



Ursinus College

Digital Commons @ Ursinus College

Number Theory

Transforming Instruction in Undergraduate
Mathematics via Primary Historical Sources
(TRIUMPHS)

Summer 2023

Lagrange's Alternate Proof of Wilson's Theorem

Carl Lienert

Follow this and additional works at: https://digitalcommons.ursinus.edu/triumphs_number



Part of the Curriculum and Instruction Commons, Educational Methods Commons, Higher Education Commons, Number Theory Commons, and the Science and Mathematics Education Commons

[Click here to let us know how access to this document benefits you.](#)

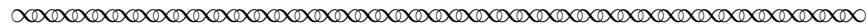
Lagrange's Alternate Proof of Wilson's Theorem

Carl Lienert*

May 25, 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 Lagrange's life, Napoleon honored him for his life's work by naming him to the Legion of Honour.

Perhaps Lagrange's largest body of mathematical work² 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



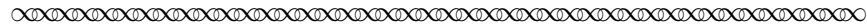
I just found, in an excellent work of Mr. Waring that I recently received, a beautiful arithmetic⁵ theorem,

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, ... 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.

¹See <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.

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

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

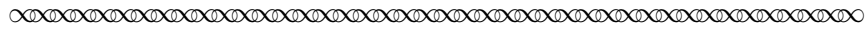
⁴All translations of Lagrange's paper in this project were prepared by the project author with minor adjustments for readability.

⁵Today, we would say "number theoretic" where Lagrange wrote "arithmetic."

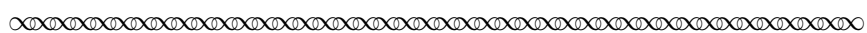
Task 1

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.”

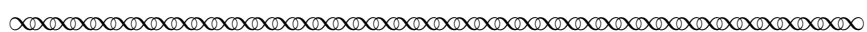


Edward Waring (1736–1798) was a Lucasian Chair of Mathematics at St. John's College Cambridge. John Wilson (1741–1793) was a student of Waring.⁶ It would be interesting to know how many values of n Wilson checked before arriving at his proposition.⁷ For $n = 17$, the number to check has 14 digits. Lagrange recorded 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 which implied a famous result known as Fermat's Little Theorem and a second which assumed Fermat's Little Theorem, and also gave a proof of its converse. This project studies Lagrange's second proof of Wilson's Theorem.⁸

1 An Alternate Proof of Wilson's Theorem

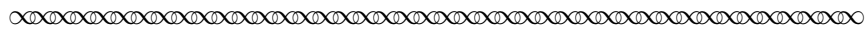
We start here by re-stating Wilson's Theorem:



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 ;



⁶See <https://mathshistory.st-andrews.ac.uk/> for some interesting information about Waring and Wilson.
⁷Optional 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.
⁸You 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 his proof of the converse of Wilson's Theorem in the project “Lagrange's Proof of the Converse of Wilson's Theorem” [Lienert, 2023b]. The material of each of the three projects is developed independently.

Lagrange used his first proof of Wilson’s theorem to prove Fermat’s Little Theorem as a consequence.⁹ More specifically, he showed that both Fermat’s Little Theorem and Wilson’s Theorem follow from a certain divisibility statement that he derived as part of his first approach to proving Wilson’s Theorem. The latter theorem can be stated as follows.

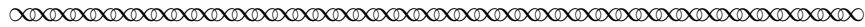
Fermat’s Little Theorem.

If p is prime and a is relatively prime to p , then p divides $a^{p-1} - 1$.

Pierre de Fermat (1601–1665) stated this result in 1640. Euler later gave several proofs of Fermat’s Little Theorem, his first in 1736.¹⁰

Lagrange claimed his own first proof of Wilson’s Theorem had the advantage of explicitly demonstrating the connection between Wilson’s Theorem and Fermat’s Little Theorem. Nonetheless, he provided a second proof of Wilson’s Theorem assuming Fermat’s Little Theorem.

