced. (That is, so that  $|h_i|_p = 1$ .) Better yet, skip mentioning the notation  $\epsilon_i$  at all and simply say, “write  $\eta_i = h_i p^{v(h_i)}$ ”; after all,  $\epsilon_i$  appears only once in the proof (as  $\epsilon_1$ , in one of the later equations).

–p5, l-9: Put more space around the word “and” in this displayed equation; otherwise, it’s hard to read.

–p5, l-8: Before “Then”, a sentence like, “Note that  $v(f) \leq 0$ , since  $v(s) = v(t) = 0$ ,” needs to be added. (It also needs to be justified using the souped-up statement of Theorem 1 or Remark following Theorem 1 that I requested in a comment above.)

–p5, l-5: “Euclidean” is misspelled.

–p6, l10: It’s been a while since equation (1), so it would be good to insert “with  $v(\zeta) = m$ ” after “For  $\zeta$ ”.

–p6, Theorem 4: The specification that  $\zeta \in \mathbb{Q}_p$  should be at the beginning of the statement of the Theorem, not in the second sentence (after  $\zeta$  has already been mentioned in the first).

–p6, Theorem 5: same complaint: begin with, “Let  $\zeta \in \mathbb{Q}_p$ , and let  $q_i \dots$ ”. Also, period before “then” (which of course therefore should become “Then”).

–p7, end of section 3. After Theorem 2, I found myself wondering whether the  $p$ -adic Euclidean algorithm necessarily **didn’t** terminate if  $\sigma$  and  $\tau$  weren’t rational. I soon realized that of course, if  $\sigma/\tau$  were rational, then Theorem 2 would imply that the algorithm terminates (even if  $\sigma$  and  $\tau$  themselves weren’t rational). Now Theorem 5 settles the question: if  $\zeta = \sigma/\tau$  is **not** rational, then the  $p$ -adic continued fraction for  $\zeta$  cannot be finite (since finite continued fractions are rational), and therefore by Theorem 5, the algorithm for  $\zeta$  doesn’t stop. Hence the algorithm for  $\sigma$  and  $\tau$  (for which all of the equations are the same as those for  $\zeta$  and 1, but with each equation multiplied by  $\tau$ ) also does not stop.

Anyhow, I think this is worth mentioning. That is, I think it’s very natural for a reader to ask the same question I did after reading Theorem 2, and since you’ve already done all the hard work involved in providing an answer by doing Theorem 5, you may as well answer the question in full (as “Theorem 6” or something).

–p7, l-4: “we”, not “you”. “You” and “I” never do anything in a math paper, but “we” do everything.

–p8, l6: “University” is misspelled.

–p8, bibliography: another well-known and absolutely great undergraduate reference for the  $p$ -adics is *p-adic Numbers: An Introduction*, by Fernando Gouvêa. (Universitext, Springer-Verlag, Berlin, 1993.)

–Throughout the paper: a lot of commas are out of place. Commas should usually appear before “and” (at least when separating clauses, including mathematical clauses) and (usually) before “then”, but (usually) **not** after “then”. Commas **should** come after “hence,” “however,” and similar words.