Lagrange’s Proof of the Converse of Wilson’s Theorem

Carl Lienert*

October 18, 2023

Joseph-Louis Lagrange (1736–1813) was an Italian-born mathematician of French descent. He succeeded Leonhard Euler (1707–1783) as Director of Mathematics at the Berlin Academy, a post that Lagrange then held for 20 years. Lagrange left Berlin in 1787 for a post at the Académie des Sciences in Paris. Unlike Louis XVI, King of France, who offered him the post, Lagrange kept his head down (and hence on!) during the Reign of Terror. In 1794, Lagrange became one of the original professors at the famous *École Polytechnique* where he continued to produce important mathematics.[1] Near the end of his life, Napoleon honored Lagrange for his life’s work by naming him to the Legion of Honour.

Perhaps Lagrange’s largest body of mathematical work[2] was in the area of analysis. He also made contributions to the theory of equations which influenced the development of group theory and Galois theory.[3] In this project, we’ll study one of his many contributions to number theory through excerpts from a paper that Lagrange wrote early in his tenure in Berlin [Lagrange, 1771]. Despite its unremarkable title, “Démonstration d’un Théorème Nouveau Concernant les Nombres Premiers” (“Proof of a New Theorem Concerning Prime Numbers”), its content is quite remarkable. Lagrange began by stating the new theorem that he wished to prove as follows:[4]

> I just found, in an excellent work of Mr. Waring that I recently received, a beautiful arithmetic[5] theorem,
>
> *If n is any prime number, the number*
>
> $$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots (n-1) + 1$$
>
> *will always be divisible by n;*
>
> that is, the continual product of numbers $1, 2, 3, \ldots$ until $n-1$ inclusively, being augmented by one, will be divisible by n, or in other words, if one divides this product by the prime number n, one will have -1, or equivalently, $n-1$ as remainder.

*Department of Mathematics, Fort Lewis College, Durango, CO, 81301; lienert_c@fortlewis.edu.

[1] See https://mathshistory.st-andrews.ac.uk/Biographies/Lagrange/ for comment on Lagrange’s teaching skills, as well as more information about his life and works.

[2] Lagrange also made important contributions to the study of astronomy, the stability of the solar system, mechanics, dynamics, and fluid mechanics.

[3] The project [Barnett, 2017] presents Lagrange’s work in the theory of equations.

[4] All translations of Lagrange’s paper in this project were prepared by the project author with minor adjustments for readability.

[5] Today, we would say “number theoretic” where Lagrange wrote “arithmetic.”

Task 1 Why do you think that Lagrange found this to be a "beautiful arithmetic theorem"? What purpose do you think it could serve in number theory? Does it remind you of other theorems you have seen in number theory, or mathematics more generally?

Lagrange went on to explain:

> Mr. Waring honors Mr. John Wilson with this theorem, but he doesn't give a proof, and he even seems to imply that no one has yet found a proof; at least it seems he considers finding the proof would be extremely difficult, ... He [Waring] adds "Proofs of propositions of this kind will be all the more difficult, because no notation can be imagined by which to express a prime number."

Edward Waring (1736–1798) was a Lucasian Chair of Mathematics at St. John's College, Cambridge. John Wilson (1741–1793) was a student of Waring.[6] It would be interesting to know how many values of n Wilson checked before arriving at his proposition.[7] For $n = 17$, the number to check has 14 digits. Lagrange recorded the result through $n = 13$ in his paper, a value for which he found that $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 + 1 = 13 \cdot 36846277$.

While Lagrange gave fair credit to Waring and Wilson for stating the theorem, he also seems to have been proud of his own proof. In fact, Lagrange gave two proofs of what today is known as Wilson's Theorem, one of which implied a famous result known as Fermat's Little Theorem, and a second that assumed Fermat's Little Theorem. He also gave a proof of the converse of Wilson's Theorem, which is the topic of this project.[8]

1 Proving the Converse of Wilson's Theorem

We start by restating Wilson's Theorem:

> *If n is any prime number, the number*
>
> $$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots (n-1) + 1$$
>
> *will always be divisible by n;*

[6] See https://mathshistory.st-andrews.ac.uk/ for some interesting information about Waring and Wilson.

[7] Optional Task: To get a feel for the theorem and the sort of computation that Wilson must have performed, do a quick verification of Wilson's Theorem for some small primes (e.g., $n = 2$, $n = 5$, $n = 7$, $n = 11$), but without using a calculator or other modern computational device.