Lagrange used the “theory of differences” for this second proof; he explained the necessary result:



We can deduce from the theorem of Mr. Fermat another proof of that of Mr. Wilson much simpler than the one we gave above.

Because, if we consider the [finite] sequence of natural numbers $1, 2, 3, \dots, n$ raised to the $(n - 1)^{\text{st}}$ power, and look for the $(n - 1)^{\text{st}}$ difference of the terms of this sequence, it is easy to see, by the theory of differences, that it will be

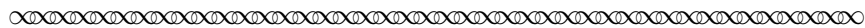
$$n^{n-1} - (n - 1)(n - 1)^{n-1} + \frac{(n - 1)(n - 2)}{2}(n - 2)^{n-1} - \frac{(n - 1)(n - 2)(n - 3)}{2 \cdot 3}(n - 3)^{n-1} + \dots + 1.$$

On the other hand, since the series

$$1, 2^{n-1}, 3^{n-1}, \dots$$

is an algebraic series of order $n - 1$, we know the difference of the same order will be expressed by the continual product of numbers $1, 2, 3, \dots, n - 1$; and thus we’ll have the equation

$$1 \cdot 2 \cdot 3 \cdot 4 \cdots (n - 1) = n^{n-1} - (n - 1)(n - 1)^{n-1} + \frac{(n - 1)(n - 2)}{2}(n - 2)^{n-1} - \frac{(n - 1)(n - 2)(n - 3)}{2 \cdot 3}(n - 3)^{n-1} + \dots + 1. \tag{1}$$



Task 2 Write 3–5 comments or questions (including at least one of each) about what Lagrange said in this excerpt. Try to include any connections you see to either Wilson’s Theorem or Fermat’s Little Theorem.

⁹That is, Lagrange showed that Fermat’s Little Theorem follows from his first proof of Wilson’s Theorem as a corollary.

¹⁰Gottfried Wilhelm Leibniz (1646–1716) was aware of Fermat’s result even earlier and perhaps had a proof, but didn’t publish one.

Before we move on, let's figure out what Lagrange was talking about. The “theory of differences” is best explained with an example. Consider the sequence of fourth powers:

$$1, 16, 81, 256, 625, 1296, \dots$$

The *first difference* is the sequence we obtain by taking the difference of successive terms:

$$15, 65, 175, 369, 671, \dots$$

Taking the difference of successive terms again will then give us the *second difference*, then the *third difference*, and so on. This process is nicely represented with a Pascal-like triangle:

1	16	81	256	625	1296	2401
	15	65	175	369	671	1105
		—	—	—	—	—
			—	—	—	
				—	—	

Task 3 Fill in the blanks above by computing the second, third, and fourth differences for this example.

If your computations were correct, then you'll have noticed that the fourth difference in this example is a constant sequence. This is true in general; that is, given any sequence $1^{n-1}, 2^{n-1}, 3^{n-1}, \dots$ of $(n-1)$ st powers, the $(n-1)$ st difference will be a constant sequence. This was well-known before Lagrange's time, as was the value of that constant.¹¹ Lagrange even told us what the constant value is, when he wrote:

“On the other hand, since the series $1, 2^{n-1}, 3^{n-1}, \dots$ is an algebraic series of order $n-1$, we know the difference of the same order [i.e., $n-1$] will be expressed by the continual product of numbers $1, 2, 3, \dots, n-1$.”

Task 4 Confirm that your computations in Task 3 are correct by checking the fourth difference against the value Lagrange indicated in the quote above.

¹¹For example, Leibniz discovered this and other interesting properties of sequence differences in his early work on calculus. In fact, he came up with his version of the Fundamental Theorem of Calculus by thinking about taking the sums of these differences.

Let's think about the details of the actual computation of the number in the fourth difference. The initial sequence is

$$1^4, 2^4, 3^4, 4^4, 5^4, \dots$$

So, the first difference is the sequence

$$2^4 - 1^4, 3^4 - 2^4, 4^4 - 3^4, 5^4 - 4^4, \dots$$

The second difference, after simplifying, is then the sequence

$$3^4 - 2 \cdot 2^4 + 1^4, 4^4 - 2 \cdot 3^4 + 2^4, 5^4 - 2 \cdot 4^4 + 3^4, \dots$$

Task 5 Give an expression for the number in the fourth difference in terms of $1^4, 2^4, 3^4, 4^4, 5^4$.

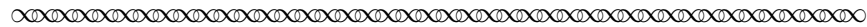
Hint: Start by expressing the first two numbers that appear in the third difference in terms of $1^4, 2^4, 3^4, 4^4, 5^4$. Then subtract those two expressions and simplify.

Task 6 Reconcile your results in Tasks 3 and 5 with the right side of the identity (1), which is restated here for your convenience.

$$1 \cdot 2 \cdot 3 \cdot 4 \cdots (n-1) = n^{n-1} - (n-1)(n-1)^{n-1} + \frac{(n-1)(n-2)}{2}(n-2)^{n-1} - \frac{(n-1)(n-2)(n-3)}{2 \cdot 3}(n-3)^{n-1} + \dots + 1 \quad (1)$$

Lagrange would have known the identity (1) from the theory of differences. It appeared in work done by Euler,¹² but it was probably known before Euler. We won't prove the identity here.

Up to this point, Lagrange's argument didn't depend on n being prime.¹³ In what follows, it will be important to remember that n is assumed to be a prime number. Lagrange continued his argument as follows.



Suppose now that we divide the second side of this equation [(1)] by n , and that we only want to keep track of the remainder that results. It is first of all clear that the term n^{n-1} will give a remainder of 0, and that the terms $(n-1)^{n-1}, (n-2)^{n-1}, \dots$ will all give a remainder of 1, by the theorem of Mr. Fermat. Thus, putting in the place of these terms their remainders 0, 1, 1, ... we'll have the total remainder

$$-(n-1) + \frac{(n-1)(n-2)}{2} - \frac{(n-1)(n-2)(n-3)}{2 \cdot 3} + \dots, \quad (2)$$

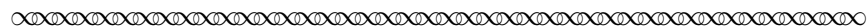
or rather

$$(1-1)^{n-1} - 1; \text{ that is, } -1. \quad (3)$$

Thus, the remainder of the division of $1 \cdot 2 \cdot 3 \cdots (n-1)$ by n will be -1 , and by consequence

$$1 \cdot 2 \cdot 3 \cdots (n-1) + 1$$

will always be divisible by n , provided that n is prime; which is exactly the condition needed to satisfy the theorem of Mr. Fermat.



¹²The result is included, for example, in the article [Euler, 1760]. In this paper, Euler proved that every prime of the form $4n+1$ is the sum of two squares.

¹³That is, the identity (1) is true for all values of n , whether they are prime or not.

Task 7 Write 3–5 comments or questions (including at least one of each) about what Lagrange said in this excerpt. Try to include any connections you see between Lagrange’s remark that “we only want to keep track of the remainder” and either Wilson’s Theorem or Fermat’s Little Theorem.

We’ll now work through the details in the last part of Lagrange’s argument.

First, recall that the **Division Theorem** says that 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*.

Task 8 Explain why “... the terms $(n - 1)^{n-1}, (n - 2)^{n-1}, \dots$ will all give a remainder of 1” using Fermat’s Little Theorem and writing an expression in the form of the Division Theorem.

Next, we need the **Binomial Theorem**. We’ll state it in the form we need:

$$(1 + x)^n = x^n + nx^{n-1} + \frac{n(n-1)}{2}x^{n-2} + \frac{n(n-1)(n-2)}{2 \cdot 3}x^{n-3} + \dots + nx + 1.$$

Task 9 Write the Binomial Theorem with $x = -1$ and replace n with $n - 1$.

It is common in number theory to treat the case of odd primes, and the case of $n = 2$ separately. We’ll do that here.

Task 10 Assume n is an odd prime. Use this fact to simplify the $(-1)^{n-k}$ factors in your answer to Task 9. Then, identify the part of the resulting expression that Lagrange showed is the remainder (2). Finally, show why the expression for the remainder given in (2) is equivalent to the expression given in (3).