[8] You can work through Lagrange's first proof of Wilson's Theorem and the implication of Fermat's Little Theorem in the related project "Lagrange's Proof of Wilson's Theorem – and More!" [Lienert, 2023a] and the alternate proof of Wilson's Theorem in the project "Lagrange's Alternate Proof of Wilson's Theorem" [Lienert, 2023b]. The material of each of the three projects is developed independently.

Task 2 State the converse of Wilson's Theorem.

Task 3 Demonstrate the converse with at least two numerical examples.

Lagrange's proof of the converse was concise:

> . . . if n is not prime, the number $[1 \cdot 2 \cdot 3 \cdots (n-1)+1]$ that we have seen must be divisible by n under the hypothesis that n is prime, will no longer be. Because if n is not a prime number, it will thus be divisible by one of the numbers $2, 3, \ldots, n-1$ less than n. Thus if
>
> $$1 \cdot 2 \cdot 3 \cdot (n-1)+1$$
>
> were divisible by n, then it would necessarily also be divisible by one of the numbers 2, 3, . . ., $(n-1)$. But this cannot be; because the number $1 \cdot 2 \cdot 3 \cdots (n-1)$ being divisible by each of these numbers, it is clear that in dividing by any of these numbers the number
>
> $$1 \cdot 2 \cdot 3 \cdots (n-1)+1$$
>
> will always have one as remainder.

Task 4 Explain why the first sentence of this excerpt is equivalent to the converse of Wilson's Theorem. Your answer to Task 2 should be useful here. It will help to rewrite the first sentence in the form "if . . ., then . . .," and keep this sentence in view while you work through the tasks below.

To understand Lagrange's argument, it will help to rephrase the last three sentences with the quantifiers "for some" and "for all" and to introduce another variable. It will also help to be explicit about Lagrange's statements concerning divisibility and remainders. This means using the following theorem:

> **Division Theorem.** For integers a and b, $b > 0$, there exist unique integers q and r with $0 \leq r < b$ such that $a = bq + r$, where r is called the remainder.

To help keep track of each part of the argument, we provide each sentence of the excerpt one at a time.

> Because if n is not a prime number, it will thus be divisible by one of the numbers $2, 3, \ldots, n-1$ less than n.

This tells us that the working assumption in Lagrange's argument was that n is *not* prime. Lagrange was explicit about what this assumption means with his statement ". . . it will thus be divisible by one of the numbers $2, 3, \ldots, n-1$ less than n."

Task 5 Rephrase the statement

> "... it will thus be divisible by one of the numbers $2, 3, \ldots, n-1$ less than n"

using a quantifier and an introduced variable, k. Your sentence will include: a quantifier, a condition on the range of k, and a divisibility statement.

We move to the next sentence in the argument:

> Thus if
>
> $$1 \cdot 2 \cdot 3 \cdot (n-1) + 1$$
>
> were divisible by n, then it would necessarily also be divisible by one of the numbers 2, 3, ..., $(n-1)$.

Task 6 When Lagrange wrote "if $1 \cdot 2 \cdot 3 \cdot (n-1) + 1$ were divisible by n ...," what type of proof was he setting up?

So, now we'll pursue the consequence of the assumption "*if* n divides $1 \cdot 2 \cdot 3 \cdots (n-1) + 1$." Remember, we are also assuming that n is not prime; keep your answer to Task 5 in mind.

Task 7 Rephrase the statement

> "it would necessarily also be divisible by one of the numbers 2, 3, ..., $(n-1)$"

using a quantifier and the introduced variable k. Your sentence will include: a quantifier, a condition on the range of k, and a divisibility statement. Also be explicit about what number the pronoun "it" refers to here.

Task 8 With the Division Theorem in mind, what is the remainder when we divide the quantity $1 \cdot 2 \cdot 3 \cdots (n-1) + 1$ by the value of k from Task 7?

And, finally, the concluding sentence in the argument:

> But this cannot be; because the number $1 \cdot 2 \cdot 3 \cdots (n-1)$ being divisible by each of these numbers, it is clear that in dividing by any of these numbers the number
>
> $$1 \cdot 2 \cdot 3 \cdots (n-1) + 1$$
>
> will always have one as remainder.