Task 11 Rewrite “the remainder of the division of $1 \cdot 2 \cdot 3 \cdots (n - 1)$ by n will be -1 ” in the form of the Division Theorem.¹⁴ Show how this, finally, gives the divisibility statement in Wilson’s Theorem.

You can make a slight modification to the argument in Task 10 to treat the $n = 2$ case. It’s impossible to know from Lagrange’s paper, but I’d be surprised if this is what he had in mind. I suspect, as is the often the case, Lagrange quickly dismissed the $n = 2$ case and didn’t bother to mention it in his paper.

Task 12 Explain why Wilson’s Theorem holds for $n = 2$. *Hint:* You don’t need any of the development presented in the project or in Lagrange’s work.

¹⁴The Division Theorem can be equivalently stated with $-\frac{b}{2} \leq r < \frac{b}{2}$.

2 Conclusion

In this project, we have studied Lagrange’s proof of Wilson’s Theorem using Fermat’s Little Theorem as the starting point. The related project “Lagrange’s Proof of Wilson’s Theorem—and More!” [Lienert, 2023a] explores the other direction. That is, in the first part of the paper Lagrange proved Wilson’s Theorem without assuming Fermat’s Little Theorem *and* then showed that Fermat’s Little Theorem follows as a consequence. Thus, Lagrange demonstrated that Wilson’s Theorem and Fermat’s Little Theorem are, in a sense, equivalent. For completeness, we conclude with some brief information about Fermat’s Little Theorem, the importance of both Wilson’s and Fermat’s Little Theorem to mathematics, and a teaser about the other results in Lagrange’s paper.

2.1 Fermat and Fermat-Euler

The form of the theorem that Lagrange was interested in is:

Fermat’s Little Theorem.

If p is prime and a is relatively prime to p , then p divides $a^{p-1} - 1$.

A more general theorem, known as the Fermat-Euler Theorem, states the following:

Fermat-Euler Theorem.

If a and m are relatively prime, then m divides $a^{\phi(m)} - 1$, where $\phi(m)$ is the number of positive integers $0 < n \leq m$ that are relatively prime to m .

Task 13 Explain why the Fermat-Euler Theorem implies Fermat’s Little Theorem.

As mentioned earlier, Fermat stated his result in 1640, and Euler provided the first published proof in 1736. Somewhat later, Euler stated and proved the generalization in 1760. Here are two suggestions for learning more about the work of Fermat and Euler:

- Study the project “Primes, Factoring and Divisibility” [Klyve, 2017] which explores Euler’s first paper on number theory, entitled “Observations on a theorem of Fermat and others concerned with prime numbers” [Euler, 1738].
- Really get your hands dirty with one of Euler’s proofs. Dickson’s *History of the Theory of Numbers* [Dickson, 1919] outlines three of Euler’s proofs and indicates where they can be found. (Finding primary sources is part of the fun.) You may find “The Euler Archive” helpful.¹⁵

2.2 Connections

You might have noticed that “Wilson’s Theorem” was proved by Lagrange, but never by Wilson (or Waring). Similarly, “Fermat’s Little Theorem” was proved by Euler, and later by Lagrange, but never by Fermat. The development of mathematics is rarely about a single individual. The development and the naming of the results studied in this project illustrate this. If you do a quick Google search you’ll also discover that neither Euler nor Lagrange were the last to contribute proofs of these theorems. They certainly weren’t the last to use the results of these theorems to produce other

¹⁵<http://eulerarchive.maa.org/>

theorems. While Euler and Lagrange were certainly superstars in this development, the importance, and even existence, of their results depended on mathematicians that came both before and after.

Task 14 Look in a modern number theory or abstract algebra textbook and find one result that depends on Wilson’s Theorem and one that depends on Fermat’s Little Theorem.