Task 9 Rephrase the statement

"the number $1 \cdot 2 \cdot 3 \cdots (n-1)$ being divisible by each of these numbers"

using a quantifier and the introduced variable k. Your sentence will include: a quantifier (careful!), a condition on the range of k, and a divisibility statement.

Task 10 Repeat the same division done in Task 8: what is the remainder when we divide $1 \cdot 2 \cdot 3 \cdots (n-1) + 1$ by k?

Task 11 Does the fact that the quantifiers from Task 7 and Task 9 are different present a problem with the argument? Explain why or why not.

Task 12 Explain how your answers to Tasks 8 and 10 complete the argument of the converse of Wilson's Theorem.

Having completed his proof of the converse of Wilson's Theorem, Lagrange continued and claimed this gave a primality test. That is, if we want to determine whether a given number n is prime, we could check whether n divides the number $1 \cdot 2 \cdot 3 \cdots (n-1) + 1$ or not. He confessed:

> I'll admit that this method would be extremely laborious and almost impractical when n is a very large number; but maybe there are ways to simplify the method; it's an open question to which we invite the Geometers.

Task 13 Illustrate how the converse to Wilson's Theorem is a primality test by using it to show 6 is not prime. Why will this process be impractical if we attempt it for a number much larger than 6?

2 Conclusion

In this project, we have studied Lagrange's proof of the converse of Wilson's Theorem. We've also seen that the converse provides a primality test, albeit an impractical one. In fact, the converse in this case turns out not to be particularly useful beyond providing mathematical completeness to the theory surrounding Wilson's Theorem. Lagrange's proof of the converse of Wilson's Theorem also provides an interesting and instructive example of a proof involving the contrapositive, contradiction, and multiple quantifiers.

Wilson's Theorem itself, on the other hand, has played an important role in mathematics developed after Lagrange. One example is the problem of quadratic reciprocity which asks the question: "*for what values of a does a given prime p divide $x^2 - a$?*" Wilson's Theorem is often used in proofs of the Law of Quadratic Reciprocity, which gives the answer to this question, and in many others that you can find in textbooks on number theory and abstract algebra.

As noted in the introduction of this project, Lagrange's proof of the converse of Wilson's Theorem comprised only part of his 1771 paper. The main part of that paper was his presentation of the first published proof of Wilson's Theorem and its implication of Fermat's Little Theorem, of which Lagrange was justifiably proud. You can explore that proof in the project "Lagrange's Proof of Wilson's Theorem—and More!" [Lienert, 2023a]. Later in his paper, Lagrange also provided a second proof of Wilson's Theorem that started from Fermat's Little Theorem, which you can explore in the project "Lagrange's Alternate Proof of Wilson's Theorem" [Lienert, 2023b].

References

Janet Heine Barnett. The Roots of Early Group Theory in the Works of Lagrange. 2017. Primary Source Project available at https://digitalcommons.ursinus.edu/triumphs_abstract/2/.

Joseph-Louis Lagrange. Démonstration d'un Théorème Nouveau Concernant les Nombres Premiers (Proof of a New Theorem Concerning Prime Numbers). *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin, année 1771*, pages 425–438, 1771. Also in *Œuvres de Lagrange*, Tome 3, pp. 425–440.

Carl Lienert. Lagrange's Proof of Wilson's Theorem—and More! 2023a. Primary Source Project available at https://digitalcommons.ursinus.edu/triumphs_number/14/.

Carl Lienert. Lagrange's Alternate Proof of Wilson's Theorem. 2023b. Primary Source Project available at https://digitalcommons.ursinus.edu/triumphs_number/16/.

Notes to Instructors

PSP Content: Topics and Goals

This Primary Source Project (PSP) is intended for an introductory number theory course. It could also be used in an Introduction to Proofs course that included some treatment of number theory. The prerequisites are minimal; any student with a bit of mathematical maturity should be able to work through the project.

This project is based on Lagrange's proof of the converse to Wilson's Theorem. While the converse may not play as large a role as Wilson's Theorem itself, Lagrange's proof is pedagogically interesting, especially for students who are new to proof writing.

In his 1771 paper, Lagrange also provided two different proofs of Wilson's Theorem, the first without the assumption of Fermat's Little Theorem and the second starting from that assumption. These proofs are featured in the related PSPs "Lagrange's Proof of Wilson's Theorem—and More!" and "Lagrange's Alternate Proof of Wilson's Theorem," respectively. The projects in this trio of PSPs are independent of each other. While they can also be implemented in any order, instructors who choose to implement the PSP based on his first proof along with either or both of the others will probably want to begin with the "first proof" project. Since the introductory sections of the three projects are nearly identical, students would not need to re-read that section in the later project(s) implemented. The two PSPs featuring proofs of Wilson's Theorem also have identical concluding sections.