2.3 And more ...

We have already mentioned the project “Lagrange’s Proof of Wilson’s Theorem—and More!” [Lienert, 2023a] which studies Lagrange’s main proof of Wilson’s Theorem and its implication of Fermat’s Little Theorem. Another part of Lagrange’s paper gave a proof of the converse of Wilson’s Theorem. You can study that proof in the project “Lagrange’s Proof of the Converse of Wilson’s Theorem” [Lienert, 2023b]. And, for those who read French, Lagrange also gave a discussion about primes in arithmetic series, which can be found in Remark III of his paper [Lagrange, 1771].

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/.
- Leonard Eugene Dickson. *History of the Theory of Numbers, Volume 1: Divisibility and Primality*. Carnegie Institute of Washington, Washington DC, 1919. Republished by AMS Chelsea Publishing, Providence RI, 1966, and by Dover, Mineola MN, 2005.
- Leonhard Euler. Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus (Observations on a theorem of Fermat and others concerned with prime numbers). *Commentarii academiae scientiarum Petropolitanae*, 6:103–107, 1738. Also in *Leonhardi Euleri Opera Omnia*, series 1, volume 2, pages 1–5.
- Leonhard Euler. Demonstratio theorematis Fermatiani omnem numerum primum formae $4n + 1$ esse summam duorum quadratorum (Proof of a theorem of Fermat that every prime number of the form $4n + 1$ is the sum of two squares). *Novi Commentarii academiae scientiarum Petropolitanae*, 5:pp. 3–13, 1760. Also in *Leonhardi Euleri Opera Omnia*, series 1, volume 2, pages 328–337.
- Dominic Klyve. Primes, Divisibility, and Factoring. 2017. Primary Source Project available at https://digitalcommons.ursinus.edu/triumphs_number/1/.
- 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 Proof of the Converse of Wilson’s Theorem. 2023b. Primary Source Project available at https://digitalcommons.ursinus.edu/triumphs_number/15/.

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 works through Lagrange’s proof of Wilson’s Theorem with Fermat’s Little Theorem as starting point. Lagrange’s proof uses differences of sequences. This topic is perhaps not typically known to modern students (it wasn’t to me when I first read the paper), but the necessary explanation is included. We do not include a proof of the required identity, but use it as known, as Lagrange would have in this instance.

In his 1771 paper, Lagrange also gave another proof of Wilson’s Theorem, based on an argument involving binomial coefficients from which he was also able to deduce Fermat’s Little Theorem. That portion of his paper is featured in the related PSP “Lagrange Proves Wilson’s Theorem—and More!” He also gave a proof of the converse of Wilson’s Theorem, which is featured in the related PSP “Lagrange’s Proof of the Converse of Wilson’s Theorem.” The projects in this trio are independent of each other. While they can also be implemented in any order, instructors who choose to implement the project 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). 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 Number Theory class. 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 stated at the appropriate juncture in a form that will be understandable even to students who have not formally seen it yet. The Binomial Theorem is needed, and is stated in the project in the form in which it is needed. The project avoids factorial notation, binomial coefficient notation, $\binom{n}{k}$, and congruence notation because all of these were developed after Lagrange.

PSP Design and Task Commentary

The project begins with a short historical introduction. It then presents Lagrange’s proof of Wilson’s Theorem starting from Fermat’s Little Theorem and using the “theory of differences.” Students need to think carefully about the identity (1) that Lagrange used here. This proof also illustrates a common technique: expanding $(1 - 1)^n$.

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.

L^AT_EX 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 PSP is a one or two day activity. As advance preparation, ask students to read the text and complete the tasks up to, and including, Task 3 as homework the day before the project is completed in class. At the end of the first class day assign the next task or two depending on where class ends.

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’s 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 L^AT_EX 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 Proof of the Converse of Wilson’s Theorem*, Carl Lienert (1 day)
Based on the same paper as the current PSP. Gives Lagrange’s proof of the converse to Wilson’s Theorem.
- *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.



With the exception of excerpts taken from published translations of the primary sources used in this project and any direct quotes from published secondary sources, this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (<https://creativecommons.org/licenses/by-sa/4.0/legalcode>). It allows re-distribution and re-use of a licensed work on the conditions that the creator is appropriately credited and that any derivative work is made available under “the same, similar or a compatible license.”

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