There is also a fourth project, entitled "Lagrange's Study of Wilson's Theorem," which includes all the above results. It is available (along with the three shorter projects) at https://digitalcommons.ursinus.edu/triumphs_number.

Student Prerequisites

The project should be accessible to students early in a first course on number theory. Students should have some familiarity with the definition of divisibility. Basic divisibility results (e.g., if $a|b$ and $b|c$, then $a|c$) appear sparingly. The Division Theorem is useful in both sections, but is stated at the appropriate junctures in each in a form that will be understandable even to students who have not formally seen it yet. Students will need to be able to provide the converse of a statement and the contrapositive. They will also need to think about quantifiers "for all" and "for some."

PSP Design and Task Commentary

The project begins with a short historical introduction. It then continues with Lagrange's proof of the converse of Wilson's Theorem, which is quick.

The possibility of using the converse of Wilson's Theorem as a primality test is briefly discussed towards the end of this section.

Suggestions for Classroom Implementation

Ideally, I would have students work on the answers to the Tasks in small groups during class time, with an occasional whole-class discussion as appropriate. That said, I think the best practice for classroom implementation is to respond to the dynamics of the students in your classroom. Individual instructors should naturally adjust according to their own strengths and preferences, and those of their students.

LaTeX code of this entire PSP is available from the author by request to facilitate preparation of advanced preparation / reading guides or 'in-class worksheets' based on tasks included in the project. The PSP itself can also be modified by instructors as desired to better suit their goals for the course.

Sample Implementation Schedule (based on a 50-minute class period)

The project is a one-day activity. As advance preparation, assign the introduction and Tasks 1–3 as homework the day before the project is completed in class.

Connections to other Primary Source Projects

The following additional projects based on primary sources are also freely available for use in teaching standard topics in an introductory course on number theory. The PSP author name of each is given (together with the general content focus, if this is not explicitly given in the project title). Classroom-ready versions of these projects can be downloaded from `https://digitalcommons.ursinus.edu/triumphs_number`. They can also be obtained (along with their LaTeX code) from their authors.

- *Gaussian Integers and Dedekind's Creation of an Ideal: A Number Theory Project*, Janet Heine Barnett (8 days)
- *Generating Pythagorean Triples: A Gnomonic Exploration*, Janet Heine Barnett (1–2 days)
- *Greatest Common Divisor: Algorithm and Proof*, Mary K. Flagg (3–4 days)
- *Lagrange's Proof Wilson's Theorem—and More!*, Carl Lienert (2–3 days)
  Based on the same paper as the current PSP. Gives Lagrange's first proof and the implication of Fermat's Little Theorem.
- *Lagrange's Alternate Proof of Wilson's Theorem*, Carl Lienert (1 day)
  Based on the same paper as the current PSP. Gives Lagrange's second proof of Wilson's Theorem, using Fermat's Little Theorem as a starting point.
- *Lagrange's Study of Wilson's Theorem*, Carl Lienert (5 days)
  Based on the same paper as the current PSP. Unifies the results of the three related shorter projects listed above into a single project.
- *Primes, Divisibility, and Factoring*, Dominic Klyve (5–7 days)
  This project discusses the Fermat-Euler Theorem which appears in the current PSP.
- *The Mobius Function and Mobius Inversion*, Carl Lienert (8 days)
- *The Origin of the Prime Number Theorem*, Dominic Klyve (2 days)
- *The Pell Equation in India*, Toke Knudsen and Keith Jones (3 days)

Acknowledgments

The development of this student project has been partially supported by the TRansforming Instruction in Undergraduate Mathematics via Primary Historical Sources (TRIUMPHS) Program with funding from the National Science Foundation's Improving Undergraduate STEM Education Program under Grant Nos. 1523494, 1523561, 1523747, 1523753, 1523898, 1524065, and 1524098. Any opinions, findings, and conclusions or recommendations expressed in this project are those of the author and do not necessarily represent the views of the National Science Foundation.

For more information about TRIUMPHS, visit https://blogs.ursinus.edu/triumphs/.